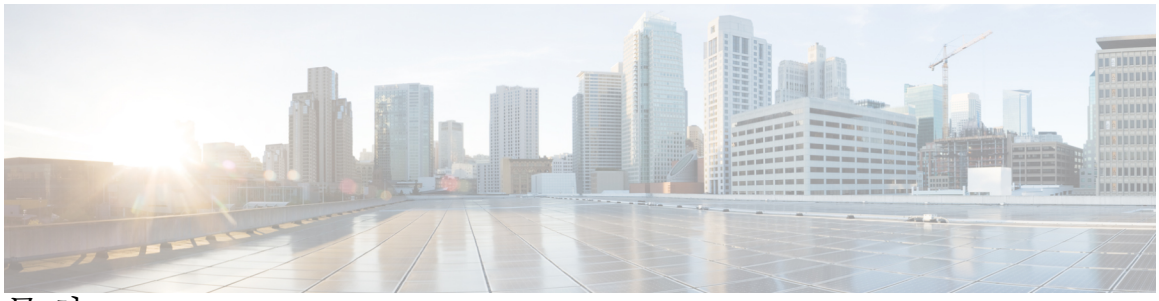
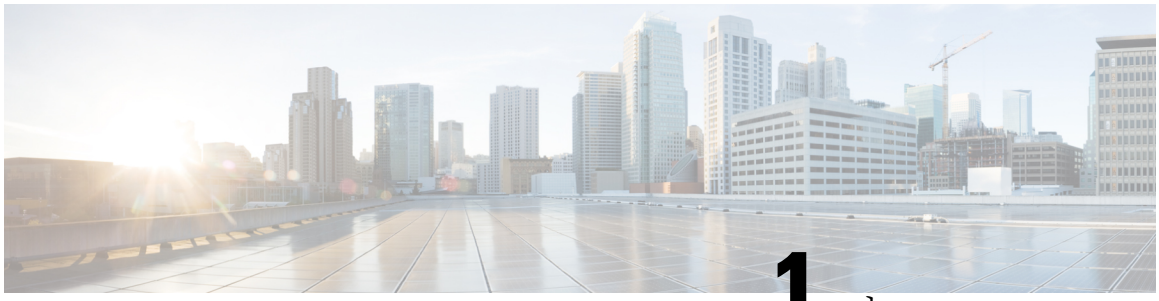
Cisco Secure Firewall Device Manager 구성 가이드, 버전 7.2

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



목 차



1 장

시작하기

다음 주제에서는 Secure Firewall Threat Defense(이전 Firepower Threat Defense) 컨피그레이션을 시작하는 방법을 설명합니다.

가이드의 적합성 확인

이 가이드에서는 threat defense 디바이스에 포함된 Secure Firewall Device Manager(이전 Firepower Device Manager) 웹 기반 컨피그레이션 인터페이스를 사용하여 threat defense를 컨피그레이션하는 방법을 설명합니다.

device manager 사용을 통해 중소규모 네트워크에서 가장 흔히 사용되는 소프트웨어의 기본 기능을 구성할 수 있습니다. Firepower Device Manager는 디바이스를 하나 또는 몇 개만 포함하는 네트워크 용도로 특별히 설계되어 고성능 다중 디바이스 관리자를 사용해 여러 threat defense 디바이스가 포함된 대규모 네트워크를 제어하기를 원하지 않을 경우에 유용합니다.

다수의 디바이스를 관리하거나 threat defense에서 허용하는 더 복잡한 기능 및 컨피그레이션을 사용하려는 경우에는 통합형 device manager 대신 Secure Firewall Management Center(이전 Firepower Management Center)를 사용하여 디바이스를 컨피그레이션하십시오.

다음 디바이스에서 device manager를 사용할 수 있습니다.

표 ***1: Device Manager*** 지원 모델

디바이스 모델	최소 **Threat Defense** 소프트웨어 버전
Firepower 1010, 1120, 1140	6.4
Firepower 1150	6.5

디바이스 모델	최소 **Threat Defense** 소프트웨어 버전
Firepower 2110, 2120, 2130, 2140	6.2.1
Secure Firewall 3110, 3120, 3130, 3140	7.1
Firepower 4110, 4115, 4120, 4125, 4140, 4145, 4150	6.5
Firepower 4112	6.6
Firepower 9300	6.5
VMware용 Threat Defense Virtual	6.2.2
Threat Defense Virtual KVM(Kernel-based Virtual Machine) 하이퍼바이저용	6.2.3
Threat Defense Virtual - Microsoft Azure Cloud용	6.5
Threat Defense Virtual - AWS(Amazon Web Services) Cloud용	6.6
ISA 3000(Cisco 3000 Series Industrial Security Appliances)	6.2.3

Device Manager/Threat Defense 버전 7.2.0의 새로운 기능

릴리스 날짜**: 2022**년 **6**월

다음 표에는 device manager를 사용하여 구성하면 사용할 수 있는 threat defense 7.2.0의 새로운 기능이 나와 있습니다.

기능	설명
방화벽 및 **IPS** 기능	
개체 그룹 검색은 액세스 제어에 대해 기본적으로 활성화되어 있습니다.	이제 CLI 구성 명령 **object-group-search access-control**이 기본적으로 활성화됩니다. FlexConfig를 사용하여 명령을 구성하는 경우 FlexConfig 개체를 제거할 수 있습니다. 기능을 비활성화해야 하는 경우 FlexConfig를 사용하여 **no object-group-search access-control** 명령을 구현합니다. 자세한 내용은 https://www.cisco.com/c/en/us/td/docs/security/asa/asa-cli-reference/I-R/asa-command-ref-I-R/o-commands.html#wp1852298285를 참고하십시오.

기능	설명
규칙 적중 횟수는 재부팅 후에도 유지됩니다.	디바이스를 재부팅해도 더 이상 액세스 제어 규칙 적중 횟수가 0으로 재설정되지 않습니다. 적중 횟수는 카운터를 직접 지우는 경우에만 재설정됩니다. 또한 개수는 HA 쌍 또는 클러스터의 각 유닛에서 개별적으로 유지 관리됩니다. **show rule hits** 명령을 사용하여 HA 쌍 또는 클러스터 전체에서 누적 카운터를 보거나 노드당 카운트를 확인할 수 있습니다. 다음 threat defense CLI 명령 **show rule hits**을 수정했습니다. 자세한 내용은 https://www.cisco.com/c/en/us/td/docs/security/firepower/720/fdm/fptd-fdm-config-guide-720/fptd-fdm-access.html#id_92394를 참고하십시오.
VPN 기능	
IPsec 플로우 오프로드.	Secure Firewall 3100에서 IPsec 플로우는 기본적으로 오프로드됩니다. IPsec 사이트 간 VPN 또는 원격 액세스 VPN 보안 연계(SA)의 초기 설정 후 IPsec 연결은 디바이스의 FTPA(field-programmable gate Array)로 오프로드되므로 디바이스 성능이 향상됩니다. FlexConfig 및 **flow-offload-ipsec** 명령을 사용하여 구성을 변경할 수 있습니다. 자세한 내용은 https://www.cisco.com/c/en/us/td/docs/security/firepower/720/fdm/fptd-fdm-config-guide-720/fptd-fdm-s2svpn.html#Cisco_Concept.dita_83d8d2c7-8a9c-4094-9649-91744c9fff06를 참고하십시오.
인터페이스 기능	
Secure Firewall 3130 및 3140에 대한 브레이크아웃 포트 지원	이제 Secure Firewall 3130 및 3140에서 각 40GB 인터페이스에 대해 10GB 브레이크아웃 포트 4개를 구성할 수 있습니다. 신규/수정된 화면: • **Devices(**디바이스**)** > **Interfaces(**인터페이스**)** 자세한 내용은 https://www.cisco.com/c/en/us/td/docs/security/firepower/720/fdm/fptd-fdm-config-guide-720/fptd-fdm-interfaces.html#Cisco_Concept.dita_14e59bb1-dd81-455d-bf70-f26fa2cc097e를 참고하십시오.
인터페이스에서 Cisco Trustsec 활성화 또는 비활성화.	물리적, 하위 인터페이스, EtherChannel, VLAN, 관리 또는 BVI 인터페이스(명명 여부에 관계없이)에서 Cisco Trustsec을 활성화하거나 비활성화할 수 있습니다. 기본적으로 Cisco Trustsec은 인터페이스의 이름을 지정할 때 자동으로 활성화됩니다. **Propagate Security Group Tag(**보안 그룹 태그 전파**)** 속성을 인터페이스 구성 대화 상자에 추가하고 **ctsEnabled** 속성을 다양한 인터페이스 API에 추가했습니다. 자세한 내용은 https://www.cisco.com/c/en/us/td/docs/security/firepower/720/fdm/fptd-fdm-config-guide-720/fptd-fdm-interfaces.html#task_D0C0FB15621B4F49B29CB010F7D6C2D1를 참고하십시오.
라이선싱 기능	

기능	설명
ISA 3000 영구 라이선스 예약 지원.	이제 ISA 3000은 승인된 고객에 대해 범용 영구 라이선스 예약을 지원합니다. 자세한 내용은 https://www.cisco.com/c/en/us/td/docs/security/firepower/720/fdm/fptd-fdm-config-guide-720/fptd-fdm-license.html#id_123878를 참고하십시오.
관리 및 트러블슈팅 기능	
전체 구축을 강제 실행하는 기능이 있습니다.	변경 사항을 구축할 때 시스템은 일반적으로 마지막 구축 이후의 변경 사항만 구축합니다. 그러나 문제가 발생하는 경우 전체 구축을 강제로 선택하여 디바이스의 구성을 완전히 새로 고칠 수 있습니다. 구축 대화 상자에 **Apply Full Deployment(**전체 구축 적용**)** 옵션을 추가했습니다. 자세한 내용은 https://www.cisco.com/c/en/us/td/docs/security/firepower/720/fdm/fptd-fdm-config-guide-720/fptd-fdm-get-started.html#task_BEE4E37389B64E518EE91FF3824476A9를 참고하십시오.
Threat Defense REST API 버전 6.3(v6).	소프트웨어 버전 7.2에 대한 threat defense REST API는 6.3 버전입니다. API URL의 v6를 사용하거나 /latest/를 사용하여 디바이스에서 지원되는 가장 최신 API 버전을 사용하고 있음을 나타내는 것이 좋습니다. 6.3의 URL 버전 경로 요소는 6.0, 6.1, 6.2와 동일한 v6입니다. 사용 중인 리소스 모델에 변경 사항이 적용되었을 수 있으므로 모든 기존 호출을 다시 평가하십시오. 리소스를 확인할 수 있는 API Explorer를 열려면 device manager에 로그인한 다음, More options(추가 옵션) 버튼( )을 클릭하고 **API Explorer**를 선택합니다. 자세한 내용은 https://www.cisco.com/c/en/us/td/docs/security/firepower/ftd-api/guide/ftd-rest-api.html를 참고하십시오.

시스템 로그인

threat defense 디바이스에 대한 인터페이스는 다음과 같이 두 개입니다.

Device Manager 웹 인터페이스

device manager가 웹 브라우저에서 실행됩니다. 이 인터페이스를 사용하여 시스템을 구성, 관리 및 모니터링합니다.

CLI(Command Line Interface, 콘솔**)**

CLI는 트러블슈팅에 사용합니다. device manager 대신 초기 설정에 사용할 수 있습니다.

다음 주제에서는 이러한 인터페이스에 로그인하고 사용자 어카운트를 관리하는 방법을 설명합니다.

볼 수 있는 정보와 수행할 수 있는 작업을 제어하는 사용자 역할

사용자 이름에는 역할이 할당되며, 역할에 따라 device manager에서 수행할 수 있는 작업이나 볼 수 있는 정보가 결정됩니다. 로컬 정의 관리 사용자에게는 모든 권한이 있지만 다른 어카운트를 사용하여 로그인하는 경우 권한이 줄어들 수 있습니다.

device manager 창의 오른쪽 상단 모서리에 사용자 이름과 권한 레벨이 표시됩니다.

권한은 다음과 같습니다.

- **Administrator(**관리자**)** - 모든 기능을 보고 사용할 수 있습니다.
- **Read-Write User(**읽기-쓰기 사용자**)** - 읽기 전용 사용자가 수행할 수 있는 모든 작업을 수행할 수 있으며 컨피그레이션 수정 및 구축도 수행할 수 있습니다. 업그레이드 설치, 백업 생성 및 복원, 감사 로그 확인, 다른 device manager 사용자의 세션 종료를 포함하는 시스템의 중요 작업만 제한됩니다.
- **Read-Only User(**읽기 전용 사용자**)** - 대시보드 및 컨피그레이션을 볼 수는 있지만 변경할 수는 없습니다. 변경을 시도하면 권한이 없음을 설명하는 오류 메시지가 표시됩니다.

이러한 권한은 CLI 사용자에게 제공되는 권한과는 관련이 없습니다.

Device Manager에 로그인

device manager을 사용하여 시스템을 구성, 관리 및 모니터링합니다. 브라우저를 통해 구성할 수 있는 기능은 CLI(Command Line Interface)를 통해서는 구성할 수 없습니다. 즉, 반드시 웹 인터페이스를 사용하여 보안 정책을 구현해야 합니다.

아래 브라우저의 최신 버전인 Firefox, Chrome, Safari, Edge를 사용하십시오.

참고 잘못된 비밀번호를 입력하고 3회 연속하여 로그인 시도에 실패할 경우, 5분 동안 어카운트가 잠깁니다. 따라서 다시 로그인을 시도하기 전에 잠시 기다려야 합니다.

시작하기 전에

처음에는 관리자 사용자 이름만 사용하여 device manager에 로그인할 수 있습니다. 그러나 첫 로그인 이후에는 Device Manager 및 Threat Defense 사용자 액세스 관리, 878 페이지의 설명에 따라 외부 AAA 서버에 정의된 추가 사용자에 대해 인증을 구성할 수 있습니다.

액티브 로그인은 한 번에 최대 5개까지 가능합니다. 여기에는 만료되지 않은 API 토큰으로 표시되는 디바이스 관리자 및 액티브 API 세션에 로그인한 사용자가 포함됩니다. 이 제한을 초과하면 가장 오래된 세션인 디바이스 관리자 로그인 또는 API 토큰이 만료되어 새 세션을 허용합니다. 이러한 제한은 SSH 세션에 적용되지 않습니다.

프로시저

단계 **1** 브라우저를 사용하여 시스템의 홈페이지(예: https://ftd.example.com)를 엽니다.

다음 주소 중 하나를 사용할 수 있습니다. IPv4 또는 IPv6 주소나 DNS 이름(구성한 경우)을 사용할 수 있습니다.

- 관리 주소. 기본적으로 대부분의 플랫폼에서 관리 인터페이스는 DHCP 클라이언트이므로 IP 주소는 DHCP 서버에 따라 달라집니다.
- HTTPS 액세스를 위해 연 데이터 인터페이스의 주소. 기본적으로 대부분의 플랫폼에서, "내부" 인터페이스는 HTTPS 액세스를 허용하므로 기본 내부 주소 192.16895.1에 연결할 수 있습니다. 모델의 내부 IP 주소에 대한 자세한 내용은 초기 설정 전의 기본 컨피그레이션, 24 페이지를 참조하십시오.

  HTTPS 데이터 포트를 변경한 경우 URL에 맞춤형 포트를 포함해야 합니다. 예를 들어 포트를 4443으로 변경한 경우: https://ftd.example.com:4443과 같습니다.

팁 브라우저가 서버 인증서를 인식하도록 구성되어 있지 않으면 신뢰할 수 없는 인증서에 대한 경고가 표시됩니다. 해당 인증서를 예외적으로 수락하거나 신뢰할 수 있는 루트 인증서 저장소에 저장하십시오.

단계 **2** 디바이스용으로 정의된 사용자 이름 및 비밀번호를 입력한 다음 **Login(**로그인**)**을 클릭합니다.

미리 정의된 사용자인 관리 사용자 이름을 사용할 수 있습니다. 기본 관리자 비밀번호는 Admin123입니다. 초기 구축 중에 사용자 데이터(**Advanced Details(**고급 세부 정보**)** > **User Data(**사용자 데이터**)**)로 기본 비밀번호를 정의하지 않는 한 AWS에서 기본 관리자 비밀번호는 AWS 인스턴스 ID입니다.

비활성 상태가 30분 동안 유지되면 세션이 만료되며, 다시 로그인하라는 메시지가 표시됩니다. 페이지 오른쪽 상단에 있는 사용자 아이콘 드롭다운 메뉴에서 **Log Out(**로그아웃**)**을 선택하면 로그아웃할 수 있습니다.

CLI(Command Line Interface) 로그인

CLI(Command Line Interface)를 사용하여 시스템을 설정하고 기본적인 시스템 트러블슈팅을 수행합니다. CLI 세션을 통해 정책을 구성할 수는 없습니다.

CLI에 로그인하려면 다음 중 하나를 수행합니다.

- 디바이스에 포함된 콘솔 케이블을 사용하여 PC를 콘솔에 연결합니다(터미널 에뮬레이터 9600 보드, 8 데이터 비트, 패리티 없음, 1 정지 비트, 흐름 제어 없음). 콘솔 케이블에 대한 자세한 내용은 디바이스용 하드웨어 가이드를 참조하십시오.

참고 Firepower 및 Secure Firewall 디바이스 모델에서 콘솔 포트의 CLI는 Secure Firewall eXtensible Operating System(FXOS)입니다. Firepower 1000/2100, 의 경우 **connect ftd** 명령을 사용하여 threat defense CLI에 액세스할 수 있습니다. Firepower 4100/9300의 경우, 애플리케이션 콘솔에 연결, 207 페이지의 내용을 참조하십시오. FXOS CLI는 새시 레벨 트러블슈팅에만 사용하십시오. 기본 컨피그레이션, 모니터링 및 일반 시스템 트러블슈팅 시에는 threat defense CLI를 사용합니다. FXOS 명령에 대한 자세한 내용은 FXOS 설명서를 참조하십시오.

- threat defense virtual의 경우에는 가상 콘솔을 여십시오.
- 관리 IP 주소에 연결하려면 SSH 클라이언트를 사용합니다. SSH 연결용 인터페이스를 여는 경우 데이터 인터페이스의 주소에 연결할 수도 있습니다(관리 액세스 목록 구성, 810 페이지 참조). 데이터 인터페이스에 대한 SSH 액세스는 기본값으로 비활성화 상태입니다. 사용자 이름 **admin** 또는 다른 CLI 사용자 계정을 사용하여 로그인합니다. 기본 관리자 비밀번호는 Admin123입니다. AWS에서 구축 중에 사용자 데이터(**Advanced Details(**고급 세부 정보**)** > **User Data(**사용자 데이터**)**)로 기본 비밀번호를 정의하지 않은 경우 threat defense virtual에 대한 기본 관리자 비밀번호는 AWS 인스턴스 ID입니다.

팁

- 로그인한 후 CLI에서 사용할 수 있는 명령에 대한 정보를 확인하려면 **help** 또는 **?**를 입력하십시오. 사용 정보는 http://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.html에서 Cisco Firepower Threat Defense 명령 참조를 참조하십시오.
- **configure user add** 명령을 사용하면 CLI에 로그인할 수 있는 로컬 사용자 계정을 생성할 수 있습니다. 그러나 이러한 사용자는 CLI에만 로그인할 수 있으며 device manager 웹 인터페이스에 로그인합니다.
- 외부 서버에서 SSH 액세스하기 위한 용도로 사용자 계정을 생성할 수 있습니다. SSH 액세스를 위한 외부 인증 컨피그레이션에 대한 내용은 Threat Defense CLI(SSH) 사용자를 위한 외부 권한 부여(AAA) 구성, 881 페이지를 참조하십시오.

비밀번호 변경

비밀번호는 정기적으로 변경해야 합니다. 다음 절차에서는 device manager에 로그인한 상태에서 비밀번호를 변경하는 방법을 설명합니다.

참고 CLI에 로그인한 경우 **configure password** 명령을 사용하여 암호를 변경할 수 있습니다. **configure user password** *username* 명령을 사용해 다른 CLI 사용자의 암호를 변경할 수 있습니다.

시작하기 전에

이 절차는 로컬 사용자에게만 적용됩니다. 사용자 어카운트가 외부 AAA 서버에 정의되어 있는 경우에는 해당 서버를 사용하여 비밀번호를 변경해야 합니다.

프로시저

단계 **1** 메뉴 오른쪽 위에 있는 사용자 아이콘 드롭다운 목록에서 **Profile(**프로파일**)**을 선택합니다.

단계 **2** **Password(**비밀번호**)** 탭을 클릭합니다.

단계 **3** 현재 비밀번호를 입력합니다.

단계 **4** 새 비밀번호를 입력하고 확인을 위해 다시 한 번 입력합니다.

Generate(생성**)**를 클릭하여 임의의 16자 비밀번호를 생성할 수 있습니다. 마스크 해제된 비밀번호를 보려면 Show Password(비밀번호 표시) () 버튼을 클릭합니다. 그런 다음 **Copy To Clipboard(**클립보드에 복사**)** 링크를 클릭하여 확인 필드에 비밀번호를 붙여넣을 수 있습니다.

단계 **5** **Change(**변경**)**를 클릭합니다.

사용자 프로파일 환경 설정 지정

사용자 인터페이스의 기본 설정을 설정하고 비밀번호를 변경할 수 있습니다.

프로시저

단계 **1** 메뉴 오른쪽 위에 있는 사용자 아이콘 드롭다운 목록에서 **Profile(**프로파일**)**을 선택합니다.

단계 **2** **Profile(**프로파일**)** 탭에서 다음 항목을 구성하고 **Save(**저장**)**를 클릭합니다.

- 작업 예약을 위한 시간대 - 백업 및 업데이트와 같은 작업을 예약하는 데 사용할 시간대를 선택합니다. 다른 시간대를 설정하는 경우 대시보드와 이벤트에 브라우저 시간대가 사용됩니다.
- 색 구성표 - 사용자 인터페이스에 사용할 색 구성표를 선택합니다.

단계 **3** **Password(**비밀번호**)** 탭에서 새 비밀번호를 입력하고 **Change(**변경**)**를 클릭할 수 있습니다.

시스템 설정

초기 컨피그레이션을 완료해야 네트워크에서 시스템이 정상적으로 작동합니다. 올바른 배포에는 케이블을 적절하게 연결하는 작업과 디바이스를 네트워크에 삽입하고 인터넷 또는 기타 업스트림 라우터에 연결하는 데 필요한 주소를 구성하는 작업이 포함됩니다. 다음 절차에서는 이러한 프로세스에 대해 설명합니다.

시작하기 전에

초기 설정을 시작하기 전에 디바이스에는 일부 기본 설정이 포함되어 있습니다. 자세한 내용은 초기 설정 전의 기본 컨피그레이션, 24 페이지를 참조해 주십시오.

프로시저

단계 **1** 인터페이스 연결, 9 페이지

단계 **2** 설정 마법사를 사용하여 초기 컨피그레이션 완료, 20 페이지

이 프로세스의 결과로 생성되는 컨피그레이션에 대한 자세한 내용은 초기 설정 후의 컨피그레이션, 27 페이지를 참조하십시오.

인터페이스 연결

기본 컨피그레이션에서는 특정 인터페이스가 내부 및 외부 네트워크에 사용된다고 가정합니다. 이러한 가정에 따라 인터페이스에 네트워크 케이블을 연결하면 초기 컨피그레이션을 더욱 쉽게 완료할 수 있습니다.

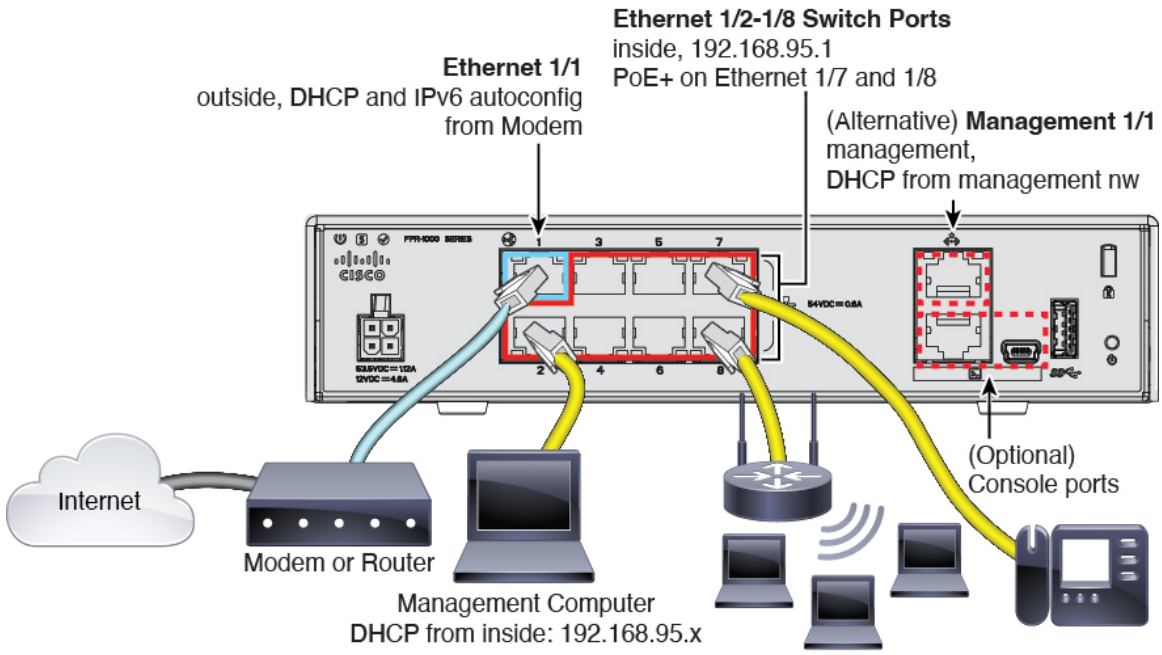
대부분 모델의 기본 컨피그레이션에서는 내부 인터페이스에 관리 컴퓨터를 연결할 수 있습니다. 워크스테이션을 관리 포트에 직접 연결할 수도 있습니다. 인터페이스는 서로 다른 네트워크에 있으므로 내부 인터페이스와 관리 포트를 같은 네트워크에 연결하지 마십시오.

활성 DHCP 서버가 있는 네트워크에 또는 내부 인터페이스를 연결하지 마십시오. 이와 같이 연결하면 내부 인터페이스에서 이미 실행 중인 DHCP 서버와 충돌하게 됩니다. 네트워크에 다른 DHCP 서버를 사용하려면 초기 설정 후 원치 않는 DHCP 서버를 비활성화하십시오.

다음 항목에서는 내부 인터페이스를 사용하여 디바이스를 구성할 때 이 토폴로지에 대해 시스템을 케이블 연결하는 방법을 설명합니다.

Firepower 1010 케이블 연결

그림 *1: Firepower 1010* 케이블 연결



- 다음 인터페이스 중 하나에 관리 컴퓨터를 연결합니다.
  - Ethernet 1/2~1/8 — 관리 컴퓨터를 내부스위치 포트(Ethernet 1/2~1/8) 중 하나에 직접 연결합니다. 내부에는 기본 IP 주소(192.168.95.1)가 있으며, DHCP 서버를 실행하여 클라이언트(관리 컴퓨터 포함)에 IP 주소를 제공하므로 이러한 설정이 기존의 내부 네트워크 설정과 충돌하지 않도록 합니다.
  - Management 1/1 — 관리 컴퓨터를 관리 네트워크에 연결합니다. Management 1/1 인터페이스는 DHCP에서 IP 주소를 가져오므로, 네트워크에 DHCP 서버가 포함되어 있어야 합니다.

    Management 1/1 IP 주소를 기본값에서 변경하여 정적 IP 주소를 구성해야 할 경우, 관리 컴퓨터도 콘솔 포트에 연결해야 합니다. (선택 사항) CLI에서 관리 네트워크 설정 변경, 19 페이지의 내용을 참조하십시오.

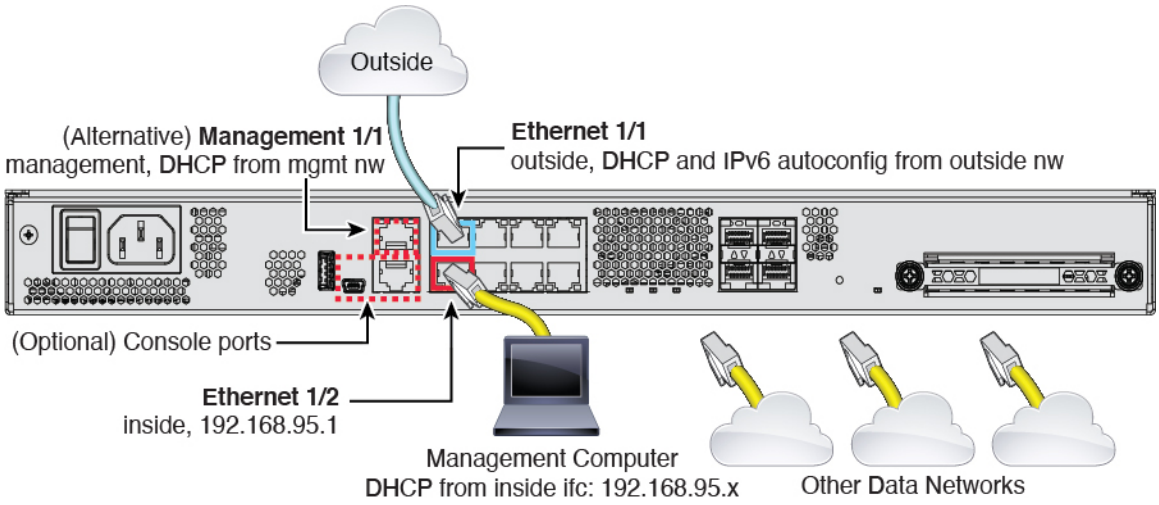
  나중에 다른 인터페이스에서 관리 액세스를 구성할 수 있습니다.
- 외부 네트워크를 Ethernet 1/1 인터페이스에 연결합니다.

  기본적으로는 IPv4 DHCP 및 IPv6 자동 설정을 사용하여 IP 주소를 가져오지만 초기 설정 중에 고정 주소를 설정할 수 있습니다.
- 나머지 스위치 포트(Ethernet 1/2~1/8)에 내부 디바이스를 연결합니다.

  Ethernet 1/7 및 1/8은 PoE+(Power over Ethernet+) 포트입니다.

Firepower 1100 케이블 연결

그림 *2: Firepower 1100* 케이블 연결



- 다음 인터페이스 중 하나에 관리 컴퓨터를 연결합니다.
  - Ethernet 1/2 — 관리 컴퓨터를 초기 컨피그레이션용 Ethernet 1/2에 직접 연결하거나, Ethernet 1/2를 내부 네트워크에 연결합니다. Ethernet 1/2에는 기본 IP 주소 (192.168.95.1)가 있는 Ethernet 1/2에서는 DHCP 서버를 실행하여 클라이언트(관리 컴퓨터 포함)에 IP 주소를 제공하므로 이러한 설정이 기존의 내부 네트워크 설정과 충돌하지 않도록 합니다.
  - Management 1/1(MGMT로 레이블이 지정됨) — 관리 컴퓨터를 관리 네트워크에 연결합니다. Management 1/1 인터페이스는 DHCP에서 IP 주소를 가져오므로, 네트워크에 DHCP 서버가 포함되어 있어야 합니다.

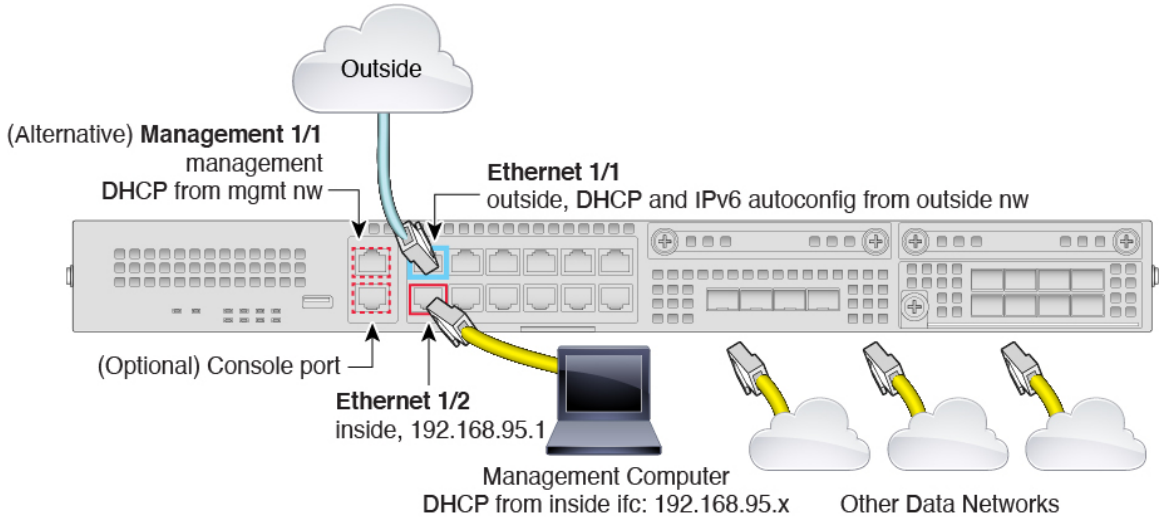
    Management 1/1 IP 주소를 기본값에서 변경하여 정적 IP 주소를 구성해야 할 경우, 관리 컴퓨터도 콘솔 포트에 연결해야 합니다. (선택 사항) CLI에서 관리 네트워크 설정 변경, 19 페이지의 내용을 참조하십시오.

  나중에 다른 인터페이스에서 관리 액세스를 구성할 수 있습니다.
- 외부 네트워크를 Ethernet1/1 인터페이스(WAN으로 레이블이 지정됨)에 연결합니다.

  기본적으로는 IPv4 DHCP 및 IPv6 자동 설정을 사용하여 IP 주소를 가져오지만 초기 설정 중에 고정 주소를 설정할 수 있습니다.
- 나머지 인터페이스에 다른 네트워크를 연결합니다.

Firepower 2100 케이블 연결

그림 *3: Firepower 2100* 케이블 연결



- 다음 인터페이스 중 하나에 관리 컴퓨터를 연결합니다.
  - Ethernet 1/2 — 관리 컴퓨터를 초기 컨피그레이션용 Ethernet 1/2에 직접 연결하거나, Ethernet 1/2를 내부 네트워크에 연결합니다. Ethernet 1/2에는 기본 IP 주소 (192.168.95.1)가 있고, DHCP 서버를 실행하여 클라이언트(관리 컴퓨터 포함)에 IP 주소를 제공하므로 이러한 설정이 기존의 내부 네트워크 설정과 충돌하지 않도록 합니다.
  - Management 1/1(MGMT로 레이블이 지정됨) — 관리 컴퓨터를 관리 네트워크에 연결합니다. Management 1/1 인터페이스는 DHCP에서 IP 주소를 가져오므로, 네트워크에 DHCP 서버가 포함되어 있어야 합니다.

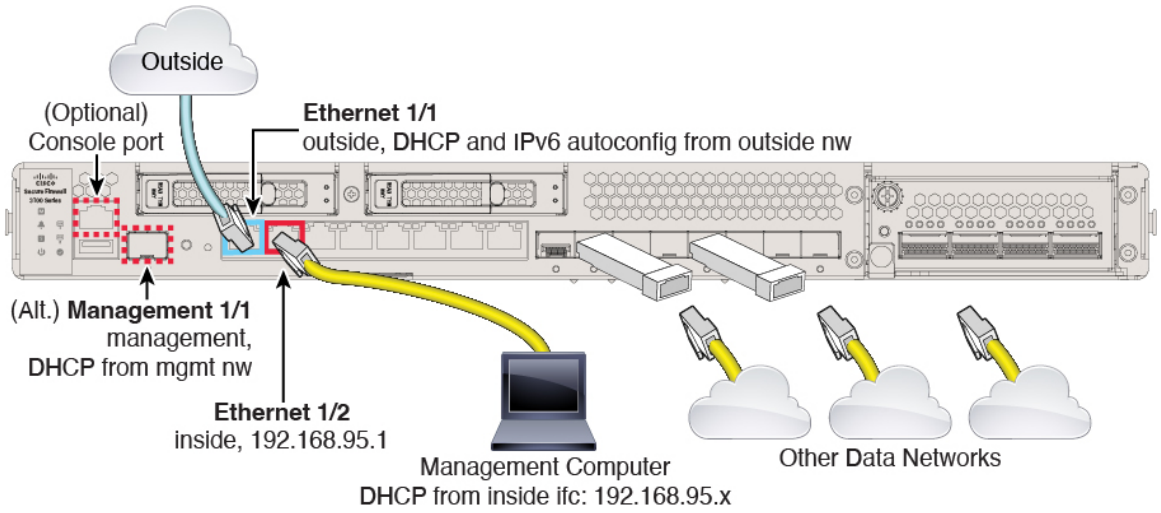
    Management 1/1 IP 주소를 기본값에서 변경하여 정적 IP 주소를 구성해야 할 경우, 관리 컴퓨터도 콘솔 포트에 연결해야 합니다. (선택 사항) CLI에서 관리 네트워크 설정 변경, 19 페이지의 내용을 참조하십시오.

  나중에 다른 인터페이스에서 관리 액세스를 구성할 수 있습니다.
- 외부 네트워크를 Ethernet1/1 인터페이스(WAN으로 레이블이 지정됨)에 연결합니다.

  기본적으로는 IPv4 DHCP 및 IPv6 자동 설정을 사용하여 IP 주소를 가져오지만 초기 설정 중에 고정 주소를 설정할 수 있습니다.
- 나머지 인터페이스에 다른 네트워크를 연결합니다.

Secure Firewall 3100 케이블 연결

그림 *4: Secure Firewall 3100* 케이블 연결



관리 1/1 또는 이더넷 1/2에서 threat defense 디바이스를 관리합니다. 기본 구성에서는 Ethernet1/1을 외부로도 구성합니다.

- 다음 인터페이스 중 하나에 관리 컴퓨터를 연결합니다.
  - Ethernet 1/2 — 관리 컴퓨터를 초기 컨피그레이션용 Ethernet 1/2에 직접 연결하거나, Ethernet 1/2를 내부 네트워크에 연결합니다. 기본 IP 주소(192.168.95.1)가 있는 이더넷 1/2에서는 DHCP 서버를 실행하여 클라이언트(관리 컴퓨터 포함)에 IP 주소를 제공하므로, 이러한 설정이 기존의 내부 네트워크 설정과 충돌하지 않도록 합니다.
  - 관리 1/1—관리 1/1을 관리 네트워크에 연결하고 관리 컴퓨터가 켜져 있는지, 또는 관리 네트워크에 대한 액세스 권한이 있는지 확인합니다. 관리 1/1은 관리 네트워크의 DHCP 서버에서 IP 주소를 가져옵니다. 이 인터페이스를 사용하는 경우 관리 컴퓨터에서 해당 IP 주소에 연결할 수 있도록 방화벽에 할당된 IP 주소를 확인해야 합니다.

    Management 1/1 IP 주소를 기본값에서 변경하여 정적 IP 주소를 구성해야 할 경우, 관리 컴퓨터도 콘솔 포트에 연결해야 합니다. (선택 사항) CLI에서 관리 네트워크 설정 변경, 19 페이지의 내용을 참조하십시오.

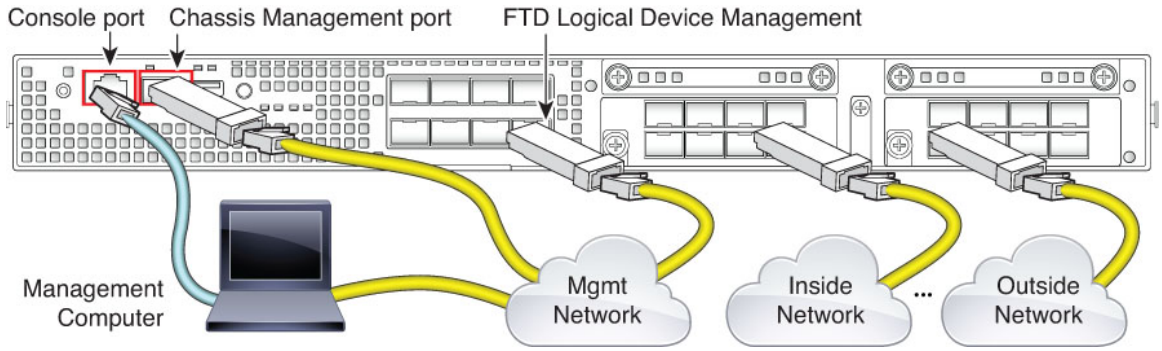
참고 관리 1/1은 SFP 모듈이 필요한 10Gb 파이버 인터페이스입니다.

- Ethernet1/1 인터페이스에 외부 네트워크를 연결합니다.

  기본적으로는 IPv4 DHCP 및 IPv6 자동 설정을 사용하여 IP 주소를 가져오지만 초기 설정 중에 고정 주소를 설정할 수 있습니다.

- 나머지 인터페이스에 다른 네트워크를 연결합니다.

Firepower 4100 케이블 연결



논리적 디바이스 관리 인터페이스에서 초기 threat defense 구성을 수행합니다. 나중에 어느 데이터 인터페이스에서든지 관리를 활성화할 수 있습니다. threat defense 디바이스에서는 라이선싱 및 업데이트를 위해 인터넷에 액세스해야 하며, 기본 동작은 디바이스를 구축할 때 지정한 게이트웨이 IP 주소로 관리 트래픽을 라우팅하는 것입니다. 백플레인을 통해 관리 트래픽을 데이터 인터페이스로 대신 라우팅하려는 경우, 나중에 device manager에서 해당 설정을 구성할 수 있습니다.

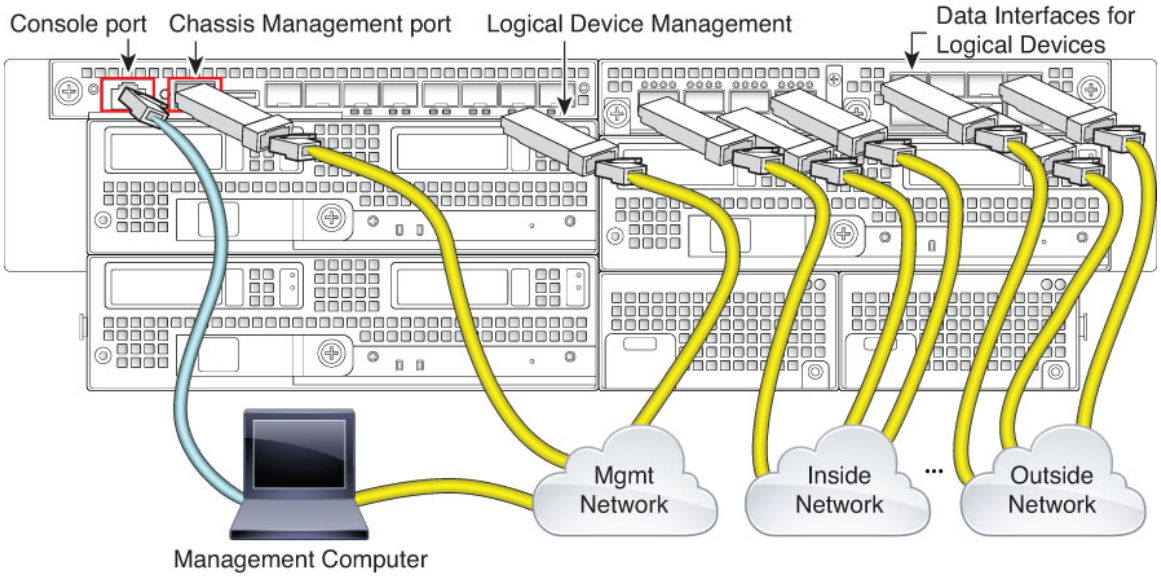
초기 섀시 설정, 지속적인 모니터링 및 논리적 디바이스 사용을 위해 다음 인터페이스에 케이블을 연결합니다.

- 콘솔 포트 — 섀시의 초기 설정을 수행하기 위해 관리 컴퓨터를 콘솔 포트에 연결합니다. Firepower 4100에는 RS-232 대 RJ-45 시리얼 콘솔 케이블이 포함되어 있습니다. 연결을 설정하려면 서드파티 시리얼-USB 케이블을 사용해야 할 수도 있습니다.
- 섀시 관리 포트 — 구성 및 지속적인 섀시 관리를 위해 섀시 관리 포트를 관리 네트워크에 연결합니다.
- Threat Defense 논리적 디바이스 관리 인터페이스 - FXOS 관리를 위해 예약된 섀시 관리 포트 이외에, 이 목적을 위해 섀시에서 어느 인터페이스든지 선택할 수 있습니다.
- 데이터 인터페이스 — 데이터 인터페이스를 논리적 디바이스 데이터 네트워크에 연결합니다. 물리적 인터페이스, EtherChannel 및 브레이크아웃 포트를 구성하여 고용량 인터페이스를 나눌 수 있습니다.

  고가용성을 위해서는 장애 조치/상태 링크에 데이터 인터페이스를 사용합니다.

참고 콘솔 포트 이외의 모든 인터페이스에는 SFP/SFP+/QSFP 트랜시버가 필요합니다. 지원되는 트랜시버에 대한 하드웨어 설치 가이드를 참조하십시오.

Firepower 9300 케이블 연결



논리적 디바이스 관리 인터페이스에서 초기 threat defense 구성을 수행합니다. 나중에 어느 데이터 인터페이스에서든지 관리를 활성화할 수 있습니다. threat defense 디바이스에서는 라이선싱 및 업데이트를 위해 인터넷에 액세스해야 하며, 기본 동작은 디바이스를 구축할 때 지정한 게이트웨이 IP 주소로 관리 트래픽을 라우팅하는 것입니다. 백플레인을 통해 관리 트래픽을 데이터 인터페이스로 대신 라우팅하려는 경우, 나중에 device manager에서 해당 설정을 구성할 수 있습니다.

초기 섀시 설정, 지속적인 모니터링 및 논리적 디바이스 사용을 위해 다음 인터페이스에 케이블을 연결합니다.

- 콘솔 포트 — 섀시의 초기 설정을 수행하기 위해 관리 컴퓨터를 콘솔 포트에 연결합니다. Firepower 9300에는 RS-232 대 RJ-45 시리얼 콘솔 케이블이 포함되어 있습니다. 연결을 설정하려면 서드파티 시리얼-USB 케이블을 사용해야 할 수도 있습니다.
- 섀시 관리 포트 — 구성 및 지속적인 섀시 관리를 위해 섀시 관리 포트를 관리 네트워크에 연결합니다.
- 논리적 디바이스 관리 인터페이스 — 하나 이상의 인터페이스를 사용하여 논리적 디바이스를 관리합니다. FXOS 관리를 위해 예약된 섀시 관리 포트 이외에, 이 목적을 위해 섀시에서 어느 인터페이스든지 선택할 수 있습니다. 관리 인터페이스는 논리적 디바이스 간에 공유될 수 있습니다. 또는 논리적 디바이스마다 별도의 인터페이스를 사용할 수 있습니다. 일반적으로는 관리 인터페이스를 모든 논리적 디바이스와 공유하며, 별도의 인터페이스를 사용하는 경우에는 단일 관리 네트워크에 배치합니다. 그러나 정확한 네트워크 요구 사항은 달라질 수 있습니다.
- 데이터 인터페이스 — 데이터 인터페이스를 논리적 디바이스 데이터 네트워크에 연결합니다. 물리적 인터페이스, EtherChannel 및 브레이크아웃 포트를 구성하여 고용량 인터페이스를 나눌 수 있습니다. 네트워크 요구 사항에 따라 여러 논리적 디바이스를 동일한 네트워크 또는 서로 다른 네트워크에 케이블로 연결할 수 있습니다. 모든 트래픽은 하나의 인터페이스에서 섀시를 종료하고 다른 인터페이스로 돌아가서 다른 논리적 디바이스에 연결해야 합니다.

  고가용성을 위해서는 장애 조치/상태 링크에 데이터 인터페이스를 사용합니다.

참고 콘솔 포트 이외의 모든 인터페이스에는 SFP/SFP+/QSFP 트랜시버가 필요합니다. 지원되는 트랜시버에 대한 하드웨어 설치 가이드를 참조하십시오.

Threat Defense Virtual 가상 케이블 연결

threat defense virtual을 설치하려면 http://www.cisco.com/c/en/us/support/security/firepower-ngfw-virtual/products-installation-guides-list.html에서 사용 중인 가상 플랫폼용 빠른 시작 가이드를 참조하십시오. device manager는 가상 플랫폼인 VMware, KVM, Microsoft Azure, AWS(Amazon Web Services)에서 지원됩니다.

threat defense virtual 기본 컨피그레이션에서는 관리 인터페이스와 내부 인터페이스를 동일한 서브넷에 배치합니다. 스마트 라이선싱을 사용하고 시스템 데이터베이스로 업데이트를 가져오려면 관리 인터페이스에서 인터넷에 연결할 수 있어야 합니다.

따라서 기본 컨피그레이션은 가상 스위치의 동일한 네트워크에 Management0/0 및 GigabitEthernet0/1(내부)을 둘 다 연결할 수 있도록 설계되어 있습니다. 기본 관리 주소는 내부 IP 주소를 게이트웨이로 사용합니다. 그러므로 관리 인터페이스는 인터넷에 연결하기 위해 내부 인터페이스와 외부 인터페이스를 차례로 통과하여 라우팅합니다.

인터넷에 액세스할 수 있는 네트워크를 사용한다면 내부 인터페이스에 사용하는 것과는 다른 서브넷에 Management0/0을 연결할 수도 있습니다. 이 경우 네트워크용으로 관리 인터페이스 IP 주소 및 게이트웨이를 적절하게 구성해야 합니다.

관리 인터페이스 IP 설정은 **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Management Interface(**관리 인터페이스**)**에서 정의합니다. 여기서 정의하는 IP 주소는 **Device(**디바이스**)** > **Interfaces(**인터페이스**)** > **View Configuration(**설정 보기**)**에 나와 있는 Management0/0(진단) 인터페이스용 IP 주소와는 동일하지 않습니다.

VMware 네트워크 어댑터 및 인터페이스가 Threat Defense 물리적 인터페이스에 매핑되는 방식

최대 10개의 인터페이스를 VMware threat defense virtual 디바이스용으로 구성할 수 있습니다. 최소 4개의 인터페이스를 구성해야 합니다.

Management0-0 소스 네트워크가 인터넷에 액세스할 수 있는 VM 네트워크에 연결되었는지 확인하십시오. 시스템이 Cisco Smart Software Manager에 연결하고 시스템 데이터베이스 업데이트를 다운로드할 수 있으려면 이러한 연결이 필요합니다.

OVF를 설치할 때 네트워크를 할당합니다. 인터페이스를 구성하면 나중에 VMware Client를 통해 가상 네트워크를 변경할 수 있습니다. 그러나 새 인터페이스를 추가해야 하는 경우 목록 끝에 인터페이스를 추가해야 합니다. 다른 곳에서 인터페이스를 추가하거나 제거하면 하이퍼바이저에서 인터페이스의 번호를 다시 매깁니다. 그러면 구성의 인터페이스 ID가 잘못된 인터페이스에 맞춰 정렬됩니다에 설명된 것처럼 더 복잡합니다.

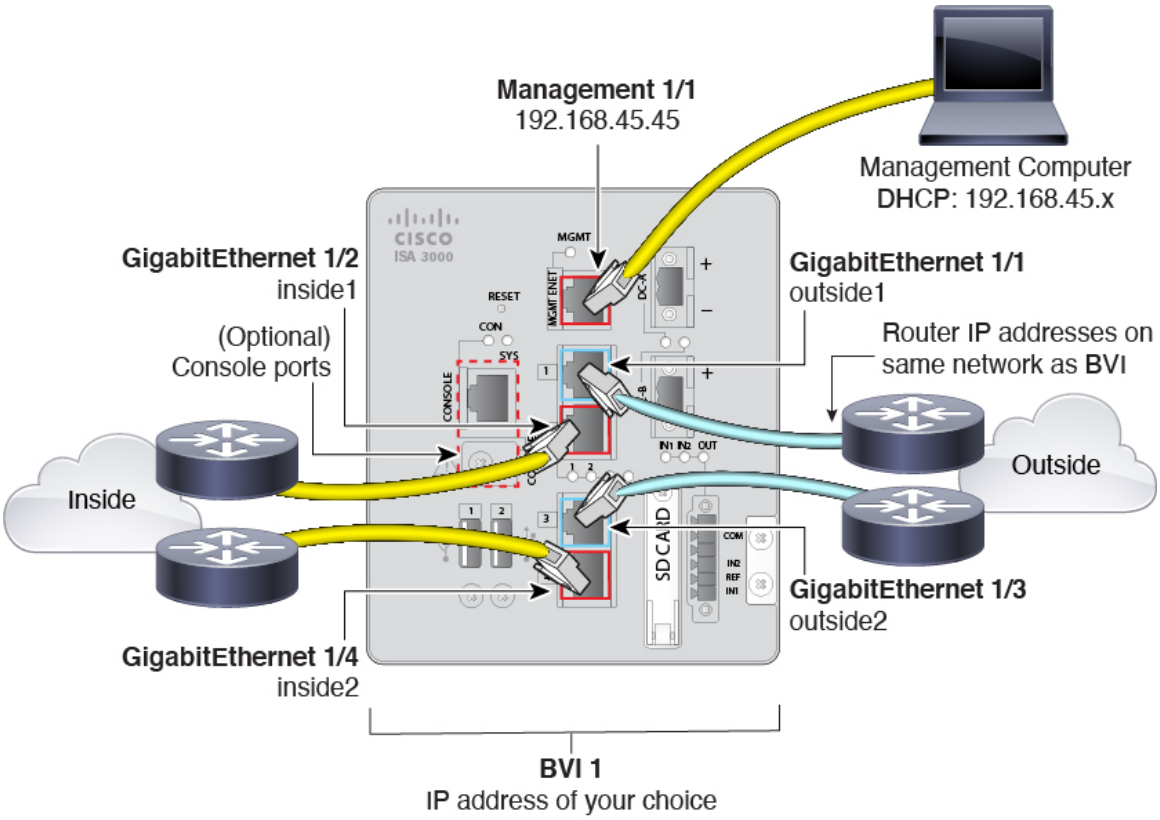
다음 표에서는 VMware 네트워크 어댑터와 소스 인터페이스가 threat defense virtual 물리적 인터페이스 이름에 매핑되는 방식을 설명합니다. 추가 인터페이스의 경우에도 같은 패턴에 따라 이름이 지정됩니다(관련 번호가 1씩 증가). 모든 추가 인터페이스는 데이터 인터페이스입니다. 가상 머신에 가상 네트워크를 할당하는 방법에 대한 자세한 내용은 VMware 온라인 도움말을 참조하십시오.

표 2: 소스-대상 네트워크 매핑

네트워크 어댑터	소스 네트워크	대상 네트워크(물리적 인터페이스 이름)	기능
네트워크 어댑터 1	Management0-0	Management 0/0	관리
네트워크 어댑터 2	Diagnostic0-0	Diagnostic0/0	진단
네트워크 어댑터 3	GigabitEthernet0-0	GigabitEthernet0/0	외부 데이터
네트워크 어댑터 4	GigabitEthernet0-1	GigabitEthernet0/1	내부 데이터
네트워크 어댑터 5	GigabitEthernet0-2	GigabitEthernet0/2	데이터 트래픽
네트워크 어댑터 6	GigabitEthernet0-3	GigabitEthernet0/3	데이터 트래픽
네트워크 어댑터 7	GigabitEthernet0-4	GigabitEthernet0/4	데이터 트래픽
네트워크 어댑터 8	GigabitEthernet0-5	GigabitEthernet0/5	데이터 트래픽
네트워크 어댑터 9	GigabitEthernet0-6	GigabitEthernet0/6	데이터 트래픽
네트워크 어댑터 10	GigabitEthernet0-7	GigabitEthernet0/7	데이터 트래픽

ISA 3000 케이블 연결

그림 *5: ISA 3000*



- GigabitEthernet 1/1을 외부 라우터에 연결하고 GigabitEthernet 1/2를 내부 라우터에 연결합니다.

  이러한 인터페이스에서는 하드웨어 우회 쌍을 형성합니다.

- GigabitEthernet 1/3을 이중 외부 라우터에 연결하고 GigabitEthernet 1/4를 이중 내부 라우터에 연결합니다.

  모델에 구리 포트가 있는 경우 이러한 인터페이스에서는 하드웨어 우회 쌍을 형성합니다. 파이버에서는 하드웨어 우회를 지원하지 않습니다. 이러한 인터페이스에서는 다른 쌍에 장애가 발생하는 경우 이중 네트워크 경로를 제공합니다. 이러한 데이터 인터페이스 4개는 모두 선택한 동일한 네트워크에 있습니다. BVI 1 IP 주소는 내부 및 외부 라우터와 동일한 네트워크에 있도록 구성해야 합니다.

- Management 1/1을 관리 컴퓨터(또는 네트워크)에 연결합니다.

  Management 1/1 IP 주소를 기본값에서 변경해야 할 경우, 관리 컴퓨터도 콘솔 포트에 연결해야 합니다. (선택 사항) CLI에서 관리 네트워크 설정 변경, 19 페이지의 내용을 참조하십시오.

(선택 사항) CLI에서 관리 네트워크 설정 변경

기본 관리 IP 주소를 사용할 수 없는 경우 콘솔 포트에 연결하고 CLI에서 관리 IP 주소, 게이트웨이 및 기타 기본적인 네트워킹 설정을 비롯한 초기 설정을 수행할 수 있습니다. 관리 인터페이스 설정만 구성할 수 있습니다. 내부 또는 외부 인터페이스는 구성할 수 없으며 나중에 GUI에서 구성할 수 있습니다.

참고 구축 시 IP 주소를 수동으로 설정했으므로 Firepower 4100/9300에는 이 절차를 사용할 필요가 없습니다.

참고 이미지 재설치 등을 통해 컨피그레이션을 지우지 않으면 CLI 설정 스크립트를 반복할 수 없습니다. 그러나 이러한 모든 설정은 **configure network**(네트워크 구성) 명령을 사용하여 CLI에서 나중에 변경할 수 있습니다. Cisco Secure Firewall Threat Defense 명령 참조의 내용을 참조하십시오.

프로시저

단계 **1** threat defense 콘솔 포트에 연결합니다. 자세한 내용은 CLI(Command Line Interface) 로그인, 6 페이지를 참조하십시오.

단계 **2** 사용자 이름 **admin**으로 로그인합니다.

기본 관리자 비밀번호는 Admin123입니다. AWS에서 구축 중에 사용자 데이터(**Advanced Details**(고급 세부 정보) > **User Data**(사용자 데이터))로 기본 비밀번호를 정의하지 않은 경우 threat defense virtual에 대한 기본 관리자 비밀번호는 AWS 인스턴스 ID입니다.

단계 **3** threat defense에 처음 로그인할 경우, 엔드 유저 라이선스 계약(EULA)에 동의하고 하라는 메시지가 표시됩니다. 그 다음에는 CLI 설정 스크립트가 표시됩니다.

기본값 또는 이전에 입력한 값이 괄호 안에 표시됩니다. 이전에 입력한 값을 승인하려면 **Enter**를 누릅니다.

다음 지침을 참조하십시오.

- **Enter the IPv4 default gateway for the management interface**(관리 인터페이스의 **IPv4** 기본 게이트웨이 입력) — 수동 IP 주소를 설정하는 경우 **data-interfaces** 또는 게이트웨이 라우터의 IP 주소를 입력합니다. **data-interfaces** 설정은 백플레인을 통해 아웃바운드 관리 트래픽을 전송하여 데이터 인터페이스를 종료합니다. 이 설정은 인터넷에 액세스할 수 있는 별도의 관리 네트워크가 없는 경우에 유용합니다. 관리 인터페이스에서 발생하는 트래픽에는 인터넷 액세스가 필요한 라이선스 등록 및 데이터베이스 업데이트가 포함되어 있습니다. **data-interfaces**를 사용하면 관리 네트워크에 직접 연결된 경우 관리 인터페이스에서 device manager(또는 SSH)을 계속 사용할 수 있지만 특정 네트워크 또는 호스트에 대한 원격 관리의 경우 **configure network static-routes** 명령을 사용하여 정적 경로를 추가해야 합니다. 데이터 인터페이스에 대한 device manager 관리는 이 설정의 영향을 받지 않습니다. DHCP를 사용하는 경우 시스템은 DHCP에서 제공하는 게이

트웨이를 사용하며, DHCP가 게이트웨이를 제공하지 않는 경우 **data-interfaces**를 대체 방법으로 사용합니다.

- **If your networking information has changed, you will need to reconnect(**네트워킹 정보가 변경된 경우 다시 연결해야 합니다**)** — SSH를 통해 기본 IP 주소에 연결되어 있지만 최초 설정에서 IP 주소를 변경한 경우 연결이 끊깁니다. 새 IP 주소 및 비밀번호를 사용하여 다시 연결합니다. 콘솔 연결에는 영향을 미치지 않습니다.
- **Manage the device locally?(**디바이스를 로컬로 관리하시겠습니까**?)** — device manager을 사용하려면 **yes**를 입력합니다. 답변이 **no**인 경우, 온프레미스 또는 클라우드 제공 management center를 사용하여 디바이스를 관리함을 의미합니다.

예제**:**

```
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
End User License Agreement
[...]

Please enter 'YES' or press <ENTER> to AGREE to the EULA:

System initialization in progress.  Please stand by.
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: 10.10.10.15
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.192
Enter the IPv4 default gateway for the management interface [data-interfaces]: 10.10.10.1
Enter a fully qualified hostname for this system [firepower]: ftd-1.cisco.com
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220]:
Enter a comma-separated list of search domains or 'none' []:
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'

Manage the device locally? (yes/no) [yes]: yes

>
```

단계 **4** 새 관리 IP 주소에서 device manager에 로그인합니다.

설정 마법사를 사용하여 초기 컨피그레이션 완료

device manager에 처음 로그인할 때는 디바이스 설정 마법사로 이동해 초기 시스템 구성을 완료합니다.

고가용성 컨피그레이션의 디바이스를 사용하려는 경우 고가용성을 위한 두 유닛 준비, 222 페이지의 내용을 참조하십시오.

참고 Firepower 4100/9300 및 ISA 3000에서는 설정 마법사를 지원하지 않으므로 이 절차는 이러한 모델에 적용되지 않습니다. Firepower 4100/9300의 경우, 섀시에서 논리적 디바이스를 구축할 때 모든 초기 구성이 설정됩니다. ISA 3000의 경우 배송 전에 특수한 기본 구성이 적용됩니다.

시작하기 전에

케이블 모뎀이나 라우터와 같은 게이트웨이 디바이스에 데이터 인터페이스를 연결해야 합니다. 이 디바이스는 엣지 구축의 경우 인터넷 연결 게이트웨이가 되며, 데이터 센터 구축의 경우에는 백본 라우터가 됩니다. 모델의 기본 "외부" 인터페이스를 사용합니다(인터페이스 연결, 9 페이지 및 초기 설정 전의 기본 컨피그레이션, 24 페이지 참조).

그런 다음 관리 컴퓨터를 하드웨어 모델의 "내부" 인터페이스에 연결합니다. 또는 관리 인터페이스에 연결할 수도 있습니다. threat defense virtual의 경우에는 관리 IP 주소에 연결할 수 있는지만 확인합니다.

(관리 IP 주소에서 인터넷 연결이 필요한 threat defense virtual 제외) 관리 인터페이스는 네트워크에 연결하지 않아도 됩니다. 기본적으로 시스템은 인터넷에 연결하는 데이터 인터페이스(대개 외부 인터페이스)를 통해 시스템 라이선싱 및 데이터베이스 업데이트와 기타 업데이트를 가져옵니다. 별도의 관리 네트워크를 대신 사용하려는 경우에는 관리 인터페이스를 네트워크에 연결하고 초기 설정을 완료한 후에 별도의 관리 게이트웨이를 구성하면 됩니다.

기본 IP 주소에 액세스할 수 없는 경우 관리 인터페이스 네트워크 설정을 변경하려면 (선택 사항) CLI에서 관리 네트워크 설정 변경, 19 페이지를 참조하십시오.

프로시저

단계 **1** device manager에 로그인합니다.

a) CLI에서 초기 컨피그레이션을 수행하지 않았다고 가정하겠습니다. **https://***ip-address*에서 device manager를 엽니다. 여기서 주소는 다음 중 하나입니다.

- 내부 인터페이스에 연결된 경우: **https://192.168.95.1**.
- () 관리 인터페이스에 연결되어 있는 경우: **https://192.168.45.45**.
- (모든 기타 모델) 관리 인터페이스에 연결되어 있는 경우: **https://***dhcp_client_ip*

b) 사용자 이름 **admin**으로 로그인합니다. 기본 관리자 비밀번호는 Admin123입니다. AWS에서 구축 중에 사용자 데이터(**Advanced Details(**고급 세부 정보**)** > **User Data(**사용자 데이터**)**)로 기본 비밀번호를 정의하지 않은 경우 threat defense virtual에 대한 기본 관리자 비밀번호는 AWS 인스턴스 ID입니다..

단계 **2** 시스템에 처음으로 로그인하며 CLI 설정 마법사를 사용하지 않은 경우에는 엔드 유저 라이선스 계약을 확인 및 동의하고 관리자 비밀번호를 변경하라는 메시지가 표시됩니다.

계속하려면 이러한 단계를 완료해야 합니다.

단계 **3** 외부 및 관리 인터페이스에 대해 다음 옵션을 구성하고 **Next(**다음**)**를 클릭합니다.

주의 **Next(**다음**)**를 클릭하면 설정이 디바이스에 구축됩니다. 인터페이스는 이름이 "외부"로 지정되어 "outside_zone" 보안 영역에 추가됩니다. 설정이 올바른지 확인합니다.

외부 인터페이스

- **IPv4** 구성 - 외부 인터페이스의 IPv4 주소를 구성합니다. DHCP를 사용하거나 수동으로 고정 IP 주소, 서브넷 마스크 및 게이트웨이를 입력할 수 있습니다. 끄기를 선택하여 IPv4 주소를 구성하지 않을 수도 있습니다. 기본 내부 주소와 동일한 서브넷에서 정적으로 또는 DHCP를 통해 IP 주소를 구성하지 마십시오(초기 설정 전의 기본 컨피그레이션, 24 페이지 참조). 설정 마법사를 사용하여 PPPoE를 구성할 수 없습니다. 인터페이스가 DSL 모뎀이나 케이블 모뎀에 연결되어 있거나 기타 ISP 연결을 사용하고 ISP에서 PPPoE를 사용하여 IP 주소를 제공하는 경우, PPPoE가 필요할 수 있습니다. 마법사를 완료한 후 PPPoE를 구성할 수 있습니다. 실제 인터페이스 구성, 260 페이지의 내용을 참조하십시오.
- **IPv6** 구성 - 외부 인터페이스의 IPv6 주소를 구성합니다. DHCP를 사용하거나 수동으로 고정 IP 주소, 접두사 및 게이트웨이를 입력할 수 있습니다. 끄기를 선택하여 IPv6 주소를 구성하지 않을 수도 있습니다.

관리 인터페이스

- **DNS** 서버 - 시스템 관리 주소용 DNS 서버를 지정합니다. 이름 확인을 위해 DNS 서버의 주소를 하나 이상 입력합니다. 기본값은 OpenDNS 공용 DNS 서버 또는 DHCP 서버에서 가져오는 DNS 서버입니다. 필드를 수정하여 기본값으로 되돌리려면 **OpenDNS(OpenDNS** 사용**)**를 클릭하여 적절한 IP 주소를 필드에 다시 로드합니다. 사용 중인 ISP에 따라서는 특정 DNS 서버를 사용해야 할 수도 있습니다. 마법사를 완료한 후 DNS 확인이 작동하지 않으면 관리 인터페이스용 DNS 문제 해결, 893 페이지의 내용을 참조하십시오.
- 방화벽 호스트 이름 - 시스템 관리 주소용 호스트 이름을 지정합니다.

단계 **4** 시스템 시간 설정을 구성하고 **Next(**다음**)**를 클릭합니다.

- 표준 시간대 - 시스템의 표준 시간대를 선택합니다.
- **NTP** 시간 서버 - 기본 NTP 서버를 사용할지 아니면 NTP 서버의 주소를 수동으로 입력할지를 선택합니다. 백업을 제공하기 위해 여러 서버를 추가할 수 있습니다.

단계 **5** 시스템에 대한 스마트 라이선스를 구성합니다.

시스템에 필요한 라이선스를 가져오고 적용하려면 스마트 라이선스 어카운트가 있어야 합니다. 처음에는 90일 평가 라이선스를 사용하고 나중에 스마트 라이선싱을 설정할 수 있습니다.

디바이스를 바로 등록하려면 디바이스를 등록하는 옵션을 선택하고 링크를 클릭하여 Smart Software Manager 어카운트에 로그인한 다음, 새 토큰을 생성하여 수정 상자에 복사합니다. 또한 서비스 지역을 선택하고 Cisco Success Network에 사용량 데이터를 전송할지 결정해야 합니다. 화면 텍스트로 이러한 설정이 자세히 설명됩니다.

디바이스를 아직 등록하지 않으려면 평가 모드 옵션을 선택합니다. 평가 기간은 최대 90일입니다. 나중에 디바이스를 등록하고 스마트 라이선스를 가져오려면 디바이스를 클릭한 다음, **Smart Licenses(**스마트 라이선스**)** 그룹에서 링크를 클릭하십시오.

단계 6 **Finish(**마침**)**를 클릭합니다.

다음에 수행할 작업

- 범주 기반 URL 필터링, 침입 검사, 악성코드 방지 등 선택 가능한 라이선스에 포함되는 기능을 사용하려면 필요한 라이선스를 활성화합니다. 선택 가능한 라이선스 활성화 또는 비활성화, 98 페이지의 내용을 참조하십시오.
- 다른 데이터 인터페이스를 고유 네트워크에 연결한 다음 인터페이스를 구성합니다. 인터페이스 구성에 대한 자세한 내용은 서브넷을 추가하는 방법, 74 페이지 및 인터페이스, 255 페이지를 참조하십시오.
- 내부 인터페이스를 통해 디바이스를 관리하는 경우 내부 인터페이스를 통해 CLI 세션을 열려면 SSH 연결에 대해 내부 인터페이스를 엽니다. 관리 액세스 목록 구성, 810 페이지의 내용을 참조하십시오.
- 제품 사용 방법을 파악하려면 활용 사례를 확인하십시오. 모범 사례: Threat Defense의 사용 사례, 43 페이지의 내용을 참조하십시오.

외부 인터페이스의 IP 주소를 획득하지 못하는 경우 해야 할 작업

기본 디바이스 컨피그레이션에는 내부 인터페이스에 대한 고정 IPv4 주소가 포함됩니다. 초기 디바이스 설치 마법사를 통해 이 주소를 변경할 수는 없지만, 나중에는 이 주소를 변경할 수 있습니다.

기본 내부 IP 주소는 디바이스에 연결되어 있는 다른 네트워크와 충돌할 수 있습니다. 특히, DHCP를 사용하여 ISP(Internet Service Provider)로부터 주소를 얻으려는 경우 그렇게 될 수 있습니다. 일부 ISP는 내부 네트워크와 동일한 서브넷을 주소 풀로 사용합니다. 동일한 서브넷의 주소를 사용하는 두 개의 데이터 인터페이스를 지닐 수 없으므로 ISP의 충돌하는 주소는 외부 인터페이스에 구성할 수 없습니다.

내부 고정 IP 주소와 외부 인터페이스의 DHCP 제공 주소 간에 충돌이 발생하는 경우, 연결 다이어그램에는 IPv4 주소 없이 관리자가 외부 인터페이스를 가동 중인 상태로 표시됩니다.

이 경우, 설치 마법사가 성공적으로 완료되고 모든 기본 NAT, 액세스 및 기타 정책 및 설정이 구성됩니다. 충돌을 제거하려면 다음 절차를 따르면 됩니다.

시작하기 전에

ISP에 정상적으로 연결되었는지 확인합니다. 서브넷 충돌이 발생하면 외부 인터페이스의 주소를 가져올 수 없게 되지만, 단순히 ISP에 대한 링크가 없는 경우에도 주소를 가져올 수 없게 됩니다.

프로시저

단계 1 **Device(**디바이스**)**를 클릭한 다음 **Interfaces(**인터페이스**)** 요약의 링크를 클릭합니다.

단계 2 내부 인터페이스의 **Actions(**작업**)** 열 위로 마우스를 가져가 수정 아이콘( )을 클릭합니다.

단계 **3** **IPv4 Address(IPv4** 주소**)** 탭에서 고유한 서브넷에 고정 주소를 입력합니다(예: 192.168.2.1/24 또는 192.168.46.1/24). 기본 관리 주소가 192.168.45.45/24인 경우 해당 서브넷을 사용하지 마십시오.

또한 이미 내부 네트워크에서 실행 중인 DHCP 서버가 있는 경우, 주소를 가져오기 위해 DHCP를 사용할 수도 있습니다. 그러나 인터페이스에서 DHCP 서버를 제거하려면 먼저 **DHCP SERVER IS DEFINED FOR THIS INTERFACE(DHCP** 서버가 이 인터페이스에 대해 정의되어 있음**)** 그룹에서 **Delete(**삭제**)**를 클릭해야 합니다.

단계 **4** **DHCP SERVER IS DEFINED FOR THIS INTERFACE(DHCP** 서버가 이 인터페이스에 대해 정의되어 있음**)** 영역에서 **Edit(**편집**)**을 클릭하고 DHCP 풀을 새로운 서브넷에 대한 범위로 변경합니다(예: 192.168.2.5-192.168.2.254).

단계 **5** **OK(**확인**)**를 클릭하여 인터페이스 변경 사항을 저장합니다.

단계 **6** 메뉴에서 **Deploy(**구축**)** 버튼을 클릭하여 변경 사항을 구축합니다.

단계 **7** **Deploy Now(**지금 구축**)**를 클릭합니다.

구축을 완료하고 나면 연결 그래픽에는 외부 인터페이스에 이제 IP 주소가 있는 것으로 표시됩니다. 내부 네트워크에서 클라이언트를 사용하여 인터넷 또는 다른 업스트림 네트워크에 연결되었는지 확인합니다.

초기 설정 전의 기본 컨피그레이션

로컬 관리자(device manager)를 사용하여 threat defense 디바이스를 처음으로 구성하기 전에 디바이스에는 다음과 같은 기본 컨피그레이션이 포함되어 있습니다.

많은 모델의 경우, 이 구성에서는 대개 인터페이스에 컴퓨터를 직접 연결하는 방식을 사용하여 내부 인터페이스를 통해 디바이스 관리자를 열며, 내부 인터페이스에 정의된 DHCP 서버를 사용하여 컴퓨터에 IP 주소를 제공한다고 가정합니다. 또는, 컴퓨터를 관리 인터페이스에 연결한 다음, DHCP를 사용하여 주소를 얻을 수도 있습니다. 그러나 일부 모델의 경우 기본 구성 및 관리 요구 사항이 다릅니다. 자세한 내용은 아래 표를 참조하십시오.

참고 마법사를 사용하여 설치를 수행하기 전에 우선 CLI 설정((선택 사항) CLI에서 관리 네트워크 설정 변경, 19 페이지)을 사용하여 이러한 여러 설정을 사전 구성할 수 있습니다.

기본 컨피그레이션 설정

설정	기본	초기 컨피그레이션 중 변경 가능 여부
관리자 사용자의 비밀번호	Admin123 Firepower 4100/9300: 논리적 디바이스를 구축할 때 비밀번호를 설정합니다. AWS: 초기 구축 중에 사용자 데이터(**Advanced Details(**고급 세부 정보**)** > **User Data(**사용자 데이터**)**)로 기본 비밀번호를 정의하지 않는 한 기본값은 AWS 인스턴스 ID입니다.	예. 기본 비밀번호를 변경해야 합니다.
관리 IP 주소	DHCP를 통해 얻습니다. Threat Defense Virtual192.168.45.45 Firepower 4100/9300: 논리적 디바이스를 구축할 때 관리 IP 주소를 설정합니다.	아니요. Firepower 4100/9300의 경우: 예.
관리 게이트웨이	디바이스의 데이터 인터페이스. 일반적으로 외부 인터페이스는 인터넷의 경로가 됩니다. 이 게이트웨이는 디바이스에서 시작되는 트래픽에 대해서만 작동합니다. 디바이스가 DHCP 서버에서 기본 게이트웨이를 수신하는 경우 해당 게이트웨이가 사용됩니다. Firepower 4100/9300: 논리적 디바이스를 구축할 때 게이트웨이 IP 주소를 설정합니다. ISA 3000: 192.168.45.1. Threat Defense Virtual: 192.168.45.1	아니요. Firepower 4100/9300의 경우: 예.
관리 인터페이스의 DNS 서버	OpenDNS 공용 DNS 서버, IPv4: 208.67.220.220 및 208.67.222.222, IPv6: 2620:119:35::35. DHCP에서 가져온 DNS 서버는 사용되지 않습니다. Firepower 4100/9300: 논리적 디바이스를 구축할 때 DNS 서버를 설정합니다.	예.

설정	기본	초기 컨피그레이션 중 변경 가능 여부
내부 인터페이스 IP 주소	192.168.95.1/24 Firepower 4100/9300: 데이터 인터페이스가 사전 구성되어 있지 않습니다. ISA 3000: BVI1 IP 주소가 사전 구성되어 있지 않습니다. BVI1에는 모든 내부 및 외부 인터페이스가 포함되어 있습니다. Threat Defense Virtual: 192.168.45.1/24	아니요.
내부 클라이언트에 대한 DHCP 서버	주소 풀 192.168.95.5-192.168.95.254를 포함하는 내부 인터페이스에서 실행됩니다. Firepower 4100/9300: 활성화된 DHCP 서버가 없습니다. ISA 3000: 활성화된 DHCP 서버가 없습니다. Threat Defense Virtual: 내부 인터페이스의 주소 풀은 192.168.45.46 - 192.168.45.254입니다.	아니요.
내부 클라이언트에 대한 DHCP 자동 컨피그레이션 (자동 컨피그레이션은 클라이언트에 WINS 및 DNS 서버용 주소를 제공)	외부 인터페이스에서 활성화됩니다.	예(간접적). 외부 인터페이스에 대해 고정 IPv4 주소를 구성하는 경우 DHCP 서버 자동 컨피그레이션은 비활성화됩니다.
외부 인터페이스 IP 주소	IPv4: ISP(Internet Service Provider) 또는 업스트림 라우터에서 DHCP를 통해 가져옵니다. IPv6: 자동 설정. Firepower 4100/9300: 데이터 인터페이스가 사전 구성되어 있지 않습니다. ISA 3000: BVI1 IP 주소가 사전 구성되어 있지 않습니다. BVI1에는 모든 내부 및 외부 인터페이스가 포함되어 있습니다.	예.

디바이스 모델별 기본 인터페이스

초기 컨피그레이션 중에는 다른 내부 및 외부 인터페이스를 선택할 수 없습니다. 컨피그레이션 후에 인터페이스 할당을 변경하려면 인터페이스 및 DHCP 설정을 수정합니다. 브리지 그룹에서 인터페이스를 제거해야 해당 인터페이스를 비스위치 인터페이스로 구성할 수 있습니다.

Threat Defense 디바이스	외부 인터페이스	내부 인터페이스
Firepower 1010	Ethernet1/1	VLAN1에는 물리적 방화벽 인터페이스인 외부 인터페이스를 제외한 다른 모든 스위치 포트가 포함되어 있습니다.
Firepower 1120, 1140, 1150	Ethernet1/1	Ethernet1/2
Firepower 2100 Series	Ethernet1/1	Ethernet1/2
Secure Firewall 3100 Series	Ethernet1/1	Ethernet1/2
Firepower 4100 Series	데이터 인터페이스가 사전 구성되어 있지 않습니다.	데이터 인터페이스가 사전 구성되어 있지 않습니다.
Firepower 9300 Appliance	데이터 인터페이스가 사전 구성되어 있지 않습니다.	데이터 인터페이스가 사전 구성되어 있지 않습니다.
Threat Defense Virtual	GigabitEthernet0/0	GigabitEthernet0/1
ISA 3000	GigabitEthernet1/1 및 GigabitEthernet1/3 GigabitEthernet1/1(outside1) 및 1/2(inside1), GigabitEthernet1/3(outside2) 및 1/4(inside2)(비파이버 모델만 해당)는 하드웨어 우회 쌍으로 구성됩니다. 모든 내부 및 외부 인터페이스는 BVI1의 일부입니다.	GigabitEthernet1/2 및 GigabitEthernet1/4

초기 설정 후의 컨피그레이션

설정 마법사를 완료한 후의 디바이스 컨피그레이션에는 다음 설정이 포함됩니다. 아래 표에는 특정 설정이 명시적으로 선택한 것인지 아니면 다른 선택 항목을 기준으로 하여 정의된 것인지가 나와 있습니다. "암시적" 컨피그레이션을 검증한 후 필요한 사항에 맞지 않으면 수정합니다.

참고 Firepower 4100/9300 및 ISA 3000에서는 설정 마법사를 지원하지 않습니다. Firepower 4100/9300의 경우, 섀시에서 논리적 디바이스를 구축할 때 모든 초기 구성이 설정됩니다. ISA 3000의 경우 배송 전에 특수한 기본 구성이 적용됩니다.

설정	컨피그레이션	명시적, 암시적 또는 기본 컨피그레이션
관리자 사용자의 비밀번호	입력한 내용	명시적
관리 IP 주소	DHCP를 통해 얻습니다. Threat Defense Virtual: 192.168.45.45 Firepower 4100/9300: 논리적 디바이스를 구축할 때 설정한 관리 IP 주소입니다.	기본
관리 게이트웨이	디바이스의 데이터 인터페이스. 일반적으로 외부 인터페이스는 인터넷의 경로가 됩니다. 관리 게이트웨이는 디바이스에서 시작되는 트래픽에 대해서만 작동합니다. 디바이스가 DHCP 서버에서 기본 게이트웨이를 수신하는 경우 해당 게이트웨이가 사용됩니다. Firepower 4100/9300: 논리적 디바이스를 구축할 때 설정한 게이트웨이 IP 주소입니다. ISA 3000: 192.168.45.1 Threat Defense Virtual: 192.168.45.1	기본
관리 인터페이스의 DNS 서버	OpenDNS 공용 DNS 서버, IPv4: 208.67.220.220, 208.67.222.222, IPv6: 2620:119:35::35, 또는 입력한 모든 값. DHCP에서 가져온 DNS 서버는 사용되지 않습니다. Firepower 4100/9300: 논리적 디바이스를 구축할 때 설정한 DNS 서버입니다.	명시적
관리 호스트 이름	**firepower** 또는 입력한 내용 Firepower 4100/9300: 논리적 디바이스를 구축할 때 설정한 호스트 이름입니다.	명시적
데이터 인터페이스를 통한 관리 액세스	데이터 인터페이스 관리 액세스 목록 규칙을 사용하면 내부 인터페이스를 통한 HTTPS 액세스가 허용됩니다. SSH 연결은 허용되지 않습니다. IPv4 및 IPv6 연결은 모두 허용됩니다. Firepower 4100/9300: 데이터 인터페이스에 기본 관리 액세스 규칙이 없습니다. ISA 3000: 데이터 인터페이스에 기본 관리 액세스 규칙이 없습니다. Threat Defense Virtual: 데이터 인터페이스에 기본 관리 액세스 규칙이 없습니다.	암시적

설정	컨피그레이션	명시적, 암시적 또는 기본 컨피그레이션
시스템 시간	선택한 표준 시간대 및 NTP 서버 Firepower 4100/9300: 시스템 시간이 섀시에서 상속됩니다. ISA 3000: Cisco NTP 서버: 0.sourcefire.pool.ntp.org, 1.sourcefire.pool.ntp.org, 2.sourcefire.pool.ntp.org	명시적
스마트 라이선스	기본 라이선스를 사용하여 등록된 라이선스 또는 사용 설정된 평가 기간 중 선택하는 항목. 서브스크립션 라이선스는 활성화하지 않습니다. 서브스크립션 라이선스를 활성화하려면 스마트 라이선싱 페이지로 이동합니다.	명시적
내부 인터페이스 IP 주소	192.168.95.1/24 Firepower 4100/9300: 데이터 인터페이스가 사전 구성되어 있지 않습니다. ISA 3000: 없음. BVI1 IP 주소를 수동으로 설정해야 합니다. Threat Defense Virtual: 192.168.45.1/24	기본
내부 클라이언트에 대한 DHCP 서버	주소 풀 192.168.95.5-192.168.95.254를 포함하는 내부 인터페이스에서 실행됩니다. Firepower 4100/9300: 활성화된 DHCP 서버가 없습니다. ISA 3000: 활성화된 DHCP 서버가 없습니다. Threat Defense Virtual: 내부 인터페이스의 주소 풀은 192.168.45.46 - 192.168.45.254입니다.	기본
내부 클라이언트에 대한 DHCP 자동 컨피그레이션(자동 컨피그레이션은 클라이언트에 WINS 및 DNS 서버용 주소를 제공)	DHCP를 사용하여 외부 인터페이스 IPv4 주소를 가져오는 경우 외부 인터페이스에서 활성화하는 것으로 설정됩니다. 고정 주소를 사용하는 경우에는 DHCP 자동 컨피그레이션이 비활성화됩니다.	명시적(간접적)

설정	컨피그레이션	명시적, 암시적 또는 기본 컨피그레이션
데이터 인터페이스 컨피그레이션	• Firepower 1010 - 외부 인터페이스(Ethernet1/1)가 물리적 방화벽 인터페이스입니다. 기타 모든 인터페이스는 활성화된 스위치 포트이며, 내부 인터페이스인 VLAN1에 포함됩니다. 엔드포인트 또는 스위치를 이러한 포트에 연결하고 내부 인터페이스용으로 DHCP 서버에서 주소를 가져올 수 있습니다. • Firepower 4100/9300- 모든 데이터 인터페이스가 비활성화되어 있습니다. • ISA 3000 - 모든 데이터 인터페이스가 활성화되어 있으며 동일한 브리지 그룹인 BVI1에 포함됩니다. GigabitEthernet1/1 및 1/3은 외부 인터페이스이고 GigabitEthernet1/2 및 1/4는 내부 인터페이스입니다. GigabitEthernet1/1(outside1) 및 1/2(inside1), GigabitEthernet1/3(outside2) 및 1/4(inside2)(비파이버 모델만 해당)는 하드웨어 우회 쌍으로 구성됩니다. • 다른 모든 모델 - 외부 및 내부 인터페이스만 구성 및 활성화됩니다. 다른 모든 데이터 인터페이스는 비활성화됩니다.	기본
외부 실제 인터페이스 및 IP 주소	디바이스 모델에 따른 기본 외부 포트. 초기 설정 전의 기본 컨피그레이션, 24 페이지를 참조하십시오. IP 주소는 DHCP 및 IPv6 자동 설정에서 가져온 주소이거나 입력한 고정 주소(IPv4, IPv6 또는 둘 다)입니다. Firepower 4100/9300: 데이터 인터페이스가 사전 구성되어 있지 않습니다. ISA 3000: 없음. BVI1 IP 주소를 수동으로 설정해야 합니다.	인터페이스: 기본 주소 지정: 명시적
정적 경로	외부 인터페이스에 대해 고정 IPv4 또는 IPv6 주소를 구성하는 경우 정적 기본 경로가 IPv4/IPv6에 대해 적절하게 구성되어 해당 주소 유형에 대해 정의한 게이트웨이를 가리킵니다. DHCP를 선택하는 경우 DHCP 서버에서 기본 경로를 가져옵니다. 게이트웨이 및 "임의" 주소에 대한 네트워크 개체도 생성됩니다(IPv4의 경우 0.0.0.0/0, IPv6의 경우 ::/0).	암시적

설정	컨피그레이션	명시적, 암시적 또는 기본 컨피그레이션
보안 영역	**inside_zone**에는 내부 인터페이스가 포함되어 있습니다. Firepower 4100/9300의 경우 이 보안 영역에 인터페이스를 수동으로 추가해야 합니다. **outside_zone**에는 내부 인터페이스가 포함되어 있습니다. Firepower 4100/9300의 경우 이 영역에 인터페이스를 수동으로 추가해야 합니다. 이러한 영역을 수정하여 다른 인터페이스를 추가하거나 영역을 직접 생성할 수 있습니다.	암시적
액세스 제어 정책	inside_zone에서 outside_zone으로 전송되는 모든 트래픽을 신뢰하는 규칙입니다. 이 규칙을 사용하면 네트워크 내의 사용자가 외부로 전송하는 모든 트래픽 및 해당 연결에 대한 모든 반환 트래픽이 검사 없이 허용됩니다. 기타 모든 트래픽에 대한 기본 작업은 차단입니다. 즉, 외부에서 시작되어 네트워크로 진입하는 모든 트래픽은 차단됩니다. Firepower 4100/9300: 사전 구성된 액세스 규칙이 없습니다. ISA 3000: inside_zone에서 outside_zone으로의 모든 트래픽을 신뢰하는 규칙, outside_zone에서 inside_zone으로의 모든 트래픽을 신뢰하는 규칙이 있습니다. 트래픽은 차단되지 않습니다. 또한 디바이스에는 inside_zone과 outside_zone의 인터페이스 간의 모든 트래픽을 신뢰하는 규칙도 있습니다. 그러므로 내부 사용자와 외부 사용자 간의 모든 트래픽을 검사하지 않아도 됩니다.	암시적
NAT	인터페이스 동적 PAT 규칙이 외부 인터페이스로 전송되는 IPv4 트래픽의 소스 주소를 외부 인터페이스 IP 주소의 고유 포트로 변환합니다. 관리 주소의 데이터 인터페이스를 통한 라우팅과 내부 인터페이스를 통한 HTTPS 액세스를 활성화하는 숨겨진 추가 PAT 규칙도 있습니다. 이러한 규칙은 NAT 테이블에는 표시되지 않지만, CLI에서 **show nat** 명령을 사용해 확인할 수 있습니다. Firepower 4100/9300: NAT가 사전 구성되어 있지 않습니다. ISA 3000: NAT가 사전 구성되어 있지 않습니다.	암시적

컨피그레이션 기본 사항

다음 항목에서는 디바이스 구성을 위한 기본 방법을 설명합니다.

디바이스 구성

device manager에 처음 로그인할 때는 기본 설정을 구성할 수 있도록 설정 마법사로 이동하게 됩니다. 마법사를 완료한 후에 다음 방법을 사용하여 다른 기능을 구성하고 디바이스 컨피그레이션을 관리합니다.

항목을 시각적으로 구분하기가 어려운 경우 사용자 프로파일에서 다른 색 구성표를 선택합니다. 페이지 오른쪽 상단에 있는 사용자 아이콘 드롭다운 메뉴에서 **Profile(**프로파일**)**을 선택합니다.

프로시저

단계 **1** 디바이스를 클릭하여 **Device Summary(**디바이스 요약**)**로 이동합니다.

대시보드에는 키 설정이 구성되어 있는지(녹색으로 표시됨) 아니면 구성해야 하는지에 대한 정보 및 활성화된 인터페이스를 비롯하여 디바이스의 시각적 상태가 표시됩니다. 자세한 내용은 인터페이스 및 관리 상태 보기, 38 페이지를 참고하십시오.

상태 이미지 위에는 디바이스 모델, 소프트웨어 버전, 시스템 및 VDB(Vulnerability Database) 버전, 침입 규칙을 마지막으로 업데이트한 시간의 요약이 표시됩니다. 이 영역에서는 기능을 컨피그레이션할 수 있는 링크를 포함한 고가용성 상태도 표시합니다. 고가용성(페일오버), 209 페이지를 참조하십시오. 또한 클라우드 관리 상태를 표시합니다. 클라우드 관리를 사용하는 경우 디바이스가 등록된 어카운트가 여기에 표시됩니다. 클라우드 서비스 구성, 838 페이지를 참조하십시오.

이미지 아래에는 구성 가능한 여러 기능의 그룹이 있으며 각 그룹의 컨피그레이션 요약과 시스템 컨피그레이션을 관리하기 위해 수행할 수 있는 작업이 표시됩니다.

단계 **2** 각 그룹의 링크를 클릭하여 설정을 구성하거나 작업을 수행합니다.

아래에는 그룹에 대한 설정이 요약되어 있습니다.

- **Interface(**인터페이스**)** — 관리 인터페이스 이외에 둘 이상의 데이터 인터페이스가 구성되어 있어야 합니다. 인터페이스, 255 페이지의 내용을 참조하십시오.
- **Routing(**라우팅**)** — 라우팅 컨피그레이션입니다. 기본 경로를 정의해야 합니다. 컨피그레이션에 따라서는 다른 경로가 필요할 수 있습니다. 라우팅, 327 페이지의 내용을 참조하십시오.
- **Updates(**업데이트**)** — 지리위치, 침입 규칙, 취약점 데이터베이스 업데이트 및 시스템 소프트웨어 업그레이드가 표시됩니다. 이러한 기능을 사용하려는 경우 최신 데이터베이스 업데이트를 받을 수 있도록 정기 업데이트 일정을 설정하십시오. 정기 일정에 따른 업데이트가 수행되기 전에 업데이트를 다운로드해야 하는 경우에도 이 페이지로 이동할 수 있습니다. 시스템 데이터베이스 및 피드 업데이트, 855 페이지의 내용을 참조하십시오.

- **System Settings(**시스템 설정**)** — 이 그룹에는 여러 설정이 포함되어 있습니다. 그 중 일부 설정은 디바이스를 초기 설정할 때 구성하며 거의 변경하지 않는 기본 설정입니다. 시스템 설정, 809 페이지의 내용을 참조하십시오.
- **Smart License(**스마트 라이선스**)** — 시스템 라이선스의 현재 상태가 표시됩니다. 시스템을 사용하려면 적절한 라이선스를 설치해야 합니다. 일부 기능의 경우 추가 라이선스가 필요합니다. 시스템 라이선싱, 89 페이지의 내용을 참조하십시오.
- **Backup and Restore(**백업 및 복원**)** — 시스템 컨피그레이션을 백업하거나 이전 백업을 복원합니다. 시스템 백업 및 복원, 865 페이지의 내용을 참조하십시오.
- **Troubleshoot(**트러블슈팅**)** — Cisco Technical Assistance Center에서 요청하는 경우 트러블슈팅 파일을 생성합니다. 트러블슈팅 파일 생성, 898 페이지의 내용을 참조하십시오.
- **Site-to-Site VPN(**사이트 대 사이트 **VPN)** — 이 디바이스와 원격 디바이스 간의 사이트 대 사이트 VPN(Virtual Private Network) 연결이 표시됩니다. 사이트 대 사이트 VPN 관리, 687 페이지의 내용을 참조하십시오.
- **Remote Access VPN(**원격 액세스 **VPN)** — 외부 클라이언트가 내부 네트워크에 연결하도록 허용하는 원격 액세스 VPN(Virtual Private Network) 컨피그레이션입니다. 원격 액세스 VPN 구성, 733 페이지의 내용을 참조하십시오.
- **Advanced Configuration(**고급 컨피그레이션**)** — device manager를 사용해서는 구성할 수 없는 기능을 FlexConfig 및 스마트 CLI를 사용하여 구성합니다. 고급 컨피그레이션, 907 페이지의 내용을 참조하십시오.
- **Device Administration(**디바이스 관리**)** — 감사 로그를 확인하거나 컨피그레이션 복사본을 내보냅니다. 감사 및 변경 관리, 871 페이지의 내용을 참조하십시오.

단계 **3** 메뉴에서 **Deploy(**구축**)** 버튼을 클릭하여 변경 사항을 구축합니다.

변경 사항은 구축할 때까지 디바이스에서 활성화되지 않습니다. 변경 사항 구축, 35 페이지의 내용을 참조하십시오.

다음에 수행할 작업

주 메뉴에서 **Policies(**정책**)**를 클릭하여 시스템의 보안 정책을 구성합니다. **Objects(**개체**)**를 클릭하여 해당 정책에 필요한 개체를 구성할 수도 있습니다.

보안 정책 구성

보안 정책을 사용하여 조직의 사용 제한 정책을 구현하고 침입 및 기타 위협으로부터 네트워크를 보호합니다.

프로시저

단계 **1** **Policies(**정책**)**를 클릭합니다.

Security Policies(보안 정책) 페이지에는 시스템 전체의 일반적인 연결 플로우와 보안 정책이 적용되는 순서가 표시됩니다.

단계 **2** 정책 이름을 클릭하여 정책을 구성합니다.

항상 액세스 제어 정책을 적용해야 하더라도 각 정책 유형을 반드시 구성할 필요는 없을 수 있습니다. 정책 요약은 다음과 같습니다.

- **SSL Decryption(SSL** 암호 해독**)** — 침입, 악성코드 등에 대한 암호화된 연결(예: HTTPS)을 검사하려는 경우, 연결을 암호 해독해야 합니다. SSL 암호 해독 정책을 사용하여 어떤 연결을 암호 해독해야 할지 확인합니다. 시스템은 검사를 수행한 후에 연결을 다시 암호화합니다. SSL 암호 해독 정책 구성, 471 페이지를 참조하십시오.
- **Identity(ID)** — 네트워크 활동과 개인 사용자의 상관관계를 분석하거나 사용자 또는 사용자 그룹 멤버십을 기반으로 네트워크 액세스를 제어하려면 ID 정책을 사용하여 지정된 소스 IP 주소와 연결된 사용자를 확인합니다. ID 정책 구성, 495 페이지를 참조하십시오.
- **Security Intelligence(**보안 인텔리전스**)** — 보안 인텔리전스 정책을 사용하여 선택된 IP 주소 또는 URL을 오가는 연결을 신속하게 삭제합니다. 알려진 유해 사이트를 차단하면 해당 사이트를 액세스 제어 정책에서 고려할 필요가 없습니다. Cisco에서는 알려진 유해 주소 및 URL에 대해 정기적으로 업데이트된 피드를 제공하므로 보안 인텔리전스 차단 목록이 동적으로 업데이트됩니다. 피드를 사용하는 경우에는 차단 목록에서 항목을 추가하거나 제거하기 위해 정책을 수정할 필요가 없습니다. 보안 인텔리전스 구성, 509 페이지를 참조하십시오.
- **NAT**(Network Address Translation) — NAT 정책을 사용하여 내부 IP 주소를 외부에서 라우팅 가능한 주소로 변환합니다. NAT 구성, 598 페이지를 참조하십시오.
- **Access Control(**액세스 제어**)** — 액세스 제어 정책을 사용하여 네트워크에서 어떤 연결이 허용되는지 확인합니다. 보안 영역, IP 주소, 프로토콜, 포트, 애플리케이션, URL, 사용자 또는 사용자 그룹을 기준으로 필터링할 수 있습니다. 액세스 제어 규칙을 사용하여 침입 및 파일(악성코드) 정책을 적용할 수도 있습니다. 이 정책을 사용하여 URL 필터링을 구현할 수 있습니다. 액세스 제어 정책 구성, 530 페이지를 참조하십시오.
- **Intrusion(**침입**)** — 침입 정책을 사용하여 알려진 위협을 검사합니다. 액세스 제어 규칙을 사용하여 침입 정책을 적용하는 경우에도 침입 정책을 편집하여 특정 침입 규칙을 선택적으로 활성화 또는 비활성화할 수 있습니다. 침입 정책, 553 페이지의 내용을 참조하십시오.

단계 **3** 메뉴에서 **Deploy(**구축**)** 버튼을 클릭하여 변경 사항을 구축합니다.

변경 사항은 구축할 때까지 디바이스에서 활성화되지 않습니다. 변경 사항 구축, 35 페이지의 내용을 참조하십시오.

규칙 또는 개체 검색

정책 규칙 또는 개체 목록에서 전체 텍스트 검색을 사용하면 수정하려는 항목을 찾는 데 도움이 됩니다. 이 기능은 수백 개의 규칙 또는 긴 개체 목록이 있는 정책을 처리할 때 특히 유용합니다.

규칙 및 개체에서 검색 기능을 사용하는 방법은 침입 정책을 제외한 모든 유형의 정책에서 동일합니다. 즉 **Search(**검색**)** 필드에서 검색할 문자열을 입력하고 Enter를 누릅니다.

이 문자열은 규칙 또는 개체의 어느 부분에도 있을 수 있으며, 부분 문자열일 수 있습니다. 별표(*)를 0개 이상의 문자와 일치하는 와일드카드로 사용할 수 있습니다. ?~!{}<>:% 문자는 검색 문자열의 일부로 지원하지 않으므로 포함하지 마십시오. ;#& 문자는 무시됩니다.

문자열은 그룹에 있는 개체 안에 표시될 수 있습니다. 예를 들어 IP 주소를 입력하고 해당 주소를 지정하는 네트워크 개체 또는 그룹을 검색할 수 있습니다.

완료했으면 검색 상자 오른쪽의 **x**를 클릭하여 필터를 지웁니다.

변경 사항 구축

정책 또는 설정을 업데이트할 때 변경 사항은 디바이스에 즉시 적용되지 않습니다. 다음과 같은 2단계 프로세스를 통해 컨피그레이션을 변경합니다.

1. 변경 사항을 적용합니다.
2. 변경 사항을 배포합니다.

이 프로세스에서는 "부분 구성" 방식으로 디바이스를 실행할 필요 없이 관련 변경 사항 그룹을 적용할 수 있습니다. 대부분의 경우, 구축에는 변경 사항만 포함되어 있습니다. 그러나 필요한 경우, 시스템에서는 네트워크를 중단시킬 수 있는 전체 컨피그레이션을 다시 적용합니다. 뿐만 아니라 일부 변경 사항에서는 검사 엔진을 재시작해야 하는데, 재시작하는 동안 트래픽 속도가 느려집니다. 따라서 잠재적 중단으로 인한 영향이 가장 적을 때 변경 사항을 구축하는 것이 좋습니다.

참고 구축 작업에 실패할 경우, 시스템에서는 이전 컨피그레이션의 부분적인 변경 사항을 롤백해야 합니다. 롤백에는 데이터 평면 컨피그레이션을 지우고 이전 버전을 다시 구축하는 작업이 포함됩니다. 이 작업을 수행하면 롤백이 완료될 때까지 트래픽이 중단됩니다.

수행하려는 변경을 완료한 후에는 다음 절차에 따라 디바이스에 변경 사항을 배포합니다.

주의 threat defense 디바이스는 소프트웨어 리소스 문제가 있어 검사 엔진이 사용 중이거나, 컨피그레이션 배포 중에 특정 컨피그레이션으로 인해 엔진을 재시작해야 하여 엔진이 다운되면 트래픽을 삭제합니다. 재시작이 필요한 변경에 대한 자세한 내용은 검사 엔진을 재시작하는 컨피그레이션 변경, 37 페이지를 참조하십시오.

프로시저

단계 **1** 웹 페이지의 오른쪽 상단에 있는 **Deploy Changes(**변경 사항 구축**)** 아이콘을 클릭합니다.

배포되지 않은 변경 사항이 있으면 아이콘이 점으로 강조 표시됩니다.

Pending Changes(보류 중인 변경 사항) 창에는 컨피그레이션의 구축된 버전과 보류 중인 변경 사항을 비교한 내용이 표시됩니다. 이러한 변경 사항은 제거, 추가 또는 수정된 요소를 나타내기 위해 색상 코드가 지정됩니다. 색상의 설명은 창의 범례를 참조하십시오.

구축 시 검사 엔진을 재시작해야 하는 경우, 페이지에는 재시작이 필요한 변경 사항에 대한 세부 정보를 제공하는 메시지가 포함되어 있습니다. 현재 일시적인 트래픽 손실을 허용할 수 없는 경우, 대화 상자를 닫고 변경 내용을 구축하기에 더 좋은 시기를 기다립니다.

아이콘이 강조 표시되지 않아도 아이콘을 클릭하면 마지막으로 성공한 구축 작업의 날짜와 시간을 확인할 수 있습니다. 구축 기록을 표시하는 링크도 있습니다. 이 링크를 클릭하면 구축 작업만 표시하도록 필터링된 감사 페이지로 이동합니다.

단계 **2** 변경 사항에 만족하는 경우 **Deploy Now(**지금 구축**)**를 클릭하여 작업을 즉시 시작할 수 있습니다.

창에는 구축이 진행 중임이 표시됩니다. 창을 닫을 수도 있고 구축이 완료될 때까지 기다릴 수도 있습니다. 구축이 진행 중인 동안 창을 닫아도 작업은 중지되지 않습니다. 작업 목록이나 감사 로그에서 결과를 확인할 수 있습니다. 창을 열어 두는 경우 결과를 확인하려면 **Deployment History(**구축 기록**)** 링크를 클릭합니다.

선택적으로 다음을 수행할 수 있습니다.

- **Name the Job(**작업 이름 지정**)** — 구축 작업의 이름을 지정하려면 **Deploy Now(**지금 구축**)** 버튼의 드롭다운 화살표를 클릭하고 **Name the Deployment Job(**구축 작업 이름 지정**)**을 선택합니다. 그런 다음 이름을 입력하고 **Deploy(**구축**)**를 클릭합니다. 그러면 이름이 작업의 일부분으로 감사 및 구축 기록에 표시되므로 작업을 더 쉽게 찾을 수 있습니다.

  예를 들어 작업 이름을 "DMZ Interface Configuration(DMZ 인터페이스 컨피그레이션)"으로 지정하는 경우 성공한 구축 이름은 "Deployment Completed: DMZ Interface Configuration(구축 완료: DMZ 인터페이스 컨피그레이션)"으로 지정됩니다. 또한, 이 이름은 구축 작업과 관련된 Task Started(작업 시작됨) 및 Task Completed(작업 완료됨) 이벤트에서도 Event Name(이벤트 이름)으로 사용됩니다.

- **Force a full deployment(**전체 구축 강제**)** - 문제가 발생하여 시스템에서 변경 사항만이 아니라 전체 구성을 강제로 구축하도록 하려면 **Deploy Now(**지금 구축**)** 버튼의 드롭다운 화살표를 클릭하고 **Apply Full Deployment(**전체 구축 적용**)**를 선택합니다. 전체 구축에서는 트래픽이 중단되므로 이 작업을 수행할 것임을 확인해야 **Deploy(**구축**)**를 클릭할 수 있습니다.

- **Discard Changes(**변경 사항 취소**)** — 보류 중인 변경 사항을 모두 취소하려면 **More Options(**기타 옵션**)** > **Discard All(**모두 취소**)**을 클릭합니다. 그러면 취소를 확인하라는 메시지가 표시됩니다.
- **Copy Changes(**변경 사항 복사**)** — 변경 사항 목록을 클립보드에 복사하려면 **More Options(**기타 옵션**)** > **Copy to Clipboard(**클립보드에 복사**)**를 클릭합니다. 이 옵션은 변경 사항 수가 500개 미만일 때만 작동합니다.
- **Download Changes(**변경 사항 다운로드**)** — 변경 사항 목록을 파일로 다운로드하려면 **More Options(**기타 옵션**)** > **Download as Text(**텍스트로 다운로드**)**를 클릭합니다. 그러면 파일을 워크스테이션에 저장하라는 메시지가 표시됩니다. 파일은 YAML 형식입니다. YAML 형식을 구체적으로 지원하는 편집기가 없으면 텍스트 편집기에서 해당 파일을 볼 수 있습니다.

검사 엔진을 재시작하는 컨피그레이션 변경

다음 컨피그레이션 또는 작업 중 하나를 수행하면 컨피그레이션 변경 사항을 구축할 때 검사 엔진이 재시작됩니다.

⚠

주의 구축 시에는 리소스 요구사항으로 인해 약간의 패킷이 검사 없이 삭제될 수 있습니다. 또한, 일부 컨피그레이션을 구축하려면 검사 엔진을 재시작해야 하므로 트래픽 검사가 중단되고 트래픽이 삭제됩니다.

구축

일부 사항을 변경하려면 검사 엔진을 재시작해야 하며 이로 인해 일시적인 트래픽 손실이 발생합니다. 다음은 검사 엔진 재시작이 필요한 변경 사항입니다.

- SSL 암호 해독 정책이 활성화 또는 비활성화된 경우
- 하나 이상의 물리적 인터페이스(하위 인터페이스 제외)에서 MTU가 변경된 경우
- 액세스 제어 규칙에서 파일 정책을 추가하거나 제거하는 경우
- VDB가 업데이트된 경우
- 고가용성 컨피그레이션을 생성 또는 해제한 경우

또한 Snort 프로세스가 CPU 사용률이 60%를 초과한 상태로 사용 중인 경우 구축 중에 일부 패킷이 삭제될 수 있습니다. **show asp inspect-dp snort** 명령을 사용하면 Snort의 현재 CPU 사용률을 확인할 수 있습니다.

시스템 데이터베이스 업데이트

규칙 데이터베이스 또는 VDB에 업데이트를 다운로드하는 경우, 이를 활성화하려면 업데이트를 구축해야 합니다. 이 구축 작업 시 검사 엔진이 재시작될 수 있습니다. 수동으로 업데이트를 다운로드하거나 업데이트 일정을 정하는 경우, 다운로드 완료 후에 시스템이 변경 사항을 자동으로 구축해야

하는지를 설정할 수 있습니다. 시스템이 업데이트를 자동으로 구축하도록 설정하지 않은 경우, 업데이트는 다음에 변경 사항을 구축할 때 적용되며 이때 검사 엔진이 재시작될 수 있습니다.

시스템 업데이트

시스템을 재부팅하지 않으며 이진 변경을 포함하는 시스템 업데이트나 패치를 설치할 때는 검사 엔진을 재시작해야 합니다. 이진 변경에는 검사 엔진, 전처리기, VDB(Vulnerability Database) 또는 공유 개체 규칙 변경이 포함될 수 있습니다. 이진 변경을 포함하지 않는 패치 시에도 Snort를 재시작해야 할 수 있습니다.

인터페이스 및 관리 상태 보기

디바이스 요약에는 디바이스의 그래픽 보기와 관리 주소에 대한 일부 설정이 포함됩니다. Device Summary(디바이스 요약)를 열려면 **Device(**디바이스**)**를 클릭합니다.

이 그래픽의 요소는 요소 상태에 따라 색이 변경됩니다. 요소 위에 마우스를 놓으면 추가 정보가 제공되는 경우도 있습니다. 이 그래픽을 통해 다음 항목을 모니터링할 수 있습니다.

참고 인터페이스 상태 정보를 비롯한 그래픽의 인터페이스 부분은 **Interfaces(**인터페이스**)** 페이지와 **Monitoring(**모니터링**)** > **System(**시스템**)** 대시보드에서도 제공됩니다.

인터페이스 상태

포트 위에 마우스를 놓으면 해당 IP 주소와 활성화 상태 및 링크 상태가 표시됩니다. IP 주소는 정적으로 할당할 수도 있고 DHCP를 사용하여 가져올 수도 있습니다. BVI(Bridge Virtual Interface) 위에 마우스를 놓으면 멤버 인터페이스의 목록도 표시됩니다.

인터페이스 포트는 다음 색 코드를 사용합니다.

- 녹색 — 인터페이스가 구성되어 있고 활성화된 상태이며 링크가 작동합니다.
- 회색 — 인터페이스를 활성화하지 않습니다.
- 주황색/빨간색 — 인터페이스가 구성되어 있고 활성화된 상태이지만 링크가 작동하지 않습니다. 유선 인터페이스의 경우 이 색은 수정해야 하는 오류 상태를 나타냅니다. 유선 인터페이스가 아닌 경우에는 이 색이 표시되는 것이 정상입니다.

내부, 외부 네트워크 연결

그래픽에는 다음 조건에 따라 외부(또는 업스트림) 및 내부 네트워크에 연결된 포트가 표시됩니다.

- 내부 네트워크 — 내부 네트워크의 포트는 이름이 "내부"인 인터페이스에 대해서만 표시됩니다. 추가 내부 네트워크는 있더라도 표시되지 않습니다. 이름을 "내부"로 지정한 인터페이스가 없으면 어떤 포트도 내부 포트로 표시되지 않습니다.

- 외부 네트워크 — 외부 네트워크의 포트는 이름이 "외부"인 인터페이스에 대해서만 표시됩니다. 내부 네트워크와 마찬가지로 이 이름은 필수 항목입니다. 이름을 지정하지 않으면 어떤 포트도 외부 포트로 표시되지 않습니다.

관리 설정 상태

그래픽에는 관리 주소에 대해 게이트웨이, DNS 서버, NTP 서버 및 스마트 라이선싱이 구성되어 있는지와 해당 설정이 올바르게 작동하고 있는지가 표시됩니다.

녹색은 기능이 구성되어 있고 정상적으로 작동함을 나타내며, 회색은 기능이 구성되어 있지 않거나 정상적으로 작동하지 않음을 나타냅니다. 예를 들어 서버에 연결할 수 없으면 DNS 상자가 회색으로 표시됩니다. 요소 위에 마우스를 올려놓으면 추가 정보가 표시됩니다.

문제가 확인되면 다음과 같이 수정하십시오.

- 관리 포트 및 게이트웨이 — **System Settings(**시스템 설정**)** > **Management Interface(**관리 인터페이스**)**를 선택합니다.
- DNS 서버 — **System Settings(**시스템 설정**)** > **DNS Server(DNS** 서버**)**를 선택합니다.
- NTP 서버 — **System Settings(**시스템 설정**)** > **NTP**를 선택합니다. NTP 트러블슈팅, 892 페이지도 참조하십시오.
- 스마트 라이선스 — 스마트 라이선스 그룹에서 **View Configuration(**컨피그레이션 보기**)** 링크를 클릭합니다.

시스템 작업 상태 보기

시스템 작업에는 다양한 데이터베이스 업데이트 검색/적용 등 사용자가 직접 개입하지 않아도 수행되는 작업이 포함됩니다. 이러한 작업 및 해당 상태의 목록을 통해 이러한 시스템 작업이 성공적으로 완료됨을 확인할 수 있습니다.

작업 목록에는 시스템 작업 및 구축 작업의 통합된 상태가 표시됩니다. 감사 로그에는 더 자세한 정보가 포함되어 있는데, 이러한 감사 로그는 **Device(**디바이스**)** > **Device Administration(**디바이스 관리**)** > **Audit Log(**감사 로그**)**에서 얻을 수 있습니다. 예를 들어 감사 로그에는 작업 시작과 작업 종료에 대해 각기 별도의 이벤트가 표시되는 반면 작업 목록에서는 이러한 이벤트가 단일 항목으로 병합됩니다. 그리고 구축에 대한 감사 로그 항목에는 구축된 변경 사항과 관련된 세부 정보가 포함됩니다.

프로시저

단계 **1** 주 메뉴에서 **Task List(**작업 목록**)** 버튼을 클릭합니다.

작업 목록이 열리고 시스템 작업의 상태와 세부정보가 표시됩니다.

단계 **2** 작업 상태를 평가합니다.

지속적으로 발생하는 문제가 있으면 디바이스 컨피그레이션을 수정해야 할 수 있습니다. 예를 들어 데이터베이스 업데이트를 가져올 때 지속적으로 장애가 발생하면 인터넷으로 이동하는 디바이스 관리 IP 주소용 경로가 없는 것일 수 있습니다. 일부 문제의 경우 작업 설명에 나와 있는 대로 Cisco TAC(Technical Assistance Center)에 문의해야 할 수 있습니다.

작업 목록을 사용하여 다음 작업을 수행할 수 있습니다.

- **Success(**성공**)** 또는 **Failures(**실패**)** 버튼을 클릭하여 이러한 상태를 기준으로 목록을 필터링합니다.
- 작업의 삭제 아이콘( )을 클릭하여 목록에서 제거합니다.
- **Remove All Completed Tasks(**완료된 모든 작업 제거**)**를 클릭하여 진행 중이지 않은 모든 작업의 목록을 비웁니다.

CLI 콘솔을 사용하여 컨피그레이션 모니터링 및 테스트

Threat Defense 디바이스에는 모니터링 및 문제해결에 사용할 수 있는 CLI(Command Line Interface)가 포함되어 있습니다. SSH 세션을 열어 모든 시스템 명령에 대한 액세스 권한을 얻을 수 있지만, device manager에서 CLI 콘솔을 열어 읽기 전용 명령(예: 다양한 **show** 명령 및 **ping**, **traceroute**, **packet-tracer**)을 사용할 수도 있습니다. 관리자 권한을 보유한 경우, **failover**, **reboot**, **shutdown** 명령을 입력할 수도 있습니다.

페이지 간을 이동하고 기능을 구성 및 구축할 때 CLI 콘솔을 열어 둘 수 있습니다. 예를 들어 새 정적 경로를 구축한 후에 CLI 콘솔에서 **ping**을 사용하여 대상 네트워크에 연결할 수 있는지 확인할 수 있습니다.

CLI 콘솔에서는 기본 threat defense CLI를 사용합니다. CLI 콘솔을 사용하여 진단 CLI, 전문가 모드 또는 FXOS CLI(FXOS를 사용하는 모델)를 시작할 수는 없습니다. 기타 CLI 모드를 시작해야 하는 경우에는 SSH를 사용합니다.

명령에 대한 세부 정보는 Cisco Firepower Threat Defense 명령 참조, https://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.html을 참조 하십시오.

참고**:**

- **ping**은 CLI 콘솔에서 지원하지만 **ping system** 명령은 지원하지 않습니다.
- 시스템은 동시 명령을 2개까지만 처리할 수 있습니다. 따라서 다른 사용자가 REST API 등을 사용하여 명령을 실행 중이라면 명령을 입력하기 전에 다른 명령이 완료될 때까지 기다려야 할 수 있습니다. 문제가 지속되면 CLI 콘솔 대신 SSH 세션을 사용하십시오.
- 명령은 구축된 컨피그레이션을 기반으로 정보를 반환합니다. device manager에서 컨피그레이션을 변경하되 이를 구축하지 않을 경우, 명령 출력에 변경 결과가 표시되지 않습니다. 예를 들어 새 정적 경로를 생성하지만 이를 구축하지 않을 경우, 해당 경로는 **show route** 출력에 표시되지 않습니다.

프로시저

단계 **1** 웹 페이지의 오른쪽 상단에 있는 **CLI Console(CLI** 콘솔**)** 버튼을 클릭합니다.

단계 **2** 프롬프트에서 명령을 입력하고 **Enter** 키를 누릅니다.

일부 명령은 다른 명령보다 출력을 생성하는 데 오래 걸릴 수 있으니 기다려 주십시오. 명령 실행 시간 제한이 초과되었다는 메시지를 받으면 다시 시도하십시오. 또한 **show perfstats**와 같은 대화형 응답이 필요한 명령을 입력하는 경우, 타임 아웃 오류가 발생합니다. 문제가 지속되면 CLI 콘솔 대신 SSH 클라이언트를 사용해야 할 수 있습니다.

창을 사용하는 방법에 몇 가지 팁은 다음과 같습니다.

- 명령의 일부만 입력하면 자동으로 전체 명령이 입력되도록 하려면 **Tab** 키를 누릅니다. 또한, Tab 키를 누르면 명령에서 해당 시점에 사용할 수 있는 파라미터가 나열됩니다. Tab 키는 키워드의 세 가지 레벨에서 작동합니다. 세 가지 레벨 이후 자세한 내용을 확인하려면 명령 참조를 사용해야 합니다.
- Ctrl+C를 눌러 명령 실행을 중지할 수 있습니다.
- 창을 이동하려면 헤더의 아무 곳이나 클릭하여 누른 상태에서 원하는 위치로 창을 끌어옵니다.
- 창을 더 크게 또는 더 작게 조정하려면 **Expand(**확장**)(**  **)** 또는 **Collapse(**축소**)(****)** 버튼을 클릭합니다.
- 웹 페이지에서 창을 분리하여 사용 중인 브라우저 창에 도킹하려면 **Undock Into Separate Window(**분리하여 별도의 창에 도킹**)(**  **)** 버튼을 클릭합니다. 다시 도킹하려면 **Dock to Main Window(**기본 창에 도킹**)(****)** 버튼을 클릭합니다.
- 클릭하고 끌어 텍스트를 강조 표시한 다음 Ctrl+C를 눌러 출력을 클립보드에 복사합니다.
- 모든 출력을 지우려면 **Clear CLI(CLI** 지우기**)(****)** 버튼을 클릭합니다.
- 입력한 마지막 명령의 출력을 클립보드에 복사하려면 **Copy Last Output(**마지막 출력 복사**)(**  **)** 버튼을 클릭합니다.

단계 **3** 작업을 마치면 콘솔 창을 닫습니다. **exit** 명령은 사용하지 마십시오.

device manager에 로그인할 때 사용하는 크리덴셜은 CLI에 대한 액세스를 검증하지만, 콘솔을 사용할 때는 CLI에 실제로 로그인하지 않습니다.

Device Manager 및 REST API 함께 사용

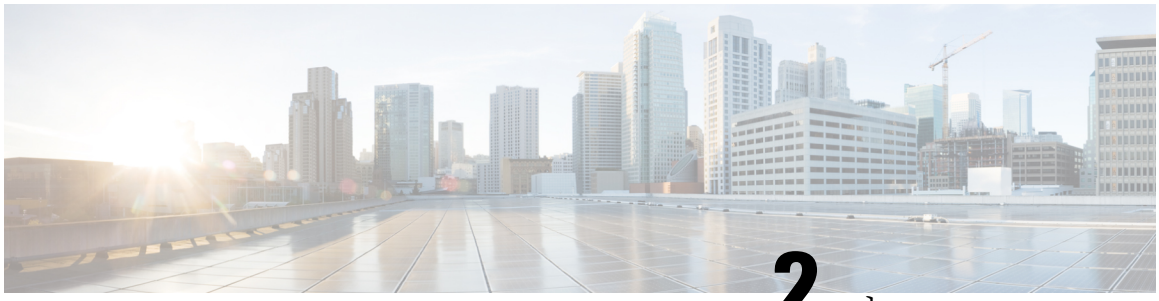
로컬 관리 모드로 디바이스를 설정할 때는 device manager와 threat defense REST API를 사용하여 디바이스를 구성할 수 있습니다. 실제로 device manager는 REST API를 사용하여 디바이스를 구성합니다.

그러나 REST API는 device manager를 통해 제공되는 기능 이외의 추가 기능을 제공할 수 있습니다. 따라서 특정 기능에 대해 device manager를 통해 컨피그레이션을 확인할 때는 표시할 수 없는 설정을 REST API를 통해서는 구성할 수도 있습니다.

REST API에서는 제공되지만 device manager에서는 제공되지 않는 기능 설정을 구성한 다음 device manager를 사용하여 원격 액세스 VPN 등의 전체 기능을 변경하는 경우에는 해당 설정이 실행 취소될 수 있습니다. API 전용 설정이 유지되는지 여부는 달라질 수 있으며, 많은 경우 device manager에서 사용할 수 없는 설정에 대한 API 변경 사항은 device manager 수정을 통해 유지됩니다. 특정 기능의 경우 변경 사항이 유지되는지 여부를 확인해야 합니다.

일반적으로, 특정 기능에 대해 device manager와 REST API를 동시에 사용해서는 안 됩니다. 대신 기능별로 한 가지 방법을 선택해 디바이스를 구성하십시오.

API Explorer를 사용하여 API 메서드를 확인하고 시도할 수 있습니다. More options(추가 옵션) 버튼 ( )을 클릭하고 **API Explorer**를 선택합니다.



2 장

모범 사례: Threat Defense의 사용 사례

다음 주제에서는 device manager를 사용하여 threat defense에서 수행할 수 있는 몇 가지 일반적인 작업에 대해 설명합니다. 이러한 활용 사례에서는 디바이스 컨피그레이션 마법사를 완료했으며 이 초기 컨피그레이션을 유지했다고 가정합니다. 초기 컨피그레이션을 수정했더라도 이러한 예를 통해 제품 사용 방법을 파악할 수 있습니다.

Device Manager에서 디바이스 구성 방법

설치 마법사를 완료하고 나면 작동 중인 디바이스에 몇 가지 기본 정책이 갖추어져 있어야 합니다.

- 외부 및 내부 인터페이스. 다른 데이터 인터페이스는 구성되지 않습니다.
- (Firepower 4100/9300) 데이터 인터페이스가 사전 구성되어 있지 않습니다.
- (ISA 3000) 브리지 그룹에는 2개의 내부 인터페이스와 2개의 외부 인터페이스가 있습니다. 설정을 완료하려면 BVI1의 IP 주소를 수동으로 설정해야 합니다.
- (Firepower 4100/9300 제외) 내부 및 외부 인터페이스용 보안 영역.
- (Firepower 4100/9300 제외) 내부에서 외부로 이동하는 모든 트래픽을 신뢰하는 액세스 규칙. ISA 3000에는 내부에서 외부로, 외부에서 내부로 이동하는 모든 트래픽을 허용하는 액세스 규칙이 있습니다.
- (Firepower 4100/9300 및 ISA 3000 제외) 내부에서 외부로 이동하는 모든 트래픽을 외부 인터페이스의 IP 주소에 있는 고유한 포트로 변환하는 인터페이스 NAT 규칙.

- (Firepower 4100/9300 및 ISA 3000 제외) 내부 인터페이스에서 실행 중인 DHCP 서버.

다음 단계에서는 구성하려는 추가적인 기능에 대한 개요가 제공됩니다. 각 단계에 대한 자세한 내용을 보려면 페이지에서 도움말 버튼(**?**)을 클릭하십시오.

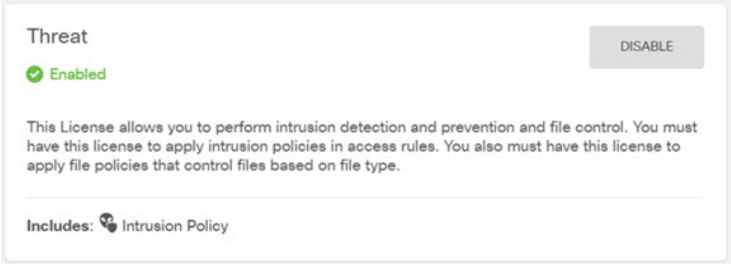
프로시저

단계 **1** 디바이스를 선택한 다음, **Smart License(**스마트 라이선스**)** 그룹에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

사용하려는 각 선택 라이선스(위협, 악성코드, URL)에서 활성화를 클릭합니다. 설치 시 디바이스를 등록한 경우, 원하는 RA VPN 라이선스를 활성화할 수도 있습니다. 필요 여부가 확실하지 않은 경우 각 라이선스에 대한 설명을 읽어보십시오.

등록하지 않은 경우에는 이 페이지에서 등록할 수 있습니다. **Register Device(**디바이스 등록**)**를 클릭하고 지침을 따릅니다. 평가 라이선스가 만료되기 전에 등록하십시오.

예를 들어 Secure Firewall Threat Defense IPS 라이선스를 활성화하면 다음과 같습니다.



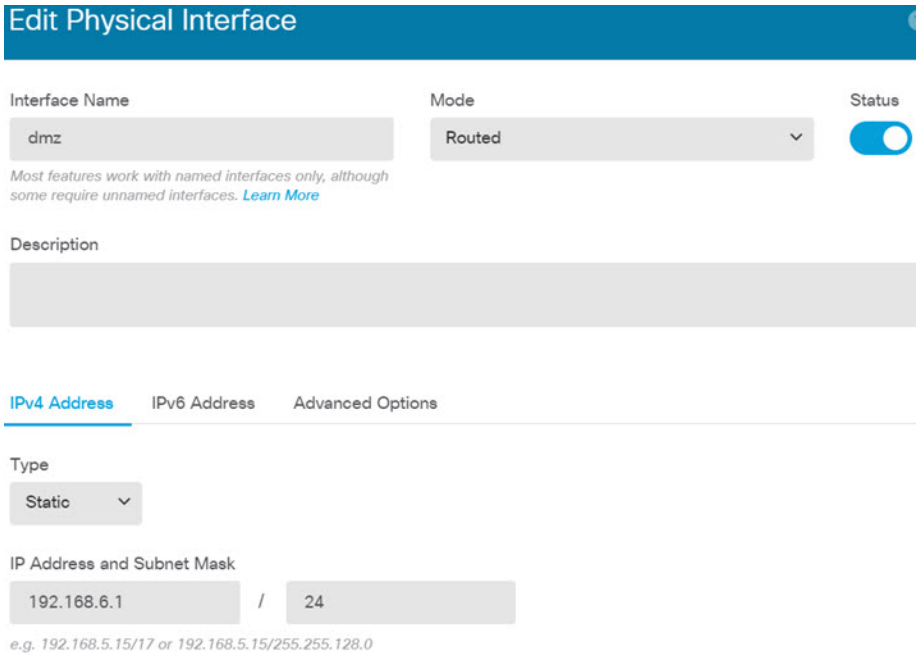
단계 **2** 다른 인터페이스에 유선으로 연결한 경우 디바이스를 선택하고 **Interfaces(**인터페이스**)** 요약의 링크를 클릭한 다음, 인터페이스 유형을 클릭하여 인터페이스 목록을 확인합니다.

- Firepower 4100/9300의 경우 이름, IP 주소 또는 보안 영역을 사용하여 사전 구성된 데이터 인터페이스가 없으므로 사용할 인터페이스를 활성화하고 구성해야 합니다.
- ISA 3000은 모든 데이터 인터페이스를 포함하는 브리지 그룹이 사전 구성된 상태로 제공되므로 이러한 인터페이스를 구성할 필요가 없습니다. 그러나 BVI에 대한 IP 주소를 수동으로 구성해야 합니다. 브리지 그룹을 분리하려는 경우에는 해당 그룹을 수정하여 개별적으로 처리할 인터페이스를 제거할 수 있습니다. 그러면 별도의 네트워크를 호스팅하도록 해당 인터페이스를 구성할 수 있습니다.

  다른 모델의 경우, 기타 인터페이스의 브리지 그룹을 생성하거나 별도의 네트워크를 구성하거나, 이 두 방법을 섞어서 사용할 수 있습니다.
- Firepower 1010의 경우 Ethernet1/1(외부)을 제외한 모든 인터페이스는 VLAN1(내부)에 할당된 액세스 모드 스위치 포트입니다. 스위치 포트를 방화벽 포트로 변경할 수 있습니다. 새 VLAN 인터페이스를 추가하고 스위치 포트를 해당 인터페이스에 할당하거나 트렁크 모드 스위치 포트를 구성합니다.

각 인터페이스의 편집 아이콘()을 클릭하여 IP 주소 및 기타 설정을 정의합니다.

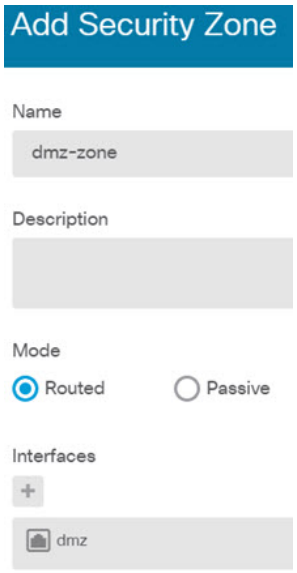
다음 예에서는 인터페이스를 웹 서버와 같이 공개적으로 액세스할 수 있는 자산을 배치하는 DMZ("Demilitarized Zone(비무장지대)")로 사용되도록 구성합니다. 완료되면 **Save(**저장**)**를 클릭합니다.



단계 **3** 새로운 인터페이스를 구성한 경우 목차에서 **Objects(**개체**)**를 선택한 다음 **Security Zones(**보안 영역**)**를 선택합니다.

새로운 영역을 적절히 편집하거나 생성합니다. 정책은 인터페이스가 아니라 보안 영역을 기반으로 구성하기 때문에 각 인터페이스는 하나의 영역에 속해 있어야 합니다. 인터페이스를 구성할 때는 영역에 인터페이스를 배치할 수 없으므로 새 인터페이스를 생성하거나 기존 인터페이스의 용도를 변경한 후에는 항상 영역 개체를 편집해야 합니다.

다음 예에는 dmz 인터페이스에서 새 dmz-zone을 생성하는 방법이 나와 있습니다.

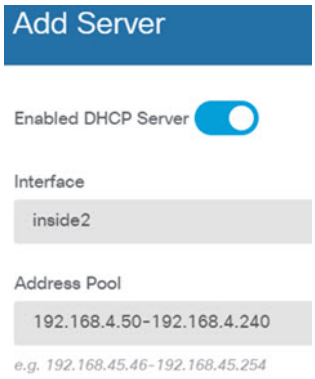


단계 **4** 내부 클라이언트가 DHCP를 사용하여 디바이스에서 IP 주소를 얻게 하려는 경우, 디바이스를 선택한 후 **System Settings(**시스템 설정**)** > **DHCP Server(DHCP** 서버**)**를 선택합니다. **DHCP Servers(DHCP** 서버**)** 탭을 선택합니다.

내부 인터페이스에 이미 DHCP 서버가 구성되어 있지만 주소 풀을 편집하거나 삭제할 수도 있습니다. 다른 내부 인터페이스를 구성한 경우, 이러한 인터페이스에서 DHCP 서버를 설정하는 것은 매우 일반적입니다. +를 클릭하여 각 내부 인터페이스에 서버 및 주소 풀을 구성합니다.

또한, **Configuration(**컨피그레이션**)** 탭에서 클라이언트에게 제공된 WINS 및 DNS 목록을 조정할 수 있습니다.

다음 예에는 주소 풀이 192.168.4.50-192.168.4.240인 inside2 인터페이스에서 DHCP 서버를 설정하는 방법이 나와 있습니다.



단계 **5** 디바이스를 선택한 후 **Routing(**라우팅**)** 그룹에서 **View Configuration(**컨피그레이션 보기**)**을 클릭하고 기본 경로를 구성합니다.

기본 경로는 일반적으로 외부 인터페이스 외에 있는 업스트림 또는 ISP 라우터를 가리킵니다. 기본 IPv4 경로는 any-ipv4(0.0.0.0/0)용인 반면, 기본 IPv6 경로는 any-ipv6(::0/0)용입니다. 사용하는 각 IP

버전에 대해 경로를 생성합니다. DHCP를 사용하여 외부 인터페이스에 대한 주소를 얻으려는 경우, 필요한 기본 경로가 이미 있을 수도 있습니다.

이 페이지에서 정의하는 경로는 데이터 인터페이스 전용입니다. 이러한 경로는 관리 인터페이스에 영향을 주지 않습니다. **System Settings(**시스템 설정**)** > **Management Interface(**관리 인터페이스**)**에서 관리 게이트웨이를 설정합니다.

다음 예에는 IPv4의 기본 경로가 나와 있습니다. 이 예에서 isp-gateway는 ISP 게이트웨이의 IP 주소(ISP에서 주소를 획득해야 함)를 식별하는 네트워크 개체입니다. 이 개체는 **Gateway(**게이트웨이**)** 드롭다운 목록의 아래쪽에서 **Create New Network(**새 네트워크 생성**)**를 클릭하여 생성할 수 있습니다.

단계 **6** **Policies(**정책**)**를 선택하고 네트워크의 보안 정책을 구성합니다.

디바이스 설치 마법사를 사용하면 외부 인터페이스로 이동할 때 모든 인터페이스에 대한 inside-zone, outside-zone 및 인터페이스 NAT 간의 트래픽 플로우가 가능합니다. 새 인터페이스를 구성하는 경우에도 inside-zone 개체에 이러한 인터페이스를 추가하면 이러한 인터페이스에 액세스 제어 규칙이 자동으로 적용됩니다.

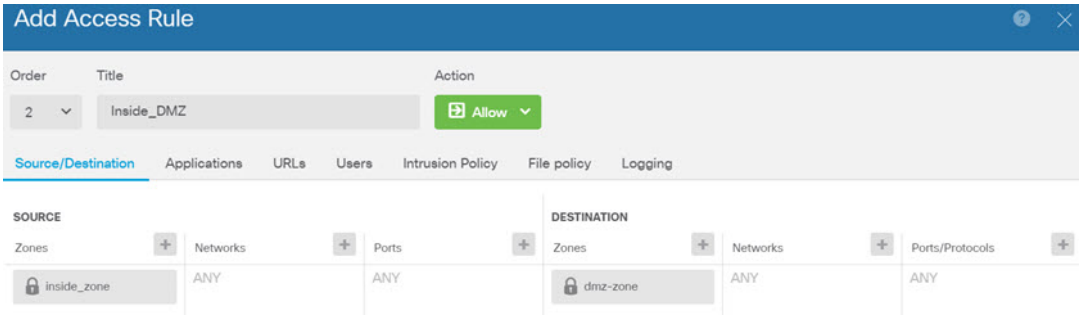
그러나 내부 인터페이스가 여러 개 있는 경우, inside-zone 간의 트래픽 플로우를 허용하기 위해 액세스 제어 규칙이 필요합니다. 다른 보안 영역을 추가하는 경우, 이러한 영역을 오고 가는 트래픽을 허용하는 규칙이 필요합니다. 이렇게 해야 변경 사항이 가장 적습니다.

또한, 다른 정책을 구성하여 추가 서비스를 제공할 수 있으며 NAT 및 액세스 규칙을 조정하여 조직에 필요한 결과를 얻을 수 있습니다. 다음과 같은 정책을 구성할 수 있습니다.

- **SSL Decryption(SSL** 암호 해독**)** — 침입, 악성코드 등에 대한 암호화된 연결(예: HTTPS)을 검사하려는 경우, 연결을 암호 해독해야 합니다. SSL 암호 해독 정책을 사용하여 어떤 연결을 암호 해독해야 할지 확인합니다. 시스템은 검사를 수행한 후에 연결을 다시 암호화합니다.
- **Identity(ID)** — 네트워크 활동과 개인 사용자의 상관관계를 분석하거나 사용자 또는 사용자 그룹 멤버십을 기반으로 네트워크 액세스를 제어하려면 ID 정책을 사용하여 지정된 소스 IP 주소와 연결된 사용자를 확인합니다.

- **Security Intelligence(보안 인텔리전스)** — 보안 인텔리전스 정책을 사용하여 선택된 IP 주소 또는 URL을 오가는 연결을 신속하게 삭제합니다. 알려진 유해 사이트를 차단하면 해당 사이트를 액세스 제어 정책에서 고려할 필요가 없습니다. Cisco에서는 알려진 유해 주소 및 URL에 대해 정기적으로 업데이트된 피드를 제공하므로 보안 인텔리전스 차단 목록이 동적으로 업데이트됩니다. 피드를 사용하는 경우에는 차단 목록에서 항목을 추가하거나 제거하기 위해 정책을 수정할 필요가 없습니다.
- **NAT**(Network Address Translation) — NAT 정책을 사용하여 내부 IP 주소를 외부에서 라우팅 가능한 주소로 변환합니다.
- **Access Control(액세스 제어)** — 액세스 제어 정책을 사용하여 네트워크에서 어떤 연결이 허용되는지 확인합니다. 보안 영역, IP 주소, 프로토콜, 포트, 애플리케이션, URL, 사용자 또는 사용자 그룹을 기준으로 필터링할 수 있습니다. 액세스 제어 규칙을 사용하여 침입 및 파일(악성코드) 정책을 적용할 수도 있습니다. 이 정책을 사용하여 URL 필터링을 구현할 수 있습니다.
- **Intrusion(침입)** — 침입 정책을 사용하여 알려진 위협을 검사합니다. 액세스 제어 규칙을 사용하여 침입 정책을 적용하는 경우에도 침입 정책을 편집하여 특정 침입 규칙을 선택적으로 활성화 또는 비활성화할 수 있습니다.

다음 예에는 액세스 제어 정책에서 inside-zone 및 dmz-zone 간의 트래픽을 허용하는 방법이 나와 있습니다. 이 예에서는 **Logging(로깅)**(**At End of Connection(연결 종료 시)**이 선택된 경우)을 제외하고는 다른 어떤 탭에도 옵션이 설정되어 있지 않습니다.



단계 **7** 변경 사항을 커밋합니다.

a) 웹 페이지의 오른쪽 상단에 있는 **Deploy Changes(변경 사항 구축)** 아이콘을 클릭합니다.

b) **Deploy Now(지금 구축)** 버튼을 클릭합니다.

구축이 완료될 때까지 기다리거나 **OK(확인)**를 클릭하고 나중에 작업 목록 또는 구축 기록을 확인할 수 있습니다.

네트워크 트래픽을 파악하는 방법

초기 디바이스 설정을 완료하고 나면 인터넷 또는 기타 업스트림 네트워크에 대한 모든 내부 트래픽 액세스를 허용하는 액세스 제어 정책과, 다른 모든 트래픽을 차단하는 기본 작업이 생성됩니다. 추가 액세스 제어 규칙을 생성하기 전에 실제로 네트워크에서 생성되는 트래픽을 파악해 두면 도움이 될 수 있습니다.

device manager의 모니터링 기능을 사용하여 네트워크 트래픽을 분석할 수 있습니다. Device Manager 보고는 다음 질문에 답하는 데 도움이 됩니다.

- 네트워크가 사용되는 용도
- 네트워크를 가장 많이 사용하는 사람
- 사용자가 이동하는 위치
- 사용자가 사용 중인 디바이스
- 가장 많이 적중된 액세스 제어 규칙(정책)

초기 액세스 규칙은 정책, 대상, 보안 영역 등 트래픽에 대한 일부 정보를 제공할 수 있습니다. 그러나 사용자 정보를 파악하려면 사용자의 인증(신원 증명)을 요구하는 ID 정책을 구성해야 합니다. 네트워크에서 사용되는 애플리케이션에 대한 정보를 파악하려면 몇 가지 추가적인 조정을 수행해야 합니다.

다음 절차에서는 트래픽을 모니터링하도록 threat defense 디바이스를 설정하는 방법을 설명하고, 정책을 컨피그레이션 및 모니터링하는 엔드 투 엔드 프로세스를 대략적으로 제시합니다.

참고 이 절차에서는 사용자가 방문하는 사이트의 웹 사이트 카테고리 및 평판 관련 정보는 제공하지 않습니다. 따라서 URL 카테고리 대시보드에서는 의미 있는 정보를 확인할 수 없습니다. 범주 및 평판 데이터를 파악하려면 범주 기반 URL 필터링을 구현하고 URL 라이선스를 활성화해야 합니다. 이 정보만 파악하려는 경우 금융 등 적절한 카테고리에 대한 액세스를 허용하는 새 액세스 제어 규칙을 추가하고, 액세스 제어 정책에서 이를 첫 번째 규칙으로 지정하면 됩니다. URL 필터링 구현에 대한 자세한 내용은 사용 제한 정책(URL 필터링)을 구현하는 방법, 65 페이지를 참조하십시오.

프로시저

단계 **1** 사용자 동작을 파악하려면 연결과 연관된 사용자를 식별할 수 있도록 ID 정책을 구성해야 합니다.

ID 정책을 활성화하면 네트워크를 사용 중인 사용자와 이러한 사용자가 사용하고 있는 리소스에 대한 정보를 수집할 수 있습니다. 이 정보는 사용자 모니터링 대시보드에서 제공됩니다. 이벤트 뷰어에서 표시되는 연결 이벤트에 대해서도 사용자 정보가 제공됩니다.

이 예시에서는 사용자 ID를 가져오기 위한 활성 인증을 구현합니다. 활성 인증을 사용하는 경우 디바이스에는 사용자에게 사용자 이름과 비밀번호를 입력하라는 메시지가 표시됩니다. 사용자는 HTTP 연결을 위해 웹 브라우저를 사용할 때만 인증을 받습니다.

사용자의 인증 시 장애가 발생해도 웹 연결은 차단되지 않습니다. 인증 장애는 연결을 위한 사용자 ID 정보가 없음을 의미할 뿐입니다. 원하는 경우 실패한 인증으로 표시되는 사용자의 트래픽을 삭제하는 액세스 제어 규칙을 생성할 수 있습니다.

a) 주 메뉴에서 **Policies(**정책**)**를 클릭한 후 **Identity(ID)**를 클릭합니다.

초기에는 ID 정책이 비활성화되어 있습니다. 활성 인증 사용 시 ID 정책은 AD(Active Directory) 서버를 통해 사용자를 인증하며, 사용자가 사용 중인 워크스테이션의 IP 주소와 사용자를 연결합니다. 그 후에 시스템은 해당 IP 주소의 트래픽을 사용자의 트래픽으로 식별합니다.

b) **Enable Identity Policy(ID** 정책 활성화**)**를 클릭합니다.

c) **Create Identity Rule(ID** 규칙 생성**)** 버튼 또는 **+** 버튼을 클릭하여 활성 인증 사용을 요구하는 규칙을 생성합니다.

이 예시에서는 모든 사용자에 대해 인증을 요구하려 한다고 가정합니다.

d) 규칙의 **Name(**이름**)**을 입력합니다. Require_Authentication 등의 원하는 이름을 선택하면 됩니다.

e) **Source/Destination(**소스/대상**)** 탭에서 기본값을 유지합니다. 이 경우 규칙이 적용되는 기준은 Any(모두)입니다.

보다 제한적인 트래픽 집합으로 정책을 적절하게 제한할 수 있습니다. 그러나 HTTP 트래픽에 대해서만 액티브 인증을 시도하므로 비HTTP 트래픽이 소스/대상 기준과 일치하는지 여부는 관계가 없습니다. ID 정책 속성에 대한 자세한 내용은 다음 주제를 참조하십시오. ID 규칙 구성, 498 페이지

f) **Action(**작업**)**에서 **Active Auth(**활성 인증**)**를 선택합니다.

ID 정책 설정을 구성하지 않았다고 가정할 때 일부 설정이 정의되지 않았으므로 Identity Policy Configuration(ID 정책 컨피그레이션) 대화 상자가 열립니다.

g) 활성 인증에 필요한 종속 포털 및 SSL 암호 해독 설정을 구성합니다.

ID 규칙에서 사용자에 대한 활성 인증을 요구하는 경우 사용자는 종속 포털 포트로 리디렉션되며, 이후에는 인증하라는 메시지가 표시됩니다. 종속 포털에는 SSL 암호 해독 규칙이 필요하며, 이러한 규칙은 시스템에서 자동으로 생성합니다. 하지만 SSL 암호 해독 규칙에 사용할 인증서는 선택해야 합니다.

- **Server Certificate(**서버 인증서**)** - 활성 인증 중에 사용자에게 제공할 내부 인증서를 선택합니다. 사전 정의된 셀프 서명한 DefaultInternalCertificate를 선택할 수도 있고, **Create New Internal Certificate(**새 내부 인증서 생성**)**를 클릭한 다음 브라우저에서 이미 신뢰하는 인증서를 업로드할 수도 있습니다.

  사용자의 브라우저에서 이미 신뢰하는 인증서를 업로드하지 않으면 사용자가 인증서를 허용해야 합니다.

- **Redirect to Host Name(**호스트 이름으로 리디렉션**)** — 활성 인증 요청에 대한 종속 포털로 사용해야 하는 인터페이스의 정규화된 호스트 이름을 정의하는 네트워크 개체를 선택합니다. 개체가 없는 경우, **Create New Network(**새 네트워크 생성**)**를 클릭합니다.

FQDN은 디바이스에 있는 인터페이스 중 하나의 IP 주소로 확인되어야 합니다. FQDN을 사용하면 클라이언트가 인식할 활성 인증에 대한 인증서를 할당할 수 있으므로, IP 주소로 리디렉션될 때 신뢰할 수 없는 인증서 경고가 표시되지 않습니다. 인증서는 인증서의 SAN(Subject Alternate Name)에 FQDN, 와일드카드 FQDN 또는 여러 FQDN을 지정할 수 있습니다.

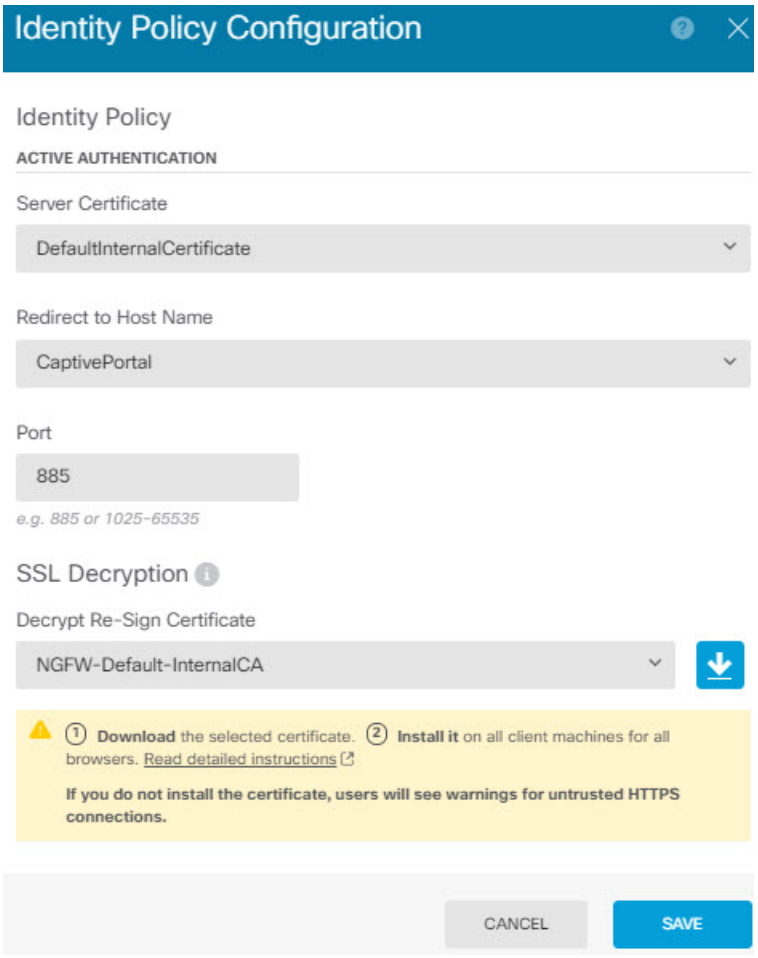
ID 규칙에서 사용자에 대한 활성 인증을 요구하지만 리디렉션 FQDN을 지정하지 않는 경우 사용자는 연결 시 사용한 인터페이스의 종속 포털 포트로 리디렉션됩니다.

- **Port(**포트**)** - 종속 포털 포트입니다. 기본값은 885(TCP)입니다. 다른 포트를 구성하는 경우에는 포트가 1025-65535 범위에 포함되어야 합니다.
- **Decrypt Re-Sign Certificate(**재서명 암호 해독 인증서**)** - 재서명된 인증서를 이용하여 암호 해독을 구현하는 규칙에 사용할 내부 CA 인증서를 선택합니다. 사전 정의된 NGFW-Default-InternalCA 인증서(기본값)를 사용하거나, 생성 또는 업로드한 인증서를 사용할 수 있습니다. 인증서가 아직 없으면 **Create Internal CA(**내부 **CA** 생성**)**를 클릭하여 생성합니다. (SSL 암호 해독 정책을 아직 활성화하지 않은 경우에만 암호 해독 재서명 인증서를 요구하는 메시지가 표시됩니다.)

  클라이언트 브라우저에서 인증서를 아직 설치하지 않은 경우, 다운로드 버튼()을 클릭하여 복사본을 획득합니다. 인증서 설치 방법에 대한 자세한 내용은 각 브라우저에 대한 설명서를 참조하십시오. 재서명 암호 해독 규칙을 위한 CA 인증서 다운로드, 484 페이지도 참조하십시오.

예제**:**

이제 ID 정책 컨피그레이션 대화 상자가 다음과 같이 표시됩니다.



h) **Save(**저장**)**를 클릭하여 활성 인증 설정을 저장합니다.

이제 Action(작업) 설정 아래에 Active Authentication(활성 인증) 탭이 나타납니다.

i) **Active Authentication(**활성 인증**)** 탭에서 **HTTP Negotiate(HTTP** 협상**)**를 선택합니다.

이 옵션을 선택하면 브라우저와 디렉토리 서버가 가장 강력한 인증 프로토콜(NTLM->HTTP 기본 순서)을 협상할 수 있습니다.

참고 호스트 이름으로 리디렉션 FQDN을 제공하지 않는 경우 HTTP 기본, HTTP 응답 페이지 및 NTLM 인증 방법에서 인터페이스의 IP 주소를 사용하여 사용자를 종속 포털로 리디렉션합니다. 그러나 HTTP 협상의 경우에는 사용자가 정규화된 DNS 이름 *firewall-hostname.AD-domain-name*을 사용하여 리디렉션됩니다. 호스트 이름으로 리디렉션 FQDN 없이 HTTP 협상을 사용하려는 경우에는 DNS 서버도 업데이트하여 활성 인증을 수행해야 하는 모든 내부 인터페이스의 IP 주소에 이 이름을 매핑해야 합니다. 이렇게 하지 않으면 리디렉션을 완료할 수 없으며 사용자가 인증할 수 없습니다. 인증 방법과 무관하게 일관된 동작을 보장하기 위해 항상 호스트 이름으로 리디렉션 FQDN을 제공하는 것이 좋습니다. 수행할 수 없거나 원치 않는 경우 DNS 서버를 업데이트하고 다른 인증 방법 중 하나를 선택합니다.

j) **AD Identity Source(AD ID 소스)**에 대해 **Create New Identity Realm(새 ID 영역 생성)**을 클릭합니다.

영역 서버 개체를 이미 생성한 경우에는 해당 개체를 선택하고 서버 구성 단계를 건너뛰면 됩니다.

다음 필드에 내용을 입력하고 **OK(확인)**를 클릭합니다.

- **Name(이름)** - 디렉토리 영역의 이름입니다.
- **Type(유형)** - 디렉터리 서버의 유형입니다. 지원되는 유형은 Active Directory뿐이며 이 필드의 내용은 변경할 수 없습니다.
- **Directory Username(디렉터리 사용자 이름)**, **Directory Password(디렉터리 비밀번호)** - 검색하려는 사용자 정보에 대한 적절한 권한이 있는 사용자의 고유 사용자 이름 및 비밀번호입니다. Active Directory의 경우에는 사용자에게 상승된 권한이 필요하지 않습니다. 도메인에 어떤 사용자라도 지정할 수 있습니다. 사용자 이름은 모든 자격 요건에 부합해야 합니다(예: 단지 Administrator가 아닌 Administrator@example.com).

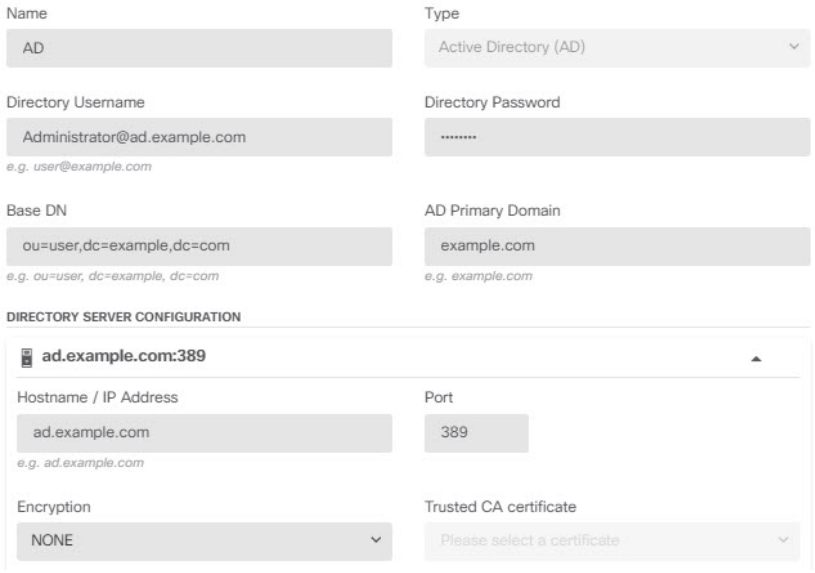
  참고 시스템은 이 정보에서 ldap-login-dn 및 ldap-login-password를 생성합니다. 예를 들어 Administrator@example.com은 cn=administrator,cn=users,dc=example,dc=com으로 변환됩니다. cn=users는 항상 이 변환에 포함되므로 일반 이름 "users" 폴더 아래에 여기서 지정하는 사용자를 구성해야 합니다.

- **Base DN(기본 DN)** - 사용자 및 그룹 정보를 검색하거나 쿼리하기 위한 디렉터리 트리, 즉 사용자와 그룹의 공통 상위 항목입니다. dc=example,dc=com을 예로 들 수 있습니다. 기본 DN을 찾는 방법에 대한 자세한 내용은 디렉터리 기본 DN 결정, 176 페이지를 참조하십시오.
- **AD Primary Domain(AD 기본 도메인)** - 디바이스가 조인해야 하는 정규화된 Active Directory 도메인 이름입니다. example.com 등을 예로 들 수 있습니다.
- **Hostname/IP Address(호스트 이름/IP 주소)** - 디렉터리 서버의 호스트 이름 또는 IP 주소입니다. 서버에 대한 암호화된 연결을 사용하는 경우에는 IP 주소가 아닌 FQDN(Fully-Qualified Domain Name)을 입력해야 합니다.
- **Port(포트)** - 서버와의 통신에 사용되는 포트 번호입니다. 기본값은 389입니다. 암호화 방법으로 LDAPS를 선택하는 경우에는 포트 636을 사용합니다.
- **Encryption(암호화)** - 사용자 및 그룹 정보를 다운로드하기 위해 암호화된 연결을 사용하려는 경우에는 **STARTTLS** 또는 **LDAPS** 중에서 원하는 방법을 선택합니다. 기본값은 **None(없음)**입니다. 이 옵션은 사용자 및 그룹 정보를 일반 텍스트로 다운로드함을 의미합니다.
  - **STARTTLS**는 암호화 방법을 협상하여 디렉토리 서버가 지원하는 가장 강력한 방법을 사용하며 포트 389를 사용합니다. 원격 액세스 VPN에 영역을 사용하는 경우에는 이 옵션이 지원되지 않습니다.
  - **LDAPS**를 선택하는 경우 LDAP over SSL이 필요합니다. 이 옵션은 포트 636을 사용합니다.

- **Trusted CA Certificate(**신뢰할 수 있는 **CA** 인증서**)** - 암호화 방법을 선택하는 경우 CA(인증 증명) 인증서를 업로드하여 시스템과 디렉터리 서버 간에 신뢰할 수 있는 연결을 설정합니다. 인증서를 사용하여 인증하는 경우에는 인증서의 서버 이름이 서버 호스트 이름/IP 주소와 일치해야 합니다. 예를 들어 IP 주소로 10.10.10.250을 사용하는데 인증서의 주소는 ad.example.com이면 연결은 실패합니다.

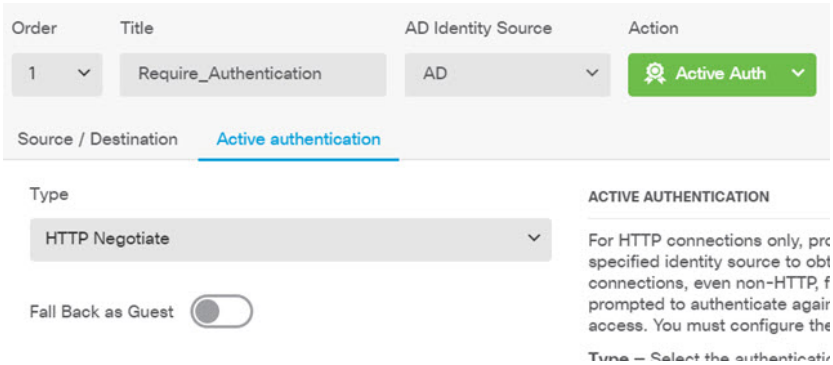
예제:

예를 들어 다음 그림에는 ad.example.com 서버에 대해 암호화되지 않은 연결을 생성하는 방법이 나와 있습니다. 여기서 기본 도메인은 example.com이고 디렉터리 사용자 이름은 Administrator@ad.example.com입니다. 모든 사용자 및 그룹 정보는 DN(고유 이름) ou=user,dc=example,dc=com 아래에 있습니다.



k) **AD Identity Source(AD ID** 소스**)**에 대해 방금 생성한 개체를 선택합니다.

규칙이 다음과 유사하게 표시됩니다.



l) **OK(**확인**)**를 클릭하여 규칙을 추가합니다.

이제 창 오른쪽 상단의 **Deploy(**구축**)** 아이콘 버튼에 점이 나타납니다. 이 점은 구축되지 않은 변경 사항이 있음을 나타냅니다. 사용자 인터페이스에서 변경을 수행한다고 해서 디바이스에서

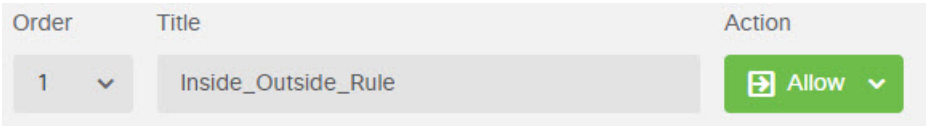
변경 사항이 구성되는 것은 아니며, 변경 사항을 구축해야 합니다. 따라서 관련 변경 집합을 먼저 수행한 후에 변경 사항을 구축하면 부분적으로 구성된 변경 사항 집합이 디바이스에서 실행되는 문제가 발생할 가능성이 없습니다. 이 절차의 뒷부분에서 변경 사항을 구축할 것입니다.

단계 **2** Inside_Outside_Rule 액세스 제어 규칙의 작업을 **Allow(**허용**)**로 변경합니다.

Inside_Outside_Rule 액세스 규칙은 신뢰 규칙으로 생성됩니다. 그러나 신뢰할 수 있는 트래픽은 검사되지 않으므로, 트래픽 일치 기준에 영역, IP 주소 및 포트 외의 기타 조건이나 애플리케이션이 포함되어 있지 않으면 시스템은 신뢰할 수 있는 트래픽의 일부 특성(예: 애플리케이션)을 확인할 수 없습니다. 트래픽을 신뢰하는 대신 허용하도록 규칙을 변경하면 시스템이 트래픽을 완전히 검사합니다.

참고 (ISA 3000) Outside_Inside_Rule, Inside_Inside_Rule 및 Outside_Outside_Rule도 Trust(신뢰)에서 Allow(허용)로 변경하는 것이 좋습니다.

a) **Policies(**정책**)** 페이지에서 **Access Control(**액세스 제어**)**을 클릭합니다.
b) Inside_Outside_Rule 행 오른쪽의 **Actions(**작업**)** 셀 위에 마우스를 올려 놓고 수정 및 삭제 아이콘이 표시되면 수정 아이콘( )을 클릭하여 규칙을 엽니다.
c) **Action(**작업**)**에 대해 **Allow(**허용**)**를 선택합니다.

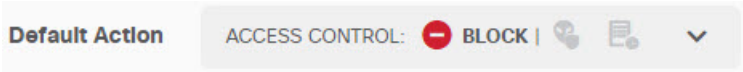


d) **OK(**확인**)**를 클릭하여 변경 사항을 저장합니다.

단계 **3** 액세스 제어 정책 기본 작업에 대해 로깅을 활성화합니다.

연결이 연결 로깅을 활성화하는 액세스 제어 규칙과 일치하는 경우에만 대시보드에 연결 관련 정보가 포함됩니다. Inside_Outside_Rule은 로깅을 활성화하지만 기본 작업에서는 로깅이 비활성화됩니다. 따라서 대시보드에는 Inside_Outside_Rule에 대한 정보만 표시되며 규칙과 일치하지 않는 연결은 대시보드에 반영되지 않습니다.

a) 액세스 제어 정책 페이지 하단의 기본 작업에서 아무 곳이나 클릭합니다.



b) **Select Log Action(**로그 작업 선택**)** > **At Beginning and End of Connection(**연결 시작 및 종료 시**)**을 선택합니다.
c) **OK(**확인**)**를 클릭합니다.

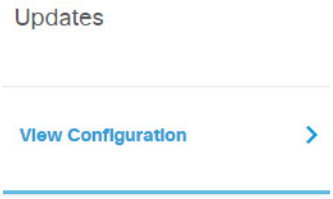
단계 **4** VDB(Vulnerability Database)의 업데이트 일정을 설정합니다.

Cisco는 VDB 업데이트를 정기적으로 제공합니다. 이 업데이트에는 연결에서 사용되는 애플리케이션을 식별할 수 있는 애플리케이션 탐지기가 포함됩니다. VDB는 정기적으로 업데이트해야 합니다. 업데이트는 수동으로 다운로드할 수도 있고 정기 일정을 설정할 수도 있습니다. 다음 절차에서는 일

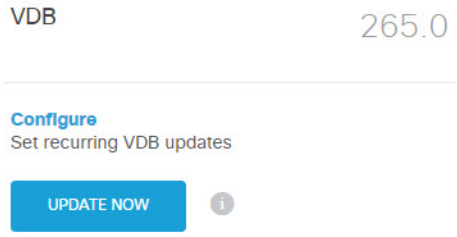
정을 설정하는 방법을 보여줍니다. VDB 업데이트는 기본적으로 비활성화되므로 VDB 업데이트를 받기 위한 작업을 수행해야 합니다.

a) 디바이스를 클릭합니다.

b) 업데이트 그룹에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.



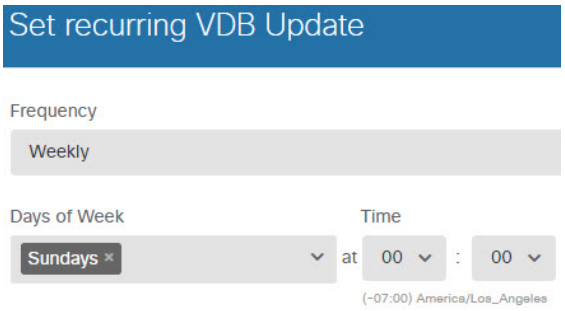
c) VDB 그룹에서 **Configure(**구성**)**를 클릭합니다.



d) 업데이트 일정을 정의합니다.

네트워크에 영향을 주지 않는 시간과 빈도를 선택합니다. 또한 시스템은 업데이트를 다운로드한 후에 자동 구축을 수행합니다. 새 탐지기를 사용하려면 자동 구축을 수행해야 합니다. 따라서 수행하고 저장했지만 구축하지는 않은 컨피그레이션 변경 사항도 구축됩니다.

예를 들어 다음 일정은 매주 일요일 자정(24시간 표기법 사용)에 VDB를 업데이트합니다.



e) **Save(**저장**)**를 클릭합니다.

단계 **5** 변경 사항을 커밋합니다.

a) 웹 페이지의 오른쪽 상단에 있는 **Deploy Changes(**변경 사항 구축**)** 아이콘을 클릭합니다.

b) **Deploy Now(**지금 구축**)** 버튼을 클릭합니다.

구축이 완료될 때까지 기다리거나 **OK(**확인**)**를 클릭하고 나중에 작업 목록 또는 구축 기록을 확인할 수 있습니다.

다음에 수행할 작업

이 시점부터 모니터링 대시보드 및 이벤트에 사용자 및 애플리케이션에 대한 정보가 표시됩니다. 이 정보를 평가하여 부적절한 패턴이 있는지 확인하고 허용할 수 없는 사용을 제한하는 새 액세스 규칙을 개발할 수 있습니다.

침입 및 악성코드 관련 정보 수집을 시작하려면 하나 이상의 액세스 규칙에 대해 침입 및 파일 정책을 활성화해야 합니다. 또한 이러한 기능에 대한 라이선스도 활성화해야 합니다.

URL 카테고리 관련 정보 수집을 시작하려면 URL 필터링을 구현해야 합니다.

위협을 차단하는 방법

액세스 제어 규칙에 침입 정책을 추가하여 차세대 IPS(침입 방지 시스템) 필터링을 구현할 수 있습니다. 침입 정책은 네트워크 트래픽을 분석하여 트래픽 콘텐츠와 알려진 위협을 비교합니다. 연결이 모니터링 대상 위협과 일치하는 경우 시스템은 연결을 삭제하여 공격을 방지합니다.

기타 모든 트래픽 처리는 네트워크 트래픽에서 침입을 검사하기 전에 수행됩니다. 침입 정책을 액세스 제어 규칙과 연결하여 시스템이 액세스 제어 규칙의 조건과 일치하는 트래픽을 통과시키기 전에 침입 정책을 사용하여 트래픽을 먼저 검사하도록 명령할 수 있습니다.

트래픽을 **allow(**허용**)**하는 규칙에 대해서만 침입 정책을 구성할 수 있습니다. 트래픽을 **trust(**신뢰**)** 또는 **block(**차단**)**하도록 설정된 규칙에 대해서는 검사가 수행되지 않습니다. 또한 기본 작업이 **allow(**허용**)**인 경우 기본 작업의 일부분으로 침입 정책을 구성할 수 있습니다.

침입 정책은 고급 설정과 침입 및 전처리기 규칙 상태를 설정한 Cisco Talos Intelligence Group(Talos)에서 고안했습니다. Snort 3을 검사 엔진으로 사용하는 경우 Talos 정책을 기반으로 고유한 맞춤형 정책을 생성할 수 있습니다.

허용하는 트래픽의 침입 가능성을 검사하는 것 외에, 보안 인텔리전스 정책을 사용하여 알려진 잘못된 IP 주소에서 나가거나 들어오는 모든 트래픽이나 알려진 잘못된 URL로 나가는 모든 트래픽을 사전에 차단할 수 있습니다.

프로시저

단계 **1** 아직 수행하지 않은 경우 위협 라이선스를 활성화합니다.

침입 정책 및 보안 인텔리전스를 사용하려면 위협 라이선스를 활성화해야 합니다. 현재 평가 라이선스를 사용 중인 경우에는 라이선스의 평가 버전이 활성화됩니다. 디바이스를 등록한 경우 필요한 라이선스를 구매해 Cisco.com에서 Smart Software Manager 어카운트에 추가해야 합니다.

a) 디바이스를 클릭합니다.
b) 스마트 라이선스 그룹에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

c) 위협 그룹에서 **Enable(**활성화**)**을 클릭합니다.

시스템이 적절하게 어카운트에 라이선스를 등록하거나 평가 라이선스를 사용 설정합니다. 그룹에 라이선스가 활성화되었다는 메시지가 표시되며 버튼이 Disable(비활성화) 버튼으로 변경됩니다.

단계 **2** 하나 이상의 액세스 규칙에 대해 침입 정책을 선택합니다.

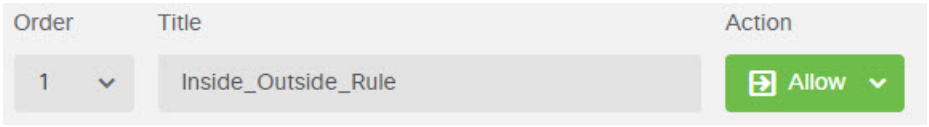
위협을 검사해야 하는 트래픽에 적용할 규칙을 결정합니다. 이 예에서는 Inside_Outside_Rule에 침입 검사를 추가합니다.

a) 주 메뉴에서 **Policies(**정책**)**를 클릭합니다.

Access Control(액세스 제어**)** 정책이 표시되는지 확인합니다.

b) Inside_Outside_Rule 행 오른쪽의 **Actions(**작업**)** 셀 위에 마우스를 올려 놓고 수정 및 삭제 아이콘이 표시되면 수정 아이콘( )을 클릭하여 규칙을 엽니다.

c) **Action(**작업**)**에 대해 **Allow(**허용**)**를 아직 선택하지 않았으면 선택합니다.

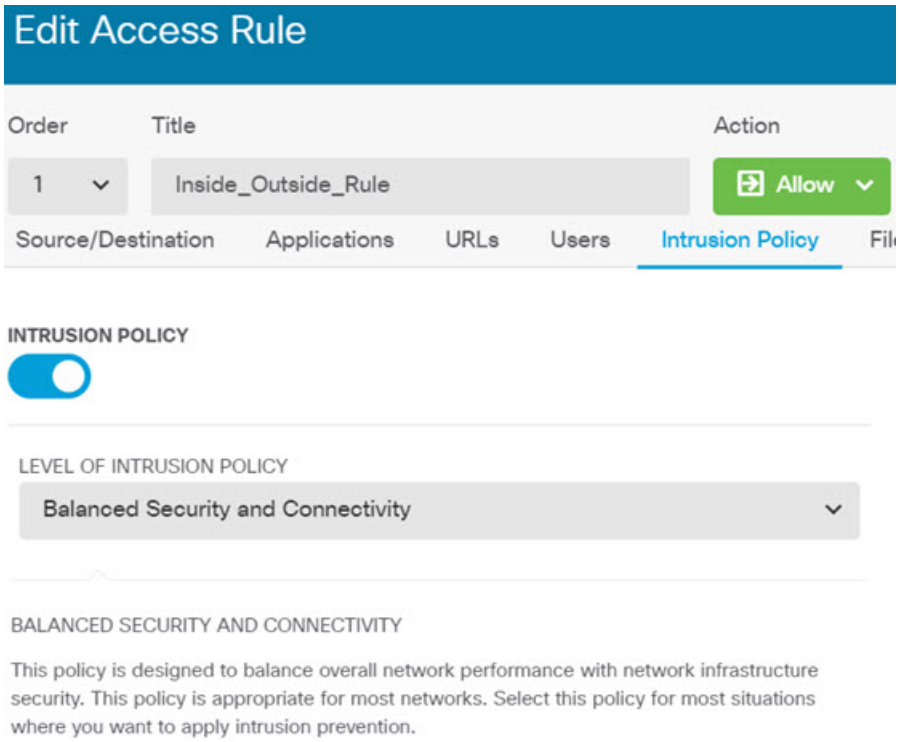


d) **Intrusion Policy(**침입 정책**)** 탭을 클릭합니다.

e) **Intrusion Policy(**침입 정책**)** 토글을 클릭하여 정책을 활성화한 다음 침입 정책을 선택합니다.

Balanced Security and Connectivity(보안과 연결의 균형 유지**)** 정책은 대부분의 네트워크에 적합합니다. 이 정책은 과도하게 적극적이지 않은 적절한 침입 방어 기능을 제공합니다. 침입 방지 기능이 너무 적극적이면 삭제되면 안 되는 트래픽이 삭제될 수 있습니다. 트래픽이 너무 많이 삭제되는지 확인하려는 경우 **Connectivity over Security(**연결이 보안에 우선함**)** 정책을 선택하여 침입 검사의 레벨을 높일 수 있습니다.

적극적인 보안을 적용해야 하는 경우에는 **Security over Connectivity(**보안이 연결에 우선함**)** 정책을 사용해 보십시오. **Maximum Detection(**최대 탐지**)** 정책은 네트워크 인프라 보안을 더욱 강화하며, 사용하는 경우 운영에 더 큰 영향을 미칠 수 있습니다.



f) **OK(**확인**)**를 클릭하여 변경 사항을 저장합니다.

단계 **3** (선택 사항) **Policies(**정책**)** > **Intrusion(**침입**)**으로 이동하여 기어 아이콘을 클릭하고 침입 정책에 대한 시스템 로그 서버를 구성합니다.

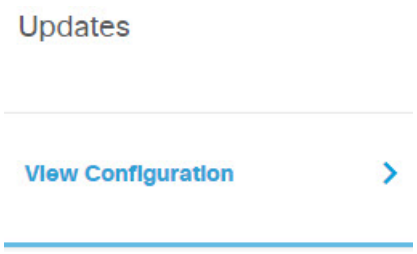
침입 이벤트는 액세스 제어 규칙에 대해 구성된 시스템 로그 서버를 사용하지 않습니다.

단계 **4** 침입 규칙 데이터베이스의 업데이트 일정을 설정합니다.

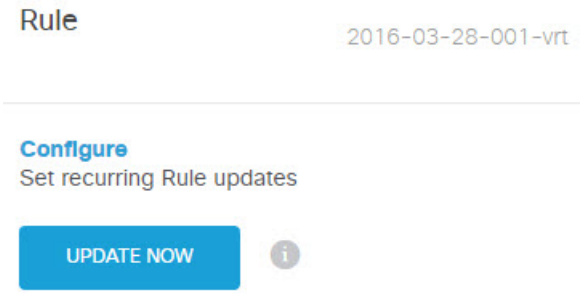
Cisco는 침입 정책이 연결을 삭제해야 하는지 여부를 결정하는 데 사용하는 침입 규칙 데이터베이스에 대한 업데이트를 정기적으로 제공합니다. 규칙 데이터베이스는 정기적으로 업데이트해야 합니다. 업데이트는 수동으로 다운로드할 수도 있고 정기 일정을 설정할 수도 있습니다. 다음 절차에서는 일정을 설정하는 방법을 보여줍니다. 기본값으로 데이터베이스 업데이트는 비활성화되므로 업데이트된 규칙을 받기 위한 작업을 수행해야 합니다.

a) 디바이스를 클릭합니다.

b) 업데이트 그룹에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.



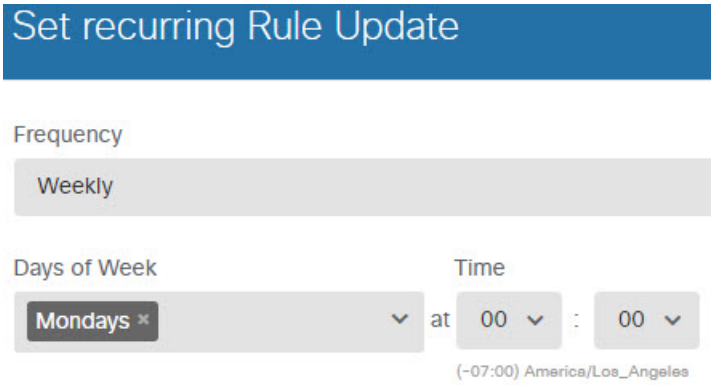
c) 규칙 그룹에서 **Configure(**구성**)**를 클릭합니다.



d) 업데이트 일정을 정의합니다.

네트워크에 영향을 주지 않는 시간과 빈도를 선택합니다. 또한 시스템은 업데이트를 다운로드한 후에 자동 구축을 수행합니다. 새 규칙을 사용하려면 자동 구축을 수행해야 합니다. 따라서 수행하고 저장했지만 구축하지는 않은 컨피그레이션 변경 사항도 구축됩니다.

예를 들어 다음 일정은 매주 월요일 자정(24시간 표기법 사용)에 규칙 데이터베이스를 업데이트합니다.



e) **Save(**저장**)**를 클릭합니다.

단계 **5** 알려진 잘못된 호스트 및 사이트와의 연결을 사전에 삭제하도록 보안 인텔리전스 정책을 구성합니다.

보안 인텔리전스를 사용하여 위협으로 알려진 호스트 또는 사이트와의 연결을 차단하면 시스템이 DPI(Deep Packet Inspection)를 수행하여 각 연결의 위협을 식별하는 데 필요한 시간을 절약할 수 있습니다. 보안 인텔리전스를 사용하면 원치 않는 트래픽을 일찍 차단할 수 있으므로 시스템이 실제로 중요한 트래픽을 처리하는 데 더 많은 시간을 할애할 수 있습니다.

a) **Device(**디바이스**)**를 클릭한 다음 **Updates(**업데이트**)** 그룹에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

b) Security Intelligence Feeds(보안 인텔리전스 피드) 그룹에서 **Update Now(**지금 업데이트**)**를 클릭합니다.

c) 또한 **Configure(**구성**)**를 클릭하여 피드에 대해 반복 업데이트를 설정합니다. 대부분의 네트워크에는 기본값인 **Hourly(**매시간**)**가 적절하지만 필요한 경우 빈도를 줄일 수 있습니다.

d) **Policies(**정책**)**를 클릭한 다음 **Security Intelligence(**보안 인텔리전스**)** 정책을 클릭합니다.

e) 정책을 아직 활성화하지 않은 경우 **Enable Security Intelligence(**보안 인텔리전스 활성화**)**를 클릭합니다.

f) **Network(**네트워크**)** 탭에서 차단/삭제 목록에 있는 **+**를 클릭하고 **Network Feeds(**네트워크 피드**)** 탭에서 모든 피드를 선택합니다. 피드 옆의 **i** 버튼을 클릭하면 각 피드의 설명을 확인할 수 있습니다.

아직 피드가 없다는 메시지가 표시되면 나중에 다시 시도하십시오. 피드 다운로드가 아직 완료되지 않은 것입니다. 이 문제가 계속되면 관리 IP 주소와 인터넷 간에 경로가 있는지 확인하십시오.

g) **OK(**확인**)**를 클릭하여 선택한 피드를 추가합니다.

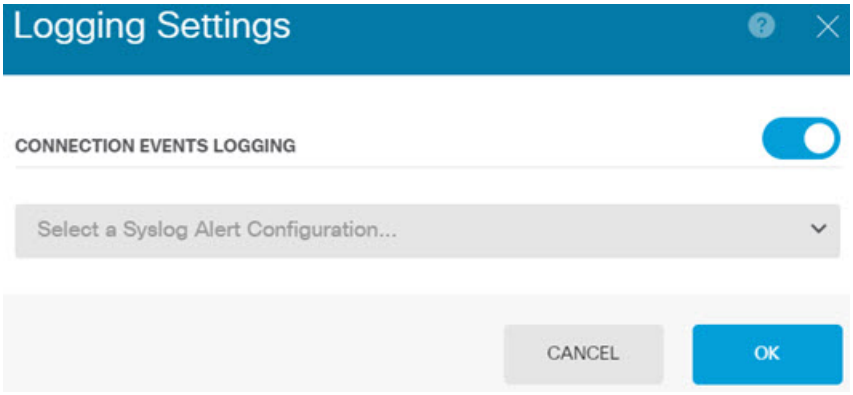
잘못된 IP 주소를 추가로 알고 있다면 **+** > **Network Objects(**네트워크 개체**)**를 클릭하고 해당 주소가 포함된 개체를 추가할 수 있습니다. 목록 아래쪽의 **Create New Network Object(**새 네트워크 개체 생성**)**를 클릭하면 지금 해당 개체를 추가할 수 있습니다.

h) **URL** 탭을 클릭한 다음 차단/삭제 목록에 있는 **+** > **URL Feeds(URL** 피드**)**를 클릭하고 모든 URL 피드를 선택합니다. **OK(**확인**)**를 클릭하여 목록에 추가합니다.

네트워크 목록과 마찬가지로 목록에 자체 URL 개체를 추가해 피드에 없는 추가 사이트를 차단할 수 있습니다. **+** > **URL Objects(URL** 개체**)**를 클릭합니다. 목록 끝에 있는 **Create New URL Object(**새 **URL** 개체 생성**)**를 클릭하면 새 개체를 추가할 수 있습니다.

i) 기어 아이콘을 클릭하고 **Connection Events Logging(**연결 이벤트 로깅**)**을 활성화하여 일치하는 연결에 대해 정책이 보안 인텔리전스 이벤트를 생성하는 정책을 활성화합니다. **OK(**확인**)**를 클릭하여 변경 사항을 저장합니다.

연결 로깅을 활성화하지 않으면 정책이 예상대로 작업을 수행하고 있는지 여부를 평가하는 데 사용할 데이터가 제공되지 않습니다. 외부 syslog 서버를 정의한 경우에는 해당 서버로도 이벤트가 전송되도록 지금 해당 서버를 선택할 수 있습니다.



j) 필요한 경우 각 탭의 **Do Not Block(**차단 안 함**)** 목록에 네트워크 또는 URL 개체를 추가하여 차단된 목록에 대한 예외를 생성할 수 있습니다.

Do Not Block(차단 안 함**)** 목록은 실제 "허용" 목록이 아닙니다. 예외 목록입니다. 예외 목록의 주소나 URL이 차단 목록에도 나타나는 경우 해당 주소나 URL에 대한 연결을 액세스 제어 정책으로 전달할 수 있습니다. 이 방법을 통해 특정 피드를 차단할 수 있습니다. 그러나 원하는 주소나 사이트가 차단되고 있음이 나중에 확인되는 경우에는 피드를 완전히 제거할 필요 없이 예외

목록을 사용하여 해당 차단을 재정의할 수 있습니다. 이러한 연결은 나중에 액세스 제어 및 침입 정책(구성된 경우)을 통해 평가됩니다. 따라서 침입 검사 중에 위협을 포함하는 연결을 식별하여 차단할 수 있습니다.

Access and SI Rules(액세스 및 SI 규칙) 대시보드와 이벤트 뷰어의 Security Intelligence(보안 인텔리전스) 보기를 사용하면 정책에 의해 실제로 삭제되는 트래픽, 그리고 **Do Not Block(**차단 안 함**)** 목록에 주소나 URL을 추가해야 하는지 여부를 확인할 수 있습니다.

단계 **6** 변경 사항을 커밋합니다.

a) 웹 페이지의 오른쪽 상단에 있는 **Deploy Changes(**변경 사항 구축**)** 아이콘을 클릭합니다.

b) **Deploy Now(**지금 구축**)** 버튼을 클릭합니다.

구축이 완료될 때까지 기다리거나 **OK(**확인**)**를 클릭하고 나중에 작업 목록 또는 구축 기록을 확인할 수 있습니다.

다음에 수행할 작업

이 시점부터 모니터링 대시보드 및 이벤트에 공격자, 대상 및 위협에 대한 정보가 표시됩니다(침입이 식별된 경우). 이 정보를 평가하여 네트워크에 추가 보안 조치가 필요한지 아니면 사용 중인 침입 정책의 레벨을 낮춰야 하는지를 결정할 수 있습니다.

보안 인텔리전스의 경우 Access and SI Rules(액세스 및 SI 규칙) 대시보드에서 정책 적중 횟수를 확인할 수 있습니다. 이벤트 뷰어에서도 보안 인텔리전스 이벤트를 확인할 수 있습니다. 트래픽은 검사 가능한 시점 이전에 차단되므로 보안 인텔리전스 차단은 침입 위협 정보에 반영되지 않습니다.

악성코드를 차단하는 방법

사용자가 인터넷 사이트 또는 이메일 등의 기타 통신 방법을 통해 악성 소프트웨어(악성코드)를 유입할 위험성은 항상 존재합니다. 신뢰할 수 있는 웹 사이트 역시 하이재킹되어 이러한 사이트를 의심하지 않는 사용자에게 악성코드를 전파할 수 있습니다. 웹 페이지는 여러 소스에서 제공되는 개체를 포함할 수 있습니다. 이러한 개체에는 이미지, 실행 파일, Javascript, 광고 등이 포함될 수 있습니다. 보안 침해된 웹 사이트의 경우 외부 소스에서 호스팅되는 개체가 통합되어 있는 경우가 많습니다. 철저한 보안을 유지하려면 초기 요청뿐 아니라 각 개체를 개별적으로 확인해야 합니다.

악성코드 방어를 사용해 악성코드를 탐지하기 위해 파일 정책을 사용합니다. 파일 제어를 수행하는 데에도 파일 정책을 사용할 수 있습니다. 그러면 파일에 악성코드가 있는지와 관계없이 특정 유형의 모든 파일에 대한 제어가 가능합니다.

악성코드 방어는 Secure Malware Analytics Cloud를 사용하여 네트워크 트래픽에서 탐지될 가능성이 있는 악성코드의 상태를 검색합니다. 관리 인터페이스에는 Secure Malware Analytics Cloud에 연결하고 악성코드 조회를 수행하기 위한 인터넷으로 연결되는 경로가 있어야 합니다. 디바이스는 적합한 파일을 탐지하면 파일의 SHA-256 해시 값을 사용하여 Secure Malware Analytics Cloud에서 파일의 상

태를 쿼리합니다. 가능한 상태는 **clean(**정상**)**, **malware(**악성코드**)** 또는 **unknown(**알 수 없음**)**(명확한 판정 없음)입니다. Secure Malware Analytics Cloud에 연결할 수 없는 경우의 상태는 **unknown(**알 수 없음**)**입니다.

파일 정책을 액세스 제어 규칙과 연결하여 시스템이 액세스 제어 규칙의 조건과 일치하는 트래픽을 통과시키기 전에 연결의 파일을 먼저 검사하도록 명령할 수 있습니다.

트래픽을 **allow(**허용**)**하는 규칙에 대해서만 파일 정책을 구성할 수 있습니다. 트래픽을 **trust(**신뢰**)** 또는 **block(**차단**)**하도록 설정된 규칙에 대해서는 검사가 수행되지 않습니다.

프로시저

단계 **1** 아직 수행하지 않은 경우 악성코드 및 위협 라이선스를 활성화합니다.

침입 정책에 필요한 위협 라이선스 외에 파일 정책을 사용하려면 악성코드를 활성화해야 합니다. 현재 평가 라이선스를 사용 중인 경우에는 라이선스의 평가 버전이 활성화됩니다. 디바이스를 등록한 경우 필요한 라이선스를 구매해 Cisco.com에서 Smart Software Manager 계정에 추가해야 합니다.

a) 디바이스를 클릭합니다.

b) 스마트 라이선스 그룹에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

c) 악성코드 그룹에서 **Enable(**활성화**)**을 클릭합니다. 아직 활성화되지 않은 경우 위협 그룹입니다.

시스템이 적절하게 어카운트에 라이선스를 등록하거나 평가 라이선스를 사용 설정합니다. 그룹에 라이선스가 활성화되었다는 메시지가 표시되며 버튼이 Disable(비활성화) 버튼으로 변경됩니다.

단계 **2** 하나 이상의 액세스 규칙에 대해 파일 정책을 선택합니다.

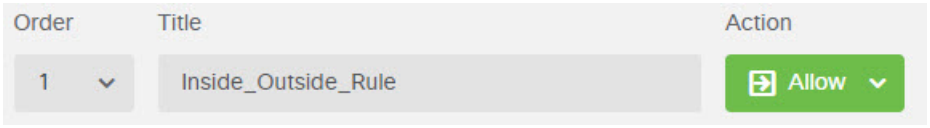
악성코드를 검사해야 하는 트래픽에 적용할 규칙을 결정합니다. 이 예에서는 Inside_Outside_Rule에 파일 검사를 추가합니다.

a) 주 메뉴에서 **Policies(**정책**)**를 클릭합니다.

Access Control(액세스 제어**)** 정책이 표시되는지 확인합니다.

b) Inside_Outside_Rule 행 오른쪽의 **Actions(**작업**)** 셀 위에 마우스를 올려 놓고 수정 및 삭제 아이콘이 표시되면 수정 아이콘( )을 클릭하여 규칙을 엽니다.

c) **Action(**작업**)**에 대해 **Allow(**허용**)**를 아직 선택하지 않았으면 선택합니다.



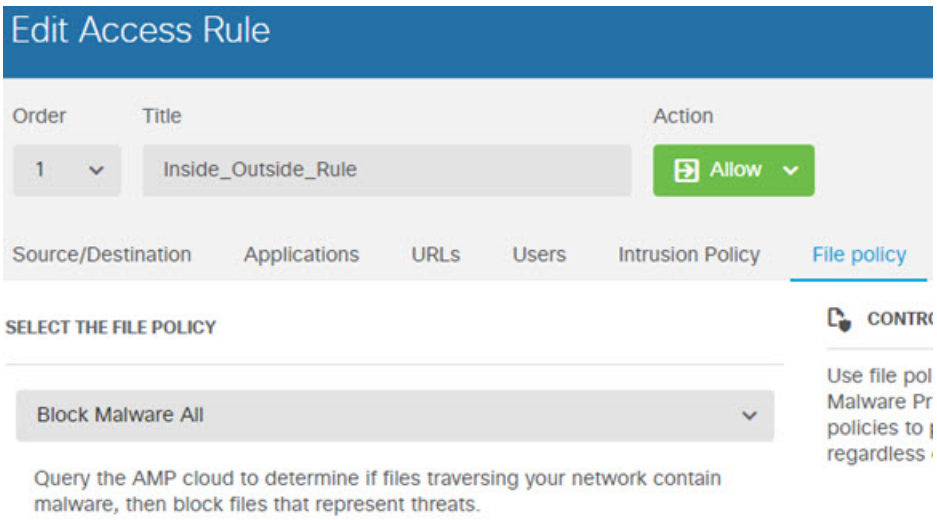
d) **File Policy(**파일 정책**)** 탭을 클릭합니다.

e) 사용하려는 파일 정책을 클릭합니다.

선택할 수 있는 주요 항목은 악성코드로 간주되는 모든 파일을 삭제하는 **Block Malware All(**악성코드 모두 차단**)**이나, 파일 상태를 확인하기 위해 Secure Malware Analytics Cloud를 쿼리하지만 차단은 수행하지 않는 **Cloud Lookup All(**클라우드 모두 조회**)**입니다. 먼저 파일을 평가하는 방법을 확인하려는 경우 클라우드 조회를 사용합니다. 파일을 평가하는 방법이 적절한 경우 나중에 차단 정책으로 전환할 수 있습니다.

악성코드를 차단하는 다른 정책도 제공됩니다. 이러한 정책은 파일 제어와 결합되어 Microsoft Office 또는 Office 및 PDF, 문서 업로드를 차단합니다. 즉, 이러한 정책은 악성코드를 차단할 뿐 아니라 사용자가 다른 네트워크로 이러한 파일 유형을 전송할 수 없도록 합니다. 요구에 맞는 경우 이러한 정책을 선택하면 됩니다.

이 예에서는 **Block Malware All(**악성코드 모두 차단**)**을 선택합니다.



f) **Logging(**로깅**)** 탭을 클릭하고 파일 이벤트 아래에서 **Log Files(**로그 파일**)**이 선택되어 있는지 확인합니다.

기본값으로, 파일 정책을 선택할 때마다 파일 로깅이 활성화됩니다. 이벤트와 대시보드에서 파일 및 악성코드 정보를 확인하려면 파일 로깅을 활성화해야 합니다.

g) **OK(**확인**)**를 클릭하여 변경 사항을 저장합니다.

단계 3 변경 사항을 커밋합니다.

a) 웹 페이지의 오른쪽 상단에 있는 **Deploy Changes(**변경 사항 구축**)** 아이콘을 클릭합니다.

b) **Deploy Now(**지금 구축**)** 버튼을 클릭합니다.

구축이 완료될 때까지 기다리거나 **OK(**확인**)**를 클릭하고 나중에 작업 목록 또는 구축 기록을 확인할 수 있습니다.

다음에 수행할 작업

이 시점부터 모니터링 대시보드 및 이벤트에 파일 유형과 파일 및 악성코드 이벤트에 대한 정보가 표시됩니다(파일 또는 악성코드가 전송된 경우). 이 정보를 평가하여 네트워크에 파일 전송과 관련된 추가 보안 조치가 필요한지를 결정할 수 있습니다.

사용 제한 정책(URL 필터링)을 구현하는 방법

네트워크에 대한 사용 제한 정책이 있을 수 있습니다. 사용 제한 정책은 조직에서 적절한 네트워크 활동과 부적절한 것으로 간주되는 활동을 구별합니다. 이러한 정책은 대개 인터넷 사용량을 중점적으로 파악하며 생산성을 유지하고, 법적 책임을 방지(예: 적대적이지 않은 업무 환경 유지)하고, 웹 트래픽을 전반적으로 제어할 수 있도록 작성되어 있습니다.

URL 필터링을 사용하여 액세스 정책을 통해 사용 제한 정책을 정의할 수 있습니다. 그러면 도박 등의 광범위한 범주를 필터링할 수 있으므로 차단해야 하는 모든 개별 웹 사이트를 식별할 필요가 없습니다. 범주가 일치하는 경우 허용하거나 차단할 사이트의 상대적 평판을 지정할 수도 있습니다. 사용자가 해당 카테고리 및 평판 조합을 가진 URL 검색을 시도하는 모든 경우, 세션이 차단됩니다.

범주 및 평판 데이터를 사용하면 정책 생성 및 관리도 간소화됩니다. 이를 통해 시스템이 웹 트래픽을 예상대로 제어할 수 있습니다. 마지막으로, Cisco의 위협 인텔리전스는 새로운 URL, 새로운 범주 및 기존 URL의 새로운 범주와 위험이 적용되어 지속적으로 업데이트되므로 시스템은 최신 정보를 사용하여 요청된 URL을 필터링할 수 있습니다. 악성코드, 스팸, 봇넷, 피싱과 같은 보안 위협을 나타내는 악성 사이트는 새로운 정책을 업데이트하고 구축하는 것보다 빠르게 나타났다 사라질 수 있습니다.

다음 절차에서는 URL 필터링을 사용하여 사용 제한 정책을 구현하는 방법을 설명합니다. 이 예에서는 여러 카테고리의 사이트(모든 평판), 위험한 소셜 네트워킹 사이트 및 분류되지 않은 사이트인 badsite.example.com을 차단합니다.

프로시저

단계 1 **URL** 라이선스를 아직 활성화하지 않은 경우 활성화합니다.

URL 카테고리 및 평판 정보를 사용하거나 대시보드 및 이벤트에서 해당 정보를 확인하려면 URL 라이선스를 활성화해야 합니다. 현재 평가 라이선스를 사용 중인 경우에는 라이선스의 평가 버전이 활성화됩니다. 디바이스를 등록한 경우 필요한 라이선스를 구매해 Cisco.com에서 Smart Software Manager 어카운트에 추가해야 합니다.

a) 디바이스를 클릭합니다.

b) 스마트 라이선스 그룹에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

c) **URL** 라이선스 그룹에서 **Enable(**활성화**)**을 클릭합니다.

시스템이 적절하게 어카운트에 라이선스를 등록하거나 평가 라이선스를 사용 설정합니다. 그룹에 라이선스가 활성화되었다는 메시지가 표시되며 버튼이 Disable(비활성화) 버튼으로 변경됩니다.

단계 **2** URL 필터링 액세스 제어 규칙을 생성합니다.

차단 규칙을 만들기 전에 먼저 사용자들이 방문하는 사이트의 범주를 확인하고자 할 수 있습니다. 이 경우 금융과 같이 허용 가능한 카테고리에 대해 허용 작업을 사용하여 규칙을 생성할 수 있습니다. URL이 이 카테고리에 속하는지를 확인하려면 모든 웹 연결을 검사해야 하므로 금융 사이트 이외의 사이트에 대해서도 카테고리 정보를 가져옵니다.

하지만 차단할 것임을 이미 알고 있는 URL 카테고리도 있을 수 있습니다. 차단 정책은 검사도 강제 수행하므로 차단된 범주뿐 아니라 차단되지 않은 범주에 대한 연결 관련 범주 정보도 가져오게 됩니다.

a) 주 메뉴에서 **Policies(**정책**)**를 클릭합니다.

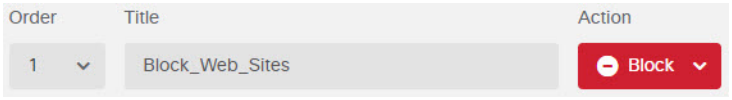
Access Control(액세스 제어**)** 정책이 표시되는지 확인합니다.

b) **+**를 클릭하여 새 규칙을 추가합니다.

c) 순서, 제목 및 작업을 구성합니다.

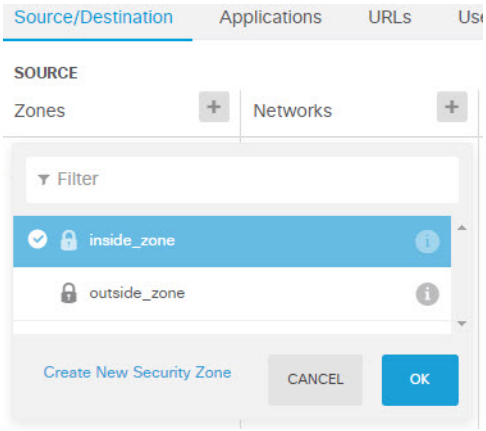
- **Order(**순서**)** - 기본적으로는 액세스 제어 정책 끝에 새 규칙을 추가합니다. 그러나 같은 소스/대상 및 기타 기준과 일치하는 규칙 앞(위)에 이 규칙을 배치해야 합니다. 그렇지 않으면 규칙이 어떤 항목과도 일치하지 않게 됩니다. 연결은 하나의 규칙, 즉 테이블에서 첫 번째로 일치하는 규칙에만 일치합니다. 이 규칙에서는 초기 디바이스 컨피그레이션 중에 생성한 Inside_Outside_Rule과 같은 소스/대상을 사용합니다. 다른 규칙도 생성했을 수 있습니다. 액세스 제어 효율성을 최대화하려면 특정 규칙을 미리 생성해 두는 것이 좋습니다. 그러면 연결을 허용할지 아니면 삭제할지를 가장 빠르게 결정할 수 있습니다. 이 예시에서는 규칙 순서로 **1**을 선택합니다.

- **Title(제목)** - Block_Web_Sites와 같이 의미 있는 이름을 규칙에 지정합니다.
- **Action(작업)** - **Block(차단)**을 선택합니다.

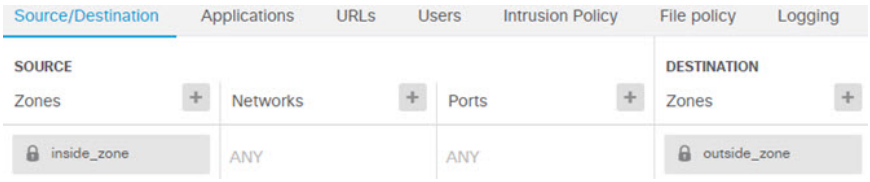


d) **Source/Destination(소스/대상)** 탭에서 **Source(소스)** > **Zones(영역)**의 +를 클릭하고 **inside_zone**을 선택한 후에 영역 대화 상자에서 **OK(확인)**를 클릭합니다.

기준을 추가하는 과정도 동일한 방식으로 수행합니다. +를 클릭하면 열리는 작은 대화 상자에서 추가할 항목을 클릭합니다. 여러 항목을 클릭할 수 있으며, 선택한 항목을 클릭하면 선택이 취소됩니다. 선택한 항목에는 확인 표시가 나타납니다. 그러나 **OK(확인)** 버튼을 클릭할 때까지는 정책에 아무 항목도 추가되지 않으므로 항목만 선택하는 것으로는 충분하지 않습니다.



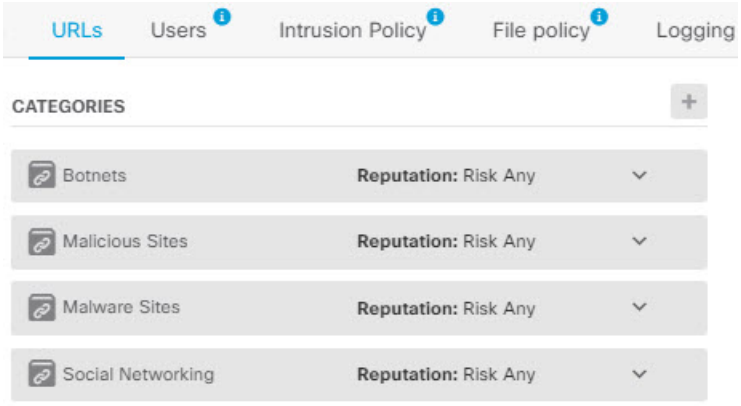
e) 동일한 기술을 사용하여 **Destination(대상)** > **Zones(영역)**에 대해 **outside_zone**을 선택합니다.



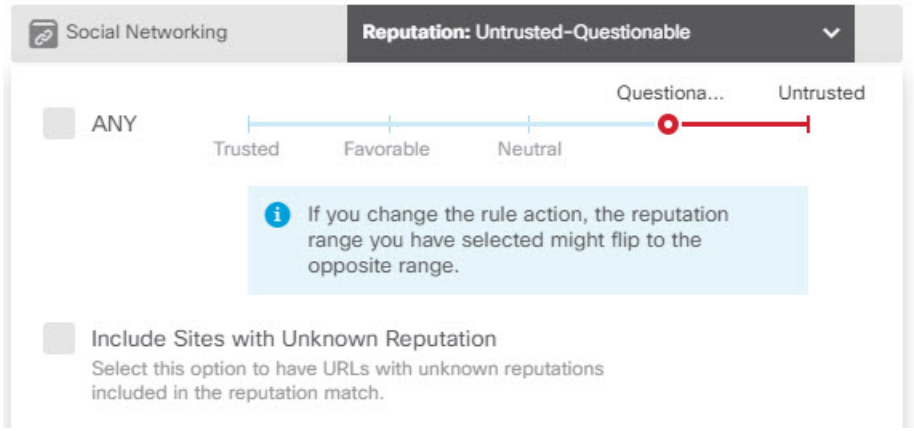
f) **URLs(URL)** 탭을 클릭합니다.

g) 범주의 +를 클릭하고 완전히 차단하거나 부분적으로 차단할 범주를 선택합니다.

이 예에서는 봇넷, 악성 사이트, 악성코드 사이트 및 소셜 네트워킹을 선택합니다. 차단해야 할 가능성이 높은 추가 범주도 있습니다. 차단하려는 사이트에 관해 알고 있지만 어떤 카테고리인지 확실하지 않은 경우, **URL to Check(확인할 URL)** 필드에 URL을 입력하고 **Go(이동)**를 클릭합니다. 그러면 조회 결과를 표시하는 웹 사이트로 이동합니다.



h) 소셜 네트워킹 카테고리에 대해 평판별 차단을 구현하려면 해당 카테고리에 대해 **Reputation: Risk Any(**평판**:** 모든 위험**)**를 클릭하고 **Any(**모두**)**를 선택 취소한 후에 슬라이더를 **Questionable(**의심스러움**)**로 이동합니다. 슬라이더 바깥쪽을 클릭하면 슬라이더가 닫힙니다.



평판 슬라이더의 왼쪽은 허용할 사이트를, 오른쪽은 차단할 사이트를 나타냅니다. 이 경우 평판이 Questionable(의심스러움) 및 Untrusted(신뢰할 수 없음) 범위에 속하는 소셜 네트워킹 사이트만 차단됩니다. 따라서 사용자는 위험성이 적은 흔히 사용되는 소셜 네트워킹 사이트에 액세스할 수 있습니다.

평판을 알 수 없는 URL을 평판 일치에 포함하려면 **Include Sites with Unknown Reputation(**평판을 알 수 없는 사이트 포함**)** 옵션을 선택합니다. 새 사이트는 일반적으로 등급이 지정되지 않으며, 사이트의 평판을 알 수 없거나 확인할 수 없는 다른 이유가 있을 수 있습니다.

평판을 사용하면 일반적으로는 허용할 범주 내의 사이트를 선택적으로 차단할 수 있습니다.

i) 범주 목록 왼쪽의 **URL** 목록 옆에 있는 **+**를 클릭합니다.

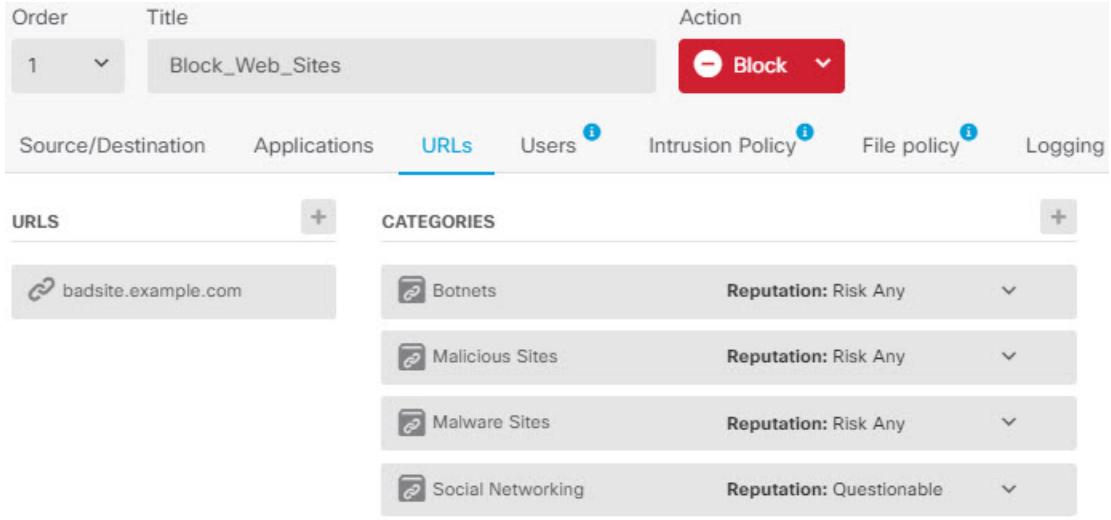
j) 팝업 대화 상자 하단의 새 **URL** 생성 링크를 클릭합니다.

k) 이름과 URL에 모두 **badsite.example.com**을 입력하고 확인을 클릭하여 개체를 생성합니다.

개체 이름은 URL과 동일하게 지정해도 되고 다른 이름을 지정해도 됩니다. URL의 경우 URL의 프로토콜 부분은 포함하지 말고 서버 이름만 추가합니다.

l) 새 개체를 선택한 다음 **OK(**확인**)**를 클릭합니다.

정책을 수정하는 중에 새 개체를 추가하면 목록에 개체가 추가되지만, 새 개체가 자동으로 선택되지는 않습니다.



m) **Logging(**로깅**)** 탭을 클릭하고 **Select Log Action(**로그 작업 선택**)** > **At Beginning and End of Connection(**연결 시작 및 종료 시**)**을 선택합니다.

웹 범주 대시보드 및 연결 이벤트로 범주 및 평판 정보를 가져오려면 로깅을 활성화해야 합니다.

n) **OK(**확인**)**를 클릭하여 규칙을 저장합니다.

단계 **3** (선택 사항). URL 필터링을 위한 기본 설정을 지정합니다.

URL 라이선스를 활성화하면 시스템에서 웹 범주 데이터베이스에 대한 업데이트를 자동으로 활성화합니다. 시스템은 30분마다 업데이트를 확인하지만, 데이터는 대개 매일 한 번씩 업데이트됩니다. 이러한 업데이트를 적용하지 않으려는 경우에는 업데이트를 끌 수 있습니다.

또한, 분석을 위해 Cisco에 분류되지 않은 URL을 전송하도록 선택할 수도 있습니다. 설치된 URL 데이터베이스에 사이트에 대한 분류가 없어도 Cisco Cloud에는 있을 수 있습니다. 이 경우 클라우드는 범주와 평판을 반환하며, 그러면 범주 기반 규칙을 URL 요청에 올바르게 적용할 수 있습니다. 메모리 제한으로 인해 더 작은 URL 데이터베이스를 설치하는 저가형 시스템에서는 이 옵션을 반드시 선택해야 합니다. 조회 결과에 대해 TTL(Time to Live)을 설정할 수 있습니다. 기본값은 조회 결과를 새로 고치지 않는 Never(안 함)입니다.

a) 디바이스를 클릭합니다.
b) **System Settings(**시스템 설정**)** > **Traffic Settings(**트래픽 설정**)** > **URL Filtering Preferences(URL** 필터링 기본 설정**)**를 클릭합니다.
c) **Cisco CSI**에서 알 수 없는 **URL** 쿼리를 선택합니다.
d) 24시간 등의 적절한 **URL Time to Live(URL Time to Live)**를 선택합니다.
e) **Save(**저장**)**를 클릭합니다.

단계 **4** 변경 사항을 커밋합니다.

a) 웹 페이지의 오른쪽 상단에 있는 **Deploy Changes(**변경 사항 구축**)** 아이콘을 클릭합니다.

b) **Deploy Now(**지금 구축**)** 버튼을 클릭합니다.

구축이 완료될 때까지 기다리거나 **OK(**확인**)**를 클릭하고 나중에 작업 목록 또는 구축 기록을 확인할 수 있습니다.

다음에 수행할 작업

이 시점부터 모니터링 대시보드 및 이벤트에 URL 카테고리 및 평판 그리고 삭제된 연결에 대한 정보가 표시되어야 합니다. 이 정보를 평가하여 URL 필터링이 부적절한 사이트만 삭제하는지 또는 특정 범주에 대한 평판 설정을 완화해야 하는지를 확인할 수 있습니다.

범주와 평판을 기준으로 웹 사이트 액세스를 차단할 것임을 사용자에게 미리 알리는 것이 좋습니다.

애플리케이션 사용량을 제어하는 방법

웹은 기업에 애플리케이션을 제공하는 데 흔히 사용되는 플랫폼으로 자리잡았습니다. 브라우저 기반 애플리케이션 플랫폼이 사용될 수도 있고, 기업 네트워크 안팎으로 애플리케이션을 전송하는 방법으로 웹 프로토콜을 사용하는 리치 미디어 애플리케이션이 사용될 수도 있습니다.

Threat Defense 연결을 검사하여 사용 중인 애플리케이션을 확인합니다. 따라서 특정 TCP/UDP 포트만 대상으로 하는 것이 아니라 애플리케이션을 대상으로 하는 액세스 제어 규칙을 작성할 수 있습니다. 그러므로 같은 포트를 사용하는 웹 기반 애플리케이션도 선택적으로 허용하거나 차단할 수 있습니다.

허용하거나 차단할 특정 애플리케이션을 선택할 수도 있지만, 유형/범주/태그/위험/사업 타당성을 기준으로 규칙을 작성할 수도 있습니다. 예를 들어, 위험도가 높고 비즈니스 관련성이 낮은 모든 애플

리케이션을 식별하여 차단하는 액세스 제어 규칙을 만들 수 있습니다. 사용자가 이러한 애플리케이션 중 하나를 사용하려고 할 경우, 세션은 차단됩니다.

Cisco에서는 시스템 및 VDB(Vulnerability Database) 업데이트를 통해 추가 애플리케이션 탐지기를 자주 업데이트하고 추가합니다. 따라서 규칙을 수동으로 업데이트하지 않아도 위험도가 높은 애플리케이션을 차단하는 규칙이 새 애플리케이션에 자동으로 적용될 수 있습니다.

이 활용 사례에서는 익명성 도구/프록시 범주에 속하는 모든 애플리케이션을 차단합니다.

시작하기 전에

이 활용 사례에서는 네트워크 트래픽을 파악하는 방법, 49 페이지 활용 사례를 완료했다고 가정합니다. 해당 활용 사례에서는 애플리케이션 사용량 정보를 수집하는 방법을 설명합니다. 이 정보는 애플리케이션 대시보드에서 분석할 수 있습니다. 실제로 사용 중인 애플리케이션을 파악하면 효율적인 애플리케이션 기반 규칙을 디자인하는 데 도움이 될 수 있습니다. VDB 업데이트를 예약하는 방법도 해당 활용 사례에 설명되어 있으므로 이 활용 사례에서 반복 설명하지 않습니다. 애플리케이션을 올바르게 식별할 수 있도록 VBD를 정기적으로 업데이트해야 합니다.

프로시저

단계 1 애플리케이션 기반 액세스 제어 규칙을 생성합니다.

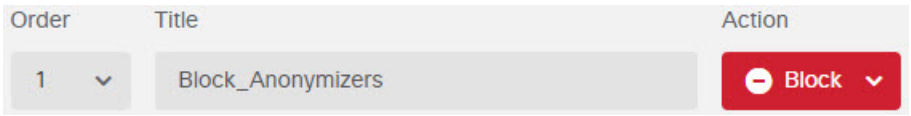
a) 주 메뉴에서 **Policies(정책)**를 클릭합니다.

Access Control(액세스 제어) 정책이 표시되는지 확인합니다.

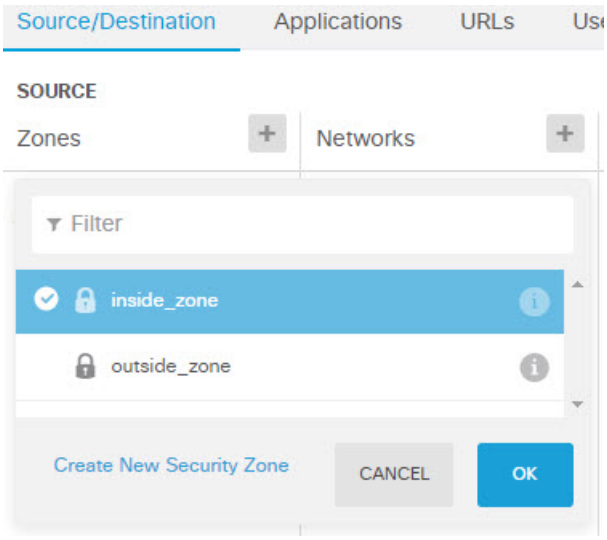
b) +를 클릭하여 새 규칙을 추가합니다.

c) 순서, 제목 및 작업을 구성합니다.

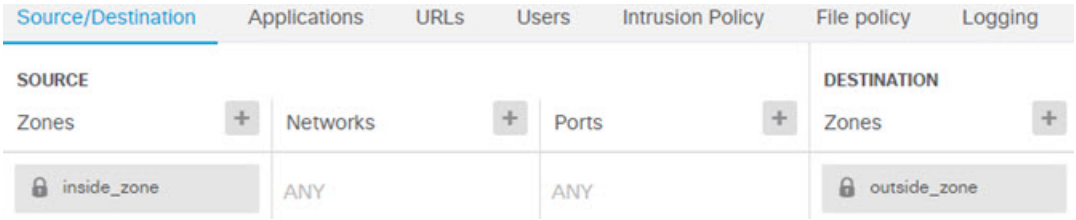
- **Order(순서)** - 기본적으로는 액세스 제어 정책 끝에 새 규칙을 추가합니다. 그러나 같은 소스/대상 및 기타 기준과 일치하는 규칙 앞(위)에 이 규칙을 배치해야 합니다. 그렇지 않으면 규칙이 어떤 항목과도 일치하지 않게 됩니다. 연결은 하나의 규칙, 즉 테이블에서 첫 번째로 일치하는 규칙에만 일치합니다. 이 규칙에서는 초기 디바이스 컨피그레이션 중에 생성한 Inside_Outside_Rule과 같은 소스/대상을 사용합니다. 다른 규칙도 생성했을 수 있습니다. 액세스 제어 효율성을 최대화하려면 특정 규칙을 미리 생성해 두는 것이 좋습니다. 그러면 연결을 허용할지 아니면 삭제할지를 가장 빠르게 결정할 수 있습니다. 이 예시에서는 규칙 순서로 **1**을 선택합니다.
- **Title(제목)** - Block_Anonymizers와 같이 의미 있는 이름을 규칙에 지정합니다.
- **Action(작업)** - **Block(차단)**을 선택합니다.



d) **Source/Destination(소스/대상)** 탭에서 **Source(소스)** > **Zones(영역)**의 +를 클릭하고 **inside_zone**을 선택한 후에 영역 대화 상자에서 **OK(확인)**를 클릭합니다.



e) 동일한 기술을 사용하여 **Destination(**대상**)** > **Zones(**영역**)**에 대해 **outside_zone**을 선택합니다.



f) **Applications(**애플리케이션**)** 탭을 클릭합니다.

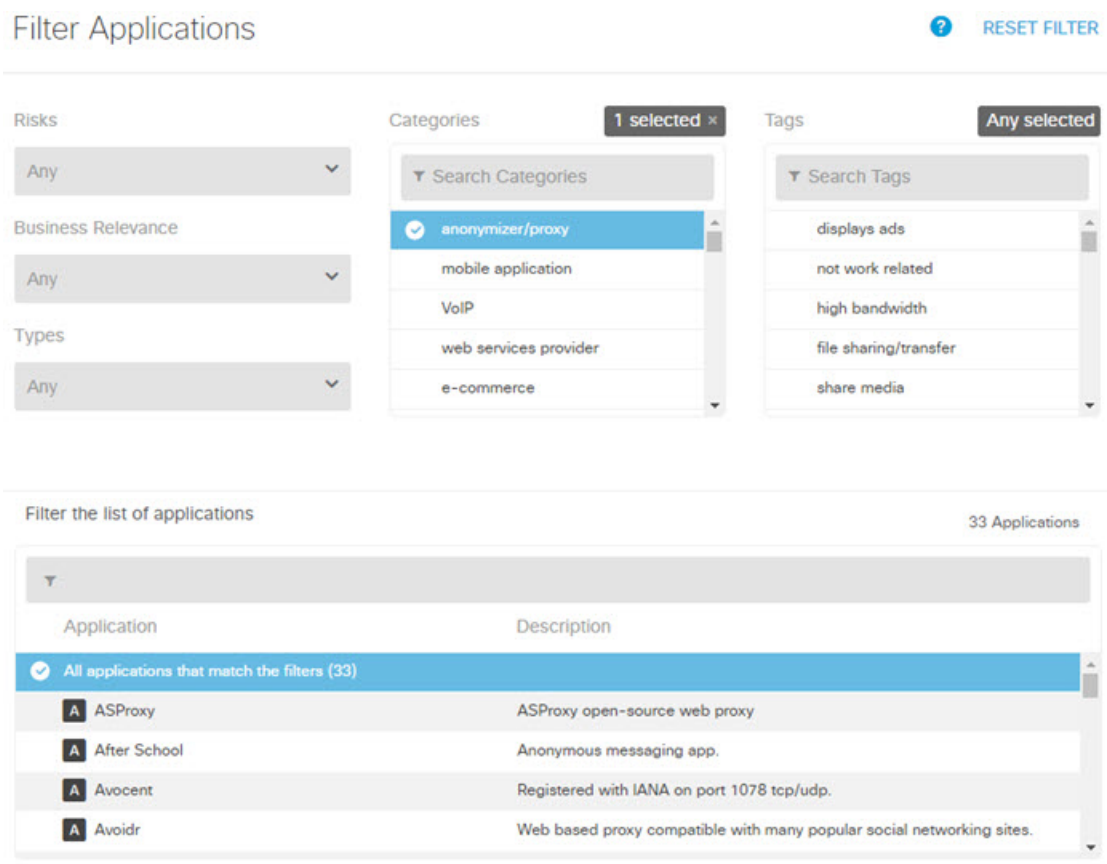
g) 애플리케이션에 대해 **+**를 클릭하고 팝업 대화 상자 하단의 **Advanced Filter(**고급 필터**)** 링크를 클릭합니다.

애플리케이션 필터 개체를 미리 생성해 두었다가 여기서 애플리케이션 필터 목록을 통해 선택할 수도 있지만, 액세스 제어 규칙에서 기준을 직접 지정하고 필요에 따라 기준을 필터 개체로 저장할 수도 있습니다. 단일 애플리케이션용 규칙을 작성하는 경우가 아니면 고급 필터 대화 상자를 사용하여 애플리케이션을 찾고 적절한 기준을 생성하는 것이 더 쉽습니다.

기준을 선택하면 대화 상자 하단의 애플리케이션 목록이 업데이트되어 기준과 일치하는 정확한 애플리케이션이 표시됩니다. 작성하는 규칙은 이러한 애플리케이션에 적용됩니다.

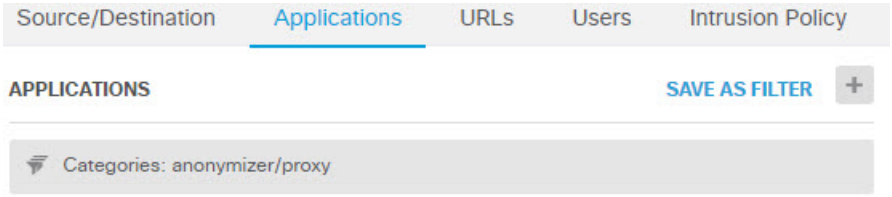
이 목록을 자세히 확인하십시오**.** 예를 들어 위험도가 매우 높은 애플리케이션은 모두 차단하는 경우가 많습니다. 하지만 이 문서를 작성하는 시점에서 Facebook과 TFTP도 위험도가 매우 높은 애플리케이션으로 분류되어 있습니다. 대부분의 조직은 해당 애플리케이션을 차단하기를 원치 않을 것입니다. 시간을 할애하여 다양한 필터 기준을 적용해 보고 선택한 필터와 일치하는 애플리케이션을 확인하십시오. 이러한 목록은 VDB가 업데이트될 때마다 변경될 수 있습니다.

이 예에서는 범주 목록에서 익명성 도구/프록시를 선택합니다.



h) 고급 필터 대화 상자에서 **Add(**추가**)**를 클릭합니다.

필터가 추가되어 애플리케이션 탭에 표시됩니다.



i) **Logging(**로깅**)** 탭을 클릭하고 **Select Log Action(**로그 작업 선택**)** > **At Beginning and End of Connection(**연결 시작 및 종료 시**)**을 선택합니다.

이 규칙에 의해 차단되는 연결에 대한 정보를 확인하려면 로깅을 활성화해야 합니다.

j) **OK(**확인**)**를 클릭하여 규칙을 저장합니다.

단계 **2** 변경 사항을 커밋합니다.

a) 웹 페이지의 오른쪽 상단에 있는 **Deploy Changes(**변경 사항 구축**)** 아이콘을 클릭합니다.

b) **Deploy Now(**지금 구축**)** 버튼을 클릭합니다.

구축이 완료될 때까지 기다리거나 **OK(**확인**)**를 클릭하고 나중에 작업 목록 또는 구축 기록을 확인할 수 있습니다.

단계 **3** **Monitoring(**모니터링**)**을 클릭하고 결과를 평가합니다.

이제 애플리케이션 위젯의 네트워크 개요 대시보드에 삭제된 연결이 표시됩니다. **All(**모두**)/Denied(**거부됨**)/Allowed(**허용됨**)** 드롭다운 옵션을 사용하여 삭제된 애플리케이션만 확인합니다.

Web Applications(웹 애플리케이션**)** 대시보드에서 애플리케이션 정보를 확인할 수도 있습니다. **Applications(**애플리케이션**)** 대시보드에는 프로토콜 관련 결과가 표시됩니다. 특정 사용자가 이러한 애플리케이션 사용을 시도하는 경우, ID 정책을 활성화하고 인증을 요구한다는 가정 하에 연결을 시도하는 사용자와 애플리케이션 간의 상관관계를 파악할 수 있어야 합니다.

서브넷을 추가하는 방법

디바이스에 사용 가능한 인터페이스가 있으면 스위치나 다른 라우터에 유선으로 연결하여 다른 서브넷에 서비스를 제공할 수 있습니다.

서브넷은 여러 가지 이유로 인해 추가할 수 있습니다. 이 활용 사례의 경우에는 다음과 같은 일반적인 시나리오를 위해 서브넷을 연결합니다.

- 서브넷은 프라이빗 네트워크 192.168.2.0/24를 사용하는 내부 네트워크입니다.
- 네트워크의 인터페이스 고정 주소는 192.168.2.1입니다. 이 예에서 실제 인터페이스는 네트워크 전용입니다. 이미 유선으로 연결된 인터페이스를 사용하고 새 네트워크용으로 하위 인터페이스를 생성할 수도 있습니다.
- 디바이스는 DHCP를 사용하여 네트워크의 워크스테이션에 주소를 제공하며, 주소 풀 192.168.2.2-192.168.2.254를 사용합니다.
- 다른 내부 네트워크와 외부 네트워크에 대한 네트워크 액세스가 허용됩니다. 외부 네트워크로 이동하는 트래픽은 NAT를 사용하여 공용 주소를 가져옵니다.

참고 이 예에서는 사용되지 않는 인터페이스가 브리지 그룹의 일부분이 아니라고 가정합니다. 현재 해당 인터페이스가 브리지 그룹 멤버인 경우에는 먼저 브리지 그룹에서 인터페이스를 제거해야 이 절차를 수행할 수 있습니다.

시작하기 전에

새 서브넷의 스위치와 인터페이스에 네트워크 케이블을 물리적으로 연결합니다.

프로시저

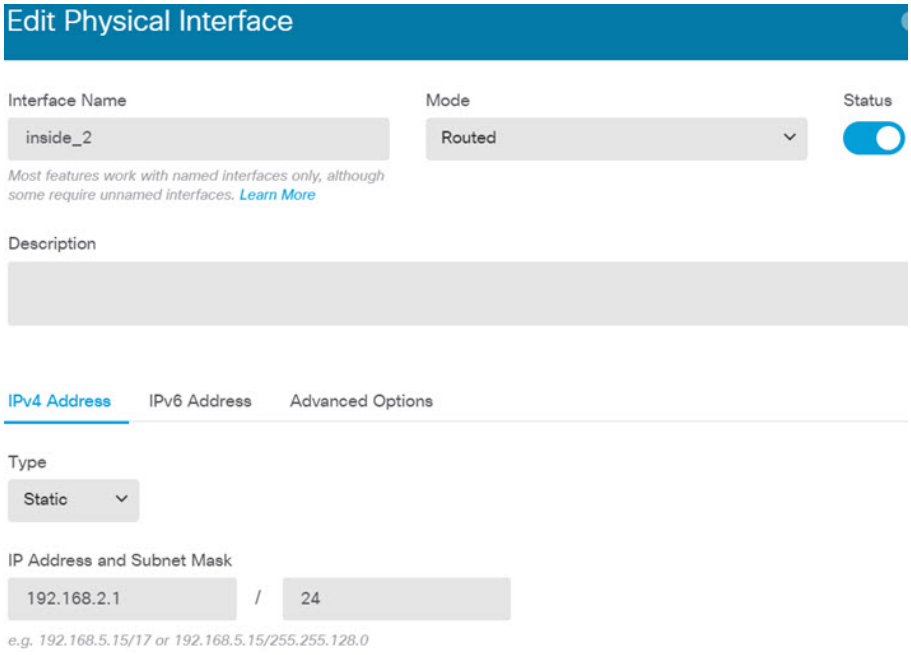
단계 **1** 인터페이스를 구성합니다.

a) **Device(**디바이스**)**를 클릭하고 **Interfaces(**인터페이스**)** 요약의 링크를 클릭한 다음, 인터페이스 유형을 클릭하여 인터페이스 목록을 확인합니다.

b) 유선으로 연결한 인터페이스 행 오른쪽의 **Actions(**작업**)** 셀 위에 마우스를 올려놓고 수정 아이콘()을 클릭합니다.

c) 기본 인터페이스 속성을 구성합니다.

- **Name(**이름**)** - 인터페이스의 고유한 이름입니다. 이 예에서 이름은 **inside_2**입니다.
- **Mode(**모드**)** - **Routed(**라우팅**)**를 선택합니다.
- **Status(**상태**)** - 상태 토글을 클릭하여 인터페이스를 활성화합니다.
- **IPv4 Address(IPv4** 주소**)** 탭 - 유형으로 고정을 선택하고 **192.168.2.1/24**를 입력합니다.



d) **Save(**저장**)**를 클릭합니다.

인터페이스 목록에 업데이트된 인터페이스 상태와 구성된 IP 주소가 표시됩니다.

단계 **2** 인터페이스용 DHCP 서버를 구성합니다.

a) 디바이스를 클릭합니다.

b) **System Settings(**시스템 설정**)** > **DHCP Server(DHCP** 서버**)**를 클릭합니다.

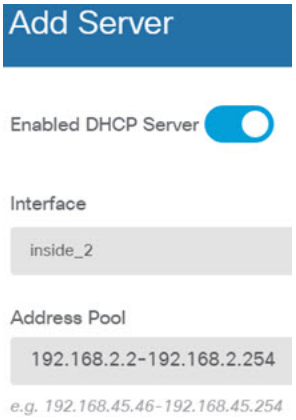
c) **DHCP Servers(DHCP** 서버**)** 탭을 클릭합니다.

테이블에 기존 DHCP 서버가 나열됩니다. 기본 컨피그레이션을 사용하는 경우 목록에는 내부 인터페이스용 DHCP 서버가 포함되어 있습니다.

d) 테이블 위의 +를 클릭합니다.

e) 서버 속성을 구성합니다.

- **Enable DHCP Server(DHCP** 서버 활성화**)** - 이 토글을 클릭하여 서버를 활성화합니다.
- **Interface(**인터페이스**)** - DHCP 서비스를 제공할 인터페이스를 선택합니다. 이 예에서는 inside_2를 선택합니다.
- **Address Pool(**주소 풀**)** - 서버가 네트워크의 디바이스에 제공할 수 있는 주소입니다. 192.168.2.2-192.168.2.254를 입력합니다. 네트워크 주소(.0), 인터페이스 주소(.1) 또는 브로드캐스트 주소(.255)는 포함하지 마십시오. 또한 네트워크의 디바이스에 고정 주소가 필요한 경우 해당 주소를 풀에서 제외합니다. 풀은 연속하는 주소의 단일 시리즈여야 하므로 범위 시작이나 끝에서 고정 주소를 선택합니다.



f) **Add(**추가**)**를 클릭합니다.

#	INTERFACE	ENABLED DHCP SERVER	ADDRESS POOL
1	inside	Enabled	192.168.1.5-192.168.1.254
2	inside_2	Enabled	192.168.2.2-192.168.2.254

단계 **3** 내부 보안 영역에 인터페이스를 추가합니다.

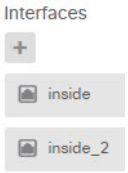
인터페이스에서 정책을 작성하려면 인터페이스가 보안 영역에 속해야 합니다. 보안 영역에 대한 정책을 작성합니다. 그러므로 영역에서 인터페이스를 추가하거나 제거하면 인터페이스에 적용되는 정책이 자동으로 변경됩니다.

a) 주 메뉴에서 **Objects(**개체**)**를 클릭합니다.

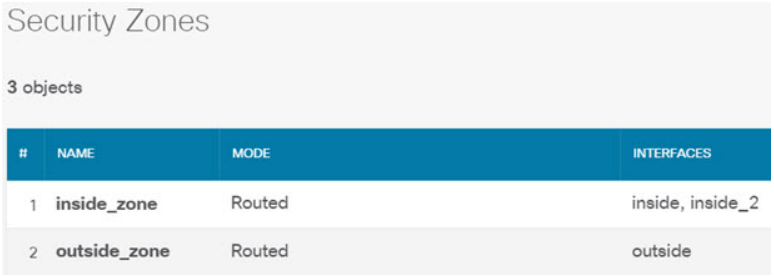
b) 개체 목차에서 **Security Zones(**보안 영역**)**을 선택합니다.

c) **inside_zone** 개체 행 오른쪽의 **Actions(**작업**)** 셀 위에 마우스를 올려놓고 수정 아이콘( )을 클릭합니다.

d) 인터페이스 아래의 +를 클릭하고 inside_2 인터페이스를 선택한 후에 인터페이스 목록에서 **OK(**확인**)**를 클릭합니다.



e) **Save(**저장**)**를 클릭합니다.



단계 **4** 내부 네트워크 간에 트래픽을 허용하는 액세스 제어 규칙을 생성합니다.

트래픽은 인터페이스 간에 자동으로 허용되지 않습니다. 원하는 트래픽을 허용하는 액세스 제어 규칙을 생성해야 합니다. 단, 액세스 제어 규칙의 기본 작업에서 트래픽을 허용하는 경우는 예외입니다. 이 예에서는 디바이스 설정 마법사가 구성하는 차단 기본 작업을 유지했다고 가정합니다. 따라서 내부 인터페이스 간에 트래픽을 허용하는 규칙을 생성해야 합니다. 이러한 규칙을 이미 생성했다면 이 단계를 건너뛰십시오.

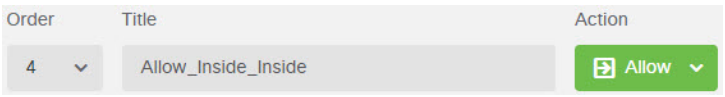
a) 주 메뉴에서 **Policies(**정책**)**를 클릭합니다.

Access Control(액세스 제어**)** 정책이 표시되는지 확인합니다.

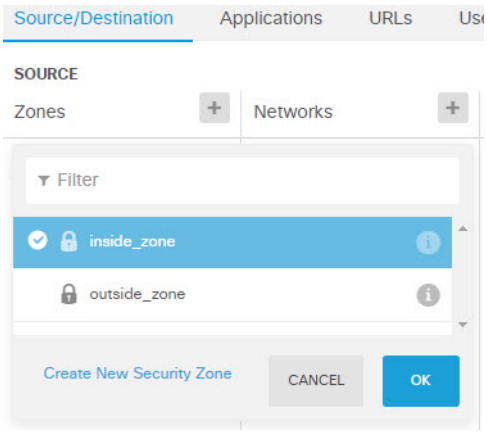
b) +를 클릭하여 새 규칙을 추가합니다.

c) 순서, 제목 및 작업을 구성합니다.

- **Order(**순서**)** - 기본적으로는 액세스 제어 정책 끝에 새 규칙을 추가합니다. 그러나 같은 소스/대상 및 기타 기준과 일치하는 규칙 앞(위)에 이 규칙을 배치해야 합니다. 그렇지 않으면 규칙이 어떤 항목과도 일치하지 않게 됩니다. 연결은 하나의 규칙, 즉 테이블에서 첫 번째로 일치하는 규칙에만 일치합니다. 이 규칙의 경우에는 고유한 소스/대상 기준을 사용할 것이므로 목록 끝에 규칙을 추가하면 됩니다.
- **Tile(**제목**)** - Allow_Inside_Inside와 같이 의미 있는 이름을 규칙에 지정합니다.
- **Action(**작업**)** - **Allow(**허용**)**를 선택합니다.

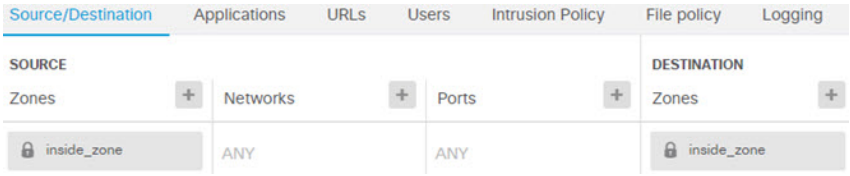


d) **Source/Destination(**소스/대상**)** 탭에서 **Source(**소스**)** > **Zones(**영역**)**의 +를 클릭하고 **inside_zone**을 선택한 후에 영역 대화 상자에서 **OK(**확인**)**를 클릭합니다.



e) 동일한 기술을 사용하여 **Destination(**대상**)** > **Zones(**영역**)**에 대해 **inside_zone**을 선택합니다.

소스와 대상에 대해 같은 영역을 선택하려면 보안 영역이 둘 이상의 인터페이스를 포함해야 합니다.



f) (선택 사항). 침입 및 악성코드 검사를 구성합니다.

내부 인터페이스가 신뢰할 수 있는 영역에 있기는 하지만 사용자는 일반적으로 랩톱을 네트워크에 연결합니다. 따라서 사용자가 의도치 않게 외부 네트워크나 Wi-Fi 핫스팟에서 네트워크 내부로 위협 요소를 유입할 수 있습니다. 그러므로 내부 네트워크 사이를 이동하는 트래픽에서 침입 및 악성코드를 검사할 수 있습니다.

이와 관련하여 다음 사항을 고려하십시오.

- **Intrusion Policy(**침입 정책**)** 탭을 클릭하고 침입 정책을 활성화한 다음 슬라이더를 사용하여 Balanced Security and Connectivity(보안과 연결의 균형 유지) 정책을 선택합니다.
- **File Policy(**파일 정책**)** 탭을 클릭한 후 악성코드 모두 차단 정책을 선택합니다.

g) **Logging(**로깅**)** 탭을 클릭하고 **Select Log Action(**로그 작업 선택**)** > **At Beginning and End of Connection(**연결 시작 및 종료 시**)**을 선택합니다.

이 규칙과 일치하는 연결에 대한 정보를 확인하려면 로깅을 활성화해야 합니다. 로깅을 사용하면 대시보드에 통계가 추가되며 이벤트 뷰어에 이벤트가 표시됩니다.

h) **OK(**확인**)**를 클릭하여 규칙을 저장합니다.

단계 **5** 새 서브넷에 대해 필요한 정책이 정의되어 있는지 확인합니다.

inside_zone 보안 영역에 인터페이스를 추가하면 inside_zone에 대한 모든 기존 정책이 새 서브넷에 자동으로 적용됩니다. 그러나 시간을 할애하여 정책을 검사해 추가 정책이 필요하지 않은지 확인해야 합니다.

초기 디바이스 컨피그레이션을 완료한 경우에는 다음 정책이 이미 적용되어 있어야 합니다.

- 액세스 제어 - Inside_Outside_Rule은 새 서브넷과 외부 네트워크 간의 모든 트래픽을 허용합니다. 이전 활용 사례를 따른 경우 이 정책은 침입 및 악성코드 검사 기능도 제공합니다. 새 네트워크와 외부 네트워크 간의 일부 트래픽을 허용하는 규칙이 있어야 합니다. 그렇지 않으면 사용자가 인터넷 또는 기타 외부 네트워크에 액세스할 수 없습니다.
- **NAT** - InsideOutsideNATrule은 외부 인터페이스로 이동하는 모든 인터페이스에 적용되며 인터페이스 PAT를 적용합니다. 이 규칙을 유지한 경우 새 네트워크에서 외부로 이동하는 트래픽의 IP 주소가 외부 인터페이스 IP 주소에서 고유한 포트로 변환됩니다. 모든 인터페이스 또는 inside_zone 인터페이스에 적용되는 규칙이 없으면 외부 인터페이스로 이동할 때 새 규칙을 생성해야 할 수 있습니다.
- **ID** - 기본 ID 정책은 없습니다. 그러나 이전 활용 사례를 따른 경우 새 네트워크에 대한 인증을 요구하는 ID 정책이 이미 있을 수 있습니다. 적용되는 ID 정책이 없는 경우 새 네트워크에 대해 사용자 기반 정보를 확인하려면 ID 정책을 생성합니다.

단계 **6** 변경 사항을 커밋합니다.

a) 웹 페이지의 오른쪽 상단에 있는 **Deploy Changes(**변경 사항 구축**)** 아이콘을 클릭합니다.

b) **Deploy Now(**지금 구축**)** 버튼을 클릭합니다.

구축이 완료될 때까지 기다리거나 **OK(**확인**)**를 클릭하고 나중에 작업 목록 또는 구축 기록을 확인할 수 있습니다.

다음에 수행할 작업

새 서브넷의 워크스테이션이 DHCP를 사용하여 IP 주소를 받으며, 다른 내부 네트워크 및 외부 네트워크에 연결할 수 있는지 확인합니다. 모니터링 대시보드 및 이벤트 뷰어를 사용하여 네트워크 사용량을 평가합니다.

네트워크에서 트래픽을 능동적으로 모니터링하는 방법

threat defense 디바이스는 대개 액티브 방화벽 및 IPS(Intrusion Prevention System) 보안 디바이스로 구축됩니다. 이 디바이스의 핵심 기능은 부적절한 연결과 위협을 삭제하는 활성 네트워크 보호를 제공하는 것입니다.

그러나 패시브 모드로 시스템을 구축할 수도 있습니다. 이 모드에서는 디바이스가 모니터링되는 스위치 포트의 트래픽을 분석만 합니다. 이 모드는 주로 데모 또는 테스트용입니다. 즉, 디바이스를 액티브 방화벽으로 구축하기 전에 패시브 모드에서 디바이스 사용법을 파악할 수 있습니다. 패시브 구축을 사용하는 경우 네트워크에 나타나는 위협의 종류, 사용자가 탐색 중인 URL 카테고리 등을 모니터링할 수 있습니다.

패시브 모드는 보통 데모나 테스트에만 사용하지만, IDS(침입 탐지 시스템, 방지 기능 없음) 등 필요한 서비스를 제공하는 경우에는 생산 환경에서도 패시브 모드를 사용할 수 있습니다. 패시브 인터페이스와 액티브 방화벽 라우티드 인터페이스를 함께 사용하면 조직에 필요한 서비스 조합을 정확하게 제공할 수 있습니다.

다음 절차에서는 시스템을 패시브 방식으로 구축하여 제한된 수의 스위치 포트를 통해 들어오는 트래픽을 분석하는 방법을 설명합니다.

참고 이 예시는 하드웨어 threat defense 디바이스용입니다. threat defense virtual에도 수동 모드를 사용할 수는 있지만, 네트워크 설정이 다릅니다. 자세한 내용은 Threat Defense Virtual 패시브 인터페이스의 VLAN 구성, 300 페이지를 참조해 주십시오. 그렇지 않으면 threat defense virtual에 이 절차가 적용됩니다.

시작하기 전에

이 절차에서는 내부 및 외부 인터페이스를 연결했으며 초기 디바이스 설정 마법사를 완료했다고 가정합니다. 패시브 구축 시에도 시스템 데이터베이스용 업데이트 다운로드를 위한 인터넷 연결이 필요합니다. 또한 관리 인터페이스에 연결하여 device manager를 열 수 있어야 합니다. 내부 또는 관리 포트에 직접 연결하면 됩니다.

또한 이 예에서는**Policies(**정책**)** > **Intrusion(**침입**)** 페이지에서 침입 정책에 대해 시스템 로그를 활성화했다고 가정합니다.

프로시저

단계 **1** 스위치 포트를 SPAN(Switched Port Analyzer) 포트로 구성하고 소스 인터페이스에 대해 모니터링 세션을 구성합니다.

다음 예시에서는 Cisco Nexus Series 스위치의 소스 인터페이스 2개에 대해 SPAN 포트 및 모니터링 세션을 설정합니다. 다른 유형의 스위치를 사용하는 경우 필요한 명령이 달라질 수 있습니다.

```
switch(config)# interface Ethernet1/48
switch(config-if)# switchport monitor
switch(config-if)# exit
switch(config)# monitor session 1
switch(config-monitor)# source interface ethernet 1/7
switch(config-monitor)# source interface ethernet 1/8
switch(config-monitor)# destination interface ethernet 1/48
switch(config-monitor)# no shut
```

설정을 확인하려면 다음 명령을 실행합니다.

```
switch# show monitor session 1 brief
   session 1
---------------
type              : local
state             : up
source intf       :
```

```
    rx            : Eth1/7        Eth1/8
    tx            : Eth1/7        Eth1/8
    both          : Eth1/7        Eth1/8
source VSANs      :
destination ports : Eth1/48

Legend: f = forwarding enabled, l = learning enabled
```

단계 **2** threat defense 인터페이스를 스위치의 SPAN 포트에 연결합니다.

threat defense 디바이스에서 현재 사용하지 않는 포트를 선택하는 것이 가장 좋습니다. 예시 스위치 컨피그레이션을 기준으로 하는 경우 스위치의 이더넷 1/48에 케이블을 연결합니다. 이 인터페이스가 모니터링 세션의 대상 인터페이스입니다.

단계 **3** 수동 모드에서 threat defense 인터페이스를 컨피그레이션하십시오.

a) **Device(**디바이스**)**를 클릭하고 **Interfaces(**인터페이스**)** 요약의 링크를 클릭한 다음, **Interfaces** 또는 **EtherChannel**를 클릭합니다.

b) 수정할 물리적 인터페이스 또는 EtherChannel의 수정 아이콘( )을 클릭합니다.

현재 사용되지 않는 인터페이스를 선택합니다. 사용 중인 인터페이스를 패시브 인터페이스로 변환하려는 경우 먼저 모든 보안 영역에서 인터페이스를 제거하고 해당 인터페이스를 사용하는 다른 모든 컨피그레이션을 제거해야 합니다.

c) **Status(**상태**)** 슬라이더를 활성화된 설정( )으로 지정합니다.

d) 다음을 구성합니다.

- **Interface Name(**인터페이스 이름**)** - 인터페이스의 이름(최대 48자)입니다. 영문자는 소문자로 입력해야 합니다. 예를 들어 **monitor**를 입력합니다.
- **Mode(**모드**)** - **Passive(**패시브**)**를 선택합니다.

e) **OK(**확인**)**를 클릭합니다.

단계 **4** 인터페이스에 대해 패시브 보안 영역을 생성합니다.

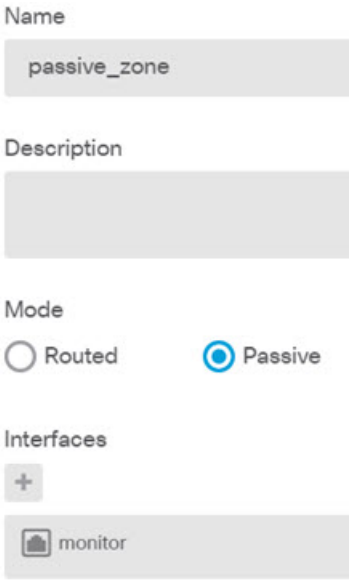
a) 목차에서 **Objects(**개체**)**와 **Security Zones(**보안 영역**)**을 차례로 선택합니다.

b) + 버튼을 클릭합니다.

c) 개체의 **Name(**이름**)** 및 설명(선택 사항)을 입력합니다. 예를 들어 **passive_zone**을 입력합니다.

d) **Mode(**모드**)**로는 **Passive(**패시브**)**를 선택합니다.

e) +를 클릭하고 패시브 인터페이스를 선택합니다.



f) **OK(**확인**)**를 클릭합니다.

단계 **5** 패시브 보안 영역에 대해 액세스 제어 규칙을 하나 이상 구성합니다.

생성하는 규칙의 수와 유형은 수집하려는 정보에 따라 달라집니다. 예를 들어 시스템을 IDS(Intrusion Detection System)로 구성하려는 경우 침입 정책이 할당된 Allow(허용) 규칙이 하나 이상 필요합니다. URL 카테고리 데이터를 수집하려는 경우에는 URL 카테고리 사양이 포함된 규칙이 하나 이상 필요합니다.

Block(차단) 규칙을 생성하면 실제 라우팅 인터페이스에서 시스템이 차단하는 연결을 확인할 수 있습니다. 인터페이스가 패시브이므로 이러한 연결이 실제로 차단되지는 않습니다. 하지만 시스템이 네트워크의 트래픽을 정리한 방식을 명확하게 확인할 수 있습니다.

다음 사용 사례에서는 액세스 제어 규칙의 기본적인 사용법을 다룹니다. 이러한 사용법은 패시브 인터페이스에도 적용됩니다. 생성하는 규칙의 보안 영역으로 패시브 보안 영역을 선택하면 됩니다.

- 위협을 차단하는 방법, 57 페이지
- 악성코드를 차단하는 방법, 62 페이지
- 사용 제한 정책(URL 필터링)을 구현하는 방법, 65 페이지
- 애플리케이션 사용량을 제어하는 방법, 70 페이지

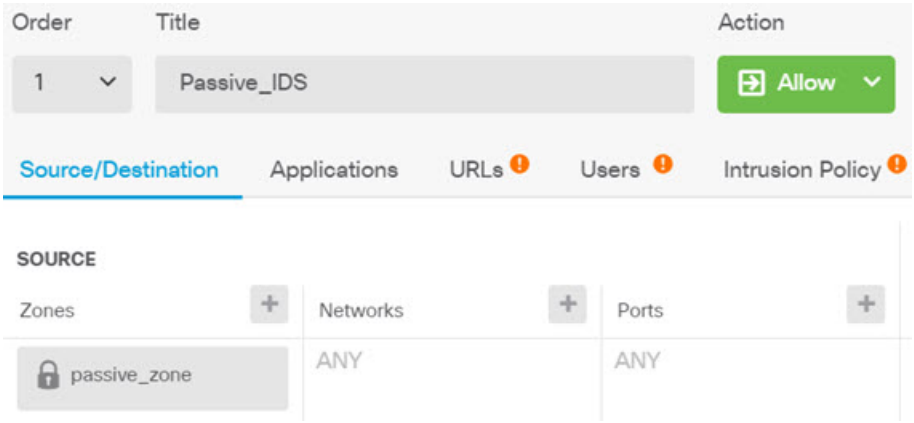
다음 절차에서는 침입 정책을 적용하고 URL 카테고리 데이터를 수집하기 위한 Allow(허용) 규칙 2개를 생성합니다.

a) **Policies(**정책**)** > **Access Control(**액세스 제어**)**을 선택합니다.
b) **+**를 클릭하여 모든 트래픽을 허용하되 침입 정책을 적용하는 규칙을 추가합니다.
c) 규칙 순서로 **1**을 선택합니다. 이 규칙은 기본 규칙보다 구체적이지만 기본 규칙과 겹치지는 않습니다. 맞춤형 규칙이 이미 있는 경우 적절한 위치를 선택합니다. 그래야 패시브 인터페이스로의 트래픽이 새로 추가하는 규칙 대신 해당 규칙과 일치하는 상황이 발생하지 않습니다.
d) 규칙의 이름(예: **Passive_IDS**)을 입력합니다.

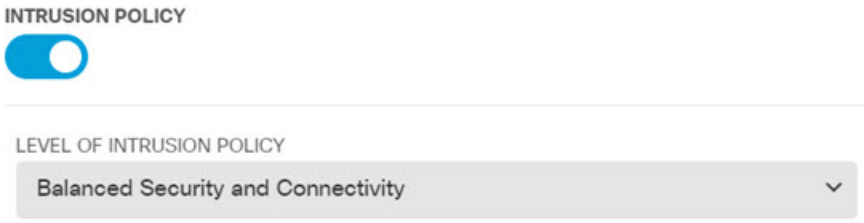
e) **Action(**작업**)**으로 **Allow(**허용**)**를 선택합니다.

f) **Source/Destination(**소스/대상**)** 탭의 **Source(**소스**)** > **Zones(**영역**)** 아래에서 패시브 영역을 선택합니다. 해당 탭의 다른 옵션은 구성하지 마십시오.

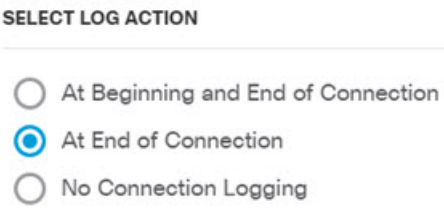
평가 모드에서 실행하는 경우 이 시점에서 규칙은 다음과 같이 표시됩니다.



g) **Intrusion Policy(**침입 정책**)** 탭을 클릭하고 슬라이더를 클릭하여 **On(**켜기**)**으로 전환한 다음 대다수 네트워크에 권장되는 **Balanced Security and Connectivity(**균형 잡힌 보안 및 연결성**)** 정책과 같은 침입 정책을 선택합니다.



h) **Logging(**로깅**)** 탭을 클릭하고 로깅 옵션으로 **At End of Connection(**연결 종료 시**)**을 선택합니다.



i) **OK(**확인**)**를 클릭합니다.

j) **+**를 클릭하여 시스템이 심층 검사를 수행해 모든 HTTP 요청의 URL 및 카테고리를 확인해야 하도록 하는 규칙을 추가합니다.

이 규칙을 사용하면 대시보드에서 URL 카테고리 정보를 확인할 수 있습니다. 시스템은 처리 시간을 절약하고 성능을 개선하기 위해 URL 카테고리 조건을 지정하는 액세스 제어 규칙이 하나 이상 있을 때만 URL 카테고리를 확인합니다.

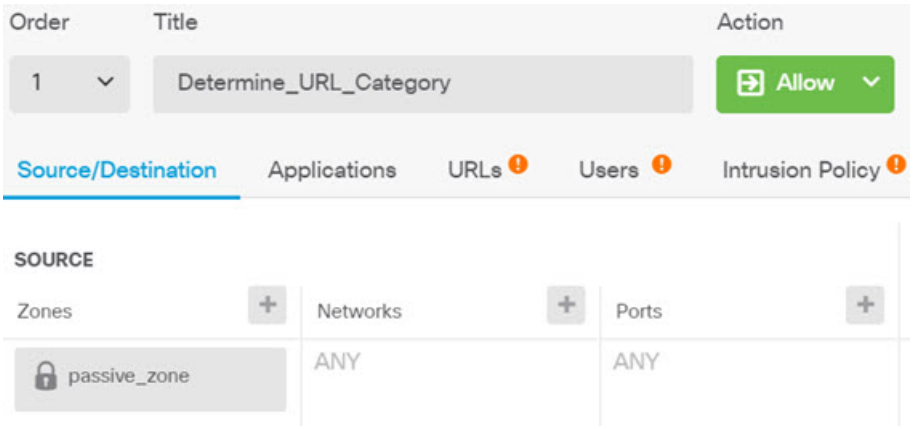
k) 규칙 순서로 **1**을 선택합니다. 그러면 해당 규칙이 이전 규칙(Passive_IDS) 위에 배치됩니다. 지금 생성하는 규칙은 해당 규칙(모든 트래픽에 적용됨) 뒤에 배치하면 어떤 트래픽과도 일치하지 않게 됩니다.

l) 규칙의 이름(예: **Determine_URL_Category**)을 입력합니다.

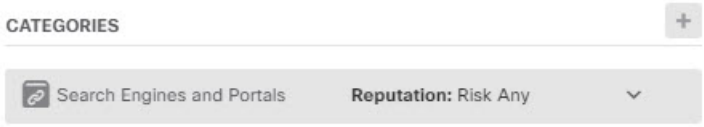
m) **Action(**작업**)**으로 **Allow(**허용**)**를 선택합니다.

Block(차단**)**을 선택할 수도 있습니다. 둘 중 어떤 작업을 선택하든 이 규칙을 추가하는 목표는 달성됩니다.

n) **Source/Destination(**소스/대상**)** 탭의 **Source(**소스**)** > **Zones(**영역**)** 아래에서 패시브 영역을 선택합니다. 해당 탭의 다른 옵션은 구성하지 마십시오.



o) **URLs(URL)** 탭을 클릭하고 **Categories(**카테고리**)** 머리글 옆의 +를 클릭한 다음 원하는 카테고리를 선택합니다. 예를 들어 **Search Engines and Portals(**검색 엔진 및 포털**)**를 선택합니다. 선택적으로 평판도를 선택할 수도 있고 기본값인 Any(모두)로 유지할 수도 있습니다.



p) **Intrusion Policy(**침입 정책**)** 탭을 클릭하고 슬라이더를 클릭하여 **On(**켜기**)**으로 전환한 다음 첫 번째 규칙에 대해 선택한 것과 같은 침입 정책을 선택합니다.

q) **Logging(**로깅**)** 탭을 클릭하고 로깅 옵션으로 **At End of Connection(**연결 종료 시**)**을 선택합니다.

그러나 작업으로 **Block(**차단**)**을 선택한 경우에는 **At Beginning and End of Connection(**연결 시작 및 종료 시**)**을 선택합니다. 차단된 연결 자체가 종료되지는 않으므로 연결 시작 시에만 로그 정보가 제공됩니다.

r) **OK(**확인**)**를 클릭합니다.

단계 **6** (선택 사항). 다른 보안 정책을 구성합니다.

다음 보안 정책을 구성하여 트래픽에 어떤 영향을 주는지를 확인할 수도 있습니다.

- **Identity(ID)** - 사용자 정보를 수집합니다. 소스 IP 주소와 연관된 사용자를 식별할 수 있도록 ID 정책의 규칙을 구성할 수 있습니다. 패시브 인터페이스용 ID 정책 구현 프로세스는 라우팅 인터

페이스용 프로세스와 같습니다. 네트워크 트래픽을 파악하는 방법, 49 페이지에 설명된 사용 사례를 따르십시오.

- **Security Intelligence(**보안 인텔리전스**)** - 알려진 잘못된 IP 주소와 URL을 차단합니다. 자세한 내용은 위협을 차단하는 방법, 57 페이지를 참조해 주십시오.

참고 패시브 인터페이스의 암호화된 트래픽은 모두 암호 해독 불가로 분류되므로 SSL 암호 해독 규칙은 적용되지 않으며 패시브 인터페이스에 적용되지 않습니다.

단계 **7** 변경 사항을 커밋합니다.

a) 웹 페이지의 오른쪽 상단에 있는 **Deploy Changes(**변경 사항 구축**)** 아이콘을 클릭합니다.

b) **Deploy Now(**지금 구축**)** 버튼을 클릭합니다.

구축이 완료될 때까지 기다리거나 **OK(**확인**)**를 클릭하고 나중에 작업 목록 또는 구축 기록을 확인할 수 있습니다.

단계 **8** 모니터링 대시보드를 사용하여 네트워크를 통해 들어오는 트래픽과 위협의 종류를 분석합니다. threat defense 디바이스가 원치 않는 연결을 능동적으로 삭제하도록 하려는 경우, 모니터링하는 네트워크에 대해 방화벽 보호를 제공하는 액티브 라우팅 인터페이스를 컨피그레이션할 수 있도록 디바이스를 재구축하십시오.

추가 예시

사용 사례 장의 예시와 더불어, 특정 서비스를 설명하는 일부 장에도 예시 컨피그레이션이 나와 있습니다. 다음과 같은 예시를 확인할 수 있습니다.

액세스 제어

- TrustSec SGT(Security Group Tag)를 사용하여 네트워크 액세스를 제어하는 방법, 546 페이지

NAT(Network Address Translation)

IPv4 주소에 대한 **NAT**

- 내부 웹 서버에 대한 액세스 제공(고정 자동 NAT), 642 페이지
- FTP, HTTP 및 SMTP용 단일 주소(포트 변환 고정 자동 NAT), 645 페이지
- 대상에 따라 다른 변환(동적 수동 PAT), 651 페이지
- 대상 주소 및 포트에 따라 다른 변환(동적 수동 PAT), 657 페이지
- DNS 회신 수정, 외부의 DNS 서버, 670 페이지
- DNS 회신 수정, 호스트 네트워크의 DNS 서버, 673 페이지

- NAT에서 사이트 대 사이트 VPN 트래픽 제외, 705 페이지

IPv6 주소에 대한 **NAT**

- NAT64/46 예: 내부 IPv6 네트워크 및 외부 IPv4 인터넷, 628 페이지
- NAT64/46 예: 내부 IPv6 네트워크와 외부 IPv4 인터넷 및 DNS 변환, 630 페이지
- NAT66 예, 네트워크 간의 고정 변환, 635 페이지
- NAT66 예, 간단한 IPv6 인터페이스 PAT, 638 페이지
- DNS 64 회신 수정, 664 페이지

RA VPN(Remote Access Virtual Private Network)

- RADIUS CoA(Change of Authorization) 구현 방법, 758 페이지
- Duo LDAP를 사용하여 이중 인증을 구성하는 방법, 768 페이지
- 원격 액세스 VPN 사용자에게 외부 인터페이스를 통해 인터넷 액세스를 제공하는 방법(헤어피닝), 775 페이지
- 원격 액세스 VPN을 통해 외부 네트워크에서 디렉터리 서버를 사용하는 방법, 780 페이지
- 그룹별로 RA VPN 액세스를 제어하는 방법, 795 페이지
- RA VPN 액세스를 다른 가상 라우터의 내부 네트워크에 허용하는 방법, 799 페이지
- Secure Client 아이콘 및 로고를 맞춤화하는 방법, 803 페이지

사이트 대 사이트 **VPN(Virtual Private Network)**

- NAT에서 사이트 대 사이트 VPN 트래픽 제외, 705 페이지
- 외부 사이트 대 사이트 VPN 사용자에게 외부 인터페이스를 통해 인터넷 액세스를 제공하는 방법(헤어피닝), 711 페이지
- 사이트 간 VPN을 통해 여러 가상 라우터의 네트워크에서 트래픽을 보호하는 방법, 719 페이지

SSL/TLS 암호 해독

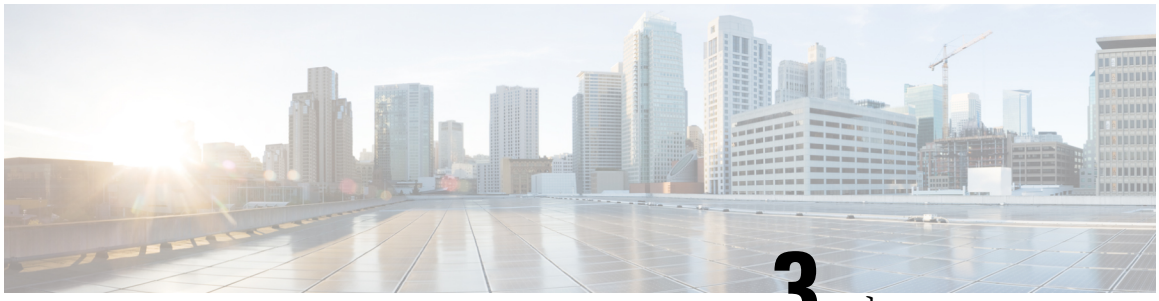
- 예: 네트워크에서 이전 SSL/TLS 버전 차단, 486 페이지

FlexConfig 정책

- 전역 기본 검사를 활성화/비활성화하는 방법, 933 페이지
- FlexConfig 변경 사항을 실행 취소하는 방법, 939 페이지
- 고유한 트래픽 클래스에 대한 검사를 활성화하는 방법, 941 페이지

가상 라우팅

- 중복된 어드레스 스페이스가 있는 여러 가상 라우터에 인터넷 액세스를 제공하는 방법 , 362 페이지
- 여러 가상 라우터를 통해 원거리 서버로 라우팅하는 방법, 356 페이지
- RA VPN 액세스를 다른 가상 라우터의 내부 네트워크에 허용하는 방법, 799 페이지
- 사이트 간 VPN을 통해 여러 가상 라우터의 네트워크에서 트래픽을 보호하는 방법, 719 페이지



3 장

시스템 라이선싱

다음 주제에서는 threat defense 디바이스 라이선싱 방법을 설명합니다.

Firewall System 스마트 라이선싱

시스코 스마트 라이선싱은 시스코 포트폴리오 및 조직 전체에서 소프트웨어를 보다 쉽고 빠르고 일관적인 방식으로 구매하고 관리할 수 있는 유연한 라이선싱 모델입니다. 또한 사용자가 액세스할 수 있는 항목을 제어할 수 있어 안전합니다. 스마트 라이선싱을 사용하면 다음과 같은 이점을 누릴 수 있습니다.

- 손쉬운 활성화: 스마트 라이선싱은 전체 조직에서 사용할 수 있는 소프트웨어 라이선스 풀을 설정하므로 더 이상 PAK(제품 활성화 키)가 필요하지 않습니다.
- 통합 관리: MCE(My Cisco Entitlements)는 사용하기 쉬운 포털에서 모든 시스코 제품 및 서비스에 대한 완벽한 보기를 제공하므로 무엇을 보유하고 있으며 무엇을 사용 중인지 항상 파악할 수 있습니다.
- 라이선스 유연성: 소프트웨어가 하드웨어에 노드로 고정되어 있지 않으므로 필요에 따라 라이선스를 쉽게 사용하고 전송할 수 있습니다.

스마트 라이선싱을 사용하려면 먼저 Cisco Software Central(software.cisco.com)에서 스마트 어카운트를 설정해야 합니다.

시스코 라이선싱에 대한 자세한 내용은 cisco.com/go/licensingguide를 참조하세요.

Cisco Smart Software Manager

threat defense 디바이스 라이선스를 1개 이상 구매한 경우, Cisco Smart Software Manager(https://software.cisco.com/#SmartLicensing-Inventory)에서 라이선스를 관리할 수 있습니다. Cisco Smart Software Manager에서는 조직의 기본 어카운트를 생성할 수 있습니다.

기본적으로는 기본 어카운트의 기본 가상 어카운트에 라이선스가 할당됩니다. 어카운트 관리자는 지역, 부서, 자회사 등에 대해 가상 어카운트를 추가로 생성할 수 있습니다. 여러 가상 어카운트가 있으면 수많은 라이선스 및 어플라이언스를 관리할 수 있습니다.

라이선스 및 어플라이언스는 가상 어카운트별로 관리됩니다. 해당 가상 어카운트의 어플라이언스만 어카운트에 할당된 라이선스를 사용할 수 있습니다. 추가 라이선스가 필요할 경우 다른 가상 계정의 미사용 라이선스를 이전할 수 있습니다. 또한 가상 어카운트 간에 어플라이언스를 전송할 수도 있습니다.

Cisco Smart Software Manager를 사용하여 디바이스를 등록할 때는 Smart Software Manager에서 제품 인스턴스 등록 토큰을 생성한 다음 device manager에 입력합니다. 등록된 디바이스는 사용하는 토큰에 따라 가상 어카운트와 연결됩니다.

Cisco Smart Software Manager에 대한 자세한 내용은 Smart Software Manager 온라인 도움말을 참조하십시오.

License Authority와의 정기적인 통신

제품 인스턴스 등록 토큰을 사용하여 threat defense 디바이스를 등록하면 디바이스가 Cisco License Authority에 등록됩니다. License Authority에서는 디바이스와 License Authority의 통신을 위해 ID 인증서를 발급합니다. 이 인증서는 6개월마다 갱신되지만 1년간 유효합니다. ID 인증서가 만료되면(대개 9개월 후 또는 통신을 수행하지 않는 경우 1년 후) 디바이스는 등록 취소된 상태로 돌아가며 라이선스 기능의 사용이 일시 중단됩니다.

디바이스는 주기적으로 License Authority와 통신합니다. Cisco Smart Software Manager에 변경이 있는 경우 변경 사항이 즉시 적용되도록 디바이스에서 권한 부여를 새로 고칠 수 있습니다. 또는 디바이스에서 예정대로 통신할 때까지 기다릴 수 있습니다. 일반 라이선스 통신은 12시간마다 이루어지지만, 유예 기간이 있으면 디바이스는 최대 90일간 콜 홈 없이 작동할 수 있습니다. 90일이 지나기 전에 License Authority에 접속해야 합니다.

스마트 라이선스 유형

다음 표에서는 threat defense 디바이스에 사용할 수 있는 라이선스에 관해 설명합니다.

threat defense 디바이스 구매 시 Base 라이선스가 자동으로 포함됩니다. 모든 추가 라이선스는 선택 사항입니다.

표 ***3:*** 스마트 라이선스 유형

라이선스	기간	부여된 기능
Base	영구	선택적 기간 라이선스가 적용되지 않는 모든 기능. Base 라이선스는 등록 시 어카운트에 자동으로 추가됩니다. 보안 방화벽 3100은 예외입니다. 방화벽을 구매하면 Base 라이선스를 받게 되며, 라이선스는 어카운트의 다른 라이선스처럼 관리됩니다. 예를 들어 등록할 때 라이선스가 올바른 가상 어카운트에 있는지 확인해야 합니다. 이 토큰을 사용하여 등록한 제품에서 내보내기 제어 기능을 허용할지도 지정해야 합니다. 현재 거주 국가가 내보내기 제어 표준을 충족하는 경우에만 이 옵션을 선택할 수 있습니다. 이 옵션은 고급 암호화 사용과 고급 암호화를 필요로 하는 기능 사용을 제어합니다.
위협	기간 기준	다음 정책을 사용하는 데 필요합니다. • 침입 • 파일(악성코드도 필요함) • 보안 인텔리전스
악성코드	기간 기준	파일 정책(위협도 필요함).
URL	기간 기준	URL 정책 - 범주 및 평판 기반 URL 필터링 또는 DNS 조회 요청 필터링. 이 라이선스가 없어도 개별 URL에 대해 URL 필터링을 수행할 수 있습니다.

라이선스	기간	부여된 기능
RA VPN: • AnyConnect Plus • AnyConnect Apex • AnyConnect VPN Only	라이선스 유형에 따라 기간 기준 또는 영구	원격 액세스 VPN 컨피그레이션 기본 라이선스는 RA VPN 구성을 위한 내보내기 제어 기능을 허용해야 합니다. 디바이스를 등록할 때 내보내기 요구사항을 충족하는지를 선택합니다. device manager는 유효한 Secure Client 라이선스를 사용할 수 있습니다. 제공되는 기능은 라이선스 유형에 따라 달라지지 않습니다. 라이선스를 아직 구매하지 않은 경우에는 원격 액세스 VPN에 대한 라이선싱 요구 사항, 732 페이지를 참조하십시오. *Cisco AnyConnect* 주문 가이드, http://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-og.pdf도 참조하십시오.

Threat Defense Virtual 라이선싱

이 섹션에서는 threat defense virtual에서 사용 가능한 성능 계층 라이선스 자격을 설명합니다.

모든 threat defense virtual 라이선스는 지원되는 threat defense virtual vCPU/메모리 설정에서 사용할 수 있습니다. 따라서 threat defense virtual 고객은 다양한 VM 리소스 사용 공간에서 실행할 수 있습니다. 또한 지원되는 AWS 및 Azure 인스턴스 유형의 수가 증가합니다. threat defense virtual VM을 설정할 때 지원되는 최대 코어 수(vCPU)는 16개이고 지원되는 최대 메모리는 32GB RAM입니다.

Threat Defense Virtual 스마트 라이선싱의 성능 계층

RA VPN의 세션 제한은 설치된 threat defense virtual 플랫폼 엔타이틀먼트 계층에 따라 결정되고, 속도 제한기를 통해 적용됩니다. 다음 테이블에는 엔타이틀먼트 계층 및 속도 제한기에 따른 세션 제한이 요약되어 있습니다.

표 *4:* 자격 기준 ***Threat Defense Virtual*** 라이선스 기능 제한

성능 계층	디바이스 사양 **(Core/RAM)**	속도 제한	**RA VPN** 세션 제한
FTDv5, 100Mbps	4 코어/8GB	100Mbps	50
FTDv10, 1Gbps	4 코어/8GB	1Gbps	250
FTDv20, 3Gbps	4 코어/8GB	3Gbps	250
FTDv30, 5Gbps	8 코어/16GB	5Gbps	250
FTDv50, 10Gbps	12 코어/24GB	10Gbps	750
FTDv100, 16Gbps	16 코어/32GB	16Gbps	10,000

Threat Defense Virtual 성능 계층 라이선싱 지침 및 제한

threat defense virtual 디바이스 라이선싱 시 다음 지침과 제한 사항에 유의하십시오.

- threat defense virtual에서는 구축 요건에 따라 다양한 처리량 레벨 및 VPN 연결 제한을 제공하는 성능 계층 라이선싱을 지원합니다.
- 모든 threat defense virtual 라이선스는 지원되는 threat defense virtual 코어/메모리 설정에서 사용할 수 있습니다. 따라서 threat defense virtual 고객은 다양한 VM 리소스 사용 공간에서 실행할 수 있습니다.
- 디바이스가 평가 모드인지 또는 이미 Cisco Smart Software Manager에 등록되어 있는지 여부와 무관하게 threat defense virtual 구축 시 성능 계층을 선택할 수 있습니다.

참고 Smart Licensing 계정에서 필요한 라이선스가 사용 가능한지 확인합니다. 어카운트에 있는 라이선스와 일치하는 계층을 선택하는 것이 중요합니다. threat defense virtual를 버전 7.0으로 업그레이드하는 경우 **FTDv - Variable(FTDv -** 변수**)**를 선택하여 현재 라이선스 컴플라이언스를 유지할 수 있습니다. threat defense virtual는 디바이스 기능(코어/RAM 수)에 따라 계속 세션 제한을 수행합니다.

- 새 threat defense virtual 디바이스를 구축하거나 REST API를 사용한 threat defense virtual 프로비저닝 시 기본 성능 계층은 FTDv50입니다.
- Base 라이선스는 구독 기반이며 성능 계층에 매핑됩니다. 가상 어카운트에는 위협, 악성코드 및 URL 필터링 라이선스는 물론 threat defense virtual 디바이스에 대한 Base 라이선스 자격이 있어야 합니다.
- 각 HA 피어는 하나의 자격을 사용하고, Base 라이선스를 포함하여 각 HA 피어의 자격이 일치해야 합니다.
- HA 쌍의 성능 계층 변경 사항을 기본 피어에 적용해야 합니다.
- 범용 PLR 라이선싱은 HA 쌍의 각 디바이스에 개별적으로 적용됩니다. 보조 디바이스는 기본 디바이스의 성능 계층을 자동으로 미러링하지 않습니다. 수동으로 업데이트해야 합니다.

내보내기 제어 설정이 암호화 기능에 미치는 영향

디바이스를 등록할 때 이 토큰을 사용하여 등록한 제품에서 내보내기 제어 기능을 허용할지도 지정해야 합니다. 현재 거주 국가가 내보내기 제어 표준을 충족하는 경우에만 이 옵션을 선택할 수 있습니다. 이 옵션은 고급 암호화 사용과 고급 암호화를 필요로 하는 기능 사용을 제어합니다.

평가 모드는 내보내기와 호환되지 않는 계정을 사용하여 등록하는 것과 동일하게 처리됩니다. 즉, 평가 모드에서 실행할 때는 원격 액세스 VPN을 구성하거나 고급 암호화 알고리즘을 사용할 수 없습니다.

특히 DES 표준은 평가 또는 내보내기와 호환되지 않는 모드에서만 사용할 수 있습니다.

따라서 사이트 간 VPN과 같은 암호화된 기능을 구성하거나 고가용성 그룹에서 페일오버 연결을 암호화하는 경우 내보내기 호환 계정에 등록한 후 연결 문제가 발생할 수 있습니다. 기능이 평가 모드에서 DES를 사용 중인 경우 계정을 등록한 후에 해당 구성이 중단됩니다.

암호화 관련 문제를 방지하려면 다음 권장 사항을 고려하십시오.

- 디바이스를 등록할 때까지 사이트 간 VPN 및 암호화된 페일오버 연결과 같은 암호화된 기능을 구성하지 마십시오.
- 내보내기 호환 계정을 사용하여 디바이스를 등록한 후 평가 모드에서 구성한 모든 암호화된 기능을 편집하고 더 안전한 암호화 알고리즘을 선택합니다. 각 기능을 테스트하고 확인하여 기능이 올바르게 작동하는지 확인합니다.

참고 평가 모드에서 HA 페일오버 암호화를 구성한 경우, 더 강력한 암호화를 사용하려면 HA 그룹의 두 디바이스를 모두 재부팅해야 합니다. 두 디바이스가 모두 활성 유닛으로 간주되는 스플릿 브레인 상황을 방지하려면 먼저 암호화를 제거하는 것이 좋습니다.

만료되거나 비활성화된 선택 가능한 라이선스의 영향

다음의 선택 가능한 라이선스 중 하나가 만료된 경우 라이선스가 필요한 기능을 계속 사용할 수 있습니다. 그러나 라이선스는 컴플라이언스 상태가 아닌 것으로 표시되며, 라이선스를 컴플라이언스 상태로 다시 설정하려면 라이선스를 구매하여 어카운트에 추가해야 합니다.

선택 가능한 라이선스를 비활성화하면 시스템은 다음과 같이 대응합니다.

- 악성코드 - 시스템에서 Secure Malware Analytics 클라우드에 대한 쿼리를 중단하며 Secure Malware Analytics 클라우드에서 전송한 회귀적 이벤트 확인도 중지합니다. 파일 정책이 포함된 경우, 기존 액세스 제어 정책은 재구축할 수 없습니다. 악성코드 라이선스가 비활성화된 매우 짧은 시간 동안 시스템은 기존에 캐시된 파일 상태를 사용할 수 있습니다. 이 기간이 만료되고 나면 시스템은 해당 파일에 사용할 수 없음 상태를 할당합니다.
- 위협 - 시스템이 더 이상 침입 또는 파일 정책을 적용하지 않습니다. 보안 인텔리전스 정책의 경우 시스템은 더 이상 정책을 적용하지 않고 피드 업데이트 다운로드를 중지합니다. 라이선스가 필요한 기존 정책은 재구축할 수 없습니다.
- URL - URL 범주 조건이 포함된 액세스 제어 규칙의 URL 또는 DNS 조회 요청 필터링이 즉시 중지되며 시스템이 URL 데이터에 대한 업데이트를 더 이상 다운로드하지 않습니다. 범주 및 평판 기반 URL 조건이 들어 있는 규칙을 포함하는 기존 액세스 제어 정책은 재적용할 수 없습니다.
- RA VPN - 원격 액세스 VPN 컨피그레이션을 수정할 수는 없지만, 제거할 수는 있습니다. 사용자는 RA VPN 컨피그레이션을 사용하여 계속 연결할 수 있습니다. 그러나 디바이스 등록을 변경하여 시스템이 더 이상 내보내기 방식을 준수하지 않는 경우에는 원격 액세스 VPN 컨피그레이션이 즉시 중지되며 원격 사용자가 VPN을 통해 연결할 수 없습니다.

스마트 라이선스 관리

스마트 라이선스 페이지를 사용하여 시스템의 현재 라이선스 상태를 확인합니다. 시스템에 라이선스가 있어야 합니다.

이 페이지에는 90일 평가 라이선스를 사용 중인지 아니면 Cisco Smart Software Manager에 등록되었는지가 표시됩니다. 등록한 경우 Cisco Smart Software Manager에 대한 연결 상태와 각 라이선스 유형의 상태를 확인할 수 있습니다.

사용 권한 부여에서 스마트 라이선스 에이전트 상태를 식별합니다.

- 권한 있음("연결됨", "충분한 라이선스") - 디바이스가 License Authority에 연결하여 정상적으로 등록되었으며, 어플라이언스에 대한 라이선스 자격이 부여되었습니다. 디바이스는 현재 컴플라이언스 상태입니다.
- 규정 미준수 - 디바이스에 대해 사용 가능한 라이선스 자격이 없습니다. 라이선스 기능은 계속 작동합니다. 그러나 추가 자격을 구매하거나 확보해야 디바이스의 컴플라이언스 상태가 될 수 있습니다.
- 권한 부여 만료됨 - 디바이스가 90일 이상 Licensing Authority와 통신하지 않았습니다. 라이선스 기능은 계속 작동합니다. 이 상태에서 스마트 라이선스 에이전트는 권한 부여 요청을 다시 시도합니다. 다시 시도가 성공하면 에이전트는 규정 미준수 또는 권한 있음 상태로 설정되며 새 권한 부여 기간이 시작됩니다. 이 경우 디바이스를 수동으로 동기화해 보십시오.

참고 스마트 라이선스 상태 옆의 **i** 버튼을 클릭하여 가상 어카운트와 내보내기 제어 기능을 확인하고 Cisco Smart Software Manager를 여는 링크를 확인합니다. 내보내기 제어 기능은 국가별 보안, 해외 정책 및 테러 방지법과 규정이 적용되는 소프트웨어를 제어합니다.

다음 절차에서는 시스템의 라이선스를 관리하는 방법을 간략하게 설명합니다.

시작하기 전에

시스템에 인터넷에 대한 경로가 없는 경우 스마트 라이선싱을 사용할 수 없습니다. 그 대신 영구 라이선스 예약(PLR) 모드로 전환합니다. 자세한 내용은 에어 갭(Air-Gapped) 네트워크에서 영구 라이선스 적용, 100 페이지를 참조하십시오.

프로시저

단계 **1** 디바이스를 클릭한 다음, 스마트 라이선스 요약에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

단계 **2** 디바이스를 등록합니다.

Cisco Smart Software Manager에 등록해야 선택 가능한 라이선스를 할당할 수 있습니다. 평가 기간이 종료되기 전에 등록하십시오.

디바이스 등록, 96 페이지의 내용을 참조하십시오.

참고 등록 시 Cisco에 사용량 데이터를 보낼지를 선택하십시오. 기어 아이콘 옆에 있는 **Go To Cisco Success Network(Cisco Success Network로 이동)** 링크를 클릭하여 선택을 변경할 수 있습니다.

단계 **3** 선택 가능한 기능 라이선스를 요청하고 관리합니다.

라이선스를 통해 제어되는 기능을 사용하려면 선택 가능한 라이선스를 등록해야 합니다. 선택 가능한 라이선스 활성화 또는 비활성화, 98 페이지의 내용을 참조하십시오.

단계 **4** 시스템 라이선싱을 유지합니다.

다음과 같은 작업을 수행할 수 있습니다.

- Cisco Smart Software Manager와 동기화, 99 페이지
- 디바이스 등록 취소, 99 페이지

디바이스 등록

threat defense 디바이스 구매 시 Base 라이선스가 자동으로 포함됩니다. Base 라이선스는 선택 가능한 라이선스에 포함되지 않는 모든 기능을 포함합니다. 영구 라이선스입니다.

초기 시스템 설정 중에 Cisco Smart Software Manager에 디바이스를 등록하라는 메시지가 표시됩니다. 90일 평가 라이선스를 대신 선택한 경우에는 평가 기간이 종료되기 전에 디바이스를 등록해야 합니다.

디바이스를 등록할 때는 가상 어카운트가 디바이스에 라이선스를 할당합니다. 디바이스를 등록하면 활성화한 선택 가능한 라이선스도 등록됩니다.

시작하기 전에

디바이스를 등록하면 해당 디바이스만 등록됩니다. 디바이스가 고가용성을 제공하도록 구성된 경우에는 고가용성 쌍의 다른 유닛에 로그인하여 해당 유닛을 등록해야 합니다.

프로시저

단계 **1** 디바이스를 클릭한 다음, 스마트 라이선스 요약에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

단계 **2** **Register Device(**디바이스 등록**)**를 클릭하고 지침을 따릅니다.

a) 링크를 클릭하여 Cisco Smart Software Manager를 열고 어카운트에 로그인하거나 필요한 경우 새 어카운트를 생성합니다.

b) 새 토큰을 생성합니다.

토큰을 생성할 때는 토큰을 사용할 수 있는 유효 기간을 지정합니다. 권장 만료 기간은 30일입니다. 이 기간은 토큰 자체의 만료 날짜를 정의하며 토큰을 사용하여 등록하는 디바이스에는 영향을 주지 않습니다. 토큰이 사용하기 전에 만료되는 경우 새 토큰을 생성하면 됩니다.

이 토큰을 사용하여 등록한 제품에서 내보내기 제어 기능을 허용할지도 지정해야 합니다. 현재 거주 국가가 내보내기 제어 표준을 충족하는 경우에만 이 옵션을 선택할 수 있습니다. 이 옵션은 고급 암호화 사용과 고급 암호화를 필요로 하는 기능 사용을 제어합니다.

c) 토큰을 복사하여 스마트 라이선스 등록 대화 상자의 수정 상자에 붙여넣습니다.

d) (**Threat Defense Virtual** 전용) threat defense virtual 디바이스에 대한 성능 계층을 선택하거나 기본 선택을 유지합니다.

성능 계층을 선택하지 않은 경우 threat defense virtual 디바이스는 4코어/8GB의 기본 설정으로 레거시 모드에서 실행됩니다. 자세한 내용은 Threat Defense Virtual 성능 계층 변경, 97 페이지의 내용을 참조하십시오.

e) Cisco Cloud Services 등록을 위한 지역을 선택합니다.

등록 후 이 지역을 변경해야 하는 경우, 디바이스를 등록 취소한 다음 다시 등록하고 새 지역을 선택해야 합니다.

f) 사용량 데이터를 Cisco에 보낼지를 결정합니다.

Cisco Success Network 단계에 나와 있는 정보를 읽고 **Sample Data(**샘플 데이터**)** 링크를 클릭하여 수집된 실제 데이터를 확인한 다음 **Enable Cisco Success Network(Cisco Success Network** 활성화**)** 옵션을 선택한 상태로 둘지를 결정합니다.

g) **Register Device(**디바이스 등록**)**를 클릭합니다.

Threat Defense Virtual 성능 계층 변경

threat defense virtual에서는 구축 요건에 따라 다양한 처리량 레벨 및 VPN 연결 제한을 제공하는 성능 계층 라이선싱을 지원합니다. 모든 threat defense virtual 라이선스는 지원되는 threat defense virtual 코어/메모리 설정에서 사용할 수 있습니다. 따라서 threat defense virtual 고객은 다양한 VM 리소스 사용 공간에서 실행할 수 있습니다. Threat Defense Virtual 스마트 라이선싱의 성능 계층, 92 페이지의 내용을 참조하십시오.

threat defense virtual의 버전 7.0 이상으로 업그레이드 시 디바이스는 "FTDv 변수" 계층으로 자동 이동하고 자격 레벨을 선택할 때까지 계층 없는 자격을 계속 사용하게 됩니다.

참고 처리량 또는 RA VPN 요구 사항에 따라 구축 요건에 맞춰 성능 계층을 변경할 수 있습니다. threat defense virtual의 경우 조정 가능한 코어 및 메모리 리소스를 사용하여 구축합니다. 선택한 성능 계층이 디바이스 사양을 초과해서는 안 됩니다.

프로시저

단계 **1** 디바이스를 클릭한 다음, 스마트 라이선스 요약에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

단계 **2** **Performance Tier(**성능 계층**)** 드롭다운 목록에서 원하는 옵션을 선택합니다.

- FTDv5(4코어/8GB)
- FTDv10(8코어/8GB)
- FTDv20(8코어/8GB)
- FTDv30(8코어/16GB)
- FTDv50(12코어/24GB)
- FTDv100(16코어/24GB)

참고 시스템은 현재 디바이스 사양에 따라 최적의 계층을 강조 표시합니다.

단계 **3** 선택 및 디바이스 사양을 검토합니다.

참고 threat defense virtual VM을 설정할 때 지원되는 최대 코어 수(vCPU)는 12개(VMware 및 KVM의 FTDv100의 경우 16개)입니다. 지원되는 최대 메모리는 24GB RAM입니다. 선택한 성능 계층이 디바이스 사양을 초과해서는 안 됩니다.

단계 **4** **YES(**예**)**를 클릭하여 성능 계층을 변경합니다.

선택 가능한 라이선스 활성화 또는 비활성화

선택 가능한 라이선스는 활성화(등록)하거나 비활성화(해제)할 수 있습니다. 라이선스를 통해 제어되는 기능을 사용하려면 라이선스를 활성화해야 합니다.

선택적 기간 라이선스가 적용되는 기능을 더 이상 사용하지 않으려는 경우 라이선스를 비활성화할 수 있습니다. 비활성화하는 라이선스는 Cisco Smart Software Manager 어카운트에서 해제되므로 다른 디바이스에 적용할 수 있습니다.

평가 모드에서 실행 중인 경우 이러한 라이선스의 평가 버전을 활성화할 수도 있습니다. 평가 모드에서 라이선스는 디바이스를 등록할 때까지 Cisco Smart Software Manager에 등록되지 않습니다. 그러나 평가 모드에서는 RA VPN 라이선스를 활성화할 수 없습니다.

시작하기 전에

라이선스를 비활성화하기 전에 해당 라이선스를 사용하고 있지 않은지 확인합니다. 라이선스가 필요한 정책은 재작성하거나 삭제합니다.

고가용성 컨피그레이션에서 작동 중인 유닛의 경우 액티브 유닛에서만 라이선스를 활성화하거나 비활성화합니다. 다음번 컨피그레이션 구축 시에 스탠바이 유닛이 필요한 라이선스를 요청하거나 해제할 때 변경 사항이 스탠바이 유닛에 반영됩니다. 라이선스를 활성화하는 경우에는 Cisco Smart Software Manager 어카운트에 사용 가능한 라이선스가 충분한지 확인해야 합니다. 그렇지 않으면 각 유닛의 컴플라이언스 상태가 서로 다를 수 있습니다.

프로시저

단계 **1** 디바이스를 클릭한 다음, 스마트 라이선스 요약에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

단계 **2** 선택 가능한 각 라이선스에 대해 **Enable(**활성화**)/Disable(**비활성화**)** 컨트롤을 필요한 대로 클릭합니다.

- **Enable(**활성화**)** - Cisco Smart Software Manager 어카운트에 라이선스를 등록하고 제어되는 기능을 활성화합니다. 이제 라이선스를 통해 제어되는 정책을 구성하고 구축할 수 있습니다.
- **Disable(**비활성화**)** - Cisco Smart Software Manager 어카운트에서 라이선스를 등록 취소하고 제어되는 기능을 비활성화합니다. 이렇게 하면 새 정책에서 기능을 구성할 수 없으며 해당 기능을 사용하는 정책을 구축할 수도 없습니다.

단계 **3** **RA VPN** 라이선스를 활성화한 경우 어카운트에서 사용 가능한 라이선스의 유형을 선택합니다.

모든 AnyConnect 라이선스(**Plus**, **Apex** 또는 **VPN** 전용)를 사용할 수 있습니다. Plus 라이선스와 Apex 라이선스가 둘 다 있으며 모두 사용하려는 경우 **Plus** 및 **Apex**를 선택할 수 있습니다.

Cisco Smart Software Manager와 동기화

시스템은 Cisco Smart Software Manager와 주기적으로 라이선스 정보를 동기화합니다. 일반 라이선스 통신은 30일마다 이루어지지만, 유예 기간이 있으므로 어플라이언스는 최대 90일간 콜 홈 없이 작동할 수 있습니다.

그러나 Cisco Smart Software Manager에서 변경을 수행할 경우 변경 사항이 즉시 적용되도록 디바이스에서 권한 부여를 새로 고칠 수 있습니다.

동기화 시에는 라이선스의 현재 상태를 가져오며 권한 부여와 ID 인증서가 갱신됩니다.

프로시저

단계 **1** 디바이스를 클릭한 다음, 스마트 라이선스 요약에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

단계 **2** 기어 드롭다운 목록에서 **Resync Connection(**연결 재동기화**)**를 선택합니다.

디바이스 등록 취소

더 이상 디바이스를 사용하지 않으려는 경우 Cisco Smart Software Manager에서 디바이스를 등록 취소할 수 있습니다. 등록을 취소하면 디바이스에 연결된 Base 라이선스 및 선택 가능한 모든 라이선스가 가상 어카운트에서 해제됩니다. 선택 가능한 라이선스는 다른 디바이스에 할당할 수 있습니다. 또한 디바이스는 클라우드 및 클라우드 서비스에서도 등록이 취소됩니다.

디바이스를 등록 취소한 후에도 디바이스의 현재 컨피그레이션 및 정책은 계속 원래대로 작동하지만 변경을 수행하거나 변경 사항을 구축할 수는 없습니다.

시작하기 전에

디바이스 등록을 취소하면 해당 디바이스만 등록 취소됩니다. 디바이스가 고가용성을 제공하도록 구성된 경우에는 고가용성 쌍의 다른 유닛에 로그인하여 해당 유닛을 등록 취소해야 합니다.

프로시저

단계 **1** 디바이스를 클릭한 다음, 스마트 라이선스 요약에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

단계 **2** 기어 드롭다운 목록에서 **Unregister Device(**디바이스 등록 취소**)**를 선택합니다.

단계 **3** 경고를 확인한 후에 디바이스를 등록 취소하려면 **Unregister(**등록 취소**)**를 클릭합니다.

에어 갭(Air-Gapped) 네트워크에서 영구 라이선스 적용

에어 갭(air-gapped) 네트워크는 인터넷에 대한 경로가 없는 네트워크입니다. 이러한 네트워크는 외부 입력 및 공격의 가능성을 방지하려는 상위 보안 네트워크입니다. 인터넷에 대한 경로가 없으므로 Cisco Smart Software Manager를 사용하여 디바이스를 직접 등록할 수 없습니다. 대신 영구 라이선스 예약(PLR) 모드를 사용하여 디바이스에 적용할 수 있는 라이선스를 얻을 수 있습니다.

PLR 모드를 사용해야 하는 경우에는 다음 사항에 유의하십시오.

- 인터넷에 액세스해야 하는 기능(예: 파일 정책, URL 조회 또는 공용 웹 사이트 상황별 크로스 실행)이 작동하지 않습니다.
- Web Analytics 및 Cisco Success Network를 활성화한다 해도, 인터넷 액세스가 없기 때문에 연결된 데이터를 Cisco에서 수집하지 않습니다.
- 지리위치 데이터베이스, 침입 규칙, VDB(Vulnerability Database)에 업데이트를 수동으로 업로드해야 합니다. 예를 들어 플래시 드라이브에 업데이트를 다운로드한 다음, 드라이브를 보안 구축 환경으로 가져와 보안 워크스테이션에서 이를 업로드할 수 있습니다.

참고 Cisco Smart Software Manager는 디바이스의 일련 번호를 사용하여 영구 라이선스를 할당합니다. 디바이스의 등록을 취소해야 하는 경우 일반 등록 취소 또는 취소 프로세스에서 라이선스 할당을 제거하지 못하면 Cisco 기술 지원에 문의하여 Cisco Smart Software Manager에서 등록을 제거해야 합니다. 디바이스를 다시 이미징하면 라이선스 등록이 제거되지 않습니다.

다음 주제에서는 다양한 유형의 영구 라이선스에 대해 자세히 설명하고, 이러한 라이선스를 적용하는 방법, 그리고 등록을 취소하거나 디바이스 등록을 해제하는 방법에 대해 자세히 설명합니다.

범용 대 특정 영구 라이선스 예약

영구 라이선스 예약은 별도의 두 가지 유형이 있습니다.

- 범용 영구 라이선스 예약(범용 PLR, 즉 UPLR) — 범용 영구 라이선스를 사용하면 모든 옵션 라이선스를 포함하여, 지원되는 방화벽 제품을 영구적으로 무제한 사용할 수 있습니다. 범용 영구 라이선스를 구매한 후 적용하면, 일반적으로 시간을 기반으로 적용되는 기능 라이선스를 영구적으로 적용할 수 있습니다. 그러나 교체 라이선스는 스마트 라이선스 어카운트에서 만료되므로 계속 구매해야 합니다. ISA 3000은 승인된 고객에 대해 범용 PLR을 지원합니다.
- 특정 영구 라이선스 예약(특정 PLR, 즉 SPLR) — 특정 영구 라이선스 예약에는 표준 스마트 라이선싱과 동일한 번호 및 라이선스 유형이 필요합니다. 이 라이선스를 취득하면 기본 라이선스 외에 원하는 선택적인 기능 라이선스를 선택할 수 있습니다. 라이선스가 만료될 때 해당 라이선스를 주기적으로 업데이트해야 합니다.

Device Manager은 범용 PLR만 지원합니다. device manager를 사용하여 특정 PLR을 적용할 수 없습니다.

Cisco 담당자와 협력하여 CSSM(Cisco Smart Software Manager) 어카운트에서 범용 영구 라이선스 예약(PLR) 모드를 활성화해야 합니다.

스마트 어카운트가 범용 라이선스를 제공할 수 있는지 확인

영구 라이선스를 획득하고 적용할 수 있는지 확인하려면 CSSM 어카운트에 로그인하고 **Smart Software Licensing(**스마트 소프트웨어 라이선싱**)** > **Inventory(**인벤토리**)** 페이지로 이동한 다음, **Licenses(**라이선스**)** 탭을 클릭합니다. **License Reservation(**라이선스 예약**)** 버튼이 표시되면 영구 라이선스 예약을 받을 수 있는 권한이 있는 것입니다.

그러나 이 버튼을 누르면 범용 및 특정 영구 라이선스 두 가지 모두에 대해 작동하는 마법사가 시작됩니다.

또한, 사용 가능한 라이선스 목록을 검토하여 디바이스에 대한 범용 라이선스가 있는지 확인해야 합니다. 이 라이선스는 **License Reservation(**라이선스 예약**)** 버튼을 사용하여 실행된 마법사의 2단계에서 선택 가능한 항목으로 표시됩니다.

License Reservation(라이선스 예약**)** 버튼이 표시되고 범용 라이선스를 받을 수 있는 경우, 영구 라이선스를 사용하도록 시스템을 전환하는 작업을 계속 진행할 수 있습니다. 이 버튼이 표시되지 않거나 특정 라이선스만 예약할 수 있는 경우, Cisco 담당자에게 전화하여 해당 어카운트에 대해 범용 PLR 모드가 활성화되도록 요청하십시오.

PLR 모드로 전환하고 범용 라이선스 적용

스마트 어카운트가 범용 라이선스를 제공할 수 있는지 확인, 101 페이지에 설명된 것처럼 영구 라이선스를 받을 수 있는지 확인하고, 필요한 범용 라이선스를 구매한 후에는 영구 라이선스 예약(PLR) 모드로 전환하고 라이선스를 적용할 수 있습니다.

주의 현재 평가 모드에 있는 경우 PLR 모드로 전환하면 다시 평가 모드로 전환할 수 없습니다.

시작하기 전에

디바이스가 고가용성으로 구성된 경우, HA 그룹의 두 디바이스에 대해 이 작업을 개별적으로 완료해야 합니다.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음 스마트 라이선스 요약에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

단계 **2** 스마트 라이선싱을 사용하여 디바이스를 이미 등록한 경우, 톱니바퀴 모양 드롭다운 목록에서 **Unregister Device(**디바이스 등록 해제**)**를 선택한 다음 등록 해제를 확인합니다. 계속 진행하려면 우선 등록 해제 작업이 완료될 때까지 기다려야 합니다.

단계 **3** 톱니바퀴 모양 드롭다운 목록에서 **Switch to Universal PLR(**범용 **PLR**로 전환**)**을 선택하여 범용 영구 라이선스 예약(PLR) 모드로 전환합니다.

경고 메시지를 읽고 **Yes(**예**)**를 클릭하여 전환을 확인합니다.

시스템이 PLR 모드로 변환된 다음 PLR 등록 프로세스가 시작됩니다.

단계 **4** PLR 등록을 완료합니다.

a) Universal Permanent License Reservation(범용 영구 라이선스 예약) 대화 상자가 열리면 첫 번째 단계에 사용자에게 필요한 요청 코드가 포함되어 있습니다. **Save As TXT(TXT**로 저장**)**를 클릭하여 이 코드를 텍스트 파일로 저장하거나, **Print(**인쇄**)**를 클릭하여 인쇄할 수 있습니다. 문자열을 강조 표시하고 Ctrl+C를 눌러 클립보드에 복사할 수도 있습니다.

모드 전환 후 프로세스를 취소한 경우, Licensing(라이선싱) 페이지의 **Continue Reservation(**예약 계속 진행**)** 버튼을 클릭하여 이 단계에서 다시 시작할 수 있습니다.

b) CSSM 어카운트에 로그인하고 **Smart Software Licensing(**스마트 소프트웨어 라이선싱**)** > **Inventory(**인벤토리**)** 페이지로 이동한 다음, **Licenses(**라이선스**)** 탭을 클릭합니다.

c) **License Reservation(**라이선스 예약**)** 버튼을 클릭하고 마법사의 지침을 따릅니다. 생성한 요청 코드를 입력하라는 메시지가 표시되며, 이렇게 하면 인증 코드가 제공됩니다.

마법사에는 다음 단계가 포함됩니다.

1. 라이선스 요청 코드를 입력하거나, 코드가 포함된 텍스트 파일을 업로드하고 **Next(**다음**)**를 클릭합니다.
2. 2단계에서는 라이선스를 부여하려는 시스템에 대한 제품 세부 정보, 그리고 사용 가능한 라이선스 목록이 표시됩니다. FDM에서 관리되는 threat defense 디바이스에 대한 범용 라이선스를 선택하고 **Next(**다음**)**를 클릭합니다.
3. 3단계에서는 올바른 라이선스를 선택했는지 확인했는지 확인하고 **Generate Authorization Code(**인증 코드 생성**)**를 클릭합니다.

4. 4단계에서는 인증 코드가 표시됩니다. **Download as File(**파일로 다운로드**)** 또는 **Copy to Clipboard(**클립보드에 복사**)**를 클릭하여 코드를 저장합니다.
5. **Close(**닫기**)**를 클릭하여 마법사를 종료합니다.

d) device manager으로 다시 돌아간 후, 인증 코드를 적절한 필드에 붙여넣습니다.

범용 라이선스에 대한 유효한 인증 코드 형식은 XXXXXX-XXXXXX-XXXXXX-XXXXXX-XXXXXX-XXXX입니다. 여기서 X는 영숫자 문자입니다. 인증 코드가 XML 파일인 경우, 특정 라이선스를 보유한 것이며 이 시스템에서는 사용할 수 없습니다. PLR 등록 취소, 103 페이지에 설명된 대로 등록을 취소하여 CSSM에서 예약된 라이선스를 해제하십시오. 그런 다음, Cisco 담당자와 협력하여 스마트 어카운트를 범용 PLR로 변환하십시오.

e) **Register(**등록**)**를 클릭합니다.

시스템에서 등록 프로세스를 시작합니다. Licensing(라이선싱) 페이지를 새로 고침하여 등록 상태를 확인합니다.

단계 **5** 필요에 따라 선택적인 기능 라이선스를 활성화합니다.

범용 라이선스는 Base 라이선스에 대해서만 디바이스를 등록합니다. 이제 필요한 각 기능 라이선스에 대해 **Enable(**활성화**)**을 클릭할 수 있습니다.

PLR 등록 취소

범용 영구 라이선스 예약(PLR) 요청이 완료되기 전에 이를 취소할 수 있습니다. 예를 들어 PLR 등록 프로세스를 시작한 후 Smart Software Manager 어카운트가 PLR에 설정되지 않은 것을 확인한 경우, PLR 모드에 대한 인증을 받고 스마트 라이선스 어카운트가 올바르게 설정될 때까지 이러한 등록 프로세스를 취소할 수 있습니다.

PLR 등록 프로세스를 완료한 경우에는 이를 취소할 수 없습니다. 대신 PLR 모드에서 디바이스 등록 해제, 104 페이지 섹션을 참조하십시오.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음 스마트 라이선스 요약에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

단계 **2** 톱니바퀴 모양 드롭다운 목록에서 **Cancel PLR(PLR** 취소**)**을 선택하여 취소 프로세스를 시작합니다.

단계 **3** 상황에 맞는 옵션을 선택합니다.

- **I have a license in CSSM(CSSM**에 라이선스가 있습니다**.)** — CSSM(Cisco Smart Software Manager)에서 라이선스 등록 마법사를 완료했고 인증 코드를 받은 경우 이 옵션을 사용합니다. 이 단계에서 CSSM에 예약된 라이선스가 있다면 해당 라이선스를 해제해야 합니다.

- **I do not have a license in CSSM(CSSM**에 라이선스가 없습니다**.)** — 인증 코드를 받은 시점에 CSSM 마법사를 완료하지 않은 경우 이 옵션을 사용합니다. 예를 들어, device manager에서 PLR 등록을 시작한 후 스마트 어카운트에서 **License Reservation(**라이선스 예약**)** 버튼이 제공되지 않는다는 걸 확인한 경우 이 옵션을 사용합니다.

단계 **4** (**I have a license in CSSM(CSSM**에 라이선스가 있습니다**.)**을 선택한 경우.) CSSM에서 해제 코드를 받아 라이선스가 더 이상 사용 중으로 표시되지 않도록 해야 합니다. 그러지 않으면 다른 디바이스에서 해당 라이선스를 사용할 수 없습니다.

a) 등록 시 CSSM에서 받은 인증 코드를 취소 대화 상자에 붙여넣고 **Generate Release Code(**해제 코드 생성**)**를 클릭합니다.

b) **Release License Code(**라이선스 코드 해제**)** 필드에 코드가 있을 경우, **Save As TXT(TXT**로 저장**)**를 클릭하여 이를 텍스트 파일로 저장하거나 **Print(**인쇄**)**를 클릭하여 인쇄합니다. 코드를 선택하고 Ctrl+C를 눌러 클립보드에 복사할 수도 있습니다.

c) CSSM의 **Smart Software Licensing(**스마트 소프트웨어 라이선싱**)** > **Inventory(**인벤토리**)** 페이지에서 디바이스(디바이스 일련 번호가 이름임)를 찾고, **Action(**작업**)** > **Remove(**제거**)**를 클릭한 후 해제 코드를 입력합니다.

CSSM에 제품이 제거되었다는 메시지가 표시될 때까지 기다립니다.

단계 **5** **OK(**확인**)**를 클릭하여 취소 프로세스를 완료합니다.

시스템이 스마트 라이선스 모드로 돌아갑니다. 그러나 디바이스는 등록 해제되어 평가 모드를 다시 시작할 수 없습니다. 이 단계에서는 스마트 라이선스를 사용하여 디바이스를 등록하거나, PLR 모드로 다시 전환한 후 다시 등록하여 사용해야 합니다.

PLR 모드에서 디바이스 등록 해제

예를 들어 디바이스를 디커미션하거나 별도로 라이선스를 부여하는 다른 시설로 디바이스를 옮기는 경우처럼 디바이스에 라이선스가 더 이상 필요하지 않은 경우, 디바이스를 등록 해제할 수 있습니다.

디바이스 등록을 해제하면 라이선스가 사용되지 않은 상태로 돌아갑니다. 디바이스를 등록 해제하지 않을 경우 라이선스가 계속 사용 중으로 표시되며 이를 다른 용도로 사용할 수 없습니다.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음 스마트 라이선스 요약에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

단계 **2** 톱니바퀴 모양 드롭다운 목록에서 **Unregister Universal PLR(**범용 **PLR** 등록 해제**)**을 선택한 후 경고 메시지를 읽고 **Yes(**예**)**를 클릭하여 프로세스를 시작합니다.

단계 **3** Unregister Universal Permanent License Reservation(범용 영구 라이선스 예약 등록 해제) 대화 상자가 열리면, **Release License Code(**라이선스 코드 해제**)** 필드에 CSSM 어카운트에 현재 할당된 라이선스를 해제해야 할 코드가 채워져 있습니다. **Save as TXT(TXT**로 저장**)** 또는 **Print(**인쇄**)**를 클릭하여 이 코드의 복사본을 보관합니다. 코드를 선택하고 Ctrl+C를 사용하여 클립보드에 복사할 수도 있습니다.

단계 **4** CSSM 어카운트로 이동하여 **Smart Software Licensing(**스마트 소프트웨어 라이선싱**)** > **Inventory(**인벤토리**)** 페이지에서 디바이스(디바이스 일련 번호가 이름임)를 찾고, **Action(**작업**)** > **Remove(**제거**)**를 클릭한 후 해제 코드를 입력합니다.

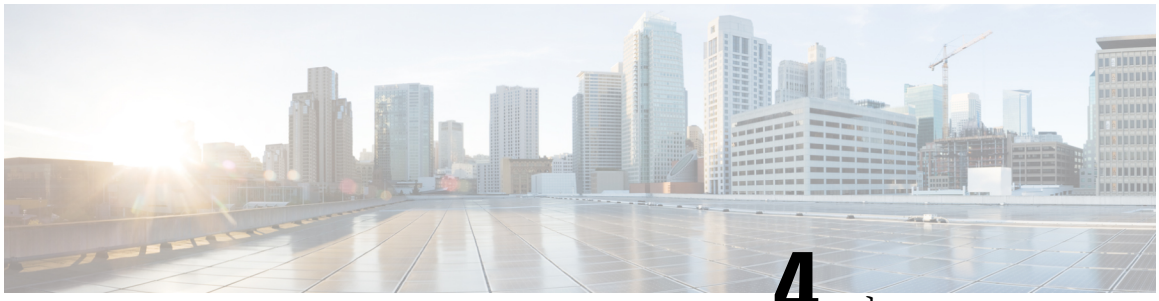
CSSM에 제품이 제거되었다는 메시지가 표시될 때까지 기다립니다.

단계 **5** device manager으로 돌아가 Unregister Device(디바이스 등록 해제)에서 **Unregister(**등록 해제**)**를 클릭합니다.

이렇게 하면 프로세스가 완료됩니다. 이제 CSSM의 라이선스를 다른 디바이스에 자유롭게 할당할 수 있으며, threat defense 디바이스에는 라이선스가 없습니다.

부

시스템 모니터링



4 장

디바이스 모니터링

시스템에는 디바이스 및 디바이스를 통과하는 트래픽을 모니터링하는 데 사용할 수 있는 대시보드와 이벤트 뷰어가 포함되어 있습니다.

트래픽 통계를 가져오도록 로깅 활성화

모니터링 대시보드 및 이벤트 뷰어를 사용하여 광범위한 트래픽 통계를 모니터링할 수 있습니다. 그러나 시스템에 수집할 통계를 지시하려면 로깅을 활성화해야 합니다. 시스템을 통과하는 연결을 파악할 수 있게 해주는 다양한 유형의 이벤트가 로깅을 통해 생성됩니다.

다음 주제에서는 특히 연결 로깅에 중점을 두어 로깅을 통해 제공되는 이벤트와 정보에 대해 자세히 설명합니다.

이벤트 유형

시스템은 다음 이벤트 유형을 생성할 수 있습니다. 모니터링 대시보드에서 관련된 통계를 확인하려면 이러한 이벤트를 생성해야 합니다.

연결 이벤트

사용자가 시스템을 통과하는 트래픽을 생성할 때 연결에 대한 이벤트를 생성할 수 있습니다. 액세스 규칙에서 연결 로깅을 활성화하여 이러한 이벤트를 생성합니다. 보안 인텔리전스 정책과 SSL 암호 해독 규칙에서 로깅을 활성화하여 연결 이벤트를 생성할 수도 있습니다.

연결 이벤트에는 소스/대상 IP 주소와 포트, 사용한 URL 및 애플리케이션, 전송된 바이트 또는 패킷의 수 등 연결에 대한 여러 가지 정보가 포함됩니다. 수행한 작업(예: 연결 허용 또는 차단) 및 연결에 적용된 정책도 이러한 정보에 포함됩니다.

침입 이벤트

시스템은 호스트 및 호스트 데이터의 가용성, 무결성 및 기밀성에 영향을 미칠 수 있는 악성 활동 탐지를 위해 네트워크를 통과하는 패킷을 검토합니다. 시스템은 침입 가능성을 식별하는 경우 익스플로잇의 날짜, 시간, 익스플로잇 유형, 그리고 공격 소스와 대상에 관한 상황 정보의 레코드인 침입 이벤트를 생성합니다. 침입 이벤트는 호출하는 액세스 제어 규칙의 로깅 컨피그레이션과 관계없이 차단하거나 알리도록 설정된 모든 침입 규칙에 대해 생성됩니다.

파일 이벤트

파일 이벤트는 파일 정책을 기준으로 하여 시스템이 네트워크 트래픽에서 탐지하고 선택적으로 차단한 파일을 나타냅니다. 이러한 이벤트를 생성하려면 파일 정책을 적용하는 액세스 규칙에 대해 파일 로깅을 활성화해야 합니다.

시스템이 파일 이벤트를 생성하는 경우 호출하는 액세스 제어 규칙의 로깅 컨피그레이션과 관계없이 시스템은 관련 연결의 종료도 로깅합니다.

악성코드 이벤트

시스템은 전체적인 액세스 제어 컨피그레이션의 일부로 네트워크 트래픽에서 악성코드를 탐지할 수 있습니다. 악성코드 대응 는 결과 이벤트의 상태와 악성코드가 탐지된 방법, 위치, 시간에 대한 상황 데이터를 포함하는 악성코드 이벤트를 생성할 수 있습니다. 이러한 이벤트를 생성하려면 파일 정책을 적용하는 액세스 규칙에 대해 파일 로깅을 활성화해야 합니다.

파일 상태는 변경될 수 있습니다(예: 정상에서 악성코드로 또는 악성코드에서 정상으로). 악성코드 대응 가 Secure Malware Analytics Cloud에 파일에 대해 쿼리하고, 쿼리한지 일주일 이내에 상태가 변경되었음을 클라우드에서 확인하는 경우, 시스템에서는 회귀적 악성코드 이벤트를 생성합니다.

보안 인텔리전스 이벤트

보안 인텔리전스 이벤트는 정책에 따라 차단되거나 또는 모니터링된 각 연결의 보안 인텔리전스 정책에 의해 생성된 연결 이벤트 유형입니다. 모든 보안 인텔리전스 이벤트에는 내용이 채워진 Security Intelligence Category(보안 인텔리전스 카테고리) 필드가 있습니다.

이러한 각 이벤트에는 해당하는 "일반" 연결 이벤트가 있습니다. 보안 인텔리전스 정책은 액세스 제어를 비롯한 다른 많은 보안 정책보다 먼저 평가되기 때문에 보안 인텔리전스에 의해 연결이 차단된 경우, 그 결과로 생성된 이벤트에는 시스템이 후속 평가를 통해 수집했을 수 있는 정보(예: 사용자 ID)가 포함되지 않습니다.

구성 가능한 연결 로깅

조직의 보안 및 규정 준수 필요에 따라 연결을 로깅해야 합니다. 사용자가 생성하고 기능을 향상시키는 이벤트의 수를 제한하는 것이 사용자의 목표라면 사용자의 분석에 중요한 연결에 대한 로깅만 사용 설정합니다. 그러나, 자료 수집을 목적으로 사용자의 네트워크 트래픽에 대한 광범위한 견해를 원할 경우, 추가 연결에 대한 로깅을 사용 설정할 수 있습니다.

시스템은 여러 가지 이유로 연결을 로깅할 수 있으므로, 한 곳의 로깅을 비활성화해도 일치하는 연결이 로깅되지 않는 것은 아닙니다.

다음 위치에서 연결 로깅을 구성할 수 있습니다.

- 액세스 제어 규칙 및 기본 작업 — 연결 종료 시 수행되는 로깅은 연결에 대한 대부분의 정보를 제공합니다. 연결 시작 시에 로깅을 수행할 수도 있지만 이러한 이벤트에 포함되는 정보는 불완전합니다. 연결 로깅은 기본적으로 비활성화되므로 추적하려는 트래픽을 대상으로 하는 각 규칙과 기본 작업에 대해 연결 로깅을 활성화해야 합니다.
- 보안 인텔리전스 정책 — 각 차단된 연결에 대한 보안 인텔리전스 연결 이벤트를 생성하도록 로깅을 활성화할 수 있습니다. 보안 인텔리전스 필터링의 결과로 시스템이 연결 이벤트를 로깅할 때 시스템은 또한 일치하는 보안 인텔리전스 이벤트도 로깅합니다. 이는 사용자가 별도로 살펴보고 분석할 수 있는 특수한 연결 이벤트입니다.
- SSL 암호 해독 규칙 및 기본 작업 — 연결 종료 시 수행되는 로깅을 구성할 수 있습니다. 차단된 연결의 경우 시스템에서 즉시 세션을 종료하고 이벤트를 생성합니다. 모니터링된 연결 및 액세스 제어 규칙으로 전달하는 연결의 경우 시스템에서 세션 종료 시 이벤트를 생성합니다.

자동 연결 로깅

시스템은 다른 로깅 컨피그레이션과 관계없이 다음의 연결 종료 이벤트를 자동으로 저장합니다.

- 시스템은 연결이 액세스 제어 정책의 기본 작업에 의해 처리되지 않는 한, 침입 이벤트와 연관된 연결을 자동으로 로깅합니다. 일치하는 트래픽에 대한 침입 이벤트를 얻으려면 기본 작업에서 로깅을 활성화해야 합니다.
- 시스템은 파일 및 악성코드 이벤트와 연관된 연결을 자동으로 로깅합니다. 이는 연결 이벤트만을 위한 작업입니다. 선택적으로 파일 및 악성코드 이벤트의 생성을 비활성화할 수 있습니다.

연결 로깅에 대한 팁

로깅 컨피그레이션 및 관련 통계 평가를 고려할 때는 다음 사항에 유의하십시오.

- 사용자가 액세스 제어 규칙을 통해 트래픽을 허용할 때, 연결된 침입 또는 파일 정책을 (또는 둘 다를) 사용하여 트래픽이 최종 목적지에 도달하기 전에 트래픽 및 침입 차단, 금지된 파일과 악성코드를 자세히 검사할 수 있습니다. 하지만. 기본 파일 및 침입에 의해 암호화된 페이로드를 위한 탐지가 사용 해제되었음을 참고하시기 바랍니다. 침입 또는 파일 정책이 연결을 차단해야 하는 이유를 확인하는 경우, 시스템은 연결 로그 설정과 관계없이 연결 종료 이벤트를 즉시 로깅합니다. 로깅이 허용되는 연결은 네트워크의 트래픽에 대해 가장 많은 통계 정보를 제공합니다.
- 신뢰할 수 있는 연결이란 액세스 제어 정책에서 신뢰 액세스 제어 규칙 또는 기본 작업이 처리한 것입니다. 그러나 신뢰할 수 있는 연결에서는 검색 데이터, 침입 또는 금지된 파일과 악성코드를 검사하지 않습니다. 따라서, 신뢰할 수 있는 연결에 대한 연결 이벤트는 제한된 정보를 포함합니다.
- 트래픽을 차단하는 액세스 제어 규칙 및 액세스 제어 정책 기본 작업의 경우 시스템은 연결 시작 이벤트를 로깅합니다. 일치하는 트래픽은 추가 검사 없이 거부됩니다.
- DoS(서비스 거부) 공격 중에 차단된 TCP 연결을 로깅하는 경우 시스템 성능에 영향을 미칠 수 있으며, 데이터베이스가 유사한 다수의 이벤트로 가득 찰 수 있습니다. 차단 규칙에 대한 로깅을

활성화하기 전에 이 규칙이 인터넷 연결 인터페이스 또는 DoS 공격에 취약한 다른 인터페이스의 트래픽을 모니터링하는지 여부를 고려하십시오.

- 원격 액세스 VPN 연결 프로파일을 컨피그레이션하거나 **sysopt connection permit-vpn** 명령을 활성화할 때 **Bypass Access Control policy for decrypted traffic(**암호 해독 트래픽에 대한 액세스 제어 우회 정책**)(sysopt permit-vpn)** 옵션을 선택하면 모든 Site-to-Site 또는 원격 액세스 VPN 트래픽이 검사 및 액세스 제어 정책을 우회합니다. 따라서 이 트래픽에 대한 연결 이벤트를 가져오지 못하고, 트래픽은 어떤 통계 대시보드에도 반영되지 않습니다.

외부 **syslog** 서버에 이벤트 전송

device manager(이벤트를 저장하는 기능은 제한되어 있음)를 통해 이벤트를 확인하는 것 외에도 규칙과 정책을 선택적으로 구성하여 이벤트를 외부 시스템 로그 서버에 전송할 수 있습니다. 그러면 선택한 syslog 서버 플랫폼의 추가 스토리지 및 기능을 사용하여 이벤트 데이터를 확인하고 분석할 수 있습니다.

외부 syslog 서버에 이벤트를 전송하려면 각 연결 로깅을 활성화하는 규칙, 기본 작업 또는 정책을 편집하고 로그 설정에서 syslog 서버 개체를 선택합니다. syslog 서버에 침입 이벤트를 전송하려면 침입 정책 설정에서 서버를 컨피그레이션하십시오. syslog 서버에 파일/악성코드 이벤트를 전송하려면 **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Logging Settings(**기록 설정**)**에서 서버를 컨피그레이션하십시오.

자세한 내용은 각 규칙 및 정책 유형에 대한 도움말과 syslog 서버 구성, 157 페이지의 내용을 참조하십시오.

SecureX Threat Response와 같은 **Cisco Cloud** 기반 서비스를 사용하여 이벤트 평가

Event Viewer 및 자체 syslog 서버를 사용하는 것 외에도 연결 이벤트 및 높은 우선순위 침입, 파일 및 악성코드 이벤트를 Cisco Cloud 기반 서버에 전송할 수 있습니다. SecureX threat response(이전 Cisco Threat Response)와 같은 Cisco Cloud 기반 서비스는 해당 클라우드 서버에서 이벤트를 끌어올 수 있으며, 해당 서비스를 사용하여 이러한 이벤트를 평가할 수 있습니다.

이러한 클라우드 기반 서비스는 threat defense 및 device manager과 별개입니다. 이러한 이벤트를 Cisco Cloud로 전송하도록 요구하는 서비스를 사용하도록 선택하는 경우, **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Cloud Services(**클라우드 서비스**)** 페이지에서 연결을 활성화해야 합니다. Cisco Cloud로 이벤트 전송, 841 페이지를 참조하십시오.

미국 지역의 경우 https://visibility.amp.cisco.com/에서, EU 지역의 경우에는 https://visibility.eu.amp.cisco.com에서, SecureX threat response에 연결할 수 있습니다. http://cs.co/CTRvideos에서 YouTube를 통해 애플리케이션의 용도와 이점에 대한 비디오를 볼 수 있습니다. SecureX threat response와 함께 threat defense를 사용하는 방법에 대한 자세한 내용은 *Cisco Secure Firewall Threat Defense* 및 *SecureX threat* 통합 가이드(https://www.cisco.com/c/en/us/support/security/defense-center/products-installation-and-configuration-guides-list.html에서 확인 가능)를 참조하십시오.

트래픽 및 시스템 대시보드 모니터링

시스템에는 디바이스를 통과하는 트래픽과 보안 정책의 결과를 분석하는 데 사용할 수 있는 여러 대시보드가 포함되어 있습니다. 대시보드의 정보를 사용하여 컨피그레이션의 전반적인 효율성을 평가하고 네트워크 문제를 식별 및 해결합니다.

고가용성 그룹의 유닛용 대시보드에는 해당 디바이스에 대한 통계만 표시됩니다. 통계는 유닛 간에 동기화되지 않습니다.

참고 트래픽 관련 대시보드에서 사용되는 데이터는 연결 또는 파일 로깅을 활성화하는 액세스 제어 규칙 및 로깅을 허용하는 기타 보안 정책에서 수집됩니다. 로깅이 활성화되어 있지 않은 규칙과 일치하는 트래픽은 대시보드에 반영되지 않습니다. 따라서 중요한 정보를 로깅하도록 규칙을 구성해야 합니다. 또한, 사용자 정보는 사용자 ID를 수집하는 ID 규칙을 구성한 경우에만 사용할 수 있습니다. 그리고 마지막으로 침입, 파일, 악성코드 및 URL 카테고리 정보는 해당 기능용 라이선스가 있고 이러한 기능을 사용하는 규칙을 구성하는 경우에만 사용할 수 있습니다.

프로시저

단계 **1** 주 메뉴에서 **Monitoring(**모니터링**)**을 클릭하여 대시보드 페이지를 엽니다.

지난 1시간, 지난 주 등의 사전 정의된 시간 범위를 선택하거나, 특정 시작 시간과 종료 시간을 사용해 맞춤형 시간 범위를 정의하여 대시보드 그래프와 테이블에 표시되는 데이터를 제어할 수 있습니다.

트래픽 관련 대시보드는 다음과 같은 유형으로 표시됩니다.

- 상위 5개 막대 그래프 - 이러한 그래프는 네트워크 개요 대시보드에 표시되며 대시보드 테이블에서 항목을 클릭하면 나타나는 항목별 요약에도 표시됩니다. 표시되는 정보를 트랜잭션 개수 또는 데이터 사용량(전송 및 수신된 총 바이트 수) 간을 전환할 수 있습니다. 모든 트랜잭션, 허용된 트랜잭션 또는 거부된 트랜잭션이 나타나도록 화면표시를 전환할 수도 있습니다. 더 보기 링크를 클릭하면 그래프와 연결된 테이블이 표시됩니다.
- 테이블 - 테이블에는 특정 유형(예: 애플리케이션 또는 URL 카테고리)의 항목과 해당 항목의 총 트랜잭션, 허용된 트랜잭션, 차단된 트랜잭션, 데이터 사용량, 전송/수신된 바이트 수가 표시됩니다. 표시되는 숫자를 원시 값과 백분율 간을 전환할 수 있으며 상위 10개, 100개, 1000개 항목을 표시할 수 있습니다. 항목이 링크인 경우 링크를 클릭하면 더욱 자세한 정보가 포함된 요약 대시보드를 확인할 수 있습니다.

단계 **2** 목차에서 대시보드 링크를 클릭하여 다음 데이터에 대한 대시보드를 표시합니다.

- **Network Overview(**네트워크 개요**)** - 네트워크의 트래픽에 대한 요약 정보가 표시됩니다. 이러한 정보에는 일치한 액세스 규칙(정책), 트래픽을 생성한 사용자, 연결에 사용된 애플리케이션, 일치한 침입 위협(서명), 액세스한 URL의 URL 카테고리, 연결에서 가장 많이 사용된 대상이 포함됩니다.

- **Users(**사용자**)** - 네트워크를 많이 사용한 사용자가 표시됩니다. 사용자 정보를 확인하려면 ID 정책을 구성해야 합니다. 사용자 ID가 없는 경우, 소스 IP 주소가 포함되어 있습니다. 다음과 같은 특수 엔티티가 표시될 수 있습니다.
  - **Failed Authentication(**실패한 인증**)** - 사용자에게 인증하라는 메시지가 표시되었는데 사용자가 허용되는 최대 횟수 이내에 유효한 사용자 이름/비밀번호 쌍을 입력하지 못했습니다. 인증에 실패해도 사용자의 네트워크 액세스가 차단되지는 않지만, 이러한 사용자의 네트워크 액세스를 제한하는 액세스 규칙을 작성할 수 있습니다.
  - **Guest(**게스트**)** - 게스트 사용자는 ID 규칙이 이러한 사용자를 게스트로 지칭하도록 구성된다는 점을 제외하면 실패한 인증 사용자와 비슷합니다. 즉, 게스트 사용자 역시 인증하라는 메시지가 표시되었지만, 최대 시도 횟수 이내에 인증하지 못한 사용자입니다.
  - **No Authentication Required(**인증 필요 없음**)** - 사용자의 연결이 인증을 지정하지 않은 ID 규칙과 일치하여 인증하라는 메시지가 표시되지 않았습니다.
  - **Unknown(**알 수 없음**)** - IP 주소에 대한 사용자 매핑이 없으며 아직 실패한 인증 기록이 없습니다. 이는 일반적으로 해당 주소에서 HTTP 트래픽이 아직 전송되지 않았음을 의미합니다.
- **Applications(**애플리케이션**)** - 네트워크에서 가장 많이 사용되는 애플리케이션(예: HTTP)이 표시됩니다. 검사된 연결에 대해서만 정보가 제공됩니다. 영역, 주소 및 포트 이외의 기준을 사용하는 차단 규칙이나 "허용" 규칙과 일치하는 연결을 검사합니다. 따라서 검사를 요구하는 규칙에 적중하기 전에 연결이 신뢰 또는 차단되면 애플리케이션 정보가 제공되지 않습니다.
- **Web Applications(**웹 애플리케이션**)** - 네트워크에서 가장 많이 사용되는 애플리케이션(예: Google)이 표시됩니다. 웹 애플리케이션 정보 수집에 필요한 조건은 Application(애플리케이션) 대시보드의 조건과 동일합니다.
- **URL Categories(URL** 카테고리**)** - 방문한 웹 사이트의 분류를 기반으로 네트워크에서 많이 사용되는 웹 사이트 카테고리(예: Gambling(도박) 또는 Educational Institutions(교육 기관))가 표시됩니다. 이 정보를 얻으려면 트래픽 일치 기준으로 URL 카테고리를 사용하는 액세스 제어 규칙이 하나 이상 있어야 합니다. 규칙과 일치하는 트래픽 또는 규칙과 일치하는지를 확인하기 위해 검사해야 하는 트래픽에 대한 정보가 제공됩니다. 첫 번째 웹 범주 액세스 제어 규칙 앞에 오는 규칙과 일치하는 연결에 대해서는 범주 또는 평판 정보가 표시되지 않습니다.
- **Access and SI Rules(**액세스 및 **SI** 규칙**)** - 네트워크 트래픽과 가장 많이 일치하는 액세스 규칙 및 보안 인텔리전스 규칙에 상응하는 규칙이 표시됩니다.
- **Zones(**영역**)** - 트래픽이 디바이스로 들어왔다가 나가는 데 가장 많이 사용되는 보안 영역 쌍이 표시됩니다.
- **Destinations(**목적지**)** - 네트워크 트래픽에서 가장 많이 사용하는 목적지를 표시합니다.
- **Attackers(**공격자**)** - 침입 이벤트를 트리거하는 연결의 소스인 상위 공격자를 표시합니다. 이 정보를 보려면 액세스 규칙에 대한 침입 정책을 구성해야 합니다.
- **Targets(**대상**)** - 공격의 피해자인 침입 이벤트의 상위 대상을 표시합니다. 이 정보를 보려면 액세스 규칙에 대한 침입 정책을 구성해야 합니다.
- **Threats(**위협**)** - 가장 많이 트리거된 침입 규칙을 표시합니다. 이 정보를 보려면 액세스 규칙에 대한 침입 정책을 구성해야 합니다.

- **File Logs(**파일 로그**)** - 네트워크 트래픽에서 가장 많이 확인된 파일 유형을 표시합니다. 이 정보를 보려면 액세스 규칙에 대한 파일 정책을 구성해야 합니다.
- **Malware(**악성코드**)** - 가장 많이 사용되는 악성코드 작업 및 상태의 조합이 표시됩니다. 드릴다운하여 연결된 파일 유형에 대한 정보를 확인할 수 있습니다. 이 정보를 보려면 액세스 규칙에 대한 파일 정책을 구성해야 합니다.
  - 가능한 작업: 악성코드 클라우드 조회, 차단, 아카이브 차단(암호화), 탐지, 맞춤형 탐지, 클라우드 조회 시간 제한, 악성코드 차단, 아카이브 차단(깊이 초과), 맞춤형 탐지 차단, TID 차단, 아카이브 차단(검사 실패)
  - 가능한 상태: 악성코드, 알 수 없음, 정상, 맞춤형 탐지, 사용할 수 없음
- **SSL Decryption(SSL** 암호 해독**)** - 디바이스를 통과하는 암호화된 트래픽과 일반 텍스트 트래픽의 비교 내용이 표시됩니다. 또한, 암호화된 트래픽이 SSL 암호 해독 규칙에 따라 암호 해독된 방식에 대한 분석 내용도 표시됩니다.
- **System(**시스템**)** - 인터페이스 및 해당 상태(인터페이스 위에 마우스를 올려놓으면 해당 IP 주소가 표시됨), 전반적인 평균 시스템 처리량(최대 1시간 동안 5분의 버킷 기준 및 더 긴 기간 동안 1시간의 버킷 기준), 시스템 이벤트/CPU 사용량/메모리 사용량/디스크 사용량에 관한 요약 정보를 비롯한 전체 시스템 보기가 표시됩니다. 모든 인터페이스가 아닌 특정 인터페이스만 표시하도록 성능 그래프를 제한할 수 있습니다.

  참고 시스템 대시보드에 표시되는 정보는 전체 시스템 레벨의 정보입니다. 디바이스 CLI에 로그인하면 다양한 명령을 사용하여 더욱 자세한 정보를 확인할 수 있습니다. 예를 들어 **show cpu** 및 **show memory** 명령에는 기타 세부 정보를 표시하기 위한 파라미터가 포함된 반면, 이 대시보드에서는 **show cpu system** 및 **show memory system** 명령에서 제공하는 데이터를 표시합니다.

단계 **3** 목차에서 이러한 링크를 클릭할 수도 있습니다.

- **Events(**이벤트**)** - 발생하는 이벤트를 확인할 수 있습니다. 개별 액세스 규칙에서 연결 로깅을 활성화해야 해당 규칙과 관련된 연결 이벤트를 확인할 수 있습니다. 또한, 보안 인텔리전스 정책 및 SSL 암호 해독 규칙에서 로깅을 활성화하여 보안 인텔리전스 이벤트와 추가 연결 이벤트 데이터를 확인합니다. 이러한 이벤트를 확인하면 사용자의 연결 문제를 쉽게 해결할 수 있습니다.
- **Sessions(**세션**)** - device manager 사용자 세션을 보고 관리할 수 있습니다. 자세한 내용은 Device Manager 사용자 세션 관리, 882 페이지를 참고하십시오.

커맨드 라인을 사용하여 추가 통계 모니터링

device manager 대시보드에서는 디바이스를 통과하는 트래픽 및 일반 시스템 사용량과 관련된 다양한 통계를 제공합니다. 그러나 CLI 콘솔을 사용하거나 디바이스 CLI에 로그인하면 대시보드에서 통계를 제공하지 않는 영역에 대한 추가 정보를 확인할 수 있습니다(CLI(Command Line Interface) 로그인, 6 페이지 참조).

CLI에는 이러한 통계를 제공하는 다양한 **show** 명령이 포함되어 있습니다. **ping**, **traceroute** 같은 명령을 포함해 일반적인 문제해결을 위한 CLI를 사용할 수도 있습니다. 대부분의 **show** 명령에는 통계를 0으로 재설정하기 위해 함께 사용할 수 있는 **clear** 명령이 있습니다. CLI 콘솔에서는 통계를 지울 수 없습니다.

명령에 대한 문서는 Cisco Firepower Threat Defense 명령 참조, http://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.html에서 찾을 수 있습니다.

일반적으로 유용하게 활용할 수 있는 명령의 예는 다음과 같습니다.

- **show nat** NAT 규칙의 적중 횟수를 표시합니다.
- **show xlate** 활성 상태인 활성 NAT 변환을 표시합니다.
- **show conn** 디바이스를 통과하는 현재 연결에 대한 정보를 제공합니다.
- **show dhcpd** 인터페이스에 대해 구성하는 DHCP 서버에 대한 정보를 제공합니다.
- **show interface** 각 인터페이스의 사용량 통계를 제공합니다.

이벤트 보기

로깅을 활성화하는 보안 정책에서 생성된 이벤트를 확인할 수 있습니다. 트리거된 침입 및 파일 정책에 대해서도 이벤트가 생성됩니다.

이벤트 뷰어 테이블에는 생성되는 이벤트가 실시간으로 표시됩니다. 새 이벤트가 생성되면 이전 이벤트는 테이블에 표시되지 않게 됩니다.

시작하기 전에

특정 유형의 이벤트가 생성되는지 여부는 관련 정책과 일치하는 연결 외에 다음 사항에 따라서도 달라집니다.

- 연결 이벤트 - 액세스 규칙이 연결 로깅을 활성화해야 합니다. 보안 인텔리전스 정책과 SSL 암호해독 규칙에서 연결 로깅을 활성화할 수도 있습니다.
- 침입 이벤트 - 액세스 규칙이 침입 정책을 적용해야 합니다.
- 파일 및 악성코드 이벤트 - 액세스 규칙이 파일 정책을 적용하고 파일 로깅을 활성화해야 합니다.
- 보안 인텔리전스 이벤트 - 보안 인텔리전스 정책을 활성화 및 구성하고 로깅을 활성화해야 합니다.

프로시저

단계 **1** 주 메뉴에서 **Monitoring(**모니터링**)**을 클릭합니다.

단계 **2** 목차에서 **Events(**이벤트**)**를 선택합니다.

이벤트 뷰어에서는 탭의 이벤트가 이벤트 유형을 기준으로 구성됩니다. 자세한 내용은 이벤트 유형, 109 페이지를 참고하십시오.

단계 **3** 보려는 이벤트의 유형이 표시된 탭을 클릭합니다.

이벤트 목록을 사용하여 다음 작업을 수행할 수 있습니다.

- 이벤트를 보다 쉽게 찾고 분석할 수 있도록 새 이벤트 추가를 중지하려면 **Pause(**일시정지**)**를 클릭합니다. 새 이벤트가 표시되도록 하려면 **Resume(**재시작**)**를 클릭합니다.
- 새 이벤트가 표시되는 속도를 제어하려면 여러 새로고침 속도(5초, 10초, 20초, 60초) 중에서 선택합니다.
- 원하는 열이 포함된 맞춤형 보기를 생성합니다. 맞춤형 보기를 생성하려면 탭 막대에서 + 버튼을 클릭하거나 **Add/Remove Columns(**열 추가/제거**)**를 클릭합니다. 사전 설정된 탭은 변경할 수 없으므로 열을 추가하거나 제거하면 새 보기가 생성됩니다. 자세한 내용은 맞춤형 보기 구성, 118 페이지를 참고하십시오.
- 열의 폭을 변경하려면 열 제목 구분선을 클릭하여 원하는 폭으로 끌어옵니다.
- 이벤트 위에 마우스를 올려 놓고 **View Details(**세부정보 보기**)**를 클릭하면 이벤트에 대한 전체 정보를 확인할 수 있습니다. 이벤트 내의 여러 필드에 대한 설명은 이벤트 필드 설명, 120 페이지를 참조하십시오.

단계 **4** 필요한 경우 다양한 이벤트 속성에 따라 원하는 이벤트를 쉽게 찾을 수 있도록 테이블에 필터를 적용합니다.

새 필터를 생성하려면 드롭다운 목록에서 원자성 요소를 선택하고 필터 값을 입력하여 필터를 수동으로 입력하거나, 필터링할 값이 포함된 이벤트 테이블에서 셀 하나를 클릭하여 필터를 작성합니다. 같은 열의 여러 셀을 클릭하여 값 간의 OR 조건을 생성할 수도 있고, 서로 다른 열의 셀을 클릭하여 열 간의 AND 조건을 생성할 수도 있습니다. 셀을 클릭하여 필터를 작성하는 경우에는 결과로 생성되는 필터를 수정하여 미세 조정할 수 있습니다. 필터 규칙 생성에 대한 자세한 내용은 이벤트 필터링, 118 페이지를 참조하십시오.

필터를 작성한 후에는 다음 중에서 원하는 작업을 수행합니다.

- 필터를 적용하고 필터와 일치하는 이벤트만 표시되도록 테이블을 업데이트하려면 **Filter(**필터**)** 버튼을 클릭합니다.
- 적용한 전체 필터를 지우고 테이블을 필터링되지 않은 상태로 되돌리려면 **Filter(**필터**)** 상자에서 **Reset Filters(**필터 재설정**)**를 클릭합니다.
- 필터의 원자성 요소 중 하나를 지우려면 해당 요소 위에 마우스를 올려 놓고 요소에 대해 표시되는 **X**를 클릭합니다. 그런 다음 **Filter(**필터**)** 버튼을 클릭합니다.

맞춤형 보기 구성

이벤트를 확인할 때 원하는 열을 쉽게 볼 수 있도록 맞춤형 보기를 생성할 수 있습니다. 맞춤형 보기는 수정하거나 삭제할 수도 있습니다. 사전 정의된 보기는 수정하거나 삭제할 수 없습니다.

프로시저

단계 **1** **Monitoring(**모니터링**)** > **Events(**이벤트**)**를 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 기존 맞춤형 보기 또는 사전 정의된 보기를 기준으로 새 보기를 생성하려면 보기의 탭을 클릭하고 탭 왼쪽에 있는 **+** 버튼을 클릭합니다.
- 기존 맞춤형 보기를 수정하려면, 보기의 탭을 클릭합니다.

참고 맞춤형 보기를 삭제하려는 경우에는 보기 탭에서 **X** 버튼만 클릭하면 됩니다. 삭제는 취소할 수 없습니다.

단계 **3** 오른쪽의 이벤트 테이블 위에 있는 열 추가/제거 링크를 클릭한 다음, 보기에 포함하려는 열만 선택한 목록에 포함될 때까지 열을 선택하거나 선택을 취소합니다.

열을 클릭한 다음 끌어서 사용할 수 있지만 사용하지 않은 목록과 선택한 목록 간을 이동합니다. 선택한 목록에서 열을 클릭하고 끌어서 테이블 내의 열 순서(왼쪽에서 오른쪽)를 변경할 수도 있습니다. 열에 대한 설명은 이벤트 필드 설명, 120 페이지를 참조하십시오.

작업을 완료한 후 **OK(**확인**)**를 클릭하여 열 변경 사항을 저장합니다.

참고 사전 정의된 보기가 표시된 상태에서 열 선택을 변경하면 새 보기가 생성됩니다.

단계 **4** 필요한 경우 열 구분 기호를 클릭하고 끌어서 열 너비를 변경합니다.

이벤트 필터링

이벤트 테이블에 현재 확인하고자 하는 이벤트만 표시되도록 제한하는 복잡한 필터를 생성할 수 있습니다. 다음과 같은 기술을 단독으로 사용하거나 조합하여 필터를 작성할 수 있습니다.

열 클릭

필터를 작성하는 가장 쉬운 방법은 필터링할 값이 포함된 이벤트 테이블의 셀을 클릭하는 것입니다. 셀을 클릭하면 해당 값 및 필드 조합에 대해 올바르게 작성된 규칙을 사용하여 필터 필드가 업데이트됩니다. 그러나 이 기술을 사용하려면 기존 이벤트 목록에 원하는 값이 포함되어 있어야 합니다.

모든 열을 필터링할 수는 없습니다. 셀의 콘텐츠를 필터링할 수 있는 경우 해당 셀 위에 마우스를 올려놓으면 셀에 밑줄이 표시됩니다.

원자성 요소 선택

필터 필드를 클릭하고 드롭다운 목록에서 원하는 원자성 요소를 선택한 다음 일치 값을 입력하여 필터를 작성할 수도 있습니다. 이러한 요소는 이벤트 테이블에 열로 표시되지 않는 이벤트 필드를 포함합니다. 또한 입력하는 값과 표시할 이벤트 간의 관계를 정의하는 연산자도 포함합니다. 열을 클릭할 때는 항상 "같음(=)" 필터가 적용되는 반면 요소를 선택할 때는 숫자 필드에 대해 "보다 큼(>)" 또는 "보다 작음(<)"도 선택할 수 있습니다.

Filter(필터**)** 필드에 요소를 추가하는 방법과 관계없이 필드에 값을 입력하여 연산자나 값을 조정할 수 있습니다. 테이블에 필터를 적용하려면 필터를 클릭합니다.

이벤트 필터용 연산자

이벤트 필터에서는 다음 연산자를 사용할 수 있습니다.

=	같음. 이벤트가 지정된 값과 일치합니다. 와일드카드는 사용할 수 없습니다.
!=	같지 않음. 이벤트가 지정된 값과 일치하지 않습니다. 같지 않음 식을 작성하려면 !(느낌표)를 입력해야 합니다.
>	보다 큼. 이벤트에 지정된 값보다 큰 값이 포함되어 있습니다. 이 연산자는 포트 및 IP 주소와 같은 숫자 값에만 사용할 수 있습니다.
<	보다 작음. 이벤트에 지정된 값보다 작은 값이 포함되어 있습니다. 이 연산자는 숫자 값에만 사용할 수 있습니다.

복잡한 이벤트 필터에 대한 규칙

여러 원자성 요소가 포함된 복잡한 필터를 작성할 때는 다음 규칙에 주의하십시오.

- 유형이 같은 요소의 경우 해당 유형의 모든 값 간에 OR 관계가 설정됩니다. 예를 들어 이니시에이터 IP=10.100.10.10 및 이니시에이터 IP=10.100.10.11을 포함하는 경우 트래픽 소스로 이러한 주소 중 하나를 포함하는 이벤트가 일치 항목으로 표시됩니다.
- 유형이 다른 요소의 경우 AND 관계가 설정됩니다. 예를 들어 이니시에이터 IP=10.100.10.10 및 대상 포트/ICMP 유형=80을 포함하는 경우 이 소스 주소와 대상 포트를 모두 포함하는 이벤트만 일치 항목으로 표시됩니다. 10.100.10.10에서 다른 대상 포트로 향하는 이벤트는 표시되지 않습니다.
- IPv4 및 IPv6 주소를 포함한 숫자 요소의 경우 범위를 지정할 수 있습니다. 예를 들어 대상 포트=50-80을 지정하여 해당 범위 내의 포트에 대한 모든 트래픽을 캡처할 수 있습니다. 하이픈을 사용하여 시작 숫자와 종료 숫자를 분리합니다. 모든 숫자 필드에 범위를 사용할 수 있는 것은 아닙니다. 예를 들어 소스 요소에서는 IP 주소 범위를 지정할 수 없습니다.
- 와일드카드나 정규식은 사용할 수 없습니다.

이벤트 필드 설명

이벤트는 다음 정보를 포함할 수 있습니다. 이벤트 세부사항을 볼 때 이 정보를 확인할 수 있습니다. 이벤트 뷰어 테이블에 열을 추가하여 가장 관심이 높은 정보를 표시할 수도 있습니다.

아래에는 사용 가능한 필드의 전체 목록이 나와 있습니다. 모든 이벤트 유형에 모든 필드가 적용되는 것은 아닙니다. 개별 이벤트에 사용 가능한 정보는 시스템에서 연결을 로깅한 방법, 이유 및 시기에 따라 달라질 수 있습니다.

작업

연결 또는 보안 인텔리전스 이벤트의 경우 연결이 기록된 기본 작업 또는 액세스 제어 규칙과 관련된 작업은 다음과 같습니다.

허용

명시적으로 허용된 연결

신임

신뢰할 수 있는 연결. 첫 번째 패킷의 신뢰 규칙에 의해 탐지된 TCP 연결은 연결 종료 이벤트만 생성합니다. 시스템에서는 최종 세션 패킷이 끝난 지 한 시간 후에 이벤트를 생성합니다.

차단

차단된 연결. 다음 상황에서 차단 작업을 허용 액세스 규칙과 연결할 수 있습니다.

- 침입 정책에 따라 익스플로잇이 차단된 연결
- 파일 정책에 따라 파일이 차단된 연결
- 보안 인텔리전스에 의해 차단된 연결.
- SSL 정책에 따라 차단된 연결

기본 작업

연결이 기본 작업에 의해 처리되었습니다.

파일 또는 악성코드 이벤트의 경우, 파일과 일치하는 규칙에 대한 규칙 작업과 관련된 파일 규칙 작업 및 관련된 모든 파일 규칙 작업 옵션

허용된 연결

시스템이 이벤트에 대한 트래픽 흐름을 허용하는지 여부

애플리케이션

연결에서 탐지된 애플리케이션

애플리케이션 비즈니스 관련성

연결에서 탐지된 애플리케이션 트래픽과 연계된 사업 타당성으로, 매우 높음, 높음, 중간, 낮음, 매우 낮음이 있습니다. 연결에서 탐지된 각 애플리케이션 유형에는 관련된 사업 타당성이 있습니다. 이 필드에는 그중 가장 낮은 값(가장 연관성이 적음)이 표시됩니다.

애플리케이션 범주, 애플리케이션 태그

애플리케이션의 기능을 파악하는 데 도움이 될 수 있도록 애플리케이션의 특성을 분류하는 기준

애플리케이션 위험성

연결에서 탐지된 애플리케이션 트래픽과 관련된 위험성으로, 매우 높음, 높음, 중간, 낮음, 매우 낮음이 있습니다. 연결에서 탐지된 웹 애플리케이션의 각 유형에는 관련된 위험이 있습니다. 이 필드에는 그중 가장 높은 위험이 표시됩니다.

차단 유형

이벤트의 트래픽 흐름과 일치하는 액세스 제어 규칙에서 지정된 차단 유형: 차단 또는 양방향 차단

클라이언트 애플리케이션, 클라이언트 버전

연결에서 탐지된 클라이언트 애플리케이션 및 클라이언트 버전

클라이언트 비즈니스 관련성

연결에서 탐지된 클라이언트 트래픽과 관련된 사업 타당성으로, 매우 높음, 높음, 중간, 낮음, 매우 낮음이 있습니다. 연결에서 탐지된 각 클라이언트 유형에는 관련된 사업 타당성이 있습니다. 이 필드에는 그중 가장 낮은 값(가장 연관성이 적음)이 표시됩니다.

클라이언트 범주, 클라이언트 태그

애플리케이션의 기능을 파악하는 데 도움이 될 수 있도록 애플리케이션의 특성을 분류하는 기준

클라이언트 위험성

연결에서 탐지된 클라이언트 트래픽과 관련된 위험성으로, 매우 높음, 높음, 중간, 낮음, 매우 낮음이 있습니다. 연결에서 탐지된 클라이언트의 각 유형에는 관련된 위험이 있습니다. 이 필드에는 그중 가장 높은 위험이 표시됩니다.

연결

내부에서 생성되는 트래픽 흐름의 고유 ID

연결 차단 유형 표시기

이벤트의 트래픽 흐름과 일치하는 액세스 제어 규칙에서 지정된 차단 유형: 차단 또는 양방향 차단

연결 바이트

연결에 대한 총 바이트

연결 시간

연결 시작 시간

연결 타임 스탬프

연결이 탐지된 시간

거부된 연결

시스템이 이벤트에 대한 트래픽 흐름을 거부하는지 여부

대상 국가 및 대륙

수신 호스트의 국가와 대륙

목적지 **IP**

침입, 파일 또는 악성코드 이벤트에서 수신 호스트가 사용하는 IP 주소

대상 포트**/ICMP** 코드**,** 대상 포트**,** 대상 **Icode**

세션 responder가 사용하는 포트 또는 ICMP 코드

대상 **SGT(Security Group Tag),** 대상 **SGT(Security Group Tag)** 이름

대상과 연결된 TrustSec SGT(Security Group Tag) 번호 및 이름(있는 경우)

방향

파일의 전송 방향

속성

파일의 속성

악성코드

Secure Malware Analytics Cloud가 파일을 악성코드로 분류했거나, 파일의 위협 점수가 파일 정책에서 정의된 악성코드 임계값을 초과했음을 나타냅니다. 로컬 악성코드 분석을 통해 파일을 악성코드로 표시할 수도 있습니다.

정상

Secure Malware Analytics Cloud가 파일을 정상으로 분류했거나, 사용자가 파일을 정상 목록에 추가했음을 나타냅니다.

알 수 없음

시스템이 Secure Malware Analytics Cloud를 쿼리했으나 파일에 상태가 할당되지 않았음을 나타냅니다. 즉, Secure Malware Analytics Cloud에서 파일을 분류하지 않았습니다.

맞춤형 탐지

사용자가 파일을 커스텀 탐지 목록에 추가했음을 나타냅니다.

사용 불가능

시스템이 Secure Malware Analytics Cloud를 쿼리하지 못했음을 나타냅니다. 이 속성을 통해 이벤트의 일부를 확인할 수 있습니다. 이는 예상된 작업입니다.

해당 없음

파일 탐지 또는 파일 차단 규칙이 파일을 처리했으며 시스템이 Secure Malware Analytics Cloud를 쿼리하지 않았음을 나타냅니다.

이그레스 인터페이스**,** 이그레스 보안 영역

연결이 디바이스에서 외부로 나간 인터페이스 및 영역

이그레스 가상 라우터

대상 인터페이스가 속한 가상 라우터의 이름(있는 경우)

이벤트**,** 이벤트 유형

이벤트 유형.

이벤트 초**,** 이벤트 마이크로초

이벤트가 탐지된 시간(단위: 초 또는 마이크로초)

파일 카테고리

파일 유형의 일반적인 범주(예: Office 문서, 아카이브, 멀티미디어, 실행 파일, PDF 파일, 인코딩, 그래픽 또는 시스템 파일 등)

파일 이벤트 타임 스탬프

파일 또는 악성코드 파일이 생성된 시간 및 날짜

파일 이름

파일의 이름

파일 규칙 작업

파일을 탐지한 파일 정책 규칙과 연결된 작업 및 관련된 모든 파일 규칙 작업 옵션

파일 **SHA-256**

파일의 SHA-256 해시 값

파일 크기**(KB)**

킬로바이트 단위의 파일 크기. 파일이 완전히 수신되기 전에 시스템에서 파일을 차단한 경우에는 파일 크기를 비워 둘 수 있습니다.

파일 유형

HTML 또는 MSEXE 등의 파일 형식

파일/악성코드 정책

이벤트 생성과 관련된 파일 정책

파일 로그 차단 유형 표시기

이벤트의 트래픽 흐름과 일치하는 파일 규칙에서 지정된 차단 유형: 차단 또는 양방향 차단

방화벽 정책 규칙**,** 방화벽 규칙

연결을 처리한 액세스 제어 규칙 또는 기본 작업

첫 번째 패킷

세션의 첫 번째 패킷이 표시된 날짜 및 시간

HTTP 참조 페이지

연결(다른 URL에 링크를 제공하는 웹사이트 또는 다른 URL에서 링크를 가져온 웹사이트 등)에서 탐지된 HTTP 트래픽에 대해 요청된 URL의 참조 페이지를 나타내는 HTTP 참조 페이지

HTTP 응답

연결을 통해 클라이언트의 HTTP 요청에 대한 응답으로 전송된 HTTP 상태 코드

IDS 분류

이벤트를 생성한 규칙이 속하는 분류

인그레스 인터페이스**,** 인그레스 보안 영역

연결이 디바이스로 들어온 인터페이스 및 영역

인그레스 가상 라우터

소스 인터페이스가 속한 가상 라우터의 이름(있는 경우)

이니시에이터 바이트**,** 이니시에이터 패킷

세션 이니시에이터가 전송한 총 바이트 또는 패킷 수

초기자 국가 및 대륙

세션을 시작한 호스트의 국가 및 대륙. 이니시에이터 IP 주소를 라우팅할 수 있는 경우에만 사용 가능합니다.

초기자 **IP**

연결 또는 보안 인텔리전스 이벤트에서 세션을 시작한 호스트 IP 주소(및 호스트 이름 - DNS 확인을 활성화한 경우)

인라인 결과

인라인 모드에서 작동하는 경우 침입 이벤트를 트리거한 패킷을 시스템에서 삭제했거나 삭제할 수 있었는지 여부. 비워 두는 경우 트리거된 규칙이 삭제 및 이벤트 생성으로 설정되지 않았음을 나타냅니다.

침입 정책

이벤트를 생성한 규칙이 활성화된 침입 정책

IPS 차단 유형 표시기

이벤트의 트래픽 흐름과 일치하는 침입 규칙의 작업

마지막 패킷

세션의 마지막 패킷이 표시된 날짜 및 시간

MPLS 레이블

이 침입 이벤트를 트리거한 패킷에 연결된 Multiprotocol Label Switching(다중 프로토콜 레이블 스위칭) 레이블

악성코드 차단 유형 표시기

이벤트의 트래픽 흐름과 일치하는 파일 규칙에서 지정된 차단 유형: 차단 또는 양방향 차단

메시지

침입 이벤트의 경우 이벤트를 설명하는 텍스트. 악성코드 또는 파일 이벤트의 경우 악성코드 이벤트와 관련된 모든 추가 정보.

NAT 대상 **IP**

NAT(Network Address Translation) 대상 패킷의 경우 변환된 대상 IP 주소입니다.

NAT 대상 포트

NAT(Network Address Translation) 대상 패킷의 경우 변환된 대상 포트입니다.

NAT 소스 **IP**

NAT(Network Address Translation) 대상 패킷의 경우 변환된 소스 IP 주소입니다.

NAT 소스 포트

NAT(Network Address Translation) 대상 패킷의 경우 변환된 소스 포트입니다.

NetBIOS 도메인

세션에서 사용되는 NetBIOS 도메인

원본 클라이언트 국가 및 대륙

세션을 시작한 원본 클라이언트 호스트의 국가와 대륙. 원본 클라이언트 IP 주소를 라우팅할 수 있는 경우에만 사용 가능합니다.

원본 클라이언트 **IP**

HTTP 연결을 시작한 클라이언트의 원본 IP 주소. 이 주소는 XFF(X-Forwarded-For) 또는 True-Client-IP HTTP 헤더 필드나 그와 동일한 필드에서 파생됩니다.

정책**,** 정책 수정

이벤트와 연결된 액세스(방화벽) 규칙을 포함하는 액세스 제어 정책 및 해당 수정

우선순위

Cisco Talos Intelligence Group(Talos)에서 결정하는 이벤트 우선순위(높음, 보통, 낮음)

프로토콜

연결에 사용된 전송 프로토콜

이유

다음 표에 설명된 상황에서 연결이 로깅된 이유. 해당하지 않는 경우 이 필드는 비어 있습니다.

이유	설명
DNS 차단	시스템에서 도메인 이름 및 보안 인텔리전스 데이터를 기준으로 하여 검사 없이 연결을 거부했습니다. DNS 차단 이유는 DNS 규칙 작업에 따라 차단, 도메인을 찾을 수 없음 또는 싱크홀과 페어링됩니다.

이유	설명
DNS 모니터링	시스템에서 도메인 이름 및 보안 인텔리전스 데이터를 기준으로 하여 연결을 거부해야 했지만 사용자가 시스템에서 연결을 거부하는 대신 모니터링하도록 구성했습니다.
엘리펀트 플로우	연결은 전체 시스템 성능에 영향을 미칠 만큼 충분히 큰 플로우인 엘리펀트 플로우으로 간주되기에 충분합니다. 기본적으로 엘리펀트 플로우는 1GB/10초보다 큰 상태입니다. **system support elephant-flow-detection** 명령을 사용하여 디바이스 CLI에서 엘리펀트 플로우 식별을 위한 바이트 및 시간 임계값을 조정할 수 있습니다.
파일 차단	시스템이 전송을 차단한 파일 또는 악성코드 파일이 연결에 포함되었습니다. 파일 차단 이유는 항상 차단 작업과 페어링됩니다.
파일 맞춤형 탐지	시스템이 전송을 차단한 맞춤형 탐지 목록의 파일이 연결에 포함되었습니다.
파일 모니터링	시스템이 연결에서 특정 파일 유형을 탐지했습니다.
파일 재시작 허용	파일 전송이 파일 차단 또는 악성코드 차단 파일 규칙에 의해 원래 차단되었다가, 해당 파일을 허용하는 새 액세스 제어 정책이 구축된 후 HTTP 세션이 자동으로 재시작되었습니다.
파일 재시작 차단	파일 전송이 파일 탐지 또는 악성코드 클라우드 조회 파일 규칙에 의해 원래 허용되었다가, 해당 파일을 차단하는 새 액세스 제어 정책이 구축된 후 HTTP 세션이 자동으로 중지되었습니다.
침입 차단	시스템이 연결에서 탐지된 익스플로잇(침입 정책 위반)을 차단했거나 차단할 수도 있었음을 나타냅니다. 침입 차단 이유는 차단된 익스플로잇의 경우 차단 작업과, 차단될 수도 있었던 익스플로잇의 경우 허용과 페어링됩니다.
침입 모니터링	시스템이 연결에서 탐지된 익스플로잇을 탐지했지만 차단하지는 않았습니다. 트리거된 침입 규칙의 상태가 이벤트 생성으로 설정되어 있으면 이러한 현상이 나타납니다.
IP 차단	시스템에서 IP 주소 및 보안 인텔리전스 데이터를 기준으로 하여 검사 없이 연결을 거부했습니다. IP 차단 이유는 항상 차단 작업과 페어링됩니다.
SSL 차단	시스템에서 SSL 검사 컨피그레이션을 기준으로 하여 암호화된 연결을 차단했습니다. SSL 차단 이유는 항상 차단 작업과 페어링됩니다.
URL 차단	시스템에서 URL 및 보안 인텔리전스 데이터를 기준으로 하여 검사 없이 연결을 거부했습니다. URL 차단 이유는 항상 차단 작업과 페어링됩니다.

수신된 시간

이벤트가 생성된 날짜 및 시간

참조된 호스트

연결의 프로토콜이 HTTP, 또는 HTTPS인 경우 이 필드에는 각 프로토콜이 사용했던 호스트 이름이 표시됩니다.

Responder Bytes, Responder Packets

세션 Responder가 전송한 총 바이트 또는 패킷 수

응답기 국가 및 대륙

세션에 응답한 호스트의 국가 및 대륙. Responder IP 주소를 라우팅할 수 있는 경우에만 사용 가능합니다.

응답기 **IP**

연결 또는 보안 인텔리전스 이벤트에서 세션 응답기의 호스트 IP 주소(및 호스트 이름 - DNS 확인을 활성화한 경우)

SI 카테고리 **ID(**보안 인텔리전스 카테고리**)**

네트워크 또는 URL 개체 이름 등 차단된 항목을 포함하는 개체의 이름 또는 피드 범주의 이름

서명

파일/악성코드 이벤트의 서명 ID

소스 국가 및 대륙

전송 호스트의 국가와 대륙 소스 IP 주소를 라우팅할 수 있는 경우에만 사용 가능합니다.

소스 **IP**

침입, 파일 또는 악성코드 이벤트에서 전송 호스트가 사용하는 IP 주소

소스 포트**/ICMP** 유형**,** 소스 포트**,** 소스 포트 **Itype**

세션 이니시에이터가 사용하는 포트 또는 ICMP 유형

소스 **SGT(Security Group Tag),** 소스 **SGT(Security Group Tag)** 이름

소스와 연결된 TrustSec SGT(Security Group Tag) 번호 및 이름(있는 경우)

SSL 실제 작업

시스템이 연결에 적용한 실제 작업. 이는 정상적인 작업과 다를 수 있습니다. 예를 들어 연결이 암호 해독을 적용하는 규칙과 일치할 수 있으나, 어떠한 이유로든 암호 해독되지 않을 수 있습니다.

작업	설명
차단/차단 및 재설정	차단된 암호화된 연결을 나타냅니다.
암호 해독(재서명)	다시 서명된 서버 인증서를 사용하여 암호 해독된 발신 연결을 나타냅니다.

작업	설명
암호 해독(대체 키)	대체된 공개 키가 있는 자체 서명된 서버 인증서를 사용하여 암호 해독된 발신 연결을 나타냅니다.
암호 해독(알려진 키)	알려진 개인 키를 사용하여 암호 해독된 수신 연결을 나타냅니다.
기본 작업	연결이 기본 작업에 의해 처리되었음을 나타냅니다.
암호 해독 안 함	시스템이 암호 해독하지 않은 연결을 나타냅니다.

SSL 인증서 핑거프린트

인증서를 인증하는 데 사용되는 SHA 해시 값입니다.

SSL 인증서 상태

이는 인증서 상태 SSL 규칙 조건을 구성한 경우에만 적용됩니다. 암호화된 트래픽이 SSL 규칙과 일치할 경우, 이 필드에는 다음 서버 인증서 상태 값 중 하나 이상이 표시됩니다.

- Self Signed(셀프 서명)
- Valid(유효)
- Invalid Signature(잘못된 서명)
- Invalid Issuer(잘못된 발급자)
- Expired(만료됨)
- Unknown(알 수 없음)
- Not Valid Yet(아직 유효하지 않음)
- Revoked(취소됨)

해독 불가능한 트래픽이 SSL 규칙과 일치할 경우, 이 필드는 Not Checked(확인되지 않음)로 표시됩니다.

SSL 암호 그룹

연결에 사용된 암호 그룹입니다.

SSL 예상 작업

연결과 일치하는 SSL 규칙에 지정된 작업입니다.

SSL 플로우 플래그

암호화된 연결에 대한 처음 10개의 디버깅 수준 플래그입니다.

SSL 플로우 메시지

SSL 핸드셰이크 도중 클라이언트와 서버 간에 교환되는 SSL/TLS 메시지(예: HELLO_REQUEST 및 CLIENT_HELLO)입니다. TLS 연결에서 교환되는 메시지에 대한 자세한 내용은 http://tools.ietf.org/html/rfc5246를 참조하십시오.

SSL 정책

연결에 적용되는 SSL 암호 해독 정책의 이름입니다.

SSL 규칙

연결에 적용되는 SSL 암호 해독 규칙의 이름입니다.

SSL 세션 **ID**

SSL 핸드셰이크 도중 클라이언트와 서버 간에 협상된 16진수 Session ID입니다.

SSL 티켓 **ID**

SSL 핸드셰이크 도중 전송된 세션 티켓 정보의 16진수 해시 값입니다.

SSL URL 카테고리

SSL 암호 해독 처리 도중에 확인된 대상 웹 서버의 URL 카테고리입니다.

SSL 버전

연결에 사용된 SSL/TLS 버전입니다.

TCP 플래그

연결에서 탐지된 TCP 플래그

총 패킷

연결에서 전송된 패킷의 총 수(**Initiator Packets(**이니시에이터 패킷**)** + **Responder Packets(**응답기 패킷**)**)

URL, URL 범주**, URL** 평판**, URL** 평판 점수

세션 중에 모니터링된 호스트에서 요청한 URL과 관련 범주, 평판 및 평판 점수(사용 가능한 경우)

DNS 조회 요청 필터링의 경우 DNS Query(DNS 쿼리) 필드에 표시되는 FQDN에 대한 범주 및 평판입니다. 웹 요청이 아닌 DNS 요청에 대해 범주/평판 조회를 수행하므로 URL 필드는 비어 있습니다.

시스템에서 SSL 애플리케이션을 식별하거나 차단한 경우, 요청한 URL은 암호화된 트래픽에 있으므로 시스템은 SSL 인증서를 기준으로 해당 트래픽을 식별합니다. 따라서 SSL 애플리케이션의 경우 URL은 인증서에 포함된 공용 이름을 나타냅니다.

사용자

이니시에이터 IP 주소와 연결된 사용자

VLAN

이벤트를 트리거한 패킷에 관련된 가장 안쪽의 VLAN ID

웹 애플리케이션 비즈니스 관련성

연결에서 탐지된 웹 애플리케이션 트래픽과 연계된 비즈니스 관련성: Very High(매우 높음), High(높음), Medium(중간), Low(낮음), 또는 Very Low(매우 낮음) 연결에서 탐지된 웹 애플리케이션의 각 유형은 관련된 비즈니스 관련성을 가지며, 이 필드는 가장 낮은(가장 타당성이 적은) 것을 표시합니다.

웹 애플리케이션 범주**,** 웹 애플리케이션 태그

웹 애플리케이션의 기능을 파악하는 데 도움이 될 수 있도록 웹 애플리케이션의 특성을 분류하는 기준

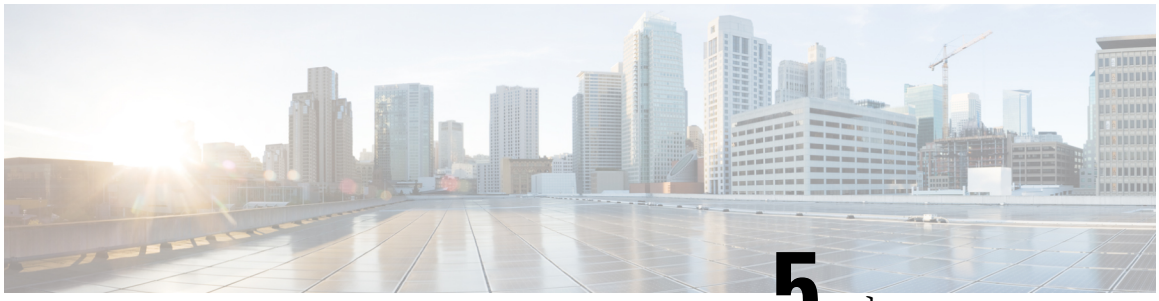
웹 애플리케이션 위험성

연결에서 탐지된 웹 애플리케이션 트래픽과 관련된 위험성으로, 매우 높음, 높음, 중간, 낮음, 매우 낮음이 있습니다. 연결에서 탐지된 웹 애플리케이션의 각 유형에는 관련된 위험이 있습니다. 이 필드에는 그중 가장 높은 위험이 표시됩니다.

웹 애플리케이션

연결에서 탐지된 HTTP 트래픽의 콘텐츠 또는 요청한 URL을 나타내는 웹 애플리케이션

웹 애플리케이션이 이벤트의 URL과 매칭되지 않을 경우, 해당 트래픽은 참조 트래픽(예: 광고 트래픽)일 가능성이 높습니다. 시스템이 참조 트래픽을 탐지할 경우, 시스템은 제공되는 참조 애플리케이션을 저장하고 해당 애플리케이션을 웹 애플리케이션으로 나열합니다.



5 장

Cisco ISA 3000에 대한 알람

원치 않는 상황이 발생하면 알림을 받을 수 있도록 Cisco ISA 3000 디바이스의 알람 시스템을 구성할 수 있습니다.

알람 정보

여러 조건에 대해 알람을 생성하도록 ISA 3000을 구성할 수 있습니다. 조건이 구성된 설정과 일치하지 않으면 시스템은 알람을 트리거합니다. 이러한 알람은 LED, syslog 메시지, SNMP 트랩 및 알람 출력 인터페이스에 연결된 외부 디바이스를 통해 보고됩니다. 기본적으로 알람이 트리거되면 syslog 메시지만 발급됩니다.

다음을 모니터링하도록 알람 시스템을 구성할 수 있습니다.

- 전원 공급 장치
- 기본 및 보조 온도 센서
- 알람 입력 인터페이스

ISA 3000에는 내부 센서와 알람 입력 인터페이스 2개, 알람 출력 인터페이스 1개가 있습니다. 도어 센서와 같은 외부 센서를 알람 입력에 연결할 수 있습니다. 버저나 표시등과 같은 외부 알람 디바이스를 알람 출력 인터페이스에 연결할 수 있습니다.

알람 출력 인터페이스는 릴레이 메커니즘입니다. 알람 조건에 따라 릴레이가 활성화되거나 비활성화됩니다. 릴레이가 활성화되면 인터페이스에 연결된 디바이스가 활성화됩니다. 릴레이가 비활성화되면 연결된 디바이스가 비활성 상태가 됩니다. 알람이 트리거되는 동안에는 릴레이가 활성화된 상태로 유지됩니다.

외부 센서와 알람 릴레이 연결에 대한 자세한 정보는 Cisco ISA 3000 Industrial Security Appliance 하드웨어 설치 가이드를 참조하십시오.

알람 입력 인터페이스

도어가 열린 상태를 탐지하는 센서 등의 외부 센서에 알람 입력 인터페이스나 접촉부를 연결할 수 있습니다.

각 알람 입력 인터페이스에는 해당하는 LED가 있습니다. 이러한 LED는 각 알람 입력의 알람 상태를 전달합니다. 각 알람 입력에 대해 트리거와 심각도를 구성할 수 있습니다. LED 외에도 출력 릴레이를 트리거하여 외부 알람을 활성화하고 syslog 메시지와 SNMP 트랩을 전송하는 접촉부를 구성할 수도 있습니다.

다음 표에서는 알람 입력에 대한 알람 조건에 대응하는 LED의 상태를 설명합니다. 또한 출력 릴레이, syslog 메시지 및 SNMP 트랩(알람 입력에 대해 이러한 응답을 활성화하는 경우)의 동작도 설명합니다.

알람 상태	**LED**	출력 릴레이	**Syslog**	**SNMP** 트랩
알람이 구성되지 않음	Off	—	—	—
알람이 트리거되지 않음	녹색	—	—	—
알람 활성화됨	경미한 알람 - 빨간색으로 켜짐 중요한 알람 - 빨간색으로 깜박임	릴레이 활성화됨	Syslog 생성됨	SNMP 트랩 전송됨
알람 종료됨	녹색	릴레이 비활성화됨	Syslog 생성됨	—

알람 출력 인터페이스

버저나 표시등과 같은 외부 알람을 알람 출력 인터페이스에 연결할 수 있습니다.

알람 출력 인터페이스는 릴레이로 작동하며 해당하는 LED도 가지고 있습니다. 이러한 LED는 입력 인터페이스에 연결된 외부 센서와 듀얼 전원 공급 장치 및 온도 센서 등의 내부 센서의 알람 상태를 전달합니다. 출력 릴레이(있는 경우)를 활성화하는 알람을 구성합니다.

다음 표에서는 알람 조건에 대응하는 LED 및 출력 릴레이의 상태를 설명합니다. 또한 syslog 메시지 및 SNMP 트랩(알람에 대해 이러한 응답을 활성화하는 경우)의 동작도 설명합니다.

알람 상태	**LED**	출력 릴레이	**Syslog**	**SNMP** 트랩
알람이 구성되지 않음	Off	—	—	—
알람이 트리거되지 않음	녹색	—	—	—
알람 활성화됨	빨간색으로 켜짐	릴레이 활성화됨	Syslog 생성됨	SNMP 트랩 전송됨

알람 상태	LED	출력 릴레이	Syslog	SNMP 트랩
알람 종료됨	녹색	릴레이 비활성화됨	Syslog 생성됨	—

Syslog 알람

기본적으로 시스템은 특정 알람이 트리거될 때 syslog 메시지를 전송합니다. 메시지가 전송되지 않도록 하려는 경우 syslog 메시지를 비활성화할 수 있습니다.

시스템 로그 알람을 작동하게 하려면 **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Logging Settings(**로깅 설정**)**에서 진단 로깅도 활성화해야 합니다. 시스템 로그 서버, 콘솔 로깅 또는 내부 버퍼 로깅을 구성합니다.

진단 로깅의 대상을 활성화하지 않으면 알람 시스템은 어떤 위치로도 syslog 메시지를 전송하지 않습니다.

SNMP 트랩 알람

SNMP 트랩을 SNMP 서버로 전송할 때의 알람을 선택적으로 구성할 수 있습니다. SNMP 트랩 알람을 작동하게 하려면 SNMP 설정도 구성해야 합니다.

threat defense API를 사용하여 SNMP를 구성합니다. More options(추가 옵션) 버튼( )을 클릭하고 API Explorer를 선택합니다. 그런 다음, SNMP 리소스를 찾아 모델 설명서에서 기능을 구성하는 방법에 대한 정보를 확인합니다. SNMP 버전 2c 또는 3을 사용할 수 있습니다. 버전 1은 지원되지 않습니다. SNMP 구성에 대한 전체 정보는 최신 버전 ASA 소프트웨어용 *CLI* 설명서 *1: Cisco ASA* 시리즈 일반 작업 *CLI* 컨피그레이션 가이드의 SNMP 장을 참조하십시오. 이 가이드는 https://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html에서 확인할 수 있습니다.

알람 기본값

다음 표에는 알람 입력 인터페이스(접촉부), 예비 전원 공급 장치 및 온도의 기본값이 지정되어 있습니다.

	경보	트리거	심각도	SNMP 트랩	출력 릴레이	Syslog 메시지
알람 접촉부 1	활성화	닫힌 상태	경미	비활성화됨	비활성화	활성화
알람 접촉부 2	활성화	닫힌 상태	경미	비활성화됨	비활성화	활성화
예비 전원 공급 장치(활성화된 경우)	활성화	—	—	비활성화됨	비활성화	활성화

	경보	트리거	심각도	**SNMP** 트랩	출력 릴레이	**Syslog** 메시지
온도	기본 온도 알람에 대해 활성화됨(최고 임계값과 최저 임계값의 기본값은 각각 92°C 및 -40°C) 보조 알람에 대해 비활성화됨.	—	—	기본 온도 알람에 대해 활성화됨	기본 온도 알람에 대해 활성화됨	기본 온도 알람에 대해 활성화됨

ISA 3000에 대한 알람 구성

FlexConfig를 사용하여 ISA 3000에 대한 알람을 구성합니다. 다음 주제에서는 다양한 유형의 알람을 구성하는 방법을 설명합니다.

알람 입력 접촉부 구성

알람 입력 접촉부(인터페이스)를 외부 센서에 연결하는 경우에는 센서의 입력을 기준으로 하여 알람을 생성하도록 접촉부를 구성할 수 있습니다. 실제로 접촉부는 닫히는 경우(즉, 접촉부를 통한 전류 흐름이 중지되는 경우) 기본적으로 syslog 메시지를 전송하도록 설정됩니다. 기본값이 요구 사항을 충족하지 않는 경우에만 접촉부를 구성해야 합니다.

알람 접촉부의 번호는 1번과 2번으로 지정되므로 정확한 설정을 구성하려면 물리적 핀을 유선 연결한 방법을 파악해야 합니다. 접촉부는 개별적으로 구성합니다.

프로시저

단계 **1** **Device(**디바이스**)** > **Advanced Configuration(**고급 컨피그레이션**)**에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

단계 **2** Advanced Configuration(고급 컨피그레이션) 목차에서 **FlexConfig** > **FlexConfig Objects(FlexConfig** 개체**)**를 클릭합니다.

단계 **3** **+** 버튼을 클릭하여 새 개체를 생성합니다.

단계 **4** 개체의 이름을 입력합니다. 예를 들어 **Enable_Alarm_Contact**를 입력합니다.

단계 **5** **Template(**템플릿**)** 편집기에서 접촉부를 구성하는 데 필요한 명령을 입력합니다.

a) 알람 접촉부의 설명을 구성합니다.

alarm contact {**1** | **2**} **description** *string(*문자열*)*

예를 들어 접촉부 1의 설명을 "Door Open(도어 열림)"으로 설정하려면 다음을 입력합니다.

```
alarm contact 1 description Door Open
```

b) 알람 접촉부의 심각도를 구성합니다.

alarm contact {**1** | **2** | **any**} **severity** {**major** | **minor** | **none**}

하나의 접촉부를 컨피그레이션하는 대신 **any**를 지정하여 모든 접촉부의 심각도를 변경할 수 있습니다. 심각도는 접촉부와 연결된 LED의 동작을 제어합니다.

- **major**- LED가 빨간색으로 깜박입니다.
- **minor**- LED가 빨간색으로 켜져 있습니다. 이는 기본값입니다.
- **none**- LED가 꺼져 있습니다.

예를 들어 접촉부 1의 심각도를 Major(중대)로 설정하려면 다음을 입력합니다.

```
alarm contact 1 severity major
```

c) 알람 접촉부의 트리거를 구성합니다.

alarm contact {**1** | **2** | **any**} **trigger** {**open** | **closed**}

하나의 접촉부를 컨피그레이션하는 대신 **any**를 지정하여 모든 접촉부의 트리거를 변경할 수 있습니다. 트리거는 알림 신호를 보내는 전기적 상태를 결정합니다.

- **open**- 접촉부의 기본 상태가 닫힌 상태(즉, 전류가 접촉부를 통과하고 있음)입니다. 접촉부가 열리면(즉, 전류 흐름이 중지됨) 알림이 트리거됩니다.
- **closed**- 접촉부의 기본 상태가 열린 상태(전류가 접촉부를 통과하지 않음)입니다. 접촉부가 닫히면(즉, 전류가 접촉부를 통과하기 시작함) 알림이 트리거됩니다. 이는 기본값입니다.

도어 센서를 알람 입력 접촉부 1에 연결하고 해당 접촉부의 기본 상태가 알람 접촉부를 통한 전류 흐름이 없는 상태(접촉부가 열린 상태)인 경우를 예로 들어 보겠습니다. 도어가 열리면 접촉부는 닫히며 알람 접촉부를 통해 전류가 흐릅니다. 이 경우에는 전류 흐름이 시작되면 알람이 꺼지도록 알람 트리거를 닫힘으로 설정합니다.

```
alarm contact 1 trigger closed
```

d) 알람 접촉부가 트리거될 때 수행할 작업을 구성합니다.

alarm facility input-alarm {**1** | **2**} {**relay** | **syslog** | **notifies**}

여러 작업을 구성할 수 있습니다. 예를 들어 외부 알람을 활성화하고, syslog 메시지를 보내고, SNMP 트랩도 전송하도록 디바이스를 구성할 수 있습니다.

- **relay(**릴레이**)** - 알람 출력 릴레이를 활성화합니다. 그러면 버저, 플래쉬 등 접촉부에 부착한 외부 알람이 활성화됩니다. 또한 출력 LED가 빨간색으로 바뀝니다.
- **syslog** - syslog 메시지를 보냅니다. 이 옵션은 기본적으로 활성화되어 있습니다.
- **notifies(**알림**)** - SNMP 트랩을 보냅니다.

예를 들어 알람 입력 접촉부 1에 대해 모든 작업을 활성화하려면 다음을 입력합니다.

```
alarm facility input-alarm 1 relay
alarm facility input-alarm 1 syslog
alarm facility input-alarm 1 notifies
```

단계 **6** **Negate Template(**무효화 템플릿**)** 편집기에 이 컨피그레이션을 실행 취소하는 데 필요한 행을 입력합니다.

이 모든 명령은 **no** 형식을 취해 비활성화되고 기본 설정으로 되돌아갑니다. 예를 들어 이 템플릿에 이 절차에 나와 있는 모든 명령 예시가 포함되어 있는 경우 무효화 템플릿은 다음과 같습니다.

```
no alarm contact 1 description Door Open
no alarm contact 1 severity major
no alarm contact 1 trigger closed
no alarm facility input-alarm 1 relay
no alarm facility input-alarm 1 syslog
no alarm facility input-alarm 1 notifies
```

단계 **7** **OK(**확인**)**를 클릭하여 개체를 저장합니다.

단계 **8** FlexConfig 정책에 개체를 추가합니다.

a) 목차에서 **FlexConfig Policy(FlexConfig** 정책**)**를 클릭합니다.

b) Group List(그룹 목록)에서 **+**를 클릭합니다.

c) Enable_Alarm_Contact 개체를 선택하고 **OK(**확인**)**를 클릭합니다.

템플릿의 명령으로 미리보기가 업데이트됩니다. 올바른 명령이 표시되는지 확인합니다.

d) **Save(**저장**)**를 클릭합니다.

이제 정책을 구축할 수 있습니다.

단계 **9** 구축을 완료한 후에 CLI 콘솔 또는 SSH 세션에서 **show running-config** 명령을 사용하여 실행 중인 컨피그레이션에 변경 사항이 정확히 적용되었는지 확인합니다. 외부 센서를 테스트하여 알람이 트리거되는지 확인합니다.

전원 공급 장치 알람 구성

ISA 3000에는 전원 공급 장치 두 개가 있습니다. 기본적으로 시스템은 단일 전원 모드에서 작동합니다. 그러나 듀얼 모드로 작동하도록 시스템을 구성할 수 있습니다. 그러면 기본 전원 공급 장치에서 장애가 발생하는 경우 두 번째 전원 공급 장치가 자동으로 전원을 공급합니다. 듀얼 모드를 활성화하면 syslog 알림을 전송하도록 전원 공급 장치 알람이 자동으로 활성화됩니다. 하지만 알림을 완전히 비활성화할 수도 있고 SNMP 트랩 또는 알람 하드웨어 릴레이를 활성화할 수도 있습니다.

다음 절차에서는 듀얼 모드를 활성화하고 전원 공급 장치 알람을 구성하는 방법을 설명합니다.

프로시저

단계 **1** **Device(**디바이스**)** > **Advanced Configuration(**고급 컨피그레이션**)**에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

단계 **2** Advanced Configuration(고급 컨피그레이션) 목차에서 **FlexConfig** > **FlexConfig Objects(FlexConfig** 개체**)**를 클릭합니다.

단계 **3** **+** 버튼을 클릭하여 새 개체를 생성합니다.

단계 **4** 개체의 이름을 입력합니다. 예를 들어 **Enable_Power_Supply_Alarm**을 입력합니다.

단계 **5** **Template(**템플릿**)** 편집기에서 전원 공급 장치 알람을 구성하는 데 필요한 명령을 입력합니다.

a) 듀얼 전원 공급 장치 모드를 활성화합니다.

power-supply dual

예를 들면 다음과 같습니다.

```
power-supply dual
```

b) 전원 공급 장치 알람이 트리거될 때 수행할 작업을 구성합니다.

alarm facility power-supply rps {**relay** | **syslog** | **notifies** | **disable**}

여러 작업을 구성할 수 있습니다. 예를 들어 외부 알람을 활성화하고, syslog 메시지를 보내고, SNMP 트랩도 전송하도록 디바이스를 구성할 수 있습니다.

- **relay(**릴레이**)** - 알람 출력 릴레이를 활성화합니다. 그러면 버저, 플래쉬 등 접촉부에 부착한 외부 알람이 활성화됩니다. 또한 출력 LED가 빨간색으로 바뀝니다.
- **syslog** - syslog 메시지를 보냅니다. 이 옵션은 기본적으로 활성화되어 있습니다.
- **notifies(**알림**)** - SNMP 트랩을 보냅니다.
- **disable(**비활성**)** - 전원 공급 장치 알람을 비활성화합니다. 전원 공급 장치 알람에 대해 구성된 기타 모든 작업은 작동하지 않습니다.

예를 들어 전원 공급 장치 알람에 대한 모든 작업을 활성화하려면 다음 명령을 입력합니다.

```
alarm facility power-supply rps relay
alarm facility power-supply rps syslog
alarm facility power-supply rps notifies
```

단계 **6** **Negate Template(**무효화 템플릿**)** 편집기에 이 컨피그레이션을 실행 취소하는 데 필요한 행을 입력합니다.

이 모든 명령은 **no** 형식을 취해 비활성화되고 기본 설정으로 되돌아갑니다. 예를 들어 이 템플릿에 이 절차에 나와 있는 모든 명령 예시가 포함되어 있는 경우 무효화 템플릿은 다음과 같습니다.

```
no power-supply dual
no alarm facility power-supply rps relay
no alarm facility power-supply rps syslog
no alarm facility power-supply rps notifies
```

단계 **7** **OK(**확인**)**를 클릭하여 개체를 저장합니다.

단계 **8** FlexConfig 정책에 개체를 추가합니다.

a) 목차에서 **FlexConfig Policy(FlexConfig** 정책**)**를 클릭합니다.

b) Group List(그룹 목록)에서 **+**를 클릭합니다.

c) Enable_Power_Supply_Alarm 개체를 선택하고 **OK(**확인**)**를 클릭합니다.

템플릿의 명령으로 미리보기가 업데이트됩니다. 올바른 명령이 표시되는지 확인합니다.

d) **Save(**저장**)**를 클릭합니다.

이제 정책을 구축할 수 있습니다.

단계 **9** 구축을 완료한 후에 CLI 콘솔 또는 SSH 세션에서 **show running-config** 명령을 사용하여 실행 중인 컨피그레이션에 변경 사항이 정확히 적용되었는지 확인합니다.

온도 알람 구성

디바이스의 CPU 카드 온도를 기준으로 알람을 구성할 수 있습니다.

기본 및 보조 온도 범위를 설정할 수 있습니다. 온도가 최저 임계값 아래로 떨어지거나 최고 임계값을 초과하면 알람이 트리거됩니다.

기본 온도 알람은 모든 알람 작업(출력 릴레이, syslog, SNMP)에 대해 기본적으로 활성화됩니다. 기본 온도 범위의 기본 설정은 -40°C~92°C입니다.

보조 온도 알람은 기본적으로 비활성화됩니다. 보조 온도는 -35°C~85°C 범위 내에서 설정할 수 있습니다.

보조 온도 범위는 기본 범위보다 더 제한적이므로 보조 최저 온도나 최고 온도를 설정하는 경우, 기본 설정에 대해 기본값이 아닌 값을 구성하더라도 이 설정으로 인해 해당하는 기본 설정이 비활성화됩니다. 최고 온도 알람 2개와 최저 온도 알람 2개를 각기 별도로 활성화할 수는 없습니다.

따라서 실제로는 최고 온도와 최저 온도에 대해 기본 설정이나 보조 설정만 구성해야 합니다.

프로시저

단계 **1** **Device(**디바이스**)** > **Advanced Configuration(**고급 컨피그레이션**)**에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

단계 **2** Advanced Configuration(고급 컨피그레이션) 목차에서 **FlexConfig** > **FlexConfig Objects(FlexConfig** 개체**)**를 클릭합니다.

단계 **3** **+** 버튼을 클릭하여 새 개체를 생성합니다.

단계 **4** 개체의 이름을 입력합니다. 예를 들어 **Enable_Temperature_Alarm**을 입력합니다.

단계 **5** **Template(**템플릿**)** 편집기에서 온도 알람을 구성하는 데 필요한 명령을 입력합니다.

a) 허용 가능한 온도 범위를 구성합니다.

alarm facility temperature {**primary** | **secondary**} {**low** | **high**} *temperature*

온도는 섭씨 단위입니다. 기본 알람에 대해 허용되는 범위는 -40~92(기본 범위)입니다. 보조 알람에 대해 허용되는 범위는 -35~85입니다. 최저 온도 값은 최고 온도 값보다 작아야 합니다.

예를 들어 더 제한적인 온도 범위인 -20~80(보조 알람에 대해 허용되는 범위 내)을 설정하려면 다음과 같이 보조 알람을 구성합니다.

```
alarm facility temperature secondary low -20
alarm facility temperature secondary high 80
```

b) 온도 알람이 트리거될 때 수행할 작업을 구성합니다.

alarm facility temperature {**primary** | **secondary**} {**relay** | **syslog** | **notifies**}

여러 작업을 구성할 수 있습니다. 예를 들어 외부 알람을 활성화하고, syslog 메시지를 보내고, SNMP 트랩도 전송하도록 디바이스를 구성할 수 있습니다.

- **relay(**릴레이**)** - 알람 출력 릴레이를 활성화합니다. 그러면 버저, 플래쉬 등 접촉부에 부착한 외부 알람이 활성화됩니다. 또한 출력 LED가 빨간색으로 바뀝니다.
- **syslog** - syslog 메시지를 보냅니다.
- **notifies(**알림**)** - SNMP 트랩을 보냅니다.

예를 들어 보조 온도 알람에 대해 모든 작업을 활성화하려면 다음 명령을 입력합니다.

```
alarm facility temperature secondary relay
alarm facility temperature secondary syslog
alarm facility temperature secondary notifies
```

단계 **6** **Negate Template(**무효화 템플릿**)** 편집기에 이 컨피그레이션을 실행 취소하는 데 필요한 행을 입력합니다.

이 모든 명령은 **no** 형식을 취해 기본 설정으로 되돌아가거나(기본 알람의 경우) 비활성화(보조 알람의 경우)됩니다. 예를 들어 이 템플릿에 이 절차에 나와 있는 모든 명령 예시가 포함되어 있는 경우 무효화 템플릿은 다음과 같습니다.

```
no alarm facility temperature secondary low -20
no alarm facility temperature secondary high 80
no alarm facility temperature secondary relay
no alarm facility temperature secondary syslog
no alarm facility temperature secondary notifies
```

단계 **7** **OK(**확인**)**를 클릭하여 개체를 저장합니다.

단계 **8** FlexConfig 정책에 개체를 추가합니다.

a) 목차에서 **FlexConfig Policy(FlexConfig** 정책**)**를 클릭합니다.

b) Group List(그룹 목록)에서 +를 클릭합니다.

c) Enable_Temperature_Alarm 개체를 선택하고 **OK(**확인**)**를 클릭합니다.

템플릿의 명령으로 미리보기가 업데이트됩니다. 올바른 명령이 표시되는지 확인합니다.

d) **Save(**저장**)**를 클릭합니다.

이제 정책을 구축할 수 있습니다.

단계 **9** 구축을 완료한 후에 CLI 콘솔 또는 SSH 세션에서 **show running-config** 명령을 사용하여 실행 중인 컨피그레이션에 변경 사항이 정확히 적용되었는지 확인합니다.

알람 모니터링

다음 주제에서는 알람을 모니터링하고 관리하는 방법을 설명합니다.

알람 상태 모니터링

CLI에서 다음 명령을 사용하여 알람을 모니터링할 수 있습니다.

- **show alarm settings**

  가능한 각 알람의 현재 컨피그레이션을 표시합니다.

- **show environment alarm-contact**

  입력 알람 접촉부의 물리적 상태에 대한 정보를 표시합니다.

- **show facility-alarm relay**

  출력 릴레이를 트리거한 알람에 대한 정보를 표시합니다.

- **show facility-alarm status** [**info** | **major** | **minor**]

  트리거된 모든 알람에 대한 정보를 표시합니다. **major** 또는 **minor** 상태를 기준으로 필터링하여 보기를 제한할 수 있습니다. **info** 키워드를 사용하면 키워드를 사용하지 않을 때와 출력이 동일합니다.

Syslog 메시지에서 알람 모니터링

구성하는 알람 유형에 따라 다음 syslog 메시지가 표시될 수 있습니다.

듀얼 전원 공급 장치 알람

- %FTD-1-735005: Power Supply Unit Redundancy OK(전원 공급 장치 유닛 이중화 정상)
- %FTD-1-735006: Power Supply Unit Redundancy Lost(전원 공급 장치 유닛 이중화 손실)

온도 알람

이러한 알람에서 *Celsius*는 디바이스에서 탐지된 온도(섭씨)로 대체됩니다.

- %FTD-6-806001: Primary alarm CPU temperature is High(기본 알람 CPU 온도 높음) 섭씨
- %FTD-6-806002: Primary alarm for CPU high temperature is cleared(CPU 고온에 대한 기본 알람이 해제됨)
- %FTD-6-806003: Primary alarm CPU temperature is Low(기본 알람 CPU 온도 낮음) 섭씨
- %FTD-6-806004: Primary alarm for CPU Low temperature is cleared(CPU 저온에 대한 기본 알람이 해제됨)
- %FTD-6-806005: Secondary alarm CPU temperature is High(보조 알람 CPU 온도 높음) 섭씨

- %FTD-6-806006: Secondary alarm for CPU high temperature is cleared(CPU 고온에 대한 보조 알람이 해제됨)
- %FTD-6-806007: Secondary alarm CPU temperature is Low(보조 알람 CPU 온도 낮음) 섭씨
- %FTD-6-806008: Secondary alarm for CPU Low temperature is cleared(CPU 저온에 대한 보조 알람이 해제됨)

알람 입력 접촉부 알람

이러한 알람에서 *description*은 구성한 접촉부에 대한 설명입니다.

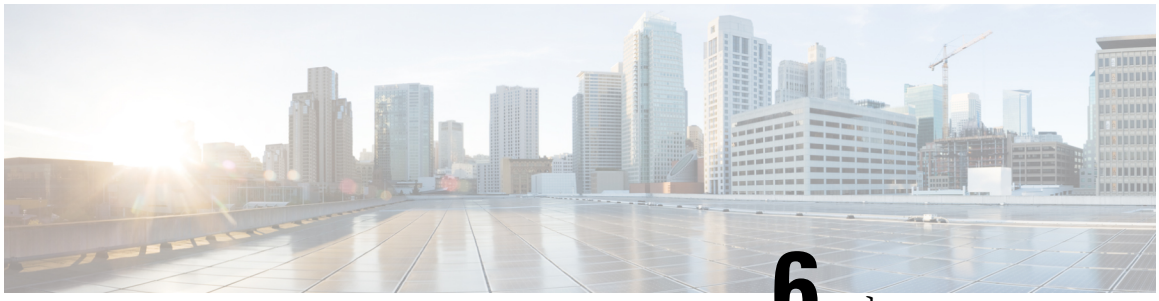
- %FTD-6-806009: Alarm asserted for ALARM_IN_1 *alarm_1_description*(ALARM_IN_1 alarm_1_description에 대해 알람 어셜션됨)
- %FTD-6-806010: Alarm cleared for ALARM_IN_1 *alarm_1_description*(ALARM_IN_1 alarm_1_description에 대한 알람 해제됨)
- %FTD-6-806011: Alarm asserted for ALARM_IN_2 *alarm_2_description*(ALARM_IN_2 alarm_2_description에 대해 알람 어셜션됨)
- %FTD-6-806012: Alarm cleared for ALARM_IN_2 *alarm_2_description*(ALARM_IN_2 alarm_2_description에 대해 알람 해제됨)

외부 알람 끄기

알람 출력에 연결된 외부 알람을 사용 중인 경우, 알람이 트리거되면 **clear facility-alarm output** 명령을 사용하여 디바이스 CLI에서 외부 알람을 끌 수 있습니다. 이 명령은 출력 PIN을 비활성화하며 출력 LED도 끕니다.

II 부

재사용 가능 개체



6 장

개체

개체는 정책이나 기타 설정에서 사용하려는 기준을 정의하는 재사용 가능 컨테이너입니다. 예를 들어 네트워크 개체는 호스트 및 서브넷 주소를 정의합니다.

개체를 사용하면 기준을 정의하여 서로 다른 여러 정책에서 같은 기준을 쉽게 재사용할 수 있습니다. 개체를 업데이트하면 해당 개체를 사용하는 모든 정책이 자동으로 업데이트됩니다.

개체 유형

다음과 같은 유형의 개체를 생성할 수 있습니다. 대부분의 경우에는 정책이나 설정이 개체를 허용하는 경우 개체를 사용해야 합니다.

개체 유형	주요 용도	설명
Secure Client 프로파일	원격 액세스 VPN	Secure Client 프로파일은 Secure Client 소프트웨어와 함께 클라이언트에 다운로드됩니다. 이러한 프로파일은 시작 시의 자동 연결 및 자동 다시 연결, 그리고 엔드 유저가 Secure Client 환경 설정 및 고급 설정에서 옵션을 변경할 수 있는지 여부와 같은 여러 클라이언트 관련 옵션을 정의합니다. 클라이언트 프로파일 구성 및 업로드, 734 페이지의 내용을 참조하십시오.
애플리케이션 필터	액세스 제어 규칙	애플리케이션 필터 개체는 IP 연결에 사용되는 애플리케이션 또는 유형, 범주, 태그, 위험, 사업 타당성에 따라 애플리케이션을 정의하는 필터를 정의합니다. 포트 사양을 사용하는 대신 정책에서 이러한 개체를 사용하여 트래픽을 제어할 수 있습니다. 애플리케이션 필터 개체 구성, 153 페이지의 내용을 참조하십시오.

개체 유형	주요 용도	설명
인증서	ID 정책 원격 액세스 VPN SSL 암호 해독 규칙 관리 웹 서버	디지털 인증서는 인증을 위해 디지털 신원 확인을 담당합니다. 인증서는 HTTPS 및 LDAPS와 같은 SSL(Secure Socket Layer), TLS(Transport Layer) 및 DTLS(Datagram TLS) 연결에 사용됩니다. 인증서 구성, 164 페이지의 내용을 참조하십시오.
DNS 그룹	관리 및 데이터 인터페이스용 DNS 설정	DNS 그룹은 DNS 서버 및 일부 관련 특성의 목록을 정의합니다. www.example.com과 같은 FQDN(Fully Qualified Domain Name)을 IP 주소로 확인하려면 DNS 서버가 필요합니다. DNS 그룹 구성, 826 페이지의 내용을 참조하십시오.
이벤트 목록 필터	선택한 기록 대상에 대한 시스템 기록 설정	이벤트 목록 필터를 사용하면 syslog 메시지에 대한 맞춤형 필터 목록이 생성됩니다. 이 필터를 사용해 syslog 서버 또는 내부 로그 버퍼와 같은 특정 기록 위치로 전송되는 메시지를 제한할 수 있습니다. 이벤트 목록 필터 구성, 817 페이지를 참조하십시오.
지리위치	보안 정책	지리위치 개체는 트래픽의 소스나 대상인 디바이스를 호스팅하는 국가와 대륙을 정의합니다. IP 주소를 사용하는 대신 정책에서 이러한 개체를 사용하여 트래픽을 제어할 수 있습니다. 지리위치 개체 구성, 157 페이지의 내용을 참조하십시오.
ID 소스	ID 정책 원격 액세스 VPN Device Manager 액세스.	ID 소스는 사용자 어카운트를 정의하는 서버와 데이터베이스입니다. 이 정보는 IP 주소와 연결된 사용자 ID를 제공하거나, 원격 액세스 VPN 연결 또는 device manager 액세스를 인증하는 등 다양한 방식으로 사용할 수 있습니다. ID 소스, 173 페이지의 내용을 참조하십시오.
IKE 정책	VPN	IKE(Internet Key Exchange) 정책 개체는 IPsec 피어를 인증하고, IPsec 암호화 키를 협상 및 배포하고, IPsec SA(보안 연계)를 자동으로 설정하는 데 사용되는 IKE 제안을 정의합니다. IKEv1과 IKEv2용으로 별도의 개체가 있습니다. 글로벌 IKE 정책 구성, 694 페이지의 내용을 참조하십시오.
IPSec 제안	VPN	IPsec 제안 개체는 IKE 2단계 협상 중에 사용되는 IPsec 제안을 구성합니다. IPsec 제안은 IPsec 터널에서 트래픽을 보호하는 보안 프로토콜 및 알고리즘 조합을 정의합니다. IKEv1과 IKEv2용으로 별도의 개체가 있습니다. IPsec 제안 구성, 699 페이지의 내용을 참조하십시오.

개체 유형	주요 용도	설명
네트워크	보안 정책 및 다양한 디바이스 설정	네트워크 그룹과 네트워크 개체(네트워크 개체로 총칭함)는 호스트 또는 네트워크의 주소를 정의합니다. 네트워크 개체 및 그룹 구성, 149 페이지의 내용을 참조하십시오.
포트	보안 정책	포트 그룹과 포트 개체(포트 개체로 총칭함)는 트래픽용 프로토콜, 포트 또는 ICMP 서비스를 정의합니다. 포트 개체 및 그룹 구성, 150 페이지의 내용을 참조하십시오.
비밀 키	스마트 CLI 및 FlexConfig 정책	비밀 키 개체는 암호화하여 숨기려는 비밀번호 또는 기타 인증 문자열을 정의합니다. 비밀 키 개체 구성, 931 페이지의 내용을 참조하십시오.
보안 영역	보안 정책	보안 영역은 인터페이스의 그룹입니다. 이러한 영역은 트래픽을 쉽게 관리 및 분류할 수 있도록 네트워크를 세그먼트로 구분합니다. 보안 영역 구성, 152 페이지의 내용을 참조하십시오.
SGT 그룹	액세스 제어 정책	트러스트섹(Trustsec) SGT(Security Group Tag)는 Cisco ISE(Identity Services Engine)에 정의된 대로 트래픽에 대한 태그를 정의합니다. 이러한 개체를 생성하려면 먼저 ISE를 구성해야합니다. 엑세스 제어 규칙에서는 개체를 소스/대상 매칭 기준으로 사용할 수 있습니다. SGT(Security Group Tag) 그룹 구성, 159 페이지의 내용을 참조하십시오.
SLA 모니터	정적 경로	SLA 모니터에서는 정적 경로를 모니터링하는 데 사용할 대상 IP 주소를 정의합니다. 모니터에서 대상 IP 주소에 더 이상 연결할 수 없다고 판단하는 경우, 시스템에서는 백업 정적 경로를 설치할 수 있습니다. SLA 모니터 개체 컨피그레이션, 341 페이지의 내용을 참조하십시오.
SSL 암호	SSL 설정	SSL 암호 개체는 threat defense에 대한 SSL 연결을 설정할 때 사용할 수 있는 보안 레벨, TLS/DTLS 프로토콜 버전 및 암호화 알고리즘의 조합을 정의합니다. 시스템 설정에서 이러한 개체를 사용하여 상자에 TLS/SSL 연결을 수행하는 사용자에 대한 보안 요구 사항을 정의합니다. TLS / SSL 암호 설정 설정, 851 페이지의 내용을 참조하십시오.

개체 유형	주요 용도	설명
Syslog 서버	액세스 제어 규칙 진단 로깅 보안 인텔리전스 정책 SSL 암호 해독 규칙 침입 정책 파일/악성코드 정책	syslog 서버 개체는 연결 지향형 또는 진단 시스템 로그(syslog) 메시지를 수신할 수 있는 서버를 식별합니다. syslog 서버 구성, 157 페이지의 내용을 참조하십시오.
URL	액세스 제어 규칙 보안 인텔리전스 정책	URL 개체 및 그룹(URL 개체로 총칭함)은 웹 요청의 URL 또는 IP 주소를 정의합니다. URL 개체 및 그룹 구성, 155 페이지의 내용을 참조하십시오.
사용자	원격 액세스 VPN	원격 액세스 VPN에 사용할 디바이스에서 직접 사용자 어카운트를 생성할 수 있습니다. 외부 인증 소스 대신 또는 외부 인증 소스와 함께 로컬 사용자 어카운트를 사용할 수 있습니다. 로컬 사용자 구성, 192 페이지의 내용을 참조하십시오.

개체 관리

개체는 개체 페이지를 통해 직접 구성할 수도 있고 정책을 수정하면서 구성할 수도 있습니다. 둘 중 어떤 방법을 사용하든 결과는 같습니다(새 개체가 생성되거나 기존 개체가 업데이트됨). 그러므로 작업 시 필요에 맞는 기술을 사용하면 됩니다.

다음 절차에서는 개체 페이지를 통해 개체를 직접 생성하고 관리하는 방법에 대해 설명합니다.

참고 정책이나 설정을 수정할 때 속성에 개체가 필요한 경우 이미 정의된 개체 목록이 표시되며, 여기서 적절한 개체를 선택합니다. 원하는 개체가 아직 없는 경우 목록에 표시된 **Create New Object(**새 개체 생성**)** 링크를 클릭하면 됩니다.

프로시저

단계 **1** **Objects(**개체**)**를 선택합니다.

개체 페이지에는 사용 가능한 개체 유형이 나열된 목차가 있습니다. 개체 유형을 선택할 때는 기존 개체 목록이 표시되며, 이 목록에서 새 개체를 생성할 수 있습니다. 개체 내용과 유형도 확인할 수 있습니다.

단계 **2** 목차에서 개체 유형을 선택하고 다음 중 원하는 작업을 수행합니다.

- 개체를 생성하려면 + 버튼을 클릭합니다. 개체의 내용은 유형에 따라 다릅니다. 구체적인 정보는 각 개체 유형에 대한 컨피그레이션 주제를 참조하십시오.
- 그룹 개체를 생성하려면 **Add Group(**그룹 추가**)**( ) 버튼을 클릭합니다. 그룹 개체에는 항목이 두 개 이상 포함됩니다.
- 개체를 수정하려면 개체의 수정 아이콘( )을 클릭하십시오. 사전 정의된 개체의 내용은 수정할 수 없습니다.
- 개체를 삭제하려면 개체의 삭제 아이콘( )을 클릭합니다. 정책 또는 다른 개체에서 현재 사용되고 있는 개체 또는 사전 정의된 개체는 삭제할 수 없습니다.

네트워크 개체 및 그룹 구성

네트워크 그룹과 네트워크 개체(네트워크 개체로 총칭함)를 사용하여 호스트 또는 네트워크의 주소를 정의합니다. 그런 후에는 이러한 개체를 보안 정책에서 사용하여 트래픽 일치 기준을 정의하거나, 설정에서 사용하여 서버 또는 기타 리소스의 주소를 정의할 수 있습니다.

네트워크 개체는 단일 호스트 또는 네트워크 주소를 정의하는 반면 네트워크 그룹 개체는 여러 주소를 정의할 수 있습니다.

다음 절차에서는 개체 페이지를 통해 개체를 직접 생성하고 수정할 수 있는 방법을 설명합니다. 개체 목록에 표시되는 **Create New Network(**새 네트워크 생성**)** 링크를 클릭하여 주소 속성을 수정하면서 네트워크 개체를 생성할 수도 있습니다.

프로시저

단계 **1** 목차에서 **Objects(**개체**)**와 **Network(**네트워크**)**를 차례로 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 개체를 생성하려면 + 버튼을 클릭합니다.
- 그룹을 생성하려면 **Add Group(**그룹 추가**)**( ) 버튼을 클릭합니다.
- 개체 또는 그룹을 수정하려면 개체의 수정 아이콘( )을 클릭하십시오.

참조되지 않는 개체를 삭제하려면 해당 개체의 휴지통 아이콘( )을 클릭합니다.

단계 **3** 개체의 이름과 설명(선택 사항)을 입력하고 개체 콘텐츠를 정의합니다.

개체 콘텐츠 또는 독립형 IP 주소에서 개체 이름을 쉽게 확인할 수 있도록 해당 이름에 IP 주소만 사용하지 않는 것이 좋습니다. 이름에 IP 주소를 사용하려는 경우, host-192.168.1.2 또는 network-192.168.1.0 같이 의미 있는 접두사를 붙이십시오. 이름으로 IP 주소를 사용하는 경우 시스템은 접두사로 수직 바

를 추가합니다(예:192.168.1.2). Device Manager에서는 개체 선택기에 막대를 표시하지 않지만, CLI에서 **show running-config**명령을 사용하여 실행 중인 컨피그레이션을 검토하는 경우에는 이 명명 표준을 표시합니다.

단계 **4** 개체의 콘텐츠를 컨피그레이션합니다.

네트워크 개체

개체 **Type(**유형**)**을 선택하고 내용을 구성합니다.

- **Network(**네트워크**)** - 다음 형식 중 하나를 사용하여 네트워크 주소를 입력합니다.
  - 서브넷 마스크가 포함된 IPv4 주소(예: 10.100.10.0/24 또는 10.100.10.0/255.255.255.0)
  - 접두사가 포함된 IPv6 네트워크 주소(예: 2001:DB8:0:CD30::/60)
- **Host(**호스트**)** - 다음 형식 중 하나를 사용하여 호스트 IP 주소를 입력합니다.
  - IPv4 호스트 주소(예: 10.100.10.10)
  - IPv6 호스트주소(예: 2001:DB8::0DB8:800:200C:417A 또는 2001:DB8:0:0:0DB8:800:200C:417A)
- **Range(**범위**)** - 주소의 범위입니다. 시작 및 종료 주소는 하이픈으로 구분합니다. IPv4 또는 IPv6 범위를 지정할 수 있습니다. 마스크 또는 접두사를 포함하지 않습니다. 192.168.1.10-192.168.1.250 또는 2001:DB8:0:CD30::10-2001:DB8:0:CD30::100을 예로 들 수 있습니다.
- **FQDN** - www.example.com과 같은 단일 FQDN(Fully Qualified Domain Name)을 입력합니다. 와일드카드는 사용할 수 없습니다. 또한 **DNS Resolution(DNS** 확인**)**을 선택하여 사용하려는 주소(FQDN과 연결된 IPv4, IPv6 주소 중 하나 또는 두 가지 모두)를 결정합니다. 기본적으로는 IPv4와 IPv6이 모두 사용됩니다. 이러한 개체는 액세스 제어 규칙에서만 사용할 수 있습니다. 규칙은 DNS 조회를 통해 FQDN에서 획득한 IP 주소와 일치 여부를 확인합니다.

네트워크 그룹

+ 버튼을 클릭하여 그룹에 추가할 네트워크 개체 또는 그룹을 선택합니다. 새 개체를 생성할 수도 있습니다.

단계 **5** **OK(**확인**)**를 클릭하여 변경 사항을 저장합니다.

포트 개체 및 그룹 구성

포트 그룹과 포트 개체(포트 개체로 총칭함)를 사용하여 트래픽용 프로토콜, 포트 또는 ICMP 서비스를 정의합니다. 그런 후에는 이러한 개체를 보안 정책에서 사용하여 트래픽 일치 기준(예: 특정 TCP 포트에 대한 트래픽을 허용하는 액세스 규칙을 사용하기 위한 기준)을 정의할 수 있습니다.

포트 개체는 단일 프로토콜, TCP/UDP 포트나 포트 범위 또는 ICMP 서비스를 정의하는 반면 포트 그룹 개체는 여러 서비스를 정의할 수 있습니다.

시스템에는 일반 서비스를 위해 사전 정의된 개체가 여러 개 포함되어 있으며, 정책에서 이러한 개체를 사용할 수 있습니다. 그러나 시스템 정의 개체는 수정하거나 삭제할 수 없습니다.

참고 포트 그룹 개체를 생성할 때는 개체 조합이 적절한지 확인합니다. 예를 들어 개체를 사용해 액세스 규칙에서 소스 포트와 대상 포트를 모두 지정하는 경우에는 해당 개체 내에 프로토콜을 혼합하여 포함할 수 없습니다. 이미 사용 중인 개체를 수정할 때는 주의해야 합니다. 해당 개체를 사용하는 정책이 무효화되고 비활성화될 수 있기 때문입니다.

다음 절차에서는 개체 페이지를 통해 개체를 직접 생성하고 수정할 수 있는 방법을 설명합니다. 개체 목록에 표시되는 **Create New Port(**새 포트 생성**)** 링크를 클릭하여 서비스 속성을 수정하면서 포트 개체를 생성할 수도 있습니다.

프로시저

단계 **1** 목차에서 **Objects(**개체**)**와 **Ports(**포트**)**를 차례로 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 개체를 생성하려면 + 버튼을 클릭합니다.
- 그룹을 생성하려면 **Add Group(**그룹 추가**)**( ) 버튼을 클릭합니다.
- 개체 또는 그룹을 수정하려면 개체의 수정 아이콘( )을 클릭하십시오.

참조되지 않는 개체를 삭제하려면 해당 개체의 휴지통 아이콘( )을 클릭합니다.

단계 **3** 개체의 이름과 설명(선택 사항)을 입력하고 개체 콘텐츠를 정의합니다.

포트 개체

프로토콜을 선택하고 다음과 같이 프로토콜을 구성합니다.

- **TCP**, **UDP** - 80(HTTP) 또는 1~65535(모든 포트 포함)와 같이 단일 포트 또는 포트 범위 번호를 입력합니다.
- **ICMP**, **IPv6-ICMP** - ICMP 유형을 선택하고 필요한 경우 코드를 선택합니다. 해당 유형을 모든 ICMP 메시지에 적용하려면 모두를 선택합니다. 유형과 코드에 대한 자세한 내용은 다음 페이지를 참조하십시오.
  - ICMP -http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml
  - ICMPv6 -http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml
- 기타 - 원하는 프로토콜을 선택합니다.

포트 그룹

+ 버튼을 클릭하여 그룹에 추가할 포트 개체를 선택합니다. 새 개체를 생성할 수도 있습니다.

단계 **4** **OK(**확인**)**를 클릭하여 변경 사항을 저장합니다.

보안 영역 구성

보안 영역은 인터페이스의 그룹입니다. 이러한 영역은 트래픽을 쉽게 관리 및 분류할 수 있도록 네트워크를 세그먼트로 구분합니다. 여러 영역을 정의할 수 있지만, 지정된 인터페이스는 하나의 영역에만 속할 수 있습니다.

시스템은 초기 컨피그레이션 시 다음 영역을 생성합니다. 이러한 영역을 수정하여 인터페이스를 추가하거나 제거할 수도 있고, 더 이상 사용하지 않는 영역을 삭제할 수도 있습니다.

- **inside_zone** - 내부 인터페이스를 포함합니다. 내부 인터페이스가 브리지 그룹인 경우 이 영역에는 내부 BVI(브리지 가상 인터페이스) 대신 모든 브리지 그룹 멤버 인터페이스가 포함됩니다. 이 영역은 내부 네트워크를 나타내는 데 사용됩니다.
- **outside_zone** - 외부 인터페이스를 포함합니다. 이 영역은 인터넷 등 제어 범위 외부에 있는 네트워크를 나타내는 데 사용됩니다.

일반적으로는 인터페이스가 네트워크에서 수행하는 역할별로 인터페이스를 그룹화합니다. 예를 들어 인터넷에 연결하는 인터페이스는 **outside_zone** 보안 영역에 배치하고 내부 네트워크용의 모든 인터페이스는 **inside_zone** 보안 영역에 배치합니다. 그러면 외부 영역에서 들어오는 트래픽과 내부 영역으로 이동하는 트래픽에 액세스 제어 규칙을 적용할 수 있습니다.

영역을 생성하기 전에 네트워크에 적용할 액세스 규칙 및 기타 정책을 고려하십시오. 예를 들어 모든 내부 인터페이스를 같은 영역에 배치할 필요는 없습니다. 내부 네트워크가 4개인데 그중 하나를 나머지 3개와 다른 방식으로 취급하려는 경우에는 영역을 하나가 아닌 두 개 생성할 수 있습니다. 공개 웹 서버에 대한 외부 액세스를 허용해야 하는 인터페이스가 있는 경우에는 해당 인터페이스용으로 별도의 영역을 사용할 수 있습니다.

다음 절차에서는 개체 페이지를 통해 개체를 직접 생성하고 수정할 수 있는 방법을 설명합니다. 개체 목록에 표시되는 **Create New Security Zone(**새 보안 영역 생성**)** 링크를 클릭하여 보안 영역 속성을 수정하면서 보안 영역을 생성할 수도 있습니다.

프로시저

단계 **1** 목차에서 **Objects(**개체**)**와 **Security Zones(**보안 영역**)**을 차례로 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 개체를 생성하려면 **+** 버튼을 클릭합니다.
- 개체를 수정하려면 개체의 수정 아이콘( )을 클릭하십시오.

참조되지 않는 개체를 삭제하려면 해당 개체의 휴지통 아이콘( )을 클릭합니다.

단계 **3** 개체의 Name(이름) 및 설명(선택 사항)을 입력합니다.

단계 **4** 해당 영역의 **Mode(**모드**)**를 선택합니다.

모드는 인터페이스 모드(**Routed(**라우티드**)** 또는 **Passive(**패시브**)**)와 직접 관련이 있습니다. 해당 영역은 단일 인터페이스 유형을 포함할 수 있습니다. 통과 트래픽용 기본 영역의 경우 **Routed(**라우팅**)**를 선택합니다.

단계 **5** 인터페이스 목록에서 +를 클릭하고 영역에 추가할 인터페이스를 선택합니다.

목록에는 현재 영역에 포함되어 있지 않고 이름이 지정된 인터페이스가 모두 표시됩니다. 인터페이스를 구성하고 이름을 지정해야 영역에 추가할 수 있습니다.

이름이 지정된 인터페이스가 모두 이미 영역에 포함되어 있으면 이 목록은 비게 됩니다. 다른 영역으로 인터페이스를 이동하려는 경우에는 먼저 현재 영역에서 인터페이스를 제거해야 합니다.

참고 BVI(브리지 그룹 인터페이스)는 영역에 추가할 수 없습니다. 대신 멤버 인터페이스를 추가합니다. 멤버는 다른 영역에 배치할 수 있습니다.

단계 **6** **OK(**확인**)**를 클릭하여 변경 사항을 저장합니다.

애플리케이션 필터 개체 구성

애플리케이션 필터 개체는 IP 연결에 사용되는 애플리케이션 또는 유형, 범주, 태그, 위험, 사업 타당성에 따라 애플리케이션을 정의하는 필터를 정의합니다. 포트 사양을 사용하는 대신 정책에서 이러한 개체를 사용하여 트래픽을 제어할 수 있습니다.

개별 애플리케이션을 지정할 수 있으나 애플리케이션 필터를 사용하면 정책 생성 및 관리가 간소화됩니다. 예를 들어, 위험도가 높고 비즈니스 관련성이 낮은 모든 애플리케이션을 식별하여 차단하는 액세스 제어 규칙을 만들 수 있습니다. 사용자가 이러한 애플리케이션 중 하나를 사용하려고 할 경우, 세션은 차단됩니다.

애플리케이션 필터 개체를 사용하지 않고 정책에서 애플리케이션과 애플리케이션 필터를 직접 선택할 수 있습니다. 그러나 애플리케이션 또는 필터의 동일 그룹에 대해 여러 정책을 생성하려는 경우에는 개체를 사용하는 것이 편리합니다. 시스템에는 수정하거나 삭제할 수 없는 사전 정의된 여러 애플리케이션 필터가 포함되어 있습니다.

참고 Cisco에서는 시스템 및 VDB(Vulnerability Database) 업데이트를 통해 추가 애플리케이션 탐지기를 자주 업데이트하고 추가합니다. 따라서 규칙을 수동으로 업데이트하지 않아도 위험도가 높은 애플리케이션을 차단하는 규칙이 새 애플리케이션에 자동으로 적용될 수 있습니다.

다음 절차에서는 개체 페이지를 통해 개체를 직접 생성하고 수정할 수 있는 방법을 설명합니다. 애플리케이션 탭에 애플리케이션 기준을 추가한 후에 **Save As Filter(**필터로 저장**)** 링크를 클릭하여 액세스 제어 규칙을 수정하는 동안 애플리케이션 필터 개체를 생성할 수도 있습니다.

시작하기 전에

선택한 애플리케이션이 VDB 업데이트를 통해 제거된 경우 필터를 수정할 때 애플리케이션 이름 뒤에 "(Deprecated(사용되지 않음))"이라고 표시됩니다. 이러한 애플리케이션은 필터에서 제거해야 합니다. 그렇지 않으면 후속 구축 및 시스템 소프트웨어 업그레이드가 차단됩니다.

프로시저

단계 **1** 목차에서 **Objects(**개체**)**와 **Application Filters(**애플리케이션 필터**)**를 차례로 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 개체를 생성하려면 + 버튼을 클릭합니다.
- 개체를 수정하려면 개체의 수정 아이콘()을 클릭하십시오.

참조되지 않는 개체를 삭제하려면 해당 개체의 휴지통 아이콘()을 클릭합니다.

단계 **3** 개체의 Name(이름) 및 설명(선택 사항)을 입력합니다.

단계 **4** 애플리케이션 목록에서 추가 +를 클릭하고 개체에 추가할 애플리케이션 및 필터를 선택합니다.

초기 목록(계속 스크롤 가능)에는 애플리케이션이 표시됩니다. 고급 필터를 클릭하면 필터 옵션을 확인하고 애플리케이션을 더 쉽게 선택할 수 있는 보기를 표시할 수 있습니다. 원하는 항목을 선택한 후 **Add(**추가**)**를 클릭합니다. 이 프로세스를 반복하여 애플리케이션이나 필터를 더 추가할 수 있습니다.

참고 단일 필터 기준으로 여러 선택 항목이 OR 관계를 갖습니다. 예를 들어, 위험은 높음 OR 매우 높음입니다. 반면 필터 간의 관계는 AND입니다. 즉, 위험은 높음 OR 매우 높음 AND 사업 타당성은 낮음 OR 매우 낮음과 같습니다. 필터를 선택하면 디스플레이의 애플리케이션 목록이 업데이트되어 기준을 충족하는 애플리케이션만 표시됩니다. 이러한 필터를 사용하여 개별적으로 추가하려는 애플리케이션을 찾거나, 규칙에 추가할 적절한 필터를 선택하고 있는지를 확인할 수 있습니다.

위험

애플리케이션이 조직의 보안 정책과 상반되는 용도로 사용될 가능성(매우 낮음~매우 높음)

사업 타당성

조직의 비즈니스 운영(레크리에이션과 반대) 컨텍스트 내에서 애플리케이션이 사용될 가능성(매우 낮음~매우 높음)

유형

애플리케이션 유형:

- 애플리케이션 프로토콜 - 호스트 간의 통신을 나타내는 HTTP, SSH 등의 애플리케이션 프로토콜
- 클라이언트 프로토콜 - 호스트에서 실행 중인 소프트웨어를 나타내는 웹 브라우저, 이메일 클라이언트 등의 클라이언트
- 웹 애플리케이션 - HTTP 트래픽의 요청 URL 또는 콘텐츠를 나타내는 MPEG 비디오, Facebook 등의 웹 애플리케이션

범주

가장 중요한 기능을 설명하는 일반 애플리케이션 분류

태그

애플리케이션에 대한 추가 정보로, 범주와 비슷합니다.

암호화된 트래픽의 경우, 시스템은 **SSL** 프로토콜 태그가 지정된 애플리케이션만 사용하여 트래픽을 식별하고 필터링할 수 있습니다. 이 태그가 없는 애플리케이션은 암호화되지 않은 트래픽 또는 해독된 트래픽에서만 탐지할 수 있습니다. 또한 암호화된 트래픽 또는 암호화되지 않은 트래픽이 아닌 암호 해독된 트래픽에서만 탐지할 수 있는 애플리케이션에는 암호 해독된 트래픽 태그가 할당됩니다.

애플리케이션 목록**(**디스플레이 하단**)**

이 목록은 목록 위의 옵션에서 필터를 선택하면 업데이트되므로 현재 필터와 일치하는 애플리케이션을 확인할 수 있습니다. 이 목록을 사용하여 규칙에 필터 기준을 추가하려는 경우 필터가 적절한 애플리케이션을 대상으로 하는지를 확인할 수 있습니다. 특정 애플리케이션을 추가하려는 경우 이 목록에서 선택합니다.

단계 **5** **OK(**확인**)**를 클릭하여 변경 사항을 저장합니다.

URL 개체 및 그룹 구성

URL 개체 및 그룹(URL 개체로 총칭함)을 사용하여 웹 요청의 URL 또는 IP 주소를 정의합니다. 이러한 개체를 사용하여 액세스 제어 정책에서 수동 URL 필터링 또는 보안 인텔리전스 정책에서 차단 기능을 구현할 수 있습니다.

URL 개체는 단일 URL 또는 IP 주소를 정의하는 반면 URL 그룹 개체는 여러 URL 또는 주소를 정의할 수 있습니다.

URL 개체를 생성할 때는 다음 사항에 유의하십시오.

- 경로를 포함하지 않는 경우(즉, URL에 / 문자가 없음), 이 일치는 서버의 호스트 이름만을 기준으로 합니다. 호스트 이름은 :// 구분자 뒷부분 또는 호스트 이름의 의 뒷부분이 같아야 일치하는 것으로 간주됩니다. 예를 들어 ign.com은 ign.com 및 www.ign.com과 일치하지만 verisign.com과는 일치하지 않습니다.
- 하나 이상의 / 문자를 포함하는 경우, 전체 URL 문자열이 서버 이름, 경로 및 쿼리 파라미터를 비롯한 부분 문자열 일치에 사용됩니다. 그러나 서버가 재구성되고 페이지가 새 경로로 이동될 수 있으므로 개별 웹 페이지 또는 사이트 일부를 차단하거나 허용하기 위해 수동 URL 필터링은 사용하지 않는 것이 좋습니다. 부분 문자열 일치는 예기치 않은 일치로 이어질 수도 있으며, 이 경우에는 URL 개체에 포함하는 문자열도 쿼리 파라미터 내부에 있는 의도하지 않은 서버 또는 문자열의 경로와 일치됩니다.
- 시스템에서는 암호화 프로토콜(HTTP 대 HTTPS)을 무시합니다. 다시 말해, 특정 웹 사이트를 차단하는 경우 애플리케이션 조건을 사용하여 특정 프로토콜을 대상으로 하지 않는 한 해당 웹 사이트에 대한 HTTP 및 HTTPS 트래픽이 모두 차단됩니다. URL 개체를 생성할 때에는 개체 생성 시 프로토콜을 지정할 필요가 없습니다. 이를테면 http://example.com 대신 example.com을 사용하십시오.
- URL 개체를 사용하여 액세스 제어 규칙에서 HTTPS 트래픽을 매칭하려는 경우, 트래픽 암호화에 사용되는 공개 키 인증서에서 주체 CN을 사용하여 개체를 생성합니다. 또한 주체 CN에 포함

된 하위 도메인은 무시되므로 하위 도메인 정보를 포함하지 마십시오. 이를테면 www.example.com 대신 example.com을 사용하십시오.

그러나 인증서의 주체 일반 이름은 웹 사이트의 도메인 이름과 아무런 관련도 없을 수 있습니다. 예를 들어, youtube.com 인증서의 주체 일반 이름은 *.google.com입니다(언제든 변경 가능). URL 필터링 규칙이 암호 해독된 트래픽에서 작동하도록 SSL 암호 해독 정책을 사용하여 HTTPS 트래픽을 암호 해독하면 더 일관성 있는 결과를 얻게 됩니다.

참고 인증서 정보를 더 이상 사용할 수 없어 브라우저에서 TLS 세션을 다시 시작하는 경우에는 URL 개체가 HTTPS 트래픽과 일치되지 않습니다. 따라서 URL 개체를 주의하여 구성하더라도 HTTPS 연결에 대해 일관성 없는 결과를 얻을 수 있습니다.

다음 절차에서는 개체 페이지를 통해 개체를 직접 생성하고 수정할 수 있는 방법을 설명합니다. 개체 목록에 표시되는 **Create New URL(**새 **URL** 생성**)** 링크를 클릭하여 URL 속성을 수정하면서 URL 개체를 생성할 수도 있습니다.

프로시저

단계 **1** 목차에서 **Objects(**개체**)**와 **URL**을 차례로 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 개체를 생성하려면 **+** 버튼을 클릭합니다.
- 그룹을 생성하려면 **Add Group(**그룹 추가**)**( ) 버튼을 클릭합니다.
- 개체 또는 그룹을 수정하려면 개체의 수정 아이콘( )을 클릭하십시오.

참조되지 않는 개체를 삭제하려면 해당 개체의 휴지통 아이콘( )을 클릭합니다.

단계 **3** 개체의 Name(이름) 및 설명(선택 사항)을 입력합니다.

단계 **4** 개체 콘텐츠를 정의합니다.

URL 개체

URL 상자에 URL 또는 IP 주소를 입력합니다. URL에는 와일드카드를 사용할 수 없습니다.

URL 그룹

+ 버튼을 클릭하여 그룹에 추가할 URL 개체를 선택합니다. 새 개체를 생성할 수도 있습니다.

단계 **5** **OK(**확인**)**를 클릭하여 변경 사항을 저장합니다.

지리위치 개체 구성

지리위치 개체는 트래픽의 소스나 대상인 디바이스를 호스팅하는 국가와 대륙을 정의합니다. IP 주소를 사용하는 대신 정책에서 이러한 개체를 사용하여 트래픽을 제어할 수 있습니다. 지리적 위치를 사용하면 특정 국가에서 사용될 수 있는 모든 IP 주소를 몰라도 해당 국가에 대한 액세스를 쉽게 제한할 수 있습니다.

일반적으로는 지리위치 개체를 사용하지 않고 정책에서 직접 지리적 위치를 선택합니다. 그러나 국가와 대륙의 동일 그룹에 대해 여러 정책을 생성하려는 경우에는 개체를 사용하는 것이 편리합니다.

참고 최신 지리적 위치 데이터를 사용하여 트래픽을 필터링하려면 GeoDB(geolocation database)를 정기적으로 업데이트하는 것이 좋습니다.

다음 절차에서는 개체 페이지를 통해 개체를 직접 생성하고 수정할 수 있는 방법을 설명합니다. 개체 목록에 표시되는 **Create New Geolocation(**새 지리위치 생성**)** 링크를 클릭하여 네트워크 속성을 수정하면서 지리위치 개체를 생성할 수도 있습니다.

프로시저

단계 **1** 목차에서 **Objects(**개체**)**와 **Geolocation(**지리위치**)**을 차례로 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 개체를 생성하려면 **+** 버튼을 클릭합니다.
- 개체를 수정하려면 개체의 수정 아이콘( )을 클릭하십시오.

참조되지 않는 개체를 삭제하려면 해당 개체의 휴지통 아이콘( )을 클릭합니다.

단계 **3** 개체의 Name(이름) 및 설명(선택 사항)을 입력합니다.

단계 **4** 국가/대륙 목록에서 추가 **+**를 클릭하고 개체에 추가할 국가 및 대륙을 선택합니다.

대륙을 선택하면 대륙 내의 모든 국가가 선택됩니다.

단계 **5** **OK(**확인**)**를 클릭하여 변경 사항을 저장합니다.

syslog 서버 구성

syslog 서버 개체는 연결 지향형 또는 진단 시스템 로그(syslog) 메시지를 수신할 수 있는 서버를 식별합니다. 로그 수집 및 분석을 위해 syslog 서버를 설정한 경우, 개체를 생성하여 정의한 후 관련 정책에서 이 개체를 사용합니다.

다음 유형의 이벤트를 syslog 서버에 전송할 수 있습니다.

- 연결 이벤트. 액세스 제어 규칙 및 기본 작업, SSL 암호 해독 규칙 및 기본 작업, 보안 인텔리전스 정책과 같은 유형의 정책에서 syslog 서버 개체를 구성합니다.
- 침입 이벤트. 침입 정책에서 syslog 서버 개체를 구성합니다.
- 진단 이벤트. 원격 Syslog 서버에 대한 기록 컨피그레이션, 815 페이지를 참조하십시오.
- 파일/악성코드 이벤트입니다. **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Logging Settings(**기록 설정**)**에서 syslog 서버를 컨피그레이션하십시오.

다음 절차에서는 개체 페이지를 통해 개체를 직접 생성하고 수정할 수 있는 방법을 설명합니다. 개체 목록에 표시되는 **Add Syslog Server(Syslog** 서버 추가**)** 링크를 클릭하여 syslog 서버 속성을 수정하면서 syslog 서버 개체를 생성할 수도 있습니다.

프로시저

단계 **1** 목차에서 개체와 **Syslog** 서버를 차례로 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 개체를 생성하려면 **+** 버튼을 클릭합니다.
- 개체를 수정하려면 개체의 수정 아이콘()을 클릭하십시오.

참조되지 않는 개체를 삭제하려면 해당 개체의 휴지통 아이콘()을 클릭합니다.

단계 **3** syslog 서버 속성을 구성합니다.

- **IP** 주소 - syslog 서버의 IP 주소를 입력합니다.
- **Protocol Type(**프로토콜 유형**)**, **Port Number(**포트 번호**)** - syslog에 사용할 프로토콜을 선택하고 포트 번호를 입력합니다. 기본값은 UDP/514입니다. **TCP**를 선택하는 경우 시스템은 syslog 서버를 사용할 수 없는 경우를 인식할 수 있으며, 서버를 다시 사용할 수 있을 때까지 이벤트 전송을 중지합니다. 기본 UDP 포트는 514이고 기본 TCP 포트는 1470입니다. 기본값을 변경하는 경우에는 포트가 1025~65535 범위에 포함되어야 합니다.

  참고 TCP를 전송 프로토콜로 사용하는 경우 시스템은 메시지가 손실되지 않도록 syslog 서버에 대한 4개의 연결을 엽니다. syslog 서버를 사용하여 매우 많은 수의 디바이스에서 메시지를 수집하는 경우 결합된 연결 오버헤드가 서버에 비해 너무 많은 경우 UDP를 대신 사용합니다.

- **Interface for Device Logs(**디바이스 로그용 인터페이스**)** - 진단 syslog 메시지를 보내는 데 사용해야 하는 인터페이스를 선택합니다. 연결, 침입, 파일, 악성코드 이벤트 유형에서는 항상 관리 인터페이스를 사용합니다. 선택하는 인터페이스에 따라 syslog 메시지와 연결되는 IP 주소가 결정됩니다. 다음 옵션 중 하나를 선택합니다.
  - **Data Interface(**데이터 인터페이스**)** - 진단 syslog 메시지에 대해 선택하는 데이터 인터페이스를 사용합니다. 브리지 그룹 멤버 인터페이스를 통해 서버에 액세스할 수 있는 경우에는 BVI(브리지 그룹 인터페이스)를 대신 선택합니다.진단 인터페이스(물리적 관리 인터페이

스)를 통해 서버에 액세스할 수 있는 경우에는 이 옵션 대신 **Management Interface(**관리 인터페이스**)**를 선택하는 것이 좋습니다. 패시브 인터페이스는 선택할 수 없습니다.

연결, 침입, 파일 및 악성코드 syslog 메시지의 경우 소스 IP 주소는 관리 인터페이스용 또는 게이트웨이 인터페이스용(데이터 인터페이스를 통해 라우팅하는 경우)입니다. 이러한 이벤트 유형에 대해 선택된 인터페이스에서 syslog 서버로의 트래픽을 전송하는 라우팅 테이블에 적절한 경로가 있어야 합니다.

- **Management Interface(**관리 인터페이스**)** - 모든 유형의 syslog 메시지에 대해 가상 관리 인터페이스를 사용합니다. 소스 IP 주소는 관리 인터페이스용이거나, 데이터 인터페이스를 통해 라우팅하는 경우 게이트웨이 인터페이스용입니다.

단계 **4** **OK(**확인**)**를 클릭하여 변경 사항을 저장합니다.

SGT(Security Group Tag) 그룹 구성

ISE(Identity Services Engine)에서 할당한 SGT를 기반으로 소스 또는 대상 주소를 식별하려면 SGT(Security Group Tag) 그룹 개체를 사용합니다. 그 다음 트래픽 일치 기준을 정의하는 목적으로 액세스 제어 규칙의 개체를 사용할 수 있습니다.

ISE에서 검색된 정보는 액세스 제어 규칙에서 바로 사용할 수 없습니다. 대신, 다운로드한 SGT 정보를 참조하는 SGT 그룹을 생성해야 합니다. SGT 그룹에서는 둘 이상의 SGT를 참조할 수 있으므로 적절한 경우 관련된 태그 컬렉션을 기준으로 정책을 적용할 수 있습니다.

엑세스 제어를 위한 SGT 사용 방법에 대한 자세한 내용은 TrustSec SGT(Security Group Tag)를 사용하여 네트워크 액세스를 제어하는 방법, 546 페이지를 참조하십시오.

시작하기 전에

SGT 그룹을 생성하기 전에 SXP 매핑을 구독하고 변경 사항을 구축하도록 ISE ID 소스를 구성해야 합니다. 그 다음 시스템은 ISE 서버에서 SGT 정보를 검색합니다. SGT를 다운로드한 후에만 SGT 그룹을 생성할 수 있습니다.

프로시저

단계 **1** 목차에서 **Objects(**개체**)**와 **SGT Groups(SGT** 그룹**)**을 차례로 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 개체를 생성하려면 **+** 버튼을 클릭합니다.
- 개체를 수정하려면 개체의 수정 아이콘()을 클릭하십시오.

참조되지 않는 개체를 삭제하려면 해당 개체의 휴지통 아이콘()을 클릭합니다.

단계 **3** 개체의 **Name(**이름**)** 및 설명(선택 사항)을 입력합니다.

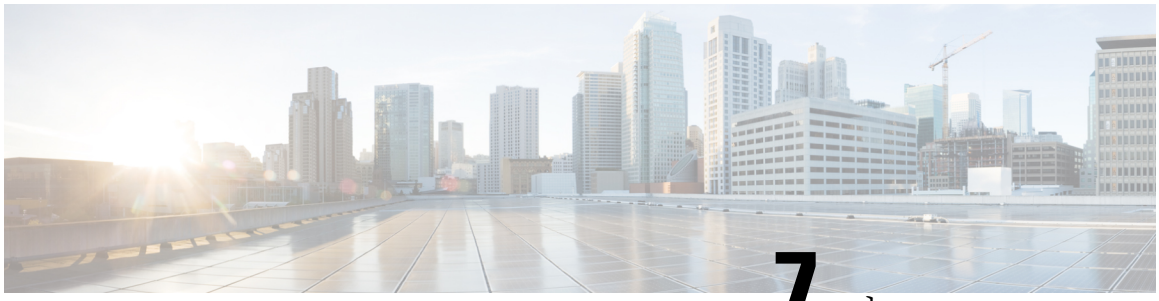
단계 **4** **Tags(**태그**)**에서 **+**를 클릭하고 개체에 포함할 다운로드된 SGT를 선택합니다.

SGT를 제거하려면 태그 이름 오른쪽에 있는 **x**를 클릭합니다.

목록이 비어 있으면 시스템에서 SGT 매핑을 다운로드할 수 없습니다. 이러한 경우에는 다음을 수행합니다.

- ISE ID 개체가 SXP 주제를 구독하고 있는지 확인합니다. 매핑을 가져오려면 SXP를 구독해야 합니다.
- 정적 매핑이 ISE에 정의되어 있고 ISE가 이러한 매핑을 게시하도록 구성되어 있는지 확인합니다. 매핑이 없는 경우에는 다운로드할 것이 없습니다. ISE에서 보안 그룹 및 SXP 게시 구성, 549 페이지의 내용을 참조하십시오.

단계 **5** **OK(**확인**)**를 클릭합니다.



7 장

인증서

디지털 인증서는 인증을 위해 디지털 신원 확인을 담당합니다. 인증서는 HTTPS 및 LDAPS와 같은 SSL(Secure Socket Layer), TLS(Transport Layer) 및 DTLS(Datagram TLS) 연결에 사용됩니다. 다음 주제에서는 인증서를 생성하고 관리하는 방법에 대해 설명합니다.

인증서 정보

디지털 인증서는 인증을 위해 디지털 신원 확인을 담당합니다. 디지털 인증서에는 어떤 디바이스나 사용자를 식별하는 정보, 이를테면 이름, 일련 번호, 회사, 부서 또는 IP 주소가 들어 있습니다. 디지털 인증서는 사용자 또는 디바이스의 공개 키 사본 하나도 포함합니다. 인증서는 HTTPS 및 LDAPS와 같은 SSL(Secure Socket Layer), TLS(Transport Layer) 및 DTLS(Datagram TLS) 연결에 사용됩니다.

다음과 같은 인증서 유형을 생성할 수 있습니다.

- 내부 인증서 — 내부 ID 인증서는 특정 시스템 또는 호스트용 인증서입니다. 이러한 인증서는 OpenSSL 툴킷을 사용하여 직접 생성하거나 인증 기관에서 받을 수 있습니다. 자체 서명 인증서를 생성할 수도 있습니다.
- 내부 CA(Certificate Authority) 인증서 — 내부 CA 인증서는 시스템에서 다른 인증서를 서명하는 데 사용할 수 있는 인증서입니다. 이러한 인증서는 CA 인증서에는 활성화되지만 ID 인증서에는 비활성화되는 기본 제약 조건 확장 및 CA 플래그와 관련된 내부 ID 인증서와 다릅니다. 이러한 인증서는 OpenSSL 툴킷을 사용하여 직접 생성하거나 인증 기관에서 받을 수 있습니다. 자체 서명된 내부 CA 인증서를 생성할 수도 있습니다. 자체 서명된 내부 CA 인증서를 구성할 경우, CA는 디바이스 자체에서 실행됩니다.
- 신뢰할 수 있는 CA(Certificate Authority) 인증서 — 신뢰할 수 있는 CA 인증서는 다른 인증서에 서명하는 데 사용됩니다. 자체 서명되며 루트 인증서라고도 합니다. 다른 CA 인증서를 통해 발급된 인증서는 하위 인증서라고 합니다.

CA(인증 증명)는 인증서에 "서명"하여 그 진위를 확인함으로써 해당 디바이스 또는 사용자의 ID를 보장하는 신뢰받는 기관입니다. CA는 PKI 컨텍스트에서 디지털 인증서를 발급하는데, PKI에서는 공개 키 또는 개인 키 암호화를 사용하여 보안을 보장합니다. CA는 VeriSign과 같이 신뢰받는 서드파티

이거나, 조직 내에서 설정한 전용 (내부) CA일 수 있습니다. CA는 인증서 요청을 관리하고 디지털 인증서를 발급하는 기능을 담당합니다. 자세한 내용은 공개 키 암호화, 162 페이지를 참고하십시오.

공개 키 암호화

RSA 암호화 시스템과 같은 공개 키 암호 방식에서는 각 사용자가 공개 키와 개인 키로 구성된 키 쌍을 갖습니다. 키는 상호 보완적 역할을 하는데, 둘 중 하나의 키로 암호화된 것은 다른 하나의 키를 사용하여 해독할 수 있습니다.

간단하게 설명하자면, 개인 키를 사용하여 데이터를 암호화할 때 서명이 생성됩니다. 이 서명이 데이터에 첨부되어 수신자에게 전송됩니다. 수신자는 발신자의 공개 키를 데이터에 적용합니다. 데이터와 함께 보내진 서명이 공개 키를 데이터에 적용한 결과와 일치하면 메시지가 유효한 것으로 확인됩니다.

이 프로세스에서는 수신자가 발신자의 공개 키 사본을 가지고 있어야 하며 이 키가 발신자를 가장하는 누군가가 아닌 발신자 본인의 것이어야 합니다.

발신자의 공개 키를 취득하는 것은 대개 외부에서 이루어지거나 설치 시 수행되는 어떤 작업을 통해 이루어집니다. 예를 들어, 대부분의 웹 브라우저는 기본적으로 여러 CA의 루트 인증서가 구성되어 있습니다.

openssl.org, Wikipedia 또는 기타 출처를 통해 디지털 인증서와 공개 키 암호화에 대해 자세히 알아볼 수 있습니다. SSL/TLS 암호화에 대해 숙지하면 디바이스에 대한 보안 연결을 쉽게 설정할 수 있습니다.

기능에 사용되는 인증서 유형

각 기능에 대해 적절한 유형의 인증서를 생성해야 합니다. 인증서가 필요한 기능은 다음과 같습니다.

ID 정책**(**캡티브 포털**) -** 내부 인증서

(선택 사항). 캡티브 포털은 ID 정책에 사용됩니다. 사용자는 신원을 증명하고 IP 주소를 사용자 이름과 연결하기 위해 디바이스에 인증할 때 이 인증서를 수락해야 합니다. 인증서를 제공하지 않으면 디바이스는 자동으로 생성된 인증서를 사용합니다.

ID 영역**(ID** 정책 및 원격 액세스 **VPN) -** 신뢰할 수 있는 **CA** 인증서

(선택 사항). 디렉터리 서버에 암호화된 연결을 사용하는 경우 디렉터리 서버 인증을 수행하려면 인증서를 허용해야 합니다. 사용자는 ID 및 원격 액세스 VPN 정책에 따라 메시지가 표시되면 인증을 해야 합니다. 디렉터리 서버에 대해 암호화를 사용하지 않는 경우에는 인증서가 필요하지 않습니다.

관리 웹 서버**(**관리 액세스 시스템 설정**)** — 내부 인증서

(선택 사항.) Device Manager는 웹 기반 애플리케이션으로, 웹 서버에서 실행됩니다. 브라우저에서 유효한 것으로 승인한 인증서를 업로드하면 신뢰할 수 없는 기관 경고를 피할 수 있습니다.

원격 액세스 **VPN -** 내부 인증서

(필수) 내부 인증서는 Secure Client가 디바이스에 대해 연결을 생성할 때 AnyConnect 클라이언트에 대해 디바이스 ID를 설정하는 외부 인터페이스용입니다. 클라이언트는 이 인증서를 허용해야 합니다.

Site-to-Site VPN - 내부 및 신뢰할 수 있는 **CA** 인증서

사이트 대 사이트 VPN 연결에 인증서 인증을 사용하는 경우 연결에서 로컬 피어 인증에 사용하는 내부 ID 인증서를 선택해야 합니다. 이 인증서가 VPN 연결 정의의 일부는 아니지만, 시스템에서 피어를 인증할 수 있도록 로컬 및 원격 피어 ID 인증서에 서명하는 데 사용한 신뢰할 수 있는 CA 인증서도 업로드해야 합니다.

SSL 암호 해독 정책 — 내부**,** 내부 **CA** 및 신뢰할 수 있는 **CA** 인증서 및 인증서 그룹

(필수) SSL 암호 해독 정책은 다음 목적을 위해 인증서를 사용합니다.

- 내부 인증서는 알려진 키 암호 해독 규칙에 사용됩니다.
- 내부 CA 인증서는 클라이언트와 threat defense 디바이스 사이에 세션을 생성할 때 암호 해독 재서명 규칙에 사용됩니다.
- 신뢰할 수 있는 CA 인증서는 threat defense 디바이스와 서버 사이에 세션을 생성할 때 암호 해독 재서명 규칙에 간접적으로 사용됩니다. 신뢰할 수 있는 CA 인증서는 서버 인증서의 서명 기관을 확인하는 데 사용됩니다. 이러한 인증서를 직접 구성하거나 정책 설정의 인증서 그룹에서 구성할 수 있습니다. 시스템에는 CTA(Cisco-Trusted-Authorities)에서 수집된 신뢰할 수 있는 CA 인증서가 많이 포함되어 있으므로 추가 인증서를 업로드할 필요가 없을 수도 있습니다.

예: **OpenSSL**을 사용하여 내부 인증서 생성

다음 예에서는 OpenSSL 명령을 사용하여 내부 서버 인증서를 생성합니다. OpenSSL은 openssl.org에서 다운로드할 수 있습니다. 구체적인 정보는 OpenSSL 설명서를 참조하십시오. 이 예에서 사용되는 명령은 변경될 수 있으며 사용하려는 옵션이 아닌 다른 옵션이 제공될 수도 있습니다.

이 절차에서는 threat defense에 업로드할 인증서를 얻는 방법을 대략 파악할 수 있습니다.

참고 여기에 표시되어 있는 OpenSSL 명령은 예로만 제공됩니다. 파라미터는 보안 요건에 맞게 조정하십시오.

프로시저

단계 **1** 키를 생성합니다.

```
openssl genrsa -out server.key 4096
```

단계 **2** CSR(인증서 서명 요청)을 생성합니다.

```
openssl req -new -key server.key -out server.csr
```

단계 **3** 키와 CSR을 사용하여 셀프 서명한 인증서를 생성합니다.

```
openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt
```

device manager는 암호화된 키를 지원하지 않으므로, 셀프 서명한 인증서를 생성할 때는 Return 키를 눌러 생성 과정에서 비밀번호를 입력하라는 메시지를 건너뜁니다.

단계 **4** device manager에서 내부 인증서 개체를 생성할 때 적절한 필드에 파일을 업로드합니다.

파일 내용을 복사하여 붙여 넣을 수도 있습니다. 샘플 명령은 다음 파일을 생성합니다.

- server.crt - 내용을 서버 인증서 필드에 업로드하거나 붙여 넣습니다.
- server.key - 내용을 인증서 키 필드에 업로드하거나 붙여 넣습니다. 키를 생성할 때 비밀번호를 입력한 경우에는 다음 명령을 사용하여 암호 해독할 수 있습니다. 출력은 stdout으로 전송되며, 여기서 출력 내용을 복사할 수 있습니다.

  ```
  openssl rsa -in server.key -check
  ```

인증서 구성

Threat Defense는 PEM 또는 DER 형식의 X509 인증서를 지원합니다. 필요한 경우 OpenSSL을 사용하여 인증서를 생성하거나, 신뢰할 수 있는 인증 증명에서 인증서를 받거나, 자체 서명 인증서를 생성합니다.

인증서에 대한 자세한 내용은 인증서 정보, 161 페이지를 참조하십시오.

각 기능에 사용되는 유형에 대한 자세한 내용은 기능에 사용되는 인증서 유형, 162 페이지를 참고하십시오.

다음 절차에서는 개체 페이지를 통해 개체를 직접 생성하고 수정할 수 있는 방법을 설명합니다. 개체 목록에 표시되는 새 인증서 생성 링크를 클릭하여 인증서 속성을 수정하면서 인증서 개체를 생성할 수도 있습니다.

프로시저

단계 **1** 목차에서 **Objects(**개체**)**와 **Certificates(**인증서**)**를 차례로 선택합니다.

시스템에는 다음과 같은 사전 정의된 인증서가 제공되며 이러한 인증서는 있는 그대로 사용하거나 대체할 수 있습니다.

- DefaultInternalCertificate
- DefaultWebserverCertificate
- NGFW-Default-InternalCA

시스템에는 서드파티 인증 증명에서 제공되는 수많은 신뢰할 수 있는 CA 인증서도 포함됩니다. 이러한 인증서는 Decrypt Re-Sign(암호 해독 재서명) 작업을 위한 SSL 암호 해독 정책에서 사용됩니다. CTA(Cisco-Trusted-Authorities) 그룹은 이러한 인증서를 모두 포함하며 SSL 암호 해독 정책에서 사용하는 기본 그룹입니다.

사전 정의된 검색 필터를 클릭하여 목록을 **System-defined(**시스템 정의**)** 또는 **User-defined(**사용자 정의**)** 인증서로 제한할 수 있습니다. 또한 **Weak Key(**약한 키**)** 필터를 사용하여 키가 권장 최소 길이보다 짧은 인증서를 찾을 수 있습니다. 이러한 인증서는 더 긴 키가 있는 인증서로 교체하는 것이 좋습니다.

단계 **2** 다음 중 하나를 수행합니다.

- 새 인증서 개체를 생성하려면 **+** 메뉴에서 인증서 유형에 맞는 명령을 사용합니다.
- 새 인증서 그룹을 생성하려면 을 클릭하고 **Add Certificate Group(**인증서 그룹 추가**)**을 선택합니다.
- 인증서 또는 그룹을 보거나 수정하려면 인증서의 수정 아이콘( ) 또는 보기 아이콘( )을 클릭합니다.
- 참조되지 않는 인증서 또는 그룹을 삭제하려면 해당 인증서의 휴지통 아이콘( )을 클릭합니다.

인증서 생성 또는 수정에 대한 자세한 내용은 다음 주제를 참조하십시오.

- 내부 및 내부 CA 인증서 업로드, 165 페이지
- 자체 서명 내부 및 내부 CA 인증서 생성, 167 페이지
- 신뢰할 수 있는 CA 인증서 업로드, 169 페이지
- 신뢰할 수 있는 CA 인증서 그룹 구성, 170 페이지

내부 및 내부 CA 인증서 업로드

내부 ID 인증서는 특정 시스템 또는 호스트용 인증서입니다.

내부 CA 인증서는 시스템에서 다른 인증서를 서명하는 데 사용할 수 있는 인증서입니다. 이러한 인증서는 CA 인증서에는 활성화되지만 ID 인증서에는 비활성화되는 기본 제약 조건 확장 및 CA 플래그와 관련된 내부 ID 인증서와 다릅니다.

OpenSSL 툴킷을 사용하여 이러한 인증서를 직접 생성하거나 인증 증명에서 가져온 후, 다음 절차를 사용하여 업로드할 수 있습니다. 키 생성의 예를 보려면 예: OpenSSL을 사용하여 내부 인증서 생성, 163 페이지를 참조하십시오.

자체 서명된 내부 ID 및 내부 CA 인증서를 생성할 수도 있습니다. 자체 서명된 내부 CA 인증서를 구성할 경우, CA는 디바이스 자체에서 실행됩니다. 자체 서명 인증서를 만드는 방법에 대한 내용은 자체 서명 내부 및 내부 CA 인증서 생성, 167 페이지를 참조하십시오.

이러한 인증서를 사용하는 기능에 대한 자세한 내용은 기능에 사용되는 인증서 유형, 162 페이지를 참조하십시오.

프로시저

단계 **1** 목차에서 **Objects(**개체**)**와 **Certificates(**인증서**)**를 차례로 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- **+** > **Add Internal Certificate(**내부 인증서 추가**)**를 클릭한 다음 **Upload Certificate and Key(**인증서 및 키 업로드**)**를 클릭합니다.
- **+** > **Add Internal CA Certificate(**내부 **CA** 인증서 추가**)**를 클릭한 다음 **Upload Certificate and Key(**인증서 및 키 업로드**)**를 클릭합니다.
- 인증서를 수정하거나 보려면 정보 아이콘()을 클릭합니다. 대화 상자에는 인증서 주체, 발급자, 유효 기간 범위가 표시됩니다. 새 인증서 및 키를 업로드하려면 Replace Certificate(인증서 교체)를 클릭합니다. 대화 상자에서 인증서 및 키를 붙여넣을 수도 있습니다.

단계 **3** 인증서의 **Name(**이름**)**을 입력합니다.

이름은 컨피그레이션에서 개체 이름으로만 사용되며 인증서 자체에 포함되지는 않습니다.

단계 **4** **Upload Certificate(**인증서 업로드**)** 또는 **Replace Certificate(**인증서 교체**)**(수정 시)를 클릭하고 인증서 파일(예: *.crt)을 선택합니다. 허용된 파일 확장명은 .pem, .cert, .cer, .crt, and .der입니다. 또는 인증서를 붙여넣습니다.

인증서는 PEM 또는 DER 형식의 X509 인증서여야 합니다.

붙여넣는 인증서는 BEGIN CERTIFICATE 및 END CERTIFICATE 줄을 포함해야 합니다. 예를 들면 다음과 같습니다.

```
-----BEGIN CERTIFICATE-----
MIICMTCCAZoCCQDdUV3NGK/cUjANBgkqhkiG9w0BAQsFADBdMQswCQYDVQQGEwJV
UzETMBEGA1UECAwKU29tZS1TdGF0ZTEhMB8GA1UECgwYSW50ZXJuZXQgV2lkZ2l0
(...5 lines removed...)
shGJDReRYJQqilhHZrYTWZAYTrD7NQPHutK+ZiJng67cPgnNDuXEn55UwMOQoHBp
HMUwmhiGZlzJM8BpX2Js2yQ3ms30pr8rO+gPCPMCAwEAATANBgkqhkiG9w0BAQsF
AAOBgQCB02CebA6YjJCGr2CJZrQSeUwSveRBpmOuoqm98o2Z+5gJM5CkqgfxwCUn
RV7LRfQGFYd76V/5uor4Wx2ZCjqy6+zuQEm4ZxWNSZpA9UBixFXJCs9MBO4qkG5D
vlk3WYJfcgyJ10h4E4b0W2xiixBU+xoOTLRATnbKY36EWAG5cw==
-----END CERTIFICATE-----
```

단계 **5** **Upload Key(**키 업로드**)** 또는 **Replace Key(**키 교체**)**(수정 시)를 클릭하고 인증서 파일(예: *.key)을 선택합니다. 파일 확장명은 .key여야 합니다. 또는 인증서의 키를 붙여넣습니다.

키는 암호화할 수 없으며, RSA 키여야 합니다.

예를 들면 다음과 같습니다.

```
-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQClSu1BknrMjzw/5FZ9YgdMLDUGJlbYgkjN7mVrkjyLQx2TYsem
r8iTiKB6iyTKbuS4iPeyEYkNF5FglCqKWEdmthNZkBhOsPs1A8e60r5mImeDrtw+
Cc0O5cSfnlTAw5CgcGkcxTCaGIZmXMkzwGlfYmzbJDeazfSmvys76A8I8wIDAQAB
AoGAUVDgEX8vXE0m9cOubPZ54pZo64KW/OJzUKP0TwxdLqGw/h39XFpkEXiIgmDL
(...5 lines removed...)
DSWvzekRDH83dmP66+MIbWePhbhty+D1OxbiuVuHV0/ZhxOhCG8tig3R8QJBAJmj
fId05+1dNI4tGbWv6hHh/H/dTP2STlZ3jERMZd29fjIRuJ9jpFC2lIDjvs8YGeAe
0YHkfSOULJn8/jOCf6kCQQDIJiHfGF/31Dk/8/5MGrg+3zau6oKXiuv6db8Rh+7l
MUOx09tvbBUy9REJq1YJWTKpeKD+E0QL+FX0bqvz4tHA
-----END RSA PRIVATE KEY-----
```

단계 **6** **OK(**확인**)**를 클릭합니다.

키 크기가 생성된 자체 서명 인증서에 대해 허용되는 최소 크기보다 작으면 인증서가 권장 최소 요구 사항을 충족하지 않는다는 경고가 표시됩니다. 인증서를 계속 업로드하려면 **Proceed(**진행**)**를 클릭합니다. 하지만 더 강력한 새 인증서를 생성하는 것이 좋습니다.

자체 서명 내부 및 내부 **CA** 인증서 생성

내부 ID 인증서는 특정 시스템 또는 호스트용 인증서입니다.

내부 CA 인증서는 시스템에서 다른 인증서를 서명하는 데 사용할 수 있는 인증서입니다. 이러한 인증서는 CA 인증서에는 활성화되지만 ID 인증서에는 비활성화되는 기본 제약 조건 확장 및 CA 플래그와 관련된 내부 ID 인증서와 다릅니다.

자체 서명 내부 ID 및 내부 CA 인증서를 생성할 수 있으며, 즉 디바이스 자체에서 인증서를 서명합니다. 자체 서명 내부 CA 인증서를 구성할 경우, CA는 디바이스에서 실행됩니다. 시스템에서는 인증서 및 키를 모두 생성합니다.

OpenSSL을 사용하여 이러한 인증서를 생성하거나, 신뢰할 수 있는 CA에서 인증서를 가져오고 업로드할 수 있습니다. 자세한 내용은 내부 및 내부 CA 인증서 업로드, 165 페이지를 참고하십시오.

이러한 인증서를 사용하는 기능에 대한 자세한 내용은 기능에 사용되는 인증서 유형, 162 페이지를 참조하십시오.

프로시저

단계 **1** 목차에서 **Objects(**개체**)**와 **Certificates(**인증서**)**를 차례로 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- **+** > **Add Internal Certificate(**내부 인증서 추가**)**를 클릭한 다음 **Self-Signed Certificate(**자체 서명 인증서**)**를 클릭합니다.
- **+** > **Add Internal CA Certificate(**내부 **CA** 인증서 추가**)**를 클릭한 다음 **Self-Signed Certificate(**자체 서명 인증서**)**를 클릭합니다.

참고 인증서를 수정하거나 보려면 정보 아이콘()을 클릭합니다. 대화 상자에는 인증서 주체, 발급자, 유효 기간 범위가 표시됩니다. 새 인증서 및 키를 업로드하려면 **Replace Certificate(**인증서 교체**)**를 클릭합니다. 인증서를 교체할 경우, 다음 단계에 설명된 자체 서명 특성을 다시 실행할 수 없습니다. 그 대신, 내부 및 내부 CA 인증서 업로드, 165 페이지에 설명된 대로 새 인증서를 붙여넣거나 업로드해야 합니다. 나머지 단계는 새로운 자체 서명 인증서에만 적용됩니다.

단계 **3** 인증서의 **Name(**이름**)**을 입력합니다.

이름은 컨피그레이션에서 개체 이름으로만 사용되며 인증서 자체에 포함되지는 않습니다.

단계 **4** 인증서 주체와 발급자 정보에 다음 중 한 가지 이상의 정보를 구성합니다.

- **Country(**국가**)**(C) — 인증서에 포함할 두 글자로 된 ISO 3166 국가 코드입니다. 예를 들어 미국의 국가 코드는 US입니다. 드롭다운 목록에서 국가 코드를 선택합니다.
- **State or Province(**주/도**)**(ST) — 인증서에 포함할 주/도입니다.
- **Locality or City(**구/군/시**)**(L) — 인증서에 포함할 구/군/시(예: 도시 이름)입니다.
- **Organization(**조직**)**(O) — 인증서에 포함할 조직 또는 회사 이름입니다.
- **Organizational Unit(Department)(**조직 단위**(**부서**))**(OU) — 인증서에 포함할 조직 단위의 이름(예: 부서 이름)입니다.
- **Common Name(**공용 이름**)**(CN) — 인증서에 포함할 X.500 공용 이름입니다. 이는 디바이스, 웹사이트 또는 다른 문자열의 이름일 수 있습니다. 일반적으로 연결에 성공하려면 이 요소가 필요합니다. 예를 들어 원격 액세스 VPN에 사용되는 내부 인증서에는 CN을 포함해야 합니다.
- **Key Type(**키 유형**)** - 이 인증서에 대해 생성할 키 유형: RSA, ECDSA(Elliptic Curve Digital Signature Algorithm) 또는 EDDSA(Edward-curve Digital Signature Algorithm).
- **Key Size(**키 크기**)** - 생성할 키의 크기. 일반적으로 키가 길수록 더 안전합니다. 그러나 모듈러스 크기가 큰 키는 생성 및 교환 프로세스에 더 오랜 시간이 걸립니다. 허용되는 크기는 키 유형에 따라 다릅니다.
  - RSA 키는 2048, 3072 또는 4096비트일 수 있습니다.
  - ECDSA 키는 256, 384 또는 521비트일 수 있습니다.

    EDDSA 키는 256비트일 수 있습니다.
- **Validity Period(**유효 기간**)** - 인증서가 유효한 것으로 간주되는 기간입니다. 기본값은 만료일 설정 방법과 무관하게 오늘을 기준으로 825일입니다. 기본값으로 돌아가려면 **Set default(**기본값으로 설정**)**를 클릭합니다. 다음 방법 중 하나를 사용하여 기간을 설정할 수 있습니다. 만료되기 전에 인증서를 교체하십시오.
  - **By Date(**날짜 기준**) - Expiration Date(**만료 날짜**)**를 클릭하고 인증서가 유효한 것으로 간주되는 마지막 날을 선택합니다.

- **By Number of Days(**일 수 기준**)** - 오늘을 시작으로 인증서가 유효한 것으로 간주되는 기간(일)을 입력합니다. 수를 입력한 후 **By Date(**날짜 기준**)**을 클릭하면 계산된 만료 날짜가 표시됩니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

신뢰할 수 있는 CA 인증서 업로드

신뢰할 수 있는 CA(Certificate Authority) 인증서는 다른 인증서에 서명하는 데 사용되며, 자체 서명되며 루트 인증서라고도 합니다. 다른 CA 인증서를 통해 발급된 인증서는 하위 인증서라고 합니다.

이러한 인증서를 사용하는 기능에 대한 자세한 내용은 기능에 사용되는 인증서 유형, 162 페이지를 참조하십시오.

외부 인증 기관으로부터 신뢰할 수 있는 CA 인증을 획득하거나, OpenSSL 도구 등 자체 내부 CA를 사용하여 CA 인증을 생성하십시오. 그런 다음, 아래 절차를 사용하여 인증서를 업로드합니다.

프로시저

단계 **1** 목차에서 **Objects(**개체**)**와 **Certificates(**인증서**)**를 차례로 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- **+** > **Add Trusted CA Certificate(**신뢰받는 **CA** 인증서 추가**)**를 클릭합니다.
- 인증서를 수정하려면 인증서의 수정 아이콘( )을 클릭합니다.

단계 **3** 인증서의 **Name(**이름**)**을 입력합니다.

이름은 컨피그레이션에서 개체 이름으로만 사용되며 인증서 자체에 포함되지는 않습니다.

단계 **4** 인증서 업로드 또는 인증서 교체(수정 시)를 클릭하고 신뢰할 수 있는 CA 인증서 파일(예: *.pem)을 선택합니다. 허용된 파일 확장명은 .pem, .cert, .cer, .crt, and .der입니다. 또는 신뢰할 수 있는 CA 인증서를 붙여넣습니다.

인증서의 서버 이름이 서버 호스트 이름/IP 주소와 일치해야 합니다. 예를 들어 IP 주소로 10.10.10.250을 사용하는데 인증서의 주소는 ad.example.com이면 연결은 실패합니다.

인증서는 PEM 또는 DER 형식의 X509 인증서여야 합니다.

붙여넣는 인증서는 BEGIN CERTIFICATE 및 END CERTIFICATE 줄을 포함해야 합니다. 예를 들면 다음과 같습니다.

```
-----BEGIN CERTIFICATE-----
MIIFgTCCA2mgAwIBAgIJANvdcLnabFGYMA0GCSqGSIb3DQEBCwUAMFcxCzAJBgNV
BAYTAlVTMQswCQYDVQQIDAJUWDEPMA0GA1UEBwwGYXVzdGluMRQwEgYDVQQKDAsx
OTIuMTY4LjEuMTEUMBIGA1UEAwwLMTkyLjE2OC4xLjEwHhcNMTYxMDI3MjIzNDE3
WhcNMTcxMDI3MjIzNDE3WjBXMQswCQYDVQQGEwJVUzELMAkGA1UECAwCVFgxDzAN
BgNVBAcMBmF1c3RpbjEUMBIGA1UECgwLMTkyLjE2OC4xLjExFDASBgNVBAMMCzE5
```

```
Mi4xNjguMS4xMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA5NceYwtP
ES6Ve+S9z7WLKGX5JlF58AvH82GPkOQdrixn3FZeWLQapTpJZt/vgtAI2FZIK31h
(...20 lines removed...)
hbr6HOgKlOwXbRvOdksTzTEzVUqbgxt5Lwupg3b2ebQhWJz4BZvMsZX9etveEXDh
PY184V3yeSeYjbSCF5rP71fObG9Iu6+u4EfHp/NQv9s9dN5PMffXKieqpuN20Ojv
2b1sfOydf4GMUKLBUMkhQnip6+3W
-----END CERTIFICATE-----
```

단계 **5** 인증서 사용을 제한하려면 **Validation Usage(**검증 사용**)**를 설정합니다.

일부 기능을 사용하면 특정 인증서에 대해 연결을 검증할 수 있는지 여부를 선택할 수 있습니다. 이러한 기능이 인증서를 유효하게 사용할 수 있음을 인증서에 표시해야 하며, 그렇지 않은 경우 연결이 거부됩니다.

이러한 옵션에 포함되지 않은 기능은 명시적 사용 허용 없이 이 인증서에 대해 검증할 수 있습니다. 예를 들어 SSL 암호 해독 정책 및 device manager을 호스팅하는 웹 서버는 Validation Usage(검증 사용) 옵션을 무시합니다. 이 필드에서 옵션을 선택하면 **show running-config** 명령을 사용하여 표시되는 실행 중인 구성에 인증서가 다운로드됩니다.

이러한 옵션의 기본 목적은 특정 인증서에 대해 검증될 수 있으므로 VPN 연결이 설정되지 않도록 하는 것입니다.

- **SSL Server(SSL** 서버**)** - 원격 SSL 서버에서 인증서를 검증합니다. 동적 DNS에 사용합니다.
- **SSL Client(SSL** 클라이언트**)** - 수신 원격 액세스 VPN 연결 인증서를 검증합니다.
- **IPsec Client(IPsec** 클라이언트**)** - 수신 IPsec 사이트 간 VPN 연결 인증서를 검증합니다.
- **Other(**기타**)** - Snort 검사 엔진에서 관리하지 않는 LDAPS 등의 기능을 검증합니다. 특정 기능에 문제가 있는 경우에만 이 옵션을 선택하십시오. **Other(**기타**)**는 다른 모든 옵션과 상호 배타적입니다. 다른 옵션을 선택하려면 먼저 **Other(**기타**)**를 선택 취소해야 하고, **Other(**기타**)**를 선택하려면 먼저 모든 옵션을 선택 취소해야 합니다.

단계 **6** **OK(**확인**)**를 클릭합니다.

신뢰할 수 있는 **CA** 인증서 그룹 구성

SSL 암호 해독 정책 설정에서 외부의 신뢰할 수 있는 CA 인증서 그룹을 사용하여 SSL 암호 해독 정책에서 신뢰해야 하는 인증서를 지정합니다. 엔드 유저가 인증서 발급자의 인증서가 신뢰할 수 있는 인증서에 속하지 않은 사이트에 연결을 시도하면 해당 유저에게 인증서를 신뢰하라는 메시지가 표시됩니다. 따라서 신뢰할 수 있는 목록에 인증서가 없는 경우 엔드 유저는 불편하지만 액세스 제어 규칙으로 수행할 수 있는 연결 자체가 차단되지는 않습니다.

기본 그룹은 CTA(Cisco-Trusted-Authorities)입니다. 다음과 같은 경우에만 고유한 그룹을 생성해야 합니다.

- 기본 그룹에 없는 인증서를 신뢰하고자 합니다. 그러면 SSL 암호 해독 정책 설정에서 기본 그룹과 새 그룹을 모두 선택합니다.

- 기본 그룹보다 제한된 인증서 목록을 신뢰하고자 합니다. 그러면 델타 뿐 아니라 신뢰할 수 있는 인증서의 전체 목록이 포함된 그룹을 생성하고 이를 SSL 암호 해독 정책 설정에서 단독 그룹으로 선택합니다.

시작하기 전에

시스템에 아직 없는 경우 그룹에 추가할 신뢰할 수 있는 CA 인증서를 모두 업로드합니다.

프로시저

단계 **1** 목차에서 **Objects(**개체**)**와 **Certificates(**인증서**)**를 차례로 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 새 인증서 그룹을 생성하려면 을 클릭하고 **Add Certificate Group(**인증서 그룹 추가**)**을 선택합니다.
- 인증서 그룹을 수정하려면 해당 그룹의 수정 아이콘( )을 클릭합니다.

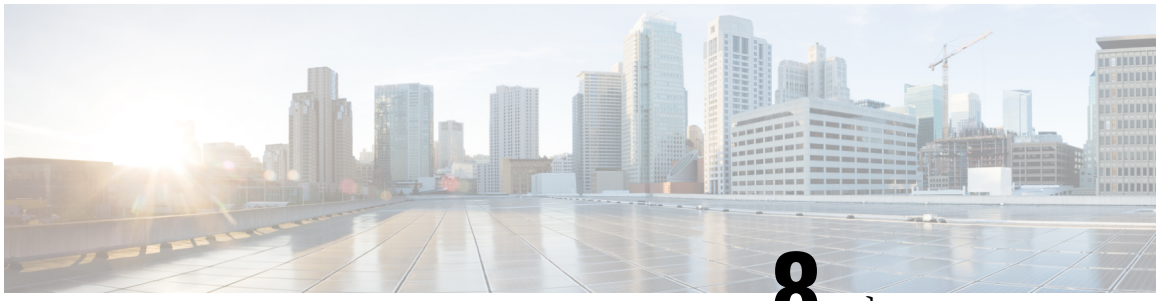
단계 **3** 인증서 그룹의 **Name(**이름**)**을 입력하고 필요한 경우 설명을 입력합니다.

단계 **4** **+**를 클릭하여 그룹에 인증서를 추가합니다.

그룹에 필요한 모든 인증서를 추가합니다. **Create New Trusted CA Certificate(**새 신뢰할 수 있는 **CA** 인증서 생성**)**를 클릭하여 그룹을 구축하는 동안 새 인증서를 업로드할 수 있습니다.

그룹에 인증서가 더 이상 필요하지 않은 경우 인증서의 X 아이콘(오른쪽)을 클릭합니다.

단계 **5** **OK(**확인**)**를 클릭합니다.



8 장

ID 소스

ID 소스는 사용자 어카운트를 정의하는 서버와 데이터베이스입니다. 이 정보는 IP 주소와 연결된 사용자 ID를 제공하거나, 원격 액세스 VPN 연결 또는 device manager 액세스를 인증하는 등 다양한 방식으로 사용할 수 있습니다.

다음 주제에서는 ID 소스를 정의하는 방법을 설명합니다. 그런 다음, ID 소스가 필요한 서비스를 구성할 때 이러한 개체를 사용할 수 있습니다.

ID 소스 정보

ID 소스는 조직 내 사용자의 사용자 어카운트를 정의하는 AAA 서버와 데이터베이스입니다. 이 정보는 IP 주소와 연결된 사용자 ID를 제공하거나, 원격 액세스 VPN 연결 또는 device manager 액세스를 인증하는 등 다양한 방식으로 사용할 수 있습니다.

Objects(개체**)** > **Identity Sources(ID** 소스**)** 페이지에서 소스를 생성하고 관리합니다. 그런 다음, ID 소스가 필요한 서비스를 구성할 때 이러한 개체를 사용할 수 있습니다.

지원되는 ID 소스와 사용 방법은 다음과 같습니다.

AD(Active Directory) ID 영역

Active Directory에서 사용자 어카운트 및 인증 정보를 제공합니다. AD(Active Directory) ID 영역, 175 페이지의 내용을 참조하십시오.

이 소스는 다음과 같은 목적으로 사용할 수 있습니다.

- 원격 액세스 VPN(기본 ID 소스로 사용) AD를 RADIUS 서버와 함께 사용할 수 있습니다.
- ID 정책(활성 인증용으로 사용/패시브 인증에 사용되는 사용자 ID 소스로 사용)

AD(Active Directory) 영역 시퀀스

AD 영역 시퀀스는 AD 영역 개체의 순서가 지정된 목록입니다. 영역 시퀀스는 네트워크에서 두 개 이상의 AD 도메인을 관리하는 경우 유용합니다. AD 영역 시퀀스 구성하기, 179 페이지의 내용을 참조하십시오.

이 소스는 다음과 같은 목적으로 사용할 수 있습니다.

- ID 정책(패시브 인증에 사용되는 사용자 ID 소스로 사용) 시퀀스에서 영역의 순서는 시스템에서 드물게 충돌이 발생하는 경우 사용자 ID를 결정하는 방식을 결정합니다.

Cisco ISE(Identity Services Engine) 또는 **Cisco ISE PIC(Identity Services Engine Passive Identity Connector)**

ISE를 사용하는 경우 threat defense 디바이스를 ISE 구축과 통합할 수 있습니다. Identity Services Engine (ISE), 186 페이지의 내용을 참조하십시오.

이 소스는 다음과 같은 목적으로 사용할 수 있습니다.

- ID 정책(ISE에서 사용자 ID를 수집하기 위한 패시브 ID 소스로 사용)

RADIUS 서버**, RADIUS** 서버 그룹

RADIUS 서버를 사용하는 경우 device manager와 함께 사용할 수도 있습니다. 각 서버를 별도의 개체로 정의한 후에 서버 그룹에 포함할 수 있습니다. 여기서 지정된 그룹의 서버는 서로의 복사본입니다. 개별 서버가 아닌 서버 그룹을 기능에 할당해야 합니다. RADIUS 서버 및 그룹, 182 페이지의 내용을 참조하십시오.

이 소스는 다음과 같은 목적으로 사용할 수 있습니다.

- 인증용 ID 소스이자 권한 부여 및 과금 용도의 원격 액세스 VPN. AD를 RADIUS 서버와 함께 사용할 수 있습니다.
- ID 정책(원격 액세스 VPN 로그인에서 사용자 ID를 수집하기 위한 패시브 ID 소스로 사용)
- device manager 또는 threat defense CLI 관리 사용자에 대한 외부 인증. 인증 레벨이 각기 다른 여러 관리 사용자를 지원할 수 있습니다. 이 사용자는 디바이스 컨피그레이션 및 모니터링을 위해 시스템에 로그인할 수 있습니다.

SAML 서버

SAML 2.0(Security Assertion Markup Language 2.0)은 당사자 간에 인증 및 권한 부여 데이터, 특히 IdP(Identity Provider)와 SP(Service Provider)를 교환하기 위한 개방형 표준입니다.

이 소스는 다음과 같은 목적으로 사용할 수 있습니다.

- SSO(Single Sign-On) 인증 소스로서의 원격 액세스 VPN.

로컬 **ID** 소스

device manager에서 정의한 사용자를 포함하는 로컬 사용자 데이터베이스입니다. 이 데이터베이스에서 사용자 어카운트를 관리하려면 **Objects(**개체**)** > **Users(**사용자**)**를 선택합니다. 로컬 사용자, 192 페이지의 내용을 참조하십시오.

참고 로컬 ID 소스 데이터베이스에는 CLI 액세스를 위해 **configure user add** 명령을 사용하여 CLI에서 구성한 사용자는 포함되지 않습니다. CLI 사용자는 device manager에서 생성하는 사용자와는 완전히 별개의 사용자입니다.

이 소스는 다음과 같은 목적으로 사용할 수 있습니다.

- 원격 액세스 VPN(기본 또는 대체 ID 소스로 사용)
- ID 정책(원격 액세스 VPN 로그인에서 사용자 ID를 수집하기 위한 패시브 ID 소스로 사용)

AD(Active Directory) ID 영역

Microsoft AD(Active Directory)는 사용자 어카운트를 정의합니다. Active Directory 도메인의 AD ID 영역을 생성할 수 있습니다. 다음 주제에서는 AD ID 영역을 정의하는 방법을 설명합니다.

지원되는 디렉터리 서버

Windows Server 2012, 2016, 및 2019에서 Microsoft AD(Active Directory)를 사용할 수 있습니다.

서버 컨피그레이션과 관련하여 다음 사항에 유의하십시오.

- 사용자 그룹 또는 그룹 내의 사용자에 대해 사용자 제어를 수행하려면 디렉터리 서버에서 사용자 그룹을 구성해야 합니다. 서버가 기본 개체 계층으로 사용자를 구성하는 경우 시스템은 사용자 그룹 제어를 수행할 수 없습니다.
- 디렉터리 서버는 시스템에 대해 다음 표에 나와 있는 필드 이름을 순서대로 사용하여 해당 필드에 대한 사용자 메타데이터를 서버에서 검색해야 합니다.

메타데이터	**Active Directory Field(Active Directory** 필드**)**
LDAP user name(LDAP 사용자 이름)	samaccountname
first name(이름)	givenname
last name(성)	sn
email address(이메일 주소)	mail userprincipalname(메일에 값이 없는 경우)
department(부서)	department distinguishedname(부서에 값이 없는 경우)
telephone number(전화번호)	telephonenumber

사용자 수 제한사항

Device Manager는 디렉터리 서버에서 최대 50,000명의 사용자에 대한 정보를 다운로드할 수 있습니다.

디렉터리 서버에 50,000개가 넘는 사용자 계정이 포함되어 있으면 액세스 규칙에서 사용자를 선택할 때 또는 사용자 기반 대시보드 정보를 확인할 때 가능한 이름이 모두 표시되지 않으며, 다운로드한 이름에 대해서만 규칙을 작성할 수 있습니다.

이 제한은 그룹과 연결된 이름에도 적용됩니다. 그룹의 구성원이 50,000명보다 많으면 다운로드한 50,000개의 이름에 대해서만 그룹 구성원 자격과의 일치 여부를 확인할 수 있습니다.

디렉터리 기본 **DN** 결정

디렉터리 속성을 구성할 때는 사용자와 그룹에 대한 공통 기본 DN(고유 이름)을 지정해야 합니다. 이 기준은 디렉터리 서버에서 정의되며 네트워크마다 다릅니다. 올바른 기준을 입력해야 ID 정책이 실행됩니다. 기준이 잘못된 경우 시스템이 사용자 또는 그룹 이름을 확인할 수 없으므로 ID 기반 정책이 실행될 수 없습니다.

팁 올바른 기준을 가져오려면 디렉터리 서버 담당 관리자에게 문의하십시오.

Active Directory의 경우, 도메인 관리자로 Active Directory 서버에 로그인하여 다음과 같이 명령 프롬프트에 **dsquery** 명령을 사용해 기준을 확인하여 올바른 기준을 확인할 수 있습니다.

사용자 검색 기준

알려진 사용자 이름(부분 또는 전체)을 포함한 **dsquery user** 명령을 입력하여 기본 고유 이름을 확인합니다. 예를 들어, 다음 명령은 부분 이름 "John*"를 사용하여 "John"으로 시작되는 모든 사용자에 대한 정보를 반환합니다.

```
C:\Users\Administrator>dsquery user -name "John*"
"CN=John Doe,CN=Users,DC=csc-lab,DC=example,DC=com"
```

이 경우 기본 DN은 "DC=csc-lab,DC=example,DC=com"이 됩니다.

그룹 검색 기준

알려진 그룹 이름을 포함한 **dsquery group** 명령을 입력하여 기본 고유 이름을 확인합니다. 예를 들어, 다음 명령은 그룹 이름 Employees를 사용하여 고유 이름을 반환합니다.

```
C:\>dsquery group -name "Employees"
"CN=Employees,CN=Users,DC=csc-lab,DC=example,DC=com"
```

이 경우 그룹 기본 DN은 "DC=csc-lab,DC=example,DC=com"이 됩니다.

ADSI 수정 프로그램을 사용하여 Active Directory 구조를 찾을 수도 있습니다(**Start(**시작**)** > **Run(**실행**)** > **adsiedit.msc**). ADSI 수정에서 조직 단위(OU), 그룹, 사용자 등의 개체를 마우스 오른쪽 단추로

클릭하고 **Properties(**속성**)**를 선택하여 고유 이름을 확인합니다. 그러면 DC 값 문자열을 기준으로 복사할 수 있습니다.

기준이 올바른지를 확인하려면 다음 단계를 수행합니다.

1. 디렉터리 속성의 연결 테스트 버튼을 클릭하여 연결을 확인합니다. 모든 문제를 해결하고 디렉터리 속성을 저장합니다.
2. 디바이스에 변경 사항을 커밋합니다.
3. 액세스 규칙을 생성하고 **Users(**사용자**)** 탭을 선택한 다음 디렉터리에서 알려진 사용자 및 그룹 이름을 추가해 봅니다. 디렉터리가 포함된 영역에서 일치하는 사용자 및 그룹을 입력하면 자동 완성 제안 사항이 표시됩니다. 이러한 제안 사항이 드롭다운 목록에 표시되는 경우 시스템이 디렉터리를 정상적으로 쿼리한 것입니다. 입력한 문자열이 사용자 또는 그룹 이름에 포함되어 있는데 제안 사항이 표시되지 않으면 해당하는 검색 기준을 수정해야 합니다.

AD ID 영역 구성

ID 영역은 디렉터리 서버와 인증 서비스를 제공하는 데 필요한 기타 특성입니다. 디렉터리 서버는 네트워크 액세스가 허용되는 사용자 및 사용자 그룹에 대한 정보를 포함합니다.

Active Directory의 경우 영역은 Active Directory 도메인과 동일합니다. 지원해야 하는 각 AD 도메인에 대해 별도 영역을 생성합니다.

영역은 다음 정책에서 사용됩니다.

- ID - 영역은 사용자 ID 및 그룹 멤버십 정보를 제공합니다. 액세스 제어 규칙에서 이러한 정보를 사용할 수 있습니다. 시스템은 매일 마지막 시간(UTC)에 모든 사용자와 그룹에 대한 업데이트된 정보를 다운로드합니다. 디렉터리 서버는 관리 인터페이스에서 연결 가능해야 합니다.
- 원격 액세스 VPN — 영역은 연결 허용 여부를 결정하는 인증 서비스를 제공합니다. 디렉터리 서버는 RA VPN 외부 인터페이스에서에서 연결 가능해야 합니다.
- 액세스 제어, SSL 암호 해독 — 규칙의 사용자 기준에서 영역을 선택하여 이 규칙을 영역 내 모든 사용자에게 적용할 수 있습니다.

디렉터리 관리자와 협의하여 디렉터리 서버 속성을 구성하는 데 필요한 값을 가져오십시오.

참고 디렉터리 서버가 연결된 네트워크에 있지 않거나 기본 경로를 통해 사용할 수 없는 상태이면 서버에 대해 정적 경로를 생성합니다. **Device(**디바이스**)** > **Routing(**라우팅**)** > **View Configuration(**설정 보기**)**을 선택하여 정적 경로를 생성합니다.

다음 절차에서는 개체 페이지를 통해 개체를 직접 생성하고 수정할 수 있는 방법을 설명합니다. 개체 목록에 표시되는 새 **ID** 영역 생성 링크를 클릭하여 영역 속성을 수정하면서 ID 영역 개체를 생성할 수도 있습니다.

시작하기 전에

디렉터리 서버, threat defense 디바이스 및 클라이언트에서 시간 설정이 서로 일치하는지 확인합니다. 이러한 디바이스 간에 시간이 바뀌면 사용자가 정상적으로 인증하지 못할 수 있습니다. 여기서 "일치"란 여러 표준 시간대를 사용할 수는 있지만 이러한 표준 시간대를 기준으로 할 때 시간이 동일해야 한다는 의미입니다. 예를 들어 PST로 오전 10시는 EST로 오후 1시에 해당합니다.

프로시저

단계 **1** 목차에서 **Objects(**개체**)**와 **Identity Sources(ID** 소스**)**를 차례로 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- AD 영역을 생성하려면 **+** > **AD**를 클릭합니다.
- 영역을 수정하려면 해당 영역의 수정 아이콘( )을 클릭합니다.

참조되지 않는 개체를 삭제하려면 해당 개체의 휴지통 아이콘( )을 클릭합니다.

단계 **3** 기본 영역 속성을 구성합니다.

- **Name(**이름**)** - 디렉토리 영역의 이름입니다.
- **Type(**유형**)** - 디렉터리 서버의 유형입니다. 지원되는 유형은 Active Directory뿐이며 이 필드의 내용은 변경할 수 없습니다.
- **Directory Username(**디렉터리 사용자 이름**)**, **Directory Password(**디렉터리 비밀번호**)** - 검색하려는 사용자 정보에 대한 적절한 권한이 있는 사용자의 고유 사용자 이름 및 비밀번호입니다. Active Directory의 경우에는 사용자에게 상승된 권한이 필요하지 않습니다. 도메인에 어떤 사용자라도 지정할 수 있습니다. 사용자 이름은 모든 자격 요건에 부합해야 합니다(예: 단지 Administrator가 아닌 Administrator@example.com).

  참고 시스템은 이 정보에서 ldap-login-dn 및 ldap-login-password를 생성합니다. 예를 들어 Administrator@example.com은 cn=administrator,cn=users,dc=example,dc=com으로 변환됩니다. cn=users는 항상 이 변환에 포함되므로 일반 이름 "users" 폴더 아래에 여기서 지정하는 사용자를 구성해야 합니다.

- **Base DN(**기본 **DN)** - 사용자 및 그룹 정보를 검색하거나 쿼리하기 위한 디렉터리 트리, 즉 사용자와 그룹의 공통 상위 항목입니다. cn=users,dc=example,dc=com을 예로 들 수 있습니다. 기본 DN을 찾는 방법에 대한 자세한 내용은 디렉터리 기본 DN 결정, 176 페이지를 참조하십시오.
- **AD Primary Domain(AD** 기본 도메인**)** - 디바이스가 조인해야 하는 정규화된 Active Directory 도메인 이름입니다. example.com 등을 예로 들 수 있습니다.

단계 **4** 디렉터리 서버 속성을 구성합니다.

- **Hostname/IP Address(**호스트 이름**/IP** 주소**)** - 디렉터리 서버의 호스트 이름 또는 IP 주소입니다. 서버에 대한 암호화된 연결을 사용하는 경우에는 IP 주소가 아닌 FQDN(Fully-Qualified Domain Name)을 입력해야 합니다.

- **Port(포트)** - 서버와의 통신에 사용되는 포트 번호입니다. 기본값은 389입니다. 암호화 방법으로 LDAPS를 선택하는 경우에는 포트 636을 사용합니다.
- **Encryption(암호화)** - 사용자 및 그룹 정보를 다운로드하기 위해 암호화된 연결을 사용하려는 경우에는 **STARTTLS** 또는 **LDAPS** 중에서 원하는 방법을 선택합니다. 기본값은 **None(없음)**입니다. 이 옵션은 사용자 및 그룹 정보를 일반 텍스트로 다운로드함을 의미합니다.
  - **STARTTLS**는 암호화 방법을 협상하여 디렉토리 서버가 지원하는 가장 강력한 방법을 사용하며 포트 389를 사용합니다. 원격 액세스 VPN에 영역을 사용하는 경우에는 이 옵션이 지원되지 않습니다.
  - **LDAPS**를 선택하는 경우 LDAP over SSL이 필요합니다. 이 옵션은 포트 636을 사용합니다.
- **Trusted CA Certificate(신뢰할 수 있는 CA 인증서)** - 암호화 방법을 선택하는 경우 CA(인증 증명) 인증서를 업로드하여 시스템과 디렉터리 서버 간에 신뢰할 수 있는 연결을 설정합니다. 인증서를 사용하여 인증하는 경우에는 인증서의 서버 이름이 서버 호스트 이름/IP 주소와 일치해야 합니다. 예를 들어 IP 주소로 10.10.10.250을 사용하는데 인증서의 주소는 ad.example.com이면 연결은 실패합니다.

단계 **5** 해당 영역에 여러 개의 서버가 있는 경우, **Add Another Configuration(다른 컨피그레이션 추가)**을 클릭하고 각 추가 서버에 대해 속성을 입력합니다.

해당 영역에 최대 10개의 AD 서버를 추가할 수 있습니다. 이 서버들은 서로의 중복이어야 하고 동일한 AD 도메인을 지원해야 합니다.

편의에 따라 각 서버 항목을 축소 및 확장할 수 있습니다. 섹션에는 호스트네임/IP 주소 및 포트로 레이블이 지정됩니다.

단계 **6** **Test(테스트)** 버튼을 클릭하여 시스템이 서버에 연결할 수 있는지 확인합니다.

시스템은 별도의 프로세스와 인터페이스를 사용하여 서버에 액세스하므로, 연결이 특정 사용 유형에는 작동하지만 다른 유형에는 작동하지 않음을 나타내는 오류가 발생합니다. 연결을 ID 정책에는 사용할 수 있지만, 원격 액세스 VPN에는 사용할 수 없는 경우를 예로 들 수 있습니다. 서버에 연결할 수 없는 경우에는 IP 주소와 호스트 이름이 올바른지와 DNS 서버에 호스트 이름의 항목이 있는지 등을 확인합니다. 서버에 대한 정적 경로를 구성해야 할 수 있습니다. 자세한 내용은 디렉터리 서버 연결 트러블슈팅, 180 페이지를 참고하십시오.

단계 **7** **OK(확인)**를 클릭합니다.

AD 영역 시퀀스 구성하기

패시브 ID 규칙에서 AD 영역 시퀀스를 사용하여 시스템이 둘 이상의 AD 서버에서 사용자를 일치시키려고 시도할 수 있습니다. 영역 시퀀스에서는 각 AD 서버가 다른 영역 또는 도메인(예: engineering.example.com 및 marketing.example.com)을 관리하는 AD 영역의 순서가 지정된 목록을 구성합니다.

영역 시퀀스는 두 개 이상의 AD 도메인을 지원하고, 다른 도메인의 사용자가 threat defense 디바이스를 통해 트래픽을 전송할 수 있는 경우에만 유용합니다. 영역은 소극적으로 인증된 사용자 세션에 대

한 ID를 찾기 위해 사용됩니다. 이 영역의 순서는 충돌이 발생할 수 있는 드문 경우를 비롯하여 ID 충돌을 해결하는 데 사용됩니다.

프로시저

단계 **1** 목차에서 **Objects(**개체**)**와 **Identity Sources(ID** 소스**)**를 차례로 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- AD 영역 시퀀스를 생성하려면 **+** > **AD** 영역 시퀀스를 클릭합니다.
- AD 영역 시퀀스를 수정하려면 개체의 edit icon(수정 아이콘)()을 클릭하십시오.

참조되지 않는 개체를 삭제하려면 해당 개체의 휴지통 아이콘()을 클릭합니다.

단계 **3** 영역 시퀀스 속성을 구성합니다:

- **Name(**이름**)** - 개체의 이름입니다.
- **Description(**설명**)** - 개체의 설명(선택 사항)입니다.
- **AD Realms(AD** 영역**)** — AD 영역 개체를 시퀀스에 추가하려면 **+**를 클릭합니다. 영역을 추가한 후에는 원하는 순서가 지정된 시퀀스로 영역을 클릭하여 끌어다 놓습니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

이제 패시브 ID 규칙에서 AD 영역 시퀀스를 선택할 수 있습니다.

디렉터리 서버 연결 트러블슈팅

시스템은 디렉터리 서버와 통신하기 위해 기능에 따라 다양한 프로세스를 사용합니다. 따라서, ID 정책에 대한 연결은 성공하는 반면 원격 액세스 VPN에 대한 연결에는 실패할 수 있습니다.

이러한 프로세스는 각기 다른 인터페이스를 사용하여 디렉터리 서버와 통신합니다. 다음 인터페이스에서의 연결을 확인해야 합니다.

- ID 정책용 관리 인터페이스.
- 원격 액세스 VPN용 데이터 인터페이스(외부 인터페이스).

ID 영역을 구성할 때 연결에 성공할 수 있는지 확인하기 위해 **Test(**테스트**)** 버튼을 사용합니다. 실패 메시지는 연결에 문제가 있는 기능을 나타냅니다. 다음은 인증 특성 및 라우팅/인터페이스 컨피그레이션에 따라 사용자가 접할 수 있는 일반적인 문제입니다.

디렉터리 사용자 인증 문제입니다**.**

사용자 이름 또는 비밀번호로 인해 시스템이 디렉터리 서버에 로그인할 수 없는 문제의 경우, 이름 및 비밀번호가 디렉터리 서버에 대해 정확하고 유효한지 확인하십시오. Active Directory의 경우에는 사용자에게 상승된 권한이 필요하지 않습니다. 도메인에 어떤 사용자라도 지정할 수 있

습니다. 사용자 이름은 모든 자격 요건에 부합해야 합니다(예: 단지 Administrator가 아닌 Administrator@example.com).

시스템은 사용자 이름 및 비밀번호 정보에서 ldap-login-dn 및 ldap-login-password를 생성합니다. 예를 들어 Administrator@example.com은 cn=administrator,cn=users,dc=example,dc=com으로 변환됩니다. cn=users는 항상 이 변환에 포함되므로 일반 이름 "users" 폴더 아래에 여기서 지정하는 사용자를 구성해야 합니다.

디렉터리 서버에는 데이터 인터페이스를 통해 액세스할 수 있습니다.

디렉터리 서버가 데이터 인터페이스(예: GigabitEthernet 인터페이스)에 직접 연결된 네트워크에 있거나 직접 연결된 네트워크에서 라우팅 가능한 경우, 가상 관리 인터페이스 및 디렉터리 서버 간에 경로가 있는지 확인해야 합니다.

- **data-interfaces**를 관리 게이트웨이로 사용할 경우, 라우팅에 성공해야 합니다.
- 관리 인터페이스에 명시적 게이트웨이가 있는 경우, 해당 게이트웨이 라우터는 디렉터리 서버에 대한 경로를 갖고 있어야 합니다.
- 가상 관리 인터페이스에서 사용하는 실제 인터페이스인 진단 인터페이스에서 IP 주소를 구성할 필요가 없습니다. 그러나 주소를 구성하는 경우 디렉터리 서버에 대한 트래픽을 진단 인터페이스로 리디렉션하는 정적 경로(예: 기본 경로)를 구성하지 마십시오.
- 직접 연결된 네트워크와 디렉터리 서버를 호스팅하는 네트워크 사이에 라우터가 있는 경우, 디렉터리 서버에 대한 정적 경로를 구성합니다(**Device(**디바이스**)** > **Routing(**라우팅**)**).
- 데이터 인터페이스에 올바른 IP 주소 및 서브넷 마스크가 있는지 확인합니다.

디렉터리 서버에는 관리 실제 인터페이스를 통해 액세스할 수 있습니다.

디렉터리 서버가 관리 실제 인터페이스(예: Management0/0)에 직접 연결된 네트워크에 있거나 해당 네트워크에서 라우팅 가능한 경우, 다음 작업을 수행해야 합니다.

- **Device(**디바이스**)** > **Interfaces(**인터페이스**)**에서 관리 인터페이스(논리적 이름이 진단)의 IPv4 주소를 설정합니다. IP 주소는 가상 관리 주소(**Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Management Interface(**관리 인터페이스**)**)와 동일한 서브넷에 있어야 합니다.
- 디렉터리 서버와 관리 인터페이스 사이에 라우터가 있는 경우, 진단 인터페이스에 대해 **Device(**디바이스**)** > **Routing(**라우팅**)**에서 디렉터리 서버의 경로를 설정합니다.
- 진단 인터페이스와 관리 인터페이스에 올바른 IP 주소 및 서브넷 마스크가 있는지 확인합니다.

디렉터리 서버는 외부 네트워크에 있습니다.

디렉터리 서버가 외부(업링크) 인터페이스의 다른 쪽에 있는 네트워크에 있는 경우, 사이트 대 사이트 VPN 연결을 구성해야 할 수 있습니다. 자세한 절차는 원격 액세스 VPN을 통해 외부 네트워크에서 디렉터리 서버를 사용하는 방법, 780 페이지를 참조하십시오.

RADIUS 서버 및 그룹

RADIUS 서버를 사용하여 원격 액세스 VPN 연결과 device manager 및 threat defense CLI 관리 사용자를 인증하고 권한을 부여할 수 있습니다. 예를 들어 Cisco ISE(Identity Services Engine) 및 해당 RADIUS 서버도 사용하는 경우에는 이 서버를 device manager에 사용할 수 있습니다.

RADIUS 서버를 사용하도록 기능을 구성할 때는 개별 서버 대신 RADIUS 그룹을 선택합니다. RADIUS 그룹은 서로의 복사본인 RADIUS 서버가 모인 컬렉션입니다. 그룹에 서버가 여러 개 포함된 경우 이러한 서버는 백업 서버 체인을 형성하여 한 서버를 사용할 수 없는 경우 이중화를 제공합니다. 하지만 서버가 하나뿐이더라도 멤버가 하나인 그룹을 생성하여 기능에 대한 RADIUS 지원을 구성해야 합니다.

다음 주제에서는 RADIUS 서버와 그룹을 지원되는 기능에서 사용할 수 있도록 RADIUS 서버와 그룹을 구성하는 방법을 설명합니다.

RADIUS 서버 구성

RADIUS 서버는 AAA(인증, 권한 부여 및 계정 관리) 서비스를 제공합니다. RADIUS 서버를 통해 사용자를 인증하고 권한을 부여하는 경우 device manager에 해당 서버를 사용할 수 있습니다.

각 RADIUS 서버에 해당하는 개체를 생성한 후에는 각 중복 서버 그룹을 포함할 RADIUS 서버 그룹을 생성합니다.

시작하기 전에

RA VPN에 대해 리디렉션 ACL을 컨피그레이션하려는 경우, 서버 개체를 생성 또는 수정하기 전에 스마트 CLI를 사용해 확장된 ACL을 생성해야 합니다. 개체를 수정하는 동안에는 ACL을 생성할 수 없습니다.

프로시저

단계 **1** 목차에서 **Objects(**개체**)**와 **Identity Sources(ID** 소스**)**를 차례로 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 개체를 생성하려면 **+** > **RADIUS Server(RADIUS** 서버**)**를 클릭합니다.
- 개체를 수정하려면 개체의 수정 아이콘()을 클릭하십시오.

참조되지 않는 개체를 삭제하려면 해당 개체의 휴지통 아이콘()을 클릭합니다.

단계 **3** 다음 속성을 구성합니다.

- **Name(**이름**)** - 개체의 이름입니다. 이 이름은 서버에 구성된 항목과 일치하지 않아도 됩니다.
- **Server Name or IP Address(**서버 이름 또는 **IP** 주소**)** - 서버의 정규화된 호스트 이름(FQDN) 또는 IP 주소입니다. 예를 들어 radius.example.com 또는 10.100.10.10을 입력합니다.

- **Authentication Port(**인증 포트**)** - RADIUS 인증 및 권한 부여가 수행되는 포트입니다. 기본값은 1,812입니다.
- **Timeout(**시간 제한**)** - 시스템이 다음 서버로 요청을 보내기 전까지 서버의 응답을 기다리는 시간(1~300초)입니다. 기본값은 10초입니다. 이 서버를 원격 액세스 VPN에 대한 보조 인증 소스로 사용하는 경우(예: 인증 토큰을 요청하는 메시지 표시), 이 시간제한을 60초 이상으로 높일 수 있습니다. 이를 통해 사용자가 토큰을 획득해 입력할 시간을 제공합니다.
- **Server Secret Key(**서버 비밀 키**)** - (선택 사항). threat defense 디바이스와 RADIUS 서버 간의 데이터를 암호화하는 데 사용되는 공유 암호입니다. 이 키는 대/소문자를 구분하며 공백은 포함하지 않는 영숫자 문자열(최대 64자)입니다. 또한 영숫자 문자 또는 밑줄로 시작해야 하며 특수 문자 $ & - _ . + @는 포함할 수 없습니다. 문자열은 RADIUS 서버에 구성된 것과 일치해야 합니다. 비밀 키를 구성하지 않으면 연결이 암호화되지 않습니다.

단계 **4** (선택 사항). 원격 액세스 VPN 권한 부여 변경 컨피그레이션을 위해 서버를 사용 중인 경우, **RA VPN Only(RA VPN**만**)** 링크를 클릭하여 다음 옵션을 컨피그레이션할 수 있습니다.

- **Redirect ACL(**리디렉션 **ACL)** - RA VPN 리디렉션 ACL에 사용할 확장 ACL을 선택합니다. **Device(**장치**)** > **Advanced Configuration(**고급 구성**)** > **Smart CLI(**스마트 **CLI)** > **Objects(**개체**)** 페이지에서 스마트 CLI **Extended Access List(**확장 액세스 목록**)** 개체를 사용하여 확장 ACL을 생성합니다.

  리디렉션 ACL의 목적은 Cisco ISE(Identity Services Engine)에 초기 트래픽을 전송하여 ISE에서 클라이언트 보안 상태를 평가할 수 있게 하는 것입니다. ACL에서는 ISE에 HTTPS 트래픽을 전송해야 하지만, 이미 ISE가 대상으로 지정된 트래픽 또는 이름 확인을 위해 DNS 서버로 전송되는 트래픽은 전송해서는 안 됩니다. 예시는 Threat Defense 디바이스에서 COA(Change of Authorization) 컨피그레이션, 760 페이지를 참조하십시오.

- **Interface Used to Connect to RADIUS Server(RADIUS** 서버에 연결하는 데 사용할 인터페이스**)** - 서버와 통신할 때 사용할 인터페이스를 결정합니다. **Resolve via Route Lookup(**경로 조회를 통해 확인**)**을 선택하면 시스템에서는 항상 라우팅 테이블을 사용해 어떤 인터페이스를 사용할지 결정합니다. **Manually Choose Interface(**수동으로 인터페이스 선택**)**를 선택하면 시스템에서는 선택한 인터페이스를 항상 사용합니다.

  CoA(Change of Authorization)를 컨피그레이션하려면 시스템에서 인터페이스의 CoA 리스너를 올바르게 활성화할 수 있도록 특정 인터페이스를 선택해야 합니다.

  서버가 관리 주소와 동일한 네트워크에 있는 경우(진단 인터페이스 선택을 의미함), 진단 인터페이스의 IP 주소도 설정해야 합니다. 관리 IP 주소로는 충분하지 않습니다. **Device(**디바이스**)** > **Interfaces(**인터페이스**)**로 이동하여 관리 IP 주소와 동일한 서브넷에 있는 진단 인터페이스에서 IP 주소를 설정합니다.

  또한 device manager 관리 액세스를 위해 이 서버를 사용하는 경우, 이 인터페이스는 무시됩니다. 관리 액세스 시도는 항상 관리 IP 주소를 통해 인증됩니다.

단계 **5** (선택 사항, 개체 수정 시에만 사용함.) **Test(**테스트**)**를 클릭하여 시스템이 서버에 연결할 수 있는지 확인합니다.

사용자 이름과 비밀번호를 입력하라는 메시지가 표시됩니다. 테스트에서는 서버에 연결할 수 있는지, 그리고 서버에 연결할 수 있는 경우 사용자 이름을 인증할 수 있는지를 확인합니다.

단계 **6** **OK(**확인**)**를 클릭합니다.

RADIUS 서버 그룹 구성

RADIUS 서버 그룹은 하나 이상의 RADIUS 서버 개체를 포함합니다. 그룹 내의 서버는 서로의 복사본이어야 합니다. 이러한 서버는 백업 서버 체인을 형성하므로 첫 번째 서버를 사용할 수 없으면 시스템이 목록의 다음 서버 사용을 시도할 수 있습니다.

특정 기능에서 RADIUS 지원을 구성할 때는 서버 그룹을 선택해야 합니다. 따라서 RADIUS 서버가 하나뿐이더라도 해당 서버를 포함하는 서버 그룹을 생성해야 합니다.

프로시저

단계 **1** 목차에서 **Objects(**개체**)**와 **Identity Sources(ID** 소스**)**를 차례로 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 개체를 생성하려면 **+** > **RADIUS Server Group(RADIUS** 서버 그룹**)**을 클릭합니다.
- 개체를 수정하려면 개체의 수정 아이콘( )을 클릭하십시오.

참조되지 않는 개체를 삭제하려면 해당 개체의 휴지통 아이콘( )을 클릭합니다.

단계 **3** 다음 속성을 구성합니다.

- **Name(**이름**)** - 개체의 이름입니다. 이 이름은 서버에 구성된 항목과 일치하지 않아도 됩니다.
- **Dead Time(**비활성 시간**)** - 모든 서버에서 장애가 발생해야 장애 발생 서버가 다시 활성화됩니다. 비활성 시간이란 마지막 서버가 실패한 이후, 모든 서버를 재활성화하기 이전의 대기 시간(0~1440분)입니다. 기본은 10분입니다.
- **Maximum Failed Attempts(**최대 실패 시도 횟수**)** - 다음 서버 사용을 시도하기 전에 그룹의 RADIUS 서버로 전송되었으나 실패한 AAA 트랜잭션(즉, 응답을 받지 못한 요청)의 수입니다. 1~5 사이의 값을 지정할 수 있으며 기본값은 3입니다. 최대 실패 시도 횟수가 초과되면 시스템에서 해당 서버를 Failed(장애 발생)로 표시합니다.

  특정 기능에 대해 로컬 데이터베이스를 사용하여 대체 방법을 구성했는데 그룹의 모든 서버가 응답하지 않으면 해당 그룹은 응답이 없는 것으로 간주되고 대체 방법을 시도합니다. 서버 그룹은 비활성 시간 동안 응답이 없는 것으로 표시됩니다. 따라서 이 기간 내에는 추가 AAA 요청이 서버 그룹 연결을 시도하지 않으며 대체 방법이 즉시 사용됩니다.
- **Dynamic Authorization(**동적 인증**)(RA VPN**에만 해당**)**, **Port(**포트**)** - RADIUS 동적 인증 또는 이 RADIUS 서버 그룹에 대한 CoA(Change of Authorization) 서비스를 활성화할 경우, 해당 그룹은 CoA 알림이 등록되며 ISE(Identity Services Engine)의 CoA 정책 업데이트를 위해 지정된 포트를 수신합니다. 기본 수신 포트는 1700입니다. 또는 1024~65535 범위 내에서 다른 포트를 지정할 수 있습니다. ISE와 함께 원격 액세스 VPN에서 이 서버 그룹을 사용하는 경우에만 동적 인증을 활성화합니다.

- **Realm that Supports the RADIUS Server(RADIUS** 서버를 지원하는 영역**)** - 사용자 인증을 위해 AD 서버를 사용하도록 RADIUS 서버를 컨피그레이션하는 경우, 이 RADIUS 서버와 함께 사용되는 AD 서버를 지정하는 AD 영역을 선택합니다. 영역이 아직 없는 경우, 목록 아래에 있는 **Create New Identity Realm(**새 **ID** 영역 생성**)**을 클릭하여 영역을 바로 컨피그레이션합니다.
- **RADIUS Server list(RADIUS** 서버 목록**)** - 그룹의 서버를 정의하는 RADIUS 서버 개체를 16개까지 선택합니다. 이러한 개체는 우선순위대로 추가합니다. 목록의 첫 번째 서버가 응답이 없는 상태가 될 때까지 계속 사용됩니다. 개체를 추가한 후에는 끌어 놓기를 통해 개체를 다시 정렬할 수 있습니다. 필요한 개체가 아직 없으면 **Create New RADIUS Server(**새 **RADIUS** 서버 생성**)**를 클릭하여 바로 추가합니다.

  Test(테스트**)** 링크를 클릭하여 시스템이 서버에 연결할 수 있는지를 확인할 수도 있습니다. 사용자 이름과 비밀번호를 입력하라는 메시지가 표시됩니다. 테스트에서는 서버에 연결할 수 있는지, 그리고 서버에 연결할 수 있는 경우 사용자 이름을 인증할 수 있는지를 확인합니다.

단계 **4** (선택 사항). **Test All Servers(**모든 서버 테스트**)** 버튼을 클릭하여 그룹의 각 서버에 대한 연결을 확인합니다.

사용자 이름과 비밀번호를 입력하라는 메시지가 표시됩니다. 시스템은 각 서버에 연결할 수 있는지, 그리고 각 서버에서 사용자 이름을 인증할 수 있는지를 확인합니다.

단계 **5** **OK(**확인**)**를 클릭합니다.

RADIUS 서버 및 그룹 트러블슈팅

외부 권한 부여가 작동하지 않는 경우 확인할 수 있는 몇 가지 사항은 다음과 같습니다.

- RADIUS 서버 및 서버 그룹 개체의 **Test(**테스트**)** 버튼을 사용하여 디바이스에서 서버에 연결할 수 있는지 확인합니다. 테스트 전에 개체를 저장해야 합니다. 테스트에 실패하는 경우 다음을 수행합니다.
  - 테스트에서 서버에 대해 구성된 인터페이스를 무시하고 항상 관리 인터페이스를 사용한다는 점을 이해하십시오. RADIUS 인증 프록시가 관리 IP 주소의 요청에 응답하도록 구성되지 않은 경우 테스트는 실패할 것으로 예상됩니다.
  - 테스트 중에 정확한 사용자 이름/비밀번호 조합을 입력했는지 확인합니다. 이러한 정보가 부정확한 경우에는 Bad Credentials(잘못된 크리덴셜) 메시지가 표시됩니다.
  - 서버의 비밀 키, 포트 및 IP 주소를 확인합니다. 호스트 이름을 사용하는 경우 관리 인터페이스에 대해 DNS가 구성되어 있는지 확인합니다. 비밀 키가 RADIUS 서버에서는 변경되었는데 디바이스 컨피그레이션에서는 변경되지 않았을 가능성을 고려합니다.
  - 테스트에 계속 실패하면 RADIUS 서버에 대한 정적 경로를 구성해야 할 수 있습니다. CLI 콘솔이나 SSH 세션에서 서버에 ping을 시도하여 서버에 연결할 수 있는지 확인합니다.
- 이전에는 작동한 외부 인증이 중지된 경우 모든 서버가 비활성 시간에 있는 가능성을 고려합니다. 특정 그룹 내의 모든 RADIUS 서버에 장애가 발생한 경우 비활성 시간은 첫 번째 서버 연결

을 다시 시도할 때까지 시스템이 대기하는 시간(분)입니다. 기본값은 10분이지만 최대 1440분까지 구성할 수 있습니다.

- HTTPS 외부 인증이 일부 사용자에 대해서만 작동하는 경우, 각 사용자 계정에 대해 RADIUS 서버에 정의된 cisco-av-pair 속성을 평가합니다. 이 특성이 올바르지 않게 구성되어 있을 수 있습니다. 속성이 누락되거나 올바르지 않은 경우, 해당 사용자 계정에 대한 모든 HTTS 액세스가 차단됩니다.
- SSH 외부 인증이 일부 사용자에 대해서만 작동하는 경우, 각 사용자 계정에 대해 RADIUS 서버에 정의된 Service-Type 속성을 평가합니다. 이 특성이 올바르지 않게 구성되어 있을 수 있습니다. 속성이 누락되거나 올바르지 않은 경우, 해당 사용자 계정에 대한 모든 SSH 액세스가 차단됩니다.

Identity Services Engine (ISE)

Cisco ISE(Identity Services Engine) 또는 ISE-PIC(ISE Passive Identity Connector) 구축을 threat defense 디바이스와 통합하여 ISE/ISE-PIC를 패시브 인증에 사용할 수 있습니다.

신뢰할 수 있는 ID 소스인 ISE/ISE-PIC는 AD(Active Directory), LDAP, RADIUS 또는 RSA를 사용하여 인증하는 사용자에 대한 사용자 인식 데이터를 제공합니다. 그러나 threat defense의 경우에는 사용자 ID 인식을 위해 ISE를 사용할 때 AD만 사용할 수 있습니다. 사용자 ID를 액세스 제어 및 SSL 암호 해독 정책에서 일치 기준으로 사용할 수 있습니다. 또한 다양한 모니터링 대시보드 및 이벤트에서 사용자 정보를 확인할 수 있습니다.

Cisco ISE/ISE-PIC에 대한 자세한 내용은 *Cisco Identity Services Engine* 관리자 가이드 (https://www.cisco.com/c/en/us/support/security/identity-services-engine/tsd-products-support-series-home.html) 및 *ISE-PIC(Identity Services Engine Passive Identity Connector)* 설치 및 관리자 가이드(https://www.cisco.com/c/en/us/support/security/ise-passive-identity-connector/tsd-products-support-series-home.html)를 참조하십시오.

ISE에 대한 지침 및 제한 사항

- 방화벽 시스템에서는 Active Directory 인증과 함께 802.1x 디바이스 인증을 지원하지 않습니다. 이는 시스템에서 디바이스 인증을 사용자에게 연결하지 않기 때문입니다. 802.1x 활성 로그인을 사용하는 경우에는 802.1x 활성 로그인(디바이스와 사용자 둘 다)만 보고하도록 ISE를 구성합니다. 이렇게 하면 디바이스 로그인이 시스템에 한 번만 보고됩니다.
- ISE/ISE-PIC에서는 ISE 게스트 서비스 사용자의 활동을 보고하지 않습니다.
- ISE/ISE-PIC 서버와 디바이스의 시간을 동기화합니다. 그렇지 않으면 시스템이 예기치 않은 간격으로 사용자 시간 제한을 수행할 수 있습니다.
- 많은 사용자 그룹을 모니터링하도록 ISE-PIC를 구성하는 경우 시스템은 메모리 제한으로 인해 그룹을 기준으로 사용자 매핑을 삭제할 수 있습니다. 그 결과, 영역이 있는 규칙 또는 사용자 조건이 정상적으로 수행되지 않을 수 있습니다.

- 이 시스템 버전과 호환되는 특정 ISE/ISE-PIC 버전에 대한 자세한 내용은 *Cisco Secure Firepower* 호환성 가이드(https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-device-support-tables-list.html)를 참고하십시오.
- 사용 중인 ISE 버전이 IPv6을 지원하는지 확인하지 않았다면 ISE 서버의 IPv4 주소를 사용하십시오.

ISE(Identity Services Engine) 구성

Cisco ISE(Identity Services Engine) 또는 Cisco ISE PIC(Identity Services Engine Passive Identity Connector)를 패시브 ID 소스로 사용하려면 ISE pxGrid(Platform Exchange Grid) 서버에 대한 연결을 구성해야 합니다.

시작하기 전에

- ISE에서 pxGrid 및 MNT 서버 인증서를 내보냅니다. 예를 들어 ISE PIC 2.2에서는 **Certificates(**인증서**)** > **Certificate Management(**인증서 관리**)** > **System Certificates(**시스템 인증서**)** 페이지에서 이러한 인증서를 확인할 수 있습니다. 인증서 목록의 Used By(사용한 사람) 열에는 MNT(모니터링 및 트러블슈팅 노드)가 Admin(관리자)로 표시됩니다. 인증서는 **Objects(**개체**)** > **Certificates(**인증서**)** 페이지에서 신뢰할 수 있는 CA 인증서로 업로드할 수도 있고 다음 절차 중에 업로드할 수도 있습니다. 이러한 노드는 동일한 인증서를 사용 중일 수 있습니다.
- AD ID 영역도 구성해야 합니다. 시스템은 AD에서 사용자 목록을 가져오며 ISE에서 사용자-IP 주소 매핑 정보를 가져옵니다.
- 정적 보안 그룹 태그 매핑을 사용하거나 사용하지 않고 액세스 제어에 SGT(Security Group Tag)를 사용하여 SXP 주제를 수신하려면 ISE에 SXP 및 이러한 매핑을 구성해야 합니다. ISE에서 보안 그룹 및 SXP 게시 구성, 549 페이지의 내용을 참조하십시오.

프로시저

단계 **1** 목차에서 **Objects(**개체**)**와 **Identity Sources(ID** 소스**)**를 차례로 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 개체를 생성하려면 **+** > **ISE(Identity Services Engine)**를 클릭합니다. ISE 개체는 하나까지만 생성할 수 있습니다.
- 개체를 수정하려면 개체의 수정 아이콘()을 클릭하십시오.

참조되지 않는 개체를 삭제하려면 해당 개체의 휴지통 아이콘()을 클릭합니다.

단계 **3** 다음 속성을 구성합니다.

- **Name(**이름**)** - 개체의 이름입니다.
- **Status(**상태**)** - 토글을 클릭하여 개체를 활성화하거나 비활성화합니다. 비활성화하면 ID 규칙에서 ISE를 ID 소스로 사용할 수 없습니다.

- **Description(**설명**)** - 개체의 설명(선택 사항)입니다.
- **Primary Node Hostname/IP Address(**기본 노드 호스트 이름**/IP** 주소**)** - 기본 pxGrid ISE 서버의 호스트 이름 또는 IP 주소입니다. 사용 중인 ISE 버전이 IPv6을 지원하는지 확인하지 않았다면 IPv6 주소를 지정하지 마십시오.
- **Secondary Node Hostname/IP Address(**보조 노드 호스트네임**/IP** 주소**)** - 고가용성을 위해 보조 ISE 서버를 설정하는 경우, **Add Secondary Node Hostname/IP Address(**보조 노드 호스트네임**/IP** 주소 추가**)**를 클릭하고 보조 pxGrid ISE 서버의 호스트네임 또는 IP 주소를 입력합니다.
- **pxGrid Server CA Certificate(pxGrid** 서버 **CA** 인증서**)** - 신뢰할 수 있는 pxGrid 프레임워크용 인증 기관 인증서입니다. 구축에 기본 및 보조 pxGrid 노드가 포함된 경우 동일한 인증 증명으로 두 가지 노드의 인증서를 서명해야 합니다.
- **MNT Server CA Certificate(MNT** 서버 **CA** 인증서**)** - 일괄 다운로드를 수행할 때 신뢰할 수 있는 ISE 인증서용 인증 기관 인증서입니다. MNT(모니터링 및 트러블슈팅) 서버가 별도로 지정되어 있지 않은 경우 pxGrid 서버 인증서와 같을 수 있습니다. 구축에 기본 및 보조 MNT 노드가 포함된 경우 동일한 인증 증명으로 두 가지 노드의 인증서를 서명해야 합니다.
- **Server Certificate(**서버 인증서**)** - ISE에 연결하거나 일괄 다운로드를 수행할 때 threat defense 디바이스가 ISE에 제공해야 하는 내부 ID 인증서입니다.
- **Subscribe To(**구독 대상**)** — 어떤 ISE pxGrid 주제를 구독할지 선택합니다. 주제를 구독하면 해당 주제와 관련된 데이터를 다운로드할 수 있습니다.
  - **Session Directory Topic(**세션 디렉토리 주제**)** — 사용자 세션에 대한 SGT 매핑을 비롯한 사용자 세션에 대한 정보를 가져올지 여부입니다. 이 옵션은 기본적으로 활성화되어 있습니다. 보안 정책에 사용하고 모니터링 대시보드에서 볼 수 있도록 패시브 사용자 ID를 가져오려면 이 옵션을 선택해야 합니다.
  - **SXP Topic(SXP** 주제**)** — 정적 SGT-IP 주소 매핑을 가져올지 여부입니다. SGT(Security Group Tag)를 기반으로 액세스 제어 규칙을 작성하려면 이 항목을 선택합니다.
- **ISE Network Filters(ISE** 네트워크 필터**) - ISE**가 시스템에 보고하는 데이터를 제한하기 위해 설정할 수 있는 선택적 필터입니다. 네트워크 필터를 제공하는 경우 ISE는 필터 내의 네트워크에서만 데이터를 보고합니다. **+**를 클릭하고 네트워크를 식별하는 네트워크 개체를 선택한 후에 **OK(**확인**)**를 클릭합니다. 개체를 생성해야 하는 경우 **Create New Network(**새 네트워크 생성**)**를 클릭합니다. IPv4 네트워크 개체만 구성합니다.

단계 **4** **Test(**테스트**)** 버튼을 클릭하여 시스템이 ISE 서버에 연결할 수 있는지 확인합니다.

테스트에 실패하는 경우 **See Logs(**로그 보기**)** 링크를 클릭하여 자세한 오류 메시지를 확인합니다. 예를 들어 다음 메시지는 시스템이 필요한 포트에서 서버에 연결하지 못했음을 나타냅니다. 호스트로의 경로가 없거나, ISE 서버가 필요한 포트를 사용하고 있지 않거나, 연결을 차단하는 액세스 제어 규칙이 문제일 수 있습니다.

```
Captured Jabberwerx log:2018-05-11T16:10:30 [   ERROR]: connection timed out while
trying to test connection to host=10.88.127.142:ip=10.88.127.142:port=5222
```

단계 **5** **OK(**확인**)**를 클릭하여 개체를 저장합니다.

다음에 수행할 작업

ISE를 구성한 후 ID 정책을 활성화하고, 패시브 인증 규칙을 구성하고, 컨피그레이션을 구축합니다. 그런 다음 ISE/ISE PIC로 이동하여 디바이스를 서브스크라이버로 수락해야 합니다. ISE/ISE PIC가 서브스크라이버를 자동 수락하도록 구성하면 서브스크립션을 수동으로 수락할 필요가 없습니다.

ISE/ISE-PIC ID 소스 트러블슈팅

ISE/ISE-PIC 연결

ISE 또는 ISE-PIC 연결에 문제가 발생한 경우 다음을 확인하십시오.

- ISE를 threat defense 디바이스와 성공적으로 통합하려면 우선 ISE에서 pxGrid Identity Mapping(pxGrid ID 매핑) 기능을 활성화해야 합니다.
- ISE 서버와 threat defense 디바이스 간의 연결에 성공하려면 ISE에서 클라이언트를 수동으로 승인해야 합니다.

  Cisco Identity Services Engine 관리자 가이드의 사용자 및 외부 ID 소스 관리 장에서 설명하는 것처럼 ISE에서 **Automatically approve new accounts(**새 어카운트 자동 승인**)**를 활성화할 수도 있습니다.
- threat defense 디바이스(서버) 인증서는 **clientAuth** 확장 키 사용 값을 포함해야 하거나 아무 확장 키 사용 값도 포함하지 않아야 합니다. clientAuth 확장 키 사용이 설정되어 있는 경우에는 키 사용이 설정되어 있지 않거나 디지털 서명 키 사용 값이 설정되어 있어야 합니다. device manager를 사용하여 생성할 수 있는 자체 서명 ID 인증서는 이러한 요구 사항을 충족합니다.
- ISE 서버의 시간은 threat defense 디바이스의 시간과 동기화되어야 합니다. 어플라이언스가 동기화되지 않은 경우, 시스템이 예기치 않은 간격으로 사용자 시간 제한을 수행할 수 있습니다.

ISE/ISE-PIC 사용자 데이터

ISE 또는 ISE-PIC에서 보고된 사용자 데이터에 문제가 발생한 경우 다음을 참고하십시오.

- 데이터베이스에 데이터가 아직 없는 ISE 사용자의 활동이 탐지되면 시스템은 서버에서 관련된 정보를 검색합니다. 시스템이 사용자 다운로드에서 사용자에 대한 정보를 성공적으로 검색할 때까지는 ISE 사용자가 확인한 활동이 액세스 제어 규칙으로 처리되지 않으며, 대시보드에 표시되지도 않습니다.
- LDAP, RADIUS 또는 RSA 도메인 컨트롤러에서 인증된 ISE 사용자에 대해서는 사용자 제어를 수행할 수 없습니다.
- 시스템은 ISE 게스트 서비스 사용자의 사용자 데이터를 수신하지 않습니다.

SAML 서버

원격 액세스 VPN 연결을 위한 SSO(Single Sign-On) 인증 소스로 사용할 SAML 2.0(Security Assertion Markup Language 2.0) 서버를 구성할 수 있습니다. SAML은 당사자 간에 인증 및 권한 부여 데이터, 특히 IdP(Identity Provider)와 SP(Service Provider)를 교환하기 위한 개방형 표준입니다.

참고 지원되는 SAML 서버: Duo

SAML 서버 구성

원격 액세스 VPN 연결을 위한 SSO(Single Sign-On) 인증 소스로 사용할 SAML 2.0(Security Assertion Markup Language 2.0) 서버를 구성할 수 있습니다. 예를 들어 DAG(Duo Access Gateway)는 SAML 서버입니다.

RA VPN에서 SAML 서버를 인증 방법으로 사용하는 경우 SAML 서버는 IdP(Identity Provider)로 작동하는 반면 threat defense 디바이스는 SP(Service Provider)로 작동합니다.

SAML 서버를 기본 인증 소스로 사용할 수 있습니다. SAML을 사용할 때는 보조 인증 소스를 구성할 수 없으며 대체 소스를 구성할 수도 없습니다.

시작하기 전에

SAML 서버 ID 공급자에서 다음 정보를 가져옵니다.

- SAML 서버 메타데이터를 제공하는 엔티티 ID URL
- 로그인 URL
- 로그아웃 URL
- ID 공급자 인증서

프로시저

단계 **1** 다음 중 하나를 수행하여 SAML 서버 페이지로 이동합니다.

- 목차에서 **Objects(**개체**)**와 **Identity Sources(ID** 소스**)**를 차례로 선택합니다.
- **Device(**디바이스**)** > **Remote Access VPN(**원격 액세스 **VPN)** > **SAML Servers(SAML** 서버**)**를 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 개체를 생성하려면 **+** > **SAML Server(SAML** 서버**)**를 클릭합니다.
- 개체를 수정하려면 개체의 수정 아이콘( )을 클릭하십시오.

참조되지 않는 개체를 삭제하려면 해당 개체의 휴지통 아이콘( )을 클릭합니다.

단계 **3** 다음 속성을 구성합니다.

- **Name(**이름**)** - 개체의 이름입니다.
- **Description(**설명**)** - 개체의 설명(선택 사항)입니다.
- **Identity Provider (IDP) Entity ID URL(IdP(ID** 공급자**)** 엔티티 **ID URL)** — SAML 발급자가 요청에 응답하는 방법을 설명하는 메타데이터 XML을 제공하는 페이지의 URL입니다. 일부 SAML 서버 제품에서는 이를 엔티티 ID라고 하고, 일부는 메타데이터 URL이라고 합니다. URL은 프로토콜 https://를 포함하여 4~256자 사이여야 합니다. (예: https://191.168.2.21/dag/saml2/idp/metadata.php)
- **Sign-In URL(**로그인 **URL)** — ID 공급자 SAML 서버에 로그인하기 위한 URL입니다. URL은 프로토콜을 포함하여 4~500자 사이여야 합니다. http:// 및 https:// 모두 허용됩니다. (예: https://191.168.2.21/dag/saml2/idp/SSOService.php)
- **Sign-Out URL(**로그아웃 **URL)** - ID 공급자 SAML 서버에서 로그아웃하기 위한 URL입니다. URL은 프로토콜을 포함하여 4~500자 사이여야 합니다. http:// 및 https:// 모두 허용됩니다. (예: https://191.168.2.21/dag/saml2/idp/SingleLogoutService.php)
- **Service Provider Certificate(FTD** 서비스 공급자 인증서**)** — threat defense 디바이스에 사용할 내부 인증서입니다. 원칙적으로는 인증된 서드 파티에서 서명한 인증서를 이미 업로드했으므로 지금 선택할 수 있습니다. 또한 내장된 DefaultInternalCertificate를 사용하거나 **Create New Internal Certificate(**새 내부 인증서 생성**)**를 클릭하여 서명된 인증서를 지금 업로드할 수도 있습니다. SAML 서버 ID 공급자는 이 인증서를 신뢰해야 하므로 SAML 서버에 이를 업로드해야 할 수 있습니다. 인증서를 업로드하거나 서비스 공급자와의 신뢰 관계를 활성화하는 방법에 대한 자세한 내용은 SAML 서버 설명서를 참조하십시오.
- **Identity Provider Certificate(ID** 공급자 인증서**)** — SAML 서버 ID 공급자에 대해 신뢰할 수 있는 CA 인증서입니다. SAML 서버에서 이 인증서를 다운로드합니다. 아직 업로드하지 않은 경우 **Create New Trusted CA Certificate(**새 신뢰할 수 있는 **CA** 인증서 생성**)**를 클릭하여 지금 업로드합니다.
- **Request Signature(**서명 요청**)** — 로그인 요청에 서명할 때 사용할 암호화 알고리즘입니다. 암호화를 비활성화하려면 None(없음)을 선택합니다. 그렇지 않은 경우에는 SHA1, SHA256, SHA384, SHA512(가장 약한 순서에서 가장 강한 순서로 나열) 중 하나를 선택합니다.
- **Request Timeout(**요청 시간 초과**)** - SAML 어설션에는 유효 기간이 있습니다. 사용자는 유효 기간 내에 SSO(Single Sign-On) 요청을 완료해야 합니다. 시간 초과(초 단위)를 설정하여 이 기간을 변경할 수 있습니다. 어설션의 NotOnOrAfter 조건보다 긴 값으로 시간 초과를 설정할 경우 이 시간 초과를 무시하고 NotOnOrAfter가 적용됩니다. 범위는 1~7200초입니다. 기본값은 300초입니다.
- **This SAML identity provider (IDP) is on an internal network(**이 **SAML ID** 공급자**(IDP)**가 내부 네트워크에 있습니다**)** — SAML 서버가 보호받는 네트워크의 외부가 아닌 내부 네트워크에서 작동하는지 여부.

- **Request IDP re-authentication at login(**로그인 시 **IDP** 재인증 요청**)** — SAML 서버가 이전 인증 세션을 다시 사용하지 않고 사용자가 로그인할 때마다 재인증하려면 이 옵션을 선택합니다. 이 옵션은 기본적으로 활성화되어 있습니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

로컬 사용자

로컬 사용자 데이터베이스(LocalIdentitySource)에는 device manager에 정의한 사용자가 포함되어 있습니다.

로컬에서 정의된 사용자는 다음과 같은 목적으로 사용할 수 있습니다.

- 원격 액세스 VPN(기본 또는 대체 ID 소스로 사용)
- 관리 액세스(device manager 사용자에 대한 기본 또는 보조 소스로 사용).

  관리 사용자는 시스템 정의 로컬 사용자입니다. 그러나 관리 사용자는 원격 액세스 VPN에 로그인할 수 없습니다. 추가 로컬 관리 사용자를 생성할 수도 없습니다.

  관리 액세스용 외부 인증을 정의하는 경우에는 디바이스에 로그인하는 외부 사용자가 로컬 사용자 목록에 표시됩니다.
- ID 정책(원격 액세스 VPN 로그인에서 사용자 ID를 수집하기 위한 패시브 ID 소스로 간접 사용).

다음 주제에서는 로컬 사용자를 구성하는 방법을 설명합니다.

로컬 사용자 구성

원격 액세스 VPN에 사용할 디바이스에서 직접 사용자 어카운트를 생성할 수 있습니다. 외부 인증 소스 대신 또는 외부 인증 소스와 함께 로컬 사용자 어카운트를 사용할 수 있습니다.

로컬 사용자 데이터베이스를 원격 액세스 VPN용 대체 인증 방법으로 사용하는 경우, 외부 데이터베이스의 이름과 같은 사용자 이름/비밀번호를 로컬 데이터베이스에서 구성해야 합니다. 그렇지 않으면 대체 메커니즘이 적용되지 않습니다.

여기서 정의하는 사용자는 디바이스 CLI에 로그인할 수 없습니다.

프로시저

단계 **1** **Objects(**개체**)** > **Users(**사용자**)**를 선택합니다.

목록에 사용자 이름과 서비스 유형이 표시되며, 다음과 같습니다.

- MGMT - device manager에 로그인할 수 있는 관리 사용자입니다. 관리 사용자는 항상 정의되어 있으며 삭제할 수 없습니다. 추가 MGMT 사용자를 구성할 수도 없습니다. 그러나 관리 액세스용

외부 인증을 정의하는 경우에는 디바이스에 로그인하는 외부 사용자가 로컬 사용자 목록에 MGMT 사용자로 표시됩니다.

- RA VPN - 디바이스에 구성된 원격 액세스 VPN에 로그인할 수 있는 사용자입니다. 기본 또는 보조(대체) 소스용 로컬 데이터베이스도 선택해야 합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 사용자를 추가하려면 +를 클릭합니다.
- 사용자를 수정하려면 해당 사용자의 수정 아이콘()을 클릭합니다.

특정 사용자 어카운트가 더 이상 필요하지 않으면 해당 사용자의 삭제 아이콘()을 클릭합니다.

단계 **3** 사용자 속성을 구성합니다.

이름과 비밀번호는 인쇄 가능한 모든 ASCII 영숫자 또는 특수 문자(공백과 물음표 제외)를 포함할 수 있습니다. 인쇄 가능한 문자는 ASCII 코드 33~126입니다.

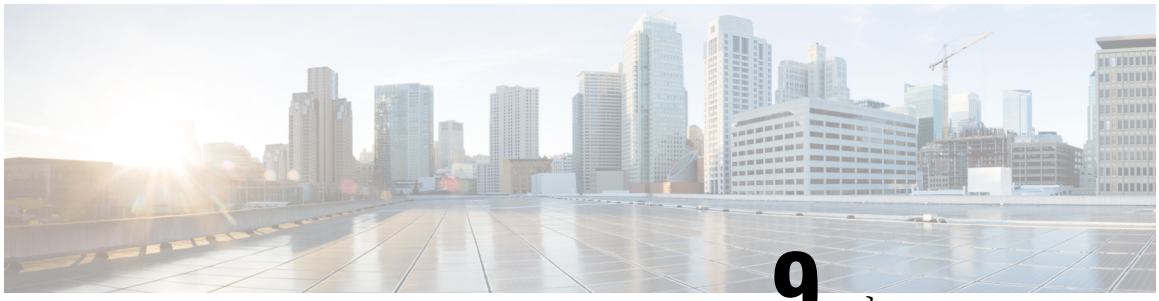
- **Name(**이름**)** - 원격 액세스 VPN에 로그인하기 위한 사용자 이름입니다. 이 이름은 4~64자로 지정할 수 있으며 공백은 포함할 수 없습니다. 예를 들어 johndoe와 같은 이름을 사용합니다.
- **Password(**비밀번호**)**, **Confirm Password(**비밀번호 확인**)** - 어카운트의 비밀번호를 입력합니다. 비밀번호는 8~16자여야 하며 같은 문자를 연속으로 포함할 수는 없습니다. 또한 숫자, 대/소문자, 특수 문자를 각각 하나 이상 포함해야 합니다.

참고 사용자는 비밀번호를 변경할 수 없습니다. 관리자가 사용자에게 비밀번호를 알려 주어야 하며, 비밀번호를 변경해야 하는 경우 관리자가 사용자 어카운트를 수정해야 합니다. 또한 외부 MGMT 사용자의 비밀번호는 업데이트하지 마십시오. 해당 비밀번호는 외부 AAA 서버를 통해 제어됩니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

III 부

기본 사항



9 장

Firepower 4100/9300의 논리적 디바이스

Firepower 4100/9300은 하나 이상의 논리적 디바이스를 설치할 수 있는 유연한 보안 플랫폼입니다.

섀시 인터페이스를 구성하고, 논리적 디바이스를 추가하고, Secure Firewall 섀시 관리자 또는 FXOS CLI를 사용하는 Firepower 4100/9300 섀시의 디바이스에 인터페이스를 할당해야 합니다. device manager에서는 이러한 작업을 수행할 수 없습니다.

이 장에서는 기본 인터페이스 구성 및 섀시 관리자를 사용하여 독립형 디바이스 또는 고가용성 논리적 디바이스를 추가하는 방법을 설명합니다. FXOS CLI를 사용하려면 FXOS CLI 구성 가이드를 참조하십시오. 고급 FXOS 절차 및 트러블슈팅에 대한 자세한 내용은 FXOS 구성 가이드를 참조하십시오.

인터페이스 정보

Firepower 4100/9300 섀시에서는 물리적 인터페이스 및 EtherChannel(포트-채널) 인터페이스를 지원합니다. EtherChannel 인터페이스는 동일한 유형의 멤버 인터페이스를 최대 16개까지 포함할 수 있습니다.

섀시 관리 인터페이스

섀시 관리 인터페이스는 SSH 또는 섀시 관리자를 통한 FXOS 섀시 관리에 사용됩니다. 이 인터페이스는 애플리케이션 관리용 논리적 디바이스에 할당하는 관리 유형 인터페이스와는 별개입니다.

이 인터페이스의 파라미터는 CLI에서 구성해야 합니다. FXOS CLI에서 이 인터페이스에 대한 정보를 확인하려면 로컬 관리에 연결한 다음 관리 포트를 표시합니다.

Firepower # **connect local-mgmt**

Firepower(local-mgmt) # **show mgmt-port**

실제 케이블이나 SFP 모듈 연결을 해제하거나 **mgmt-port shut** 명령을 수행하더라도 섀시 관리 인터페이스는 계속 작동합니다.

참고 섀시 관리 인터페이스는 점보 프레임을 지원하지 않습니다.

인터페이스 유형

물리적 인터페이스 EtherChannel(포트-채널) 인터페이스는 다음 유형 중 하나가 될 수 있습니다.

- Data(데이터) - 일반 데이터에 사용합니다. 데이터 인터페이스는 논리적 디바이스 간에 공유할 수 없으며 논리적 디바이스는 백플레인을 통해 다른 논리적 디바이스와 통신할 수 없습니다. 데이터 인터페이스의 트래픽의 경우, 모든 트래픽은 하나의 인터페이스에서 섀시를 종료하고 다른 인터페이스로 돌아가서 다른 논리적 디바이스에 연결해야 합니다.
- Data-sharing(데이터 공유) - 일반 데이터에 사용합니다. 컨테이너 인스턴스에서만 지원되는 이러한 데이터 인터페이스는 하나 이상의 논리적 디바이스/컨테이너 인스턴스(threat defense-사용-management center 전용).에서 공유할 수 있습니다.
- Mgmt(관리) - 애플리케이션 인스턴스를 관리하는 데 사용합니다. 이러한 인터페이스는 외부 호스트에 액세스하기 위해 하나 이상의 논리적 디바이스에서 공유할 수 있습니다. 단, 논리적 디바이스에서는 인터페이스를 공유하는 다른 논리적 디바이스와 이 인터페이스를 통해 통신할 수 없습니다. 논리적 디바이스당 관리 인터페이스 1개만 할당할 수 있습니다. 애플리케이션 및 관리자에 따라 나중에 데이터 인터페이스에서 관리를 활성화할 수 있습니다. 데이터 관리를 활성화한 후 이를 사용하지 않으려는 경우에도 관리 인터페이스를 논리적 디바이스에 할당해야 합니다.개별 섀시 관리 인터페이스에 대한 내용은 섀시 관리 인터페이스, 197 페이지 항목을 참조하십시오.

참고 관리 인터페이스를 변경하면 논리적 디바이스가 재부팅됩니다. 예를 들어 e1/1에서 e1/2로 변경하면 논리적 디바이스가 재부팅되어 새 관리가 적용됩니다.

- 이벤트 처리—threat defense-사용-management center 디바이스의 보조 관리 인터페이스로 사용합니다.

참고 각 애플리케이션 인스턴스가 설치될 때 가상 이더넷 인터페이스가 할당됩니다. 애플리케이션에서 이벤트 인터페이스를 사용하지 않는 경우 가상 인터페이스는 관리자 중단 상태가 됩니다.

```
Firepower # show interface Vethernet775
Firepower # Vethernet775 is down (Administratively down)
Bound Interface is Ethernet1/10
Port description is server 1/1, VNIC ext-mgmt-nic5
```

- Cluster(클러스터) - 클러스터형 논리적 디바이스용 클러스터 제어 링크로 사용합니다. 기본적으로, 클러스터 제어 링크는 Port-channel 48에서 자동으로 생성됩니다. 이 클러스터 유형은 EtherChannel 인터페이스에서만 지원됩니다. device manager 및 CDO는 클러스터링을 지원하지 않습니다.

FXOS 인터페이스와 애플리케이션 인터페이스 비교

Firepower 4100/9300에서는 물리적 인터페이스 및 EtherChannel(포트-채널) 인터페이스의 기본 이더넷 설정을 관리합니다. 애플리케이션 내에서는 상위 레벨 설정을 구성합니다. 예를 들어 FXOS에서는 Etherchannel만 생성할 수 있습니다. 그러나 애플리케이션 내의 EtherChannel에 IP 주소를 할당할 수 있습니다.

다음 섹션에서는 FXOS와 인터페이스에 대한 애플리케이션 간의 상호 작용에 대해 설명합니다.

VLAN 하위 인터페이스

논리적 디바이스의 경우에는 애플리케이션 내에서 VLAN 하위 인터페이스를 생성할 수 있습니다.

섀시와 애플리케이션의 독립 인터페이스 상태

관리를 위해 섀시와 애플리케이션에서 인터페이스를 활성화하고 비활성화할 수 있습니다. 인터페이스는 두 운영 체제에서 모두 활성화해야 작동합니다. 인터페이스 상태는 독립적으로 제어되므로 섀시와 애플리케이션에서 상태가 일치하지 않을 수도 있습니다.

Firepower 9300 하드웨어 및 소프트웨어 조합에 대한 요건 및 사전 요구 사항

Firepower 9300에는 3개의 보안 모듈 슬롯 및 여러 유형의 보안 모듈이 포함되어 있습니다. 다음 요건을 참조하십시오.

- 보안 모듈 유형 - Firepower 9300에 다양한 유형의 모듈을 설치할 수 있습니다. 예를 들어, SM-48을 모듈 1로, SM-40을 모듈 2로, SM-56를 모듈 3으로 설치할 수 있습니다.
- 기본 및 컨테이너 인스턴스 - 보안 모듈에 컨테이너 인스턴스를 설치하는 경우 해당 모듈에서는 다른 컨테이너 인스턴스만 지원할 수 있습니다. 기본 인스턴스에서는 모듈의 모든 리소스를 사용하므로 모듈에는 하나의 기본 인스턴스만 설치할 수 있습니다. 일부 모듈에서는 기본 인스턴스를, 다른 모듈에서는 컨테이너 인스턴스를 사용할 수 있습니다. 예를 들어 모듈 1 및 모듈 2에는 기본 인스턴스를 설치할 수 있지만, 모듈 3에는 컨테이너 인스턴스를 설치할 수 있습니다.
- 고가용성 - 고가용성은 Firepower 9300에서 동일한 유형의 모듈 간에만 지원됩니다. 그러나 두 섀시에는 혼합 모듈을 포함할 수 있습니다. 각 섀시에 SM-56, SM-48 및 SM-40이 있는 경우를 예로 들 수 있습니다. SM-40 모듈 간, SM-48 모듈 간, SM-56 모듈 간에 고가용성 쌍을 생성할 수 있습니다.

- ASA 및 threat defense애플리케이션 유형 - 섀시의 개별 모듈에 서로 다른 애플리케이션 유형을 설치할 수 있습니다. 예를 들어, 모듈 1 및 모듈 2에는 ASA를 설치하고 모듈 3에는 threat defense를 설치할 수 있습니다.
- ASA 또는 threat defense 버전 - 애플리케이션 인스턴스 유형의 서로 다른 버전을 별도의 모듈에서 실행하거나 동일한 모듈에서 별도의 컨테이너 인스턴스로 실행할 수 있습니다. 예를 들어, 모듈 1에는 threat defense 6.3을, 모듈 2에는 threat defense 6.4를 설치하고, 모듈 3에는 threat defense 6.5를 설치할 수 있습니다.

논리적 디바이스 관련 지침 및 제한 사항

지침 및 제한 사항은 다음 섹션을 참조하십시오.

인터페이스에 대한 지침 및 제한 사항

기본 MAC 주소

기본 MAC 주소 할당은 인터페이스의 유형에 따라 다릅니다.

- 물리적 인터페이스 - 물리적 인터페이스는 버닝된 MAC 주소를 사용합니다.
- EtherChannel - EtherChannel의 경우 채널 그룹에 속한 모든 인터페이스가 동일한 MAC 주소를 공유합니다. 이 기능은 EtherChannel을 네트워크 애플리케이션 및 사용자에게 투명하게 만듭니다. 이들은 논리적 연결만 볼 수 있으며, 개별 링크에 대해서는 모르기 때문입니다. 포트 채널 인터페이스는 풀의 고유 MAC 주소를 사용하며 인터페이스 멤버십은 MAC 주소에 영향을 주지 않습니다.

일반 지침 및 제한 사항

고가용성

- 애플리케이션 구성 내에서 고가용성을 구성합니다.
- 모든 데이터 인터페이스를 페일오버 및 상태 링크로 사용할 수 있습니다.
- 고가용성 페일오버 설정에는 2개의 유닛이 필요합니다.
  - 같은 모델이어야 합니다.
  - 고가용성 논리 디바이스에는 동일한 인터페이스가 할당되어야 합니다.
  - 인터페이스 개수와 유형이 같아야 합니다. 고가용성을 활성화하기 전에 모든 인터페이스는 FXOS와 동일하게 사전 설정되어야 합니다.
- 자세한 내용은 고가용성을 위한 시스템 요구 사항, 218 페이지를 참고하십시오.

인터페이스 구성

기본적으로 물리적 인터페이스는 비활성화되어 있습니다. 인터페이스 활성화, EtherChannels 추가, 인터페이스 속성 수정 구성 작업을 수행할 수 있습니다.

인터페이스 활성화 또는 비활성화

각 인터페이스의 **Admin State(**관리 상태**)**를 활성화 또는 비활성화로 변경할 수 있습니다. 기본적으로 물리적 인터페이스는 비활성화되어 있습니다.

프로시저

단계 **1** **Interfaces(**인터페이스**)**를 선택하여 Interfaces(인터페이스) 페이지를 엽니다.

Interfaces(인터페이스) 페이지는 페이지 상단에 현재 설치된 인터페이스를 시각적으로 표시하며 아래 표에서 설치된 인터페이스 목록을 제공합니다.

단계 **2** 인터페이스를 활성화하려면 비활성화된 슬라이더 비활성화됨()를 클릭하여 활성화된 슬라이더 활성화됨()로 변경합니다.

Yes(예**)**를 클릭하여 변경을 확인합니다. 해당 인터페이스의 시각적 표시가 회색에서 녹색으로 변경됩니다.

단계 **3** 인터페이스를 비활성화하려면 활성화된 슬라이더 활성화됨()를 클릭하여 비활성화된 슬라이더 비활성화됨()로 변경합니다.

Yes(예**)**를 클릭하여 변경을 확인합니다. 해당 인터페이스의 시각적 표시가 녹색에서 회색으로 변경됩니다.

실제 인터페이스 구성

인터페이스를 물리적으로 활성화 및 비활성화할 뿐만 아니라 인터페이스 속도 및 듀플렉스를 설정할 수 있습니다. 인터페이스를 사용하려면 FXOS에서 인터페이스를 물리적으로 활성화하고 애플리케이션에서 논리적으로 활성화해야 합니다.

시작하기 전에

- 이미 EtherChannel의 멤버인 인터페이스는 개별적으로 수정할 수 없습니다. EtherChannel에 인터페이스를 추가하기 전에 설정을 구성하십시오.

EtherChannel(포트 채널) 추가

EtherChannel(포트 채널로 알려짐)은 동일한 미디어 유형 및 용량의 멤버 인터페이스를 최대 16개까지 포함할 수 있으며 동일한 속도 및 듀플렉스로 설정해야 합니다. 미디어 유형은 RJ-45 또는 SFP일 수 있으며 서로 다른 유형(구리 및 광섬유)의 SFP를 혼합할 수 있습니다. 더 큰 용량의 인터페이스에서는 속도를 낮게 설정하여 인터페이스 용량(예: 1GB 및 10GB 인터페이스)을 혼합하여 사용할 수 없습니다. LACP(Link Aggregation Control Protocol)에서는 두 네트워크 디바이스 간의 LACPDU(Link Aggregation Control Protocol Data Units)를 교환하여 인터페이스를 취합합니다.

EtherChannel의 각 물리적 데이터 인터페이스를 다음과 같이 구성할 수 있습니다.

- Active(활성화) — LACP 업데이트를 보내고 받습니다. 액티브 EtherChannel은 액티브 또는 패시브 EtherChannel과의 연결을 설정할 수 있습니다. LACP 트래픽 양을 최소화할 필요가 없는 한 액티브 모드를 사용해야 합니다.
- On(켜짐) — EtherChannel은 항상 켜져 있으며 LACP는 사용되지 않습니다. "on"으로 된 EtherChannel은 오로지 또 다른 "on" 상태의 EtherChannel과 연결을 설정할 수 있습니다.

참고 On에서 활성화, 또는 활성화에서 On으로 모드를 변경하는 경우 EtherChannel가 작동하는 데 최대 3분이 걸립니다.

Firepower 4100/9300 섀시는 각 멤버 인터페이스가 LACP 업데이트를 송수신할 수 있도록 액티브 LACP 모드에서만 EtherChannel을 지원합니다. 액티브 EtherChannel은 액티브 또는 패시브 EtherChannel과의 연결을 설정할 수 있습니다. LACP 트래픽 양을 최소화할 필요가 없는 한 액티브 모드를 사용해야 합니다.

LACP에서는 사용자의 작업 없이 EtherChannel에 링크를 자동으로 추가 및 삭제하는 작업을 조율합니다. 또한 구성 오류를 처리하고 멤버 인터페이스의 양끝이 모두 올바른 채널 그룹에 연결되어 있는지 확인합니다. "On" 모드에서는 인터페이스가 중단될 경우 채널 그룹의 스탠바이 인터페이스를 사용할 수 없으며, 연결 및 구성이 확인되지 않습니다.

Firepower 4100/9300 섀시에서 EtherChannel을 생성하면 물리적 링크가 가동 중이더라도 EtherChannel은 논리적 디바이스에 할당될 때까지 Active LACP(액티브 LACP) 모드인 경우 **Suspended(**일시 중단**)** 상태로, On LACP(LACP 켜짐) 모드인 경우 **Down(**중단**)** 상태로 유지됩니다. 다음의 상황에서는 EtherChannel의 **Suspended(**일시 중단**)** 상태가 해제됩니다.

- EtherChannel이 독립형 논리적 디바이스에 대한 데이터 인터페이스 또는 관리 인터페이스로 추가됩니다.
- EtherChannel이 클러스터의 일부인 논리적 디바이스에 대한 관리 인터페이스 또는 클러스터 제어 링크로 추가됩니다.
- EtherChannel이 클러스터의 일부이며 유닛 하나 이상이 클러스터에 조인된 논리적 디바이스에 대한 데이터 인터페이스로 추가됩니다.

EtherChannel은 논리적 디바이스에 할당될 때까지 나타나지 않습니다. EtherChannel을 논리적 디바이스에서 제거하거나 논리적 디바이스가 삭제된 경우, EtherChannel은 **Suspended(**일시 중단**)** 또는 **Down(**중단**)** 상태로 전환됩니다.

논리적 디바이스 구성

Firepower 4100/9300 섀시에서 독립형 논리적 디바이스 또는 고가용성 쌍을 추가합니다.

Device Manager에 대한 독립형 Threat Defense 추가

네이티브 인스턴스로 device manager을 사용할 수 있습니다. 컨테이너 인스턴스는 지원되지 않습니다. 독립형 논리적 디바이스는 단독으로 작동하거나 고가용성 쌍으로 작동합니다.

시작하기 전에

- Cisco.com에서 논리적 디바이스에 사용할 애플리케이션 이미지를 다운로드한 다음 해당 이미지를 Firepower 4100/9300 섀시.
- 논리적 디바이스에 사용할 관리 인터페이스를 구성합니다. 관리 인터페이스는 필수 항목입니다. 이 관리 인터페이스는 섀시 관리용으로만 사용되는 섀시 관리 포트와는 다릅니다.
- 최소 하나 이상의 데이터 유형 인터페이스도 구성해야 합니다.
- 다음 정보를 수집합니다.
  - 이 디바이스의 인터페이스 ID
  - 관리 인터페이스 IP 주소 및 네트워크 마스크
  - Gateway IP address(게이트웨이 IP 주소)
  - DNS 서버 IP 주소
  - Threat Defense 호스트 이름 및 도메인 이름

프로시저

보안 정책 구성을 시작하려면 device manager 구성 가이드를 참조하십시오.

고가용성 쌍 추가

Threat Defense 고가용성(장애 조치라고도 함)은 FXOS가 아닌 애플리케이션 내에 구성됩니다. 그러나 고가용성을 사용할 수 있도록 섀시를 준비하려는 경우 다음 단계를 참조하십시오.

시작하기 전에

고가용성을 위한 시스템 요구 사항, 218 페이지의 내용을 참조하십시오.

프로시저

단계 **1** 각 논리적 디바이스에 동일한 인터페이스를 할당합니다.

단계 **2** 페일오버 및 상태 링크용으로 데이터 인터페이스 1~2개를 할당합니다.

이러한 인터페이스는 두 섀시 간의 고가용성 트래픽을 교환합니다. 페일오버 및 상태 링크를 함께 사용하려면 10GB 데이터 인터페이스를 사용하는 것이 좋습니다. 사용 가능한 인터페이스가 있다면 페일오버 및 상태 링크를 각각 별도로 사용할 수 있습니다. 상태 링크에는 최대 대역폭이 필요합니다. 관리 유형 인터페이스는 페일오버 또는 상태 링크용으로 사용할 수 없습니다. 페일오버 인터페이스와 같은 네트워크 세그먼트에 다른 디바이스가 없는 상태로 섀시 간에 스위치를 사용하는 것이 좋습니다.

단계 **3** 논리적 디바이스에서 고가용성을 활성화합니다. 고가용성(페일오버), 209 페이지 섹션을 참조하십시오.

단계 **4** 고가용성을 활성화한 후에 인터페이스를 변경해야 하는 경우에는 먼저 스탠바이 유닛에서 변경을 수행한 다음 액티브 유닛에서 변경을 수행합니다.

Threat Defense 논리적 디바이스에서 인터페이스 변경

threat defense 논리적 디바이스에서 인터페이스를 할당 또는 할당 해제할 수 있습니다. 그런 다음 device manager에서 인터페이스 구성을 동기화할 수 있습니다.

새 인터페이스를 추가하거나 사용하지 않는 인터페이스를 삭제하는 경우 threat defense 구성에 미치는 영향은 아주 적습니다. 그러나 보안 정책에 사용되는 인터페이스를 삭제하면 구성에 영향이 미칩니다. 액세스 규칙, NAT, SSL, ID 규칙, VPN, DHCP 서버 등 threat defense 구성의 여러 위치에서 인터페이스를 직접 참조할 수 있습니다. 보안 영역을 참조하는 정책은 영향을 받지 않습니다. 논리적 디바이스에 영향을 주거나 device manager에서 동기화할 필요 없이 할당된 EtherChannel의 멤버십을 수정할 수도 있습니다.

기존 인터페이스를 삭제하기 전에 한 인터페이스에서 다른 인터페이스로 구성을 마이그레이션할 수 있습니다.

시작하기 전에

- 인터페이스를 구성하고 실제 인터페이스 구성, 201 페이지 및 EtherChannel(포트 채널) 추가, 202 페이지에 따라 EtherChannel을 추가합니다.
- 모든 인터페이스가 기본적으로 클러스터에 할당된 경우와 같이 이미 할당된 인터페이스를 EtherChannel에 추가하려는 경우에는 먼저 논리적 디바이스에서 인터페이스 할당을 해제한 다음 EtherChannel에 인터페이스를 추가해야 합니다. 새 EtherChannel의 경우 이렇게 한 후에 디바이스에 EtherChannel을 할당할 수 있습니다.

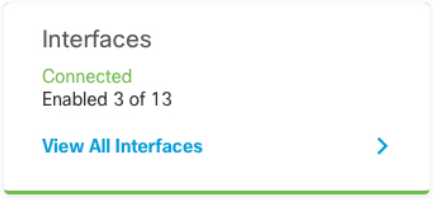
- 고가용성의 경우에는 device manager에서 구성을 동기화하기 전에 모든 유닛에서 인터페이스를 추가하거나 제거해야 합니다. 인터페이스는 먼저 스탠바이 유닛에서 변경한 후에 액티브 유닛에서 변경하는 것이 좋습니다. 새 인터페이스는 관리를 위해 다운된 상태로 추가되므로 인터페이스 모니터링에는 영향을 주지 않습니다.

프로시저

단계 **1** device manager에서 인터페이스를 동기화하고 마이그레이션합니다.

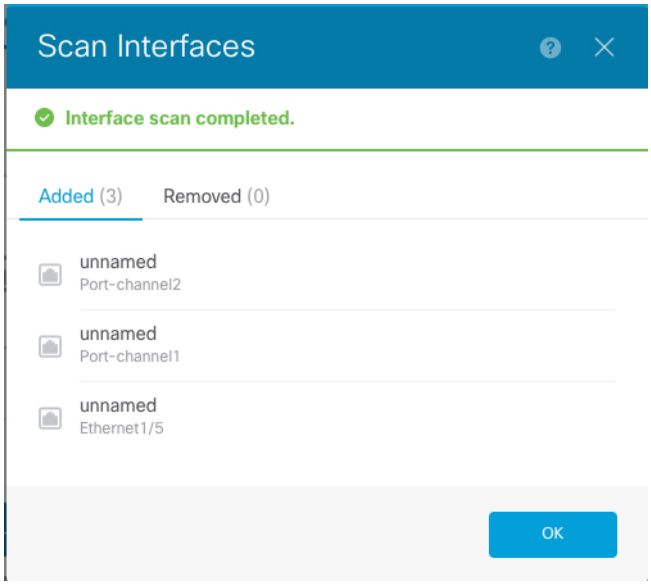
a) device manager에 로그인합니다.

b) **Device(**디바이스**)**를 클릭한 다음, **Interfaces(**인터페이스**)** 요약에서 **View All Interfaces(**모든 인터페이스 보기**)** 링크를 클릭합니다.



c) **Scan Interfaces icon(**인터페이스 스캔 아이콘**)**을 클릭합니다.

d) 인터페이스가 스캔될 때까지 기다린 다음, **OK(**확인**)**를 클릭합니다.



e) 이름, IP 주소 등을 사용하여 새 인터페이스를 구성합니다.

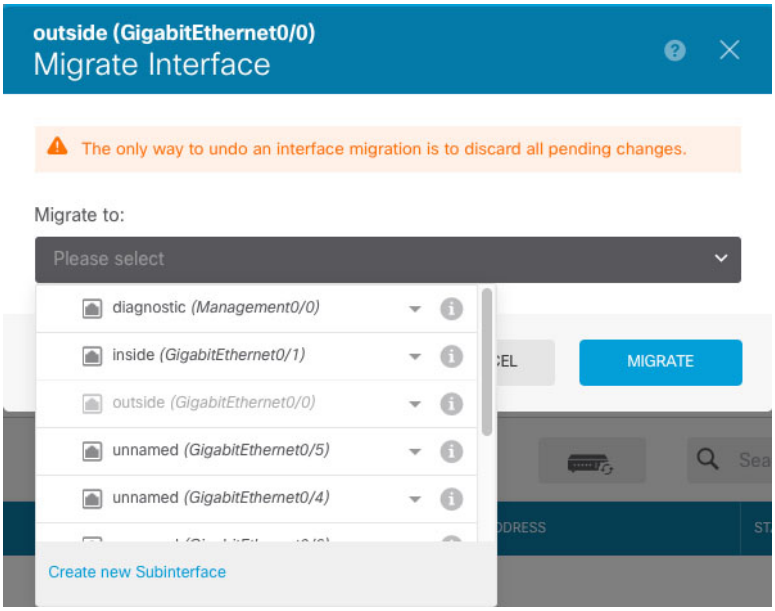
제거할 인터페이스의 기존 IP 주소 및 이름을 사용하려는 경우에는 새 인터페이스에서 해당 설정을 사용할 수 있도록 기존 인터페이스를 더미 이름 및 IP 주소로 다시 구성해야 합니다.

f) 기존 인터페이스를 새 인터페이스로 교체하려면 기존 인터페이스의 Replace(교체) 아이콘을 클릭합니다.

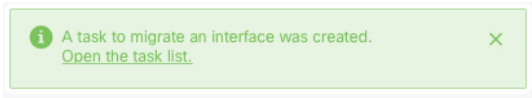
바꾸기 아이콘

이 프로세스에서는 인터페이스를 참조하는 모든 구성 설정에서 기존 인터페이스가 새 인터페이스로 교체됩니다.

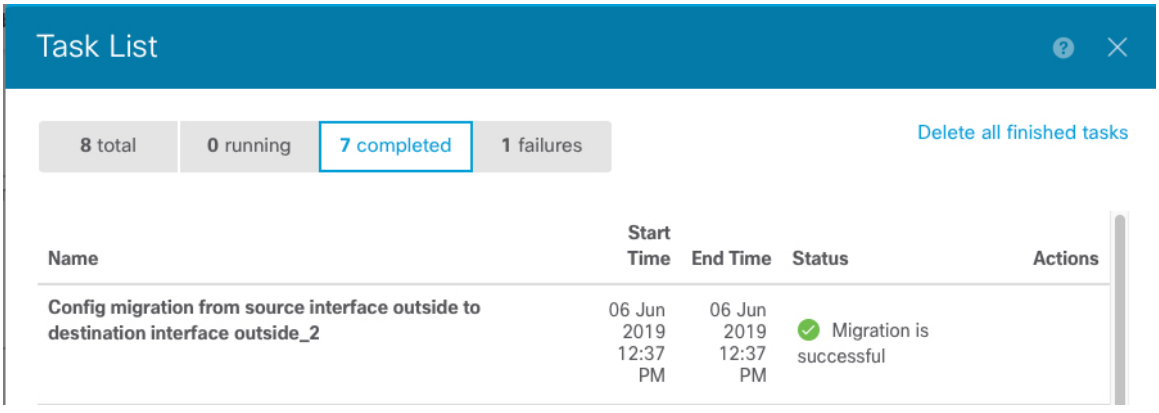
g) **Replacement Interface(**교체 인터페이스**)** 드롭다운 목록에서 새 인터페이스를 선택합니다.



h) **Interfaces(**인터페이스**)** 페이지에 메시지가 나타납니다. 메시지에서 링크를 클릭합니다.

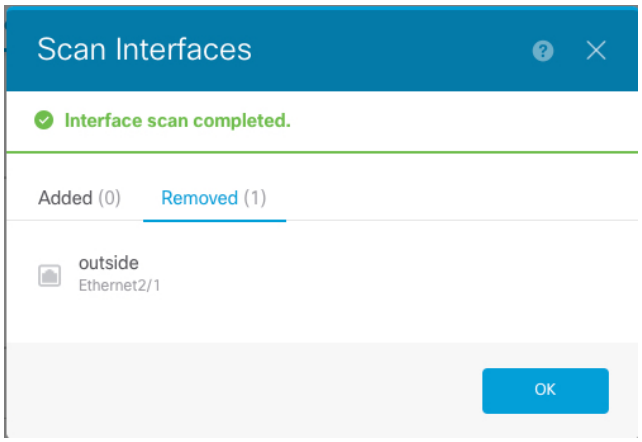


i) **Task List(**작업 목록**)**를 확인하여 마이그레이션에 성공했는지 확인합니다.



단계 **2** device manager에서 인터페이스를 다시 동기화합니다.

그림 *6: Device Manager* 스캔 인터페이스



애플리케이션 콘솔에 연결

다음 절차를 수행하여 애플리케이션의 콘솔에 연결합니다.

프로시저

단계 **1** 콘솔 연결 또는 텔넷 연결을 사용하여 모듈 CLI에 연결합니다.

connect module *slot_number* {**console** | **telnet**}

여러 보안 모듈을 지원하지 않는 디바이스의 보안 엔진에 연결하려면 항상 **1**을 *slot_number*로 사용합니다.

텔넷 연결 사용 시에는 동시에 여러 세션을 모듈에 연결할 수 있으며 연결 속도가 더 빠르다는 이점이 있습니다.

예제:

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

단계 **2** 애플리케이션 콘솔에 연결합니다.

connect ftd *name*

인스턴스 이름을 확인하려면 이름 없이 명령을 입력합니다.

예제:

```
Firepower-module1> connect ftd ftd1
Connecting to ftd(ftd-native) console... enter exit to return to bootCLI
[...]
>
```

단계 **3** 애플리케이션 콘솔을 FXOS 모듈 CLI로 종료합니다.

- Threat Defense - **exit**를 입력합니다.

단계 **4** FXOS CLI의 Supervisor(관리자) 수준으로 돌아갑니다.

콘솔을 종료합니다**.**

a) **~**를 입력합니다.

텔넷 애플리케이션을 종료합니다.

b) 텔넷 애플리케이션을 종료하려면 다음을 입력합니다.

telnet>**quit**

텔넷 세션을 종료합니다**.**

a) **Ctrl-], .**를 입력합니다.

Firepower 4100/9300 논리적 디바이스의 기록

기능	버전	세부 사항
Firepower 4100/9300의 device manager 지원	6.5.0	이제 Firepower 4100/9300에서 threat defense 논리적 디바이스와 함께 device manager를 사용할 수 있습니다. device manager에서는 다중 인스턴스 기능을 지원하지 않습니다. 네이티브 인스턴스만 지원됩니다. 참고 FXOS 2.7.1이 필요합니다.

10 장

고가용성(페일오버)

다음 주제에서는 threat defense 시스템의 고가용성을 달성하기 위해 액티브/스탠바이 페일오버를 컨피그레이션하고 관리하는 방법을 설명합니다.

고가용성(페일오버) 정보

고가용성 또는 페일오버 설정에서는 두 디바이스가 조인하므로 기본 디바이스에 장애가 발생하면 보조 디바이스가 대신 작동할 수 있습니다. 그러면 디바이스 장애 시 네트워크를 계속 운영하는 데 도움이 됩니다.

고가용성을 컨피그레이션하려면 2개의 동일한 threat defense 디바이스가 전용 페일오버 링크와 선택 사항인 상태 링크를 통해 서로 연결되어 있어야 합니다. 두 유닛은 페일오버 링크를 통해 지속적으로 통신하면서 각 유닛의 작동 상태를 확인하고 구축된 컨피그레이션 변경 사항을 동기화합니다. 시스템은 상태 링크를 사용해 연결 상태 정보를 스탠바이 디바이스에 전달하므로, 페일오버가 발생할 경우 사용자 연결이 유지됩니다.

두 유닛은 액티브/패시브 쌍을 이루는데, 여기서 하나는 액티브 유닛이며 트래픽을 전달합니다. 스탠바이 유닛은 능동적으로 트래픽을 전달하지 않지만, 액티브 유닛에서 컨피그레이션 및 기타 상태 정보를 동기화합니다.

액티브 유닛의 상태(하드웨어, 인터페이스, 소프트웨어 및 환경 상태)를 모니터링하여 특정 페일오버 조건이 충족되는지 확인합니다. 페일오버 조건이 충족되면 액티브 유닛은 스탠바이 유닛으로 페일오버를 시작하며, 이때 스탠바이 유닛이 액티브 유닛이 됩니다.

액티브/스탠바이 페일오버 정보

액티브/스탠바이 페일오버에서는 스탠바이 위협 방지 디바이스를 사용해 장애가 발생한 유닛의 기능을 인수할 수 있습니다. 액티브 유닛에 장애가 발생하는 경우 스탠바이 유닛이 액티브 유닛이 됩니다.

기본/보조 역할 및 액티브/스탠바이 상태

페일오버 쌍의 두 유닛의 주된 차이점은 어느 유닛이 액티브 유닛이고 어느 유닛이 스탠바이 유닛인지와 관련 있습니다. 즉, 어떤 IP 주소를 사용하고 어떤 유닛이 트래픽을 능동적으로 전달하는지에 달려 있습니다.

그러나 유닛 간의 몇몇 차이점은 어느 유닛이 기본(컨피그레이션에 지정된 사항에 따라) 유닛이고 어느 유닛이 보조 유닛인지에 따라서도 결정됩니다.

- 두 유닛이 동시에 시작되고 둘 다 정상적인 상태로 작동될 경우 기본 유닛은 항상 액티브 유닛이 됩니다.
- 기본 유닛의 MAC 주소는 액티브 IP 주소와 항상 연계됩니다. 보조 유닛이 액티브 유닛이 되고 페일오버 링크를 통해 기본 유닛의 MAC 주소를 획득할 수 없는 경우에는 이러한 규칙에 예외가 발생합니다. 이 경우 보조 유닛의 MAC 주소가 사용됩니다.

시작 시 액티브 유닛 결정

액티브 유닛은 다음에 따라 결정됩니다.

- 유닛이 부팅되고 이미 액티브로 실행 중인 피어가 감지된 경우, 해당 유닛은 스탠바이 유닛이 됩니다.
- 유닛이 부팅되고 피어가 감지되지 않은 경우 해당 유닛은 액티브 유닛이 됩니다.
- 두 유닛이 동시에 부팅될 경우 기본 유닛이 액티브 유닛이 되고 보조 유닛은 스탠바이 유닛이 됩니다.

페일오버 이벤트

액티브/스탠바이 페일오버 시 페일오버는 유닛을 기준으로 실행됩니다.

다음 표에서는 각 페일오버 이벤트에 대한 페일오버 작업을 보여줍니다. 이 표에는 각 페일오버 이벤트에 적용되는 페일오버 정책(페일오버 실행 또는 페일오버 없음), 액티브 유닛에서 시행한 조치, 스탠바이 유닛에서 시행한 조치, 페일오버 조건 및 각 조치에 대한 특별 참고 사항이 나와 있습니다.

표 ***5:*** 페일오버 이벤트

오류 이벤트	정책	액티브 유닛 조치	스탠바이 유닛 조치	참고
액티브 유닛 오류(전력 또는 하드웨어)	페일오버	해당 없음	액티브 상태가 됨 액티브가 실패한 것으로 표시됨	모니터링된 인터페이스 또는 페일오버 링크에 대한 hello 메시지가 수신되지 않음

오류 이벤트	정책	액티브 유닛 조치	스탠바이 유닛 조치	참고
이전 액티브 유닛 복구	페일오버 없음	스탠바이 상태가 됨	작업 없음	없음
스탠바이 유닛 오류(전력 또는 하드웨어)	페일오버 없음	스탠바이가 실패한 것으로 표시됨	해당 없음	스탠바이 유닛이 실패한 것으로 표시될 경우, 액티브 유닛에서는 페일오버를 시도하지 않으며 인터페이스 오류 임계값을 넘은 경우에도 마찬가지입니다.
작동 중 페일오버 링크에 오류 발생	페일오버 없음	페일오버 링크가 실패한 것으로 표시됨	페일오버 링크가 실패한 것으로 표시됨	페일오버가 중단된 동안에는 유닛에서 스탠바이 유닛으로 페일오버를 시작하지 못하므로 최대한 빨리 페일오버 링크를 복구해야 합니다.
시작 시 페일오버 링크에 오류 발생	페일오버 없음	액티브 상태가 됨 페일오버 링크가 실패한 것으로 표시됨	액티브 상태가 됨 페일오버 링크가 실패한 것으로 표시됨	시작 시 페일오버 링크가 중단되면 두 유닛 모두 액티브 상태가 됩니다.
상태 링크 오류 발생	페일오버 없음	작업 없음	작업 없음	페일오버가 실행될 경우 상태 정보가 최신이 아닌 것으로 변경되며 세션이 종료됩니다.
임계값을 넘은 액티브 유닛에서 인터페이스 오류 발생	페일오버	액티브가 실패한 것으로 표시됨	액티브 상태가 됨	없음
임계값을 넘은 스탠바이 유닛에서 인터페이스 오류 발생	페일오버 없음	작업 없음	스탠바이가 실패한 것으로 표시됨	스탠바이 유닛이 실패한 것으로 표시될 경우, 액티브 유닛에서는 페일오버를 시도하지 않으며 인터페이스 오류 임계값을 넘은 경우에도 마찬가지입니다.

페일오버 및 스테이트풀 페일오버 링크

페일오버 링크는 두 유닛 사이의 전용 연결입니다. 스테이트풀 페일오버 링크 역시 전용 연결이지만, 페일오버 링크 하나를 페일오버/상태가 결합된 링크로 사용할 수도 있고 별도의 전용 상태 링크를 생

성할 수도 있습니다. 페일오버 링크만 사용하는 경우에는 스테이트풀 정보가 해당 링크를 통해 전송되며 스테이트풀 페일오버 기능도 유지됩니다.

기본적으로 페일오버 및 스테이트풀 페일오버 링크의 통신은 암호화되지 않은 일반 텍스트로 이루어집니다. IPsec 암호화 키를 구성하면 통신을 암호화하여 보안을 강화할 수 있습니다.

다음 주제에서는 이러한 인터페이스에 대해 더 자세히 설명하며, 최고의 결과를 얻기 위해 디바이스를 유선 연결하는 방법에 대한 권장 사항을 제공합니다.

페일오버 링크

페일오버 쌍의 두 유닛은 페일오버 링크를 통해 지속적으로 통신하여 각 유닛의 작동 상태를 확인하고 컨피그레이션 변경 사항을 동기화합니다.

다음 정보는 페일오버 링크를 통해 전달됩니다.

- 유닛 상태(액티브 또는 스탠바이).
- Hello 메시지(keep-alive).
- 네트워크 링크 상태.
- MAC 주소 교환.
- 컨피그레이션 복제 및 동기화.
- 시스템 데이터베이스 업데이트. 여기에는 VDB 및 규칙은 포함되지만 지리위치 및 보안 인텔리전스 데이터베이스는 포함되지 않습니다. 각 시스템은 지리위치 및 보안 인텔리전스 업데이트를 개별적으로 다운로드합니다. 업데이트 일정을 생성하는 경우에는 동기화 상태를 유지해야 합니다. 하지만 액티브 디바이스에서 수동 지리위치 또는 보안 인텔리전스 업데이트를 수행하는 경우에는 스탠바이 디바이스에서도 업데이트를 수행해야 합니다.

참고 이벤트, 보고 및 감사 로그 데이터는 동기화되지 않습니다. 이벤트 뷰어 및 대시보드에는 지정된 유닛과 관련된 데이터만 표시됩니다. 또한 구축 기록, 작업 기록 및 기타 감사 로그 이벤트는 동기화되지 않습니다.

스테이트풀 페일오버 링크

시스템은 상태 링크를 사용해 연결 상태 정보를 스탠바이 디바이스에 전달합니다. 페일오버 수행 시에 스탠바이 유닛은 이 정보를 사용하여 기존 연결을 유지할 수 있습니다.

인터페이스를 유지하는 가장 좋은 방법은 페일오버 및 스테이트풀 페일오버 링크 모두에 단일 링크를 사용하는 것입니다. 그러나 컨피그레이션 규모가 크고 네트워크의 트래픽이 많은 경우에는 상태 링크와 페일오버 링크에 대해 전용 인터페이스를 사용하는 것을 고려해야 합니다.

장애 조치 및 상태 링크의 인터페이스

사용되지 않지만 활성화되어 있는 데이터 인터페이스(물리적 또는 EtherChannel)를 장애 조치 링크로 사용할 수 있습니다. 그러나 현재 이름이 구성된 인터페이스는 지정할 수 없습니다. 장애 조치 링크

인터페이스는 일반적인 네트워킹 인터페이스로 구성되지 않으며, 장애 조치 통신용으로만 존재합니다. 이 인터페이스는 장애 조치 링크용으로만 사용할 수 있습니다(또한 상태 링크용으로도 사용 가능). 장애 조치에는 관리 인터페이스, 하위 인터페이스, VLAN 인터페이스 또는 스위치 포트를 사용할 수 없습니다.

threat defense 디바이스에서는 사용자 데이터와 장애 조치 링크 간에 인터페이스 공유를 지원하지 않습니다.

장애 조치 및 상태 링크 크기 조정에 대한 다음 지침을 참조하십시오.

- Firepower 4100/9300 - 페일오버 및 상태 링크를 통합하려면 10GB 데이터 인터페이스를 사용하는 것이 좋습니다.
- 기타 모델 — 1GB 인터페이스는 통합된 장애 조치 및 상태 링크에 충분한 크기입니다.

EtherChannel 인터페이스를 장애 조치 또는 상태 링크로 사용하는 경우, 고가용성을 설정하기 전에 동일한 ID 및 멤버 인터페이스를 사용하는 동일한 EtherChannel이 두 디바이스에 있는지 확인해야 합니다. EtherChannel이 일치하지 않는 경우에는 HA를 비활성화하고 이전의 보조 유닛에서 구성을 수정해야 합니다. 패킷의 오류를 방지하기 위해 EtherChannel에서는 하나의 인터페이스만 사용됩니다. 해당 인터페이스에 오류가 발생할 경우 EtherChannel의 다음 인터페이스가 사용됩니다. 장애 조치 링크로 사용 중인 경우 EtherChannel 컨피그레이션을 변경할 수 없습니다.

페일오버 및 스테이트풀 페일오버 인터페이스 연결

사용되지 않는 모든 데이터 물리적 인터페이스를 페일오버 링크 및 전용 상태 링크(선택 사항)로 사용할 수 있습니다. 그러나 현재 특정 이름으로 구성되어 있거나 하위 인터페이스가 있는 인터페이스는 선택할 수 없습니다. 페일오버 및 스테이트풀 페일오버 링크 인터페이스는 일반 네트워킹 인터페이스로 구성되지 않습니다. 이러한 인터페이스는 페일오버 통신에만 사용되며 통과 트래픽 또는 관리 액세스에는 사용할 수 없습니다.

컨피그레이션이 디바이스 간에 동기화되므로 링크의 양쪽 끝에 같은 포트 번호를 선택해야 합니다. 예를 들어 페일오버 링크를 위해 두 디바이스에서 모두 GigabitEthernet1/3을 선택합니다.

다음의 두 가지 방식 중 하나로 페일오버 링크와 전용 상태 링크(사용하는 경우)를 연결합니다.

- 같은 네트워크 세그먼트(브로드캐스트 도메인 또는 VLAN)에 다른 디바이스가 없는 상태에서 스위치를 threat defense 디바이스의 페일오버 인터페이스로 사용합니다. 전용 상태 링크의 요구 사항도 같지만, 이 링크는 페일오버 링크와 다른 네트워크 세그먼트에 있어야 합니다.

참고 스위치를 사용하는 장점은 유닛 인터페이스 중 하나가 중단되는 경우 장애가 발생한 인터페이스를 쉽게 트러블슈팅할 수 있다는 것입니다. 다이렉트 케이블 연결을 사용하는 경우 인터페이스 하나에서 장애가 발생하면 두 피어에서 모두 링크가 중단되므로 결함이 있는 디바이스를 확인하기가 어렵습니다.

- 외부 스위치를 사용할 필요 없이 이더넷 케이블을 사용하여 유닛을 직접 연결합니다. threat defense에서는 구리 이더넷 포트의 Auto-MDI/MDIX를 지원하므로 crossover 케이블 또는 straight-through

케이블을 사용할 수 있습니다. 다이렉트 케이블을 사용할 경우 인터페이스에서는 케이블을 자동으로 감지하고 송/수신 쌍 중 하나를 MDIX로 교체합니다.

장거리 페일오버를 사용할 경우 최적의 성능을 보장하려면 페일오버 링크의 레이턴시는 10밀리초 미만이어야 하고 250밀리초를 초과해서는 안 됩니다. 레이턴시가 10밀리초를 초과하는 경우 페일오버 메시지의 재전송으로 인해 성능이 다소 저하됩니다.

페일오버 및 데이터 링크 중단 방지

페일오버 링크 및 데이터 인터페이스가 다른 경로를 통해 이동하도록 설정하여 모든 인터페이스에 동시 다발적으로 오류가 발생하는 가능성을 줄이는 것이 좋습니다. 페일오버 링크가 중단될 경우 threat defense 디바이스는 데이터 인터페이스를 사용하여 페일오버가 필요한지 여부를 확인할 수 있습니다. 그런 다음 페일오버 링크 상태가 복원될 때까지는 페일오버 작업이 보류됩니다.

복원력이 뛰어난 페일오버 네트워크를 설계하려면 다음 연결 시나리오를 참조하십시오.

시나리오 **1** — 권장하지 않음

단일 스위치 또는 스위치 집합을 사용하여 두 threat defense 디바이스 간의 페일오버 및 데이터 인터페이스를 모두 연결한 상태에서 스위치 또는 스위치 간 링크가 중단될 경우 두 threat defense 디바이스 모두 액티브 상태가 됩니다. 따라서 아래의 그림에 있는 다음 2가지 연결 방법은 권장하지 않습니다.

그림 ***7:*** 단일 스위치로 연결 - 권장하지 않음

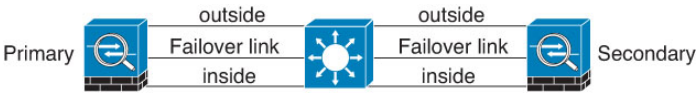
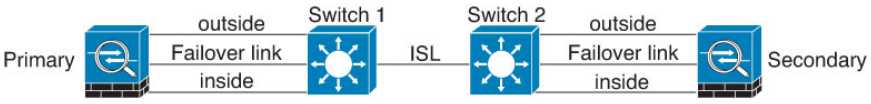


그림 ***8:*** 이중 스위치로 연결 - 권장하지 않음



시나리오 **2** - 권장함

페일오버 링크에서는 데이터 인터페이스와 같은 스위치를 사용하지 않는 것이 좋습니다. 대신 다음 그림에 나와 있는 것처럼 다른 스위치를 사용하거나 다이렉트 케이블을 사용하여 페일오버 링크에 연결합니다.

그림 ***9:*** 다른 스위치로 연결

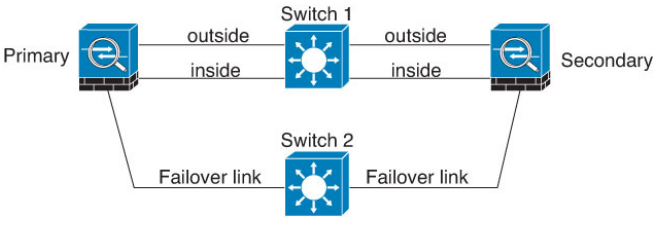
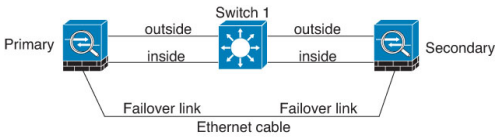


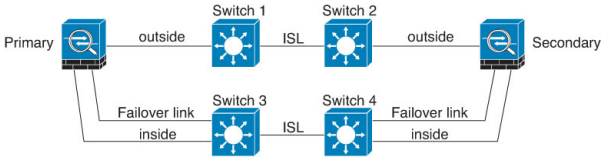
그림 ***10:*** 케이블로 연결



시나리오 **3** — 권장

threat defense 데이터 인터페이스가 여러 개의 스위치 집합에 연결되어 있는 경우, 페일오버 링크는 이러한 스위치 중 하나에 연결될 수 있으며 다음 그림에 나온 것처럼 주로 네트워크의 보안(내부) 측에 있는 스위치일 가능성이 높습니다.

그림 ***11:*** 보안 스위치로 연결



스테이트풀 페일오버가 사용자 연결에 주는 영향

액티브 유닛은 스탠바이 유닛과 연결 상태 정보를 공유합니다. 즉, 스탠바이 유닛은 사용자에게 영향을 주지 않고 특정 유형의 연결을 유지할 수 있습니다.

그러나 스테이트풀 페일오버를 지원하지 않는 연결 유형도 있습니다. 이러한 연결의 경우, 페일오버가 있으면 사용자가 연결을 다시 설정해야 합니다. 이러한 과정은 대개 연결에 사용되는 프로토콜의 동작을 기반으로 하여 자동으로 진행되는 경우가 많습니다.

다음 주제에서는 스테이트풀 페일오버에 지원되는 기능과 지원되지 않는 기능을 설명합니다.

지원 기능

스테이트풀 페일오버에서는 다음 상태 정보가 스탠바이 위협 방지 디바이스로 전달됩니다.

- NAT 변환 테이블.
- TCP 및 UDP 연결과 상태(HTTP 연결 상태 포함). 다른 유형의 IP 프로토콜과 ICMP는 새 패킷이 도착하면 새 액티브 유닛에서 설정되므로 액티브 유닛에서 구문 분석되지 않습니다.
- Snort 연결 상태, 검사 결과 및 핀홀 정보(엄격한 TCP 적용 포함).
- ARP 테이블
- 레이어 2 브리지 테이블(브리지 그룹용)
- ISAKMP 및 IPsec SA 테이블
- GTP PDP 연결 데이터베이스
- SIP 시그널링 세션 및 핀홀.

- 정적 및 동적 라우팅 테이블 - 스테이트풀 페일오버는 OSPF 및 EIGRP 같은 동적 라우팅 프로토콜에 참여하므로, 액티브 유닛에서 동적 라우팅 프로토콜을 통해 확인한 경로는 스탠바이 유닛의 RIB(Routing Information Base) 테이블에 유지됩니다. 페일오버 이벤트 발생 시 액티브 보조 유닛에서는 초기 규칙에 따라 기본 유닛을 미러링하므로 트래픽 중단을 최소화면서도 패킷이 정상적으로 이동됩니다. 페일오버가 끝난 직후에는 새 액티브 유닛에서 재통합 타이머가 시작됩니다. 그러면 RIB 테이블의 시간대 숫자가 늘어납니다. 재통합을 수행하는 동안 OSPF 및 EIGRP 경로는 새 시간대 숫자로 업데이트됩니다. 타이머가 만료되면 오래된 경로 항목(시간대 숫자에 의해 결정됨)이 테이블에서 제거됩니다. 그런 다음 RIB에 새 액티브 유닛에 대한 최신 라우팅 프로토콜 전달 정보가 포함됩니다.

참고 경로는 액티브 유닛의 링크 작동 또는 링크 중단 이벤트가 있을 경우에만 동기화됩니다. 스탠바이 유닛에서 링크가 작동하거나 중단될 경우, 액티브 유닛에서 전송된 동적 경로가 손실될 수 있습니다. 이는 일반적이고 정상적인 동작입니다.

- DHCP 서버 - DHCP 주소 임대는 복제되지 않습니다. 그러나 인터페이스에 구성된 DHCP 서버는 ping을 전송하여 특정 주소가 사용 중이지 않음을 확인한 후에 DHCP 클라이언트에 해당 주소를 부여하므로 서비스에는 영향이 없습니다. 상태 정보는 DHCP 릴레이 또는 DDNS와 관련이 없습니다.
- 액세스 제어 정책 결정 - 트래픽 일치(URL, URL 카테고리, 지리위치 등), 침입 탐지, 악성코드 및 파일 유형과 관련된 결정은 페일오버 중에 그대로 유지됩니다. 그러나 페일오버 시점에서 평가 중인 연결의 경우 다음 경고가 적용됩니다.
  - AVC - 앱-ID 판정은 복제되지만 탐지 상태는 복제되지 않습니다. 페일오버가 수행되기 전에 앱-ID 판정이 완료 및 동기화되면 적절한 동기화가 수행됩니다.
  - 침입 탐지 상태 - 페일오버 시 중간 플로우 픽업이 발생하면 새 검사는 완료되지만 이전 상태는 손실됩니다.
  - 파일 악성코드 차단 - 페일오버 전에 파일 상태를 확인할 수 있어야 합니다.
  - 파일 유형 탐지 및 차단 - 페일오버 전에 파일 유형이 식별되어야 합니다. 원래 액티브 디바이스가 파일을 식별하는 중에 페일오버가 수행되면 파일 유형이 동기화되지 않습니다. 따라서 파일 정책에서 해당 파일 유형을 차단하더라도 새 액티브 디바이스는 파일을 다운로드합니다.
- ID 정책의 패시브 사용자 ID 결정(종속 포털을 통한 활성 인증을 통해 수집된 결정은 제외).
- 보안 인텔리전스 결정.
- RA VPN - 원격 액세스 VPN 최종 사용자는 페일오버 후 VPN 세션을 다시 인증하거나 다시 연결하지 않아도 됩니다. 그러나 VPN 연결을 통해 작동하는 애플리케이션의 경우 페일오버 프로세스 도중 패킷이 손실될 수 있으며 패킷이 손실되면 복구되지 않습니다.
- 모든 연결 중에서 설정된 연결만 스탠바이 ASA에 복제됩니다.

지원되지 않는 기능

스테이트풀 페일오버에서는 다음 상태 정보가 스탠바이 위협 방지 디바이스로 전달되지 않습니다.

- GRE 또는 IP-in-IP와 같은 일반 텍스트 터널의 . 터널 내의 세션은 복제되지 않으며, 새 액티브 노드는 기존 검사 판정을 재사용하여 정확한 정책 규칙 일치 여부를 확인할 수 없습니다.
- 암호 해독된 TLS/SSL 연결 - 암호 해독 상태가 동기화되지 않고 만약 액티브 유닛에 장애가 발생하면 암호 해독된 연결이 재설정됩니다. 새 활성 유닛에 새 연결을 설정해야 합니다. 암호 해독되지 않은 연결(TLS/SSL 암호 해독 안 함 규칙 작업과 일치하는 연결)은 영향을 받지 않으며, 올바르게 복제됩니다.
- 멀티캐스트 라우팅.

스탠바이 유닛에서 허용되는 컨피그레이션 변경 사항 및 작업

고가용성 모드에서 작동 중일 때는 액티브 유닛에서만 컨피그레이션을 변경합니다. 컨피그레이션을 구축하면 새 변경 사항이 스탠바이 유닛에도 전송됩니다.

하지만 스탠바이 유닛에만 있는 속성도 있습니다. 스탠바이 유닛에서 변경할 수 있는 항목은 다음과 같습니다.

- 관리 IP 주소 및 게이트웨이.
- (CLI에서만 가능) 관리자 사용자 계정 및 기타 로컬 사용자 계정의 비밀번호. CLI에서만 이것을 변경할 수 있고, device manager에서는 할 수 없습니다. 모든 로컬 사용자는 두 유닛 모두의 비밀번호를 개별적으로 변경해야 합니다.

또한 스탠바이 디바이스에서는 다음과 같은 작업이 가능합니다.

- 고가용성 작업(예: HA 일시 중단, 다시 시작, 재설정, 해제, 액티브 및 스탠바이 유닛 간 모드 전환).
- 대시보드 및 이벤트 데이터는 디바이스별로 고유하며 동기화되지 않습니다. 여기에는 이벤트 뷰어의 맞춤형 보기가 포함됩니다.
- 감사 로그 정보는 디바이스별로 고유합니다.
- 스마트 라이선싱 등록. 그러나 선택적 라이선스는 액티브 유닛에서 활성화하거나 비활성화해야 하며, 해당 작업은 스탠바이 유닛과 동기화됩니다. 그러면 스탠바이 유닛이 적절한 라이선스를 요청하거나 해제합니다.
- 백업(복원은 아님). 백업을 복원하려면 유닛에서 HA를 해제해야 합니다. 백업이 HA 컨피그레이션을 포함하는 경우 유닛이 HA 그룹에 다시 조인합니다.
- 소프트웨어 업그레이드 설치.
- 트러블슈팅 로그 생성.

- 지리위치 또는 보안 인텔리전스 데이터베이스 수동 업데이트. 이러한 데이터베이스는 유닛 간에 동기화되지 않습니다. 업데이트 일정을 생성하는 경우 유닛은 일관성을 독립적으로 유지할 수 있습니다.
- **Monitoring(**모니터링**)** > **Sessions(**세션**)** 페이지에서 활성 device manager 사용자 세션을 볼 수 있으며 세션을 삭제할 수 있습니다.

고가용성을 위한 시스템 요구 사항

다음 주제에서는 고가용성 컨피그레이션으로 두 디바이스를 통합하기 전에 충족해야 하는 요구 사항을 설명합니다.

HA의 하드웨어 요구 사항

고가용성 컨피그레이션에서 두 디바이스를 연결하려면 다음 하드웨어 요구 사항을 충족해야 합니다.

- 디바이스의 하드웨어 모델이 정확히 동일해야 합니다.

  Firepower 9300의 경우 고가용성은 동일한 유형의 모듈 간에만 지원되지만, 두 섀시는 혼합된 모듈을 포함할 수 있습니다. 예를 들어, 각 섀시에는 SM-36 및 SM-44가 있습니다. SM-36 모듈 간, SM-44 모듈 간에 고가용성 쌍을 생성할 수 있습니다.

- 디바이스의 인터페이스 수와 유형이 동일해야 합니다.

  Firepower 4100/9300 섀시의 경우, HA를 활성화하기 전에 FXOS에서 모든 인터페이스를 사전에 동일하게 구성해야 합니다. HA를 활성화한 후에 인터페이스를 변경하는 경우에는 스탠바이 유닛의 FXOS에서 인터페이스를 변경한 다음, 액티브 유닛에서 동일하게 변경을 수행합니다.

- 디바이스에 동일한 모듈이 설치되어 있어야 합니다. 예를 들어, 한 디바이스에 네트워크 인터페이스 모듈(선택 사항)이 있는 경우 다른 디바이스에도 동일한 모듈을 설치해야 합니다.
- Firepower 9300용 섀시 내 고가용성은 지원되지 않습니다. 동일한 Firepower 9300섀시에서 별도의 논리적 디바이스 간에 HA를 구성할 수는 없습니다.

HA의 소프트웨어 요구 사항

고가용성 컨피그레이션에서 두 디바이스를 연결하려면 다음 소프트웨어 요구 사항을 충족해야 합니다.

- 두 디바이스가 정확히 동일한 소프트웨어 버전을 실행해야 합니다. 즉, 주 버전 번호(첫 번째), 부 버전 번호(두 번째) 및 유지 보수 버전 번호(세 번째)가 같아야 합니다. device manager의 **Devices(**디바이스**)** 페이지에서 버전을 확인하거나 CLI에서 **show version** 명령을 사용할 수 있습니다. 각기 다른 버전이 설치된 디바이스도 조인할 수는 있지만, 유닛을 같은 소프트웨어 버전으로 업그레이드할 때까지는 컨피그레이션을 스탠바이 유닛으로 가져올 수 없으며 페일오버가 작동하지 않습니다.

- 두 디바이스가 모두 로컬 관리자 모드여야 합니다(device manager을 사용하여 구성되어 있어야 함). 두 시스템에서 모두 device manager에 로그인할 수 있다면 로컬 관리자 모드인 것입니다. CLI에서 **show managers** 명령을 사용하여 확인할 수도 있습니다.
- 각 디바이스에 대해 초기 설정 마법사를 완료해야 합니다.
- 각 디바이스에 자체 관리 IP 주소가 있어야 합니다. 관리 인터페이스의 컨피그레이션은 디바이스 간에 동기화되지 않습니다.
- 디바이스의 NTP 컨피그레이션이 같아야 합니다.
- DHCP를 사용하여 주소를 획득하도록 인터페이스를 구성할 수는 없습니다. 즉, 모든 인터페이스에 고정 IP 주소가 있어야 합니다.
- 클라우드 서비스의 경우 두 디바이스를 같은 지역에 등록해야 하거나 두 디바이스를 모두 등록할 수 없습니다. 혼합 클라우드 서비스 등록은 할 수 없습니다.
- 고가용성을 구성하기 전에 보류 중인 변경 사항을 모두 구축해야 합니다.

HA의 라이선스 요구 사항

유닛은 고가용성을 구성하기 전에 동일한 상태여야 합니다. 즉, 두 유닛이 모두 Base 라이선스로 등록되어 있거나 평가 모드여야 합니다. 등록된 디바이스는 다른 Cisco Smart Software Manager 어카운트에 등록할 수 있습니다. 단, 이러한 어카운트의 내보내기 제어 기능 설정 상태가 같아야 합니다(둘 다 활성화되어 있거나 비활성화되어 있어야 함). 그러나 각 유닛에 각기 다른 선택적 라이선스를 활성화했는지는 중요하지 않습니다. 두 유닛을 모두 등록하는 경우, 디바이스에 대해 동일한 Cisco Cloud Services 지역을 선택해야 합니다.

디바이스가 등록된 경우 스마트 라이선스 또는 PLR(영구 라이선스 예약) 중 하나의 모드를 동일하게 사용해야 합니다.

작동 중에는 고가용성 쌍의 유닛은 라이선스가 동일해야 합니다. 활성 유닛에서의 라이선스 변경은 구축 중에 스탠바이 유닛에서도 반복됩니다.

고가용성 컨피그레이션에서는 디바이스 쌍의 각 디바이스에 대해 하나씩, 두 개의 Smart License 자격이 필요합니다. 어카운트에 각 디바이스에 적용할 라이선스가 충분한지 확인해야 합니다. 라이선스가 부족하면 디바이스별로 컴플라이언스 상태가 달라질 수 있습니다.

예를 들어 액티브 디바이스에는 Base 라이선스와 위협 라이선스가 있는데 스탠바이 디바이스에 Base 라이선스만 있는 경우, 스탠바이 유닛은 Cisco Smart Software Manager와 통신하여 어카운트에서 사용 가능한 위협 라이선스를 가져옵니다. Smart License 어카운트에 구매한 자격이 충분히 없으면, 정확한 수의 라이선스를 구매할 때까지 어카운트는 컴플라이언스 위반 상태가 됩니다(액티브 디바이스는 컴플라이언스 준수 상태이더라도 스탠바이 디바이스는 컴플라이언스 위반 상태).

참고 내보내기 제어 기능에 대한 설정이 서로 다른 계정에 디바이스를 등록하거나 한 유닛은 등록하고 다른 유닛은 평가 모드에 있는 HA 쌍을 생성하려는 경우, HA 가입에 실패할 수 있습니다. 내보내기 제어 기능에 대한 일관성 없는 설정으로 IPsec 암호화 키를 구성하면 HA를 활성화한 후에 두 디바이스가 모두 활성화됩니다. 이로 인해 지원되는 네트워크 세그먼트에서의 라우팅이 영향을 받게 되고, 이를 복구하기 위해서는 보조 유닛에서 HA를 수동으로 해제해야 합니다.

고가용성에 대한 지침

모델 지원

- Firepower 9300 - Firepower 9300에서 HA를 구성할 수 있습니다. 그러나 동일한 Firepower 9300 섀시에서 별도의 논리적 디바이스 간에 HA를 컨피그레이션할 수는 없습니다.
- Firepower 1010:
  - 고가용성 사용 시 스위치 포트 기능을 사용해서는 안 됩니다. 스위치 포트는 하드웨어에서 작동하므로 액티브 및 스탠바이 유닛에서 계속 트래픽을 전달합니다. 고가용성은 트래픽이 스탠바이 유닛을 통과하는 것을 방지하기 위해 고안되었지만 스위치 포트로 확장되지는 않습니다. 일반 고가용성 네트워크 설정에서 두 유닛의 액티브 스위치 포트는 네트워크 루프로 이어집니다. 모든 스위칭 기능에는 외부 스위치를 사용하는 것이 좋습니다. VLAN 인터페이스는 장애 조치를 통해 모니터링될 수 있지만 스위치 포트는 그럴 수 없습니다. 이론적으로는 VLAN에 단일 스위치 포트를 배치하고 고가용성을 정상적으로 사용할 수 있지만, 물리적 방화벽 인터페이스를 대신 사용하면 더 간단하게 설정할 수 있습니다.
  - 방화벽 인터페이스만 장애 조치 링크로 사용할 수 있습니다.
- Threat Defense Virtual — HA 컨피그레이션은 Microsoft Azure Cloud 또는 AWS(Amazon Web Services) Cloud용 threat defense virtual에 대해 지원되지 않습니다.

추가 지침

- 169.254.0.0/16 및 fd00:0:0:*::/64는 내부적으로 사용되는 서브넷이며 페일오버 또는 상태 링크에 사용할 수 없습니다.
- 액티브 유닛에서 컨피그레이션 작업을 실행하면 액티브 유닛에서 구축 작업을 실행할 때 스탠바이 유닛에 동기화됩니다. 그러나 일부 변경 사항은 스탠바이 유닛에 동기화되지 않은 상태라 하더라도 해당 변경 사항을 구축할 때까지는 보류 중 변경 사항에 표시되지 않습니다. 다음 중 어느 것을 변경하는 경우, 해당 변경 사항은 표시되지 않으며 먼저 구축 작업을 실행해야 스탠바이 유닛에 컨피그레이션됩니다. 변경 사항을 즉시 적용해야 하는 경우, 보류 중인 변경 사항에 표시되는 다른 변경 작업을 수행해야 합니다. 표시되지 않은 변경 사항에는 규칙 예약, 지오데이터베이스, 보안 인텔리전스 또는 VDB 업데이트, 백업 예약, NTP, 관리 인터페이스용 DNS, 등에 대한 수정 사항이 포함되어 있습니다.

- 기본 유닛과 보조 유닛에서 모두 백업을 수행해야 합니다. 백업을 복원하려면 먼저 HA를 해제해야 합니다. 두 유닛에서 동일한 백업을 복원하지 마십시오. 이렇게 하면 두 유닛이 모두 액티브로 설정됩니다. 대신 액티브로 설정할 유닛에서 백업을 먼저 복원한 후에 다른 유닛에서 해당하는 백업을 복원합니다.
- 여러 ID 소스의 **Test(**테스트**)** 버튼은 액티브 유닛에서만 작동합니다. 스탠바이 디바이스에 대한 ID 소스 연결을 테스트해야 하는 경우 먼저 모드를 전환하여 스탠바이 피어를 액티브 피어로 설정해야 합니다.
- 고가용성 컨피그레이션을 생성하거나 해제하는 경우, 컨피그레이션 변경 사항을 구축하면 두 디바이스에서 모두 Snort 검사 프로세스가 재시작됩니다. 그러면 프로세스가 완전히 재시작될 때까지 통과 트래픽이 중단될 수 있습니다.
- 고가용성을 처음 구성할 때 보조 유닛의 보안 인텔리전스 및 지리위치 데이터베이스 버전이 기본 유닛과 다르면 데이터베이스를 업데이트하는 작업이 보조 유닛에서 예약됩니다. 이러한 작업은 액티브 유닛에서 다음 구축 시에 실행됩니다. HA 조인에 실패하는 경우 이러한 작업은 유지되며 다음 구축 시에 실행됩니다.
- 액티브 유닛에서 스탠바이 유닛으로 페일오버를 시작할 경우, STP(Spanning Tree Protocol)를 실행 중인 연결된 스위치 포트에서는 토폴로지 변경을 인지하는 경우 30초 ~ 50초 동안 차단 상태가 될 수 있습니다. 포트가 차단 상태일 때 트래픽 손실을 방지하기 위해 스위치에서 STP PortFast 기능을 활성화할 수 있습니다.

  interface *interface_id* **spanning-tree portfast**

  이 해결 방법은 라우팅 모드 및 브리지 그룹 인터페이스에 모두 연결된 스위치에 적용됩니다. PortFast 기능을 사용하면 링크 작동 시 포트가 STP 전달 모드로 즉시 전환됩니다. 포트는 STP에 계속 참여합니다. 따라서 포트가 루프의 일부인 경우 포트가 STP 차단 모드로 전환됩니다.
- 고가용성 쌍에 연결된 스위치에서 포트 보안을 구성할 경우 페일오버 이벤트가 발생할 때 통신에 문제가 생길 수 있습니다. 이러한 문제는 한 보안 포트에서 구성하거나 확인한 보안 MAC 주소가 다른 보안 포트로 이동될 경우 발생하며, 스위치 포트 보안 기능에 의해 위반 여부가 플래그로 표시됩니다.
- 액티브/스탠바이 고가용성 및 VPN IPsec 터널의 경우, VPN 터널을 통해 SNMP를 사용하여 액티브 유닛과 스탠바이 유닛을 모두 모니터링할 수는 없습니다. 스탠바이 유닛에는 활성 VPN 터널이 없으며 NMS(Network Management System)로 전송되는 트래픽은 삭제됩니다. 암호화 기능이 있는 SNMPv3을 대신 사용하면 IPsec 터널을 사용하지 않아도 됩니다.

고가용성 구성

디바이스에서 장애가 발생하더라도 네트워크에 연결할 수 있도록 하려면 고가용성 설정을 사용합니다. 액티브/스탠바이 고가용성을 사용하는 경우에는 두 디바이스가 연결되므로 액티브 디바이스에서 장애가 발생하면 스탠바이 디바이스가 작업을 이어받으며 사용자에는 연결 문제가 잠시 동안만 표시됩니다.

다음 절차에서는 액티브/스탠바이 고가용성 쌍을 설정하는 전체 프로세스를 설명합니다.

프로시저

단계 **1** 고가용성을 위한 두 유닛 준비, 222 페이지.

단계 **2** 고가용성을 위한 기본 유닛 구성, 224 페이지.

단계 **3** 고가용성을 위한 보조 유닛 구성, 227 페이지.

단계 **4** 상태 모니터링을 위한 페일오버 기준 구성, 228 페이지.

기준에는 피어 모니터링과 인터페이스 모니터링이 포함됩니다. 모든 페일오버 기준에는 기본 설정이 있지만, 최소한 기본 설정을 검사하여 네트워크에서 기본 설정이 작동하는지를 확인해야 합니다.

- 피어 유닛 상태 모니터링 페일오버 기준 구성, 229 페이지.
- 인터페이스 상태 모니터링 페일오버 기준 구성, 230 페이지.

  인터페이스 테스트에 대한 정보는 시스템이 인터페이스 상태를 테스트하는 방법, 232 페이지의 내용을 참조하십시오.

단계 **5** (선택 사항, 권장함.) 스탠바이 IP 및 MAC 주소 구성, 233 페이지.

단계 **6** (선택 사항). 고가용성 컨피그레이션 확인, 234 페이지.

고가용성을 위한 두 유닛 준비

고가용성을 적절하게 구성하려면 몇 가지 사항을 정확하게 준비해야 합니다.

프로시저

단계 **1** 디바이스가 HA의 하드웨어 요구 사항, 218 페이지에 설명되어 있는 요구 사항을 충족하는지 확인합니다.

단계 **2** 단일 페일오버 링크를 사용할 것인지 아니면 별도의 페일오버 링크와 스테이트풀 페일오버 링크를 사용할지를 결정하고, 사용할 포트를 식별합니다.

각 링크에 대해 각 디바이스에서 같은 포트 번호를 사용해야 합니다. 예를 들어 두 디바이스에서 모두 페일오버 링크용으로 GigabitEthernet 1/3을 사용합니다. 실수로 해당 포트 번호를 다른 용도에 사용하는 일이 없도록, 사용할 포트를 확실히 파악해야 합니다. 자세한 내용은 페일오버 및 스테이트풀 페일오버 링크, 211 페이지를 참고하십시오.

단계 **3** 디바이스를 설치하고 네트워크에 연결한 다음 각 디바이스에서 초기 설정 마법사를 완료합니다.

a) 페일오버 및 데이터 링크 중단 방지, 214 페이지에서 권장 네트워크 설계를 검토합니다.

b) 인터페이스 연결, 9 페이지에 설명된 대로 최소한 외부 인터페이스를 연결합니다.

다른 인터페이스도 연결할 수 있지만, 이 경우에는 각 디바이스에서 동일한 포트를 사용하여 지정된 서브넷에 연결해야 합니다. 디바이스는 같은 컨피그레이션을 공유하므로 병렬 방식으로 네트워크에 연결해야 합니다.

참고 설정 마법사에서는 관리 및 내부 인터페이스의 IP 주소를 변경할 수 없습니다. 그러므로 기본 디바이스에서 이러한 인터페이스 중 하나를 네트워크에 연결하는 경우 보조 디바이스에서도 해당 인터페이스를 연결하면 안 됩니다. 이렇게 하면 IP 주소가 충돌하게 됩니다. 워크스테이션을 이러한 인터페이스 중 하나에 직접 연결하고 DHCP를 통해 주소를 얻을 수 있습니다. 그러면 device manager에 연결하여 디바이스를 구성할 수 있습니다.

c) 각 디바이스에서 초기 설정 마법사를 완료합니다. 외부 인터페이스에 대한 정적 IP 주소를 지정했는지 확인합니다. 그리고 동일한 NTP 서버를 구성합니다. 자세한 내용은 설정 마법사를 사용하여 초기 컨피그레이션 완료, 20 페이지를 참고하십시오.

유닛에 대해 동일한 라이선싱 및 Cisco Success Network 옵션을 선택합니다. 예를 들어 각 유닛을 평가 모드로 설정하거나 디바이스를 등록합니다.

d) 보조 디바이스에서 **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Management Interface(**관리 인터페이스**)**를 선택한 다음 고유한 IP 주소를 구성하고, 필요한 경우 게이트웨이를 변경하고, 필요에 맞게 DHCP 서버 설정을 비활성화하거나 변경합니다.

e) 보조 디바이스에서 **Device(**디바이스**)** > **Interface(**인터페이스**)**를 선택하고 내부 인터페이스를 수정합니다. IP 주소를 삭제하거나 변경합니다. 또한 인터페이스에 대해 정의된 DHCP 서버를 삭제합니다. 같은 네트워크에 DHCP 서버가 두 개일 수는 없기 때문입니다.

f) 보조 디바이스에서 컨피그레이션을 구축합니다.

g) 네트워크 토폴로지에 따라 필요한 경우 기본 디바이스에 로그인한 다음 관리 주소, 게이트웨이 및 DHCP 서버 설정과 내부 인터페이스 IP 주소 및 DHCP 서버 설정을 변경합니다. 변경을 하는 경우에는 컨피그레이션을 구축합니다.

h) 내부 인터페이스 또는 관리 인터페이스(별도의 관리 네트워크 사용 시)를 연결하지 않은 경우에는 지금 해당 인터페이스를 스위치에 연결할 수 있습니다.

단계 **4** 디바이스의 소프트웨어 버전이 정확히 동일한지 확인합니다. 주 버전 번호(첫 번째 숫자), 부 버전 번호(두 번째 숫자) 및 유지 보수 버전 번호(세 번째 숫자)가 같아야 합니다. device manager의 Devices(디바이스) 페이지에서 버전을 확인하거나 CLI에서 **show version** 명령을 사용할 수 있습니다.

디바이스가 동일한 소프트웨어 버전을 실행하고 있지 않다면 Cisco.com에서 원하는 소프트웨어 버전을 다운로드하여 각 디바이스에 설치합니다. 자세한 내용은 Threat Defense 소프트웨어 업그레이드, 860 페이지를 참조해 주십시오.

단계 **5** 페일오버 및 스테이트풀 페일오버 링크를 연결하고 구성합니다.

a) 페일오버 및 데이터 링크 중단 방지, 214 페이지에서 선택한 원하는 네트워크 설계에 따라 각 디바이스에 대해 페일오버 인터페이스를 적절하게 연결합니다(스위치에 연결하거나 인터페이스를 서로 직접 연결).

b) 별도의 상태 링크를 사용하는 경우에는 각 디바이스에 대해 스테이트풀 장애 조치 인터페이스도 적절하게 연결합니다.

c) 각 디바이스에 차례로 로그인한 다음, **Device(**디바이스**)** > **Interface(**인터페이스**)**로 이동합니다. 각 인터페이스를 수정하고 인터페이스 이름 또는 IP 주소가 구성되어 있지 않는지 확인합니다.

이름이 지정된 인터페이스가 구성되어 있으면 보안 영역에서 해당 인터페이스를 제거하고 다른 컨피그레이션을 삭제해야 이름을 삭제할 수 있습니다. 이름 삭제에 실패하면 오류 메시지를 검사하여 수행해야 하는 기타 변경 작업을 확인합니다.

단계 **6** 기본 디바이스에서 나머지 데이터 인터페이스를 연결하고 디바이스를 구성합니다.

a) **Device(**디바이스**)** > **Interface(**인터페이스**)**를 선택하고 통과 트래픽에 사용되는 각 인터페이스를 수정한 다음 기본 고정 IP 주소를 구성합니다.

b) 보안 영역에 인터페이스를 추가하고 연결된 네트워크에서 트래픽을 처리하는 데 필요한 기본 정책을 구성합니다. 예시 컨피그레이션은 모범 사례: Threat Defense의 사용 사례, 43 페이지에 나와 있는 주제를 참조하십시오.

c) 컨피그레이션을 구축합니다.

단계 **7** HA의 소프트웨어 요구 사항, 218 페이지에 설명되어 있는 모든 요구 사항을 충족하는지 확인합니다.

단계 **8** 라이선싱이 일치하는지(등록됨 또는 평가 모드) 확인합니다. 자세한 내용은 HA의 라이선스 요구 사항, 219 페이지를 참고하십시오.

단계 **9** 보조 디바이스에서 나머지 데이터 인터페이스를 기본 디바이스의 해당 인터페이스와 동일한 네트워크에 연결합니다. 인터페이스를 구성하지는 마십시오.

단계 **10** 각 디바이스에서 **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Cloud Services(**클라우드 서비스**)**를 선택하고 설정이 동일한지 확인합니다.

이제 기본 디바이스에서 고가용성을 구성할 준비가 되었습니다.

고가용성을 위한 기본 유닛 구성

액티브/스탠바이 고가용성 쌍을 설정하려면 먼저 기본 디바이스를 구성해야 합니다. 기본 디바이스는 정상적인 상황에서 액티브 상태로 운영할 유닛입니다. 보조 디바이스는 기본 유닛이 사용 불가 상태가 될 때까지 스탠바이 모드로 유지됩니다.

기본으로 지정할 디바이스를 선택한 다음 해당 디바이스에서 device manager에 로그인하여 이 절차를 수행합니다.

참고 고가용성 쌍을 설정한 후 이 절차에서 설명하는 컨피그레이션을 수정하려면 해당 쌍을 해제해야 합니다.

시작하기 전에

페일오버 및 스테이트풀 페일오버 링크에 대해 구성하는 인터페이스에 이름이 지정되어 있지 않은지 확인합니다. 이러한 인터페이스에 현재 이름이 지정되어 있는 경우 보안 영역 개체를 포함하여 해당 이름을 사용하는 정책에서 인터페이스를 제거한 다음, 인터페이스를 수정하여 이름을 삭제해야 합니다. 또한 인터페이스는 패시브 모드가 아닌 라우팅 모드여야 합니다. 이러한 인터페이스는 HA 컨피그레이션 전용이어야 하며 다른 용도로는 사용할 수 없습니다.

보류 중인 변경 사항이 있는 경우 변경 사항을 구축해야 HA를 구성할 수 있습니다.

프로시저

단계 **1** 디바이스를 클릭합니다.

단계 **2** 디바이스 요약 오른쪽의 **High Availability(**고가용성**)** 옆에 있는 **Configure(**구성**)**를 클릭합니다.

디바이스에서 HA를 처음 구성하는 경우 그룹이 다음과 같이 표시됩니다.

단계 **3** High Availability(고가용성) 페이지에서 **Primary Device(**기본 디바이스**)** 확인란을 클릭합니다.

보조 디바이스가 이미 구성되어 있으며 클립보드에 컨피그레이션을 복사한 경우 **Paste from Clipboard(**클립보드에서 붙여넣기**)** 버튼을 클릭하여 컨피그레이션을 붙여넣을 수 있습니다. 이렇게 하면 필드가 적절한 값으로 업데이트되며, 그러면 해당 값을 확인할 수 있습니다.

단계 **4** **Failover Link(**페일오버 링크**)** 속성을 구성합니다.

페일오버 쌍의 두 유닛은 페일오버 링크를 통해 지속적으로 통신하여 각 유닛의 작동 상태를 확인하고 컨피그레이션 변경 사항을 동기화합니다. 자세한 내용은 페일오버 링크, 212 페이지를 참고하십시오.

- **Physical Interface(**물리적 인터페이스**)** - 페일오버 링크로 사용할 보조 디바이스에 연결한 인터페이스를 선택합니다. 이 인터페이스에는 이름이 지정되어 있지 않아야 합니다.

  EtherChannel 인터페이스를 장애 조치 또는 상태 링크로 사용하는 경우, 고가용성을 설정하기 전에 동일한 ID 및 멤버 인터페이스를 사용하는 동일한 EtherChannel이 두 디바이스에 있는지 확인해야 합니다. EtherChannel이 일치하지 않는 경우에는 HA를 비활성화하고 이전의 보조 유닛에서 구성을 수정해야 합니다. 패킷의 오류를 방지하기 위해 EtherChannel에서는 하나의 인터페이스만 사용됩니다. 해당 인터페이스에 오류가 발생할 경우 EtherChannel의 다음 인터페이스가 사용됩니다. 장애 조치 링크로 사용 중인 경우 EtherChannel 컨피그레이션을 변경할 수 없습니다.

- **Type(**유형**)** - 인터페이스에 사용할 주소(IPv4 또는 IPv6)를 선택합니다. 한 가지 유형의 주소만 구성할 수 있습니다.

- **Primary IP(**기본 **IP)** - 이 디바이스의 인터페이스 IP 주소를 입력합니다. 예를 들어 192.168.10.1을 입력합니다. IPv6 주소의 경우에는 2001:a0a:b00::a0a:b70/64와 같이 표준 표기법의 접두사 길이를 포함해야 합니다.

- **Secondary IP(**보조 **IP)** - 보조 디바이스의 인터페이스에 대해 링크 반대쪽에 구성해야 하는 IP 주소를 입력합니다. 해당 주소는 기본 주소와 같은 서브넷에 있어야 하며 기본 주소와는 달라야 합니다. 예를 들어 192.168.10.2 또는 2001:a0a:b00::a0a:b71/64를 입력합니다.

- **Netmask(**넷마스크**)**(IPv4 주소에만 해당) - 기본/보조 IP 주소의 서브넷 마스크를 입력합니다.

단계 **5** 스테이트풀 페일오버 링크 속성을 구성합니다.

시스템은 상태 링크를 사용해 연결 상태 정보를 스탠바이 디바이스에 전달합니다. 페일오버 수행 시에 스탠바이 유닛은 이 정보를 사용하여 기존 연결을 유지할 수 있습니다. 같은 링크를 페일오버 링크로 사용하거나 별도의 링크를 구성할 수 있습니다.

- **Use the Same Interface as the Failover Link(**페일오버 링크와 같은 인터페이스 사용**)** - 페일오버 및 스테이트풀 페일오버 통신에 단일 링크를 사용하려는 경우 이 옵션을 선택합니다. 이 옵션을 선택하는 경우 다음 단계를 계속 진행합니다.
- **Physical Interface(**물리적 인터페이스**)** - 별도의 스테이트풀 페일오버 링크를 사용하려는 경우 스테이트풀 페일오버 링크로 사용할 보조 디바이스에 연결한 인터페이스를 선택합니다. 이 인터페이스에는 이름이 지정되어 있지 않아야 합니다. 그런 다음, 다음의 속성을 구성합니다.
  - **Type(**유형**)** - 인터페이스에 사용할 주소(IPv4 또는 IPv6)를 선택합니다. 한 가지 유형의 주소만 구성할 수 있습니다.
  - **Primary IP(**기본 **IP)** - 이 디바이스의 인터페이스 IP 주소를 입력합니다. 해당 주소는 페일오버 링크에 사용한 주소와 다른 서브넷에 있어야 합니다. 예를 들어 192.168.11.1를 입력합니다. IPv6 주소의 경우에는 2001:a0a:b00:a::a0a:b70/64와 같이 표준 표기법의 접두사 길이를 포함해야 합니다.
  - **Secondary IP(**보조 **IP)** - 보조 디바이스의 인터페이스에 대해 링크 반대쪽에 구성해야 하는 IP 주소를 입력합니다. 해당 주소는 기본 주소와 같은 서브넷에 있어야 하며 기본 주소와는 달라야 합니다. 예를 들어 192.168.11.2 또는 2001:a0a:b00:a::a0a:b71/64를 입력합니다.
  - **Netmask(**넷마스크**)**(IPv4 주소에만 해당) - 기본/보조 IP 주소의 서브넷 마스크를 입력합니다.

단계 **6** (선택 사항). 디바이스 쌍의 두 유닛 간 통신을 암호화하려면 **IPsec Encryption Key(IPsec** 암호화 키**)** 문자열을 입력합니다.

보조 노드에서 정확히 동일한 키를 구성해야 하므로 입력하는 문자열을 적어 두십시오.

키를 입력하지 않으면 페일오버 및 스테이트풀 페일오버 링크의 모든 통신에는 일반 텍스트가 사용됩니다. 인터페이스 간에 다이렉트 케이블 연결을 사용하지 않는 경우 보안 문제가 발생할 수 있습니다.

참고 평가 모드에서 HA 페일오버 암호화를 구성하는 경우 시스템은 암호화에 DES를 사용합니다. 그런 다음 내보내기 호환 계정을 사용하여 디바이스를 등록하면 디바이스는 재부팅 후 AES를 사용합니다. 따라서 업그레이드를 설치한 후를 포함하여 어떤 이유로든 시스템을 재부팅하면 피어가 통신할 수 없으며 두 유닛이 모두 활성 유닛이 됩니다. 디바이스를 등록할 때까지는 암호화를 구성하지 않는 것이 좋습니다. 평가 모드에서 구성하는 경우 디바이스를 등록하기 전에 암호화를 제거하는 것이 좋습니다.

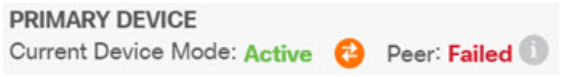
단계 **7** **Activate HA(HA** 활성화**)**를 클릭합니다.

시스템이 디바이스에 컨피그레이션을 즉시 구축합니다. 따라서 구축 작업을 시작할 필요가 없습니다. 컨피그레이션이 저장되었으며 구축이 진행 중이라는 메시지가 표시되지 않으면 페이지 위쪽으로 스크롤하여 오류 메시지를 확인합니다.

컨피그레이션은 클립보드에도 복사됩니다. 이 복사본을 사용하면 보조 유닛을 빠르게 구성할 수 있습니다. 보안 강화를 위해 암호화 키는 클립보드 복사본에 포함되지 않습니다.

컨피그레이션이 완료되면 수행해야 하는 다음 단계를 설명하는 메시지가 표시됩니다. 해당 정보를 확인한 후 **Got It(**확인**)**을 클릭합니다.

이 시점에서 High Availability(고가용성) 페이지가 표시되며 디바이스 상태는 "Negotiating(협상 중)"이라고 나타나야 합니다. 상태는 피어를 구성하기 전에 Active(활성)로 전환됩니다. 피어를 구성하기 전까지는 Failed(장애 발생)로 표시됩니다.



이제 보조 유닛을 구성할 수 있습니다. 고가용성을 위한 보조 유닛 구성, 227 페이지의 내용을 참조하십시오.

참고 선택한 인터페이스는 직접 구성되지 않습니다. 하지만 CLI에서 **show interface**를 입력하면 인터페이스가 지정한 IP 주소를 사용 중임을 확인할 수 있습니다. 인터페이스 이름은 "failover-link"로 지정되며 별도의 상태 링크를 구성하는 경우에는 "stateful-failover-link"로 지정됩니다.

고가용성을 위한 보조 유닛 구성

액티브/스탠바이 고가용성용 기본 디바이스를 구성한 후에는 보조 디바이스를 구성해야 합니다. 해당 디바이스에서 device manager에 로그인하여 다음 절차를 수행합니다.

참고 고가용성 컨피그레이션을 기본 디바이스에서 클립보드로 아직 복사하지 않은 경우 이를 복사합니다. 데이터를 수동으로 입력하는 것보다 복사/붙여넣기를 사용하여 보조 디바이스를 구성하는 것이 훨씬 더 쉽습니다.

프로시저

단계 **1** 디바이스를 클릭합니다.

단계 **2** 디바이스 요약 오른쪽의 **High Availability(**고가용성**)** 옆에 있는 **Configure(**구성**)**를 클릭합니다.

디바이스에서 HA를 처음 구성하는 경우 그룹이 다음과 같이 표시됩니다.

단계 **3** High Availability(고가용성) 페이지에서 **Secondary Device(**보조 디바이스**)** 확인란을 클릭합니다.

단계 **4** 다음 중 하나를 수행합니다.

- 쉬운 방법 - **Paste from Clipboard(**클립보드에서 붙여넣기**)** 버튼을 클릭하고 컨피그레이션에 붙여넣은 다음 **OK(**확인**)**를 클릭합니다. 이렇게 하면 필드가 적절한 값으로 업데이트되며, 그러면 해당 값을 확인할 수 있습니다.
- 수동 방법 - 페일오버 및 스테이트풀 페일오버 링크를 직접 구성합니다. 기본 디바이스에 입력한 것과 정확히 동일한 설정을 보조 디바이스에 입력합니다.

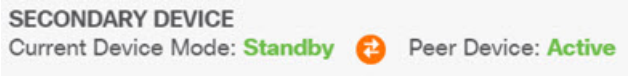
단계 **5** 기본 디바이스에서 **IPSec Encryption Key(IPSec** 암호화 키**)**를 구성한 경우에는 보조 디바이스에 대해 정확히 동일한 키를 입력합니다.

단계 **6** **Activate HA(HA** 활성화**)**를 클릭합니다.

시스템이 디바이스에 컨피그레이션을 즉시 구축합니다. 따라서 구축 작업을 시작할 필요가 없습니다. 컨피그레이션이 저장되었으며 구축이 진행 중이라는 메시지가 표시되지 않으면 페이지 위쪽으로 스크롤하여 오류 메시지를 확인합니다.

컨피그레이션이 완료되면 HA를 구성했다는 메시지가 표시됩니다. **Got It(**확인**)**을 클릭하여 메시지를 해제합니다.

이 시점에서 High Availability(고가용성) 페이지가 표시되며 디바이스 상태에는 디바이스가 보조 디바이스임이 표시되어야 합니다. 기본 디바이스에 정상적으로 조인한 경우 디바이스는 기본 디바이스와 동기화되며, 최종적으로 이 디바이스의 모드가 Standby(스탠바이)로 설정되고 피어는 Active(액티브)로 설정되어야 합니다.



참고 선택한 인터페이스는 직접 구성되지 않습니다. 하지만 CLI에서 **show interface**를 입력하면 인터페이스가 지정한 IP 주소를 사용 중임을 확인할 수 있습니다. 인터페이스 이름은 "failover-link"로 지정되며 별도의 상태 링크를 구성하는 경우에는 "stateful-failover-link"로 지정됩니다.

상태 모니터링을 위한 페일오버 기준 구성

고가용성 컨피그레이션의 유닛은 자체 모니터링을 통해 전반적인 상태와 인터페이스 상태를 확인합니다.

페일오버 기준은 피어에서 장애가 발생했는지 확인하는 상태 모니터링 메트릭을 정의합니다. 기준을 위반하는 유닛이 액티브 피어이면 스탠바이 유닛으로 페일오버를 트리거합니다. 기준을 위반하는 유닛이 스탠바이 피어이면 해당 유닛은 장애 발생 상태로 표시되며 페일오버에 사용할 수 없게 됩니다.

페일오버 기준은 액티브 디바이스에서만 구성할 수 있습니다.

다음 표에는 페일오버를 트리거하는 이벤트 및 관련 장애 탐지 타이밍이 나와 있습니다.

표 ***6:*** 페일오버 기준에 따른 페일오버 시간

페일오버를 트리거하는 이벤트	최소	기본	최대
액티브 유닛의 전원이 중단되거나 정상적인 작동이 중지됩니다.	800밀리초	15초	45초
액티브 유닛 인터페이스의 물리적 링크가 중단됩니다.	500밀리초	5초	15초

페일오버를 트리거하는 이벤트	최소	기본	최대
액티브 유닛 인터페이스가 작동하지만 연결 문제로 인해 인터페이스 테스트가 실행됩니다.	5초	25초	75초

다음 주제에서는 페일오버 상태 모니터링 기준을 맞춤 설정하는 방법과 시스템이 인터페이스를 테스트하는 방법을 설명합니다.

피어 유닛 상태 모니터링 페일오버 기준 구성

고가용성 컨피그레이션의 각 피어는 hello 메시지를 사용해 페일오버 링크를 모니터링하여 다른 유닛의 상태를 확인합니다. 페일오버 링크에서 hello 메시지가 유닛에 3번 연속으로 수신되지 않는 경우, 유닛에서는 페일오버 링크를 비롯한 각 데이터 인터페이스에 LANTEST 메시지를 전송하여 피어의 응답 여부를 검증합니다. 디바이스에서 취하는 조치는 다른 유닛의 응답에 따라 달라집니다.

- 디바이스가 페일오버 링크에서 응답을 수신하는 경우 디바이스는 페일오버를 수행하지 않습니다.
- 디바이스가 페일오버 링크에서는 응답을 수신하지 못했으나 데이터 인터페이스에서는 응답을 수신한 경우 유닛이 페일오버를 수행하지 않습니다. 페일오버 링크가 실패한 것으로 표시됩니다. 페일오버 링크가 중단된 동안에는 유닛에서 스탠바이 유닛으로 페일오버할 수 없으므로 최대한 빨리 페일오버 링크를 복원해야 합니다.
- 디바이스가 어떤 인터페이스에서도 응답을 받지 못한 경우 스탠바이 유닛은 액티브 모드로 전환되고 다른 유닛을 장애 발생 상태로 분류합니다.

hello 메시지의 폴링 및 대기 시간을 구성할 수 있습니다.

프로시저

단계 **1** 액티브 디바이스에서 **Device(**디바이스**)**를 클릭합니다.

단계 **2** 디바이스 요약의 오른쪽에서 **High Availability(**고가용성**)** 링크를 클릭합니다.

High Availability(고가용성) 페이지의 오른쪽 열에 Failover Criteria(페일오버 기준)가 나열됩니다.

단계 **3** **Peer Timing Configuration(**피어 타이밍 컨피그레이션**)**을 정의합니다.

이러한 설정에 따라 액티브 디바이스가 스탠바이 디바이스로 페일오버할 수 있는 속도가 결정됩니다. 폴링 시간이 빠를수록 디바이스에서 더 빨리 장애를 탐지하고 페일오버를 더 빨리 트리거할 수 있습니다. 그러나 감지 기능이 빨라지면 네트워크에 일시적으로 정체 현상이 일어났을 때 불필요한 전환이 발생할 수 있습니다. 기본 설정은 대부분의 상황에 적합합니다.

한 차례의 폴링 기간 동안 유닛이 페일오버 인터페이스에서 hello 패킷을 수신하지 않은 경우, 나머지 인터페이스 전체에 추가 테스트가 이루어집니다. 대기 시간에도 피어 유닛의 응답이 없을 경우 그 유닛에 오류가 발생한 것으로 간주하며, 오류가 발생한 유닛이 활성 유닛이었다면 대기 유닛이 활성 유닛으로 전환합니다.

- **Poll Time(**폴링 시간**)** - hello 메시지 간의 시간입니다. 1~15초 또는 200~999밀리초를 입력합니다. 기본값은 1초입니다.
- **Hold Time(**대기 시간**)** - 유닛이 페일오버 링크에서 hello 메시지를 수신해야 하는 시간입니다. 이 시간이 지나면 피어 유닛은 장애 발생 상태로 선언됩니다. 대기 시간은 폴링 시간의 3배 이상이어야 합니다. 1~45초 또는 800~999밀리초를 입력합니다. 기본값은 15초입니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

인터페이스 상태 모니터링 페일오버 기준 구성

사용 중인 디바이스 모델에 따라 최대 211개의 인터페이스를 모니터링할 수 있습니다. 중요한 인터페이스를 모니터링해야 합니다. 중요 네트워크 간의 처리량을 확인하는 인터페이스를 예로 들 수 있습니다. 인터페이스용 스탠바이 IP 주소를 구성하는 경우 및 인터페이스가 항상 작동해야 하는 경우에만 인터페이스를 모니터링합니다.

2번의 폴링 기간 동안 모니터링된 인터페이스에 대한 hello 메시지가 유닛에 수신되지 않을 경우 인터페이스 테스트가 실행됩니다. 인터페이스에 대한 모든 인터페이스 테스트가 실패하였으나 다른 유닛에 있는 이 동일한 인터페이스에서는 지속적으로 트래픽을 전달할 수 있는 경우, 해당 인터페이스는 오류가 발생한 것으로 간주합니다. 오류가 발생한 인터페이스의 임계값이 충족될 경우 페일오버가 실행됩니다. 다른 유닛의 인터페이스에서도 모든 네트워크 테스트에 실패할 경우, 두 인터페이스 모두 "Unknown(알 수 없음)" 상태가 되며 페일오버 한도에 합산되지 않습니다.

트래픽이 수신될 경우 인터페이스는 다시 작동을 시작합니다. 인터페이스 오류 임계값이 더 이상 충족되지 않을 경우 장애가 발생한 디바이스는 스탠바이 모드로 돌아갑니다.

CLI 또는 CLI 콘솔에서 **show monitor-interface** 명령을 사용하여 인터페이스 HA 상태를 모니터링할 수 있습니다. 자세한 내용은 HA 모니터링 인터페이스의 상태 모니터링, 247 페이지를 참고하십시오.

참고 인터페이스가 중단될 때 페일오버의 경우 계속 유닛 문제로 간주됩니다. 유닛에서 인터페이스가 중단되었음을 탐지하면 인터페이스 대기 시간까지 기다리지 않고 페일오버가 즉시 수행됩니다(기본 임계값인 1개 인터페이스를 유지하는 경우). 인터페이스 대기 시간은 피어에서 hello 패킷이 수신되지 않더라도 유닛이 인터페이스 상태를 정상으로 간주하는 경우에만 유용합니다.

시작하기 전에

기본적으로 모든 명명된 물리적 인터페이스는 HA 모니터링 대상으로 선택됩니다. 따라서 중요하지 않은 물리적 인터페이스에서는 모니터링을 비활성화해야 합니다. 하위 인터페이스 또는 브리지 그룹의 경우 모니터링을 수동으로 활성화해야 합니다.

인터페이스 모니터링을 완전히 비활성화하고 인터페이스 오류로 인한 페일오버를 방지하려는 경우, HA 모니터링에 대해 활성화된 인터페이스가 없는지 확인하기만 하면 됩니다.

프로시저

단계 **1** 액티브 디바이스에서 **Device(**디바이스**)**를 클릭합니다.

단계 **2** 디바이스 요약의 오른쪽에서 **High Availability(**고가용성**)** 링크를 클릭합니다.

High Availability(고가용성) 페이지의 오른쪽 열에 Failover Criteria(페일오버 기준)가 나열됩니다.

단계 **3** **Interface Failure Threshold(**인터페이스 오류 임계값**)**를 정의합니다.

장애가 발생한 인터페이스의 수가 임계값에 도달하면 유닛은 자체 상태를 장애 발생으로 표시합니다. 해당 유닛이 액티브 유닛인 경우 스탠바이 유닛으로 페일오버를 수행합니다. 또한 해당 유닛이 스탠바이 유닛인 경우에는 자체 상태를 장애 발생으로 표시하므로 액티브 유닛이 해당 유닛을 페일오버에 사용할 수 있는 유닛으로 간주하지 않습니다.

이 기준을 설정할 때는 모니터링 중인 인터페이스 수를 고려합니다. 예를 들어 인터페이스 2개에서만 모니터링을 활성화하는 경우에는 임계값(인터페이스 10개)에 도달하지 않습니다. 인터페이스 속성을 수정할 때 **Advanced Options(**고급 옵션**)** 탭에서 **Enable for HA Monitoring(HA** 모니터링에 대해 활성화**)** 옵션을 선택하여 인터페이스에 대해 모니터링을 구성합니다.

기본적으로는 모니터링하는 인터페이스 하나에서 장애가 발생하면 유닛은 자체 상태를 장애 발생으로 표시합니다.

다음의 **Failover Criteria(**페일오버 기준**)** 옵션 중 하나를 선택하여 인터페이스 오류 임계값을 설정할 수 있습니다.

- **Number of failed interfaces exceeds(**장애 발생 인터페이스의 수가 다음 값을 초과함**)** - 인터페이스의 원시 수를 입력합니다. 기본값은 1입니다. 최대값은 실제로 디바이스 모델에 따라 달라지며 모델별로 다를 수 있지만 211보다 큰 값은 입력할 수 없습니다. 이 기준을 사용하는 경우 디바이스가 지원하는 것보다 큰 수를 입력하면 구축 오류가 발생합니다. 오류 발생 시에는 더 작은 숫자를 입력하거나 퍼센트를 대신 사용해 보십시오.
- **Percentage of failed interfaces exceeds(**장애 발생 인터페이스의 퍼센트가 다음 값을 초과함**)** - 1~100 사이의 숫자를 입력합니다. 예를 들어 인터페이스 10개를 모니터링하는 데 50%를 입력하는 경우 인터페이스 5개에서 장애가 발생하면 디바이스가 자체 상태를 장애 발생으로 표시합니다.

단계 **4** **Interface Timing Configuration(**인터페이스 타이밍 컨피그레이션**)**을 정의합니다.

이러한 설정은 인터페이스가 실패한 경우 활성 디바이스를 얼마나 빨리 확인할 수 있는지를 결정합니다. 폴링 시간이 더 빨라지면 디바이스는 인터페이스 오류를 더 빨리 감지할 수 있습니다. 그러나 탐지 속도가 너무 빠르면 사용 중인 인터페이스가 실제로 정상인 경우에도 장애 발생으로 표시하여 페일오버가 불필요하게 자주 발생할 수 있습니다. 기본 설정은 대부분의 상황에 적합합니다.

인터페이스 링크가 중단되면 인터페이스 테스트가 시행되지 않으며, 장애가 발생한 인터페이스 수가 구성된 인터페이스 페일오버 임계값과 일치하거나 이를 초과할 경우 한 차례의 인터페이스 폴링 기간 동안에만 스탠바이 유닛이 액티브 상태가 됩니다.

- **Poll Time(**폴링 시간**)** - hello 패킷이 데이터 인터페이스에서 전송되는 빈도입니다. 1~15초 또는 500~999밀리초를 입력합니다. 기본값은 5초입니다.

- **Hold Time(**대기 시간**)** - 대기 시간은 인터페이스가 장애 발생 상태로 표시될 때 hello 패킷이 손실될 때까지 걸리는 시간을 결정합니다. 5~75초를 입력합니다. 대기 시간은 폴링 시간보다 5배 적게 입력할 수 없습니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

단계 **6** 모니터링할 각 인터페이스에 대해 HA 모니터링을 활성화합니다.

a) **Device(**디바이스**)** > **Interfaces(**인터페이스**)**를 선택합니다.

인터페이스를 모니터링하는 경우 Monitor for HA(HA에 대해 모니터링) 열에 Enabled(활성화)가 표시됩니다.

b) 모니터링 상태를 변경할 인터페이스에 대해 수정 아이콘( )을 클릭합니다.

페일오버 또는 스테이트풀 페일오버 인터페이스는 수정할 수 없습니다. 이러한 인터페이스에는 인터페이스 모니터링이 적용되지 않습니다.

c) **Advanced Options(**고급 옵션**)** 탭을 클릭합니다.

d) **Enable for HA Monitoring(HA** 모니터링에 대해 활성화**)** 확인란을 원하는 대로 선택하거나 선택 취소합니다.

e) **OK(**확인**)**를 클릭합니다.

단계 **7** (선택 사항, 권장함.) 모니터링하는 인터페이스에 대해 스탠바이 IP 주소와 MAC 주소를 구성합니다. 스탠바이 IP 및 MAC 주소 구성, 233 페이지의 내용을 참조하십시오.

시스템이 인터페이스 상태를 테스트하는 방법

시스템은 사용자가 고가용성 상태를 확인하기 위해 모니터링하는 인터페이스를 지속적으로 테스트합니다. 인터페이스 테스트에 사용되는 주소는 사용자가 구성하는 주소 유형을 기준으로 합니다.

- 인터페이스에 IPv4 및 IPv6 주소가 모두 구성되어 있으면 디바이스는 IPv4 주소를 사용하여 상태 모니터링을 수행합니다.
- 인터페이스에 IPv6 주소만 구성되어 있으면 디바이스는 ARP 대신 IPv6 네이버 검색을 사용하여 상태 모니터링 테스트를 수행합니다. 브로드캐스트 ping 테스트의 경우 디바이스는 IPv6 모든 노드 주소를 사용합니다(FE02::1).

시스템은 각 유닛에서 다음 테스트를 수행합니다.

1. 링크 작동/중단 테스트 - 인터페이스 상태에 대한 테스트입니다. 링크 작동/중단 테스트는 인터페이스가 중단되었는지를 나타내며, 인터페이스가 중단된 경우 유닛은 인터페이스에 장애가 발생한 것으로 간주합니다. 상태가 Up(작동 중)인 경우 유닛은 네트워크 활동 테스트를 수행합니다.
2. 네트워크 활동 테스트 - 수신된 네트워크 활동 테스트입니다. 이 테스트의 목적은 LANTEST 메시지를 사용하는 네트워크 트래픽을 생성하여 어떤 유닛에서 오류가 발생했는지 확인하는 것입니다. 테스트를 시작할 때마다 각 유닛에서는 해당 인터페이스에 대한 수신된 패킷 수를 지웁니다. 유닛에서 테스트 동안(최대 5초) 임의의 패킷을 수신하는 즉시, 인터페이스는 작동 중으로 간주됩니다. 한 유닛에는 트래픽이 수신되고 다른 유닛에는 수신되지 않을 경우, 트래픽이 수신되지

않은 유닛은 오류가 발생한 것으로 간주합니다. 어떤 유닛도 트래픽을 받지 못했으면 유닛은 ARP 테스트를 시작합니다.

3. ARP 테스트 - 최근에 얻은 항목 2개의 유닛 ARP 캐시를 읽는 테스트입니다. 유닛에서는 한 번에 하나씩 ARP 요청을 이러한 디바이스에 전송하여 네트워크 트래픽을 자극합니다. 각 요청 후 유닛에서는 최대 5초 동안 수신된 모든 트래픽의 수를 셉니다. 트래픽이 수신된 경우 해당 인터페이스는 제대로 작동 중인 것으로 간주합니다. 트래픽이 수신되지 않으면 ARP 요청이 다음 디바이스에 전송됩니다. 목록 마지막까지 트래픽이 수신되지 않은 경우 유닛은 ping 테스트를 시작합니다.
4. 브로드캐스트 ping 테스트 - 브로드캐스트 ping 요청을 전송하는 작업으로 이루어진 ping 테스트입니다. 그런 다음 유닛에서는 최대 5초 동안 수신된 모든 패킷의 수를 셉니다. 이 간격 동안 언제라도 수신된 패킷이 있을 경우 인터페이스가 작동 중인 것으로 간주되며 테스트가 중지됩니다. 모든 트래픽이 수신되지 않으면, 테스트는 ARP 테스트와 함께 다시 시작됩니다.

스탠바이 IP 및 MAC 주소 구성

인터페이스를 구성할 때는 동일한 네트워크에서 액티브 IP 주소 및 스탠바이 IP 주소를 지정할 수 있습니다. 스탠바이 주소는 지정하는 것이 좋지만 필수 항목은 아닙니다. 스탠바이 IP 주소가 없으면 액티브 유닛이 네트워크 테스트를 수행하여 스탠바이 인터페이스 상태를 확인할 수 없으며 링크 상태만 추적할 수 있습니다. 관리 목적으로 해당 인터페이스에서 스탠바이 유닛에 연결할 수도 없습니다.

1. 기본 유닛에서 페일오버가 수행될 때 보조 유닛에서는 기본 유닛의 IP 주소와 MAC 주소를 가정하고 트래픽 전달을 시작합니다.
2. 이제 스탠바이 상태가 된 유닛에서는 스탠바이 IP 주소와 MAC 주소를 인수합니다.

네트워크 디바이스에서는 MAC-IP 주소 쌍의 변화가 감지되지 않으므로, 네트워크 어디에서도 ARP 항목의 변경이나 시간 초과가 발생하지 않습니다.

기본 유닛을 감지하지 않고 부팅되는 보조 유닛은 액티브 유닛이 되며 기본 유닛의 MAC 주소를 알지 못하므로 고유한 MAC 주소를 사용합니다. 그러나 기본 유닛이 사용 가능해지면 보조(액티브) 유닛이 MAC 주소를 기본 유닛의 주소로 변경하므로 네트워크 트래픽이 중단될 수 있습니다. 마찬가지로, 기본 유닛을 새 하드웨어로 교체하면 새 MAC 주소가 사용됩니다.

시작 시 보조 유닛에 액티브 MAC 주소가 알려지므로 가상 MAC 주소에서는 이러한 중단을 방지하며, 새 기본 유닛 하드웨어가 사용될 경우에도 가상 MAC 주소는 그대로 유지됩니다. 가상 MAC 주소를 수동으로 구성할 수 있습니다.

가상 MAC 주소를 구성하지 않을 경우, 연결된 라우터에서 ARP 테이블을 지워 트래픽 흐름을 복원해야 할 수 있습니다. MAC 주소가 변경될 경우 위협 방지 디바이스에서는 고정 NAT 주소에 불필요한 ARP를 전송하지 않으므로, 연결된 라우터에서는 이러한 주소의 MAC 주소 변경을 알지 못합니다.

프로시저

단계 **1** **Device(**디바이스**)** > **Interfaces(**인터페이스**)**를 선택합니다.

최소한 HA를 모니터링하는 인터페이스에 대해 스탠바이 IP 및 MAC 주소를 구성해야 합니다. 인터페이스를 모니터링하는 경우 Monitor for HA(HA에 대해 모니터링) 열에 Enabled(활성화)가 표시됩니다.

단계 **2** 스탠바이 주소를 구성할 인터페이스의 수정 아이콘( )을 클릭합니다.

페일오버 또는 스테이트풀 페일오버 인터페이스는 수정할 수 없습니다. 고가용성을 구성할 때 이러한 인터페이스에 대해 IP 주소를 설정합니다.

단계 **3** **IPv4 Address(IPv4** 주소**)** 및 **IPv6 Address(IPv6** 주소**)** 탭에서 스탠바이 IP 주소를 구성합니다.

스탠바이 디바이스의 이 인터페이스에서 스탠바이 주소를 사용합니다. 스탠바이 IP 주소를 설정하지 않으면 액티브 유닛이 네트워크 테스트를 사용하여 스탠바이 인터페이스를 모니터링할 수 없으며 링크 상태만 추적할 수 있습니다. 사용 중인 각 IP 버전에 대해 스탠바이 주소를 구성합니다.

단계 **4** **Advance Options(**고급 옵션**)** 탭을 클릭하고 MAC 주소를 구성합니다.

시스템은 기본적으로 인터페이스에 대해 NIC(Network Interface Card)에 버닝된 MAC 주소를 사용합니다. 따라서 인터페이스의 모든 하위 인터페이스는 같은 MAC 주소를 사용하므로 하위 인터페이스별로 고유한 주소를 생성할 수 있습니다. 고가용성을 구성하는 경우에는 액티브/스탠바이 MAC 주소도 수동으로 구성하는 것이 좋습니다. MAC 주소를 정의하면 페일오버 시 네트워크에서 일관성을 유지할 수 있습니다.

- **MAC Address(MAC** 주소**)** - H.H.H. 형식의 MAC(Media Access Control) 주소입니다. 여기서 H는 16비트 16진수입니다. 예를 들어 MAC 주소 00-0C-F1-42-4C-DE는 000C.F142.4CDE로 입력합니다. MAC 주소에는 멀티캐스트 비트를 설정해서는 안 됩니다(즉, 왼쪽에서 두 번째 16진수는 홀수일 수 없음).
- **Standby MAC Address(**스탠바이 **MAC** 주소**)** - 고가용성에 사용할 주소입니다. 액티브 유닛이 페일오버되고 스탠바이 유닛이 액티브 상태가 되면, 네트워크 중단을 최소화하기 위해 새 액티브 유닛에서 액티브 MAC 주소를 사용하기 시작하고 기존 액티브 유닛은 스탠바이 주소를 사용합니다.

단계 **5** **OK(**확인**)**를 클릭합니다.

고가용성 컨피그레이션 확인

고가용성 컨피그레이션을 완료한 후에는 디바이스 상태에 두 디바이스가 모두 작동하며 액티브/스탠바이 모드임이 표시됨을 확인합니다.

다음 절차에 따라 고가용성 컨피그레이션이 작동함을 확인할 수 있습니다.

프로시저

단계 **1** 활성 유닛에서 FTP(예)를 사용하여 정상적으로 트래픽을 전달하여 다른 인터페이스의 호스트 간에 파일을 전송하는지 테스트합니다.

최소한 워크스테이션 하나에서 구성된 각 인터페이스에 연결되어 있는 시스템으로의 연결을 테스트합니다.

단계 **2** 다음 중 하나를 수행하여 액티브 유닛이 이제 스탠바이 유닛이 되도록 모드를 전환합니다.

- device manager에서 **Device(**디바이스**)** > **High Availability(**고가용성**)**페이지의 기어 메뉴에 있는 **Switch Mode(**모드 전환**)**를 선택합니다.
- 액티브 유닛의 CLI에 **no failover active**를 입력합니다.

단계 **3** 연결 테스트를 반복하여 고가용성 쌍의 다른 유닛을 통해서도 같은 연결을 설정할 수 있는지 확인합니다.

테스트가 실패하는 경우 다른 유닛의 동일 인터페이스와 같은 네트워크에 유닛 인터페이스를 연결했는지 확인합니다.

High Availability(고가용성) 페이지에서 HA 상태를 확인할 수 있습니다. 유닛의 CLI 또는 CLI 콘솔을 사용해 **show failover** 명령을 입력하여 페일오버 상태를 확인할 수도 있습니다. 또한 **show interface** 명령을 사용하여 실패한 연결 테스트에서 사용한 인터페이스의 인터페이스 컨피그레이션을 확인합니다.

이러한 작업에서 문제가 식별되지 않는 경우 다른 단계를 수행할 수 있습니다. 고가용성 트러블슈팅(페일오버), 248 페이지의 내용을 참조하십시오.

단계 **4** 작업을 완료한 후 모드를 전환하여 원래 액티브였던 유닛을 액티브 상태로 되돌릴 수 있습니다.

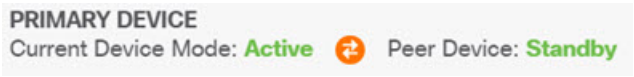
고가용성 관리

Device Summary(디바이스 요약**)** 페이지에서 **High Availability(**고가용성**)** 링크를 클릭하면 고가용성 쌍을 관리할 수 있습니다.

High Availability(고가용성) 페이지에는 다음 항목이 포함되어 있습니다.

- **Role and Mode Status(**역할 및 모드 상태**)** - 왼쪽 상태 영역에는 그룹에서 디바이스가 Primary(기본) 디바이스인지 아니면 Secondary(보조) 디바이스인지 표시됩니다. 모드는 이 디바이스의 상태(액티브/스탠바이) 또는 HA가 일시 중단되었는지 아니면 디바이스가 피어 디바이스 조인을 기다리고 있는지를 나타냅니다. 또한 피어 디바이스의 상태도 표시됩니다. 이 상태는 Active(액티브), Standby(스탠바이), Suspended(일시 중단됨) 또는 Failed(장애 발생) 중 하나일 수 있습니다. 예를 들어 기본 디바이스이자 액티브 디바이스에 로그인하는 경우, 보조 디바이스가 정상 상태

이며 필요 시 페일오버 준비가 되어 있다면 상태는 다음과 같이 표시됩니다. 피어 사이의 아이콘을 클릭하면 디바이스 간의 컨피그레이션 동기화 상태에 대한 정보를 가져올 수 있습니다.



- **Last Failure Reason(**마지막 실패 사유**)** - 액티브 디바이스를 사용할 수 없게 되고 스탠바이 디바이스에 장애 조치를 수행하는 등의 이유로 HA(고가용성) 구성이 실패하는 경우, 마지막 실패 사유가 역할 및 모드 상태에 대한 상태 정보 아래에 표시됩니다. 이 메시지는 장애 조치 기록에서 파생됩니다.
- **Failover History(**페일오버 기록**)** 링크 - 이 링크를 클릭하면 디바이스 쌍에 포함된 디바이스 상태의 세부 기록을 확인할 수 있습니다. 시스템에서는 CLI 콘솔을 열고 **show failover history details** 명령을 실행합니다.
- **Deployment History(**구축 기록**)** 링크 - 이 링크를 클릭하면 구축 작업만 표시하도록 필터링된 이벤트를 포함하는 감사 로그로 이동하게 됩니다.
- 기어 버튼 - 이 버튼을 클릭하면 디바이스에 대해 작업을 수행할 수 있습니다.
  - **Suspend HA(HA** 일시 중단**)/Resume HA(HA** 다시 시작**)** - HA를 일시 중단하면 디바이스가 고가용성 쌍으로 작동하지 않게 되지만 HA 컨피그레이션은 제거되지 않습니다. 나중에 디바이스에서 HA를 다시 시작(다시 활성화)할 수 있습니다. 자세한 내용은 고가용성 일시 중단 또는 다시 시작, 237 페이지를 참조해 주십시오.
  - **Break HA(HA** 해제**)** - HA를 해제하면 두 디바이스에서 모두 고가용성 컨피그레이션이 제거되며 모두 독립형 디바이스로 돌아갑니다. 자세한 내용은 고가용성 해제, 238 페이지를 참조해 주십시오.
  - **Switch Mode(**모드 전환**)** - 모드를 전환하면 작업을 수행하는 디바이스에 따라 액티브 디바이스를 스탠바이 디바이스로, 또는 스탠바이 디바이스를 액티브 디바이스로 강제 설정할 수 있습니다. 자세한 내용은 액티브 및 스탠바이 피어 전환(강제 페일오버), 239 페이지를 참조해 주십시오.
- **High Availability Configuration(**고가용성 컨피그레이션**)** - 이 패널에는 페일오버 쌍의 컨피그레이션이 표시됩니다. **Copy to Clipboard(**클립보드에 복사**)** 버튼을 클릭하여 정보를 클립보드에 로드하고 보조 디바이스의 컨피그레이션에 정보를 붙여넣을 수 있습니다. 또한 기록을 위해 다른 파일로 복사할 수도 있습니다. 이 정보에는 IPsec 암호화 키를 정의했는지 여부가 표시되지 않습니다.

참고 HA용 인터페이스 컨피그레이션은 Interfaces(인터페이스) 페이지(**Device(**디바이스**)** > **Interfaces(**인터페이스**)**)에 반영되지 않습니다. HA 컨피그레이션에서 사용하는 인터페이스는 수정할 수 없습니다.

- **Failover Criteria(**페일오버 기준**)** - 이 패널에는 액티브 유닛에서 장애가 발생하여 스탠바이 유닛이 액티브 유닛으로 설정되어야 하는지 여부를 평가할 때 사용되는 상태 기준을 결정하는 설정이 포함되어 있습니다. 네트워크에 필요한 페일오버 성능을 얻을 수 있도록 이러한 기준을 조

정할 수 있습니다. 자세한 내용은 상태 모니터링을 위한 페일오버 기준 구성, 228 페이지를 참조해 주십시오.

다음 주제에서는 고가용성 컨피그레이션과 관련된 다양한 관리 작업을 설명합니다.

고가용성 일시 중단 또는 다시 시작

고가용성 쌍의 유닛을 일시 중단할 수 있습니다. 이렇게 하면 다음과 같은 경우에 유용합니다.

- 두 유닛이 모두 액티브-액티브인 상태에서 페일오버 링크의 통신을 수정해도 문제가 해결되지 않는 경우.
- 액티브 또는 스탠바이 유닛을 트러블슈팅하고 트러블슈팅 중에는 유닛을 페일오버하지 않으려는 경우.
- 스탠바이 디바이스에 소프트웨어 업그레이드를 설치하는 동안 페일오버를 방지하려는 경우.

고가용성을 일시 중단하면 디바이스 쌍이 더 이상 페일오버 유닛으로 동작하지 않게 됩니다. 현재 액티브 디바이스는 액티브 상태로 유지되어 모든 사용자 연결을 처리합니다. 그러나 페일오버 기준은 더 이상 모니터링되지 않으며 시스템은 현재 의사 스탠바이 디바이스로 페일오버되지 않습니다. 스탠바이 디바이스의 컨피그레이션은 보존되지만 해당 디바이스는 비활성 상태로 유지됩니다.

HA 일시 중단과 해제의 주요 차이점은 일시 중단된 HA 디바이스에서는 고가용성 컨피그레이션이 보존된다는 것입니다. 반면 HA를 해제하면 컨피그레이션이 지워집니다. 따라서 일시 중단된 시스템에서 HA를 다시 시작하는 옵션이 제공됩니다. 그러면 기존 컨피그레이션이 활성화되며 두 디바이스가 다시 페일오버 쌍으로 작동합니다.

액티브 유닛에서 고가용성을 일시 중단하면 액티브 유닛과 스탠바이 유닛 둘 다에서 컨피그레이션이 일시 중단됩니다. 스탠바이 유닛에서 고가용성을 일시 중단하는 경우에는 스탠바이 유닛에서만 고가용성이 일시 중단되며 액티브 유닛은 일시 중단된 유닛으로의 페일오버를 시도하지 않습니다.

Suspended(일시 중단됨) 상태인 유닛만 다시 시작할 수 있습니다. 이 유닛은 피어 유닛과 액티브/스탠바이 상태를 협상합니다.

참고 필요한 경우, **configure high-availability suspend** 명령을 입력하여 CLI에서 HA를 일시 중단할 수 있습니다. HA를 다시 시작하려면 **configure high-availability resume** 명령을 입력합니다.

시작하기 전에

device manager를 통해 고가용성을 일시 중단하면 유닛을 다시 로드하더라도 고가용성은 다시 시작할 때까지 일시 중단된 상태로 유지됩니다. 그러나 CLI를 통해 고가용성을 일시 중단하는 경우에는 일시 중단 상태가 일시적으로만 유지되며, 유닛을 다시 로드하면 고가용성 컨피그레이션이 자동으로 다시 시작되고 피어와의 액티브/스탠바이 상태 협상이 진행됩니다.

스탠바이 유닛에서 고가용성을 일시 중단하는 경우에는 액티브 유닛이 현재 구축 작업을 실행하고 있는지를 확인하십시오. 구축 작업이 진행 중일 때 모드를 전환하면 작업이 실패하고 컨피그레이션 변경 사항이 손실됩니다.

프로시저

단계 **1** 디바이스를 클릭합니다.

단계 **2** 디바이스 요약의 오른쪽에서 **High Availability(**고가용성**)** 링크를 클릭합니다.

단계 **3** 기어 아이콘(⚙)에서 적절한 명령을 선택합니다.

- **Suspend HA(HA** 일시 중단**)** - 작업을 확인하라는 프롬프트가 표시 됩니다. 메시지를 확인하고 **OK(**확인**)**를 클릭합니다. HA 상태에 디바이스가 Suspended(일시 중단됨) 모드임이 표시됩니다.
- **Resume HA(HA** 다시 시작**)** - 작업을 확인하라는 프롬프트가 표시 됩니다. 메시지를 확인하고 **OK(**확인**)**를 클릭합니다. 유닛이 피어와 상태를 협상하고 나면 HA 상태가 정상(액티브 또는 스탠바이) 상태로 돌아갑니다.

고가용성 해제

두 디바이스가 더 이상 고가용성 쌍으로 작동하지 않도록 하려면 HA 컨피그레이션을 해제할 수 있습니다. HA를 해제하면 각 디바이스는 독립형 디바이스가 됩니다. 디바이스의 컨피그레이션은 다음과 같이 변경됩니다.

- 액티브 디바이스의 경우 해제 전의 전체 컨피그레이션이 유지되며 HA 컨피그레이션은 제거됩니다.
- 스탠바이 디바이스의 경우 HA 컨피그레이션과 함께 모든 인터페이스 컨피그레이션이 제거됩니다. 하위 인터페이스는 비활성화되지 않지만 모든 물리적 인터페이스는 비활성화됩니다. 디바이스에 로그인하여 디바이스를 재구성할 수 있도록 관리 인터페이스는 액티브 상태로 유지됩니다.

참고 또는 API Explorer에서 BreakHAStatus API 리소스를 사용하고 **interfaceOption** 속성을 사용함으로써 시스템에서 스탠바이 IP 주소를 사용하여 스탠바이 디바이스의 인터페이스를 재구성하도록 지시할 수 있습니다. 이러한 결과를 원하는 경우 API를 사용해야 합니다. device manager에서는 항상 인터페이스를 비활성화합니다. 시스템은 IP 주소를 재구성하지만 그 외에는 모든 인터페이스 옵션을 다시 구성하지 않으므로, 브레이크 이후에 변경 사항을 구축할 때까지 트래픽이 예상대로 작동하지 않을 수 있습니다.

HA 해제가 실제로 유닛에 미치는 영향은 해제를 수행할 때의 각 유닛의 상태에 따라 달라집니다.

- 유닛이 정상 액티브/스탠바이 상태라면 액티브 유닛에서 HA를 해제합니다. 이렇게 하면 HA 쌍의 두 디바이스에서 모두 HA 컨피그레이션이 제거됩니다. 스탠바이 유닛에서만 HA를 해제하려는 경우에는 해당 유닛에 로그인한 다음 먼저 HA를 일시 중단해야 HA를 해제할 수 있습니다.

- 스탠바이 유닛이 일시 중단 또는 장애 발생 상태인 경우, 액티브 유닛에서 HA를 해제하면 액티브 유닛에서만 HA 컨피그레이션이 제거됩니다. 그러므로 스탠바이 유닛에 로그인하여 해당 유닛에서도 HA를 해제해야 합니다.
- 피어가 아직 HA를 협상하거나 컨피그레이션을 동기화하는 중이라면 HA를 해제할 수 없습니다. 협상 또는 동기화가 완료되거나 시간이 초과될 때까지 기다리십시오. 시스템이 이 상태로 멈춘 것 같다면 HA를 일시 중단한 후에 해제할 수 있습니다.

참고 device manager를 사용할 때는 **configure high-availability disable** 명령을 사용하여 CLI에서 HA를 해제할 수 없습니다.

시작하기 전에

원하는 결과를 얻으려면 디바이스를 정상적인 액티브/스탠바이 상태로 설정하고 액티브 디바이스에서 이 작업을 수행합니다.

프로시저

단계 **1** 디바이스를 클릭합니다.

단계 **2** 디바이스 요약의 오른쪽에서 **High Availability(**고가용성**)** 링크를 클릭합니다.

단계 **3** 기어 아이콘( )에서 **Break HA(HA** 해제**)**를 선택합니다.

단계 **4** 확인 메시지를 읽고 인터페이스를 비활성화하는 옵션을 선택할지 여부를 결정한 다음 **OK(**확인**)**를 클릭합니다.

스탠바이 유닛에서 HA를 해제하는 경우 인터페이스를 비활성화하는 옵션을 선택해야 합니다.

시스템은 이 디바이스와 피어 디바이스(가능한 경우)에서 모두 변경 사항을 즉시 구축합니다. 각 디바이스에서 구축이 완료되고 각 디바이스가 독립 유닛으로 설정되려면 몇 분 정도 걸릴 수 있습니다.

액티브 및 스탠바이 피어 전환(강제 페일오버)

작동 중인 고가용성 쌍(피어 하나는 액티브, 다른 하나는 스탠바이 상태임)의 액티브/스탠바이 모드를 전환할 수 있습니다. 예를 들어 소프트웨어 업그레이드를 설치하는 경우 업그레이드가 사용자 트래픽에 영향을 주지 않도록 액티브 유닛을 스탠바이로 전환할 수 있습니다.

액티브 또는 스탠바이 유닛에서 모드를 전환할 수는 있지만, 다른 유닛의 시점에서 볼 때 피어 유닛이 작동해야 합니다. 즉, 특정 유닛이 일시 중단되거나(먼저 HA를 다시 시작해야 함) 장애가 발생하는 경우에는 모드를 전환할 수 없습니다.

참고 필요한 경우에는 CLI에서 액티브 및 스탠바이 모드 간을 전환할 수 있습니다. 스탠바이 유닛에서 **failover active** 명령을 입력합니다. 액티브 유닛에서 **no failover active** 명령을 입력합니다.

시작하기 전에

모드를 전환하기 전에 액티브 유닛이 구축 작업을 수행하고 있지 않은지 확인합니다. 모드를 전환하기 전에 구축이 완료될 때까지 기다리십시오.

액티브 유닛에 보류 중인 구축되지 않은 변경 사항이 있는 경우 모드를 전환하기 전에 구축하십시오. 이렇게 하지 않으면 새 액티브 유닛에서 구축 작업을 실행하는 경우 변경 사항이 손실됩니다.

프로시저

단계 **1** 디바이스를 클릭합니다.

단계 **2** 디바이스 요약의 오른쪽에서 **High Availability(**고가용성**)** 링크를 클릭합니다.

단계 **3** 기어 아이콘(⚙)에서 **Switch Mode(**모드 전환**)**를 선택합니다.

단계 **4** 확인 메시지를 읽고 **OK(**확인**)**를 클릭합니다.

시스템이 페일오버를 강제로 수행하여 액티브 유닛은 스탠바이 유닛이 되고 스탠바이 유닛은 새 활성 유닛이 됩니다.

페일오버 후 구축되지 않은 컨피그레이션 변경 사항 보존

고가용성 쌍의 유닛에서 컨피그레이션을 변경할 때 액티브 유닛의 컨피그레이션을 수정합니다. 그런 다음, 변경 사항을 구축하면 액티브 유닛과 스탠바이 유닛이 모두 새 컨피그레이션으로 업데이트됩니다. 액티브 유닛이 기본 디바이스인지 아니면 보조 디바이스인지는 중요하지 않습니다.

그러나 구축되지 않은 변경 사항은 유닛 간에 동기화되지 않습니다. 구축되지 않은 변경 사항은 해당 변경을 수행한 유닛에서만 사용할 수 있습니다.

따라서 구축되지 않은 변경 사항이 있을 때 페일오버가 수행되면 새 액티브 유닛에서는 해당 변경 사항을 사용할 수 없습니다. 하지만 이제 스탠바이 상태의 유닛에 변경 사항이 그대로 유지됩니다.

구축되지 않은 변경 사항을 검색하려면 모드를 전환하여 페일오버를 강제로 수행하고 다른 유닛을 액티브 상태로 되돌려야 합니다. 새 액티브 유닛에 로그인하면 구축되지 않은 변경 사항을 사용할 수 있으며 구축할 수 있습니다. 이렇게 하려면 **High Availability(**고가용성**)** 설정 기어 메뉴(⚙)에서 **Switch Modes(**모드 전환**)** 명령을 사용합니다.

다음 사항에 유의하십시오.

- 스탠바이 유닛에 구축되지 않은 변경 사항이 있는 상태에서 액티브 유닛의 변경 사항을 구축하면 스탠바이 유닛의 구축되지 않은 변경 사항은 지워지며 검색할 수 없게 됩니다.

- 스탠바이 유닛이 고가용성 쌍에 조인하면 스탠바이 유닛의 구축되지 않은 변경 사항은 지워집니다. 유닛이 쌍에 조인하거나 다시 조인할 때마다 컨피그레이션이 동기화됩니다.
- 구축되지 않은 변경 사항이 포함된 유닛에서 심각한 장애가 발생하여 해당 유닛을 교체하거나 이미지를 재설치해야 하는 경우에는 구축되지 않은 변경 사항이 영구적으로 손실됩니다.

고가용성 모드에서 라이선스 및 등록 변경

고가용성 쌍의 유닛은 라이선스 및 등록 상태가 동일해야 합니다. 이러한 상태를 변경하려면 다음을 수행해야 합니다.

- 액티브 유닛에서 선택적 라이선스를 활성화하거나 비활성화합니다. 그런 다음, 컨피그레이션을 구축하면 스탠바이 유닛이 필요한 라이선스를 요청하거나 해제합니다. 라이선스를 활성화하는 경우에는 Cisco Smart Software Manager 어카운트에 사용 가능한 라이선스가 충분한지 확인해야 합니다. 그렇지 않으면 각 유닛의 컴플라이언스 상태가 서로 다를 수 있습니다.
- 각 유닛을 개별적으로 등록하거나 등록 취소합니다. 유닛은 둘 다 평가 모드이거나 등록되어 있어야 정상적으로 작동합니다. 유닛을 다른 Cisco Smart Software Manager 어카운트에 등록할 수 있습니다. 단, 이러한 어카운트의 내보내기 제어 기능 설정 상태가 같아야 합니다(둘 다 활성화되어 있거나 비활성화되어 있어야 함). 유닛의 등록 상태가 불일치하는 경우에는 컨피그레이션 변경 사항을 구축할 수 없습니다.

HA IPsec 암호화 키 또는 **HA** 컨피그레이션 수정

액티브 유닛에 로그인하고 변경을 수행한 다음 변경 사항을 구축하면 페일오버 기준을 변경할 수 있습니다.

그러나 페일오버 링크에 사용되는 IPsec 암호 키를 변경해야 하거나, 페일오버 또는 스테이트풀 페일오버 링크의 인터페이스 또는 IP 주소를 변경해야 하는 경우에는 먼저 HA 구성을 해제해야 합니다. 그런 다음 새 암호화 키 또는 페일오버/스테이트풀 페일오버 링크 설정을 사용하여 기본 유닛과 보조 유닛을 다시 구성할 수 있습니다.

장애가 발생한 유닛을 정상 상태로 표시

고가용성 컨피그레이션의 유닛은 정기적 상태 모니터링으로 인해 장애 발생 상태로 표시될 수 있습니다. 해당 유닛이 정상 상태인 경우, 상태 모니터링 요구 사항을 다시 충족했을 때 정상 상태로 되돌려야 합니다. 정상 디바이스가 자주 장애 발생 상태로 표시되는 경우에는 피어 시간 제한을 늘리거나, 중요도가 낮은 인터페이스의 모니터링을 중지하거나, 인터페이스 모니터링 시간 제한을 변경할 수 있습니다.

CLI에서 **failover reset** 명령을 입력하면 장애 발생 상태로 표시된 유닛을 정상 상태로 강제 전환할 수 있습니다. 액티브 유닛에서 명령을 입력하는 것이 좋습니다. 그러면 스탠바이 유닛 상태가 재설정됩니다. **show failover** 또는 **show failover state** 명령을 사용하여 유닛의 페일오버 상태를 표시할 수 있습니다.

장애 발생 유닛을 장애 미발생 상태로 복원해도 해당 유닛이 자동으로 액티브 상태로 설정되지는 않습니다. 복원된 유닛은 페일오버(강제 또는 자연)를 통해 액티브로 전환될 때까지 스탠바이 상태로 유지됩니다.

디바이스 상태를 재설정해도 디바이스가 장애 발생 상태로 표시된 문제가 해결되지는 않습니다. 문제를 해결하지 않거나 모니터링 시간 제한을 늘리지 않으면 디바이스가 장애 발생 상태로 다시 표시될 수 있습니다.

HA 디바이스에서 소프트웨어 업그레이드 설치

네트워크에서 트래픽을 중단하지 않고 고가용성 쌍의 디바이스에서 실행 중인 시스템 소프트웨어를 업그레이드할 수 있습니다. 기본적으로는 액티브 디바이스가 트래픽을 계속 처리하도록 스탠바이 디바이스를 업그레이드합니다. 업그레이드가 완료되고 나면 역할을 전환하여 스탠바이 유닛을 다시 업그레이드합니다.

섀시에서 FXOS 버전도 업데이트해야 하는 경우 다음 절차를 사용하여 설치하기 전에 각 디바이스에 FXOS 업그레이드를 설치합니다. 동일한 기술을 사용합니다. FXOS 업그레이드를 대기 디바이스에 설치하고, 역할을 전환하여 대기 디바이스를 활성 상태로 만든 다음 새 (하위 레벨) 대기 디바이스에 업그레이드를 설치합니다.

고가용성 그룹의 유닛이 서로 다른 소프트웨어 버전을 실행하는 동안에는 페일오버가 불가능합니다. 정상적인 상황에서는 유닛이 동일한 소프트웨어 버전을 실행해야 합니다. 유닛이 서로 다른 버전을 실행해도 되는 경우는 소프트웨어 업그레이드를 설치하는 동안뿐입니다.

이 절차에서는 업그레이드 프로세스를 요약하여 설명합니다. 자세한 내용은 Threat Defense 소프트웨어 업그레이드, 860 페이지를 참조하십시오.

참고 업그레이드 시 시스템에서는 시스템 라이브러리를 업데이트(자동 구축 포함)하는 동안 HA를 일시 중단합니다. 이 프로세스의 마지막 부분을 수행하는 동안에는 SSH 연결에 시스템을 사용할 수 있으므로 업그레이드를 적용한 후 바로 로그인하는 경우 HA가 일시 중단된 상태로 표시될 수 있습니다. 시스템이 자체적으로 스탠바이 준비 상태로 돌아가지 않으며 device manager이 사용 가능해지고 자동 구축이 완료된 후에도 이 문제가 계속되면 HA 페이지로 이동하여 HA를 수동으로 다시 시작하십시오.

시작하기 전에

업그레이드 프로세스를 시작하기 전에 액티브 노드에서 보류 중인 변경 사항을 구축해야 합니다. 디바이스를 업그레이드하는 중에는 컨피그레이션을 변경하거나, 한 디바이스를 업그레이드하고 나서 다른 디바이스를 업그레이드하기 전에 구축을 시작하지 마십시오. 이렇게 하지 않으면 구축에서 장애가 발생하며 변경 사항이 손실될 수 있습니다.

대기 모드를 업그레이드한 후에 액티브 유닛에 변경 사항을 구축해야 하는 경우, 액티브 유닛을 업그레이드하기 전에 두 유닛 모두에 해당 구성 변경을 해야 합니다. 그렇지 않으면 하위 레벨 액티브 유닛을 업그레이드한 후 변경 사항을 잃게 됩니다.

작업 목록을 확인하고 실행 중인 작업이 없는지 확인하십시오. 데이터베이스 업데이트 등 모든 작업이 완료될 때까지 대기했다가 업그레이드를 설치하십시오. 예약된 작업도 모두 확인하십시오. 예약 작업이 업그레이드 작업과 중복되지 않게 하십시오.

업데이트를 수행하기 전에 더 이상 사용되지 않는 애플리케이션이 애플리케이션 필터, 액세스 규칙 또는 SSL 암호 해독 규칙에 없는지 확인하십시오. 이러한 애플리케이션의 이름 뒤에는 "(사용되지 않음)"이라고 적혀 있습니다. 이러한 개체에는 더 이상 사용되지 않는 애플리케이션을 추가할 수 없으며, 후속 VDB 업데이트를 수행하면 이전에 유효했던 애플리케이션이 더 이상 사용되지 않게 될 수 있습니다. 이러한 상황이 발생하면 업그레이드에 실패하고 디바이스는 사용할 수 없는 상태가 됩니다.

Cisco 지원 및 다운로드 사이트에서 https://www.cisco.com/go/ftd-software 업그레이드 파일을 다운로드합니다.

- 제품군 또는 시리즈의 모든 모델에 동일한 업그레이드 패키지를 사용하십시오. 올바른 버전을 찾으려면 모델을 선택하거나 검색한 다음 해당 버전의 소프트웨어 다운로드 페이지로 이동합니다. 파일 유형이 REL.tar인 적절한 업그레이드 파일을 다운로드해야 합니다. 시스템 소프트웨어 패키지 또는 부트 이미지를 다운로드하지 마십시오.
- 업그레이드 파일의 이름을 바꾸지 마십시오. 이름이 바뀐 파일은 유효하지 않은 것으로 간주됩니다.
- 다운그레이드하거나 패치를 제거할 수는 없습니다.
- 업그레이드에 필요한 베이스라인 이미지를 실행 중인지 확인합니다. 호환성 정보는 *Cisco Secure Firewall* 호환성 가이드 http://www.cisco.com/c/en/us/td/docs/security/firepower/compatibility/firepower-compatibility.html을 참조하십시오.
- 새 버전의 릴리스 노트를 확인합니다. 릴리스 노트는 http://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-release-notes-list.html에서 확인할 수 있습니다.

프로시저

단계 **1** 스탠바이 유닛에 로그인하여 업그레이드를 설치합니다.

a) **Device(**디바이스**)**를 선택한 다음 업데이트 요약에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

b) **System Upgrade(**시스템 업그레이드**)** 그룹에서 **Browse(**찾아보기**)** 또는 **Upload Another File(**다른 파일 업로드**)**를 클릭하여 이미지를 업로드합니다.

c) **Install(**설치**)**을 클릭하여 설치 프로세스를 시작합니다.

참고 "you must deploy all uncommitted changes before starting a system upgrade(시스템 업그레이드 시작 전에 커밋되지 않은 모든 변경 사항을 구축해야 합니다)" 오류 메시지가 표시되고 활성 유닛에 커밋되지 않은 변경 사항이 없는 경우 활성 유닛에서 약간의 변경 사항을 생성하고 이를 구축합니다. 그런 다음 변경 사항을 취소 할 수 있습니다. 이 방법으로 문제가 해결되지 않고 권장 사항과 일치하지 않는 버전의 HA 그룹을 실행한 경우에는 역할을 전환하여 대기 유닛을 활성 상태로 만든 다음 HA를 일시 중단해야 할 수 있습니다. 그런 다음 활성/일시 중단된 유닛에서 배포하고 HA를 다시 시작한 다음 역할을 전환하여 활성 유닛을 다시 대기 상태로 설정할 수 있습니다. 그러면 업그레이드가 작동합니다.

설치가 완료될 때까지 기다린 후에 다시 로그인하여 시스템이 정상적으로 작동하는지 확인할 수 있습니다.

참고 고가용성 상태를 확인하는 경우 애플리케이션 동기화 실패가 표시될 수 있습니다. 스탠바이 디바이스가 소프트웨어를 업그레이드하는 동안 액티브 디바이스에서 변경 사항을 구축하는 경우에만 이러한 현상이 발생합니다.

단계 **2** 스탠바이 유닛에서 **Device(**디바이스**)** > **High Availability(**고가용성**)**를 클릭한 다음 기어 메뉴( )에서 **Switch Mode(**모드 전환**)**를 선택합니다.

이 작업을 수행하면 강제 페일오버가 수행되며 로그인되어 있는 유닛이 액티브 유닛으로 설정됩니다. 유닛 상태가 액티브로 변경될 때까지 기다립니다.

계속 진행하기 전에 선택적으로 네트워크를 테스트하여 디바이스가 연결된 네트워크를 통해 트래픽 플로우가 진행됨을 확인할 수 있습니다.

단계 **3** 원래 액티브 유닛이었던 새 스탠바이 유닛에 로그인하여 업그레이드를 설치합니다.

해당 프로세스는 위에서 설명한 것과 같습니다. 소프트웨어 업그레이드는 다른 유닛에서 복사되지 않으므로 업로드해야 합니다.

설치가 완료되면 스탠바이 유닛에 다시 로그인하여 설치가 정상적으로 수행되었는지와 유닛이 정상 액티브/스탠바이 상태로 돌아왔는지를 확인합니다. 이 유닛은 자동으로 액티브 상태로 다시 설정되지 않습니다.

참고 고가용성 상태를 확인하는 경우 애플리케이션 동기화 실패가 표시되지 않습니다. 유닛은 이제 동일한 소프트웨어 버전을 실행하므로 액티브 유닛에서 컨피그레이션 가져오기가 성공해야 합니다. 자동 구축에 실패하거나 디바이스가 달리 스탠바이 준비 상태로 전환되지 않는 경우, 기어 메뉴에서 **Resume HA(HA** 다시 시작**)**를 클릭합니다.

단계 **4** 현재 액티브 유닛에 로그인합니다. 보류 중인 변경 사항이 있는 경우 구축하고 구축이 정상 완료될 때까지 기다립니다.

단계 **5** (선택 사항). 현재 스탠바이 유닛을 다시 액티브 상태로 설정하려면 **Device(**디바이스**)** > **High Availability(**고가용성**)**를 클릭한 다음 두 유닛 중 하나의 기어 메뉴에서 **Switch Mode(**모드 전환**)**를 선택합니다.

예를 들어 이 프로세스를 시작할 때 기본 유닛이 액티브 유닛이었으며 해당 유닛을 다시 액티브 유닛으로 설정하려는 경우 모드를 전환합니다.

고가용성 쌍의 유닛 교체

필요한 경우에는 네트워크 트래픽을 중단하지 않고 고가용성 그룹에서 유닛을 교체할 수 있습니다.

프로시저

단계 **1** 교체할 유닛이 작동 중이라면 피어 유닛으로 페일오버를 수행한 다음, 디바이스 CLI에서 **shutdown** 명령을 사용하여 디바이스를 정상적으로 중단해야 합니다. 해당 유닛이 작동하지 않는 경우에는 피어가 액티브 모드로 작동 중인지 확인합니다.

관리자 권한이 있는 경우 device manager CLI 콘솔을 통해 **shutdown** 명령을 입력할 수도 있습니다.

단계 **2** 네트워크에서 유닛을 제거합니다.

단계 **3** 대체 유닛을 설치하고 인터페이스를 다시 연결합니다.

단계 **4** 대체 유닛에서 디바이스 설정 마법사를 완료합니다.

단계 **5** 피어 유닛에서 High Availability(고가용성) 페이지로 이동하여 컨피그레이션을 클립보드에 복사합니다. 유닛이 기본 유닛인지 아니면 보조 유닛인지를 확인합니다.

보류 중인 변경 사항이 있으면 지금 구축하고 구축이 완료될 때까지 기다린 후에 계속 진행합니다.

단계 **6** 대체 유닛에서 **High Availability(**고가용성**)** 그룹의 **Configure(**구성**)**를 클릭한 다음 피어에서 반대 유닛 유형을 선택합니다. 즉, 피어가 기본 유닛이면 **Secondary(**보조**)**를 선택하고 피어가 보조 유닛이면 **Primary(**기본**)**를 선택합니다.

단계 **7** 피어에서 HA 컨피그레이션을 붙여넣은 다음 IPsec 키(사용하는 경우)를 입력합니다. **Activate HA(HA** 활성화**)**를 클릭합니다.

구축이 완료되면 유닛이 피어에 연결하고 HA 그룹에 조인합니다. 이때 액티브 피어의 컨피그레이션을 가져오며, 교체 유닛은 선택한 옵션에 따라 그룹에서 기본 유닛이나 보조 유닛이 됩니다. 이제 HA가 올바르게 작동하는지 확인할 수 있으며 원하는 경우 모드를 전환해 새 유닛을 액티브 유닛으로 설정할 수 있습니다.

고가용성 모니터링

다음 주제에서는 고가용성을 모니터링하는 방법을 설명합니다.

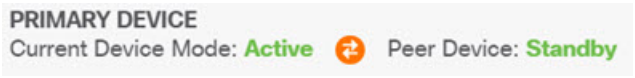
이벤트 뷰어 및 대시보드에는 로그인되어 있는 디바이스와 관련된 데이터만 표시됩니다. 두 디바이스에 대해 병합된 정보는 표시되지 않습니다.

일반 페일오버 상태 및 기록 모니터링

다음과 같은 방법을 사용하여 일반 고가용성 상태 및 기록을 모니터링할 수 있습니다.

- (Device Summary(디바이스 요약)(**Device(**디바이스**)** 클릭)의 High Availability(고가용성) 그룹에 유닛 상태가 표시됩니다.

- (High Availability(고가용성) 페이지(**Device(**디바이스**)** > **High Availability(**고가용성**)** 클릭)에서 두 유닛의 상태를 확인할 수 있습니다. 실패가 발생하면 장애 조치 기록에서 마지막 실패 사유가 표시됩니다. 유닛 사이의 동기화 아이콘을 클릭하면 추가 상태를 확인할 수 있습니다.



- High Availability(고가용성) 페이지에서 상태 옆의 **Failover History(**페일오버 기록**)** 링크를 클릭합니다. 시스템에서는 CLI 콘솔을 열고 **show failover history details** 명령을 실행합니다. CLI 또는 CLI 콘솔에 직접 이 명령을 입력할 수도 있습니다.

CLI 명령

CLI 또는 CLI에서 콘솔에서 다음 명령을 사용할 수 있습니다.

- **show failover**

  유닛의 페일오버 상태에 대한 정보를 표시합니다.

- **show failover history** [**details**]

  이전 페일오버 상태 변경 사항과 상태 변경의 이유가 표시됩니다. 피어 유닛의 페일오버 기록을 표시하려면 **details** 키워드를 추가합니다. 이 정보는 트러블슈팅에 도움이 됩니다.

- **show failover state**

  두 유닛의 페일오버 상태가 표시됩니다. 이 정보에는 유닛의 기본/보조 상태, 유닛의 액티브/스탠바이 상태, 마지막으로 보고된 페일오버의 이유가 포함됩니다.

- **show failover statistics**

  페일오버 인터페이스의 전송(tx) 및 수신(rx) 패킷 수가 표시됩니다. 예를 들어 유닛이 패킷을 전송은 하지만 수신은 하지 않는 것으로 출력에 표시되는 경우 링크에 문제가 있는 것입니다. 예를 들어 전선이 불량이거나, 피어에 잘못된 IP 주소가 구성되어 있거나, 유닛이 페일오버 인터페이스를 다른 서브넷에 연결하는 등의 문제가 있을 수 있습니다.

```
> show failover statistics
        tx:320875
        rx:0
```

- **show failover interface**

페일오버 및 스테이트풀 페일오버 링크의 컨피그레이션이 표시됩니다. 예를 들면 다음과 같습니다.

```
> show failover interface
        interface failover-link GigabitEthernet1/3
                System IP Address: 192.168.10.1 255.255.255.0
                My IP Address    : 192.168.10.1
                Other IP Address : 192.168.10.2
        interface stateful-failover-link GigabitEthernet1/4
                System IP Address: 192.168.11.1 255.255.255.0
                My IP Address    : 192.168.11.1
                Other IP Address : 192.168.11.2
```

- **show monitor-interface**

  고가용성을 모니터링하는 인터페이스에 대한 정보가 표시됩니다. 자세한 내용은 HA 모니터링 인터페이스의 상태 모니터링, 247 페이지를 참조해 주십시오.

- **show running-config failover**

  실행 중인 구성의 페일오버 명령을 표시합니다. 이는 고가용성을 구성하는 명령입니다.

HA 모니터링 인터페이스의 상태 모니터링

특정 인터페이스에 대해 HA 모니터링을 활성화한 경우에는 모니터링하는 인터페이스의 상태를 CLI 또는 CLI 콘솔에서 **show monitor-interface** 명령을 사용해 확인할 수 있습니다.

```
> show monitor-interface
 This host: Primary - Active
  Interface inside (192.168.1.13): Normal (Monitored)
  Interface outside (192.168.2.13): Normal (Monitored)
 Other host: Secondary - Standby Ready
  Interface inside (192.168.1.14): Normal (Monitored)
  Interface outside (192.168.2.14): Normal (Monitored)
```

모니터링한 인터페이스에는 다음과 같은 상태가 표시될 수 있습니다.

- Unknown (Waiting)(알 수 없음(대기 중)) 등의 다른 상태와 결합된 (Waiting)(대기 중) - 인터페이스가 피어 유닛의 해당 인터페이스에서 hello 패킷을 아직 수신하지 않았습니다.
- Unknown - 초기 상태입니다. 이 상태는 상태를 확인할 수 없음을 의미할 수도 있습니다.
- Normal - 인터페이스를 트래픽을 받는 중입니다.
- Testing - 다섯 번의 폴링 시간 동안 인터페이스에 Hello 메시지가 수신되지 않았습니다.
- Link Down - 관리자가 인터페이스 또는 VLAN을 중단했습니다.
- No Link - 인터페이스에 대한 물리적 링크가 중단되었습니다.
- Failed - 인터페이스에 수신된 트래픽이 없지만 피어 인터페이스에는 트래픽이 수신되었습니다.

HA 관련 Syslog 메시지 모니터링

시스템에서는 심각한 상황을 나타내는 우선순위 레벨 2에 해당하는 페일오버와 관련된 여러 syslog 메시지를 생성합니다. 페일오버와 관련된 메시지 ID의 범위는 101xxx, 102xxx, 103xxx, 104xxx, 105xxx, 210xxx, 311xxx, 709xxx, 727xxx입니다. 예를 들어 105032 및 105043은 페일오버 링크의 문제를 나타냅니다. 시스템 로그 메시지에 대한 설명은 *Cisco Threat Defense Syslog* 메시지 가이드 (https://www.cisco.com/c/en/us/td/docs/security/firepower/Syslogs/b_fptd_syslog_guide.html)를 참조하십시오.

참고 페일오버가 실행되는 동안에는 시스템에서 인터페이스를 논리적으로 종료했다가 작동시키므로 syslog 메시지 411001 및 411002가 생성됩니다. 이는 정상적인 동작입니다.

syslog 메시지를 확인하려면 **Device(**디바이스**)** > **Logging Settings(**로깅 설정**)**에서 진단 로깅을 구성해야 합니다. 메시지를 안정적으로 모니터링할 수 있도록 외부 syslog 서버를 설정하십시오.

피어 유닛에서 원격으로 CLI 명령 실행

CLI에서는 피어에 로그인할 필요 없이 failover exec 명령을 사용하여 피어 디바이스에서 show 명령을 입력할 수 있습니다.

failover exec {**active** | **standby** | **mate**} *command*

명령을 실행해야 하는 유닛(액티브 또는 스탠바이)을 지정하거나, 로그인한 유닛 대신 다른 유닛이 응답하도록 하려는 경우에는 **mate**를 입력해야 합니다.

예를 들어 피어 인터페이스의 컨피그레이션과 통계를 확인하려는 경우 다음 명령을 입력할 수 있습니다.

```
> failover exec mate show interface
```

configure 명령은 입력할 수 없습니다. 이 기능은 **show** 명령과 함께 사용할 수 있습니다.

참고 액티브 유닛에 로그인된 경우에는 **failover reload-standby** 명령을 사용하여 스탠바이 유닛을 다시 로드할 수 있습니다.

device manager CLI 콘솔을 통해 이러한 명령을 입력할 수는 없습니다.

고가용성 트러블슈팅(페일오버)

고가용성 그룹의 유닛이 정상적으로 작동하지 않으면 컨피그레이션 트러블슈팅을 위해 다음 단계 수행을 고려하십시오.

액티브 유닛에 피어 유닛이 Failed(장애 발생)로 표시되는 경우 유닛의 장애 발생 상태 트러블슈팅, 251 페이지의 내용을 참조하십시오.

프로시저

단계 **1** 각 디바이스(기본 및 보조)에서 다음 작업을 수행합니다.

- 다른 디바이스의 IP 주소에 ping을 실행하여 페일오버 링크를 확인합니다.
- 별도의 링크를 사용하는 경우에는 다른 디바이스의 IP 주소에 ping을 실행하여 스테이트풀 페일오버 링크를 확인합니다.

ping에 실패하면 각 디바이스의 인터페이스가 같은 네트워크 세그먼트에 연결되어 있는지 확인합니다. 직접 케이블 연결을 사용하는 경우에는 케이블을 확인합니다.

단계 **2** 다음과 같은 일반 확인을 수행합니다.

- 기본 디바이스와 보조 디바이스에서 중복 관리 IP 주소를 확인합니다.
- 유닛에서 중복 페일오버 및 스테이트풀 페일오버 IP 주소를 확인합니다.
- 각 디바이스의 동일 인터페이스 포트가 같은 네트워크 세그먼트에 연결되어 있는지 확인합니다.

단계 **3** 스탠바이 디바이스에서 작업 목록 또는 감사 로그를 확인합니다. 액티브 디바이스에서 모든 구축이 성공하고 나면 "Configuration import from Active node(액티브 노드에서 컨피그레이션 가져오기" 작업이 성공했음이 표시되어야 합니다. 작업에 실패한 경우 페일오버 링크를 확인하고 구축을 다시 시도합니다.

참고 작업 목록에 실패한 구축 작업이 있었던 것으로 표시되면 구축 작업 중에 장애 조치가 발생한 것일 수 있습니다. 구축 작업을 시작할 때는 스탠바이 디바이스가 액티브 유닛이었더라도 작업 중에 장애 조치가 발생하면 구축에 실패합니다. 이 문제를 해결하려면 모드를 전환하여 스탠바이 유닛을 액티브 유닛으로 다시 설정한 다음, 구성 변경 사항을 다시 구축합니다.

단계 **4** **show failover history** 명령을 사용하여 디바이스에서 상태 변경 사항에 대한 세부 정보를 파악합니다.

확인해야 하는 몇 가지 사항은 다음과 같습니다.

- 앱 동기화 실패:

```
12:41:24 UTC Dec 6 2017

App Sync      Disabled      HA state progression failed due to APP SYNC timeout
```

애플리케이션 동기화 단계에서는 액티브 디바이스의 컨피그레이션이 스탠바이 디바이스로 전송됩니다. 애플리케이션 동기화 실패가 발생하면 디바이스는 비활성화 상태가 되며 더 이상 활성화할 수 없습니다.

디바이스가 앱 동기화 문제로 인해 비활성화되는 경우 페일오버 및 스테이트풀 페일오버 링크의 엔드포인트에 대해 디바이스에서 서로 다른 인터페이스를 사용 중인 것일 수 있습니다. 링크의 양 끝에서 같은 포트 번호를 사용해야 합니다.

show failover 명령 실행 시 보조 디바이스가 Pseudo Standby(의사 스탠바이) 상태로 표시되는 경우, 해당 상태는 페일오버 링크에 대해 기본 디바이스에서 구성한 것과 다른 IP 주소를 보조 디바이스에서 구성했음을 나타내는 것일 수 있습니다. 페일오버 링크에 대해 두 디바이스에서 같은 기본/보조 IP 주소를 사용 중인지 확인합니다.

Pseudo Standby(의사 스탠바이) 상태는 기본 디바이스와 보조 디바이스에서 서로 다른 IPsec 키를 구성했음을 나타낼 수도 있습니다.

추가 앱 동기화 문제는 HA 앱 동기화 실패 트러블슈팅, 251 페이지의 내용을 참조하십시오.

- 페일오버가 너무 자주 수행되는 경우(디바이스 상태가 액티브 -> 스탠바이 -> 액티브로 계속 전환됨) 페일오버 링크에 문제가 있는 것일 수 있습니다. 최악의 경우에는 두 유닛이 모두 액티브 상태가 되어 통과 트래픽이 중단될 수도 있습니다. 링크의 양 끝에 대해 ping을 실행하여 연결을 확인합니다. **show arp** 명령을 사용하여 페일오버 IP 주소와 ARP 매핑이 적절한지 확인할 수도 있습니다.

  페일오버 링크가 정상 상태이며 정확하게 구성되어 있는 경우에는 피어 폴링 및 대기 시간/인터페이스 폴링 및 대기 시간을 늘리거나, HA를 모니터링하는 인터페이스 수를 줄이거나, 인터페이스 임계값을 늘리는 방법을 고려해 보십시오.

- 인터페이스 확인으로 인한 오류. Interface Check(인터페이스 확인) 이유에는 장애가 발생한 것으로 간주된 인터페이스 목록이 포함됩니다. 이러한 인터페이스가 정확하게 구성되어 있으며 하드웨어 문제가 없는지 확인합니다. 링크 반대쪽의 스위치 컨피그레이션에 문제가 없는지 확인합니다. 문제가 없는 경우 해당 인터페이스에서 HA 모니터링 비활성화를 고려해 보십시오. 인터페이스 오류 임계값이나 타이밍을 늘리는 옵션도 있습니다.

```
06:17:51 UTC Jan 15 2017

Active     Failed     Interface check

                          This Host:3

                             admin: inside

                             ctx-1: ctx1-1

                             ctx-2: ctx2-1

                          Other Host:0
```

단계 **5** 스탠바이 유닛을 탐지할 수 없으며 페일오버 링크에서 잘못된 LAN 또는 케이블 연결과 같은 구체적인 이유를 찾을 수 없다면 다음 단계를 시도해 보십시오.

a) 스탠바이 유닛에서 CLI에 로그인한 다음, **failover reset** 명령을 입력합니다. 이 명령을 실행하면 유닛이 장애 발생 상태에서 장애 미발생 상태로 변경됩니다. 이제 액티브 디바이스에서 HA 상태를 확인합니다. 이제 스탠바이 피어가 탐지되면 작업이 완료된 것입니다.

b) 액티브 유닛에서 CLI에 로그인한 다음, **failover reset** 명령을 입력합니다. 그러면 액티브 유닛과 스탠바이 유닛 둘 다에서 HA 상태가 재설정됩니다. 디바이스 간의 링크가 재설정되는 것이 가장 좋습니다. HA 상태를 확인하여 아직도 상태가 정확하지 않으면 다음 단계를 계속 진행합니다.

c) 액티브 디바이스의 CLI 또는 device manager에서 먼저 HA를 일시 중단했다가 다시 시작합니다. CLI 명령은 **configure high-availability suspend** 및 **configure high-availability resume**입니다.

d) 이러한 단계에서 장애가 발생하면 스탠바이 디바이스를 **reboot**합니다.

유닛의 장애 발생 상태 트러블슈팅

피어 유닛의 고가용성 상태(**Device(**디바이스**)** 또는 **Device(**디바이스**)** > **High Availability(**고가용성**)** 페이지)에서 유닛이 Failed(장애 발생)로 표시되는 경우, 유닛 A가 액티브 유닛이고 유닛 B가 장애 발생 피어라고 가정할 때 일반적으로 가능한 원인은 다음과 같습니다.

- 유닛 B가 아직 고가용성으로 구성되지 않은 경우(해당 유닛이 아직 독립형 모드임) 유닛 A에 유닛 B가 Failed(장애 발생)로 표시됩니다.
- 유닛 B에서 HA를 일시 중단하면 유닛 A에 유닛 B가 Failed(장애 발생)로 표시됩니다.
- 유닛 B를 리부팅하는 경우 유닛 B의 리부팅이 완료되고 페일오버 링크를 통한 통신이 다시 시작될 때까지 유닛 A에 유닛 B가 Failed(장애 발생)로 표시됩니다.
- 유닛 B에서 애플리케이션 동기화(앱 동기화)에 실패하면 유닛 A에 유닛 B가 Failed(장애 발생)로 표시됩니다. HA 앱 동기화 실패 트러블슈팅, 251 페이지의 내용을 참조하십시오.
- 유닛 B에서 유닛 또는 인터페이스 상태 모니터링에 실패하면 유닛 A에서 유닛 B를 Failed(장애 발생)로 표시합니다. 유닛 B에서 시스템 문제를 확인합니다. 디바이스를 리부팅해 봅니다. 유닛이 전반적으로 정상 상태이면 유닛 또는 인터페이스 상태 모니터링 설정 완화를 고려합니다. **show failover history** 출력에서는 인터페이스 상태 확인 실패에 대한 정보를 제공해야 합니다.
- 두 유닛이 모두 액티브 상태가 되면 각 유닛에는 피어가 Failed(장애 발생)로 표시됩니다. 이러한 상태는 대개 페일오버 링크의 문제를 나타냅니다.

  라이선싱 관련 문제를 표시할 수도 있습니다. 디바이스의 라이선싱은 일관성이 있어야 합니다. 즉 둘 다 평가 모드이거나 등록 상태이어야 합니다. 등록한 경우, 사용하는 스마트 라이선스 계정이 다를 수 있습니다. 하지만 두 계정 모두 내보내기 제어 기능에 대해 동일한 선택을 해야 합니다. 즉 활성화 또는 비활성화 상태여야 합니다. 내보내기 제어 기능에 대한 일관성 없는 설정으로 IPsec 암호화 키를 구성하면 HA를 활성화한 후에 두 디바이스가 모두 활성화됩니다. 이로 인해 지원되는 네트워크 세그먼트에서의 라우팅이 영향을 받게 되고, 이를 복구하기 위해서는 보조 유닛에서 HA를 수동으로 해제해야 합니다.

HA 앱 동기화 실패 트러블슈팅

피어 유닛이 HA 그룹에 조인하지 못하거나 액티브 유닛에서 변경 사항을 구축하는 중에 피어 유닛에서 장애가 발생하는 경우 장애가 발생한 유닛에 로그인하여 **High Availability(**고가용성**)** 페이지로 이동한 다음 **Failover History(**페일오버 기록**)** 링크를 클릭합니다. **show failover history** 출력에서 App

Sync(앱 동기화) 실패를 표시하는 경우에는 유닛이 고가용성 그룹으로 정상 작동할 수 있는지를 시스템에서 확인하는 HA 검증 단계에서 문제가 발생한 것입니다.

이러한 유형의 장애는 다음과 같이 표시될 수 있습니다.

```
==========================================================================
From State                To State                  Reason
==========================================================================
16:19:34 UTC May 9 2018
Not Detected              Disabled                  No Error

17:08:25 UTC May 9 2018
Disabled                  Negotiation               Set by the config command

17:09:10 UTC May 9 2018
Negotiation               Cold Standby              Detected an Active mate

17:09:11 UTC May 9 2018
Cold Standby              App Sync                  Detected an Active mate

17:13:07 UTC May 9 2018
App Sync                  Disabled                  CD App Sync error is
High Availability State Link Interface Mismatch between Primary and Secondary Node
```

문제가 없는 경우에는 From State(시작 상태)가 App Sync(앱 동기화)일 때 "All validation passed(모든 검증 통과)" 메시지를 확인할 수 있으며 노드가 Standby Ready(스탠바이 준비) 상태가 됩니다. 검증 실패 시에는 피어가 Disabled(Failed)(비활성화(장애 발생)) 상태로 전환됩니다. 이 경우 문제를 해결해야 피어가 고가용성 그룹으로 다시 작동합니다. 액티브 유닛을 변경하여 앱 동기화 오류를 해결하는 경우에는 해당 항목을 구축한 다음, 피어 노드가 조인하도록 HA를 다시 시작해야 합니다.

아래에는 장애를 나타내는 메시지와 문제를 해결하는 방법에 대한 설명이 나와 있습니다. 이러한 오류는 노드 조인과 각 후속 구축에서 발생할 수 있습니다. 노드를 조인하는 동안 시스템에서는 액티브 유닛에서 마지막으로 구축된 구성을 확인합니다.

- License registration mode mismatch between Primary and Secondary Node(기본 노드와 보조 노드 간의 라이선스 등록 모드 불일치).

  라이선스 오류는 피어 하나는 등록되어 있는데 다른 피어는 평가 모드임을 나타냅니다. 피어는 둘 다 등록되어 있거나 평가 모드여야 HA 그룹에 조인할 수 있습니다. 등록된 디바이스는 평가 모드로 되돌릴 수 없으므로 **Device(**디바이스**)** > **Smart License(**스마트 라이선스**)** 페이지에서 다른 피어를 등록해야 합니다.

  등록하는 디바이스가 액티브 유닛이면 디바이스 등록 후에 구축을 수행합니다. 구축을 하면 유닛이 강제로 새로 고쳐지며 컨피그레이션이 동기화됩니다. 그러면 보조 유닛이 고가용성 그룹에 올바르게 조인할 수 있게 됩니다.

- License export compliance mismatch between Primary and Secondary Node(기본 노드와 보조 노드 간의 라이선스 내보내기 컴플라이언스 불일치).

  라이선스 컴플라이언스 오류는 두 디바이스가 각기 다른 Cisco Smart Software Manager 어카운트에 등록되어 있는데 내보내기 제어 기능이 어카운트 하나에서는 활성화되어 있고 다른 어카운트에서는 활성화되어 있지 않음을 나타냅니다. 디바이스는 내보내기 제어 기능을 사용하려면

같은 설정(활성화 또는 비활성화)을 사용하는 어카운트에 등록되어 있어야 합니다. **Device(**디바이스**)** > **Smart License(**스마트 라이선스**)** 페이지에서 디바이스 등록을 변경합니다.

- Software version mismatch between Primary and Secondary Node(기본 노드와 보조 노드 간의 소프트웨어 버전 불일치).

  소프트웨어 불일치 오류는 두 피어가 각기 다른 버전의 threat defense 소프트웨어를 실행 중임을 나타냅니다. 소프트웨어 불일치 상태는 소프트웨어 업그레이드를 한 디바이스에 하나씩 설치하는 동안에만 일시적으로 허용됩니다. 그러나 두 피어를 업그레이드하는 시간 사이에는 컨피그레이션 변경 사항을 구축할 수 없습니다. 이 문제를 해결하려면 피어를 업그레이드한 다음 구축을 다시 수행합니다.

- Physical interfaces mismatch between Primary and Secondary Node(기본 노드와 보조 노드 간의 물리적 인터페이스 불일치)

  HA 그룹의 스탠바이 유닛에는 액티브 유닛에 있는 모든 물리적 인터페이스가 있어야 하며, 이러한 인터페이스의 하드웨어 이름 및 유형(예: GigabitEthernet1/1)은 동일해야 합니다. 이 오류는 액티브 유닛에 있는 일부 인터페이스가 스탠바이 유닛에는 없음을 나타냅니다. 액티브 유닛보다 스탠바이 유닛에 더 많은 인터페이스를 포함할 수 있으므로 액티브 상태인 유닛을 전환하거나 다른 피어 유닛을 선택하십시오. 그러나 예를 들어, 한 유닛에서 인터페이스 모듈을 교체 중이며 해당 유닛을 짧은 시간 동안 모듈 없이 실행해야 하는 경우 일치하지 않는 인터페이스는 임시 상태여야 합니다. 일반적인 작업의 경우에는 두 유닛의 인터페이스 수 및 유형이 동일해야 합니다.

- Failover link interface mismatch between Primary and Secondary Node(기본 노드와 보조 노드 간의 페일오버 링크 인터페이스 불일치).

  각 유닛의 네트워크에 페일오버 물리적 인터페이스를 연결할 때는 같은 물리적 인터페이스를 선택해야 합니다. 예를 들어 각 유닛에서 GigabitEthernet1/8을 선택합니다. 이 오류는 각기 다른 인터페이스를 사용했음을 나타냅니다. 오류를 해결하려면 피어 유닛에서 케이블링을 수정합니다.

- Stateful failover link interface mismatch between Primary and Secondary Node(기본 노드와 보조 노드 간의 스테이트풀 페일오버 링크 인터페이스 불일치).

  별도의 스테이트풀 페일오버 링크를 사용하는 경우 각 유닛의 네트워크에 스테이트풀 페일오버 물리적 인터페이스를 연결할 때는 같은 물리적 인터페이스를 선택해야 합니다. 예를 들어 각 유닛에서 GigabitEthernet1/7을 선택합니다. 이 오류는 각기 다른 인터페이스를 사용했음을 나타냅니다. 오류를 해결하려면 피어 유닛에서 케이블링을 수정합니다.

- Failover/Stateful failover link EtherChannel's member interfaces mismatch between Primary and Secondary Node(기본 노드와 보조 노드 간의 장애 조치/스테이트풀 장애 조치 링크 EtherChannel 멤버 인터페이스 불일치)

  장애 조치 또는 스테이트풀 장애 조치 인터페이스에 대해 EtherChannel 인터페이스를 선택하는 경우, EtherChannel은 각 디바이스에서 ID 및 멤버 인터페이스가 동일해야 합니다. 이 오류 메시지를 통해 불일치가 발생한 곳이 장애 조치인지 스테이트풀 장애 조치 링크인지 알 수 있습니다. 이 오류를 해결하려면 동일한 ID를 사용하고 각 디바이스에 동일한 인터페이스를 포함하도록 EtherChannel 인터페이스의 구성을 수정합니다.

- Device Model Number mismatch between Primary and Secondary Node(기본 노드와 보조 노드 간의 디바이스 모델 번호 불일치).

HA 그룹에 조인할 피어는 정확히 동일한 모델의 디바이스여야 합니다. 이 오류는 피어가 동일한 디바이스 모델이 아님을 나타냅니다. HA를 구성하려면 다른 피어를 선택해야 합니다.

- Active and Standby Nodes cannot be on the same chassis.(액티브 노드와 스탠바이 노드는 동일한 섀시에 있을 수 없습니다.)

  동일한 하드웨어 섀시에서 호스팅되는 디바이스를 사용하여 고가용성을 구성할 수는 없습니다. 동일한 섀시의 여러 디바이스를 지원하는 모델에서 고가용성을 구성하는 경우 별도의 하드웨어에 있는 디바이스를 선택해야 합니다.

- Unknown error occurred, please try again(알 수 없는 오류가 발생했습니다. 다시 시도하십시오).

  앱 동기화 중에 문제가 발생했는데 시스템에서 문제를 파악할 수 없는 경우입니다. 컨피그레이션 구축을 다시 시도하십시오.

- Rule package is corrupted. Please update the rule package and try again(규칙 패키지가 손상되었습니다. 규칙 패키지를 업데이트하고 다시 시도하십시오).

  침입 규칙 데이터베이스에 문제가 있습니다. 장애가 발생한 피어에서 **Device(**디바이스**)** > **Updates(**업데이트**)**로 이동한 다음 **Rule(**규칙**)** 그룹에서 **Update Now(**지금 업데이트**)**를 클릭합니다. 업데이트가 완료될 때까지 기다렸다가 변경 사항을 구축합니다. 그리고 나면 액티브 유닛에서 구축을 재시도할 수 있습니다.

- 클라우드 서비스 등록 상태가 기본 노드와 보조 노드 사이에서 일치하지 않습니다.

  노드 중 하나는 Cisco 클라우드에 등록되었지만 다른 노드는 등록되지 않았습니다. 두 노드를 모두 등록해야 하며, 그렇지 않은 경우 등록을 통해 고가용성 그룹을 형성할 수 없습니다. 각 디바이스에서 **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Cloud Services(**클라우드 서비스**)**로 이동하고 두 디바이스 모두 동일한 클라우드 서비스 지역에 등록되어 있는지 확인합니다.

- Active and Standby Nodes cannot have different cloud regions.(액티브 노드와 스탠바이 노드의 클라우드 지역은 같아야 합니다.)

  디바이스가 서로 다른 Cisco Cloud Services 지역에 등록되어 있습니다. 올바른 지역을 확인하고 스마트 라이선싱에서 다른 디바이스를 등록 취소한 다음, 재등록 시 올바른 지역을 선택합니다. 두 디바이스의 지역이 잘못된 경우, 두 디바이스를 모두 등록 취소하고 올바른 지역에 다시 등록합니다.

- Deployment package is corrupted. Please try again(구축 패키지가 손상되었습니다. 다시 시도하십시오).

  이러한 현상은 시스템 오류입니다. 구축을 다시 시도하면 문제가 해결됩니다.

11 장

인터페이스

다음 주제에서는 threat defense 디바이스에서 인터페이스를 컨피그레이션하는 방법을 설명합니다.

Threat Defense 인터페이스에 대한 정보

Threat Defense에는 데이터 인터페이스와 관리/진단 인터페이스가 포함되어 있습니다.

물리적 또는 가상 인터페이스 연결에 케이블을 연결하려면 인터페이스를 구성해야 합니다. 최소한 인터페이스 이름을 지정하고 트래픽을 전달하도록 인터페이스를 활성화해야 합니다. 인터페이스가 브리지 그룹의 멤버인 경우에는 이 작업만 수행하면 됩니다. 비브리지 그룹 멤버의 경우에는 인터페이스에 IP 주소도 지정해야 합니다. 지정된 포트의 단일 실제 인터페이스가 아닌 VLAN 하위 인터페이스를 생성하려는 경우에는 일반적으로 실제 인터페이스가 아닌 하위 인터페이스에 IP 주소를 구성합니다. VLAN 하위 인터페이스를 사용하면 물리적 인터페이스를 각기 다른 VLAN ID로 태그가 지정된 여러 논리적 인터페이스로 분할할 수 있습니다. 이는 스위치의 트렁크 포트에 연결할 때 유용합니다. 패시브 인터페이스에서는 IP 주소를 구성하지 않습니다.

Interfaces(인터페이스**)** 페이지에는 인터페이스 유형의 하위 페이지인 **Interfaces(**인터페이스**)**(물리적 인터페이스용), **Bridge Groups(**브리지 그룹**)**, **Virtual Tunnel Interfaces**, **EtherChannels** 및 **VLAN**(for

the Firepower 1010)이 포함되어 있습니다. device manager이 아니라 FXOS에서만 EtherChannel 파라미터를 수정할 수 있기 때문에 Firepower 4100/9300 EtherChannel은 **Interfaces(**인터페이스**)** 페이지에 나열되며 **EtherChannel** 페이지에는 나열되지 않습니다. 각 페이지에는 사용 가능한 인터페이스, 해당 이름, 주소, 모드 및 상태가 표시됩니다. 인터페이스 목록에서 바로 인터페이스의 상태를 켜기 또는 끄기로 변경할 수 있습니다. 목록에는 컨피그레이션을 기준으로 인터페이스 특성이 표시됩니다. 브리지 그룹, EtherChannel 또는 VLAN 인터페이스의 열기/닫기 화살표를 사용하여 멤버 인터페이스를 확인하십시오. 이러한 인터페이스는 해당 목록에서 단독으로도 표시됩니다. 지원되는 상위 인터페이스의 하위 인터페이스도 확인할 수 있습니다. 이러한 인터페이스가 가상 인터페이스 및 네트워크 어댑터에 매핑되는 방식에 대한 자세한 정보는 VMware 네트워크 어댑터 및 인터페이스가 Threat Defense 물리적 인터페이스에 매핑되는 방식, 16 페이지의 내용을 참조하십시오.

다음 항목에서는 device manager를 통해 인터페이스를 구성할 때의 제한사항과 기타 인터페이스 관리 개념에 관해 설명합니다.

인터페이스 모드

각 인터페이스에 대해 다음과 같은 모드 중 하나를 구성할 수 있습니다.

라우팅 모드

각 Layer 3 라우팅 인터페이스에는 고유한 서브넷의 IP 주소가 필요합니다. 이러한 인터페이스는 보통 스위치, 다른 라우터의 포트 또는 ISP/WAN 게이트웨이에 연결합니다.

수동

패시브 인터페이스는 스위치 SPAN(Switched Port Analyzer) 또는 미러 포트를 사용하여 네트워크를 통과하는 트래픽을 모니터링합니다. SPAN 또는 미러 포트를 사용하면 스위치의 다른 포트에서 트래픽을 복사할 수 있습니다. 이 기능을 사용하면 네트워크 트래픽의 플로우 내에 있지 않더라도 시스템 가시성이 확보됩니다. 수동 구축으로 구성된 시스템에서는 트래픽 차단 또는 형성과 같은 특정 작업을 할 수 없습니다. 패시브 인터페이스는 모든 트래픽을 조건 없이 수신하며 이러한 인터페이스에서 수신된 트래픽은 재전송되지 않습니다.

스위치 포트**(Firepower 1010)**

스위치 포트에서는 하드웨어에서 스위칭 기능을 사용하여 레이어 2에서 트래픽을 전달합니다. 동일한 VLAN의 스위치 포트는 하드웨어 스위칭을 사용하여 서로 통신할 수 있으며 트래픽에는 threat defense 보안 정책이 적용되지 않습니다. 액세스 포트의 경우 태그 없는 트래픽만 허용되며 이러한 포트는 단일 VLAN에 할당할 수 있습니다. 트렁크 포트의 경우 태그 없는 트래픽과 태그 있는 트래픽이 허용되며 둘 이상의 VLAN에 속할 수 있습니다. 관리 인터페이스는 스위치 포트로 구성할 수 없습니다.

BridgeGroupMember

브리지 그룹은 threat defense 디바이스에서 경로 대신 브리징하는 인터페이스 그룹입니다. 모든 인터페이스는 동일한 네트워크에 있습니다. 브리지 그룹은 브리지 네트워크에 IP 주소가 있는 BVI(브리지 가상 인터페이스)로 표시됩니다.

BVI의 이름을 지정하면 라우팅 인터페이스와 BVI를 라우팅할 수 있습니다. 이 경우 BVI는 멤버 인터페이스와 라우팅 인터페이스 간의 게이트웨이 역할을 합니다. BVI의 이름을 지정하지 않으면 브리지 그룹 멤버 인터페이스의 트래픽은 브리지 그룹을 벗어날 수 없습니다. 일반적으로는 인터넷에 멤버 인터페이스를 라우팅할 수 있도록 인터페이스 이름을 지정합니다.

라우팅 모드에서 브리지 그룹을 사용하는 방식 중 하나는 외부 스위치 대신 threat defense 디바이스에서 추가 인터페이스를 사용하는 것입니다. 브리지 그룹 멤버 인터페이스에 엔드포인트를 직접 연결할 수 있습니다. 또한 스위치를 연결하여 BVI와 같은 네트워크에 엔드포인트를 더 추가할 수도 있습니다.

관리/진단 인터페이스

레이블이 관리(threat defense virtual의 경우 Management0/0 가상 인터페이스)인 물리적 포트에는 실제로 두 개의 별도 인터페이스가 연결되어 있습니다.

- 관리 가상 인터페이스 - 시스템 통신에 사용되는 IP 주소입니다. 이 주소는 시스템이 데이터베이스 업데이트를 검색할 때와 스마트 라이선싱에 사용하는 주소입니다. 이 주소에 대해 관리 세션(device manager 및 CLI)을 열 수 있습니다. **System Settings(**시스템 설정**)** > **Management Interface(**관리 인터페이스**)**에서 정의되는 관리 주소를 설정해야 합니다.
- 진단 가상 인터페이스 — 이 인터페이스를 사용하여 외부 시스템 로그 서버로 시스템 로그 메시지를 전송할 수 있습니다. 진단 인터페이스에 대한 IP 주소는 필요한 경우에만 구성하면 됩니다. 즉, 시스템 로그 메시지에 사용하려는 경우 인터페이스를 구성합니다. 이 인터페이스는 **Device(**디바이스**)** > **Interfaces(**인터페이스**)** 페이지에 표시되며 해당 페이지에서 구성할 수 있습니다. 진단 인터페이스는 관리 트래픽만 허용하며 통과 트래픽은 허용하지 않습니다.

(하드웨어 디바이스.) 관리/진단을 구성하는 한 가지 방법은 물리적 포트를 네트워크에 유선으로 연결하지 않는 것입니다. 대신 관리 IP 주소만 구성하고 인터넷에서 업데이트를 가져오는 게이트웨이로 데이터 인터페이스를 사용하도록 해당 주소를 구성합니다. 그런 다음 HTTPS/SSH 트래픽으로 연결되는 내부 인터페이스를 열고(기본값으로 HTTPS는 활성화되어 있음) 내부 IP 주소를 사용하여 device manager를 엽니다(관리 액세스 목록 구성, 810 페이지 참조).

threat defense virtual의 경우 권장되는 컨피그레이션은 Management0/0을 내부 인터페이스와 같은 네트워크에 연결하고 내부 인터페이스를 게이트웨이로 사용하는 것입니다. 진단에 대해 별도의 주소를 구성하지는 마십시오.

별도의 관리 네트워크 구성에 대한 권장 사항

(하드웨어 디바이스.) 별도의 관리 네트워크를 사용하려는 경우 스위치 또는 라우터에 물리적 관리 인터페이스를 유선으로 연결합니다.

threat defense virtual의 경우, 임의의 데이터 인터페이스에서 별도의 네트워크에 Management0/0을 연결합니다. 기본 IP 주소를 계속 사용 중인 경우에는 동일한 서브넷에 있는 관리 IP 주소 또는 내부 인터페이스 IP 주소를 변경해야 합니다.

그런 후에 다음 항목을 구성합니다.

- **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Management Interface(**관리 인터페이스**)**를 선택하고 연결된 네트워크에서 IPv4 또는 IPv6 주소, 또는 두 가지를 모두 설정합니다. 원하는 경우 네트워크의 다른 엔드포인트에 IPv4 주소를 제공하도록 DHCP 서버를 구성할 수 있습니다. 관리 네트워크에 인터넷으로의 경로가 포함된 라우터가 있으면 해당 라우터를 게이트웨이로 사용합니다. 그렇지 않은 경우에는 데이터 인터페이스를 게이트웨이로 사용합니다.

- 인터페이스를 통해 syslog 메시지를 시스템 로그 서버로 보내려는 경우에만 **Device(**디바이스**)** > **Interfaces(**인터페이스**)**에서 진단 인터페이스의 주소를 설정합니다. 그렇지 않은 경우에는 진단용 주소가 필요하지 않으므로 구성하지 마십시오. 구성하는 모든 IP 주소는 관리 IP 주소와 같은 서브넷에 있어야 하며 DHCP 서버 풀에 있을 수는 없습니다. 예를 들어, 관리 주소로 192.168.45.45를 사용하고 DHCP 풀로 192.168.45.46-192.168.45.254를 사용할 경우 192.168.45.1-192.168.45.44 범위에 포함되는 임의의 주소를 사용하여 진단을 구성할 수 있습니다.

보안 영역

각 인터페이스는 단일 보안 영역에 할당할 수 있습니다. 그런 후에 영역을 기준으로 하여 보안 정책을 적용합니다. 예를 들어 내부 인터페이스는 내부 영역에, 외부 인터페이스는 외부 영역에 할당할 수 있습니다. 예를 들어, 트래픽이 내부에서 외부로는 이동하되 외부에서 내부로는 이동할 수 없도록 액세스 제어 정책을 구성할 수 있습니다.

각 영역은 라우팅 또는 패시브 모드가 됩니다. 이 모드는 인터페이스 모드와 직접 관련이 있습니다. 라우팅 및 패시브 인터페이스는 같은 모드의 보안 영역에만 추가할 수 있습니다.

브리지 그룹의 경우 영역에 멤버 인터페이스를 추가할 수는 있지만 BVI(브리지 가상 인터페이스)는 추가할 수 없습니다.

영역에는 관리/진단 인터페이스를 포함하지 않습니다. 영역은 데이터 인터페이스에만 적용됩니다.

개체 페이지에서 보안 영역을 생성할 수 있습니다.

IPv6 주소 지정

IPv6를 위해 2가지 유형의 유니캐스트 주소를 구성할 수 있습니다.

- 전역—전역 주소는 공용 네트워크에서 사용할 수 있는 공용 주소입니다. 브리지 그룹의 경우 각 멤버 인터페이스가 아닌 BVI(브리지 가상 인터페이스)에 대해 글로벌 주소를 구성합니다. 다음 항목은 글로벌 주소로 지정할 수 없습니다.
  - 내부에서 예약된 IPv6 주소: fd00::/56(from=fd00:: to= fd00:0000:0000:00ff:ffff:ffff:ffff:ffff)
  - ::/128 등의 지정되지 않은 주소
  - 루프백 주소(::1/128)
  - 멀티캐스트 주소(ff00::/8)
  - 링크-로컬 주소(fe80::/10)
- 링크-로컬—링크-로컬 주소는 직접 연결된 네트워크에서만 사용할 수 있는 사설 주소입니다. 라우터에서 링크-로컬 주소를 사용하여 패킷을 전달하지 않습니다. 이는 특정 물리적 네트워크 세그먼트에서의 통신에만 사용됩니다. 이러한 주소는 주소 확인 및 네이버 검색과 같은 네트워크 검색 기능이나 주소 컨피그레이션에만 사용할 수 있습니다. 브리지 그룹에서 BVI에 대해 IPv6를 활성화하면 각 브리지 그룹 멤버 인터페이스에 대해 링크-로컬 주소가 자동으로 구성됩니다. 각 인터페이스에는 자체 주소가 있어야 합니다. 링크-로컬 주소는 세그먼트에서만 사용 가능하며 인터페이스 MAC 주소와 연결되기 때문입니다.

적어도 IPv6가 작동하려면 링크-로컬 주소를 구성해야 합니다. 전역 주소를 설정하면 링크-로컬 주소가 인터페이스에서 자동으로 구성되므로 링크-로컬 주소를 특별히 구성하지 않아도 됩니다. 전역 주소를 구성하지 않은 경우 자동으로 또는 수동으로 링크-로컬 주소를 구성해야 합니다.

Auto-MDI/MDIX 기능

RJ-45 인터페이스의 경우 기본 자동 협상 설정에는 Auto-MDI/MDIX 기능도 포함됩니다. Auto-MDI/MDIX는 자동 협상 단계에서 직선 케이블이 감지된 경우 내부 크로스오버를 수행하므로 크로스오버 케이블이 필요 없습니다. 인터페이스에서 Auto-MDI/MDIX를 활성화하려면 속도 또는 양방향을 자동 협상하도록 설정해야 합니다. 속도와 양방향 둘 다 명시적으로 고정 값으로 설정한 경우 두 설정 모두에 대해 자동 협상을 사용 해제하면 Auto-MDI/MDIX도 사용 해제됩니다. 기가비트 인터넷의 경우 속도와 양방향을 1000 및 최대로 설정하면 인터페이스에서 항상 자동 협상이 실행되므로 Auto-MDI/MDIX 기능도 항상 사용 설정된 상태이고 이를 사용 해제할 수 없습니다.

인터페이스에 대한 지침 및 제한 사항

다음 주제에서는 인터페이스의 몇 가지 제한 사항에 대해 다룹니다.

인터페이스 컨피그레이션에 대한 제한 사항

device manager를 사용하여 디바이스를 구성할 때는 인터페이스 구성에 여러 가지 제한이 적용됩니다. 다음 기능 중 어느 것이든 필요한 경우, management center를 사용하여 디바이스를 구성해야 합니다.

- 라우팅 방화벽 모드만 지원됩니다. 투명 방화벽 모드 인터페이스는 구성할 수 없습니다.
- 패시브 인터페이스는 구성할 수 있지만 ERSPAN 인터페이스는 구성할 수 없습니다.
- 인터페이스를 IPS 전용 처리를 위해 인라인(인라인 집합 내) 또는 인라인 탭으로 구성할 수는 없습니다. IPS 전용 모드 인터페이스는 여러 방화벽 검사를 건너뛰며 IPS 보안 정책만 지원합니다. 그에 비해 방화벽 모드 인터페이스는 흐름 유지, IP 및 TCP 레이어 둘 다에서 흐름 상태 추적, IP 조각 모음 및 TCP 표준화와 같은 방화벽 기능에 트래픽을 적용합니다. 보안 정책에 따라 이 방화벽 모드 트래픽에 대해 IPS 기능을 선택 사항으로 구성할 수도 있습니다.
- 이중 인터페이스는 구성할 수 없습니다.
- Firepower 1000, Firepower 2100, Secure Firewall 3100, ISA 3000 모델에 대해 device manager에서 EtherChannel을 구성할 수 있습니다. Firepower 4100/9300에서는 EtherChannel을 지원하지만 사용자는 섀시의 FXOS에서 EtherChannel의 모든 하드웨어 구성을 수행해야 합니다. Firepower 4100/9300 EtherChannel은 단일한 물리적 인터페이스와 함께 device manager **Interfaces(**인터페이스**)** 페이지에 표시됩니다.
- 브리지 그룹은 하나만 추가할 수 있습니다.
- Threat Defense는 라우팅 인터페이스에서만 IPv4 PPPoE를 지원합니다. 고가용성 장치에서는 PPPoE가 지원되지 않습니다.

디바이스 모델별 **VLAN** 하위 인터페이스의 최대 수

디바이스 모델은 구성할 수 있는 VLAN 하위 인터페이스의 최대 수를 제한합니다. 하위 인터페이스는 데이터 인터페이스에서만 구성할 수 있으며 관리 인터페이스에서는 구성할 수 없습니다.

다음 표에서는 각 디바이스 모델의 제한 사항에 대해 설명합니다.

모델	**VLAN** 하위 인터페이스의 최대 수
Firepower 1010	60
Firepower 1120	512
Firepower 1140, 1150	1024
Firepower 2100	1024
Secure Firewall 3100	1024
Firepower 4100	1024
Firepower 9300	1024
Threat Defense Virtual	50
ISA 3000	100

실제 인터페이스 구성

실제 인터페이스를 사용하려면 최소한 인터페이스를 활성화해야 합니다. 일반적으로는 실제 인터페이스의 이름을 지정하고 IP 주소를 구성합니다. VLAN 하위 인터페이스를 생성하려는 경우, 패시브 모드 인터페이스를 구성하는 경우 또는 인터페이스를 브리지 그룹에 추가하려는 경우에는 IP 주소를 구성하지 않습니다. Firepower 4100/9300 EtherChannel은 단일한 물리적 인터페이스와 함께 device manager **Interfaces(**인터페이스**)** 페이지에 표시되며, 이 절차는 그러한 EtherChannel에도 적용됩니다. 사용자는 섀시의 FXOS에서 Firepower 4100/9300 EtherChannel의 모든 하드웨어 구성을 수행해야 합니다.

참고 물리적 인터페이스를 Firepower 1010 스위치 포트로 구성하려면 VLAN 인터페이스 및 스위치 포트 구성(Firepower 1010), 280 페이지의 내용을 참조하십시오.

물리적 인터페이스를 패시브 인터페이스로 구성하려면 패시브 모드로 물리적 인터페이스 구성, 301 페이지의 내용을 참조하십시오.

인터페이스를 비활성화하여 연결된 네트워크에서 전송을 일시적으로 차단할 수 있습니다. 인터페이스 컨피그레이션을 제거할 필요는 없습니다.

프로시저

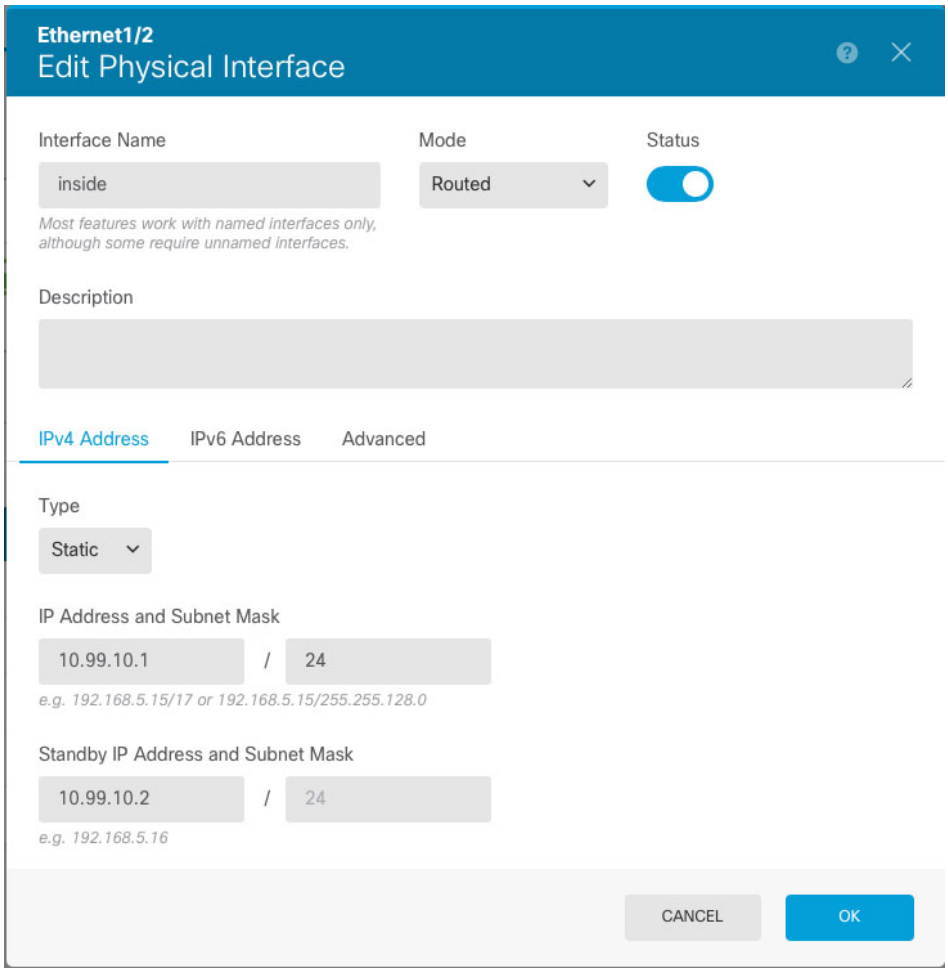
단계 **1** **Device(**디바이스**)**를 클릭한 다음, **Interfaces(**인터페이스**)** 요약의 링크를 클릭합니다.

기본적으로는 **Interfaces(**인터페이스**)** 페이지가 선택됩니다. 인터페이스 목록에는 물리적 인터페이스, 해당 이름, 주소 및 상태가 표시됩니다.

단계 **2** 수정할 실제 인터페이스의 수정 아이콘( )을 클릭합니다.

고가용성 컨피그레이션에서 페일오버 또는 스테이트풀 페일오버 링크로 사용 중인 인터페이스는 수정할 수 없습니다.

단계 **3** 다음을 설정합니다.



a) **Interface Name(**인터페이스 이름**)**을 설정합니다.

인터페이스의 이름을 최대 48자로 설정합니다. 영문자는 소문자로 입력해야 합니다. 예를 들면 **inside** 또는 **outside**와 같이 입력합니다. 이름을 입력하지 않으면 나머지 인터페이스 컨피그레이션이 무시됩니다. 하위 인터페이스를 구성하는 경우가 아니면 인터페이스에는 이름이 있어야 합니다. 참고**:** EtherChannel에 추가할 인터페이스의 이름을 구성하지 마십시오.

참고 이름을 변경하는 경우 보안 영역, syslog 서버 개체, DHCP 서버 정의 등 이전 이름을 사용했던 모든 위치에서 변경 사항이 자동으로 반영됩니다. 그러나 해당 이름을 사용하는 모든 컨피그레이션을 먼저 제거해야 이름을 제거할 수 있습니다. 일반적으로는 정책이나 설정에 대해 이름이 없는 인터페이스를 사용할 수 없기 때문입니다.

b) **Mode(**모드**)**를 선택합니다.

- **Routed(**라우팅**)** - 라우팅 모드 인터페이스는 플로우 유지, IP 및 TCP 레이어 모두에서 플로우 상태 추적, IP 조각 모음, TCP 정규화 등의 모든 방화벽 기능과 방화벽 정책에 트래픽을 적용합니다. 이 모드가 기본 인터페이스 모드입니다.
- **Passive(**패시브**)** - 패시브 인터페이스는 스위치 SPAN 또는 미러 포트를 사용하여 네트워크를 통과하는 트래픽을 모니터링합니다. SPAN 또는 미러 포트를 사용하면 스위치의 다른 포트에서 트래픽을 복사할 수 있습니다. 이 기능을 사용하면 네트워크 트래픽의 플로우 내에 있지 않더라도 시스템 가시성이 확보됩니다. 수동 구축으로 구성된 시스템에서는 트래픽 차단 또는 형성과 같은 특정 작업을 할 수 없습니다. 패시브 인터페이스는 모든 트래픽을 조건 없이 수신하며 이러한 인터페이스에서 수신된 트래픽은 재전송되지 않습니다. 이 모드를 선택하는 경우 이 절차의 나머지 단계를 수행하지 마십시오. 대신 패시브 모드로 물리적 인터페이스 구성, 301 페이지 섹션을 참조하십시오. 패시브 인터페이스에서는 IP 주소를 구성할 수 없습니다.
- **Switch Port(**스위치 포트**)** - (Firepower 1010) 스위치 포트를 사용하면 동일한 VLAN에 있는 포트 간에 하드웨어 스위칭이 가능합니다. 스위칭된 트래픽에는 보안 정책이 적용되지 않습니다. 이 모드를 선택하는 경우 이 절차의 나머지 단계를 수행하지 마십시오. 대신, 다음을 참조하십시오. VLAN 인터페이스 및 스위치 포트 구성(Firepower 1010), 280 페이지

나중에 이 인터페이스를 브리지 그룹에 추가하면 모드가 자동으로 **BridgeGroupMember**로 변경됩니다. 브리지 그룹 멤버 인터페이스에서는 IP 주소를 구성할 수 없습니다.

c) **Status(**상태**)** 슬라이더를 활성화된 설정()으로 지정합니다.

Firepower 4100/9300 디바이스에 있는 인터페이스의 경우 FXOS에서 인터페이스도 활성화해야 합니다.

이 실제 인터페이스에 대해 하위 인터페이스를 구성하려는 경우에는 이러한 작업만 수행하면 될 가능성이 높습니다. **Save(**저장**)**를 클릭하고 VLAN 하위 인터페이스 및 802.1Q 트렁킹 구성, 292 페이지를 계속 진행합니다. 그렇지 않으면 아래 작업을 계속합니다.

참고 하위 인터페이스를 구성할 때도 인터페이스 이름을 지정하고 IP 주소를 제공할 수 있습니다. 이러한 방식은 일반적인 설정은 아니지만, 필요한 경우에는 해당 설정을 구성할 수 있습니다.

d) (선택 사항) **Description(**설명**)**을 설정합니다.

설명은 줄 바꿈 없이 1줄, 최대 200자로 작성할 수 있습니다.

단계 **4** **IPv4 Address(IPv4** 주소**)** 탭을 클릭하고 IPv4 주소를 구성합니다.

Type(유형**)** 필드에서 다음 옵션 중 하나를 선택합니다.

- **DHCP** — 네트워크의 DHCP 서버에서 주소를 가져와야 하는 경우 이 옵션을 선택합니다. 고가용성을 구성하는 경우 이 옵션을 사용할 수 없습니다. 필요에 따라 다음 옵션을 변경합니다.
  - **Route Metric(**경로 메트릭**)** - DHCP 서버에서 기본 경로를 가져오는 경우 확인된 경로까지의 관리 거리(1~255)입니다. 기본값은 1입니다.
  - **Obtain Default Route(**기본 경로 얻기**)** - DHCP 서버에서 기본 경로를 가져올지 여부를 선택합니다. 일반적으로는 이 옵션을 선택합니다(기본값).

- **Static(**고정**)** - 변경되면 안 되는 주소를 할당하려면 이 옵션을 선택합니다. 인터페이스에 연결된 네트워크에 대해 인터페이스의 IP 주소와 서브넷 마스크를 입력합니다. 예를 들어 10.100.10.0/24 네트워크를 연결하는 경우 10.100.10.1/24를 입력할 수 있습니다. 주소가 네트워크에서 이미 사용되고 있지 않은지 확인합니다.

  고가용성을 구성했으며 이 인터페이스에서 HA를 모니터링하는 중이라면 같은 서브넷에 스탠바이 IP 주소도 구성합니다. 스탠바이 디바이스의 이 인터페이스에서 스탠바이 주소를 사용합니다. 스탠바이 IP 주소를 설정하지 않으면 액티브 유닛이 네트워크 테스트를 사용하여 스탠바이 인터페이스를 모니터링할 수 없으며 링크 상태만 추적할 수 있습니다.

  참고 인터페이스에 대해 구성된 DHCP 서버가 있을 경우, 해당 컨피그레이션이 표시됩니다. DHCP 주소 풀을 수정하거나 삭제할 수 있습니다. 인터페이스 IP 주소를 다른 서브넷으로 변경할 경우, 인터페이스 변경 사항을 저장하려면 우선 DHCP 서버를 삭제하거나, 새 서브넷에서 주소 풀을 구성해야 합니다. DHCP 서버 설정, 819 페이지의 내용을 참조하십시오.

- **PPPoE** — PPPoE(Point-to-Point Protocol over Ethernet)를 사용하여 주소를 가져와야 하는 경우 이 옵션을 선택합니다. 인터페이스가 DSL 모뎀이나 케이블 모뎀에 연결되어 있거나 기타 ISP 연결을 사용하고 ISP에서 PPPoE를 사용하여 IP 주소를 제공하는 경우, PPPoE가 필요할 수 있습니다. 고가용성을 구성하는 경우 이 옵션을 사용할 수 없습니다. 다음 값을 설정합니다.
  - **Group Name(**그룹 이름**)** — 이 연결을 나타내는 그룹 이름을 원하는 대로 지정합니다.
  - **PPPoE Username(PPPoE** 사용자 이름**)** — ISP에서 제공한 사용자 이름을 지정합니다.
  - **PPPoE Password(PPPoE** 비밀번호**)** — ISP에서 제공한 비밀번호를 지정합니다.
  - **PPP Authentication(PPP** 인증**) - PAP**, **CHAP**, 또는**MSCHAP**를 선택합니다.

    PAP에서는 인증이 진행되는 동안 일반 텍스트 사용자 이름 및 비밀번호를 전달하므로 안전하지 않습니다. CHAP를 사용하면 클라이언트에서는 서버 챌린지에 대한 응답으로 암호화된 [challenge plus password]와 함께 일반 텍스트로 된 사용자 이름을 반환합니다. CHAP는 PAP보다 안전하지만 데이터가 암호화되지 않습니다. MSCHAP는 CHAP와 유사하지만, CHAP의 일반 텍스트로 비밀번호와 달리 서버에서 암호화된 비밀번호만 저장하고 비교하므로 훨씬 안전합니다. MSCHAP에서도 MPPE를 통해 데이터 암호화용 키를 생성합니다.
  - **PPPoE Learned Route Metric(PPPoE** 학습된 경로 메트릭**)** — 학습된 경로에 관리 거리를 할당합니다. 유효한 값은 1 ~ 255입니다. 파악된 경로의 기본 관리 거리는 1입니다.
  - **Obtain Default Route from PPPoE(PPPoE**에서 기본 경로 가져오기**)** — PPPoE 서버에서 기본 경로를 가져오려면 이 확인란을 선택합니다.

- **IP Address Type(IP** 주소 유형**)** — PPPoE 서버에서 IP 주소를 가져오려면 **Dynamic(**동적**)**을 선택합니다. 또는 ISP에서 정적 IP 주소를 할당한 경우 **Static(**정적**)**을 선택할 수 있습니다.

단계 **5** (선택 사항). **IPv6 Address(IPv6** 주소**)** 탭을 클릭하고 IPv6 주소를 구성합니다.

- **Sate(**상태**)** - 글로벌 어드레스를 구성하지 않는 경우 IPv6 처리를 활성화하고 링크-로컬 주소를 자동으로 구성하려면 **Enabled(**활성화됨**)**를 선택합니다. 링크 로컬 주소는 인터페이스 MAC 주소(수정된 EUI-64 형식)를 기반으로 생성됩니다.

  참고 IPv6를 비활성화해도 명시적 IPv6 주소로 구성되었거나 자동 컨피그레이션용으로 활성화된 인터페이스에서 IPv6 처리가 비활성화되지는 않습니다.

- **Address Auto Configuration(**주소 자동 컨피그레이션**)** - 주소를 자동으로 구성하려면 이 옵션을 선택합니다. IPv6 스테이트리스 자동 컨피그레이션에서는 디바이스가 있는 링크에 IPv6 서비스를 제공하도록 구성된 라우터가 있는 경우에만 글로벌 IPv6 주소를 생성합니다. 이러한 서비스에는 링크에서 사용할 IPv6 글로벌 접두사 알림이 포함됩니다. 링크에서 IPv6 라우팅 서비스를 사용할 수 없는 경우에는 링크-로컬 IPv6 주소만 제공됩니다. 디바이스의 직접 네트워크 링크 외부에서는 이 주소에 액세스할 수 없습니다. 링크 로컬 주소는 수정된 EUI-64 인터페이스 ID를 기반으로 합니다.

  RFC 4862에서는 스테이트리스 자동 컨피그레이션에 대해 구성한 호스트에서 라우터 알림 메시지를 전송하지 않도록 지정하지만, 이 경우에는 threat defense 디바이스에서 라우터 알림 메시지를 전송합니다. 메시지를 표시하지 않고 RFC를 준수하려면 **RA** 표시 안 함을 선택합니다.

- **Static Address/Prefix(**고정 주소/접두사**)** - 스테이트리스 자동 컨피그레이션을 사용하지 않는 경우 전체 고정 글로벌 IPv6 주소와 네트워크 접두사를 입력합니다. 예를 들어, 2001:0DB8::BA98:0:3210/48와 같이 입력합니다. IPv6 주소 지정에 대한 자세한 내용은 IPv6 주소 지정, 258 페이지를 참조하십시오.

  주소를 링크 로컬 전용으로 사용하려는 경우 링크-로컬 옵션을 선택합니다. 로컬 네트워크 외부에서는 링크 로컬 주소에 액세스할 수 없습니다. 브리지 그룹 인터페이스에서는 링크-로컬 주소를 구성할 수 없습니다.

  참고 링크-로컬 주소는 FE8, FE9, FEA 또는 FEB로 시작해야 합니다(예: fe80::20d:88ff:feee:6a82). Modified EUI-64 형식으로 링크-로컬 주소를 자동으로 지정하는 것이 좋습니다. 만약 다른 디바이스에서 Modified EUI-64 형식을 강제 적용하는 경우 수동으로 지정된 링크-로컬 주소 때문에 패킷이 폐기될 수 있습니다.

- **Standby IP Address(**스탠바이 **IP** 주소**)** - 고가용성을 구성하는 경우 이 인터페이스에서 HA를 모니터링하는 중이라면 같은 서브넷에 스탠바이 IPv6 주소도 구성합니다. 스탠바이 디바이스의 이 인터페이스에서 스탠바이 주소를 사용합니다. 스탠바이 IP 주소를 설정하지 않으면 액티브 유닛이 네트워크 테스트를 사용하여 스탠바이 인터페이스를 모니터링할 수 없으며 링크 상태만 추적할 수 있습니다.

- **Suppress RA(RA** 표시 안 함**)** - 라우터 알림을 표시하지 않을지를 선택합니다. threat defense는 인접 디바이스가 기본 라우터 주소를 동적으로 학습할 수 있도록 라우터 알림에 참여할 수 있습니다. 기본적으로 라우터 알림 메시지(ICMPv6 유형 134)는 IPv6가 구성된 각 인터페이스에 주기적으로 전송됩니다.

라우터 광고는 라우터 요청 메시지에 대한 응답으로도 보내집니다(ICMPv6 Type 133). 예정된 다음 라우터 광고 메시지를 기다릴 필요 없이 호스트가 즉시 자동 구성을 할 수 있도록 시스템 시동 시 라우터 요청 메시지가 전송됩니다.

threat defense 디바이스에서 IPv6 접두사를 제공하지 않도록 하려는 인터페이스(예: 외부 인터페이스)에서는 이러한 메시지를 표시하지 않을 수 있습니다.

단계 **6** (선택 사항). 고급 옵션 구성, 304 페이지에 전달하는 고성능 고속 어플라이언스입니다.

고급 설정에는 대부분의 네트워크에 적합한 기본값이 있습니다. 네트워크 문제를 해결하는 경우에만 이러한 기본값을 수정하십시오.

단계 **7** **OK(**확인**)**를 클릭합니다.

다음에 수행할 작업

- 적절한 보안 영역에 인터페이스를 추가합니다. 보안 영역 구성, 152 페이지의 내용을 참조하십시오.
- 동적 DNS 서비스 제공자에 FQDN(Fully Qualified Domain Name)을 등록하고 DNS 서버가 IPv4 및 IPv6 인터페이스 주소로 업데이트되도록 DDNS를 설정합니다. 동적 DNS 구성, 823 페이지의 내용을 참조하십시오.

브리지 그룹 구성

브리지 그룹은 하나 이상의 인터페이스를 그룹화하는 가상 인터페이스입니다. 인터페이스를 그룹화하는 주요 이유는 스위치 인터페이스 그룹을 생성하기 위해서입니다. 따라서 브리지 그룹에 포함된 인터페이스에 워크스테이션 또는 기타 엔드포인트 디바이스를 직접 연결할 수 있습니다. 이러한 워크스테이션이나 디바이스는 별도의 물리적 스위치를 통해 연결할 필요는 없지만, 브리지 그룹 멤버에 스위치를 연결할 수도 있습니다.

그룹 멤버에는 IP 주소가 없습니다. 대신 모든 멤버 인터페이스는 BVI(브리지 가상 인터페이스)의 IP 주소를 공유합니다. BVI에서 IPv6를 활성화하는 경우 멤버 인터페이스에는 고유한 링크-로컬 주소가 자동으로 할당됩니다.

멤버 인터페이스는 개별적으로 활성화 및 비활성화합니다. 그러므로 사용하지 않는 인터페이스는 브리지 그룹에서 제거할 필요 없이 비활성화할 수 있습니다. 브리지 그룹 자체는 항상 활성화됩니다.

일반적으로는 BVI(브리지 그룹 인터페이스)에서 DHCP 서버를 구성합니다. 이 서버는 멤버 인터페이스를 통해 연결된 모든 엔드포인트에 대해 IP 주소를 제공합니다. 그러나 원하는 경우에는 멤버 인터페이스에 연결된 엔드포인트에서 고정 주소를 구성할 수 있습니다. 브리지 그룹 내의 모든 엔드포인트에는 브리지 그룹 IP 주소와 같은 서브넷의 IP 주소가 있어야 합니다.

지침 및 제한 사항

- 브리지 그룹을 한 개 추가할 수 있습니다.

- Device Manager 정의 EtherChannel은 브리지 그룹 멤버로 지원되지 않습니다. Firepower 4100/9300의 EtherChannel은 브리지 그룹 멤버가 될 수 있습니다.
- Firepower 2100 Series 또는 threat defense virtual 디바이스에서는 브리지 그룹을 구성할 수 없습니다.
- Firepower 1010의 경우, 동일한 브리지 그룹에서 논리적 VLAN 인터페이스와 물리적 방화벽 인터페이스를 혼합할 수 없습니다.
- ISA 3000는 브리지 그룹 BVI1으로 사전 구성된 상태로 제공됩니다(이름은 지정되어 있지 않으며, 이는 라우팅에 참여하지 않음을 의미). BVI1에는 모든 데이터 인터페이스(GigabitEthernet1/1(outside1), GigabitEthernet1/2(inside1), GigabitEthernet1/3(outside2), GigabitEthernet1/4(inside2))가 포함되어 있습니다. 네트워크와 일치하도록 BVI1 IP 주소를 설정해야 합니다.

시작하기 전에

브리지 그룹의 멤버로 추가할 인터페이스를 구성합니다. 구체적으로 각 멤버 인터페이스는 다음 요건을 충족해야 합니다.

- 인터페이스에 이름이 있어야 합니다.
- 인터페이스에 대해 IPv4 또는 IPv6 주소(고정 주소 또는 DHCP를 통해 제공된 주소)가 정의되어 있으면 안 됩니다. 현재 사용 중인 인터페이스에서 주소를 제거해야 하는 경우에는 주소가 있는 인터페이스를 사용하는 인터페이스의 다른 컨피그레이션(예: 정적 경로, DHCP 서버 또는 NAT 규칙)도 제거해야 할 수 있습니다.
- 인터페이스가 보안 영역에 있는 경우 보안 영역에서 인터페이스를 제거하고 인터페이스에 대한 NAT 규칙을 삭제해야 브리지 그룹에 인터페이스를 추가할 수 있습니다.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭하고 **Interfaces(**인터페이스**)** 요약의 링크를 클릭한 다음, **Bridge Groups(**브리지 그룹**)**를 클릭합니다.

브리지 그룹 목록에는 기존 브리지 그룹이 표시됩니다. 각 브리지 그룹의 멤버 인터페이스를 보려면 열기/닫기 화살표를 클릭합니다. 멤버 인터페이스는 **Interfaces(**인터페이스**)** 또는 **VLAN** 페이지에 개별적으로도 표시됩니다.

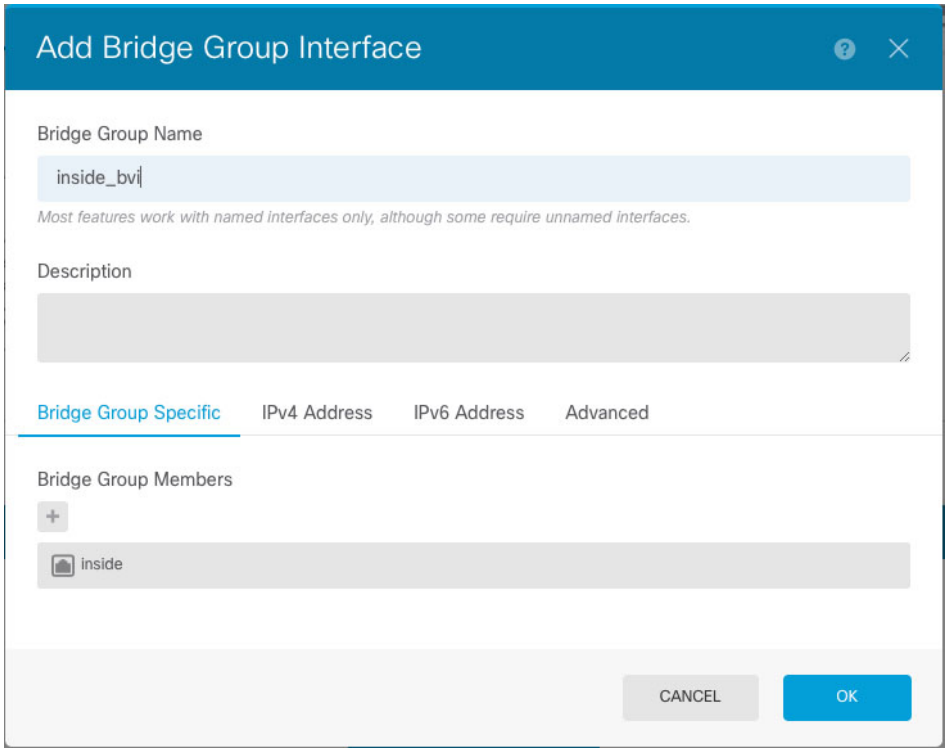
단계 **2** 다음 중 하나를 수행합니다.

- BVI1 브리지 그룹의 수정 아이콘( )을 클릭합니다.
- **Create Bridge Group(**브리지 그룹 생성**)** 또는 더하기 아이콘(+)을 클릭하여 새 그룹을 생성합니다.

  참고 단일 브리지 그룹을 생성할 수 있습니다. 브리지 그룹을 이미 정의한 경우에는 새 그룹을 생성하는 대신 해당 그룹을 수정해야 합니다. 새 브리지 그룹을 생성해야 하는 경우 먼저 기존 브리지 그룹을 삭제해야 합니다.

- 더 이상 필요하지 않은 브리지 그룹의 삭제 아이콘( )을 클릭합니다. 브리지 그룹을 삭제하면 해당 멤버는 표준 라우팅 인터페이스가 되며 모든 NAT 규칙 또는 보안 영역 멤버십은 유지됩니다. 인터페이스를 수정하여 IP 주소를 지정할 수 있습니다. 새 브리지 그룹에 인터페이스를 추가하려는 경우에는 먼저 NAT 규칙을 제거하고 인터페이스를 해당 보안 영역에서 제거해야 합니다.

단계 **3** 다음을 구성합니다.



a) (선택 사항) **Interface Name(**인터페이스 이름**)**을 설정합니다.

브리지 그룹의 이름을 최대 48자로 설정합니다. 영문자는 소문자로 입력해야 합니다. 예를 들면 **inside** 또는 **outside**와 같이 입력합니다. 이 BVI가 해당 인터페이스와 다른 명명된 인터페이스 간의 라우팅에 참여하게 만들려면 이름을 설정합니다.

참고 이름을 변경하는 경우 보안 영역, syslog 서버 개체, DHCP 서버 정의 등 이전 이름을 사용했던 모든 위치에서 변경 사항이 자동으로 반영됩니다. 그러나 해당 이름을 사용하는 모든 컨피그레이션을 먼저 제거해야 이름을 제거할 수 있습니다. 일반적으로는 정책이나 설정에 대해 이름이 없는 인터페이스를 사용할 수 없기 때문입니다.

b) (선택 사항) **Description(**설명**)**을 설정합니다.

설명은 줄 바꿈 없이 1줄, 최대 200자로 작성할 수 있습니다.

c) **Bridge Group Members(**브리지 그룹 멤버**)** 목록을 수정합니다.

단일 브리지 그룹에는 인터페이스 또는 하위 인터페이스를 64개까지 추가할 수 있습니다.

- 인터페이스 추가 — 더하기 아이콘(+)을 클릭하고 하나 이상의 인터페이스를 클릭한 다음, **OK(**확인**)**를 클릭합니다.
- 인터페이스 제거 — 인터페이스 위에 마우스를 올려놓고 오른쪽의 **x**를 클릭합니다.

단계 **4** **IPv4 Address(IPv4** 주소**)** 탭을 클릭하고 IPv4 주소를 구성합니다.

Type(유형**)** 필드에서 다음 옵션 중 하나를 선택합니다.

- **Static(**고정**)** - 변경되면 안 되는 주소를 할당하려면 이 옵션을 선택합니다. 브리지 그룹의 IP 주소와 서브넷 마스크를 입력합니다. 연결되는 모든 엔드포인트는 이 네트워크에 포함됩니다. 주소가 네트워크에서 이미 사용되고 있지 않은지 확인합니다.

  고가용성을 구성했으며 이 인터페이스에서 HA를 모니터링하는 중이라면 같은 서브넷에 스탠바이 IP 주소도 구성합니다. 스탠바이 디바이스의 이 인터페이스에서 스탠바이 주소를 사용합니다. 스탠바이 IP 주소를 설정하지 않으면 액티브 유닛이 네트워크 테스트를 사용하여 스탠바이 인터페이스를 모니터링할 수 없으며 링크 상태만 추적할 수 있습니다.

  참고 인터페이스에 대해 구성된 DHCP 서버가 있을 경우, 해당 컨피그레이션이 표시됩니다. DHCP 주소 풀을 수정하거나 삭제할 수 있습니다. 인터페이스 IP 주소를 다른 서브넷으로 변경할 경우, 인터페이스 변경 사항을 저장하려면 우선 DHCP 서버를 삭제하거나, 새 서브넷에서 주소 풀을 구성해야 합니다. DHCP 서버 설정, 819 페이지의 내용을 참조하십시오.

- **Dynamic(**동적**)**(DHCP) - 네트워크의 DHCP 서버에서 주소를 가져와야 하는 경우 이 옵션을 선택합니다. 이 옵션은 브리지 그룹에 대해 일반적으로 구성하는 항목은 아니지만 필요한 경우 구성할 수 있습니다. 고가용성을 구성하는 경우 이 옵션을 사용할 수 없습니다.필요에 따라 다음 옵션을 변경합니다.
  - **Route Metric(**경로 메트릭**)** - DHCP 서버에서 기본 경로를 가져오는 경우 확인된 경로까지의 관리 거리(1~255)입니다. 기본값은 1입니다.
  - **Obtain Default Route(**기본 경로 얻기**)** - DHCP 서버에서 기본 경로를 가져올지 여부를 선택합니다. 일반적으로는 이 옵션을 선택합니다(기본값).

단계 **5** (선택 사항). **IPv6 Address(IPv6** 주소**)** 탭을 클릭하고 IPv6 주소를 구성합니다.

- **Sate(**상태**)** - 글로벌 어드레스를 구성하지 않는 경우 IPv6 처리를 활성화하고 링크-로컬 주소를 자동으로 구성하려면 **Enabled(**활성화됨**)**를 선택합니다. 링크 로컬 주소는 인터페이스 MAC 주소(수정된 EUI-64 형식)를 기반으로 생성됩니다.

  참고 IPv6를 비활성화해도 명시적 IPv6 주소로 구성되었거나 자동 컨피그레이션용으로 활성화된 인터페이스에서 IPv6 처리가 비활성화되지는 않습니다.

- **Static Address/Prefix(**고정 주소/접두사**)** - 스테이트리스 자동 컨피그레이션을 사용하지 않는 경우 전체 고정 글로벌 IPv6 주소와 네트워크 접두사를 입력합니다. 예를 들어, 2001:0DB8::BA98:0:3210/48와 같이 입력합니다. IPv6 주소 지정에 대한 자세한 내용은 IPv6 주소 지정, 258 페이지를 참조하십시오.

주소를 링크 로컬 전용으로 사용하려는 경우 링크-로컬 옵션을 선택합니다. 로컬 네트워크 외부에서는 링크 로컬 주소에 액세스할 수 없습니다. 브리지 그룹 인터페이스에서는 링크-로컬 주소를 구성할 수 없습니다.

참고 링크-로컬 주소는 FE8, FE9, FEA 또는 FEB로 시작해야 합니다(예: fe80::20d:88ff:feee:6a82). Modified EUI-64 형식으로 링크-로컬 주소를 자동으로 지정하는 것이 좋습니다. 만약 다른 디바이스에서 Modified EUI-64 형식을 강제 적용하는 경우 수동으로 지정된 링크-로컬 주소 때문에 패킷이 폐기될 수 있습니다.

- **Standby IP Address(**스탠바이 **IP** 주소**)** - 고가용성을 구성하는 경우 이 인터페이스에서 HA를 모니터링하는 중이라면 같은 서브넷에 스탠바이 IPv6 주소도 구성합니다. 스탠바이 디바이스의 이 인터페이스에서 스탠바이 주소를 사용합니다. 스탠바이 IP 주소를 설정하지 않으면 액티브 유닛이 네트워크 테스트를 사용하여 스탠바이 인터페이스를 모니터링할 수 없으며 링크 상태만 추적할 수 있습니다.
- **Suppress RA(RA** 표시 안 함**)** - 라우터 알림을 표시하지 않을지를 선택합니다. 위협 방지 디바이스는 인접 디바이스가 기본 라우터 주소를 동적으로 학습할 수 있도록 라우터 알림에 참여할 수 있습니다. 기본적으로 라우터 알림 메시지(ICMPv6 유형 134)는 IPv6가 구성된 각 인터페이스에 주기적으로 전송됩니다.

  라우터 광고는 라우터 요청 메시지에 대한 응답으로도 보내집니다(ICMPv6 Type 133). 예정된 다음 라우터 광고 메시지를 기다릴 필요 없이 호스트가 즉시 자동 구성을 할 수 있도록 시스템 시동 시 라우터 요청 메시지가 전송됩니다.

  threat defense 디바이스에서 IPv6 접두사를 제공하지 않도록 하려는 인터페이스(예: 외부 인터페이스)에서는 이러한 메시지를 표시하지 않을 수 있습니다.

단계 **6** (선택 사항). 고급 옵션 구성, 304 페이지에 전달하는 고성능 고속 어플라이언스입니다.

대부분의 고급 옵션은 브리지 그룹 멤버 인터페이스에 대해 구성하지만 브리지 그룹 인터페이스에 대해 사용할 수 있는 옵션도 있습니다.

고급 설정에는 대부분의 네트워크에 적합한 기본값이 있습니다. 네트워크 문제를 해결하는 경우에만 이러한 기본값을 수정하십시오.

단계 **7** **OK(**확인**)**를 클릭합니다.

다음에 수행할 작업

- 사용하려는 모든 멤버 인터페이스가 활성화되어 있는지 확인합니다.
- 브리지 그룹에 대해 DHCP 서버를 구성합니다. DHCP 서버 설정, 819 페이지를 참조하십시오.
- 적절한 보안 영역에 멤버 인터페이스를 추가합니다. 보안 영역 구성, 152 페이지를 참조하십시오.
- ID, NAT, 액세스 등의 정책이 브리지 그룹 및 멤버 인터페이스에 필요한 서비스를 제공하는지 확인합니다.

EtherChannel 구성

이 섹션에서는 EtherChannel 및 이를 구성하는 방법에 대해 설명합니다.

참고 device manager의 EtherChannels을 다음 모델에 추가할 수 있습니다.

- Firepower 1000
- Firepower 2100
- Secure Firewall 3100
- ISA 3000

Firepower 4100/9300에서는 EtherChannel을 지원하지만 사용자는 섀시의 FXOS에서 EtherChannel의 모든 하드웨어 구성을 수행해야 합니다. Firepower 4100/9300 EtherChannel은 단일한 물리적 인터페이스와 함께 device manager 인터페이스 페이지에 표시됩니다. 또한 threat defense virtual와 같은 다른 모델에서는 device manager에서 EtherChannel을 설정할 수 없습니다.

EtherChannel 정보

802.3ad EtherChannel은 개별 이더넷 링크(채널 그룹)의 번들로 구성된 논리적 인터페이스(일명 포트 채널 인터페이스)이므로, 단일 네트워크의 대역폭을 늘리게 됩니다. 포트 채널 인터페이스는 인터페이스 관련 기능을 구성할 경우 물리적 인터페이스와 동일한 방식으로 사용됩니다.

모델에서 지원하는 인터페이스의 수에 따라 최대 48개의 EtherChannel을 구성할 수 있습니다.

채널 그룹 인터페이스

각 채널 그룹에는 최대 8개의 액티브 인터페이스를 포함할 수 있습니다.

채널 그룹의 모든 인터페이스는 유형과 속도가 같아야 합니다. 채널 그룹에 추가된 첫 번째 인터페이스에서는 올바른 유형과 속도를 결정합니다.

EtherChannel에서는 채널에서 사용 가능한 모든 활성 인터페이스 전반의 트래픽을 취합합니다. 소스 또는 목적지 MAC 주소, IP 주소, TCP 및 UDP 포트 번호, VLAN 번호를 기준으로 전용 해시 알고리즘을 사용하여 인터페이스를 선택합니다.

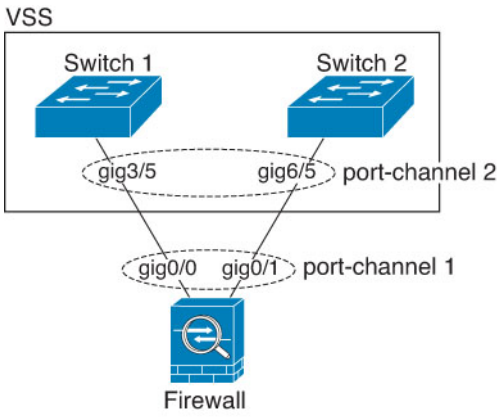
다른 디바이스에서 EtherChannel에 연결

threat defense EtherChannel을 연결하는 디바이스에서는 802.3ad EtherChannel도 지원해야 합니다. 예를 들어 Catalyst 6500 스위치 또는 Cisco Nexus 7000에 연결할 수 있어야 합니다.

스위치가 VSS(Virtual Switching System) 또는 vPC(Virtual Port Channel)의 일부인 경우, 동일한 EtherChannel 내에서 threat defense 인터페이스를 연결하여 VSS/vPC에서 스위치를 분리할 수 있습니

다. 이러한 별도의 스위치는 단일 스위치 역할을 하므로, 스위치 인터페이스는 동일한 EtherChannel 포트 채널 인터페이스의 멤버입니다.

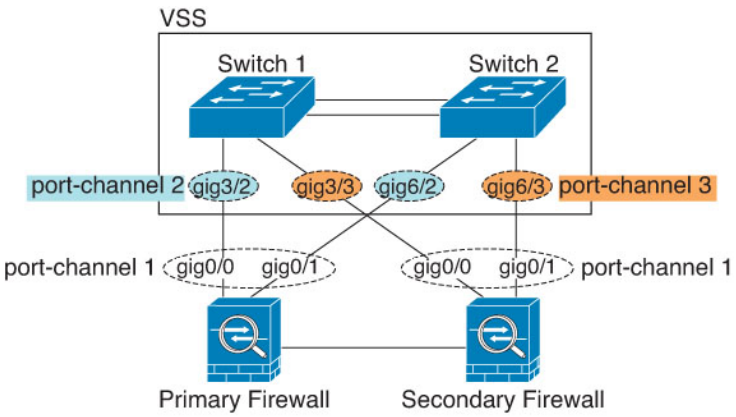
그림 ***12: VSS/vPC***에 연결



참고 threat defense 디바이스의 모드가 투명 방화벽 모드이고, 두 VSS/vPC 스위치 세트 사이에 threat defense 디바이스의 배치가 이루어지는 경우, EtherChannel을 사용하여 threat defense 디바이스에 연결된 모든 스위치 포트에서 UDLD(Unidirectional Link Detection)를 비활성화해야 합니다. UDLD를 활성화하면 스위치 포트가 다른 VSS/vPC 쌍의 두 스위치에서 제공되는 UDLD 패킷을 수신할 수 있습니다. 수신 스위치는 "UDLD 인접한 라우터 불일치"라는 이유와 함께 수신 인터페이스를 중단 상태로 설정합니다.

활성/대기 장애 조치 구축 시 threat defense 디바이스를 사용할 경우 VSS/vPC의 스위치에 각 threat defense 디바이스에 별도의 EtherChannel을 생성해야 합니다. 각 threat defense 디바이스에서 하나의 EtherChannel이 두 스위치 모두에 연결됩니다. 모든 스위치 인터페이스를 threat defense 디바이스에 연결된 단일 EtherChannel으로 그룹화하는 것은 가능하지만(이 경우 별도의 threat defense 시스템 ID로 인해 EtherChannel이 설정되지 않음), 스탠바이 threat defense 디바이스로 트래픽이 전송되는 것은 바람직하지 않으므로 단일 EtherChannel은 권장되지 않습니다.

그림 ***13:*** 액티브/스탠바이 장애 조치 및 ***VSS/vPC***



LACP(Link Aggregation Control Protocol)

LACP(Link Aggregation Control Protocol)에서는 두 네트워크 디바이스 간의 LACPDU(Link Aggregation Control Protocol Data Units)를 교환하여 인터페이스를 취합합니다.

EtherChannel의 각 물리적 인터페이스를 다음과 같이 구성할 수 있습니다.

- Active(활성화) — LACP 업데이트를 보내고 받습니다. 액티브 EtherChannel은 액티브 또는 패시브 EtherChannel과의 연결을 설정할 수 있습니다. LACP 트래픽 양을 최소화할 필요가 없는 한 액티브 모드를 사용해야 합니다.
- On(켜짐) — EtherChannel은 항상 켜져 있으며 LACP는 사용되지 않습니다. "on"으로 된 EtherChannel은 오로지 또 다른 "on" 상태의 EtherChannel과 연결을 설정할 수 있습니다.

LACP에서는 사용자의 작업 없이 EtherChannel에 링크를 자동으로 추가 및 삭제하는 작업을 조율합니다. 또한 구성 오류를 처리하고 멤버 인터페이스의 양끝이 모두 올바른 채널 그룹에 연결되어 있는지 확인합니다. "On" 모드에서는 인터페이스가 중단될 경우 채널 그룹의 스탠바이 인터페이스를 사용할 수 없으며, 연결 및 컨피그레이션이 확인되지 않습니다.

부하 균형

threat defense 디바이스에서는 패킷의 소스 및 대상 IP 주소를 해싱하여 EtherChannel의 인터페이스에 패킷을 분산시킵니다(이 조건은 구성 가능함). 결과의 나머지 부분에 따라 흐름을 보유하는 인터페이스가 결정되는 모듈로 작업의 액티브 링크 수를 기준으로 결과 해시가 분할됩니다. *hash_value* **mod** *active_links*의 결과가 0인 모든 패킷은 EtherChannel의 첫 번째 인터페이스로 이동하고, 결과가 1인 패킷은 두 번째 인터페이스, 결과가 2인 패킷은 세 번째 인터페이스로 이동하는 방식이 이어집니다. 예를 들어 액티브 링크가 15개 있는 경우 모듈로 작업에서는 0에서 14까지의 값을 제공합니다. 액티브 링크가 6개인 경우 해당 값은 0 ~ 5가 되며, 이런 식으로 계속 적용할 수 있습니다.

액티브 인터페이스가 중단되고 스탠바이 인터페이스로 대체되지 않을 경우, 나머지 링크 간의 트래픽이 다시 밸런싱됩니다. 오류는 Layer 2의 스패닝 트리와 Layer 3의 라우팅 테이블에서 모두 마스킹되므로, 전환 작업은 다른 네트워크 디바이스에 투명하게 이루어집니다.

EtherChannel MAC 주소

채널 그룹의 일부인 모든 인터페이스에서는 동일한 MAC 주소를 공유합니다. 이 기능은 EtherChannel을 네트워크 애플리케이션 및 사용자에게 투명하게 만듭니다. 이들은 논리적 연결만 볼 수 있으며, 개별 링크에 대해서는 모르기 때문입니다.

포트-채널 인터페이스는 가장 낮은 번호의 채널 그룹 인터페이스 MAC 주소를 포트-채널 MAC 주소로 사용합니다. 또는 포트-채널 인터페이스의 MAC 주소를 직접 구성할 수도 있습니다. 그룹 채널 인터페이스 멤버십이 변경될 경우에 대비하여 직접 고유한 MAC 주소를 구성하는 것이 좋습니다. 포트-채널 MAC 주소를 제공하던 인터페이스를 삭제한 경우, 포트-채널 MAC 주소가 그다음으로 낮은 번호의 인터페이스로 바뀌면서 트래픽 중단이 일어납니다.

EtherChannel용 가이드라인

브리지 그룹

Device Manager정의 EtherChannel은 브리지 그룹 멤버로 지원되지 않습니다. Firepower 4100/9300의 EtherChannel은 브리지 그룹 멤버가 될 수 있습니다.

고가용성

- 이중 또는 EtherChannel 인터페이스를 고가용성 링크로 사용할 경우, 고가용성 쌍의 두 유닛에 모두 이를 사전 구성해야 합니다. 복제를 위해서는 고가용성링크 자체가 필요하므로 이러한 인터페이스를 기본 유닛에 구성한 다음 이를 보조 유닛에 복제할 수 없습니다.
- 상태 링크에 EtherChannel 인터페이스를 사용할 경우, 특별한 컨피그레이션이 필요하지 않으며 컨피그레이션을 기본 유닛에서 정상적으로 복제할 수 있습니다. Firepower 4100/9300 섀시의 경우, EtherChannel을 비롯한 모든 인터페이스를 두 유닛에서 모두 사전 구성해야 합니다.
- **monitor-interface**명령을 사용하여 고가용성를 위한 EtherChannel 인터페이스를 모니터링. 액티브 멤버 인터페이스에서 스탠바이 인터페이스로 장애 조치를 시작할 경우, 디바이스 수준의 고가용성가 모니터링되고 있으면 이 작업을 수행해도 EtherChannel 인터페이스에 장애를 발생시키지 않습니다. 모든 물리적 인터페이스에 장애가 발생하는 경우에만 EtherChannel 인터페이스에 장애가 발생하는 것으로 나타납니다.
- 고가용성 또는 상태 링크에 EtherChannel 인터페이스를 사용할 경우, 패킷의 장애를 방지하기 위해 EtherChannel에서 하나의 인터페이스만 사용됩니다. 해당 인터페이스에 오류가 발생할 경우 EtherChannel의 다음 인터페이스가 사용됩니다. 고가용성 링크로 사용 중인 경우 EtherChannel 구성을 변경할 수 없습니다. 구성을 변경하려면 고가용성을 일시적으로 비활성화해야 합니다. 이렇게 하면 지속 시간 동안 고가용성이 발생하지 않습니다.

모델 지원

- device manager의 EtherChannels을 다음 모델에 추가할 수 있습니다.
  - Firepower 1000
  - Firepower 2100
  - Secure Firewall 3100
  - ISA 3000

  Firepower 4100/9300에서는 EtherChannel을 지원하지만 사용자는 섀시의 FXOS에서 EtherChannel의 모든 하드웨어 구성을 수행해야 합니다. Firepower 4100/9300 EtherChannel은 단일한 물리적 인터페이스와 함께 device manager 인터페이스 페이지에 표시됩니다. 또한 ASA 5500-X 시리즈와 같은 다른 모델에서는 device manager에서 EtherChannel을 설정할 수 없습니다.
- EtherChannel에서는 Firepower 1010 스위치 포트 또는 VLAN 인터페이스를 사용할 수 없습니다.

EtherChannel 일반 지침

- 모델에서 사용할 수 있는 인터페이스의 수에 따라 최대 48개의 EtherChannel을 구성할 수 있습니다.
- 각 채널 그룹에는 최대 8개의 액티브 인터페이스를 포함할 수 있습니다.
- 채널 그룹의 모든 인터페이스는 미디어 유형 및 속도 용량 미디어 유형은 RJ-45 또는 SFP일 수 있으며 서로 다른 유형(구리 및 광섬유)의 SFP를 혼합할 수 있습니다. 속도가 Detect SFP(SFP 탐지)로 설정되어 있는 한 다른 인터페이스 용량을 지원하는 Secure Firewall 3100의 경우를 제외하고, 대용량 인터페이스에서는 속도를 더 낮게 설정하여 인터페이스 용량(예: 1GB 및 10GB 인터페이스)을 혼합할 수 없습니다. .
- threat defense EtherChannel을 연결하는 디바이스에서는 802.3ad EtherChannel도 지원해야 합니다.
- threat defense 디바이스에서는 VLAN 태그 처리된 LACPDU를 지원하지 않습니다. Cisco IOS **vlan dot1Q tag native** 명령을 사용하여 인접한 스위치에서 네이티브 VLAN 태깅을 활성화할 경우, threat defense 디바이스에서는 태그 처리된 LACPDU를 제거합니다. 인접한 스위치에서 네이티브 VLAN 태깅을 비활성화해야 합니다.
- Firepower 1000 및 Firepower 2100, Secure Firewall 3100은 LACP 속도, fast(빠르게)를 지원하지 않습니다. LACP는 항상 정상 속도를 사용합니다. 이 설정은 구성 가능하지 않습니다. FXOS에서 EtherChannel을 구성하는 Firepower 4100/9300의 LACP 속도는 기본적으로 fast(빠르게)로 설정되어 있습니다. 이러한 플랫폼에서는 속도를 구성할 수 있습니다.
- 15.1(1)S2 이전 Cisco IOS 소프트웨어 버전에서는 threat defense가 EtherChannel과 스위치 스택 간의 연결을 지원하지 않았습니다. 기본 스위치 설정으로 threat defense EtherChannel이 교차 스택에 연결되어 있는 상태에서 기본 스위치의 전원이 꺼질 경우, 나머지 스위치에 연결된 EtherChannel은 가동되지 않습니다. 호환성을 개선하려면 **stack-mac persistent timer** 명령을 다시 로드 시간을 고려하여 충분히 큰 값으로 설정합니다(예: 8분 또는 무한인 경우 0). 또는 15.1(1)S2 같은 더 안정적인 스위치 소프트웨어 버전으로 업그레이드할 수 있습니다.
- 모든 threat defense 컨피그레이션에서는 멤버 물리적 인터페이스 대신 논리적 EtherChannel 인터페이스를 참조합니다.

EtherChannel 추가

EtherChannel을 추가하고 멤버 인터페이스를 할당합니다.

참고 device manager의 EtherChannels을 다음 모델에 추가할 수 있습니다.

- Firepower 1000
- Firepower 2100
- Secure Firewall 3100
- ISA 3000

Firepower 4100/9300에서는 EtherChannel을 지원하지만 사용자는 섀시의 FXOS에서 EtherChannel의 모든 하드웨어 구성을 수행해야 합니다. Firepower 4100/9300 EtherChannel은 단일한 물리적 인터페이스와 함께 device manager 인터페이스 페이지에 표시됩니다. 또한 ASA 5500-X 시리즈와 같은 다른 모델에서는 device manager에서 EtherChannel을 설정할 수 없습니다.

시작하기 전에

- 채널 그룹의 모든 인터페이스는 미디어 유형 및 속도 용량 미디어 유형은 RJ-45 또는 SFP일 수 있으며 서로 다른 유형(구리 및 광섬유)의 SFP를 혼합할 수 있습니다. 속도가 Detect SFP(SFP 탐지)로 설정되어 있는 한 다른 인터페이스 용량을 지원하는 Secure Firewall 3100의 경우를 제외하고, 대용량 인터페이스에서는 속도를 더 낮게 설정하여 인터페이스 용량(예: 1GB 및 10GB 인터페이스)을 혼합할 수 없습니다. .
- 멤버 인터페이스의 이름을 지정할 수 없습니다.

주의 구성에서 인터페이스를 이미 사용 중인 경우, 이름을 제거하면 인터페이스에서 참조하는 모든 구성이 지워집니다.

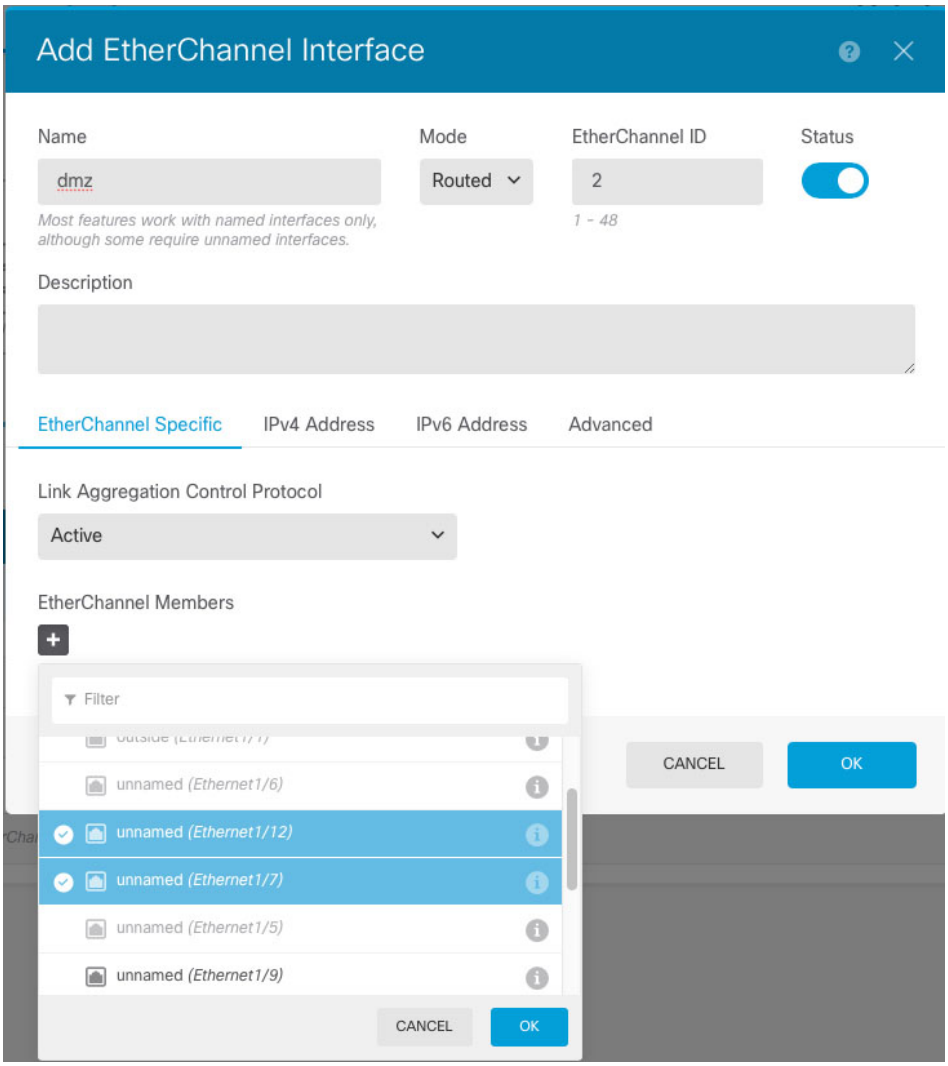
프로시저

단계 **1** **Device(**디바이스**)**를 클릭하고 **Interfaces(**인터페이스**)** 요약의 링크를 클릭한 다음, **EtherChannel**을 클릭합니다.

EtherChannel 목록에는 기존 EtherChannel, 해당 이름, 주소 및 상태가 표시됩니다. 각 EtherChannel의 멤버 인터페이스를 보려면 열기/닫기 화살표를 클릭합니다. 멤버 인터페이스는 **Interfaces(**인터페이스**)** 페이지에 개별적으로도 표시됩니다.

단계 **2** **Create EtherChannel(EtherChannel** 생성**)**(현재 EtherChannel이 없는 경우) 또는 더하기 아이콘(+ ˅)을 클릭한 다음, **EtherChannel**을 클릭하여 새 EtherChannel을 생성합니다.

단계 **3** 다음을 구성합니다.



a) **Interface Name(**인터페이스 이름**)**을 설정합니다.

EtherChannel의 이름을 최대 48자로 설정합니다. 영문자는 소문자로 입력해야 합니다. 예를 들면 **inside** 또는 **outside**와 같이 입력합니다.

참고 이름을 변경하는 경우 보안 영역, syslog 서버 개체, DHCP 서버 정의 등 이전 이름을 사용했던 모든 위치에서 변경 사항이 자동으로 반영됩니다. 그러나 해당 이름을 사용하는 모든 컨피그레이션을 먼저 제거해야 이름을 제거할 수 있습니다. 일반적으로는 정책이나 설정에 대해 이름이 없는 인터페이스를 사용할 수 없기 때문입니다.

b) **Mode(**모드**)**를 설정합니다.

- **Routed(**라우팅**)** — 라우팅 모드 인터페이스는 플로우 유지, IP 및 TCP 레이어 모두에서 플로우 상태 추적, IP 조각 모음, TCP 정규화 등의 모든 방화벽 기능과 방화벽 정책에 트래픽을 적용합니다. 트래픽이 인터페이스를 통과하도록 하려는 경우 이 모드를 사용합니다. 이 모드가 기본 인터페이스 모드입니다.

- **Passive(패시브)** - 패시브 인터페이스는 스위치 SPAN 또는 미러 포트를 사용하여 네트워크를 통과하는 트래픽을 모니터링합니다. SPAN 또는 미러 포트를 사용하면 스위치의 다른 포트에서 트래픽을 복사할 수 있습니다. 이 기능을 사용하면 네트워크 트래픽의 플로우 내에 있지 않더라도 시스템 가시성이 확보됩니다. 수동 구축으로 구성된 시스템에서는 트래픽 차단 또는 형성과 같은 특정 작업을 할 수 없습니다. 패시브 인터페이스는 모든 트래픽을 조건 없이 수신하며 이러한 인터페이스에서 수신된 트래픽은 재전송되지 않습니다. 이 모드를 선택하는 경우 이 절차의 나머지 단계를 수행하지 마십시오. 대신 패시브 모드로 물리적 인터페이스 구성, 301 페이지 섹션을 참조하십시오.

c) **EtherChannel ID**를 1~48(Firepower 1010의 경우 1~8)로 설정합니다.

d) **Status(상태)** 슬라이더를 활성화된 설정()으로 지정합니다.

e) (선택 사항) **Description(설명)**을 설정합니다.

설명은 줄 바꿈 없이 1줄, 최대 200자로 작성할 수 있습니다.

f) **EtherChannel Mode(EtherChannel 모드)**를 선택합니다.

- **Active(액티브)** — (권장) LACP 업데이트를 보내고 받습니다. 액티브 EtherChannel은 액티브 또는 패시브 EtherChannel과의 연결을 설정할 수 있습니다. LACP 트래픽 양을 최소화할 필요가 없는 한 액티브 모드를 사용해야 합니다.
- **On(켜짐)** — EtherChannel은 항상 켜져 있으며 LACP는 사용되지 않습니다. "on"으로 된 EtherChannel은 오로지 또 다른 "on" 상태의 EtherChannel과 연결을 설정할 수 있습니다.

g) **EtherChannel Members(EtherChannel 멤버)**를 추가합니다.

EtherChannel에는 최대 8개(이름 미지정)의 인터페이스를 추가할 수 있습니다.

- 인터페이스 추가 — 더하기 아이콘()을 클릭하고 하나 이상의 인터페이스를 클릭한 다음, **OK(확인)**를 클릭합니다.
- 인터페이스 제거 — 인터페이스 위에 마우스를 올려놓고 오른쪽의 **x**를 클릭합니다.

단계 **4** **IPv4 Address(IPv4 주소)** 탭을 클릭하고 IPv4 주소를 구성합니다.

Type(유형) 필드에서 다음 옵션 중 하나를 선택합니다.

- **DHCP** — 네트워크의 DHCP 서버에서 주소를 가져와야 하는 경우 이 옵션을 선택합니다. 고가용성을 구성하는 경우 이 옵션을 사용할 수 없습니다. 필요에 따라 다음 옵션을 변경합니다.
  - **Route Metric(경로 메트릭)** - DHCP 서버에서 기본 경로를 가져오는 경우 확인된 경로까지의 관리 거리(1~255)입니다. 기본값은 1입니다.
  - **Obtain Default Route(기본 경로 얻기)** - DHCP 서버에서 기본 경로를 가져올지 여부를 선택합니다. 일반적으로는 이 옵션을 선택합니다(기본값).
- **Static(고정)** - 변경되면 안 되는 주소를 할당하려면 이 옵션을 선택합니다. 인터페이스에 연결된 네트워크에 대해 인터페이스의 IP 주소와 서브넷 마스크를 입력합니다. 예를 들어 10.100.10.0/24 네트워크를 연결하는 경우 10.100.10.1/24를 입력할 수 있습니다. 주소가 네트워크에서 이미 사용되고 있지 않은지 확인합니다.

고가용성을 구성했으며 이 인터페이스에서 HA를 모니터링하는 중이라면 같은 서브넷에 스탠바이 IP 주소도 구성합니다. 스탠바이 디바이스의 이 인터페이스에서 스탠바이 주소를 사용합니다. 스탠바이 IP 주소를 설정하지 않으면 액티브 유닛이 네트워크 테스트를 사용하여 스탠바이 인터페이스를 모니터링할 수 없으며 링크 상태만 추적할 수 있습니다.

참고 인터페이스에 대해 구성된 DHCP 서버가 있을 경우, 해당 컨피그레이션이 표시됩니다. DHCP 주소 풀을 수정하거나 삭제할 수 있습니다. 인터페이스 IP 주소를 다른 서브넷으로 변경할 경우, 인터페이스 변경 사항을 저장하려면 우선 DHCP 서버를 삭제하거나, 새 서브넷에서 주소 풀을 구성해야 합니다. DHCP 서버 설정, 819 페이지의 내용을 참조하십시오.

- **PPPoE** — PPPoE(Point-to-Point Protocol over Ethernet)를 사용하여 주소를 가져와야 하는 경우 이 옵션을 선택합니다. 인터페이스가 DSL 모뎀이나 케이블 모뎀에 연결되어 있거나 기타 ISP 연결을 사용하고 ISP에서 PPPoE를 사용하여 IP 주소를 제공하는 경우, PPPoE가 필요할 수 있습니다. 고가용성을 구성하는 경우 이 옵션을 사용할 수 없습니다. 다음 값을 설정합니다.
  - **Group Name(**그룹 이름**)** — 이 연결을 나타내는 그룹 이름을 원하는 대로 지정합니다.
  - **PPPoE Username(PPPoE** 사용자 이름**)** — ISP에서 제공한 사용자 이름을 지정합니다.
  - **PPPoE Password(PPPoE** 비밀번호**)** — ISP에서 제공한 비밀번호를 지정합니다.
  - **PPP Authentication(PPP** 인증**) - PAP**, **CHAP**, 또는**MSCHAP**를 선택합니다.

    PAP에서는 인증이 진행되는 동안 일반 텍스트 사용자 이름 및 비밀번호를 전달하므로 안전하지 않습니다. CHAP를 사용하면 클라이언트에서는 서버 챌린지에 대한 응답으로 암호화된 [challenge plus password]와 함께 일반 텍스트로 된 사용자 이름을 반환합니다. CHAP는 PAP보다 안전하지만 데이터가 암호화되지 않습니다. MSCHAP는 CHAP와 유사하지만, CHAP의 일반 텍스트로 비밀번호와 달리 서버에서 암호화된 비밀번호만 저장하고 비교하므로 훨씬 안전합니다. MSCHAP에서도 MPPE를 통해 데이터 암호화용 키를 생성합니다.
  - **PPPoE Learned Route Metric(PPPoE** 학습된 경로 메트릭**)** — 학습된 경로에 관리 거리를 할당합니다. 유효한 값은 1 ~ 255입니다. 파악된 경로의 기본 관리 거리는 1입니다.
  - **Obtain Default Route from PPPoE(PPPoE**에서 기본 경로 가져오기**)** — PPPoE 서버에서 기본 경로를 가져오려면 이 확인란을 선택합니다.
  - **IP Address Type(IP** 주소 유형**)** — PPPoE 서버에서 IP 주소를 가져오려면 **Dynamic(**동적**)**을 선택합니다. 또는 ISP에서 정적 IP 주소를 할당한 경우 **Static(**정적**)**을 선택할 수 있습니다.

단계 **5** (선택 사항). **IPv6 Address(IPv6** 주소**)** 탭을 클릭하고 IPv6 주소를 구성합니다.

- **Sate(**상태**) -** 글로벌 어드레스를 구성하지 않는 경우 IPv6 처리를 활성화하고 링크-로컬 주소를 자동으로 구성하려면 **Enabled(**활성화됨**)**를 선택합니다. 링크 로컬 주소는 인터페이스 MAC 주소(수정된 EUI-64 형식)를 기반으로 생성됩니다.

  참고 IPv6를 비활성화해도 명시적 IPv6 주소로 구성되었거나 자동 컨피그레이션용으로 활성화된 인터페이스에서 IPv6 처리가 비활성화되지는 않습니다.

- **Address Auto Configuration(**주소 자동 컨피그레이션**)** - 주소를 자동으로 구성하려면 이 옵션을 선택합니다. IPv6 스테이트리스 자동 컨피그레이션에서는 디바이스가 있는 링크에 IPv6 서비스를 제공하도록 구성된 라우터가 있는 경우에만 글로벌 IPv6 주소를 생성합니다. 이러한 서비스에는 링크에서 사용할 IPv6 글로벌 접두사 알림이 포함됩니다. 링크에서 IPv6 라우팅 서비스를 사용할 수 없는 경우에는 링크-로컬 IPv6 주소만 제공됩니다. 디바이스의 직접 네트워크 링크 외부에서는 이 주소에 액세스할 수 없습니다. 링크 로컬 주소는 수정된 EUI-64 인터페이스 ID를 기반으로 합니다.

  RFC 4862에서는 스테이트리스 자동 컨피그레이션에 대해 구성한 호스트에서 라우터 알림 메시지를 전송하지 않도록 지정하지만, 이 경우에는 threat defense 디바이스에서 라우터 알림 메시지를 전송합니다. 메시지를 표시하지 않고 RFC를 준수하려면 **RA** 표시 안 함을 선택합니다.

- **Static Address/Prefix(**고정 주소/접두사**)** - 스테이트리스 자동 컨피그레이션을 사용하지 않는 경우 전체 고정 글로벌 IPv6 주소와 네트워크 접두사를 입력합니다. 예를 들어, 2001:0DB8::BA98:0:3210/48와 같이 입력합니다. IPv6 주소 지정에 대한 자세한 내용은 IPv6 주소 지정, 258 페이지를 참조하십시오.

  주소를 링크 로컬 전용으로 사용하려는 경우 링크-로컬 옵션을 선택합니다. 로컬 네트워크 외부에서는 링크 로컬 주소에 액세스할 수 없습니다. 브리지 그룹 인터페이스에서는 링크-로컬 주소를 구성할 수 없습니다.

  참고 링크-로컬 주소는 FE8, FE9, FEA 또는 FEB로 시작해야 합니다(예: fe80::20d:88ff:feee:6a82). Modified EUI-64 형식으로 링크-로컬 주소를 자동으로 지정하는 것이 좋습니다. 만약 다른 디바이스에서 Modified EUI-64 형식을 강제 적용하는 경우 수동으로 지정된 링크-로컬 주소 때문에 패킷이 폐기될 수 있습니다.

- **Standby IP Address(**스탠바이 **IP** 주소**)** - 고가용성을 구성하는 경우 이 인터페이스에서 HA를 모니터링하는 중이라면 같은 서브넷에 스탠바이 IPv6 주소도 구성합니다. 스탠바이 디바이스의 이 인터페이스에서 스탠바이 주소를 사용합니다. 스탠바이 IP 주소를 설정하지 않으면 액티브 유닛이 네트워크 테스트를 사용하여 스탠바이 인터페이스를 모니터링할 수 없으며 링크 상태만 추적할 수 있습니다.

- **Suppress RA(RA** 표시 안 함**)** - 라우터 알림을 표시하지 않을지를 선택합니다. threat defense는 인접 디바이스가 기본 라우터 주소를 동적으로 학습할 수 있도록 라우터 알림에 참여할 수 있습니다. 기본적으로 라우터 알림 메시지(ICMPv6 유형 134)는 IPv6가 구성된 각 인터페이스에 주기적으로 전송됩니다.

  라우터 광고는 라우터 요청 메시지에 대한 응답으로도 보내집니다(ICMPv6 Type 133). 예정된 다음 라우터 광고 메시지를 기다릴 필요 없이 호스트가 즉시 자동 구성을 할 수 있도록 시스템 시동 시 라우터 요청 메시지가 전송됩니다.

  threat defense 디바이스에서 IPv6 접두사를 제공하지 않도록 하려는 인터페이스(예: 외부 인터페이스)에서는 이러한 메시지를 표시하지 않을 수 있습니다.

단계 **6** **Advanced(**고급**)**를 클릭하고 속도를 설정하여 멤버 인터페이스의 속도를 설정합니다.

다른 고급 옵션을 구성할 수도 있습니다. 고급 옵션 구성, 304 페이지의 내용을 참조하십시오.

단계 **7** **OK(**확인**)**를 클릭합니다.

다음에 수행할 작업

- 적절한 보안 영역에 EtherChannel을 추가합니다. 보안 영역 구성, 152 페이지의 내용을 참조하십시오.

VLAN 인터페이스 및 스위치 포트 구성(Firepower 1010)

각 Firepower 1010 인터페이스가 일반 방화벽 인터페이스 또는 레이어 2 하드웨어 스위치 포트로 실행되도록 구성할 수 있습니다. 이 섹션에는 스위치 모드의 활성화 또는 비활성화, VLAN 인터페이스 생성 및 VLAN에 스위치 포트 할당 등을 비롯하여 스위치 포트의 구성을 시작하기 위한 작업이 포함되어 있습니다. 이 섹션에서는 지원되는 인터페이스에서 PoE(Power over Ethernet)를 맞춤화하는 방법에 대해서도 설명합니다.

Firepower 1010 포트 및 인터페이스 이해

포트 및 인터페이스

각 물리적 Firepower 1010 인터페이스의 경우, 해당 작업을 방화벽 인터페이스 또는 스위치 포트로 설정할 수 있습니다. 물리적 인터페이스, 포트 유형 및 스위치 포트를 할당할 논리적 VLAN 인터페이스에 대한 다음과 같은 정보를 참조하십시오.

- 물리적 방화벽 인터페이스 - 라우팅 모드에서 이러한 인터페이스는 구성된 보안 정책을 사용해 방화벽과 VPN 서비스를 적용하여 레이어 3에서 네트워크 간에 트래픽을 전달합니다. 라우팅 모드에서는 일부 인터페이스와의 통합 라우팅 및 브리징을 브리지 그룹 멤버로 사용하고 기타 인터페이스를 레이어 3 인터페이스로 사용할 수도 있습니다. 기본적으로 Ethernet 1/1 인터페이스는 방화벽 인터페이스로 구성됩니다.이러한 인터페이스를 IPS 전용(패시브 인터페이스)으로 구성할 수도 있습니다.
- 물리적 스위치 포트 - 스위치 포트에서는 하드웨어에서 스위칭 기능을 사용하여 레이어 2에서 트래픽을 전달합니다. 동일한 VLAN의 스위치 포트는 하드웨어 스위칭을 사용하여 서로 통신할 수 있으며 트래픽에는 threat defense 보안 정책이 적용되지 않습니다. 액세스 포트의 경우 태그 없는 트래픽만 허용되며 이러한 포트는 단일 VLAN에 할당할 수 있습니다. 트렁크 포트의 경우 태그 없는 트래픽과 태그 있는 트래픽이 허용되며 둘 이상의 VLAN에 속할 수 있습니다. 기본적으로, Ethernet 1/2~1/8은 VLAN 1에서 액세스 스위치 포트로 설정됩니다. 관리 인터페이스는 스위치 포트로 구성할 수 없습니다.
- 논리적 VLAN 인터페이스 - 이러한 인터페이스는 물리적 방화벽 인터페이스와 동일하게 작동합니다. 단, 하위 인터페이스IPS 전용 인터페이스(인라인 집합 및 패시브 인터페이스) 또는 EtherChannel 인터페이스는 생성할 수 없습니다. 스위치 포트가 다른 네트워크와 통신해야 하는 경우, threat defense 디바이스에서 VLAN 인터페이스에 보안 정책을 적용하고 다른 논리적 VLAN 인터페이스 또는 방화벽 인터페이스로 라우팅됩니다. VLAN 인터페이스와의 통합 라우팅 및 브리징을 브리지 그룹 멤버로 사용할 수도 있습니다. 동일한 VLAN의 스위치 포트 간 트래픽에는

threat defense 보안 정책이 적용되지 않지만, 브리지 그룹에 있는 VLAN 간의 트래픽에는 보안 정책이 적용됩니다. 따라서 특정 세그먼트 간에 보안 정책을 적용하려면 레이어 브리지 그룹 및 스위치 포트를 계층화하도록 선택할 수 있습니다.

PoE(Power over Ethernet)

Ethernet 1/7 및 Ethernet 1/8에서는 PoE+(Power over Ethernet+)를 지원합니다.

Firepower 1010 스위치 포트에 대한 지침 및 제한 사항

고가용성

- 고가용성 사용 시 스위치 포트 기능을 사용해서는 안 됩니다. 스위치 포트는 하드웨어에서 작동하므로 액티브 및 스탠바이 유닛에서 계속 트래픽을 전달합니다. 고가용성은 트래픽이 스탠바이 유닛을 통과하는 것을 방지하기 위해 고안되었지만 스위치 포트로 확장되지는 않습니다. 일반 고가용성 네트워크 설정에서 두 유닛의 액티브 스위치 포트는 네트워크 루프로 이어집니다. 모든 스위칭 기능에는 외부 스위치를 사용하는 것이 좋습니다. VLAN 인터페이스는 장애 조치를 통해 모니터링될 수 있지만 스위치 포트는 그럴 수 없습니다. 이론적으로는 VLAN에 단일 스위치 포트를 배치하고 고가용성을 정상적으로 사용할 수 있지만, 물리적 방화벽 인터페이스를 대신 사용하면 더 간단하게 설정할 수 있습니다.
- 방화벽 인터페이스만 장애 조치 링크로 사용할 수 있습니다.

논리적 **VLAN** 인터페이스

- 최대 60개의 VLAN 인터페이스를 생성할 수 있습니다.
- 방화벽 인터페이스에서 VLAN 하위 인터페이스도 사용하는 경우에는 논리적 VLAN 인터페이스에 동일한 VLAN ID를 사용할 수 없습니다.
- MAC 주소:
  - 모든 VLAN 인터페이스에서는 MAC 주소를 공유합니다. 연결된 스위치가 이 시나리오에 도움이 될 수 있을지 확인하십시오. 연결된 스위치에 고유한 MAC 주소가 필요한 경우, MAC 주소를 수동으로 할당할 수 있습니다. 고급 옵션 구성, 304 페이지의 내용을 참조하십시오.

브리지 그룹

동일한 브리지 그룹에서 논리적 VLAN 인터페이스와 물리적 방화벽 인터페이스를 혼합할 수는 없습니다.

VLAN 인터페이스 및 스위치 포트에서 지원되지 않는 기능

VLAN 인터페이스 및 스위치 포트에서는 다음을 지원하지 않습니다.

- 동적 라우팅
- 멀티캐스트 라우팅

- ECMP(Equal-Cost Multi-Path) 라우팅
- 패시브 인터페이스
- EtherChannel
- 장애 조치 및 상태 링크

기타 지침 및 제한 사항

- Firepower 1010에서 명명된 인터페이스를 최대 60개 구성할 수 있습니다.
- 관리 인터페이스는 스위치 포트로 구성할 수 없습니다.

기본 설정

- Ethernet 1/1은 방화벽 인터페이스입니다.
- Ethernet 1/2~Ethernet 1/8은 VLAN 1에 할당된 스위치 포트입니다.
- 기본 속도 및 듀플렉스 - 기본적으로 속도 및 듀플렉스는 자동 협상으로 설정됩니다.

VLAN 인터페이스 구성

이 섹션에서는 연결된 스위치 포트에 사용할 VLAN 인터페이스를 구성하는 방법에 대해 설명합니다. 먼저 스위치 포트에 할당할 각 VLAN에 대해 VLAN 인터페이스를 구성해야 합니다.

참고 특정 VLAN의 스위치 포트 간에만 스위칭을 활성화하고 VLAN과 기타 VLAN 또는 방화벽 인터페이스 간에는 라우팅하지 않으려는 경우에는 VLAN 인터페이스 이름을 비워 둡니다. 이 경우에도 IP 주소를 구성할 필요가 없습니다. 즉, 모든 IP 구성은 무시됩니다.

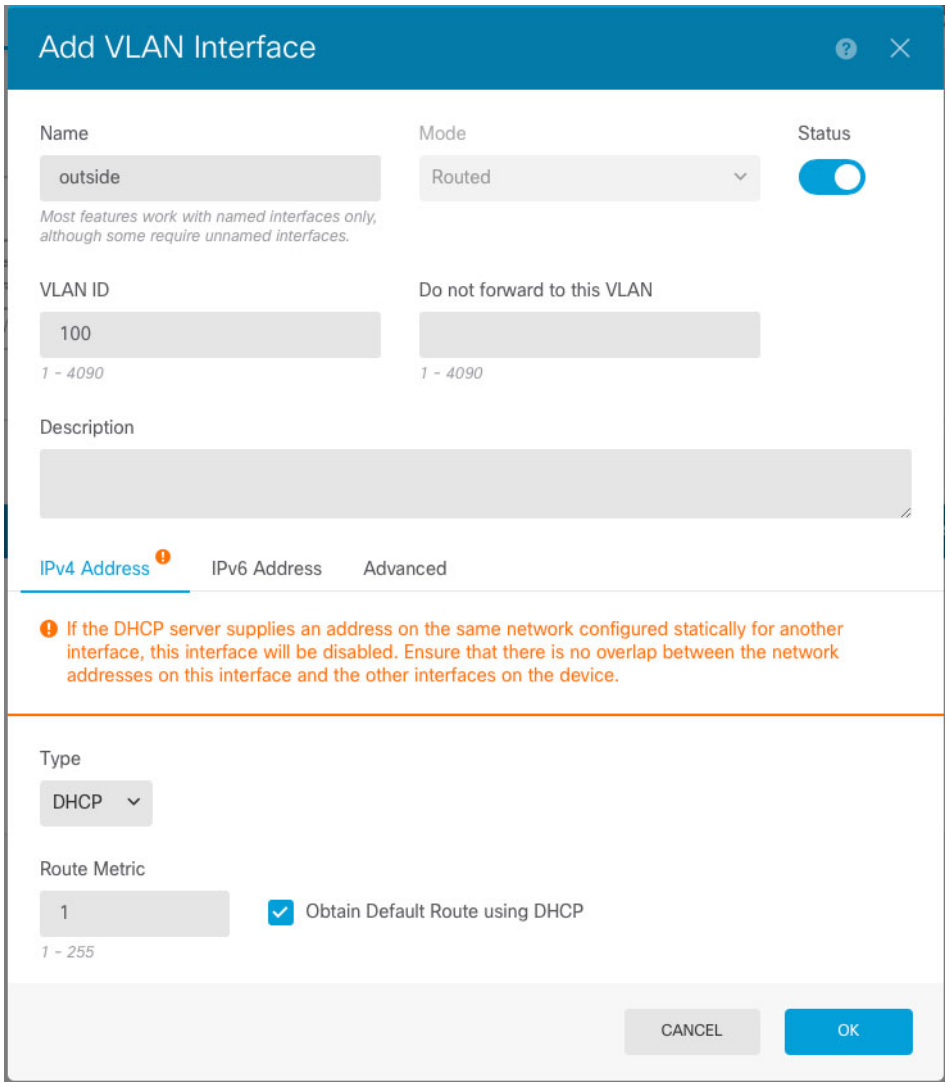
프로시저

단계 **1** **Device(**디바이스**)**를 클릭하고 **Interfaces(**인터페이스**)** 요약의 링크를 클릭한 다음, **VLAN**을 클릭합니다.

VLAN 목록에는 기존 VLAN 인터페이스가 표시됩니다. 각 VLAN과 연결된 스위치 포트를 보려면 열기/닫기 화살표를 클릭합니다. 스위치 포트는 **Interfaces(**인터페이스**)** 페이지에 개별적으로도 표시됩니다.

단계 **2** **Create VLAN Interface(VLAN** 인터페이스 생성**)** (현재 VLAN이 없는 경우) 또는 더하기 아이콘(+)을 클릭하여 새 VLAN 인터페이스를 생성합니다.

단계 **3** 다음을 구성합니다.



a) **Interface Name(**인터페이스 이름**)**을 설정합니다.

VLAN의 이름을 최대 48자로 설정합니다. 영문자는 소문자로 입력해야 합니다. 예를 들면 **inside** 또는 **outside**와 같이 입력합니다.

VLAN과 기타 VLAN 또는 방화벽 인터페이스 간에 라우팅하지 않으려는 경우에는 VLAN 인터페이스 이름을 비워 둡니다.

참고 이름을 변경하는 경우 보안 영역, syslog 서버 개체, DHCP 서버 정의 등 이전 이름을 사용했던 모든 위치에서 변경 사항이 자동으로 반영됩니다. 그러나 해당 이름을 사용하는 모든 컨피그레이션을 먼저 제거해야 이름을 제거할 수 있습니다. 일반적으로는 정책이나 설정에 대해 이름이 없는 인터페이스를 사용할 수 없기 때문입니다.

b) 이 **Mode(**모드**)**를 **Routed(**라우팅**)**인 상태로 둡니다.

나중에 이 VLAN 인터페이스를 브리지 그룹에 추가하면 모드가 자동으로 **BridgeGroupMember**로 변경됩니다. 브리지 그룹 멤버 인터페이스에서는 IP 주소를 구성할 수 없습니다.

c) **Status(**상태**)** 슬라이더를 활성화된 설정()으로 지정합니다.

d) 1~4070의 **VLAN ID**를 설정합니다.

인터페이스를 저장한 후에는 VLAN ID를 변경할 수 없습니다. VLAN ID는 사용된 VLAN 태그이자 구성의 인터페이스 ID입니다.

e) (선택 사항) **Do not forward to this VLAN(**이 **VLAN**으로 전달하지 않음**)** 필드에 이 VLAN 인터페이스에서 트래픽을 시작할 수 없는 VLAN ID를 입력합니다.

예를 들어, 인터넷 액세스를 위해 외부에 VLAN 1개를, 내부 비즈니스용 네트워크에 또 다른 VLAN 1개를 그리고 홈 네트워크에 3번째 VLAN을 할당합니다. 홈 네트워크에서는 비즈니스 네트워크에 액세스할 필요가 없으므로 홈 VLAN에서 Block Traffic From this Interface to(이 인터페이스에서 다음 위치로 가는 트래픽 차단) 옵션을 사용할 수 있습니다. 비즈니스 네트워크에서는 홈 네트워크에 액세스할 수 있지만 홈 네트워크에서는 비즈니스 네트워크에 액세스할 수 없습니다.

f) (선택 사항) **Description(**설명**)**을 설정합니다.

설명은 줄 바꿈 없이 1줄, 최대 200자로 작성할 수 있습니다.

단계 **4** **IPv4 Address(IPv4** 주소**)** 탭을 클릭하고 IPv4 주소를 구성합니다.

Type(유형**)** 필드에서 다음 옵션 중 하나를 선택합니다.

- **DHCP** — 네트워크의 DHCP 서버에서 주소를 가져와야 하는 경우 이 옵션을 선택합니다. 고가용성을 구성하는 경우 이 옵션을 사용할 수 없습니다. 필요에 따라 다음 옵션을 변경합니다.
  - **Route Metric(**경로 메트릭**)** - DHCP 서버에서 기본 경로를 가져오는 경우 확인된 경로까지의 관리 거리(1~255)입니다. 기본값은 1입니다.
  - **Obtain Default Route(**기본 경로 얻기**)** - DHCP 서버에서 기본 경로를 가져올지 여부를 선택합니다. 일반적으로는 이 옵션을 선택합니다(기본값).

- **Static(**고정**)** - 변경되면 안 되는 주소를 할당하려면 이 옵션을 선택합니다. 인터페이스에 연결된 네트워크에 대해 인터페이스의 IP 주소와 서브넷 마스크를 입력합니다. 예를 들어 10.100.10.0/24 네트워크를 연결하는 경우 10.100.10.1/24를 입력할 수 있습니다. 주소가 네트워크에서 이미 사용되고 있지 않은지 확인합니다.

  고가용성을 구성했으며 이 인터페이스에서 HA를 모니터링하는 중이라면 같은 서브넷에 스탠바이 IP 주소도 구성합니다. 스탠바이 디바이스의 이 인터페이스에서 스탠바이 주소를 사용합니다. 스탠바이 IP 주소를 설정하지 않으면 액티브 유닛이 네트워크 테스트를 사용하여 스탠바이 인터페이스를 모니터링할 수 없으며 링크 상태만 추적할 수 있습니다.

  참고 인터페이스에 대해 구성된 DHCP 서버가 있을 경우, 해당 컨피그레이션이 표시됩니다. DHCP 주소 풀을 수정하거나 삭제할 수 있습니다. 인터페이스 IP 주소를 다른 서브넷으로 변경할 경우, 인터페이스 변경 사항을 저장하려면 우선 DHCP 서버를 삭제하거나, 새 서브넷에서 주소 풀을 구성해야 합니다. DHCP 서버 설정, 819 페이지의 내용을 참조하십시오.

- **PPPoE** — PPPoE(Point-to-Point Protocol over Ethernet)를 사용하여 주소를 가져와야 하는 경우 이 옵션을 선택합니다. 인터페이스가 DSL 모뎀이나 케이블 모뎀에 연결되어 있거나 기타 ISP 연결

을 사용하고 ISP에서 PPPoE를 사용하여 IP 주소를 제공하는 경우, PPPoE가 필요할 수 있습니다. 고가용성을 구성하는 경우 이 옵션을 사용할 수 없습니다. 다음 값을 설정합니다.

- **Group Name(**그룹 이름**)** — 이 연결을 나타내는 그룹 이름을 원하는 대로 지정합니다.
- **PPPoE Username(PPPoE** 사용자 이름**)** — ISP에서 제공한 사용자 이름을 지정합니다.
- **PPPoE Password(PPPoE** 비밀번호**)** — ISP에서 제공한 비밀번호를 지정합니다.
- **PPP Authentication(PPP** 인증**) - PAP**, **CHAP**, 또는**MSCHAP**를 선택합니다.

  PAP에서는 인증이 진행되는 동안 일반 텍스트 사용자 이름 및 비밀번호를 전달하므로 안전하지 않습니다. CHAP를 사용하면 클라이언트에서는 서버 챌린지에 대한 응답으로 암호화된 [challenge plus password]와 함께 일반 텍스트로 된 사용자 이름을 반환합니다. CHAP는 PAP보다 안전하지만 데이터가 암호화되지 않습니다. MSCHAP는 CHAP와 유사하지만, CHAP의 일반 텍스트로 비밀번호와 달리 서버에서 암호화된 비밀번호만 저장하고 비교하므로 훨씬 안전합니다. MSCHAP에서도 MPPE를 통해 데이터 암호화용 키를 생성합니다.
- **PPPoE Learned Route Metric(PPPoE** 학습된 경로 메트릭**)** — 학습된 경로에 관리 거리를 할당합니다. 유효한 값은 1 ~ 255입니다. 파악된 경로의 기본 관리 거리는 1입니다.
- **Obtain Default Route from PPPoE(PPPoE**에서 기본 경로 가져오기**)** — PPPoE 서버에서 기본 경로를 가져오려면 이 확인란을 선택합니다.
- **IP Address Type(IP** 주소 유형**)** — PPPoE 서버에서 IP 주소를 가져오려면 **Dynamic(**동적**)**을 선택합니다. 또는 ISP에서 정적 IP 주소를 할당한 경우 **Static(**정적**)**을 선택할 수 있습니다.

단계 **5** (선택 사항). **IPv6 Address(IPv6** 주소**)** 탭을 클릭하고 IPv6 주소를 구성합니다.

- **Sate(**상태**) -** 글로벌 어드레스를 구성하지 않는 경우 IPv6 처리를 활성화하고 링크-로컬 주소를 자동으로 구성하려면 **Enabled(**활성화됨**)**를 선택합니다. 링크 로컬 주소는 인터페이스 MAC 주소(수정된 EUI-64 형식)를 기반으로 생성됩니다.

  참고 IPv6를 비활성화해도 명시적 IPv6 주소로 구성되었거나 자동 컨피그레이션용으로 활성화된 인터페이스에서 IPv6 처리가 비활성화되지는 않습니다.

- **Address Auto Configuration(**주소 자동 컨피그레이션**) -** 주소를 자동으로 구성하려면 이 옵션을 선택합니다. IPv6 스테이트리스 자동 컨피그레이션에서는 디바이스가 있는 링크에 IPv6 서비스를 제공하도록 구성된 라우터가 있는 경우에만 글로벌 IPv6 주소를 생성합니다. 이러한 서비스에는 링크에서 사용할 IPv6 글로벌 접두사 알림이 포함됩니다. 링크에서 IPv6 라우팅 서비스를 사용할 수 없는 경우에는 링크-로컬 IPv6 주소만 제공됩니다. 디바이스의 직접 네트워크 링크 외부에서는 이 주소에 액세스할 수 없습니다. 링크 로컬 주소는 수정된 EUI-64 인터페이스 ID를 기반으로 합니다.

  RFC 4862에서는 스테이트리스 자동 컨피그레이션에 대해 구성한 호스트에서 라우터 알림 메시지를 전송하지 않도록 지정하지만, 이 경우에는 threat defense 디바이스에서 라우터 알림 메시지를 전송합니다. 메시지를 표시하지 않고 RFC를 준수하려면 **RA** 표시 안 함을 선택합니다.

- **Static Address/Prefix(**고정 주소/접두사**) -** 스테이트리스 자동 컨피그레이션을 사용하지 않는 경우 전체 고정 글로벌 IPv6 주소와 네트워크 접두사를 입력합니다. 예를 들어,

2001:0DB8::BA98:0:3210/48와 같이 입력합니다. IPv6 주소 지정에 대한 자세한 내용은 IPv6 주소 지정, 258 페이지를 참조하십시오.

주소를 링크 로컬 전용으로 사용하려는 경우 링크-로컬 옵션을 선택합니다. 로컬 네트워크 외부에서는 링크 로컬 주소에 액세스할 수 없습니다. 브리지 그룹 인터페이스에서는 링크-로컬 주소를 구성할 수 없습니다.

참고 링크-로컬 주소는 FE8, FE9, FEA 또는 FEB로 시작해야 합니다(예: fe80::20d:88ff:feee:6a82). Modified EUI-64 형식으로 링크-로컬 주소를 자동으로 지정하는 것이 좋습니다. 만약 다른 디바이스에서 Modified EUI-64 형식을 강제 적용하는 경우 수동으로 지정된 링크-로컬 주소 때문에 패킷이 폐기될 수 있습니다.

- **Standby IP Address(**스탠바이 **IP** 주소**)** - 고가용성을 구성하는 경우 이 인터페이스에서 HA를 모니터링하는 중이라면 같은 서브넷에 스탠바이 IPv6 주소도 구성합니다. 스탠바이 디바이스의 이 인터페이스에서 스탠바이 주소를 사용합니다. 스탠바이 IP 주소를 설정하지 않으면 액티브 유닛이 네트워크 테스트를 사용하여 스탠바이 인터페이스를 모니터링할 수 없으며 링크 상태만 추적할 수 있습니다.
- **Suppress RA(RA** 표시 안 함**)** - 라우터 알림을 표시하지 않을지를 선택합니다. threat defense는 인접 디바이스가 기본 라우터 주소를 동적으로 학습할 수 있도록 라우터 알림에 참여할 수 있습니다. 기본적으로 라우터 알림 메시지(ICMPv6 유형 134)는 IPv6가 구성된 각 인터페이스에 주기적으로 전송됩니다.

  라우터 광고는 라우터 요청 메시지에 대한 응답으로도 보내집니다(ICMPv6 Type 133). 예정된 다음 라우터 광고 메시지를 기다릴 필요 없이 호스트가 즉시 자동 구성을 할 수 있도록 시스템 시동 시 라우터 요청 메시지가 전송됩니다.

  threat defense 디바이스에서 IPv6 접두사를 제공하지 않도록 하려는 인터페이스(예: 외부 인터페이스)에서는 이러한 메시지를 표시하지 않을 수 있습니다.

단계 **6** (선택 사항). 고급 옵션 구성, 304 페이지에 전달하는 고성능 고속 어플라이언스입니다.

고급 설정에는 대부분의 네트워크에 적합한 기본값이 있습니다. 네트워크 문제를 해결하는 경우에만 이러한 기본값을 수정하십시오.

단계 **7** **OK(**확인**)**를 클릭합니다.

다음에 수행할 작업

- 적절한 보안 영역에 VLAN을 추가합니다. 보안 영역 구성, 152 페이지의 내용을 참조하십시오.

스위치 포트를 액세스 포트로 구성

단일 VLAN에 스위치 포트를 할당하려면 해당 포트를 액세스 포트로 구성합니다. 기본적으로, Ethernet 1/2~Ethernet 1/8 스위치 포트는 활성화되며 VLAN 1에 할당됩니다.

참고 Firepower 1010에서는 네트워크에서의 루프 탐지를 위해 Spanning Tree Protocol을 지원하지 않습니다. 따라서 threat defense와의 연결이 네트워크 루프에서 종료되지 않도록 해야 합니다.

시작하기 전에

액세스 포트를 할당할 VLAN ID에 대한 VLAN 인터페이스를 추가합니다. 액세스 포트에서는 태그 없는 트래픽만 허용됩니다. VLAN 인터페이스 구성, 282 페이지의 내용을 참조하십시오.

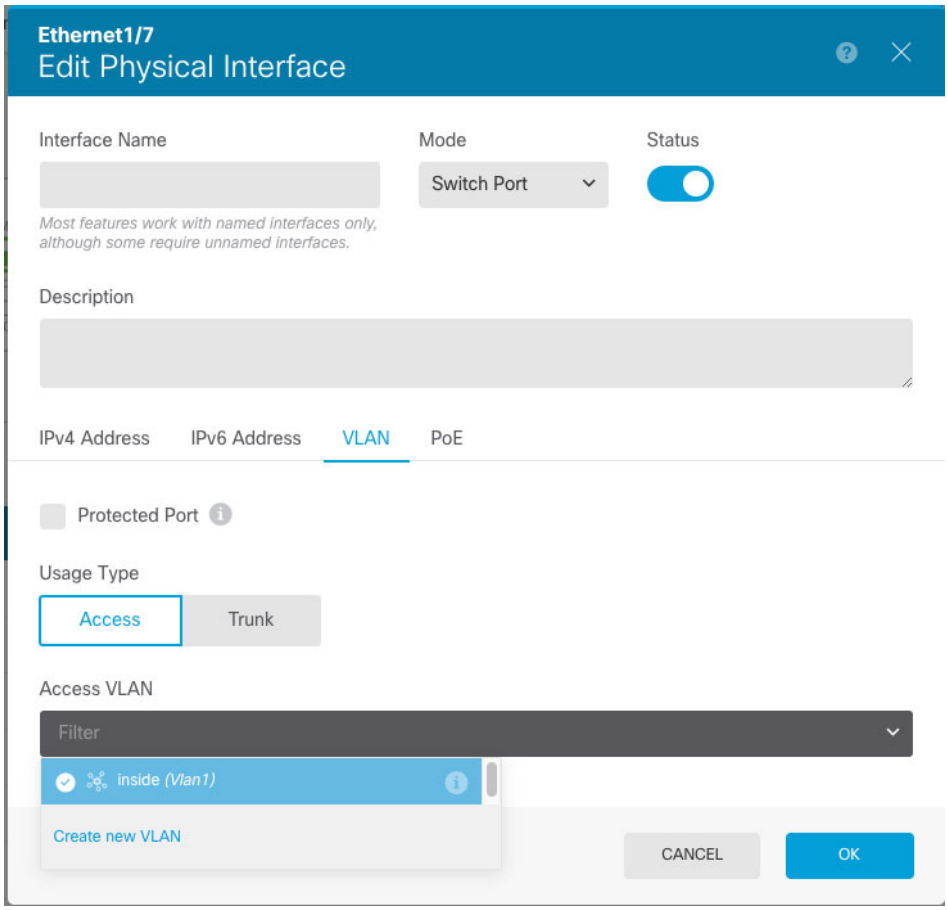
프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음, **Interfaces(**인터페이스**)** 요약의 링크를 클릭합니다.

기본적으로는 **Interfaces(**인터페이스**)** 페이지가 선택됩니다. 인터페이스 목록에는 물리적 인터페이스, 해당 이름, 주소 및 상태가 표시됩니다.

단계 **2** 수정할 실제 인터페이스의 수정 아이콘( )을 클릭합니다.

단계 **3** 다음을 설정합니다.



a) 스위치 포트에 대한 **Interface Name(**인터페이스 이름**)**은 설정하지 마십시오. 연결된 VLAN 인터페이스만 명명된 인터페이스입니다.

b) **Mode(**모드**)**를 **Switch Port(**스위치 포트**)**로 설정합니다.

c) **Status(**상태**)** 슬라이더를 활성화된 설정( )으로 지정합니다.

d) (선택 사항) **Description(**설명**)**을 설정합니다.

설명은 줄 바꿈 없이 1줄, 최대 200자로 작성할 수 있습니다.

단계 **4** **VLAN**을 클릭하여 다음을 설정합니다.

a) (선택 사항) **Protected Port(**보호된 포트**)** 확인란을 선택하여 이 스위치 포트를 보호된 상태로 설정합니다. 그러면 스위치 포트가 동일한 VLAN에서 보호되는 다른 스위치 포트와 통신하는 것을 방지할 수 있습니다.

스위치 포트의 디바이스가 주로 다른 VLAN에서 액세스되어 VLAN 간 액세스를 허용할 필요가 없으며 감염 또는 기타 보안 침입 시 디바이스를 서로 분리하려는 경우 스위치 포트가 서로 통신하지 못하도록 할 수 있습니다. 예를 들어 세 개의 웹 서버를 호스팅하는 DMZ가 있는 경우, 이 옵션을 각 스위치 포트에 적용하면 웹 서버를 서로 분리할 수 있습니다. 내부 및 외부 네트워크 둘 다 세 개의 웹 서버와 통신할 수 있지만 웹 서버 간에 서로 통신할 수는 없습니다.

b) **Usage Type(**사용 유형**)**에서 **Access(**액세스**)**를 클릭합니다.

c) **Access VLAN(**액세스 **VLAN)**의 경우, 아래쪽 화살표를 클릭하여 기존의 VLAN 인터페이스 중 하나를 선택합니다.

Create new VLAN(새 **VLAN** 생성**)**을 클릭하여 새 VLAN 인터페이스를 추가할 수 있습니다. VLAN 인터페이스 구성, 282 페이지의 내용을 참조하십시오.

단계 **5** **OK(**확인**)**를 클릭합니다.

스위치 포트를 트렁크 포트로 구성

이 절차에서는 802.1Q 태깅을 사용하여 여러 VLAN을 전송할 수 있는 트렁크 포트를 생성하는 방법에 대해 설명합니다. 트렁크 포트의 경우 태그 없는 트래픽과 태그 있는 트래픽이 허용됩니다. 허용된 VLAN의 트래픽에서는 트렁크 포트가 변경되지 않은 상태로 전달됩니다.

트렁크에서는 태그 없는 트래픽을 수신하는 경우 ASA에서 해당 트래픽을 올바른 스위치 포트로 전달하거나 다른 방화벽 인터페이스로 라우팅할 수 있도록 해당 트래픽을 네이티브 VLAN ID에 대해 태그 지정합니다. ASA에서는 트렁크 포트 외부로 네이티브 VLAN ID 트래픽을 전송하는 경우 VLAN 태그를 제거합니다. 태그 없는 트래픽이 동일한 VLAN에 대해 태그 지정될 수 있도록 다른 스위치의 트렁크 포트에서 동일한 네이티브 VLAN을 설정해야 합니다.

시작하기 전에

트렁크 포트를 할당할 각 VLAN ID에 대한 VLAN 인터페이스를 추가합니다. VLAN 인터페이스 구성, 282 페이지의 내용을 참조하십시오.

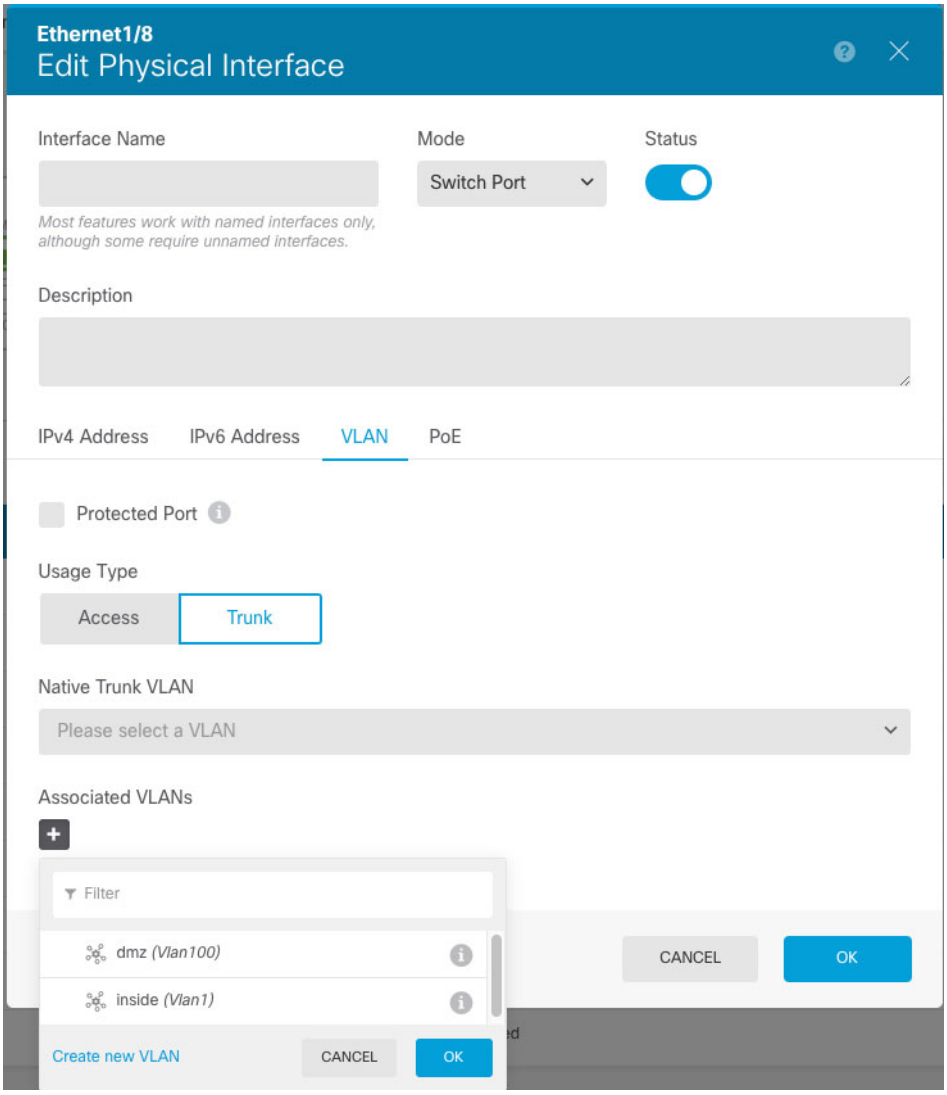
프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음, **Interfaces(**인터페이스**)** 요약의 링크를 클릭합니다.

기본적으로는 **Interfaces(**인터페이스**)** 페이지가 선택됩니다. 인터페이스 목록에는 물리적 인터페이스, 해당 이름, 주소 및 상태가 표시됩니다.

단계 **2** 수정할 실제 인터페이스의 수정 아이콘( )을 클릭합니다.

단계 **3** 다음을 설정합니다.



a) 스위치 포트에 대한 **Interface Name(**인터페이스 이름**)**은 설정하지 마십시오. 연결된 VLAN 인터페이스만 명명된 인터페이스입니다.

b) **Mode(**모드**)**를 **Switch Port(**스위치 포트**)**로 설정합니다.

c) **Status(**상태**)** 슬라이더를 활성화된 설정( )으로 지정합니다.

d) (선택 사항) **Description(**설명**)**을 설정합니다.

설명은 줄 바꿈 없이 1줄, 최대 200자로 작성할 수 있습니다.

단계 **4** **VLAN**을 클릭하여 다음을 설정합니다.

a) (선택 사항) **Protected Port(**보호된 포트**)** 확인란을 선택하여 이 스위치 포트를 보호된 상태로 설정합니다. 그러면 스위치 포트가 동일한 VLAN에서 보호되는 다른 스위치 포트와 통신하는 것을 방지할 수 있습니다.

스위치 포트의 디바이스가 주로 다른 VLAN에서 액세스되어 VLAN 간 액세스를 허용할 필요가 없으며 감염 또는 기타 보안 침입 시 디바이스를 서로 분리하려는 경우 스위치 포트가 서로 통신하지 못하도록 할 수 있습니다. 예를 들어 세 개의 웹 서버를 호스팅하는 DMZ가 있는 경우, 이 옵션을 각 스위치 포트에 적용하면 웹 서버를 서로 분리할 수 있습니다. 내부 및 외부 네트워크 둘 다 세 개의 웹 서버와 통신할 수 있지만 웹 서버 간에 서로 통신할 수는 없습니다.

b) **Usage Type(**사용 유형**)**에서 **Trunk(**트렁크**)**를 클릭합니다.

c) (선택 사항) **Native Trunk VLAN(**기본 트렁크 **VLAN)**의 경우, 아래쪽 화살표를 클릭하여 네이티브 VLAN에 대해 기존의 VLAN 인터페이스 중 하나를 선택합니다.

기본 네이티브 VLAN ID는 1입니다.

각 포트에는 하나의 네이티브 VLAN만 있을 수 있지만, 모든 포트의 네이티브 VLAN은 같거나 다를 수 있습니다.

Create new VLAN(새 **VLAN** 생성**)**을 클릭하여 새 VLAN 인터페이스를 추가할 수 있습니다. VLAN 인터페이스 구성, 282 페이지의 내용을 참조하십시오.

d) **Associated VLAN(**연결된 **VLAN)**의 경우, 더하기 아이콘(+)을 클릭하여 기존의 VLAN 인터페이스를 하나 이상 선택합니다.

이 필드에 네이티브 VLAN을 포함하는 경우 해당 VLAN은 무시됩니다. 트렁크 포트에서는 포트 외부로 네이티브 VLAN 트래픽을 전송할 때 항상 VLAN 태깅을 제거합니다. 뿐만 아니라, 이렇게 한 후에도 네이티브 VLAN 태깅이 있는 트래픽은 수신하지 않습니다.

Create new VLAN(새 **VLAN** 생성**)**을 클릭하여 새 VLAN 인터페이스를 추가할 수 있습니다. VLAN 인터페이스 구성, 282 페이지의 내용을 참조하십시오.

단계 **5** **OK(**확인**)**를 클릭합니다.

PoE(Power over Ethernet) 구성

Ethernet1/7 및 Ethernet1/8에서는 IP 전화기 또는 무선 액세스 포인트와 같은 디바이스에 대해 PoE(Power over Ethernet)를 지원합니다. Firepower 1010에서는 IEEE 802.3af(PoE) 및 802.3at(PoE+)을 모두 지원합니다. PoE+에서는 LLDP(Link Layer Discovery Protocol)를 사용하여 전력 레벨을 협상합니다. PoE+에서는 전력 디바이스에 최대 30와트를 제공할 수 있습니다. 전원은 필요한 경우에만 제공됩니다.

인터페이스를 종료한 경우 디바이스의 전원을 비활성화합니다.

PoE는 Ethernet1/7 및 Ethernet1/8에서 기본적으로 활성화되어 있습니다. 이 절차에서는 PoE를 비활성화하는 방법과 활성화하는 방법, 파라미터(선택 사항)를 설정하는 방법을 설명합니다.

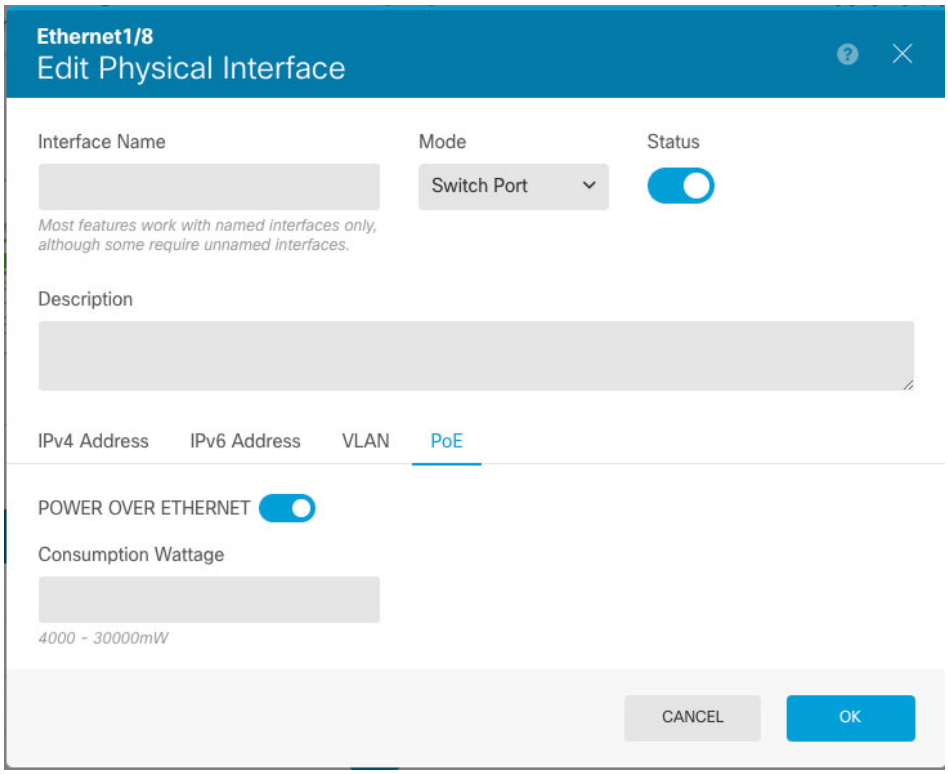
프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음, **Interfaces(**인터페이스**)** 요약의 링크를 클릭합니다.

기본적으로는 **Interfaces(**인터페이스**)** 페이지가 선택됩니다. 인터페이스 목록에는 물리적 인터페이스, 해당 이름, 주소 및 상태가 표시됩니다.

단계 **2** Ethernet1/7 또는 1/8에 대해 수정 아이콘( )을 클릭합니다.

단계 **3** **PoE**를 클릭하고 다음을 설정합니다.



a) **PoE(Power over Ethernet)**를 활성화하려면 슬라이더( )를 클릭하여 활성화합니다.

PoE는 기본적으로 활성화되어 있습니다.

b) (선택 사항) 필요한 전력량을 정확히 알고 있는 경우 **Consumption Wattage(**소비 전력량**)**를 입력합니다.

기본적으로 PoE에서는 전력 디바이스의 클래스에 적절한 전력량을 사용하여 전력 디바이스에 전원을 자동으로 제공합니다. Firepower 1010에서는 LLDP를 사용하여 정확한 전력량을 추가로 협상합니다. 특정 전력량을 알고 있으며 LLDP 협상을 비활성화하려는 경우 4,000~30,000 밀리와트의 값을 입력합니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

VLAN 하위 인터페이스 및 802.1Q 트렁킹 구성

VLAN 하위 인터페이스를 사용하면 실제 인터페이스를 각기 다른 VLAN ID로 태그가 지정된 여러 논리적 인터페이스로 분할할 수 있습니다. 하나 이상의 VLAN 하위 인터페이스가 포함된 인터페이스는 자동으로 802.1Q 트렁크로 구성됩니다. VLAN을 사용하면 정해진 실제 인터페이스에서 트래픽을 따로 유지할 수 있으므로, 실제 인터페이스 또는 디바이스를 더 추가하지 않고 네트워크에 사용 가능한 인터페이스 수를 늘릴 수 있습니다.

스위치의 트렁크 포트에 물리적 인터페이스를 연결하는 경우 하위 인터페이스를 생성합니다. 스위치 트렁크 포트에 표시될 수 있는 각 VLAN에 대해 하위 인터페이스를 생성합니다. 스위치의 액세스 포트에 물리적 인터페이스를 연결하는 경우 하위 인터페이스를 생성할 필요가 없습니다.

지침 및 제한 사항

- 물리적 인터페이스의 태그 지정되지 않은 패킷 방지 — 하위 인터페이스를 사용할 경우, 일반적으로 물리적 인터페이스에서 트래픽을 전달하지 않도록 하고자 합니다. 물리적 인터페이스에서는 태그 지정되지 않은 패킷을 전달하기 때문입니다. 하위 인터페이스에서 트래픽을 전달하려면 실제 인터페이스를 활성화해야 하므로, 인터페이스의 이름을 지정하지 않는 방법을 통해 실제 인터페이스가 트래픽을 전달하지 않도록 해야 합니다. 실제 인터페이스에서 태그가 지정되지 않은 패킷을 전달할 수 있도록 하려면 일반적인 방식으로 인터페이스 이름을 지정하면 됩니다.
- Firepower 1010 - 하위 인터페이스는 스위치 포트 또는 VLAN 인터페이스에서 지원되지 않습니다.
- 브리지 그룹 멤버 인터페이스에서는 IP 주소를 구성할 수 없습니다. 그러나 필요에 따라 고급 설정을 수정할 수는 있습니다.
- 동일한 상위 인터페이스에 있는 모든 하위 인터페이스는 브리지 그룹 멤버 또는 라우팅 인터페이스 중 하나여야 하며 이를 혼합하고 일치시킬 수 없습니다.
- Threat Defense에서는 DTP(Dynamic Trunking Protocol)를 지원하지 않으므로 조건 없이 트렁킹을 수행할 연결된 스위치 포트를 구성해야 합니다.
- threat defense 디바이스에 정의된 하위 인터페이스에서 상위 인터페이스의 번인된(burned-in) MAC 주소와 동일한 주소를 사용하므로 이 하위 인터페이스에 고유한 MAC 주소를 할당해야 할 수 있습니다. 이를테면 서비스 공급자가 MAC 주소를 기준으로 액세스 제어를 수행하려 합니다. 또한 IPv6 링크 로컬 주소는 MAC 주소에 근거하여 생성되므로 하위 인터페이스에 고유한 MAC 주소를 할당하면 고유한 IPv6 링크 로컬 주소를 사용할 수 있습니다. 이에 따라 threat defense 디바이스의 특정 인스턴스에서 트래픽이 중단되는 것을 방지할 수 있습니다.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음, **Interfaces(**인터페이스**)** 요약의 링크를 클릭합니다.

기본적으로는 **Interfaces(**인터페이스**)** 페이지가 선택됩니다. EtherChannel에 하위 인터페이스를 추가하려면 **EtherChannel**을 클릭합니다. 인터페이스 목록에는 물리적 인터페이스, 해당 이름, 주소 및 상태가 표시됩니다.

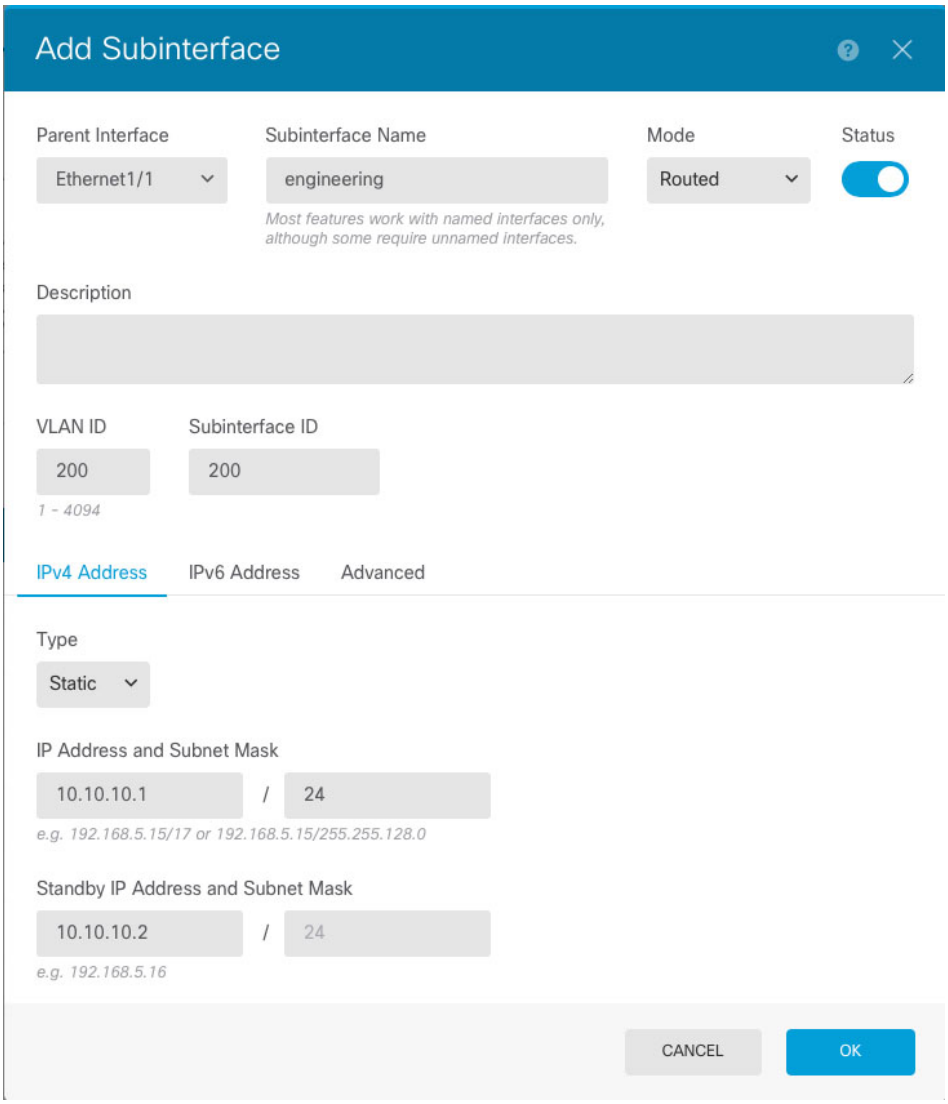
단계 **2** 다음 중 하나를 수행합니다.

- **Interfaces(**인터페이스**)** 페이지에서 더하기 아이콘(+)을 클릭하여 새 하위 인터페이스를 생성합니다.
- **EtherChannel** 페이지에서 더하기 및 아래쪽 화살표 아이콘(+ˇ)을 클릭하고 **Subinterface(**하위 인터페이스**)**를 선택합니다.
- 수정할 하위 인터페이스의 수정 아이콘(✎)을 클릭합니다.

하위 인터페이스가 더 이상 필요하지 않은 경우, 해당 하위 인터페이스의 삭제 아이콘(🗑)을 클릭하여 삭제합니다.

단계 **3** **Status(**상태**)** 슬라이더를 활성화된 설정(⬤)으로 지정합니다.

단계 **4** 상위 인터페이스, 이름 및 설명을 구성합니다.



a) **Parent Interface(**상위 인터페이스**)**를 선택합니다.

상위 인터페이스는 하위 인터페이스를 추가할 물리적 인터페이스입니다. 하위 인터페이스를 생성한 후에는 상위 인터페이스를 변경할 수 없습니다.

b) **Subinterface Name(**하위 인터페이스 이름**)**이름을 최대 48자로 설정합니다.

영문자는 소문자로 입력해야 합니다. 예를 들면 **inside** 또는 **outside**와 같이 입력합니다. 이름을 입력하지 않으면 나머지 인터페이스 컨피그레이션이 무시됩니다.

참고 이름을 변경하는 경우 보안 영역, syslog 서버 개체, DHCP 서버 정의 등 이전 이름을 사용했던 모든 위치에서 변경 사항이 자동으로 반영됩니다. 그러나 해당 이름을 사용하는 모든 컨피그레이션을 먼저 제거해야 이름을 제거할 수 있습니다. 일반적으로는 정책이나 설정에 대해 이름이 없는 인터페이스를 사용할 수 없기 때문입니다.

c) **Mode(**모드**)**를 **Routed(**라우팅**)**로 설정합니다.

나중에 이 인터페이스를 브리지 그룹에 추가하면 모드가 자동으로 **BridgeGroupMember**로 변경됩니다. 브리지 그룹 멤버 인터페이스에서는 IP 주소를 구성할 수 없습니다.

d) (선택 사항) **Description(**설명**)**을 설정합니다.

설명은 줄 바꿈 없이 1줄, 최대 200자로 작성할 수 있습니다.

e) **VLAN ID**를 설정합니다.

이 하위 인터페이스에서 패킷에 태그를 지정하는 데 사용할 1~4094의 VLAN ID를 입력합니다.

f) **Subinterface ID(**하위 인터페이스 **ID)**를 설정합니다.

하위 인터페이스 ID를 1~4294967295의 정수로 입력합니다. 이 ID는 인터페이스 ID에 추가됩니다(예: Ethernet1/1.100). 편의를 위해 VLAN ID를 일치시킬 수 있으나 꼭 그렇게 해야 하는 것은 아닙니다. 하위 인터페이스를 생성한 후에는 ID를 변경할 수 없습니다.

단계 **5** **IPv4 Address(IPv4** 주소**)** 탭을 클릭하고 IPv4 주소를 구성합니다.

Type(유형**)** 필드에서 다음 옵션 중 하나를 선택합니다.

- **DHCP** — 네트워크의 DHCP 서버에서 주소를 가져와야 하는 경우 이 옵션을 선택합니다. 고가용성을 구성하는 경우 이 옵션을 사용할 수 없습니다. 필요에 따라 다음 옵션을 변경합니다.
  - **Route Metric(**경로 메트릭**)** - DHCP 서버에서 기본 경로를 가져오는 경우 확인된 경로까지의 관리 거리(1~255)입니다. 기본값은 1입니다.
  - **Obtain Default Route(**기본 경로 얻기**)** - DHCP 서버에서 기본 경로를 가져올지 여부를 선택합니다. 일반적으로는 이 옵션을 선택합니다(기본값).
- **Static(**고정**)** - 변경되면 안 되는 주소를 할당하려면 이 옵션을 선택합니다. 인터페이스에 연결된 네트워크에 대해 인터페이스의 IP 주소와 서브넷 마스크를 입력합니다. 예를 들어 10.100.10.0/24 네트워크를 연결하는 경우 10.100.10.1/24를 입력할 수 있습니다. 주소가 네트워크에서 이미 사용되고 있지 않은지 확인합니다.

  고가용성을 구성했으며 이 인터페이스에서 HA를 모니터링하는 중이라면 같은 서브넷에 스탠바이 IP 주소도 구성합니다. 스탠바이 디바이스의 이 인터페이스에서 스탠바이 주소를 사용합니다. 스탠바이 IP 주소를 설정하지 않으면 액티브 유닛이 네트워크 테스트를 사용하여 스탠바이 인터페이스를 모니터링할 수 없으며 링크 상태만 추적할 수 있습니다.

  참고 인터페이스에 대해 구성된 DHCP 서버가 있을 경우, 해당 컨피그레이션이 표시됩니다. DHCP 주소 풀을 수정하거나 삭제할 수 있습니다. 인터페이스 IP 주소를 다른 서브넷으로 변경할 경우, 인터페이스 변경 사항을 저장하려면 우선 DHCP 서버를 삭제하거나, 새 서브넷에서 주소 풀을 구성해야 합니다. DHCP 서버 설정, 819 페이지의 내용을 참조하십시오.

- **PPPoE** — PPPoE(Point-to-Point Protocol over Ethernet)를 사용하여 주소를 가져와야 하는 경우 이 옵션을 선택합니다. 인터페이스가 DSL 모뎀이나 케이블 모뎀에 연결되어 있거나 기타 ISP 연결을 사용하고 ISP에서 PPPoE를 사용하여 IP 주소를 제공하는 경우, PPPoE가 필요할 수 있습니다. 고가용성을 구성하는 경우 이 옵션을 사용할 수 없습니다. 다음 값을 설정합니다.
  - **Group Name(**그룹 이름**)** — 이 연결을 나타내는 그룹 이름을 원하는 대로 지정합니다.

- **PPPoE Username(PPPoE** 사용자 이름**)** — ISP에서 제공한 사용자 이름을 지정합니다.
- **PPPoE Password(PPPoE** 비밀번호**)** — ISP에서 제공한 비밀번호를 지정합니다.
- **PPP Authentication(PPP** 인증**) - PAP**, **CHAP**, 또는**MSCHAP**를 선택합니다.

  PAP에서는 인증이 진행되는 동안 일반 텍스트 사용자 이름 및 비밀번호를 전달하므로 안전하지 않습니다. CHAP를 사용하면 클라이언트에서는 서버 챌린지에 대한 응답으로 암호화된 [challenge plus password]와 함께 일반 텍스트로 된 사용자 이름을 반환합니다. CHAP는 PAP보다 안전하지만 데이터가 암호화되지 않습니다. MSCHAP는 CHAP와 유사하지만, CHAP의 일반 텍스트로 비밀번호와 달리 서버에서 암호화된 비밀번호만 저장하고 비교하므로 훨씬 안전합니다. MSCHAP에서도 MPPE를 통해 데이터 암호화용 키를 생성합니다.
- **PPPoE Learned Route Metric(PPPoE** 학습된 경로 메트릭**)** — 학습된 경로에 관리 거리를 할당합니다. 유효한 값은 1 ~ 255입니다. 파악된 경로의 기본 관리 거리는 1입니다.
- **Obtain Default Route from PPPoE(PPPoE**에서 기본 경로 가져오기**)** — PPPoE 서버에서 기본 경로를 가져오려면 이 확인란을 선택합니다.
- **IP Address Type(IP** 주소 유형**)** — PPPoE 서버에서 IP 주소를 가져오려면 **Dynamic(**동적**)**을 선택합니다. 또는 ISP에서 정적 IP 주소를 할당한 경우 **Static(**정적**)**을 선택할 수 있습니다.

단계 **6** (선택 사항). **IPv6 Address(IPv6** 주소**)** 탭을 클릭하고 IPv6 주소를 구성합니다.

- **Sate(**상태**) -** 글로벌 어드레스를 구성하지 않는 경우 IPv6 처리를 활성화하고 링크-로컬 주소를 자동으로 구성하려면 **Enabled(**활성화됨**)**를 선택합니다. 링크 로컬 주소는 인터페이스 MAC 주소(수정된 EUI-64 형식)를 기반으로 생성됩니다.

  참고 IPv6를 비활성화해도 명시적 IPv6 주소로 구성되었거나 자동 컨피그레이션용으로 활성화된 인터페이스에서 IPv6 처리가 비활성화되지는 않습니다.

- **Address Auto Configuration(**주소 자동 컨피그레이션**) -** 주소를 자동으로 구성하려면 이 옵션을 선택합니다. IPv6 스테이트리스 자동 컨피그레이션에서는 디바이스가 있는 링크에 IPv6 서비스를 제공하도록 구성된 라우터가 있는 경우에만 글로벌 IPv6 주소를 생성합니다. 이러한 서비스에는 링크에서 사용할 IPv6 글로벌 접두사 알림이 포함됩니다. 링크에서 IPv6 라우팅 서비스를 사용할 수 없는 경우에는 링크-로컬 IPv6 주소만 제공됩니다. 디바이스의 직접 네트워크 링크 외부에서는 이 주소에 액세스할 수 없습니다. 링크 로컬 주소는 수정된 EUI-64 인터페이스 ID를 기반으로 합니다.

  RFC 4862에서는 스테이트리스 자동 컨피그레이션에 대해 구성한 호스트에서 라우터 알림 메시지를 전송하지 않도록 지정하지만, 이 경우에는 threat defense 디바이스에서 라우터 알림 메시지를 전송합니다. 메시지를 표시하지 않고 RFC를 준수하려면 **RA** 표시 안 함을 선택합니다.
- **Static Address/Prefix(**고정 주소/접두사**) -** 스테이트리스 자동 컨피그레이션을 사용하지 않는 경우 전체 고정 글로벌 IPv6 주소와 네트워크 접두사를 입력합니다. 예를 들어, 2001:0DB8::BA98:0:3210/48와 같이 입력합니다. IPv6 주소 지정에 대한 자세한 내용은 IPv6 주소 지정, 258 페이지를 참조하십시오.

주소를 링크 로컬 전용으로 사용하려는 경우 링크-로컬 옵션을 선택합니다. 로컬 네트워크 외부에서는 링크 로컬 주소에 액세스할 수 없습니다. 브리지 그룹 인터페이스에서는 링크-로컬 주소를 구성할 수 없습니다.

참고 링크-로컬 주소는 FE8, FE9, FEA 또는 FEB로 시작해야 합니다(예: fe80::20d:88ff:feee:6a82). Modified EUI-64 형식으로 링크-로컬 주소를 자동으로 지정하는 것이 좋습니다. 만약 다른 디바이스에서 Modified EUI-64 형식을 강제 적용하는 경우 수동으로 지정된 링크-로컬 주소 때문에 패킷이 폐기될 수 있습니다.

- **Standby IP Address(**스탠바이 **IP** 주소**)** - 고가용성을 구성하는 경우 이 인터페이스에서 HA를 모니터링하는 중이라면 같은 서브넷에 스탠바이 IPv6 주소도 구성합니다. 스탠바이 디바이스의 이 인터페이스에서 스탠바이 주소를 사용합니다. 스탠바이 IP 주소를 설정하지 않으면 액티브 유닛이 네트워크 테스트를 사용하여 스탠바이 인터페이스를 모니터링할 수 없으며 링크 상태만 추적할 수 있습니다.
- **Suppress RA(RA** 표시 안 함**)** - 라우터 알림을 표시하지 않을지를 선택합니다. threat defense는 인접 디바이스가 기본 라우터 주소를 동적으로 학습할 수 있도록 라우터 알림에 참여할 수 있습니다. 기본적으로 라우터 알림 메시지(ICMPv6 유형 134)는 IPv6가 구성된 각 인터페이스에 주기적으로 전송됩니다.

  라우터 광고는 라우터 요청 메시지에 대한 응답으로도 보내집니다(ICMPv6 Type 133). 예정된 다음 라우터 광고 메시지를 기다릴 필요 없이 호스트가 즉시 자동 구성을 할 수 있도록 시스템 시동 시 라우터 요청 메시지가 전송됩니다.

  threat defense 디바이스에서 IPv6 접두사를 제공하지 않도록 하려는 인터페이스(예: 외부 인터페이스)에서는 이러한 메시지를 표시하지 않을 수 있습니다.

단계 **7** (선택 사항). 고급 옵션 구성, 304 페이지에 전달하는 고성능 고속 어플라이언스입니다.

고급 설정에는 대부분의 네트워크에 적합한 기본값이 있습니다. 네트워크 문제를 해결하는 경우에만 이러한 기본값을 수정하십시오.

단계 **8** **OK(**확인**)**를 클릭합니다.

다음에 수행할 작업

- 적절한 보안 영역에 하위 인터페이스를 추가합니다. 보안 영역 구성, 152 페이지의 내용을 참조하십시오.
- 동적 DNS 서비스 제공자에 FQDN(Fully Qualified Domain Name)을 등록하고 DNS 서버가 IPv4 및 IPv6 인터페이스 주소로 업데이트되도록 DDNS를 설정합니다. 동적 DNS 구성, 823 페이지의 내용을 참조하십시오.

패시브 인터페이스 구성

패시브 인터페이스는 스위치 SPAN(Switched Port Analyzer) 또는 미러 포트를 사용하여 네트워크를 통과하는 트래픽을 모니터링합니다. SPAN 또는 미러 포트를 사용하면 스위치의 다른 포트에서 트래픽을 복사할 수 있습니다. 이 기능을 사용하면 네트워크 트래픽의 플로우 내에 있지 않더라도 시스템 가시성이 확보됩니다.

패시브 구축으로 구성된 시스템은 트래픽 차단 등의 특정 작업을 수행할 수 없습니다. 패시브 인터페이스는 모든 트래픽을 조건 없이 수신하며 이러한 인터페이스에서 수신된 트래픽은 재전송되지 않습니다.

패시브 인터페이스를 사용하여 네트워크의 트래픽을 모니터링해 트래픽에 대한 정보를 수집합니다. 예를 들어 침입 정책을 적용해 네트워크에 피해를 주는 위협 유형을 파악하거나 사용자가 보내는 웹 요청의 URL 카테고리를 확인할 수 있습니다. 다양한 보안 정책과 규칙을 구현하여 시스템이 능동적으로 구축될 때 어떤 작업을 수행할지 확인할 수 있습니다. 그러면 시스템이 액세스 제어 규칙과 기타 규칙에 따라 트래픽을 삭제할 수 있습니다.

그러나 패시브 인터페이스는 트래픽에 영향을 줄 수 없으므로 여러 가지 컨피그레이션 제한이 적용됩니다. 이러한 인터페이스를 사용하는 시스템은 트래픽을 확인할 수만 있으며, 패시브 인터페이스로 들어가는 패킷은 디바이스에서 나가지 않습니다.

다음 주제에서는 패시브 인터페이스 및 패시브 인터페이스 구성 방법을 더 자세히 설명합니다.

패시브 인터페이스를 사용하는 이유

패시브 인터페이스를 사용하는 주요 목적은 단순 데모 모드를 제공하기 위해서입니다. 단일 소스 포트를 모니터링하도록 스위치를 설정한 다음 워크스테이션을 사용하여 패시브 인터페이스가 모니터링하는 테스트 트래픽을 전송할 수 있습니다. 그러므로 threat defense 시스템에서 어떻게 연결을 평가하고 위협을 식별하는지 등을 확인할 수 있습니다. 시스템의 작업 수행 방식에 만족하는 경우 네트워크에서 해당 컨피그레이션을 능동적으로 구축하고 패시브 인터페이스 컨피그레이션은 제거할 수 있습니다.

하지만 다음 서비스를 제공 하기 위해 프로덕션 환경에서 패시브 인터페이스를 사용할 수도 있습니다.

- 순수 IDS 구축 - 시스템을 방화벽이나 IPS(Intrusion Detection System)로 사용하지 않으려는 경우 패시브 방식을 통해 IDS(Intrusion Detection System)로 구축할 수 있습니다. 이 구축 방법에서는 액세스 제어 규칙을 사용하여 모든 트래픽에 침입 정책을 적용합니다. 시스템이 스위치의 여러 소스 포트를 모니터링하도록 지정할 수도 있습니다. 그리고 나면 대시보드를 사용하여 네트워크에서 확인되는 위협을 모니터링할 수 있습니다. 그러나 이 모드에서는 이러한 위협을 방지하기 위해 시스템이 어떤 작업도 수행할 수 없습니다.
- 혼합 구축 - 액티브 라우팅 인터페이스와 패시브 인터페이스를 같은 시스템에서 함께 사용할 수 있습니다. 즉 일부 네트워크에서는 threat defense 디바이스를 방화벽으로 구축하고 다른 네트워크에서는 트래픽을 모니터링하도록 하나 이상의 수동 인터페이스를 컨피그레이션할 수 있습니다.

패시브 인터페이스에 대한 제한 사항

패시브 모드 인터페이스로 정의하는 모든 물리적 인터페이스에는 다음 제한이 적용됩니다.

- 패시브 인터페이스에서는 하위 인터페이스를 구성할 수 없습니다.
- 브리지 그룹에는 패시브 인터페이스를 포함할 수 없습니다.
- 패시브 인터페이스에서는 IPv4 또는 IPv6 주소를 구성할 수 없습니다.
- 패시브 인터페이스에서는 Management Only(관리 전용) 옵션을 선택할 수 없습니다.
- 패시브 인터페이스는 패시브 모드 보안 영역에만 포함할 수 있으며 라우팅 보안 영역에는 포함할 수 없습니다.
- 액세스 제어 또는 ID 규칙의 소스 기준에 패시브 보안 영역을 포함할 수 있습니다. 대상 기준에는 패시브 영역을 사용할 수 없습니다. 동일한 규칙에서 패시브 영역과 라우팅 영역을 함께 사용할 수 없습니다.
- 패시브 인터페이스에서는 관리 액세스 규칙(HTTPS 또는 SSH)을 구성할 수 없습니다.
- NAT 규칙에 패시브 인터페이스를 사용할 수 없습니다.
- 패시브 인터페이스에서는 정적 경로를 구성할 수 없습니다. 라우팅 프로토콜 컨피그레이션에서는 패시브 인터페이스를 사용할 수 없습니다.
- 패시브 인터페이스에서는 DHCP 서버를 구성할 수 없습니다. 패시브 인터페이스를 사용하여 자동 컨피그레이션을 통해 DHCP 설정을 획득할 수 없습니다.
- syslog 서버 컨피그레이션에 패시브 인터페이스를 사용할 수 없습니다.
- 패시브 인터페이스에서는 어떤 유형의 VPN도 구성할 수 없습니다.

하드웨어 **Threat Defense** 패시브 인터페이스용 스위치 구성

하드웨어 threat defense 디바이스의 수동 인터페이스는 네트워크 스위치를 정확하게 컨피그레이션해야만 작동합니다. 다음 절차는 Cisco Nexus 5000 Series 스위치를 기준으로 합니다. 다른 유형의 스위치를 사용하는 경우에는 명령이 달라질 수 있습니다.

기본적으로는 SPAN(Switched Port Analyzer) 또는 미러 포트를 구성하고, 해당 포트에 패시브 인터페이스를 연결하고, 하나 이상의 소스 포트에서 SPAN 또는 미러 포트로 트래픽 복사본을 전송하도록 스위치에서 모니터링 세션을 구성합니다.

프로시저

단계 **1** 스위치의 포트를 모니터(SPAN 또는 미러) 포트로 구성합니다.

```
switch(config)# interface Ethernet1/48
switch(config-if)# switchport monitor
```

```
switch(config-if)#
```

단계 **2** 모니터링할 포트를 식별하는 모니터링 세션을 정의합니다.

SPAN 또는 미러 포트를 대상 포트로 정의해야 합니다. 다음 예시에서는 소스 포트 2개를 모니터링합니다.

```
switch(config)# monitor session 1
switch(config-monitor)# source interface ethernet 1/7
switch(config-monitor)# source interface ethernet 1/8
switch(config-monitor)# destination interface ethernet 1/48
switch(config-monitor)# no shut
```

단계 **3** (선택 사항). **show monitor session** 명령을 사용하여 컨피그레이션을 확인합니다.

다음 예시에서는 세션 1의 간략한 출력이 나와 있습니다.

```
switch# show monitor session 1 brief
   session 1
---------------
type               : local
state              : up
source intf        :
    rx             : Eth1/7        Eth1/8
    tx             : Eth1/7        Eth1/8
    both           : Eth1/7        Eth1/8
source VSANs       :
destination ports  : Eth1/48

Legend: f = forwarding enabled, l = learning enabled
```

단계 **4** threat defense 수동 인터페이스에서 스위치의 목적지 포트에 케이블을 물리적으로 연결합니다.

물리적 연결 전이나 후에 인터페이스를 패시브 모드로 구성할 수 있습니다. 패시브 모드로 물리적 인터페이스 구성, 301 페이지의 내용을 참조하십시오.

Threat Defense Virtual 패시브 인터페이스의 VLAN 구성

threat defense virtual 디바이스의 수동 인터페이스는 가상 네트워크의 VLAN을 정확하게 컨피그레이션해야만 작동합니다. 이를 위해 다음 작업을 수행해야 합니다.

- 무차별 모드에서 컨피그레이션한 VLAN에 threat defense virtual 인터페이스를 연결합니다. 그런 다음 패시브 모드로 물리적 인터페이스 구성, 301 페이지에서 설명한 대로 인터페이스를 구성합니다. 패시브 인터페이스에는 프로미스큐어스 VLAN의 모든 트래픽 복사본이 표시됩니다.
- 동일한 VLAN에 가상 Windows 시스템 등의 엔드포인트 디바이스를 하나 이상 연결합니다. VLAN에서 인터넷으로의 연결이 있는 경우 단일 디바이스를 사용할 수 있습니다. 그렇지 않은 경우에는 트래픽을 전달할 수 있는 둘 이상의 디바이스가 필요합니다. URL 카테고리에 대한 데이터를 가져오려면 인터넷 연결이 필요합니다.

패시브 모드로 물리적 인터페이스 구성

인터페이스를 패시브 모드로 구성할 수 있습니다. 인터페이스는 패시브 방식으로 작동할 때 스위치 자체(하드웨어 디바이스의 경우) 또는 프로미스큐어스 VLAN(threat defense virtual의 경우)에 구성된 모니터링 세션에서 소스 포트의 트래픽만 모니터링합니다. 스위치 또는 가상 네트워크에서 구성해야 하는 항목에 대한 세부 정보는 다음 주제를 참조하십시오.

- 하드웨어 Threat Defense 패시브 인터페이스용 스위치 구성, 299 페이지
- Threat Defense Virtual 패시브 인터페이스의 VLAN 구성, 300 페이지

트래픽에 영향을 주지 않고 모니터링되는 스위치 포트를 통해 들어오는 트래픽을 분석하려는 경우 패시브 모드를 사용합니다. 패시브 모드를 사용하는 전체 예시는 네트워크에서 트래픽을 능동적으로 모니터링하는 방법, 79 페이지의 내용을 참조하십시오.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭하고 **Interfaces(**인터페이스**)** 요약의 링크를 클릭한 다음, **Interfaces** 또는 **EtherChannel**을 클릭합니다.

단계 **2** 수정할 물리적 인터페이스 또는 EtherChannel의 수정 아이콘( )을 클릭합니다.

현재 사용되지 않는 인터페이스를 선택합니다. 사용 중인 인터페이스를 패시브 인터페이스로 변환하려는 경우 먼저 모든 보안 영역에서 인터페이스를 제거하고 해당 인터페이스를 사용하는 다른 모든 컨피그레이션을 제거해야 합니다.

단계 **3** **Status(**상태**)** 슬라이더를 활성화된 설정( )으로 지정합니다.

단계 **4** 다음을 구성합니다.

- **Interface Name(**인터페이스 이름**)** - 인터페이스의 이름(최대 48자)입니다. 영문자는 소문자로 입력해야 합니다. 예를 들어 monitor를 입력합니다.
- **Mode(**모드**)** - **Passive(**패시브**)**를 선택합니다.
- (선택 사항). **Description(**설명**)** - 설명은 줄바꿈 없이 1줄, 최대 200자로 작성합니다.

참고 IPv4 또는 IPv6 주소는 구성할 수 없습니다. Advanced(고급) 탭에서는 MTU, 이중 및 속도 설정만 변경할 수 있습니다.

단계 **5** **OK(**확인**)**를 클릭합니다.

다음에 수행할 작업

인터페이스에 표시되는 트래픽에 대한 정보를 대시보드에 채워 넣으려면 패시브 인터페이스를 생성하는 것만으로는 부족합니다. 다음 작업도 수행해야 합니다. 사용 사례에서 이러한 단계를 살펴봅니다. 네트워크에서 트래픽을 능동적으로 모니터링하는 방법, 79 페이지의 내용을 참조하십시오.

- 패시브 보안 영역을 생성하고 인터페이스를 해당 영역에 추가합니다. 보안 영역 구성, 152 페이지의 내용을 참조하십시오.
- 패시브 보안 영역을 소스 영역으로 사용하는 액세스 제어 규칙을 생성합니다. 일반적으로는 이러한 규칙에 침입 정책을 적용하여 IDS(Intrusion Detection System) 모니터링을 구현합니다. 액세스 제어 정책 구성, 530 페이지의 내용을 참조하십시오.
- 선택적으로 패시브 보안 영역용 SSL 암호 해독 및 ID 규칙을 생성하고 보안 인텔리전스 정책을 활성화합니다.

고급 인터페이스 옵션 구성

고급 옵션으로는 MTU, 하드웨어 설정, 관리 전용, MAC 주소 및 기타 설정이 있습니다.

MAC 주소 정보

MAC(Media Access Control) 주소를 수동으로 구성하여 기본값을 재정의할 수 있습니다.

고가용성 컨피그레이션의 경우, 인터페이스에 대해 액티브 및 스탠바이 MAC 주소를 모두 구성할 수 있습니다. 액티브 유닛이 페일오버하고 스탠바이 유닛이 활성화되면 새 액티브 유닛은 액티브 MAC 주소를 사용하기 시작하므로 네트워크 중단이 최소화됩니다.

기본 MAC 주소

기본 MAC 주소 할당은 인터페이스의 유형에 따라 다릅니다.

- 물리적 인터페이스 - 물리적 인터페이스는 버닝된 MAC 주소를 사용합니다.
- VLAN 인터페이스(Firepower 1010) - 모든 VLAN 인터페이스에서 MAC 주소를 공유합니다. 연결된 스위치가 이 시나리오에 도움이 될 수 있을지 확인하십시오. 연결된 스위치에 고유한 MAC 주소가 필요한 경우, MAC 주소를 수동으로 할당할 수 있습니다. 고급 옵션 구성, 304 페이지의 내용을 참조하십시오.
- EtherChannel - EtherChannel의 경우 채널 그룹에 속한 모든 인터페이스가 동일한 MAC 주소를 공유합니다. 이 기능은 EtherChannel을 네트워크 애플리케이션 및 사용자에게 투명하게 만듭니다. 이들은 논리적 연결만 볼 수 있으며, 개별 링크에 대해서는 모르기 때문입니다. 포트 채널 인터페이스는 풀의 고유 MAC 주소를 사용하며 인터페이스 멤버십은 MAC 주소에 영향을 주지 않습니다.
- 하위 인터페이스 - 물리적 인터페이스의 모든 하위 인터페이스에서도 동일한 번인된(burned-in) MAC 주소를 사용합니다. 하위 인터페이스에 고유한 MAC 주소를 할당할 수 있습니다. 이를테면 서비스 공급자가 MAC 주소를 기준으로 액세스 제어를 수행하려 합니다. 또한 IPv6 링크 로컬 주소는 MAC 주소에 근거하여 생성되므로 하위 인터페이스에 고유한 MAC 주소를 할당하면 고유한 IPv6 링크 로컬 주소를 사용할 수 있습니다. 이에 따라 threat defense의 특정 인스턴스에서 트래픽이 중단되는 것을 방지할 수 있습니다.

MTU 정보

MTU에서는 위협 방지 디바이스가 지정된 이더넷 인터페이스에서 전송할 수 있는 최대 프레임 페이로드 크기를 지정합니다. MTU 값은 이더넷 헤더, VLAN 태깅 또는 기타 오버헤드가 없는 프레임 크기입니다. 예를 들어, MTU를 1500으로 설정할 경우 예상 프레임 크기는 헤더 포함 시 1518바이트이고 VLAN 사용 시에는 1522입니다. 이러한 헤더를 수용하기 위해 MTU 값을 이보다 더 높게 설정하지 마십시오.

경로 MTU 검색

위협 방지 디바이스에서는 경로 MTU 검색을 지원하며(RFC 1191에 규정), 이 기능을 사용하면 두 호스트 간의 네트워크 경로에 있는 모든 디바이스에서 MTU를 조율할 수 있으므로, 경로의 최저 MTU에 대한 표준을 설정할 수 있습니다.

MTU 및 단편화

IPv4의 경우 지정된 MTU보다 큰 발신 IP 패킷은 2개 이상의 프레임으로 단편화됩니다. 분할된 패킷은 목적지(또는 일부 경우 중간 홉에서)에서 다시 합쳐지며, 분할이 일어날 경우 성능이 저하될 수 있습니다. IPv6의 경우에는 일반적으로 패킷의 단편화가 전혀 허용되지 않습니다. 따라서 분할을 방지하려면 IP 패킷이 MTU 크기 내에 맞아야 합니다.

UDP 또는 ICMP의 경우 애플리케이션은 단편화 방지를 위해 MTU를 고려해야 합니다.

참고 위협 방지 디바이스에서는 메모리에 공간이 있는 한 구성된 MTU보다 큰 프레임을 수신할 수 있습니다.

MTU와 점보 프레임

큰 MTU를 사용하는 경우 더 큰 패킷을 전송할 수 있습니다. 큰 패킷은 네트워크에서 더욱 효율적으로 사용할 수 있습니다. 다음 지침을 참조하십시오.

- 트래픽 경로의 MTU 일치 — 모든 threat defense 인터페이스 및 기타 디바이스 인터페이스의 MTU를 트래픽 경로와 동일하게 설정하는 것이 좋습니다. MTU를 일치시키면 패킷 분할 시 디바이스가 중간에 끼어드는 현상을 방지할 수 있습니다.
- 점보 프레임 수용 - 점보 프레임은 최대 표준 1522바이트(레이어 2 헤더 및 VLAN 헤더 포함)보다 큰 이더넷 패킷이며, 최대 9216바이트에 이릅니다. 점보 프레임을 수용하기 위해 MTU를 9000바이트 이상으로 설정할 수 있습니다. 최대값은 모델에 따라 다릅니다.

참고 MTU를 늘리면 점보 프레임에 더 많은 메모리가 할당되므로 액세스 규칙 등 다른 기능의 최대 사용량이 제한될 수 있습니다. threat defense virtual에서 MTU를 기본값인 1500 이상으로 늘리는 경우에는 시스템을 재부팅해야 합니다. 고가용성을 위해 디바이스를 컨피그레이션한 경우, 스탠바이 디바이스도 재부팅해야 합니다. 점보 프레임 지원이 항상 활성화되어 있는 다른 모델은 재부팅하지 않아도 됩니다.

고급 옵션 구성

고급 인터페이스 옵션에는 대부분의 네트워크에 적합한 기본 설정이 있습니다. 네트워킹 문제를 해결하는 경우 또는 고가용성을 구성하는 경우에만 이러한 설정을 구성하십시오.

다음 절차에서는 인터페이스가 이미 정의되어 있다고 가정합니다. 인터페이스를 처음 수정하거나 생성할 때 이러한 설정을 수정할 수도 있습니다.

제한 사항

- 브리지 그룹의 경우에는 멤버 인터페이스에서 이러한 옵션 중 대부분을 구성합니다. DAD 시도 및 Enable for HA Monitoring(HA 모니터링에 대해 활성화)를 제외하고 이러한 옵션을 BVI(Bridge Virtual Interface)에 사용할 수 없습니다.
- 에서는 관리 인터페이스의 MTU, 듀플렉스 또는 속도를 설정할 수 없습니다.
- Firepower 1010 스위치 포트에는 고급 옵션을 사용할 수 없습니다.
- Firepower 4100/9300에서는 인터페이스의 듀플렉스 또는 속도를 설정할 수 없습니다. FXOS를 사용하여 인터페이스에 대해 이러한 기능을 설정합니다.
- 패시브 인터페이스의 경우 MTU, 이중 및 속도만 설정할 수 있으며 인터페이스 관리만 수행할 수는 없습니다.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭하고 **Interfaces(**인터페이스**)** 요약의 링크를 클릭한 다음, 인터페이스 유형을 클릭하여 인터페이스 목록을 확인합니다.

단계 **2** 수정할 인터페이스의 수정 아이콘( )을 클릭합니다.

단계 **3** **Advanced Options(**고급 옵션**)**를 클릭합니다.

단계 **4** 시스템에서 고가용성 컨피그레이션의 피어 유닛으로 페일오버를 수행할지 여부를 결정할 때 인터페이스 상태를 고려하려면 **Enable for HA Monitoring(HA** 모니터링에 대해 활성화**)**을 선택합니다.

이 옵션은 고가용성을 구성하지 않는 경우 무시되며 인터페이스의 이름을 구성하지 않는 경우에도 무시됩니다.

단계 **5** 데이터 인터페이스 관리만 수행하려면 **Management Only(**관리만**)**를 선택합니다.

관리 전용 인터페이스에서는 통과 트래픽을 허용하지 않으므로 데이터 인터페이스를 관리 전용으로 설정할 때 사용할 수 있는 값은 거의 없습니다. 관리/진단 인터페이스(항상 관리 전용)의 경우에는 이 설정을 변경할 수 없습니다.

단계 **6** Cisco Trustsec을 활성화하려면 **Propagate Security Group Tag(**보안 그룹 태그 전파**)**를 선택합니다.

물리적, 하위 인터페이스, EtherChannel, VLAN, 관리 또는 BVI 인터페이스(명명 여부에 관계없이)에서 Cisco Trustsec을 활성화하거나 비활성화할 수 있습니다. 기본적으로 Cisco Trustsec은 인터페이스의 이름을 지정할 때 자동으로 활성화됩니다.

단계 **7** **MTU**(Maximum Transmission Unit)를 원하는 값으로 변경합니다.

기본 MTU는 1500바이트입니다. 최소값과 최대값은 플랫폼에 따라 다릅니다. 네트워크에서 대개 점보 프레임이 표시되면 높은 값을 설정합니다.

참고 ISA 3000 Series 디바이스 또는 threat defense virtual에서 MTU를 1500보다 큰 값으로 늘리는 경우에는 디바이스를 재부팅해야 합니다. 고가용성을 위해 디바이스를 컨피그레이션한 경우, 스탠바이 디바이스도 재부팅해야 합니다. 점보 프레임 지원이 항상 활성화되어 있는 다른 모델은 재부팅하지 않아도 됩니다.

단계 **8** (실제 인터페이스만 해당됨) 속도 및 이중 설정을 수정합니다.

기본적으로 인터페이스는 연결 반대쪽의 인터페이스와 최적의 이중 및 속도를 협상하지만, 필요한 경우 특정 이중이나 속도를 강제 적용할 수 있습니다. 나열된 옵션은 인터페이스에서 지원하는 유일한 옵션입니다. 네트워크 모듈의 인터페이스에 이러한 옵션을 설정하기 전에 인터페이스 컨피그레이션에 대한 제한 사항, 259 페이지의 내용을 읽어보십시오.

- **Duplex(**듀플렉스**)** — **Half(**하프**)** 또는 **Full(**풀**)**을 선택합니다. SFP 인터페이스는 풀 듀플렉스만 지원합니다.
- **Speed(**속도**)** - 속도(모델에 따라 다름)를 선택합니다. (Secure Firewall 3100만 해당) 설치된 SFP 모듈의 속도를 탐지하고 적절한 속도를 사용하려면 **Detect SFP(SFP** 탐지**)**를 선택합니다. Duplex(듀플렉스)는 항상 Full(풀)이며 자동 협상은 항상 활성화되어 있습니다. 이 옵션은 나중에 네트워크 모듈을 다른 모델로 변경하고 속도를 자동으로 업데이트하려는 경우에 유용합니다.
- **Auto Negotiation(**자동 협상**)** - 속도, 링크 상태 및 흐름 제어를 협상하도록 인터페이스를 설정합니다. 1000Mbps 미만의 속도에서는 이 설정을 수정할 수 없습니다. SFP 인터페이스의 경우 속도가 1000Mbps로 설정된 경우에만 자동 협상을 비활성화할 수 있습니다.
- 전달 오류 수정 모드 - (Secure Firewall 3100만 해당) 25Gbps 이상의 인터페이스에서는 전달 오류 수정을 활성화합니다. EtherChannel 멤버 인터페이스의 경우, 이를 EtherChannel에 추가하기 전에 전달 오류 수정을 구성해야 합니다.

단계 **9** **IPv6** 컨피그레이션 설정을 수정합니다.

- **IPv6** 주소 컨피그레이션에 **DHCP** 활성화 - IPv6 라우터 알림 패킷에서 관리 주소 컨피그레이션 플래그를 설정할지 여부를 선택합니다. 이 플래그는 IPv6 자동 컨피그레이션 클라이언트에게 DHCPv6를 사용하여 파생된 스테이트리스 자동 컨피그레이션 주소 이외의 주소도 얻도록 안내합니다.

- **IPv6** 비주소 컨피그레이션에 **DHCP** 활성화 - IPv6 라우터 알림 패킷에서 기타 주소 컨피그레이션 플래그를 설정할지 여부를 선택합니다. 이 플래그는 IPv6 자동 컨피그레이션 클라이언트에게 DHCPv6를 사용하여 DHCPv6로부터 추가 정보(예: DNS 서버 주소)를 얻도록 안내합니다.
- **DAD** 시도 - 인터페이스가 DAD(Duplicate Address Detection)를 수행하는 빈도를 0~600 사이의 값으로 설정합니다. 기본값은 1입니다. 스테이트리스 자동 컨피그레이션 프로세스에서 DAD는 새로운 유니캐스트 IPv6 주소가 고유한지 확인한 다음 주소를 인터페이스에 할당합니다. 중복 주소가 인터페이스의 링크-로컬 주소인 경우 인터페이스의 IPv6 패킷 처리가 사용 해제됩니다. 중복 주소가 전역 주소인 경우 주소가 사용되지 않습니다. 인터페이스에서는 네이버 요청 메시지를 사용하여 DAD를 수행합니다. DAD(Duplicate Address Detection) 처리를 비활성화하려면 값을 0으로 설정합니다.

단계 **10** (선택 사항, 하위 인터페이스 및 고가용성 유닛의 경우 권장함.) MAC 주소를 구성합니다.

시스템은 기본적으로 인터페이스에 대해 NIC(Network Interface Card)에 버닝된 MAC 주소를 사용합니다. 따라서 인터페이스의 모든 하위 인터페이스는 같은 MAC 주소를 사용하므로 하위 인터페이스별로 고유한 주소를 생성할 수 있습니다. 고가용성을 구성하는 경우에는 액티브/스탠바이 MAC 주소도 수동으로 구성하는 것이 좋습니다. MAC 주소를 정의하면 페일오버 시 네트워크에서 일관성을 유지할 수 있습니다.

- **MAC Address(MAC** 주소**)** - H.H.H. 형식의 MAC(Media Access Control) 주소입니다. 여기서 H는 16비트 16진수입니다. 예를 들어 MAC 주소 00-0C-F1-42-4C-DE는 000C.F142.4CDE로 입력합니다. MAC 주소에는 멀티캐스트 비트를 설정해서는 안 됩니다(즉, 왼쪽에서 두 번째 16진수는 홀수일 수 없음).
- **Standby MAC Address(**스탠바이 **MAC** 주소**)** - 고가용성에 사용할 주소입니다. 액티브 유닛이 페일오버되고 스탠바이 유닛이 액티브 상태가 되면, 네트워크 중단을 최소화하기 위해 새 액티브 유닛에서 액티브 MAC 주소를 사용하기 시작하고 기존 액티브 유닛은 스탠바이 주소를 사용합니다.

단계 **11** **OK(**확인**)**를 클릭합니다.

인터페이스 변경 사항 스캔 및 인터페이스 마이그레이션

디바이스에서 인터페이스를 변경하면 디바이스에서 변경 사항이 발생했음을 device manager에 알립니다. 인터페이스 스캔을 수행할 때까지 구성을 구축할 수 없습니다. device manager에서는 보안 정책의 인터페이스를 다른 인터페이스로 마이그레이션할 수 있도록 지원하므로 인터페이스는 거의 완벽하게 제거될 수 있습니다.

인터페이스 스캐닝 및 마이그레이션 정보

스캔

디바이스에서 인터페이스를 변경하면 디바이스에서 변경 사항이 발생했음을 device manager에 알립니다. 인터페이스 스캔을 수행할 때까지는 구성을 구축할 수 없습니다. 추가, 제거 또는 복원된 인터

페이스를 탐지하는 스캔을 수행한 후에 구성을 구축할 수 있습니다. 그러나 제거된 인터페이스를 참조하는 구성 부분은 구축되지 않습니다.

스캔해야 할 인터페이스 변경 사항에는 인터페이스 추가 또는 제거 작업이 포함됩니다. 네트워크 모듈 변경, Firepower 4100/9300 섀시의 할당된 인터페이스 변경, threat defense virtual의 인터페이스 변경을 예로 들 수 있습니다.

다음과 같은 항목은 변경해도 스캔 후 구축이 차단되지 않습니다.

- 보안 영역 멤버십
- EtherChannel 인터페이스 멤버십
- Firepower 1010 VLAN 인터페이스 스위치 포트 멤버십
- BVI를 참조하는 정책에 대한 브리지 그룹 인터페이스 멤버십

참고 Syslog 서버 이그레스 인터페이스를 변경하면 구축이 차단되지는 않지만, 수동으로 또는 인터페이스 교체 기능을 사용하여 syslog 서버 구성을 수정해야 합니다.

마이그레이션

새 인터페이스를 추가하거나 사용하지 않는 인터페이스를 제거하는 경우 threat defense 구성에 미치는 영향은 아주 적습니다. 그러나 보안 정책에 사용되는 인터페이스를 제거하면 구성에 영향이 미칩니다. 보안 영역, NAT, VPN, 라우팅, DHCP 서버 등 threat defense 구성의 여러 위치에서 인터페이스를 직접 참조할 수 있습니다.

Device Manager 에서는 보안 정책의 인터페이스를 다른 인터페이스로 마이그레이션할 수 있도록 지원하므로 인터페이스는 거의 완벽하게 제거될 수 있습니다.

참고 마이그레이션 기능을 사용하는 경우에는 이름, IP 주소 및 기타 구성이 한 인터페이스에서 다른 인터페이스로 복사되지 않으며, 기존 인터페이스 대신 새 인터페이스를 참조하도록 보안 정책이 변경됩니다. 마이그레이션하기 전에 새 인터페이스 설정을 수동으로 구성해야 합니다.

인터페이스를 제거해야 하는 경우, 제거하기 전에 새 인터페이스를 추가하고 기존 인터페이스를 마이그레이션하는 것이 좋습니다. 동시에 인터페이스를 추가하고 제거하는 경우에도 마이그레이션 프로세스는 계속 진행됩니다. 그러나 이를 참조하는 제거된 인터페이스 또는 정책을 수동으로 수정할 수는 없으므로 마이그레이션을 단계별로 수행하는 것이 더 쉬울 수 있습니다.

인터페이스를 동일한 유형으로 대체하는 경우(예: 네트워크 모듈을 RMA해야 하는 경우)에는 다음 작업을 수행할 수 있습니다. 1. 섀시에서 이전 모듈을 제거합니다. 2. 스캔을 수행합니다. 3. 제거된 인터페이스와 관련이 없는 변경 사항을 구축합니다. 4. 모듈을 교체합니다. 5. 새 스캔을 수행합니다. 6. 인터페이스와 관련된 모든 변경 사항을 비롯하여 구성을 구축합니다. 새 인터페이스에의 인터페이스 ID와 특성이 이전 인터페이스와 동일한 경우에는 마이그레이션을 수행할 필요가 없습니다.

인터페이스 스캐닝 및 마이그레이션에 대한 지침 및 제한 사항

지원되지 않는 인터페이스 마이그레이션

- BVI에 대한 물리적 인터페이스
- 방화벽 인터페이스에 대한 패시브 인터페이스
- 브리지 그룹 멤버
- EtherChannel 인터페이스 멤버
- ISA 3000 하드웨어 우회 멤버
- Firepower 1010 VLAN 인터페이스 또는 스위치 포트
- 진단 인터페이스
- HA 장애 조치 및 상태 링크
- 다른 유형의 인터페이스 마이그레이션(예: 브리지 그룹 인터페이스를 물리적 인터페이스가 필요한 기능으로 마이그레이션)

추가 지침

- 인터페이스를 제거해야 하는 경우, 제거하기 전에 새 인터페이스를 추가하고 기존 인터페이스를 마이그레이션하는 것이 좋습니다.
- threat defense virtual의 경우 인터페이스 목록 끝에 인터페이스만 추가하고 제거합니다. 다른 곳에서 인터페이스를 추가하거나 제거하는 경우, 하이퍼바이저에서는 인터페이스의 번호를 다시 매깁니다. 그 결과 구성에서 인터페이스 ID가 잘못된 인터페이스에 맞춰 정렬됩니다.
- 스캔/마이그레이션이 잘못된 경우, 새시에서 원래 인터페이스를 복원한 후 다시 스캔하여 원래 상태로 돌아갑니다.
- 백업의 경우 새 인터페이스를 사용하여 새 백업을 생성하십시오. 이전 구성으로 복원하면 이전 인터페이스 정보가 복원되며 스캔/교체를 다시 수행해야 합니다.
- HA의 경우, 액티브 유닛에서 인터페이스 스캔을 수행하기 전에 두 유닛에서 인터페이스를 동일하게 변경합니다. 액티브 유닛에서 스캔/마이그레이션만 수행하면 됩니다. 구성 변경 사항은 스탠바이 유닛에 복제됩니다.

인터페이스 스캔 및 마이그레이션

device manager에서 인터페이스 변경 사항을 스캔하고 제거된 인터페이스에서 인터페이스 구성을 마이그레이션합니다. 인터페이스 구성만 마이그레이션하려는 경우(및 스캔이 필요하지 않은 경우), 스캐닝과 관련된 다음 절차의 단계를 무시합니다.

참고 마이그레이션 기능을 사용하는 경우에는 이름, IP 주소 및 기타 구성이 한 인터페이스에서 다른 인터페이스로 복사되지 않으며, 기존 인터페이스 대신 새 인터페이스를 참조하도록 보안 정책이 변경됩니다. 마이그레이션하기 전에 새 인터페이스 설정을 수동으로 구성해야 합니다.

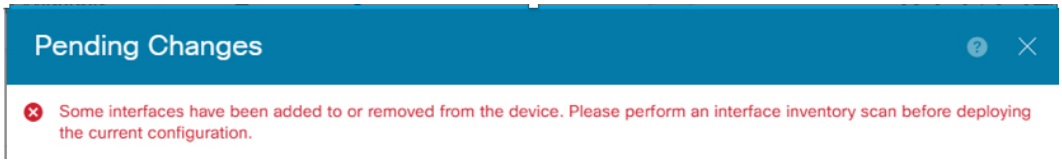
프로시저

단계 **1** 섀시에서 인터페이스를 추가하거나 제거합니다.

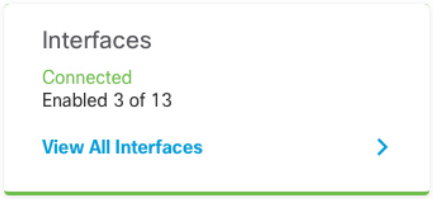
인터페이스를 제거해야 하는 경우, 제거하기 전에 새 인터페이스를 추가하고 기존 인터페이스를 교체하는 것이 좋습니다.

단계 **2** 인터페이스 변경 사항을 스캔합니다.

인터페이스 스캔을 수행할 때까지는 구성을 구축할 수 없습니다. 스캔 전에 구축을 시도하는 경우 다음 오류가 표시됩니다.

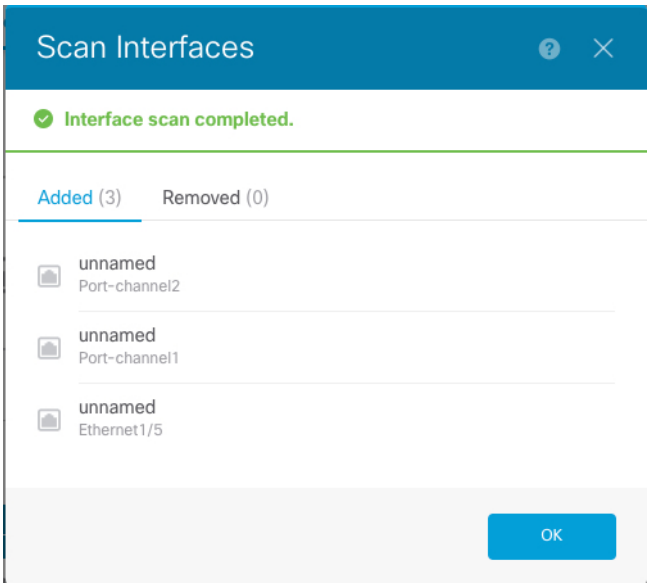


a) **Device(**디바이스**)**를 클릭한 다음, **Interfaces(**인터페이스**)** 요약에서 **View All Interfaces(**모든 인터페이스 보기**)** 링크를 클릭합니다.

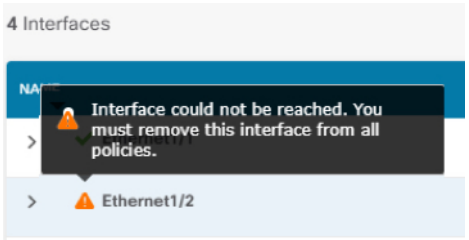


b) Scan Interfaces(인터페이스 스캔) 아이콘( )을 클릭합니다.

c) 인터페이스가 스캔될 때까지 기다린 다음, **OK(**확인**)**를 클릭합니다.



스캔 후에는 제거된 인터페이스가 다음과 같이 주의 기호와 함께 Interfaces(인터페이스) 페이지에 표시됩니다.



단계 **3** 기존 인터페이스를 새 인터페이스로 마이그레이션하려면 다음을 수행합니다.

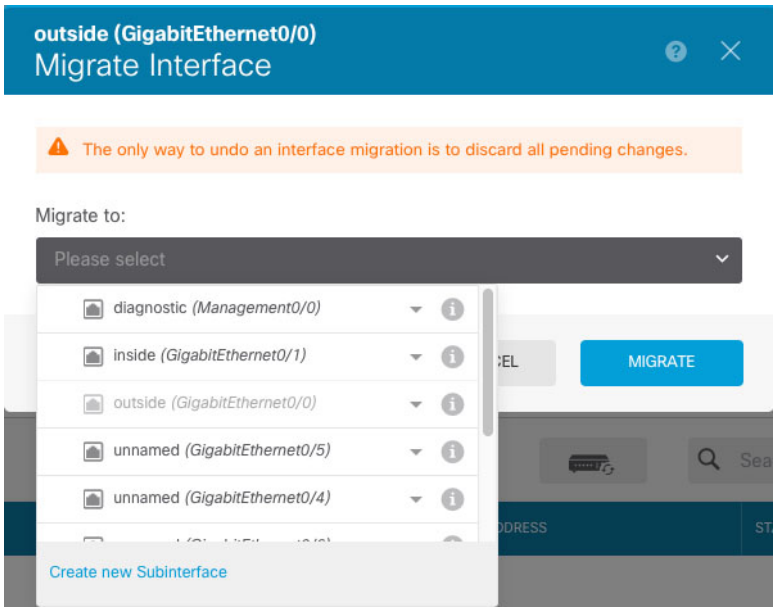
a) 이름, IP 주소 등을 사용하여 새 인터페이스를 구성합니다.

제거할 인터페이스의 기존 IP 주소 및 이름을 사용하려는 경우에는 먼저 새 인터페이스에서 해당 설정을 사용할 수 있도록 기존 인터페이스를 더미 이름 및 IP 주소로 다시 구성해야 합니다.

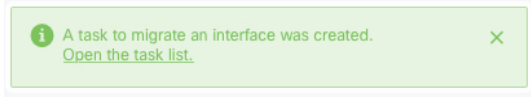
b) 기존 인터페이스의 Migrate(마이그레이션) 아이콘을 클릭합니다.

이 프로세스를 수행하면 인터페이스를 참조하는 모든 구성 설정에서 기존 인터페이스가 새 인터페이스로 마이그레이션됩니다.

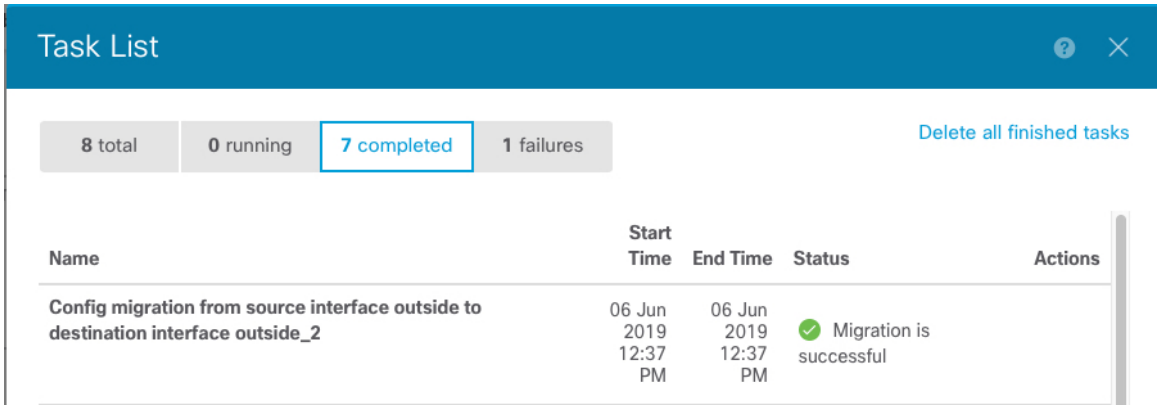
c) **Migrate to:(**마이그레이션 대상**:)** 드롭다운 목록에서 새 인터페이스를 선택합니다.



d) **Interfaces(**인터페이스**)** 페이지에 메시지가 나타납니다. 메시지에서 링크를 클릭합니다.



e) **Task List(**작업 목록**)**를 확인하여 마이그레이션에 성공했는지 확인합니다.

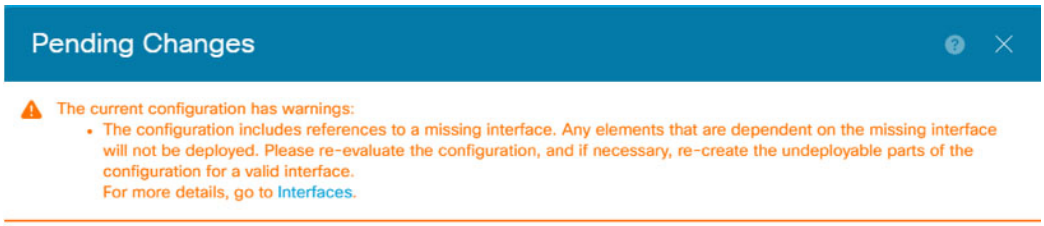


f) 마이그레이션에 실패하면 API Explorer에서 원인을 확인할 수 있습니다.

API Explorer를 열려면 More options(추가 옵션) 버튼( )을 클릭하고 **API Explorer**를 선택합니다. **Interface(**인터페이스**)** > **GET /jobs/interfacemigrations**를 선택한 다음, **Try it Out!(**시도**)**을 클릭합니다.

단계 **4** 구성을 구축합니다.

제거된 인터페이스를 참조하는 구성의 일부가 구축되지 않습니다. 이 경우 다음 메시지가 표시됩니다.



단계 **5** 섀시에서 이전 인터페이스를 제거하고 다른 스캔 작업을 수행합니다.

정책에서 더 이상 사용되지 않으며 제거된 인터페이스가 **Interfaces(**인터페이스**)** 페이지에서 제거됩니다.

단계 **6** 구성을 다시 구축하여 사용되지 않는 인터페이스를 구성에서 제거합니다.

Secure Firewall 3100용 네트워크 모듈 관리

방화벽의 전원을 켜기 전에 네트워크 모듈을 설치하는 경우에는 별도의 작업이 필요하지 않습니다. 네트워크 모듈이 활성화되었으며 사용할 준비가 되었습니다.

초기 부팅 후 네트워크 모듈 설치를 변경해야 하는 경우 다음 절차를 참조하십시오.

브레이크아웃 포트 구성

각 40GB 이상의 인터페이스에 대해 10GB 분할 포트를 구성할 수 있습니다. 이 절차에서는 포트를 분리하고 다시 조인하는 방법을 설명합니다. 브레이크아웃 포트는 EtherChannel에 추가되는 것을 포함하여 다른 물리적 이더넷 포트와 마찬가지로 사용할 수 있습니다.

고가용성을 위해 액티브 유닛에서 이 절차를 수행합니다. 인터페이스 변경 사항은 다른 유닛에 복제됩니다.

시작하기 전에

- 지원되는 브레이크아웃 케이블을 사용해야 합니다. 자세한 내용은 하드웨어 설치 가이드를 참조하십시오.
- 인터페이스는 컨피그레이션에서 사용할 수 없습니다. 하위 인터페이스를 포함하거나 EtherChannel의 일부일 수 없습니다.
- 고가용성을 위해 인터페이스의 이름을 지정하거나, 활성화하거나, 고가용성을 모니터링할 수 없습니다.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음, **Interfaces(**인터페이스**)** 요약의 링크를 클릭합니다.

기본적으로는 **Interfaces(**인터페이스**)** 페이지가 선택됩니다. 인터페이스 목록에는 물리적 인터페이스, 해당 이름, 주소 및 상태가 표시됩니다.

단계 **2** 40GB 이상의 인터페이스에서 10GB 포트를 브레이크아웃하려면 인터페이스 오른쪽에 있는 브레이크아웃 아이콘( )을 클릭합니다.

확인 대화 상자에서 **OK(**확인**)**를 클릭합니다. 인터페이스가 사용 중인 경우 오류 메시지가 표시됩니다. 모든 사용 사례를 해결해야 브레이크아웃을 다시 시도할 수 있습니다. 예를 들어 다른 인터페이스를 사용하도록 구성을 마이그레이션할 수 있습니다.

예를 들어 Ethernet2/1 40GB 인터페이스를 분리하기 위해 결과 하위 인터페이스는 Ethernet2/1/1, Ethernet2/1/2, Ethernet2/1/3 및 Ethernet2/1/4로 식별됩니다.

인터페이스 그래픽에서 분리된 포트의 모양은 다음과 같습니다. 왼쪽 및 오른쪽 화살표를 클릭하여 브레이크아웃 포트 상태를 자세히 설명하는 페이지를 스크롤할 수 있습니다.

단계 **3** 브레이크아웃 포트에 다시 조인하려면 인터페이스 오른쪽에 있는 조인 아이콘( )을 클릭합니다.

확인 대화 상자에서 **OK(**확인**)**를 클릭합니다. 하위 포트가 사용 중인 경우 오류 메시지가 표시됩니다. 모든 사용 사례를 해결해야 다시 조인할 수 있습니다. 예를 들어 다른 인터페이스를 사용하도록 구성을 마이그레이션할 수 있습니다.

인터페이스의 모든 하위 포트에 다시 조인해야 합니다.

단계 **4** 구성을 구축합니다.

네트워크 모듈 추가

초기 부팅 후 방화벽에 네트워크 모듈을 추가하려면 다음 단계를 수행합니다. 새 모듈을 추가하려면 재부팅해야 합니다.

프로시저

단계 **1** 하드웨어 설치 가이드에 따라 네트워크 모듈을 설치합니다.

고가용성을 위해 두 유닛에 네트워크 모듈을 설치합니다.

단계 **2** 방화벽을 재부팅합니다. 시스템 리부팅 또는 종료, 885 페이지의 내용을 참조하십시오. 고가용성을 위해 스탠바이 유닛을 재부팅한 다음 스탠바이 유닛에서 이 절차의 나머지를 수행합니다.

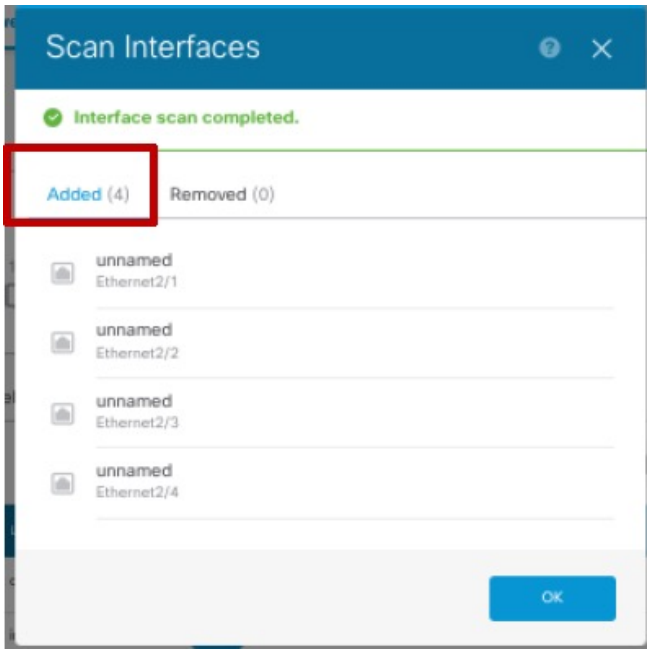
단계 **3** **Device(**디바이스**)**를 클릭한 다음, **Interfaces(**인터페이스**)** 요약에서 **View All Interfaces(**모든 인터페이스 보기**)** 링크를 클릭합니다.

그래픽은 인터페이스 스캔이 필요함을 보여줍니다.

그림 *14:* 인터페이스 스캔 필요

단계 **4** 새 네트워크 모듈 상세 정보로 페이지를 업데이트하려면 인터페이스 스캔을 클릭합니다. 인터페이스가 스캔될 때까지 기다린 다음, **OK(**확인**)**를 클릭합니다.

그림 *15:* 인터페이스 스캔

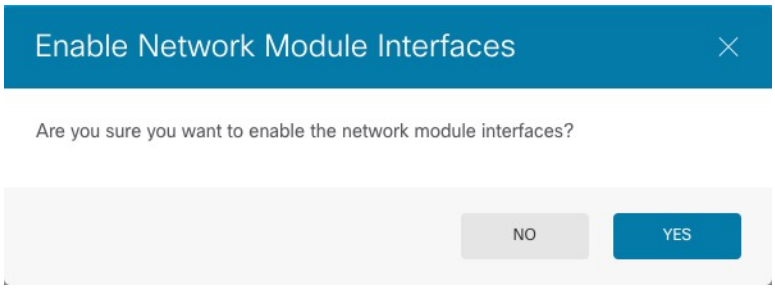


단계 **5** 인터페이스 그래픽에서 슬라이더( )를 클릭하여 네트워크 모듈을 활성화합니다.

그림 *16:* 네트워크 모듈 활성화

단계 **6** 네트워크 모듈을 켤지 확인하라는 메시지가 표시됩니다. **Yes(**예**)**를 클릭합니다.

그림 *17:* 사용 확인



단계 **7** 고가용성을 위해 액티브 유닛을 변경한 다음(액티브 및 스탠바이 피어 전환(강제 페일오버), 239 페이지 참조) 새 스탠바이 유닛에 대해 위의 단계를 수행합니다.

네트워크 모듈 핫 스왑

재부팅할 필요 없이 네트워크 모듈을 동일한 유형의 새 모듈로 핫 스왑할 수 있습니다. 그러나 안전하게 제거하려면 현재 모듈을 종료해야 합니다. 이 절차에서는 기존 모듈을 종료하고 새 모듈을 설치하고 활성화하는 방법을 설명합니다.

시작하기 전에

고가용성의 경우 페일오버 링크가 모듈에 있는 경우 네트워크 모듈을 비활성화할 수 없습니다. 고가용성을 해제해야 합니다(고가용성 해제, 238 페이지 참조). 모듈을 핫 스왑한 후 고가용성을 재편성할 수 있습니다.

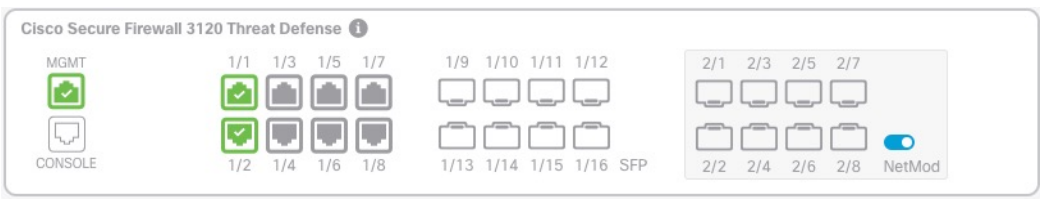
프로시저

단계 **1** 고가용성을 위해 핫 스왑을 수행할 유닛이 대기 노드인지 확인합니다. 액티브 및 스탠바이 피어 전환(강제 페일오버), 239 페이지를 참조하십시오.

단계 **2** **Device(**디바이스**)**를 클릭한 다음, **Interfaces(**인터페이스**)** 요약에서 **View All Interfaces(**모든 인터페이스 보기**)** 링크를 클릭합니다.

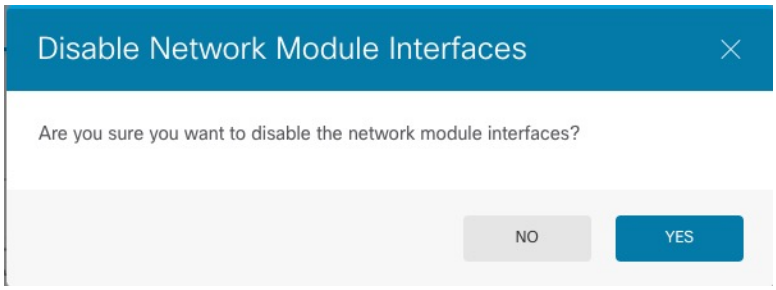
단계 **3** 인터페이스 그래픽에서 슬라이더( )를 클릭하여 네트워크 모듈을 비활성화합니다.

그림 *18:* 네트워크 모듈 비활성화



단계 **4** 네트워크 모듈을 끌지 확인하라는 메시지가 표시됩니다. **Yes(**예**)**를 클릭합니다.

그림 *19:* 사용 안 함 확인



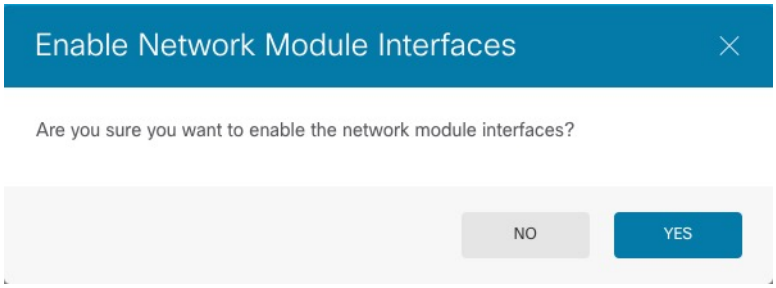
단계 **5** 하드웨어 설치 가이드에 따라 네트워크 모듈을 설치합니다.

단계 **6** 인터페이스 그래픽에서 슬라이더( )를 클릭하여 네트워크 모듈을 활성화합니다.

그림 *20:* 네트워크 모듈 활성화

단계 **7** 네트워크 모듈을 켤지 확인하라는 메시지가 표시됩니다. **Yes(**예**)**를 클릭합니다.

그림 *21:* 사용 확인



네트워크 모듈을 다른 유형으로 교체

네트워크 모듈을 다른 유형으로 교체하는 경우 재부팅해야 합니다. 새 모듈에 이전 모듈보다 인터페이스가 더 적은 경우 더 이상 존재하지 않을 인터페이스와 관련된 모든 구성을 수동으로 제거해야 합니다.

시작하기 전에

고가용성의 경우 페일오버 링크가 모듈에 있는 경우 네트워크 모듈을 비활성화할 수 없습니다. 고가용성을 해제해야 합니다(고가용성 해제, 238 페이지 참조). 즉, 액티브 유닛을 재부팅하면 다운타임이 발생합니다. 유닛 리부팅이 완료되면 고가용성을 재구성할 수 있습니다.

프로시저

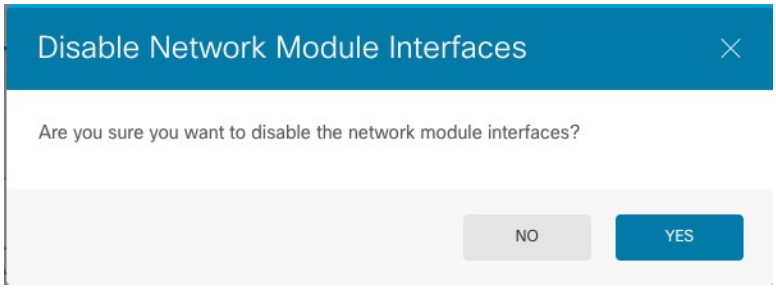
단계 **1** **Device(**디바이스**)**를 클릭한 다음, **Interfaces(**인터페이스**)** 요약에서 **View All Interfaces(**모든 인터페이스 보기**)** 링크를 클릭합니다. 고가용성을 위해 스탠바이 유닛에서 이 절차를 먼저 수행합니다.

단계 **2** 인터페이스 그래픽에서 슬라이더( )를 클릭하여 네트워크 모듈을 비활성화합니다.

그림 ***22:*** 네트워크 모듈 비활성화

단계 **3** 네트워크 모듈을 끌지 확인하라는 메시지가 표시됩니다. **Yes(**예**)**를 클릭합니다.

그림 ***23:*** 사용 안 함 확인

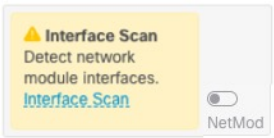


단계 **4** 디바이스에서 하드웨어 설치 가이드에 따라 기존 네트워크 모듈을 제거하고 새 네트워크 모듈로 교체합니다.

단계 **5** 방화벽을 재부팅합니다. 시스템 리부팅 또는 종료, 885 페이지의 내용을 참조하십시오.

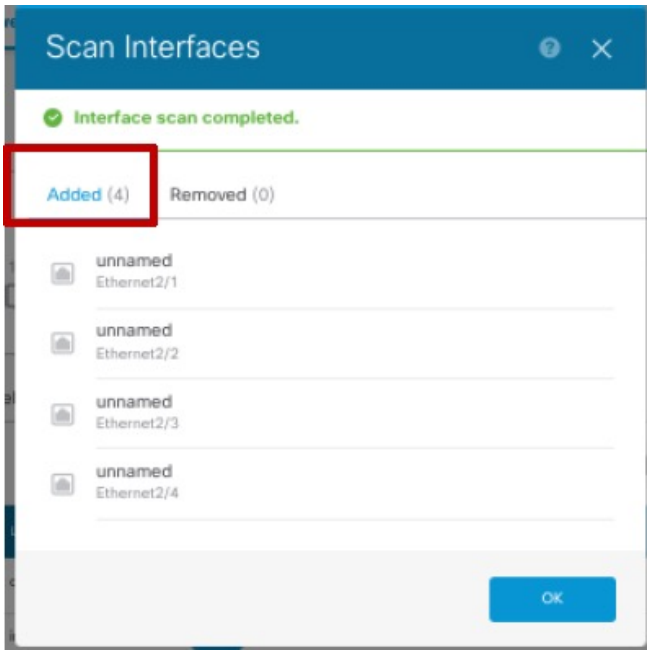
단계 **6** 인터페이스 페이지의 그래픽은 인터페이스 스캔이 필요함을 나타냅니다. 새 네트워크 모듈 상세 정보로 페이지를 업데이트하려면 인터페이스 스캔을 클릭합니다.

그림 ***24:*** 인터페이스 스캔 필요



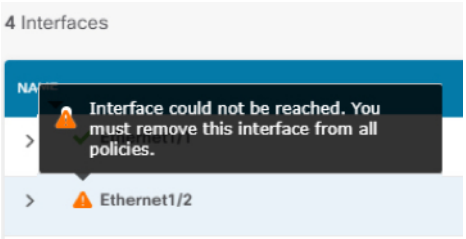
단계 **7** 인터페이스가 스캔될 때까지 기다린 다음, **OK(**확인**)**를 클릭합니다.

그림 *25:* 인터페이스 스캔



스캔 후에는 제거된 인터페이스가 다음과 같이 주의 기호와 함께 **Interfaces(**인터페이스**)** 페이지에 표시됩니다.

그림 *26:* 제거된 인터페이스



단계 **8** 네트워크 모듈의 인터페이스 수가 더 적은 경우 제거된 인터페이스를 직접 참조하는 모든 구성을 제거해야 합니다.

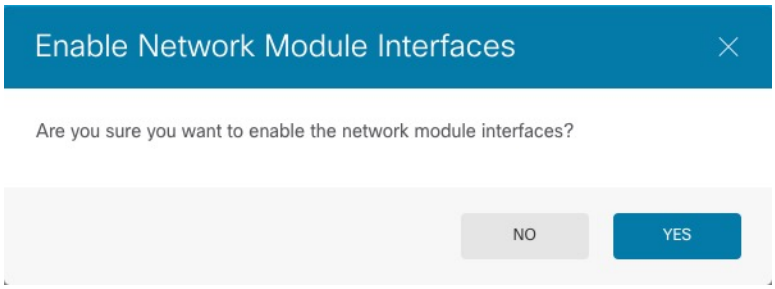
보안 영역을 참조하는 정책은 영향을 받지 않습니다. 선택적으로 구성을 다른 인터페이스로 마이그레이션할 수 있습니다. 인터페이스 스캔 및 마이그레이션, 308 페이지를 참조하십시오.

단계 **9** 인터페이스 그래픽에서 슬라이더( )를 클릭하여 네트워크 모듈을 활성화합니다.

그림 *27:* 네트워크 모듈 활성화

단계 **10** 네트워크 모듈을 켤지 확인하라는 메시지가 표시됩니다. **Yes(**예**)**를 클릭합니다.

그림 ***28:*** 사용 확인



단계 **11** 인터페이스 속도를 변경하려면 고급 옵션 구성, 304 페이지의 내용을 참조하십시오.

기본 속도는 설치된 SFP에서 올바른 속도를 탐지하는 Detect SFP(SFP 탐지)로 설정됩니다. 수동으로 속도를 특정 값으로 설정하고 이제 새 속도가 필요한 경우에만 속도를 수정해야 합니다.

단계 **12** 구성을 변경해야 하는 경우 구축 아이콘을 클릭합니다.

네트워크 모듈 변경 사항을 저장하기 위해 구축할 필요는 없습니다.

단계 **13** 고가용성을 위해 액티브 유닛을 변경한 다음(액티브 및 스탠바이 피어 전환(강제 페일오버), 239 페이지 참조) 새 스탠바이 유닛에 대해 위의 단계를 수행합니다.

네트워크 모듈 분리

네트워크 모듈을 영구적으로 제거하려면 다음 단계를 수행합니다. 네트워크 모듈을 제거하려면 재부팅해야 합니다.

시작하기 전에

고가용성의 경우 네트워크 모듈에 페일오버 링크가 없는지 확인하십시오.

프로시저

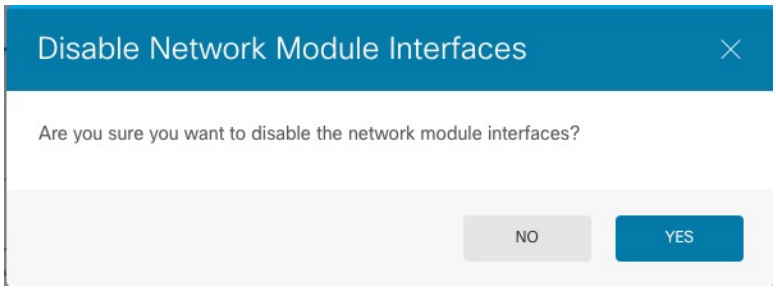
단계 **1** **Device(**디바이스**)**를 클릭한 다음, **Interfaces(**인터페이스**)** 요약에서 **View All Interfaces(**모든 인터페이스 보기**)** 링크를 클릭합니다. 고가용성을 위해 스탠바이 유닛에서 이 절차를 먼저 수행합니다.

단계 **2** 인터페이스 그래픽에서 슬라이더()를 클릭하여 네트워크 모듈을 비활성화합니다.

그림 *29:* 네트워크 모듈 비활성화

단계 **3** 네트워크 모듈을 끌지 확인하라는 메시지가 표시됩니다. **Yes(**예**)**를 클릭합니다.

그림 *30:* 사용 안 함 확인

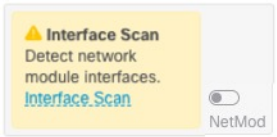


단계 **4** 방화벽에서 네트워크 모듈을 분리합니다.

단계 **5** 방화벽을 재부팅합니다. 시스템 리부팅 또는 종료, 885 페이지의 내용을 참조하십시오.

단계 **6** 인터페이스 페이지의 그래픽은 인터페이스 스캔이 필요함을 나타냅니다. 올바른 네트워크 모듈 상세 정보로 페이지를 업데이트하려면 인터페이스 스캔을 클릭합니다.

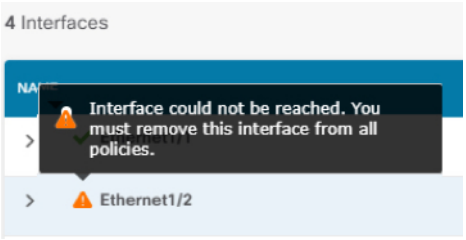
그림 *31:* 인터페이스 스캔 필요



단계 **7** 인터페이스가 스캔될 때까지 기다린 다음, **OK(**확인**)**를 클릭합니다.

스캔 후에는 제거된 인터페이스가 다음과 같이 주의 기호와 함께 **Interfaces(**인터페이스**)** 페이지에 표시됩니다.

그림 *32:* 제거된 인터페이스



단계 **8** 제거된 인터페이스를 직접 참조하는 모든 구성을 제거해야 합니다.

보안 영역을 참조하는 정책은 영향을 받지 않습니다. 선택적으로 구성을 다른 인터페이스로 마이그레이션할 수 있습니다. 인터페이스 스캔 및 마이그레이션, 308 페이지를 참조하십시오.

단계 **9** 구성을 변경해야 하는 경우 구축 아이콘을 클릭합니다.

네트워크 모듈 변경 사항을 저장하기 위해 구축할 필요는 없습니다.

단계 **10** 고가용성을 위해 액티브 유닛을 변경한 다음(액티브 및 스탠바이 피어 전환(강제 페일오버), 239 페이지 참조) 새 스탠바이 유닛에 대해 위의 단계를 수행합니다.

정전(ISA 3000)에 대한 하드웨어 우회 구성

정전 상태에서도 인터페이스 쌍 간에 트래픽 플로우가 계속되도록 하드웨어 바이패스를 활성화할 수 있습니다. 지원되는 인터페이스 쌍은 구리 인터페이스 GigabitEthernet 1/1과 1/2 및 GigabitEthernet 1/3과 1/4입니다. 파이버 이더넷 모델을 사용하는 경우에는 구리 이더넷 쌍(GigabitEthernet 1/1 및 1/2)만 하드웨어 바이패스를 지원합니다. 기본적으로 하드웨어 우회는 지원되는 경우 두 인터페이스 쌍 모두에 대해 활성화됩니다.

하드웨어 바이패스가 활성 상태이면 트래픽이 계층 1에서 이러한 인터페이스 쌍 간을 통과합니다. device manager 및 threat defense CLI는 인터페이스가 중단되는 것으로 간주합니다. 방화벽 기능은 없으므로 트래픽의 디바이스 통과를 허용하는 경우의 위험을 파악해야 합니다.

이 절차에서 설명하는 대로 TCP 시퀀스 번호 임의 설정을 비활성화하는 것이 좋습니다. 기본적으로 ISA 3000을 통과하는 TCP 연결의 ISN(초기 시퀀스 번호)는 임의의 숫자로 재작성됩니다. 하드웨어 바이패스를 활성화하면 ISA 3000은 더 이상 데이터 경로에 없으며 시퀀스 번호를 변환하지 않습니다. 수신 클라이언트는 예상치 않은 시퀀스 번호를 수신하므로 연결을 삭제합니다. 따라서 TCP 세션을 다시 설정해야 합니다. TCP 시퀀스 번호 임의 설정을 비활성화하더라도 전환 중에 일시적으로 중단되는 링크 때문에 일부 TCP 연결은 다시 설정해야 합니다.

CLI 콘솔 또는 SSH 세션에서 **show hardware-bypass** 명령을 사용하여 운영 상태를 모니터링합니다.

시작하기 전에

다음 조건을 충족해야 하드웨어 바이패스가 작동합니다.

- 같은 브리지 그룹에 인터페이스 쌍을 배치해야 합니다.
- 스위치의 액세스 포트에 인터페이스를 연결해야 합니다. 트렁크 포트에는 인터페이스를 연결하지 마십시오.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음 Interfaces(인터페이스) 요약의 링크를 클릭합니다.

페이지 상단에 있는 **Hardware Bypass(**하드웨어 우회**)** 섹션에서는 이 디바이스에 허용된 인터페이스 쌍의 현재 컨피그레이션을 표시합니다.

그러나 쌍이 동일한 브리지 그룹에 컨피그레이션되어 있는지 먼저 확인한 후에야 하드웨어 우회를 활성화할 수 있습니다.

단계 **2** **Edit(**수정**)**를 클릭하여 하드웨어 우회를 구성합니다.

Hardware Bypass Configuration(하드웨어 우회 컨피그레이션**)** 대화 상자가 나타납니다.

단계 **3** 자동 하드웨어 우회 동작을 구성하려면 각 인터페이스 쌍에 대해 **Hardware Bypass during Power Down(**정전 시 하드웨어 우회**)** 영역에서 다음 옵션 중 하나를 선택합니다.

- **Disable(**비활성화**)** — 하드웨어 우회를 비활성화합니다. 정전 시에는 트래픽이 디바이스를 통과하지 않습니다.
- **Enable(**활성화**)** — 정전 시 하드웨어 우회를 활성화합니다. 하드웨어 우회를 사용하면 정전 시에도 트래픽이 중단되지 않습니다. 우회된 트래픽은 검사되지 않으며 보안 정책이 적용되지 않습니다. 전원이 복구되면 하드웨어 우회가 자동으로 비활성화되므로 트래픽이 검사를 통해 정상적으로 통과할 수 있습니다. 하드웨어 우회가 비활성화되면 트래픽이 잠시 중단될 수 있습니다.
- **Enable with Persistence(**영구 활성화**)** — 정전 시 하드웨어 우회를 활성화하고 전력 복구 후에도 활성화 상태를 유지합니다. 전력이 복구되면 **Manual Hardware Bypass(**수동 하드웨어 우회**)** 슬라이더를 사용하여 하드웨어 우회를 비활성화해야 합니다. 이 옵션을 통해 트래픽이 일시 중단되는 시점을 제어할 수 있습니다.

단계 **4** (선택 사항) 하드웨어 우회를 수동으로 활성화하거나 또는 비활성화하려면 **Manual Hardware Bypass(**수동 하드웨어 우회**)** 슬라이더를 클릭합니다.

예를 들어 어떤 이유로 시스템을 테스트하거나 일시적으로 디바이스를 우회해야 할 경우가 있을 수 있습니다. 하드웨어 우회의 상태를 변경하려면 컨피그레이션을 구축해야 한다는 점에 유의하십시오. 설정을 변경하는 것만으로는 충분하지 않습니다.

하드웨어 바이패스를 수동으로 활성화/비활성화하면 다음 메시지가 표시됩니다. 여기서 *pair*는 1/1-1/2 또는 1/3-1/4입니다.

- %FTD-6-803002: GigabitEthernet 쌍을 통해 전송되는 트래픽은 시스템에서 보호하지 않습니다.
- %FTD-6-803003: 사용자가 GigabitEthernet 쌍에서 우회를 수동으로 비활성화했습니다.

단계 **5** **OK(**확인**)**를 클릭합니다.

변경 사항은 즉시 적용되지 않습니다. 컨피그레이션을 구축해야만 적용됩니다.

단계 **6** (선택 사항). TCP 시퀀스 번호 임의 설정을 비활성화하는 데 필요한 FlexConfig 개체 및 정책을 생성합니다.

a) **Device(**디바이스**)** > **Advanced Configuration(**고급 컨피그레이션**)**에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.
b) Advanced Configuration(고급 컨피그레이션) 목차에서 **FlexConfig** > **FlexConfig Objects(FlexConfig** 개체**)**를 클릭합니다.
c) **+** 버튼을 클릭하여 새 개체를 생성합니다.
d) 개체의 이름을 입력합니다. **Disable_TCP_Randomization**을 예로 들 수 있습니다.
e) **Template(**템플릿**)** 편집기에서 TCP 시퀀스 번호 임의 설정을 비활성화하는 명령을 입력합니다.

해당 명령은 **set connection random-sequence-number disable**이지만 정책 맵 내의 특정 클래스에 맞게 명령을 컨피그레이션해야 합니다. 현재까지 확인된 가장 쉬운 방식은 임의 시퀀스 번호를 전역적으로 비활성화하는 것입니다. 이렇게 하려면 다음 명령을 사용해야 합니다.

```
policy-map global_policy
 class default_class
  set connection random-sequence-number disable
```

f) **Negate Template(**무효화 템플릿**)** 편집기에 이 컨피그레이션을 실행 취소하는 데 필요한 행을 입력합니다.

예를 들어 TCP 시퀀스 번호 임의 설정을 전역적으로 비활성화하는 경우, 무효화 템플릿은 다음과 같습니다.

```
policy-map global_policy
 class default_class
  set connection random-sequence-number enable
```

g) **OK(**확인**)**를 클릭하여 개체를 저장합니다.

이제 개체를 FlexConfig 정책에 추가해야 합니다. 개체를 만드는 것으로는 충분하지 않습니다.

h) 목차에서 **FlexConfig Policy(FlexConfig** 정책**)**를 클릭합니다.

i) Group List(그룹 목록)에서 **+**를 클릭합니다.

j) Disable_TCP_Randomization 개체를 선택하고 **OK(**확인**)**를 클릭합니다.

템플릿의 명령으로 미리보기가 업데이트됩니다. 올바른 명령이 표시되는지 확인합니다.

k) **Save(**저장**)**를 클릭합니다.

이제 정책을 구축할 수 있습니다.

모니터링 인터페이스

다음 영역에서 인터페이스에 대한 몇 가지 기본 정보를 확인할 수 있습니다.

- **Device(**디바이스**)**. 포트 그래픽을 사용하여 인터페이스의 현재 상태를 모니터링합니다. 포트 위에 마우스를 올려놓으면 해당 IP 주소, EtherChannel 멤버십, 및 활성화 상태 및 링크 상태가 표시됩니다. IP 주소는 정적으로 할당할 수도 있고 DHCP를 사용하여 가져올 수도 있습니다.

  인터페이스 포트는 다음 색 코드를 사용합니다.

  - 녹색 — 인터페이스가 구성되어 있고 활성화된 상태이며 링크가 작동합니다.
  - 회색 — 인터페이스를 활성화하지 않습니다.
  - 주황색/빨간색 — 인터페이스가 구성되어 있고 활성화된 상태이지만 링크가 작동하지 않습니다. 유선 인터페이스의 경우 이 색은 수정해야 하는 오류 상태를 나타냅니다. 유선 인터페이스가 아닌 경우에는 이 색이 표시되는 것이 정상입니다.

- **Monitoring(**모니터링**)** > **System(**시스템**)**. 처리량 대시보드에는 시스템을 통과하는 트래픽에 대한 정보가 표시됩니다. 모든 인터페이스에서 정보를 확인할 수도 있고 검사할 특정 인터페이스를 선택할 수도 있습니다.
- **Monitoring(**모니터링**)** > **Zones(**영역**)**. 이 대시보드에는 인터페이스로 구성된 보안 영역을 기반으로 한 통계가 표시됩니다. 이 정보를 자세히 확인하여 추가 세부사항을 파악할 수 있습니다.

CLI에서 인터페이스 모니터링

CLI 콘솔을 열거나 디바이스 CLI에 로그인한 후에 다음 명령을 사용하여 인터페이스 관련 행동 및 통계에 대한 상세 정보를 가져올 수도 있습니다.

- **show interface** 인터페이스 통계 및 컨피그레이션 정보를 표시합니다. 이 명령에는 필요한 정보를 가져오는 데 사용할 수 있는 여러 키워드가 있습니다. 사용 가능한 옵션을 확인하려면 키워드로 ?를 사용합니다.
- **show ipv6 interface** 인터페이스에 대한 IPv6 컨피그레이션 정보를 표시합니다.
- **show bridge-group** 멤버 정보와 IP 주소를 비롯하여 BVI(브리지 가상 인터페이스)에 대한 정보를 표시합니다.
- **show conn** 인터페이스를 통해 현재 설정되어 있는 연결에 대한 정보를 표시합니다.
- **show traffic** 각 인터페이스를 통과하는 트래픽에 대한 통계를 표시합니다.
- **show ipv6 traffic** 디바이스를 통과하는 IPv6 트래픽에 대한 통계를 표시합니다.
- **show dhcpd** 인터페이스의 DHCP 사용량에 대한 통계와 기타 정보(특히 인터페이스에 구성된 DHCP 서버 관련)를 표시합니다.
- **show switch vlan** VLAN-스위치 포트 연결을 표시합니다.
- **show switch mac-address-table** 정적 및 동적 MAC 주소 항목을 표시합니다.
- **show arp** 동적, 정적 및 프록시 ARP 항목을 표시합니다.
- **show power inline** PoE 상태를 표시합니다.
- **show vpdn group** PPPoE 그룹 및 구성된 사용자 이름 및 인증을 표시합니다.
- **show vpdn username** PPPoE 사용자 이름 및 비밀번호를 표시합니다.
- **show vpdn session pppoe state** PPPoE 세션 상태를 표시합니다.

인터페이스의 예시

사용 사례 장에는 다음과 같은 인터페이스 관련 예시가 포함되어 있습니다.

- Device Manager에서 디바이스 구성 방법, 43 페이지
- 서브넷을 추가하는 방법, 74 페이지

• 네트워크에서 트래픽을 능동적으로 모니터링하는 방법, 79 페이지

IV 부

라우팅

12 장

라우팅 기본 사항 및 정적 경로

시스템은 라우팅 테이블을 사용하여 시스템으로 들어오는 패킷용 이그레스 인터페이스를 결정합니다. 다음 주제에서는 라우팅의 기본 사항과 디바이스에서 정적 라우팅을 구성하는 방법을 설명합니다.

라우팅에 대한 모범 사례

네트워크에서 라우팅 프로세스를 설계하는 것은 복잡한 프로세스일 수 있습니다. 이 장에서는 threat defense 디바이스가 기존 네트워크 내에서 작동하도록 구성하고, 네트워크에 이미 설정된 라우팅 프로세스에 참여하도록 구성하는 것으로 가정합니다.

그 대신 새 네트워크를 생성할 경우, 시간을 내어 라우팅 프로토콜에 대한 내용 및 네트워크에서 작동하는 효과적인 라우팅 계획을 설계하는 방법을 참조하십시오. 이 장에서는 프로토콜 선택에 대한 권장 사항을 다루지 않으며, 프로토콜이 작동하는 방식을 심층적으로 다루지 않습니다.

네트워크가 매우 소규모이고 ISP에만 연결하려는 경우, 정적 경로가 몇 개만 필요할 수 있으며 라우팅 프로토콜을 구현할 필요가 전혀 없을 수 있습니다.

그러나 많은 라우터가 포함된 대규모 네트워크를 설정할 경우에는 OSPF 같은 내부 라우팅에 대해 하나 이상의 라우팅 프로토콜을 구현해야 할 수 있습니다. 여기에는 BGP 같은 외부 라우팅에 대한 라우팅 프로토콜도 해당될 수 있습니다. 통신 사업자의 도움을 받아 귀사에 어떤 외부 라우팅이 필요한지 파악할 수 있습니다. 이러한 상황에서는 우선 threat defense를 사용해 구성할 수 있는 라우팅 프로토콜을 파악한 다음, 네트워크를 계획하고, 계획에 따라 threat defense 디바이스를 구성합니다.

라우팅 개요

다음 주제에서는 threat defense 디바이스 내에서 라우팅이 동작하는 방식을 설명합니다. 라우팅은 소스에서 대상까지 네트워크에 걸친 정보의 이동입니다. 그 과정에서 적어도 하나의 중간 노드를 일반

적으로 만나게 됩니다. 라우팅에는 2가지 기본적인 작업이 포함되는데, 최적의 라우팅 경로를 결정하는 것과 네트워크를 통한 패킷 전송입니다.

지원되는 라우팅 프로토콜

다음 표에서는 device manager을 사용하여 threat defense 디바이스에서 구성할 수 있는 라우팅 프로토콜과 기술, 그리고 컨피그레이션을 완료하는 데 사용해야 하는 방법에 대해 설명합니다.

표 *7:* 지원되는 라우팅 프로토콜

라우팅 기능	컨피그레이션 방법	참고
BGP	Smart CLI	**Device(**디바이스**)** > **Routing(**라우팅**)** 페이지에서 BGP 스마트 CLI 개체를 구성합니다. **Device(**디바이스**)** > **Advanced Configuration(**고급 컨피그레이션**)** 페이지에서 스마트 CLI 개체를 사용하여 BGP에서 사용되는 개체(예: 경로 맵)를 구성합니다.
BFD(Bi-directional Forwarding Detection)	FlexConfig	**Device(**디바이스**)** > **Advanced Configuration(**고급 컨피그레이션**)** 페이지에서 FlexConfig 개체를 사용하여 BFD를 구성합니다. BFD는 BGP에서만 지원됩니다.
EIGRP	Smart CLI	**Device(**디바이스**)** > **Routing(**라우팅**)** 페이지에서 EIGRP 스마트 CLI 개체를 구성합니다. **Device(**디바이스**)** > **Advanced Configuration(**고급 컨피그레이션**)** 페이지에서 스마트 CLI 개체를 사용하여 EIGRP에서 사용되는 개체(예: 경로 맵)를 구성합니다.
IS-IS	FlexConfig	**Device(**디바이스**)** > **Advanced Configuration(**고급 컨피그레이션**)** 페이지에서 FlexConfig 개체를 사용하여 IS-IS를 구성합니다.
멀티캐스트 라우팅	FlexConfig	**Device(**디바이스**)** > **Advanced Configuration(**고급 컨피그레이션**)** 페이지에서 FlexConfig 개체를 사용하여 멀티캐스트 라우팅을 구성합니다.
OSPFv2	Smart CLI	**Device(**디바이스**)** > **Routing(**라우팅**)** 페이지에서 OSPFv2 스마트 CLI 개체를 구성합니다. **Device(**디바이스**)** > **Advanced Configuration(**고급 컨피그레이션**)** 페이지에서 스마트 CLI 개체를 사용하여 OSPFv2에서 사용되는 개체(예: 경로 맵)를 구성합니다.
OSPFv3	—	OSPFv3 프록시 설정은 지원되지 않습니다.
PBR(Policy-Based Routing)	FlexConfig	**Device(**디바이스**)** > **Advanced Configuration(**고급 컨피그레이션**)** 페이지에서 FlexConfig 개체를 사용하여 PBR(Policy-Based Routing)을 구성합니다.

라우팅 기능	컨피그레이션 방법	참고
RIP	FlexConfig	**Device(**디바이스**)** > **Advanced Configuration(**고급 컨피그레이션**)** 페이지에서 FlexConfig 개체를 사용하여 RIP를 구성합니다.
정적 경로	Device Manager	**Device(**디바이스**)** > **Routing(**라우팅**)** 페이지에서 전역으로 또는 가상 라우터당 정적 경로를 구성합니다.
가상 라우터, VRF	Device Manager	**Device(**디바이스**)** > **Routing(**라우팅**)** 페이지에서 가상 라우터를 구성합니다.

경로 유형

경로에는 정적 유형과 동적 유형이 있습니다.

정적 경로는 명시적으로 정의하는 것입니다. 이 경로는 안정적이고 일반적으로 우선 순위가 높으며, 경로 대상으로 가는 트래픽이 항상 올바른 인터페이스로 전송되게 하는 데 사용합니다. 예를 들어 기본 정적 경로를 생성하여 기타 경로(IPv4의 경우 0.0.0.0/0, IPv6의 경우 ::/0)에서 아직 처리하지 않는 모든 트래픽을 처리할 수 있습니다. 또 다른 예로 항상 사용하려는 내부 syslog 서버로 가는 정적 경로를 들 수 있습니다.

동적 경로는 OSPF, BGP, EIGRP, IS-IS, RIP 등 라우팅 프로토콜 작업을 통해 학습된 것입니다. 경로를 직접 정의하지 않습니다. 그 대신에 라우팅 프로토콜을 컨피그레이션하면 시스템에서 인접 라우터와 통신하여 라우팅 업데이트를 전송하고 그 결과로 라우팅 업데이트를 수신합니다.

동적 라우팅 프로토콜에서는 수신 라우팅 업데이트 메시지를 분석함으로써 네트워크 상황의 변화에 따라 라우팅 테이블을 조정합니다. 네트워크 변경 사실을 알리는 메시지가 표시되면 시스템에서 경로를 다시 계산하여 새로운 라우팅 업데이트 메시지를 전송합니다. 이 메시지는 네트워크를 통과하며 라우터가 알고리즘을 다시 실행하고 라우팅 테이블을 그에 따라 변경하게 합니다.

정적 라우팅은 간단하여 기본 라우팅에 알맞습니다. 네트워크 트래픽을 상대적으로 예측하기 쉬운 환경과 네트워크 설계가 상대적으로 단순한 환경에서 효과적입니다. 하지만 직접 수정하지 않으면 정적 경로를 변경할 수 없기 때문에 네트워크에 변동이 발생한 경우, 이에 대응할 수 없습니다.

소형 네트워크가 없는 경우, 일반적으로 정적 경로를 하나 이상의 동적 라우팅 프로토콜에 결합할 수 있습니다. 하나 이상의 정적 경로를 명시적 경로와 일치하지 않는 모든 트래픽에 대한 기본 경로로 정의합니다.

참고 스마트 CLI를 사용하여 라우팅 프로토콜인 OSPF 및 BGP를 컨피그레이션할 수 있습니다. FlexConfig를 사용하여 ASA 소프트웨어에서 지원하는 다른 라우팅 프로토콜을 컨피그레이션합니다.

라우팅 테이블과 경로 선택

NAT 변환(xlates) 및 규칙에서 이그레스 인터페이스를 결정하지 않는 경우, 시스템에서는 라우팅 테이블을 사용하여 패킷의 경로를 결정합니다.

라우팅 테이블의 경로에는 지정된 경로에 대한 상대적 우선순위를 제공하는 "관리 거리"라는 메트릭이 있습니다. 패킷이 둘 이상의 경로 항목과 일치하는 경우에는 거리가 가장 짧은 항목이 사용됩니다. 직접 연결된 네트워크(인터페이스에서 정의된 네트워크)는 거리가 0이므로 항상 기본적으로 사용됩니다. 고정 경로의 기본 거리는 1이지만 1~254 범위의 원하는 거리를 사용하여 고정 경로를 생성할 수 있습니다.

특정 대상을 식별하는 경로는 기본 경로(대상이 0.0.0.0/0 또는 ::/0인 경로)보다 먼저 적용됩니다.

라우팅 테이블을 채우는 방법

threat defense 라우팅 테이블은 정적으로 정의된 경로, 직접 연결된 경로, 그리고 동적 라우팅 프로토콜에서 검색한 경로로 채울 수 있습니다. threat defense 디바이스는 라우팅 테이블에 고정 경로와 연결 경로를 가지는 것 외에도 여러 라우팅 프로토콜을 실행할 수 있기 때문에 같은 경로가 하나 이상의 방법으로 다시 발견되거나 입력될 수 있습니다. 같은 목적지로의 두 경로를 라우팅 테이블에 넣으면 라우팅 테이블에 유지되는 항목은 다음과 같이 결정됩니다.

- 두 경로의 네트워크 접두사 길이(네트워크 마스크)가 다르면 두 경로 모두 고유한 것으로 간주되어 라우팅 테이블에 입력됩니다. 그런 다음 패킷 전달 로직에서 둘 중 어느 것을 사용할지 결정합니다.

  예를 들어 RIP 및 OSPF 프로세스에서 다음 경로를 검색한 경우

  - RIP: 192.168.32.0/24
  - OSPF: 192.168.32.0/19

  비록 OSPF 경로의 관리 영역이 더 낮지만, 접두사 길이(서브넷 마스크)가 다르기 때문에 두 경로 모두 라우팅 테이블에 설치됩니다. 이들은 다른 목적지로 간주되며 패킷 전달 로직에서 사용할 경로를 결정합니다.

- threat defense 디바이스가 RIP와 같이 단일 라우팅 프로토콜에서 같은 대상으로의 여러 경로를 학습하는 경우 메트릭이 더 나은 경로(라우팅 프로토콜이 결정)가 라우팅 테이블에 입력됩니다.

  메트릭은 특정 경로와 연결되는 값이며, 선호도가 가장 높은 것부터 순위를 지정합니다. 메트릭을 결정하는 데 사용되는 매개변수는 라우팅 프로토콜에 따라 다릅니다. 가장 낮은 메트릭을 갖는 경로가 최적의 경로로 선택되고 라우팅 테이블에 설치됩니다. 동일한 목적지의 다중 경로가 메트릭 값이 같을 경우 이 동일 비용 경로에 대한 로드 밸런싱이 수행됩니다.

- threat defense 디바이스가 두 개 이상이 라우팅 프로토콜로부터 대상에 대해 학습하는 경우 경로의 AD(Administrative Distance)를 비교하고 AD가 짧은 경로가 라우팅 테이블에 입력됩니다.

경로의 관리 거리

라우팅 프로토콜에서 검색 또는 재배포되는 경로에 대한 관리 영역을 변경할 수 있습니다. 서로 다른 두 라우팅 프로토콜의 두 경로가 관리 영역이 같을 경우 기본 관리 영역이 낮은 경로가 라우팅 테이

블에 입력됩니다. EIGRP 및 OSPF 경로의 경우 EIGRP 경로와 OSPF 경로가 관리 영역이 같으면 기본적으로 EIGRP 경로가 선택됩니다.

관리 영역은 서로 다른 두 라우팅 프로토콜로부터 동일한 목적지의 서로 다른 경로가 2개 이상 나올 경우 최적의 경로를 선택하기 위해 위협 방지 디바이스에서 사용하는 경로 매개변수입니다. 라우팅 프로토콜은 다른 프로토콜과 구별되는 알고리즘을 기반으로 한 메트릭을 갖기 때문에 서로 다른 라우팅 프로토콜에서 생성된 동일 목적지의 경로 2개 중에서 최적의 경로를 결정하는 것이 가능하지 않을 수도 있습니다.

각 라우팅 프로토콜은 관리 영역 값을 사용하여 우선순위가 지정됩니다. 다음 표에는 위협 방지 디바이스에서 지원하는 라우팅 프로토콜의 기본 관리 거리 값이 정리되어 있습니다.

표 ***8:*** 지원되는 라우팅 프로토콜의 기본 관리 영역

경로 소스	기본 관리 영역
연결된 인터페이스	0
VPN 경로	1
고정 경로	1
EIGRP 요약 경로	5
외부 BGP	20
내부 EIGRP	90
OSPF	110
IS-IS	115
RIP	120
EIGRP 외부 경로	170
내부 및 로컬 BGP	200
알 수 없음	255

관리 영역의 값이 작을수록 프로토콜 우선순위가 높습니다. 예를 들어, 위협 방지 디바이스가 OSPF 라우팅 프로세스(기본 관리 거리 - 110)와 RIP 라우팅 프로세스(기본 관리 거리 - 120)로부터 모두 특정 네트워크로의 경로를 수신할 경우 위협 방지 디바이스는 우선순위가 더 높은 OSPF 경로를 선택합니다. 이러한 경우 라우터가 라우팅 테이블에 경로의 OSPF 버전을 추가합니다.

VPN 광고 경로(V-Route/RRI)는 기본 AD(Administrative Distance)가 1인 고정 경로와 같습니다. 그러나 네트워크 마스크 255.255.255.255와 마찬가지로 기본 설정이 더 높습니다.

이 예제에서, OSPF 파생 경로의 소스가 손실된 경우(예: 전원 꺼짐) 위협 방지 디바이스는 OSPF 파생 경로가 다시 나타날 때까지 RIP 파생 경로를 사용합니다.

관리 영역은 로컬 설정입니다. 예를 들어 OSPF를 통해 얻은 경로의 관리 거리를 변경하면 이 변경 사항은 이 명령을 입력한 위협 방지 디바이스의 라우팅 테이블에만 영향을 미칩니다. 관리 영역은 라우팅 업데이트에서 광고되지 않습니다.

관리 영역은 라우팅 프로세스에 영향을 주지 않습니다. 라우팅 프로세스에서는 라우팅 프로세스를 통해 검색되었거나 라우팅 프로세스로 재배포된 경로만 알립니다. 예를 들어 RIP 라우팅 프로세스는 OSPF 라우팅 프로세스를 통해 발견된 경로가 라우팅 테이블에 사용되더라도 RIP 경로를 광고합니다.

동적 및 부동 정적 경로 백업

다른 경로가 설치되었기 때문에 라우팅 테이블에 경로를 설치하려는 첫 번째 시도가 실패하면 백업 경로가 등록됩니다. 라우팅 테이블에 설치된 경로가 실패할 경우 라우팅 테이블 유지 관리 프로세스는 백업 경로를 등록한 각 라우팅 프로토콜 프로세스를 호출하고 해당 경로를 라우팅 테이블에 다시 설치하도록 요청합니다. 실패한 경로에 대해 백업이 등록된 프로토콜이 여럿인 경우 관리 영역을 기준으로 우선 경로가 선택됩니다.

이 프로세스 때문에 동적 라우팅 프로토콜을 통해 발견된 경로가 실패할 때 라우팅 테이블에 설치된 유동 고정 경로를 생성할 수 있습니다. 유동 고정 경로는 단순히 위협 방지 디바이스에서 실행되는 동적 라우팅 프로토콜보다 큰 관리 영역으로 설정된 고정 경로입니다. 동적 라우팅 프로세스에서 발견한 경로가 실패하면 라우팅 테이블에 고정 경로가 설치됩니다.

포워딩 결정 방법

포워딩 결정은 다음과 같이 이루어집니다.

- 목적지가 라우팅 테이블 내의 항목과 일치하지 않으면 패킷이 기본 경로에 지정된 인터페이스를 통해 포워딩됩니다. 기본 경로가 구성되지 않은 경우 패킷이 폐기됩니다.
- 목적지가 라우팅 테이블의 단일 항목과 일치하는 경우 패킷이 해당 경로와 연결된 인터페이스를 통해 포워딩됩니다.
- 목적지가 라우팅 테이블에 있는 두 개 이상의 항목과 일치하면 패킷은 네트워크 접두사가 더 긴 경로와 연결된 인터페이스를 통해 전달됩니다.

예를 들어 목적지가 192.168.32.1인 패킷은 라우팅 테이블의 다음 경로를 통해 인터페이스에 도착합니다.

- 192.168.32.0/24 게이트웨이 10.1.1.2
- 192.168.32.0/19 게이트웨이 10.1.1.3

이 경우 192.168.32.1이 192.168.32.0/24 네트워크 범위에 해당되기 때문에 목적지가 192.168.32.1인 패킷은 10.1.1.2로 전달됩니다. 이 주소는 라우팅 테이블 내 다른 경로에도 포함되지만, 라우팅 테이블의 다른 경로 접두사는 19비트인 데 비해 192.168.32.0/24의 접두사는 24비트이므로 이 경로의 접두사가 가장 깁니다. 패킷을 전달할 때는 항상 더 긴 접두사가 우선합니다.

참고 새로운 유사한 연결이 경로 변경으로 인해 다른 동작을 유발하는 경우에도 기존의 연결은 계속해서 설정된 인터페이스를 사용합니다.

관리 트래픽용 라우팅 테이블

표준 보안 관행으로 데이터 트래픽에서 관리 트래픽(디바이스에서)을 분리 및 격리할 필요가 있는 경우가 많습니다. 이 격리를 달성하기 위해 threat defense 디바이스에서는 데이터 트래픽과 관리 전용 트래픽에 대해 각각 별도의 라우팅 테이블을 사용합니다. 별도의 라우팅 테이블을 사용하면 데이터 및 관리를 위해 별도의 기본 경로도 생성할 수 있습니다.

각 라우팅 테이블의 트래픽 유형

디바이스를 통과하는 트래픽에서는 항상 데이터 라우팅 테이블을 사용합니다.

디바이스에서 시작되는 트래픽에서는 유형에 따라 기본적으로 관리 전용 라우팅 테이블 또는 데이터 라우팅 테이블 중 하나를 사용합니다. 기본 라우팅 테이블에서 일치하는 항목을 찾을 수 없으면 다른 라우팅 테이블을 확인합니다.

- 디바이스에서 시작되는 트래픽의 관리 전용 테이블에는 AAA 서버 통신이 포함됩니다.
- 디바이스에서 시작되는 트래픽의 데이터 테이블에는 DNS 서버 조회 및 DDNS가 포함됩니다. 단, DNS에 대해 진단 인터페이스만 지정하는 경우, threat defense 디바이스는 관리 전용 테이블만 사용합니다.

관리 전용 라우팅 테이블에 포함된 인터페이스

관리 전용 인터페이스에는 관리 x/x 인터페이스뿐 아니라 관리 전용으로 컨피그레이션한 모든 인터페이스도 포함됩니다.

참고 관리 가상 인터페이스는threat defense 경로 조회에 속하지 않는 자체 Linux 라우팅 테이블을 사용합니다. 관리 인터페이스에서 시작되는 트래픽에는 device manager 관리 세션, 라이선싱 통신 및 데이터베이스 업데이트가 포함됩니다. 그러나 논리적 진단 인터페이스는 이 섹션에서 설명된 관리 전용 라우팅 테이블을 사용합니다.

다른 라우팅 테이블로 대체

기본 라우팅 테이블에서 일치하는 항목을 찾을 수 없으면 다른 라우팅 테이블을 확인합니다.

비기본 라우팅 테이블 사용

기본 라우팅 테이블에 없는 인터페이스에서 외부로 이동하는 데 즉시 사용 가능한 트래픽이 필요한 경우, 다른 테이블로 대체하지 않고 구성할 때 해당 인터페이스를 지정해야 할 수 있습니다. threat defense에서는 지정된 인터페이스에 대한 경로만 확인합니다. 예를 들어, 데이터 인터페이스에서 RADIUS 서버와 통신해야 하는 경우, RADIUS 설정에서 해당 인터페이스를 지정합니다. 그렇지 않으면 관리 전용 라우팅 테이블에 기본 경로가 있는 경우, 이는 기본 경로와 일치하며 데이터 라우팅 테이블로 대체되지 않습니다.

ECMP(Equal-Cost Multi-Path) 라우팅

위협 방지 디바이스에서는 ECMP(Equal-Cost Multi-Path) 라우팅을 지원합니다.

인터페이스당 최대 8개의 동일 비용 정적 또는 동적 경로가 가능합니다. 예를 들어 외부 인터페이스에서 서로 다른 게이트웨이를 지정하는 여러 개의 기본 경로를 컨피그레이션할 수 있습니다.

```
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.2
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.3
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.4
```

여기서는 외부 인터페이스에서 0.1.1.2, 10.1.1.3, 10.1.1.4끼리 트래픽 로드 밸런싱을 수행합니다. 트래픽은 소스와 대상 IP 주소, 수신 인터페이스, 프로토콜, 소스 및 대상 포트를 해싱하는 알고리즘에 따라 지정된 게이트웨이 사이에서 분배됩니다.

트래픽 영역을 사용하는 여러 인터페이스의 **ECMP**

인터페이스 그룹을 포함하도록 트래픽 영역을 구성할 경우, 하나의 영역 내에서 최대 8개의 인터페이스에 걸쳐 최대 8개의 동일 비용 정적 또는 동적 경로가 가능합니다. 예를 들어 다음과 같이 영역 내 인터페이스 3개의 전 범위에 걸쳐 여러 개의 기본 경로를 컨피그레이션할 수 있습니다.

```
route for 0.0.0.0 0.0.0.0 through outside1 to 10.1.1.2
route for 0.0.0.0 0.0.0.0 through outside2 to 10.2.1.2
route for 0.0.0.0 0.0.0.0 through outside3 to 10.3.1.2
```

또한 동적 라우팅 프로토콜은 동일 비용 경로를 자동으로 구성할 수 있습니다. 위협 방지 디바이스에서는 더 강력한 로드 밸런싱 메커니즘을 통해 인터페이스 간의 트래픽을 로드 밸런싱합니다.

어떤 경로가 사라지면 디바이스에서는 다른 경로로 원활하게 플로우를 이동합니다.

고정 경로

네트워크에 대한 기본 라우팅을 제공하기 위해 정적 경로를 생성할 수 있습니다.

고정 경로 및 기본 경로 소개

비연결 호스트 또는 네트워크에 트래픽을 라우팅하려면 정적 또는 동적 라우팅을 사용하여 해당 호스트 또는 네트워크로 가는 경로를 정의해야 합니다. 일반적으로 최소한 하나의 고정 경로를 구성해야 합니다. 다른 방법으로는 기본 네트워크 게이트웨이(대개는 다음 홉 라우터)에 라우팅되지 않는 모든 트래픽을 위한 기본 경로입니다.

기본 라우터

가장 간단한 옵션은 트래픽을 라우팅해주는 라우터에 의존하여 모든 트래픽을 업스트림 라우터로 보내는 기본 정적 경로를 컨피그레이션하는 것입니다. 기본 고정 경로는 위협 방지 디바이스가 학습 경로나 고정 경로를 가지고 있지 않은 모든 IP 패킷을 보낼 게이트웨이 IP 주소를 식별합니다. 기본 정적 경로는 대상 IP 주소가 0.0.0.0/0(IPv4) 또는 ::/0(IPv6)인 정적 경로일 뿐입니다.

항상 기본 경로를 정의해야 합니다.

threat defense 디바이스에서는 데이터 트래픽 및 관리 트래픽에 대해 별도의 라우팅 테이블을 사용하므로 선택적으로 데이터 트래픽에 대한 기본 경로를 구성하고 관리 트래픽에 대한 또 다른 기본 경로를 구성할 수 있습니다. 디바이스에서 시작되는 트래픽에서는 유형에 따라 기본적으로 관리 전용 또는 데이터 라우팅 테이블 중 하나를 사용합니다. 그러나 경로를 찾을 수 없는 경우 다른 라우팅 테이블로 폴백됩니다. 기본 경로는 항상 트래픽과 일치하며 다른 라우팅 테이블로 대체되는 것을 방지합니다. 이 경우, 해당 인터페이스가 기본 라우팅 테이블에 없다면 이그레스 트래픽에 사용할 인터페이스를 지정해야 합니다. 진단 인터페이스는 관리 전용 테이블에 포함되어 있습니다. 특수 관리 인터페이스는 별도의 Linux 라우팅 테이블을 사용하며, 자체 기본 경로가 있습니다.

고정 경로

다음과 같은 경우, 고정 경로를 사용할 수 있습니다.

- 네트워크에서 지원하지 않는 라우터 검색 프로토콜을 사용합니다.
- 네트워크 규모가 작고 고정 경로를 쉽게 관리할 수 있습니다.
- 트래픽이나 CPU 오버헤드를 라우팅 프로토콜과 연결하지 않는 것이 좋습니다.
- 기본 경로만으로 충분하지 않을 때도 있습니다. 기본 게이트웨이가 목적지 네트워크에 도달할 수 없는 경우가 있기 때문에 보다 구체적인 고정 경로도 구성해야 합니다. 예를 들어 기본 게이트웨이가 밖에 있는 경우 기본 경로는 위협 방지 디바이스에 직접 연결되지 않은 내부 네트워크로 트래픽을 안내할 수 없습니다.
- 동적 라우팅 프로토콜을 지원하지 않는 기능을 사용 중입니다.

고정 경로 백업 및 고정 경로 추적

고정 경로의 문제 중 하나는 경로가 정상인지 다운되었는지 확인할 수 있는 내재적인 메커니즘이 없다는 것입니다. 다음 홉 게이트웨이를 사용할 수 없게 된다 해도 고정 경로는 라우팅 테이블에 남아 있습니다. 고정 경로는 연결된 인터페이스가 다운되는 경우에만 라우팅 테이블에서 제거됩니다.

SLA(Service Level Agreement) 모니터를 사용해 경로 추적을 실행함으로써 고정 경로의 가용성을 추적하고 기본 경로가 실패할 경우 백업 경로를 자동으로 설치할 수 있습니다. 예를 들어 기본 ISP를 사용할 수 없는 경우에 대비하여 ISP 게이트웨이로의 기본 경로와 보조 ISP로의 보조 기본 경로를 정의할 수 있습니다.

경로 추적을 사용하는 경우, 추적된 경로에 대상 네트워크의 대상 IP 주소를 연결합니다. 그러면 시스템에서는 ICMP 에코 요청을 사용하여 주기적으로 주소 연결 가능 여부를 확인합니다. 지정한 시간 내에 시스템에 에코 응답이 수신되지 않으면 호스트는 연결할 수 없는 것으로 간주되고, 시스템에서는 연결된 경로를 라우팅 테이블에서 제거합니다. 그러면 시스템에서는 메트릭이 높은 비추적 백업 경로를 제거된 경로 대신 사용할 수 있습니다.

따라서 기본 경로를 포함한 특정 대상에 대한 백업 고정 경로를 사용하려면 다음 작업을 수행해야 합니다.

1. 게이트웨이 또는 상시 가동 서버(예: 웹 서버 또는 syslog 서버) 등 대상 네트워크에서 신뢰할 수 있는 IP 주소를 모니터링하는 SLA 모니터를 생성합니다. 대상 네트워크가 정상 상태이고 사용 가능한 동안에는 오프라인 상태로 전환될 수 있는 시스템의 IP 주소를 모니터링하지 마십시오. SLA 모니터 개체 컨피그레이션, 341 페이지를 참조하십시오.

2. 대상으로 연결되는 기본 경로를 생성하고 이 경로에 대해 SLA 모니터를 선택합니다. 이 경로에 대한 메트릭은 일반적으로 1이어야 합니다. 고정 경로 구성, 339 페이지를 참조하십시오.
3. 기본 경로가 실패할 경우 사용할 백업 정적 경로를 생성합니다. 이 경로의 메트릭은 기본 경로보다 커야 합니다. 예를 들어 기본 경로가 1이면 백업 경로는 10일 수 있습니다. 또한 일반적으로 백업 경로에 대해 다른 인터페이스를 선택합니다.

정적 라우팅에 대한 지침

브리지 그룹

- 라우티드 모드에서는 BVI를 게이트웨이로 지정해야 하며 멤버 인터페이스는 지정할 수 없습니다.
- 위협 방지 디바이스(예: syslog 또는 SNMP)에서 발생하고 브리지 그룹 멤버 인터페이스를 거쳐 직접 연결되지 않은 네트워크로 가는 트래픽의 경우, 기본 경로 또는 정적 경로를 컨피그레이션하여 위협 방지 디바이스에서 어떤 브릿지 그룹 멤버 인터페이스로 트래픽을 보낼지 알 수 있게 해야 합니다. 단일 기본 경로를 통해 모두 도달할 수 없는 서버가 있다면 고정 경로를 구성해야 합니다.
- 브리지 그룹 멤버 인터페이스 또는 BVI에 대해서는 정적 경로 추적을 지원하지 않습니다.

IPv6

- 고정 경로 추적(SLA 모니터링)은 IPv6에서 지원되지 않습니다.

ECMP(Equal-Cost Multi-Path) 트래픽 영역

- 서로 다른 액세스, SSL 또는 ID 규칙이 해당 인터페이스에 적용되지 않도록 ECMP 트래픽 영역의 멤버 인터페이스를 동일한 보안 영역에 유지합니다.
- 지정된 ECMP 트래픽 영역에서 네트워크에 대해 최대 8개의 동일 비용 경로를 가질 수 있습니다.
- 영역당 최대 8개의 인터페이스를 사용하여 최대 256개의 ECMP 트래픽 영역을 생성할 수 있습니다.
- ECMP 트래픽 영역은 이름이 지정된 물리적 인터페이스, 하위 인터페이스 및 Etherchannel을 포함할 수 있습니다. 여기에는 다음을 포함할 수 없습니다.
  - 브리지 그룹(BVI) 또는 멤버
  - Etherchannel 멤버 인터페이스
  - HA 인터페이스(페일오버 또는 상태 링크)
  - 관리 전용 인터페이스
  - 사이트 대 사이트 VPN 또는 원격 액세스 VPN 연결에 사용되는 인터페이스.
  - VTI(Virtual Tunnel Interface) 또는 해당 소스 인터페이스.

- VPN 관리 액세스용으로 구성된 인터페이스.

- 영역의 인터페이스에서 DHCP 릴레이를 활성화할 수 없습니다.

고정 경로 구성

시스템의 인터페이스에 직접 연결된 네트워크로 이동하지 않는 패킷을 전송할 위치를 시스템에 지시하려면 고정 경로를 정의합니다.

네트워크 0.0.0.0/0에 대해 하나 이상의 고정 경로(기본 경로)가 필요합니다. 이 경로는 기존 NAT xlate(변환)나 고정 NAT 규칙 또는 기타 정적 경로를 통해 이그레스 인터페이스를 확인할 수 없는 패킷을 전송할 위치를 정의합니다.

기본 게이트웨이를 사용하여 모든 네트워크에 액세스할 수 없는 경우 다른 고정 경로가 필요할 수 있습니다. 예를 들어 기본 경로는 대개 외부 인터페이스의 업스트림 라우터입니다. 디바이스에 직접 연결되지 않는 추가 내부 네트워크가 있으며 기본 게이트웨이를 통해 해당 네트워크에 액세스할 수 없는 경우에는 이러한 각 내부 네트워크에 대해 고정 경로가 필요합니다.

시스템 인터페이스에 직접 연결된 네트워크에 대해서는 고정 경로를 정의할 수 없습니다. 시스템에서 이러한 경로를 자동으로 생성합니다.

프로시저

단계 **1** 디바이스를 클릭한 다음, **Routing(**라우팅**)** 요약의 링크를 클릭합니다.

단계 **2** 가상 라우터를 활성화한 경우 정적 경로를 구성 중인 라우터의 보기 아이콘( )을 클릭합니다.

단계 **3** **Static Routing(**정적 라우팅**)** 페이지에서 다음 중 하나를 수행합니다.

- 새 경로를 추가하려면 +를 클릭합니다.
- 수정할 경로의 수정 아이콘( )을 클릭합니다.

경로가 더 이상 필요하지 않은 경우 해당 경로의 휴지통 아이콘을 클릭하여 경로를 삭제합니다.

단계 **4** 경로 속성을 구성합니다.

- **Name(**이름**)** — 경로의 표시 이름입니다.
- **Description(**설명**)** — 경로의 용도에 대한 설명(선택 사항)입니다.
- **Interface(**인터페이스**)** — 트래픽을 전송하는 데 사용할 인터페이스를 선택합니다. 이 인터페이스를 통해 게이트웨이 주소에 액세스할 수 있어야 합니다.

  브리지 그룹의 경우 멤버 인터페이스가 아닌 BVI(브리지 그룹 인터페이스)에 대해 경로를 구성합니다.

  가상 라우팅 및 전달을 활성화한 경우 다른 가상 라우터에 속한 인터페이스를 선택할 수 있습니다. 가상 라우터에서 다른 가상 라우터의 인터페이스에 대한 정적 경로를 생성하는 경우, 이 경로는 가상 라우터 경계를 통과하며 이 가상 라우터의 트래픽이 다른 가상 라우터로 유출될 위험이 있습니다. 이는 원하는 결과일 수 있지만, 이러한 경로 유출이 필요한지 신중하게 판단하십시

오. 인터페이스를 선택하면 인터페이스가 속한 가상 라우터의 이름이 인터페이스 오른쪽에 표시됩니다.

- **Protocol(**프로토콜**)** — 경로가 **IPv4** 또는 **IPv6** 주소에 대한 경로인지 선택합니다.
- **Networks(**네트워크**)** — 이 경로에서 게이트웨이를 사용해야 하는 대상 네트워크 또는 호스트를 식별하는 네트워크 개체를 선택합니다.

  기본 경로를 정의하거나, 사전 정의된 임의의 ipv4 또는 ipv6 네트워크 개체를 사용하거나, 0.0.0.0/0(IPv4) 또는 ::/0(IPv6) 네트워크에 대해 개체를 생성합니다.
- **Gateway(**게이트웨이**)** — 게이트웨이의 IP 주소를 식별하는 호스트 네트워크 개체를 선택합니다. 트래픽은 이 주소로 전송됩니다. 둘 이상의 인터페이스에서 경로에 대해 동일한 게이트웨이를 사용할 수 없습니다.

  가상 라우터에서 경로를 정의하고 있으며 인터페이스가 다른 가상 라우터에 속하는 경우, 게이트웨이를 비워두어야 합니다. 시스템에서는 이러한 네트워크에 대한 트래픽을 다른 가상 라우터로 라우팅한 다음, 대상 가상 라우터의 라우팅 테이블을 사용하여 게이트웨이를 결정합니다.
- **Metric(**메트릭**)** — 경로의 관리 거리(1~254)입니다. 정적 경로의 경우 기본값은 1입니다. 인터페이스와 게이트웨이 간에 추가 라우터가 있으면 홉 수를 관리 거리로 입력합니다.

  관리 거리는 경로를 비교하는 데 사용되는 파라미터입니다. 값이 작을수록 경로에는 더 높은 우선 순위가 지정됩니다. 연결된 경로(디바이스의 인터페이스에 직접 연결되는 네트워크)가 항상 고정 경로보다 우선적으로 사용됩니다.

단계 **5** (선택 사항, IPv4 경로만 해당) 이 경로의 실행 가능성을 추적해야 하는 **SLA Monitor(SLA** 모니터**)**를 선택합니다.

SLA 모니터에서는 대상 네트워크의 항상 사용 가능한 호스트에 연결 가능한지 확인할 수 있습니다. 연결할 수 없게 되면 시스템에서 백업 경로를 설치할 수 있습니다. 따라서 SLA 모니터를 구성하는 경우 이 네트워크에 대해 더 큰 메트릭을 사용하여 또 다른 정적 경로를 구성해야 합니다. 예를 들어 이 경로에 메트릭 1이 있는 경우 메트릭 10을 사용하여 백업 경로를 생성합니다. 자세한 내용은 고정 경로 백업 및 고정 경로 추적, 337 페이지의 내용을 참고하십시오.

SLA 모니터 개체가 아직 없는 경우 목록 하단에서 **Create SLA Monitor(SLA** 모니터 생성**)** 링크를 클릭하여 바로 생성합니다.

참고 모니터링되는 주소를 ping할 수 없으므로 모니터링되는 경로가 제거되면 해당 경로가 경로에 연결할 수 없다는 경고와 함께 정적 경로 테이블에 표시됩니다. 이 문제가 일시적인지 또는 경로를 재구성해야 하는지 확인하십시오. 경로를 실행할 수는 있지만 모니터링되는 주소를 충분히 신뢰할 수는 없는 경우일 수도 있습니다.

단계 **6** **OK(**확인**)**를 클릭합니다.

SLA 모니터 개체 컨피그레이션

정적 경로와 함께 사용할 SLA(Service Level Agreement) 모니터 개체를 컨피그레이션합니다. SLA 모니터를 사용하여 정적 경로의 상태를 추적하고 실패한 경로를 새것으로 자동 교체할 수 있습니다. 경로 추적에 관한 자세한 내용은 고정 경로 백업 및 고정 경로 추적, 337 페이지를 참조하십시오.

모니터링 대상을 선택할 때, ICMP 에코 요청에 응답할 수 있는지 확인해야 합니다. 타겟은 호스트 네트워크 개체에 정의된 모든 IP 주소가 될 수 있지만, 다음 항목을 사용하는 것이 좋습니다.

- 이중 ISP 지원을 위한 ISP 게이트웨이 주소
- 다음 홉 게이트웨이 주소(게이트웨이의 가용성이 우려되는 경우)
- syslog 서버와 같이 시스템에서 통신해야 하는 대상 네트워크에 있는 서버
- 대상 네트워크에 있는 지속적인 IP 주소 야간에 꺼질 수 있는 워크스테이션은 좋은 선택이 아닙니다.

프로시저

단계 **1** 목차에서 **Objects(**개체**)**를 선택한 다음, **SLA Monitors(SLA** 모니터**)**를 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 개체를 생성하려면 + 버튼을 클릭합니다.
- 개체를 수정하려면 개체의 수정 아이콘( )을 클릭하십시오.

참조되지 않는 개체를 삭제하려면 해당 개체의 휴지통 아이콘( )을 클릭합니다.

단계 **3** 개체의 Name(이름) 및 설명(선택 사항)을 입력합니다.

단계 **4** 다음과 같이 SLA 모니터의 필수 옵션을 정의합니다.

- **Monitor Address(**모니터 주소**)** — 대상 네트워크에서 모니터링할 주소를 정의하는 호스트 네트워크 개체를 선택합니다. 필요한 개체가 없는 경우에는 **Create New Network(**새 네트워크 생성**)**를 클릭하면 됩니다.

  이 주소는 SLA 모니터를 정적 경로에 연결하는 경우에만 모니터링됩니다.

- **Target Interface(**대상 인터페이스**)** — 에코 요청 패킷을 전송할 인터페이스를 선택합니다. 일반적으로 정적 경로를 정의하는 인터페이스입니다. 인터페이스 소스 주소는 에코 요청 패킷의 소스 주소로 사용됩니다.

단계 **5** (선택 사항). **IP ICMP Echo Options(IP ICMP** 에코 옵션**)**를 조정합니다.

모든 ICMP 옵션의 기본값은 대부분의 경우에 적합하지만, 이는 필요에 따라 조정할 수 있습니다.

- **Threshold(**임계값**)** — 선언할 상승 임계값에 대한 밀리초 수(0~2147483647). 기본값은 5,000(5초)입니다. 이 값은 시간 초과에 대해 설정된 값보다 클 수 없습니다. 임계값은 연결성에 영향을 주지 않는 임계값 이벤트를 통해 표시할 때만 사용됩니다. 임계값 이벤트의 빈도를 사용해 시간 초과에 대한 설정을 평가할 수 있습니다.

- **Timeout(**시간 초과**)** — 경로 모니터링 작업에서 요청 패킷의 응답을 기다려야 할 밀리초 단위 시간입니다(0~604800000밀리초, 7일 기준). 기본값은 5,000밀리초입니다(5초). 이 기간에 모니터에서 하나 이상의 에코 요청에 대해 응답을 가져오지 않는 경우, 프로세스에서는 백업 경로를 설치합니다.
- **Frequency(**빈도**)** — SLA 프로브 사이의 밀리초 수이며(1,000~604,800,000) 1,000의 배수입니다. 시간 초과 값보다 낮은 빈도는 설정할 수 없습니다. 기본값은 60,000밀리초입니다(60초).
- **Type of Service(**서비스 유형**)** — ICMP 에코 요청 패킷의 IP 헤더에서 ToS(Type of Service) 유형을 정의하는 정수입니다(0~255). 기본값은 0입니다.
- **Number of Packets(**패킷 수**)** — 각 폴과 함께 전송되는 패킷의 수입니다(1~100). 기본값은 1패킷입니다.
- **Data Size(**데이터 크기**)** — 에코 요청 패킷에 사용할 데이터 페이로드의 크기입니다(0~16384바이트). 기본값은 28입니다. 이 설정은 페이로드의 크기만 지정하며 전체 패킷의 크기는 지정하지 않습니다.

단계 **6** **OK(**확인**)**를 클릭합니다.

이제 정적 경로에서 SLA 모니터 개체를 사용할 수 있습니다.

ECMP 트래픽 영역 구성

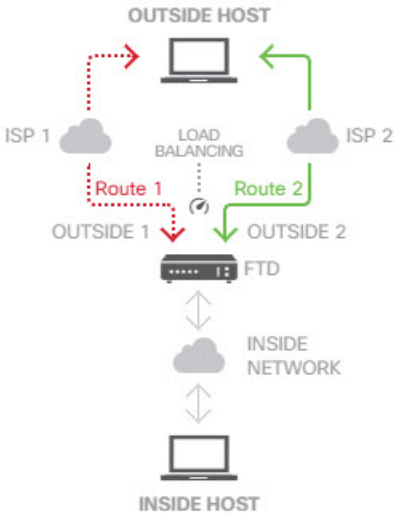
일반적으로 동일한 경로 메트릭을 사용하여 지정된 네트워크 접두사에 대해 여러 경로를 구성하려면 동일한 인터페이스에서 경로를 구성해야 합니다. 따라서 시스템은 ECMP(Equal-Cost Multi-Path) 라우팅 계산을 사용하여 인터페이스를 통해 게이트웨이로 전송되는 트래픽을 로드 밸런싱합니다.

예를 들어 서로 다른 게이트웨이를 지정하는 외부 인터페이스에서 여러 개의 기본 경로를 구성할 수 있고, 이 컨피그레이션은 추가 변경 없이 허용됩니다.

```
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.2
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.3
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.4
```

또한 ECMP를 사용하여 동일한 네트워크 접두사 및 경로 메트릭에 대한 여러 인터페이스(가상 라우터 내)에서 트래픽의 균형을 유지할 수 있습니다. 별도의 인터페이스를 통해 게이트웨이에 액세스할 수 있는 경우 이 컨피그레이션이 필요합니다. 예를 들어 ISP가 2개 있고 ISP간 로드 밸런싱을 수행하려고 하는데, ISP 게이트웨이 간 내부 주소 공간을 분할하고 싶지 않다고 가정해 보겠습니다. 하나의 ISP는 outside1 인터페이스를 통해 액세스할 수 있으며, 다른 ISP는 outside2 인터페이스를 통해 액세스할 수 있습니다. 이를 위해서는 outside1 및 outside2 인터페이스를 포함하는 라우팅 트래픽 영역을 생성해야 합니다.

```
isp-zone containing outside1 and outside2
route for 0.0.0.0 0.0.0.0 through outside1 to 10.1.1.2
route for 0.0.0.0 0.0.0.0 through outside2 to 10.1.1.3
```



참고 ECMP 라우팅 트래픽 영역은 보안 영역과 관련이 없습니다. outside1 및 outside2 인터페이스를 포함하는 보안 영역을 생성해도 ECMP 라우팅용으로 트래픽 영역이 구현되지는 않습니다.

다음 절차에서는 인터페이스 전반에서 ECMP 처리를 활용하도록 ECMP 영역을 구성하는 방법을 설명합니다.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음, **Routing(**라우팅**)** 요약의 링크를 클릭합니다.

단계 **2** 가상 라우터를 활성화한 경우 정적 경로를 구성 중인 라우터의 보기 아이콘( )을 클릭합니다.

단계 **3** **ECMP Traffic Zones(ECMP** 트래픽 영역**)** 탭을 클릭합니다.

단계 **4** **ECMP Traffic Zones(ECMP** 트래픽 영역**)** 페이지에서 다음 중 하나를 수행합니다.

- 새 영역을 추가하려면 **+** 또는 **Add ECMP Traffic Zone(ECMP** 트래픽 영역 추가**)**을 클릭합니다.
- 수정할 영역의 수정 아이콘( )을 클릭합니다.

영역이 더 이상 필요하지 않은 경우 해당 영역의 휴지통 아이콘을 클릭하여 경로를 삭제합니다. 영역을 삭제하려면 먼저 영역에 종속된 모든 정적 경로를 제거해야 합니다.

단계 **5** 영역의 **Name(**이름**)**을 입력하고 필요한 경우 설명을 입력합니다.

단계 **6** 영역에 포함할 **Interfaces(**인터페이스**)**를 8개까지 선택합니다.

- **+**를 클릭하여 인터페이스를 추가합니다.
- 인터페이스 오른쪽의 **x**를 클릭하여 제거합니다.

인터페이스를 선택할 때 다음 제한 사항에 유의하십시오.

- 물리적 인터페이스, 하위 인터페이스 및 Etherchannel을 선택할 수 있습니다.

- ECMP 트래픽 영역에는 BVI(브리지 그룹) 또는 해당 멤버, Etherchannel 멤버 인터페이스, HA 인터페이스(페일오버 또는 상태 링크), 관리 전용 인터페이스, VTI(virtual tunnel interfaces) 또는 VPN 관리 액세스를 위해 구성된 인터페이스를 포함할 수 없습니다.
- 원격 액세스 또는 사이트 대 사이트 VPN 연결에 사용되는 인터페이스는 포함할 수 없습니다.
- DHCP 릴레이에 대해 활성화된 인터페이스를 서버 또는 에이전트로 선택할 수 없습니다.
- 인터페이스는 동일한 가상 라우터에 할당해야 합니다.
- 인터페이스는 하나의 트래픽 영역에만 있을 수 있습니다.

단계 **7** **OK(**확인**)**를 클릭합니다.

다음에 수행할 작업

이제 Static Routes(정적 경로) 탭으로 이동하여 동일한 대상에 대해 이러한 인터페이스를 통해 동일 비용 경로를 생성할 수 있습니다. 또는 동적 라우팅 프로토콜이 시스템을 통해 배포되는 경우 동일 비용 경로를 자동으로 구성할 수 있습니다.

라우팅 모니터링

라우팅을 모니터링하고 트러블슈팅하려면 CLI 콘솔을 열거나 디바이스 CLI에 로그인하여 다음 명령을 사용합니다. Routing(라우팅) 페이지의 **Commands(**명령**)** 메뉴에서 이러한 명령 중 일부를 선택할 수도 있습니다.

- **show route** 직접 연결된 네트워크의 경로를 비롯하여 데이터 인터페이스에 대한 라우팅 테이블을 표시합니다.
- **show ipv6 route** 직접 연결된 네트워크의 경로를 비롯하여 데이터 인터페이스에 대한 IPv6 라우팅 테이블을 표시합니다.
- **show network**에서 관리 게이트웨이를 비롯하여 가상 관리 인터페이스의 설정을 표시합니다. 관리 게이트웨이로 데이터 인터페이스를 지정하는 경우가 아니면 가상 관리 인터페이스를 통한 라우팅은 데이터 인터페이스 라우팅 테이블에 의해 처리되지 않습니다.
- **show network-static-routes**에서는 **configure network static-routes** 명령을 사용해 가상 관리 인터페이스에 대해 설정된 정적 경로를 표시합니다. 대부분의 경우에는 관리 라우팅에 관리 게이트웨이만 사용하면 되므로, 일반적으로는 정적 경로가 없습니다. 데이터 인터페이스의 트래픽에는 이러한 경로를 사용할 수 없습니다. 이 명령은 CLI 콘솔에서 사용할 수 없습니다.
- **show ospf** OSPF 프로세스 및 확인된 경로에 대한 정보를 표시합니다. **show ospf ?**를 사용하여 OSPF에 대한 특정 정보를 보기 위해 포함할 수 있는 옵션 목록을 가져옵니다.
- **show bgp** 는 BGP 프로세스 및 확인된 경로에 대한 정보를 표시합니다. **show bgp ?**를 사용하여 BGP에 대한 특정 정보를 보기 위해 포함할 수 있는 옵션 목록을 가져옵니다.

- **show eigrp** *option*은 EIGRP 프로세스 및 확인된 경로에 대한 정보를 표시합니다. **show eigrp ?**를 사용하여 포함할 수 있는 옵션 목록을 가져옵니다. 옵션을 제공해야 합니다.
- **show isis** *option*은 IS-IS 프로세스 및 확인된 경로에 대한 정보를 표시합니다. **show isis ?**를 사용하여 포함할 수 있는 옵션 목록을 가져옵니다. 옵션을 제공해야 합니다.
- **show rip database** 는 RIP 프로세스 및 확인된 경로에 대한 정보를 표시합니다.
- **show vrf** 시스템에 정의된 가상 라우터에 대한 정보를 표시합니다.
- **show zone** 각 영역의 일부인 인터페이스를 포함하여 ECMP 트래픽 영역에 대한 정보를 표시합니다.

13 장

가상 라우터

가상 라우터를 생성하여 인터페이스 하위 집합의 트래픽을 서로 분리할 수 있습니다.

가상 라우터 및 VRF(가상 라우팅 및 포워딩) 정보

여러 가상 라우터를 생성하여 인터페이스 그룹에 대해 별도의 라우팅 테이블을 유지 관리할 수 있습니다. 각 가상 라우터에는 자체 라우팅 테이블이 있으므로 디바이스를 통과하는 트래픽에서 명확하게 분리하는 기능을 제공할 수 있습니다.

따라서 공통 네트워킹 장비 집합을 통해 둘 이상의 개별 고객을 지원할 수 있습니다. 또한 가상 라우터를 사용하여 자체 네트워크의 요소를 더 쉽게 분리할 수 있습니다. 일반 목적의 기업 네트워크에서 개발 네트워크를 격리하는 경우를 예로 들 수 있습니다.

가상 라우터에서는 가상 라우팅 및 포워딩의 "light" 버전, 즉 VRF-Lite를 구현합니다. 이는 BGP용 멀티프로토콜 확장(MBGP)을 지원하지 않습니다.

가상 라우터를 생성하는 경우 라우터에 인터페이스를 할당합니다. 특정 인터페이스는 하나의 가상 라우터에만 할당할 수 있습니다. 그런 다음 고정 경로를 정의하고 각 가상 라우터에 대해 OSPF 또는 BGP와 같은 라우팅 프로토콜을 구성합니다. 또한 모든 참여 디바이스의 라우팅 테이블이 동일한 가상 라우터 라우팅 프로세스 및 테이블을 사용하도록 전체 네트워크에 대해 별도의 라우팅 프로세스를 구성합니다. 가상 라우터를 사용하면 동일한 물리적 네트워크를 통해 논리적으로 구분된 네트워크를 생성하여 각 가상 라우터를 통해 실행되는 트래픽의 프라이버시를 확보할 수 있습니다.

라우팅 테이블은 분리되어 있으므로 가상 라우터 전체에서 동일하거나 중복되는 어드레스 스페이스를 사용할 수 있습니다. 예를 들어, 2개의 개별 물리적 인터페이스에서 지원되는 2개의 개별 가상 라우터에 대해 192.168.1.0/24 어드레스 스페이스를 사용할 수 있습니다.

가상 라우터별로 별도의 관리 및 데이터 라우팅 테이블이 있습니다. 예를 들어, 가상 라우터에 관리 전용 인터페이스를 할당하는 경우 해당 인터페이스에 대한 라우팅 테이블은 가상 라우터에 할당된 데이터 인터페이스와는 별개입니다.

가상 라우터 인식 정책 구성

가상 라우터를 생성하면 해당 가상 라우터에 대한 라우팅 테이블이 전역 가상 라우터 또는 다른 모든 가상 라우터와 자동으로 분리됩니다. 그러나 보안 정책에서는 자동으로 가상 라우터를 인식하지 않습니다.

예를 들어 "any" 소스 또는 대상 보안 영역에 적용되는 액세스 제어 규칙을 작성하는 경우, 규칙은 모든 가상 라우터의 모든 인터페이스에 적용됩니다. 이는 실제로 원하는 것과 정확히 같을 수 있습니다. 예를 들어 모든 고객이 유해한 URL 카테고리의 동일한 목록에 대한 액세스를 차단하고자 할 수 있습니다.

그러나 가상 라우터 중 하나에만 정책을 적용해야 하는 경우에는 해당 단일 가상 라우터의 인터페이스만 포함하는 보안 영역을 생성해야 합니다. 그런 다음, 보안 정책의 소스 및 대상 기준에서 가상 라우터 제한 보안 영역을 사용합니다.

해당 멤버십이 단일 가상 라우터에 할당된 인터페이스로 제한되는 보안 영역을 사용하여 다음 정책에서 가상 라우터 인식 규칙을 작성할 수 있습니다.

- 액세스 제어 정책
- 침입 및 파일 정책
- SSL 암호 해독 정책
- ID 정책 및 사용자-IP 주소 매핑 가상 라우터에서 중복 어드레스 스페이스를 사용하는 경우 각 가상 라우터에 대해 별도의 영역을 생성하고 ID 정책 규칙에서 올바르게 적용해야 합니다.

가상 라우터에서 중복 어드레스 스페이스를 사용하는 경우 보안 영역을 사용하여 적절한 정책이 적용되도록 해야 합니다. 예를 들어, 두 개의 개별 가상 라우터에서 192.168.1.0/24 어드레스 스페이스를 사용하는 경우, 두 가상 라우터의 트래픽에 192.168.1.0/24 네트워크가 적용되도록 지정하는 액세스 제어 규칙이 적용됩니다. 원하는 결과가 아닌 경우, 가상 라우터 중 하나에 대해서만 소스/대상 보안 영역을 지정하여 규칙의 적용을 제한할 수 있습니다.

NAT 등의 보안 영역을 사용하지 않는 정책의 경우에는 단일 가상 라우터에 할당된 인터페이스를 소스 및 대상 인터페이스로 선택하여 가상 라우터에 해당하는 규칙을 작성할 수 있습니다. 별도의 두 가상 라우터에서 소스 및 대상 인터페이스를 선택하는 경우, 해당 규칙이 작동하도록 가상 라우터 간에 적절한 경로가 있는지 확인해야 합니다.

가상 라우터 간 라우팅

가상 라우터 간의 트래픽을 라우팅하는 정적 경로를 구성할 수 있습니다.

예를 들어 전역 가상 라우터에 외부 인터페이스가 있는 경우, 각각의 다른 가상 라우터에서 정적 기본 경로를 설정하여 외부 인터페이스로 트래픽을 전송할 수 있습니다. 그런 다음, 지정된 가상 라우터 내에서 라우팅할 수 없는 모든 트래픽은 후속 라우팅을 위해 전역 라우터로 전송됩니다.

다른 가상 라우터로의 트래픽을 유출하고 있으므로 가상 라우터 간의 정적 경로를 경로 유출이라고 합니다. VR1 경로에서 VR2로 경로를 유출하는 경우 VR2에서 VR1로만 연결을 시작할 수 있습니다. VR1에서 VR2로의 트래픽을 전송하려면 역방향 경로를 구성해야 합니다. 다른 가상 라우터의 인터

페이스에 대한 정적 경로를 생성할 경우 게이트웨이 주소를 지정하지 않아도 됩니다. 대상 인터페이스만 선택하면 됩니다.

가상 라우터 간 경로의 경우, 시스템에서는 소스 가상 라우터에서 대상 인터페이스를 조회합니다. 그런 다음, 대상 가상 라우터에서 다음 홉의 MAC 주소를 조회합니다. 따라서 대상 가상 라우터에는 대상 주소에 대해 선택된 인터페이스의 동적(학습한) 또는 정적 경로가 있어야 합니다.

서로 다른 가상 라우터에서 소스 및 대상 인터페이스를 사용하는 NAT 규칙을 구성하면 가상 라우터 간의 트래픽이 라우팅될 수도 있습니다. NAT에 대해 경로 조회를 수행하는 옵션을 선택하지 않을 경우, 대상 변환이 발생할 때마다 규칙에 따라 NAT 적용 주소가 있는 대상 인터페이스로 트래픽이 전송됩니다. 그러나 대상 가상 라우터에는 변환된 대상 IP 주소에 대한 경로가 있어야 next-hop 조회가 성공할 수 있습니다.

디바이스 모델별 최대 가상 라우터 수

생성할 수 있는 최대 가상 라우터 수는 디바이스 모델에 따라 다릅니다. 다음 표에는 최대 한도가 나와 있습니다. 글로벌 가상 라우터를 포함하지 않는 해당 플랫폼에 대해 최대 사용자 정의 가상 라우터 수를 표시하는 **show vrf counters** 명령을 입력하여 시스템을 두 번 확인할 수 있습니다. 아래 표의 숫자에는 사용자 및 글로벌 라우터가 포함되어 있습니다. Firepower 4100/9300의 경우 이러한 숫자는 네이티브 모드에 적용됩니다.

Firepower 4100/9300 등의 다중 인스턴스 기능을 지원하는 플랫폼의 경우 최대 가상 라우터를 디바이스의 코어 수만큼 분할한 다음 가장 근접한 정수로 내림하여 인스턴스에 할당된 코어 수를 곱하여 컨테이너 인스턴스 당 최대 가상 라우터 수를 결정합니다. 예를 들어 플랫폼에서 최대 100개의 가상 라우터를 지원하고 70 코어를 보유한 경우, 각 코어는 최대 1.43개의 가상 라우터(내림됨)를 지원합니다. 따라서 6개의 코어에 할당된 인스턴스는 8.58 가상 라우터를 지원하며, 이 라우터는 8개로 내림되며, 10개의 코어가 할당된 인스턴스는 14.3 가상 라우터(내림함, 14)를 지원합니다.

디바이스 모델	최대 가상 라우터 수
Firepower 1010	가상 라우터는 이 모델에서 지원되지 않습니다.
Firepower 1120	5
Firepower 1140	10
Firepower 1150	10
Firepower 2110	10
Firepower 2120	20
Firepower 2130	30
Firepower 2140	40
Secure Firewall 3110	15
Secure Firewall 3120	25
Secure Firewall 3130	50

디바이스 모델	최대 가상 라우터 수
Secure Firewall 3140	100
Firepower 4110	60
Firepower 4112	60
Firepower 4115	80
Firepower 4120	80
Firepower 4125	100
Firepower 4140	100
Firepower 4145	100
Firepower 4150	100
Firepower 9300 Appliance, 모든 모델	100
Threat Defense Virtual, 모든 플랫폼	30
ISA 3000	10

가상 라우터 지침

디바이스 모델 지침

다음을 제외하고 모든 지원 디바이스 모델에서 가상 라우터를 구성할 수 있습니다.

- Firepower 1010

추가 지침

- 글로벌 가상 라우터에서만 다음 기능을 구성할 수 있습니다.
  - OSPFv3
  - RIP
  - EIGRP
  - IS-IS
  - BGPv6
  - 멀티캐스트 라우팅

  - 정책 기반 라우팅
  - VPN
- 각 가상 라우터에 대해 다음 기능을 개별적으로 구성할 수 있습니다.
  - 고정 경로 및 해당 SLA 모니터
  - OSPFv2
  - BGPv4
- 다음 기능은 원격 시스템을 통해 쿼리하거나 통신할 때 시스템에서 사용됩니다(from-the-box 트래픽). 이러한 기능에서는 글로벌 가상 라우터의 인터페이스만 사용합니다. 이 기능을 위해 인터페이스를 구성하는 경우 해당 인터페이스는 글로벌 가상 라우터에 속해야 합니다. 일반적으로 시스템에서는 자체 관리 목적으로 외부 서버에 연결하기 위해 경로를 조회해야 할 때마다 글로벌 가상 라우터에서 경로 조회를 수행합니다.
  - 액세스 제어 규칙 또는 **ping** 명령의 이름을 확인할 때 사용되는 정규화된 이름을 확인하는 데 사용되는 DNS 서버입니다. DNS 서버에 대한 인터페이스로 **any**를 지정하면 시스템에서는 글로벌 가상 라우터의 인터페이스만 고려합니다.
  - VPN과 함께 사용하는 경우 ID 영역 또는 AAA 서버입니다. 글로벌 가상 라우터의 인터페이스에서만 VPN을 구성할 수 있으므로, VPN에 사용되는 외부 AAA 서버(예: Active Directory)는 글로벌 가상 라우터의 인터페이스를 통해 연결할 수 있어야 합니다.
  - Syslog 서버.
  - SNMP.
- NAT에서 다른 가상 라우터에 할당된 소스 및 대상 인터페이스를 지정하는 경우 NAT 규칙에서는 다른 가상 라우터를 통해 하나의 가상 라우터에서 트래픽을 전환합니다. NAT 규칙에서 인터페이스를 실수로 혼합하지 않았는지 확인합니다. 일반적으로 소스 및 대상 인터페이스가 사용되며 수동 NAT의 대상 변환에 대한 라우팅 테이블을 포함하여 해당 라우팅 테이블이 무시됩니다. 그러나 NAT 규칙에서 경로 조회를 수행해야 하는 경우에는 인바운드 인터페이스에 대해서만 VRF 테이블에서 조회를 수행합니다. 필요한 경우 소스 가상 라우터에서 대상 인터페이스에 대한 고정 경로를 정의합니다. 인터페이스를 **any**로 둘 경우, 가상 라우터 멤버십에 관계없이 규칙이 모든 인터페이스에 적용됩니다. 가상 라우터를 사용할 경우 NAT 규칙을 신중하게 테스트하여 정상적인 동작이 나오는지 확인하십시오. 필요한 경로 유출을 정의하는 것을 잊은 경우, 어떤 경우에는 해당 규칙은 일치하는 것으로 예상되는 모든 트래픽과 일치하지 않을 수 있으며 변환이 적용되지 않습니다.
- 가상 라우터 간 경로를 구성할 경우(예: 한 가상 라우터에서 두 번째 가상 라우터로 경로를 유출하는 경우), 시스템에서는 소스 가상 라우터에서 대상 인터페이스 조회를 수행합니다. 그런 다음, 대상 가상 라우터에서 다음 홉의 MAC 주소를 조회합니다. 따라서 대상 가상 라우터에는 대상 주소에 대해 선택된 인터페이스의 동적(학습한) 또는 정적 경로가 있어야 합니다.
- 예를 들어 가상 라우터 1에서 가상 라우터 2로의 가상 라우터 간 경로(누출된 경로)를 사용하는 경우 반환 트래픽을 허용하기 위해 가상 라우터 2에서 미러(역방향) 경로를 설정할 필요가 없습

니다. 하지만 연결이 양방향에서 시작되도록 하려면 가상 라우터 1에서 2로, 그리고 가상 라우터 2에서 1로, 양방향으로 경로를 누출해야 합니다.

- 한 가상 라우터에서 다른 가상 라우터로 인터페이스를 이동할 경우, 해당 인터페이스에 대해 구성된 모든 기능이 유지됩니다. 컨피그레이션을 검토하여 새 가상 라우터의 컨텍스트 내에서 정적 경로, IP 주소, 기타 정책이 적합한지 확인합니다.
- 여러 가상 라우터에서 중복 어드레스 스페이스를 사용하는 경우 Cisco ISE(Identity Services Engine)에서 다운로드한 IP 주소 매핑에 대한 고정 SGT(보안 그룹 태그)에서 가상 라우터를 인식하지 않는다는 점에 유의하십시오. 가상 라우터마다 서로 다른 SGT 매핑을 생성해야 하는 경우 가상 라우터마다 별도의 ID 영역을 설정합니다. 각 가상 라우터에서 동일한 SGT 번호에 동일한 IP 주소를 매핑하려는 경우에는 이 작업이 필요하지 않습니다.
- 여러 가상 라우터에서 중복 어드레스 스페이스를 사용하는 경우 대시보드 데이터가 잘못될 수 있습니다. 동일한 IP 주소에 대한 연결이 집계되므로, 두 개 이상의 엔드포인트에서 공유되는 경우 특정 주소로 오고가는 트래픽이 더 많았던 것으로 표시됩니다. 별도의 ID 영역을 사용하여 ID 정책을 신중하게 구성하는 경우에는 사용자 기반 통계가 더 정확해야 합니다.
- 별도의 가상 라우터에서는 중복 DHCP 주소 풀을 사용할 수 없습니다.
- 전역 가상 라우터의 인터페이스에서만 DHCP 서버 자동 컨피그레이션을 사용할 수 있습니다. 자동 컨피그레이션은 사용자 정의 가상 라우터에 할당된 인터페이스에 대해 지원되지 않습니다.
- 전역 가상 라우터에서 새 라우터로 이동하는 등 인터페이스를 한 가상 라우터에서 다른 가상 라우터로 이동할 경우, 인터페이스를 통한 모든 기존 연결이 삭제됩니다.
- 보안 인텔리전스 정책에서는 가상 라우터를 인식하지 않습니다. IP 주소, URL 또는 DNS 이름을 차단 목록에 추가하면 해당 항목이 모든 가상 라우터에 대해 차단됩니다.

가상 라우터 관리

가상 라우터라고 하는 여러 VRF(가상 라우팅 및 포워딩) 인스턴스를 생성하여 인터페이스 그룹에 대해 별도의 라우팅 테이블을 유지 관리할 수 있습니다. 각 가상 라우터에는 자체 라우팅 테이블이 있으므로 디바이스를 통과하는 트래픽에서 명확하게 분리하는 기능을 제공할 수 있습니다.

따라서 공통 네트워킹 장비 집합을 통해 둘 이상의 개별 고객을 지원할 수 있습니다. 또한 가상 라우터를 사용하여 자체 네트워크의 요소를 더 쉽게 분리할 수 있습니다. 일반 목적의 기업 네트워크에서 개발 네트워크를 격리하는 경우를 예로 들 수 있습니다.

기본적으로 가상 라우팅은 비활성화되어 있습니다. 전체 디바이스에서는 데이터(통과) 및 관리(to/from the box) 트래픽용으로 글로벌 라우팅 테이블의 단일 집합을 사용합니다.

가상 라우팅을 활성화할 경우 초기 라우팅 페이지는 시스템에 정의된 가상 라우터의 목록입니다. 가상 라우터를 활성화하지 않을 경우 초기 라우팅 페이지는 시스템에 정의된 고정 경로의 목록입니다.

글로벌 가상 라우터는 항상 있습니다. 글로벌 라우터에서는 개별 가상 라우터에 할당되지 않은 모든 인터페이스를 보유합니다.

프로시저

단계 **1** 디바이스를 클릭한 다음, **Routing(**라우팅**)** 요약의 링크를 클릭합니다.

단계 **2** 가상 라우터를 아직 활성화하지 않은 경우 **Add Multiple Virtual Routers(**여러 가상 라우터 추가**)** 링크를 클릭한 다음, **Create First Custom Virtual Router(**첫 번째 맞춤형 가상 라우터 생성**)**를 클릭합니다.

첫 번째 가상 라우터를 생성하는 것은 기본적으로 추가 가상 라우터를 생성하는 것과 동일합니다. 자세한 내용은 가상 라우터 생성 또는 인터페이스 할당 수정, 353 페이지의 내용을 참고하십시오.

단계 **3** 다음 중 하나를 수행합니다.

- 모든 가상 라우터에 적용되는 글로벌 BGP 설정을 구성하려면 **BGP Global Settings(BGP** 글로벌 설정**)** 버튼을 클릭합니다. Smart CLI를 사용하여 이러한 설정을 구성합니다. 이 내용은 스마트 CLI 개체 구성, 918 페이지에 설명되어 있습니다. 하나 이상의 가상 라우터에서 BGP를 구성하는 경우에만 글로벌 BGP 설정을 구성합니다.
- 새 가상 라우터를 생성하려면 테이블 위의 + 버튼을 클릭합니다.
- 가상 라우터의 라우팅 속성을 수정하려면, 예를 들어, 고정 경로를 생성하거나 라우팅 프로세스를 정의하려면 가상 라우터의 Action(작업) 셀에서 보기 아이콘()을 클릭합니다.
- 가상 라우터의 이름, 설명 또는 인터페이스 할당을 수정하려면 가상 라우터의 Action(작업) 셀에서 보기 아이콘()을 클릭한 다음, **Virtual Router Properties(**가상 라우터 속성**)** 탭을 선택합니다.
- 해당 내용을 볼 때 가상 라우터 간에 전환하려면, 가상 라우터 이름 옆의 아래쪽 화살표(라우팅 테이블 위)를 클릭하고 원하는 가상 라우터를 선택합니다. **Go Back to Virtual Routers(**가상 라우터로 돌아가기**)** 화살표()를 클릭하여 목록 페이지로 돌아갈 수 있습니다.
- 가상 라우터를 삭제하려면 가상 라우터의 Action(작업) 셀에서 삭제 아이콘()을 클릭하거나 가상 라우터의 콘텐츠를 볼 때 가상 라우터 이름 옆의 삭제 아이콘을 클릭합니다. 마지막 가상 라우터(글로벌 라우터 외에는 삭제할 수 없음)를 삭제하면 VRF가 비활성화됩니다.
- 가상 라우터에서 라우팅을 모니터링하려면 해당 가상 라우터의 테이블에서 **show** 명령 중 하나에 대한 링크를 클릭합니다. 명령을 클릭하면 CLI 콘솔이 열려 CLI 명령의 출력을 검사할 수 있습니다. 경로, OSPF 및 OSPF 네이버에 대한 정보를 표시할 수 있습니다. 명령 출력은 구축된 구성을 기반으로 합니다. 구축되지 않은 수정 작업과 관련된 내용은 표시되지 않습니다.

  가상 라우터를 볼 때 **Commands(**명령**)** 드롭다운 목록에서 해당 명령을 선택하여 이러한 명령을 실행할 수도 있습니다.

가상 라우터 생성 또는 인터페이스 할당 수정

가상 라우터에서 고정 경로 또는 라우팅 프로세스를 구성하려면 먼저 라우터를 생성하고 인터페이스를 할당해야 합니다.

시작하기 전에

Interface(인터페이스**)** 페이지로 이동하여 가상 라우터에 추가하려는 각 인터페이스에 이름이 있는지 확인합니다. 이름이 있는 경우에만 가상 라우터에 인터페이스를 추가할 수 있습니다.

프로시저

단계 **1** **Device(**디바이스**)** > **Routing(**라우팅**)**을 클릭합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 가상 라우터를 아직 생성하지 않은 경우 **Add Multiple Virtual Routers(**여러 가상 라우터 추가**)** 링크를 클릭한 다음, **Create First Custom Virtual Router(**첫 번째 맞춤형 가상 라우터 생성**)**를 클릭합니다.
- 새 가상 라우터를 하나 생성하려면 가상 라우터 목록 위의 **+** 버튼을 클릭합니다.
- 가상 라우터의 수정 아이콘( )을 클릭하여 해당 속성 및 인터페이스 목록을 수정합니다.
- 가상 라우터를 볼 때 **Virtual Router Properties(**가상 라우터 속성**)** 탭을 클릭하여 보고 있는 가상 라우터의 속성을 수정합니다.
- 가상 라우터를 볼 때 가상 라우터 이름 옆의 아래쪽 화살표를 클릭하고 **Create New Virtual Router(**새 가상 라우터 생성**)**를 클릭합니다.

단계 **3** 다음과 같이 가상 라우터의 속성을 구성합니다.

- **Name(**이름**)** - 가상 라우터의 이름입니다.
- **Description(**설명**)** - 가상 라우터의 설명(선택 사항)입니다.
- **Interfaces(**인터페이스**)** - **+**를 클릭하여 가상 라우터에 포함되어야 하는 각 인터페이스를 선택합니다. 인터페이스를 제거하려면 인터페이스 위에 마우스 커서를 올려 놓고 인터페이스 카드의 오른쪽에 있는 **X**를 클릭합니다. 물리적 인터페이스, 하위 인터페이스, 브리지 그룹, EtherChannel은 가상 라우터에 할당할 수 있지만 VLAN은 할당할 수 없습니다.

  다른 인터페이스에 대한 경로를 가상 라우팅 테이블로 의도적으로 유출하지 않는 한, 라우팅 테이블은 이러한 인터페이스로 제한됩니다.

  진단(Management X/Y) 인터페이스를 전역 가상 라우터에만 할당할 수 있습니다.

단계 **4** **OK(**확인**)** 또는 **Save(**저장**)**를 클릭합니다.

고정 경로 또는 라우팅 프로세스를 구성할 수 있는 이 가상 라우터의 보기로 이동하게 됩니다.

가상 라우터에서 고정 경로 및 라우팅 프로세스 구성

각 가상 라우터에는 자체 정적 경로 및 라우팅 프로세스가 있습니다. 이 둘은 다른 가상 라우터에 대해 정의된 경로 및 라우팅 프로세스와 별개로 작동합니다.

고정 경로를 구성할 때 가상 라우터 외부에 있는 대상 인터페이스를 선택할 수 있습니다. 그러면 대상 인터페이스가 포함된 가상 라우터로 경로가 유출됩니다. 더 많은 트래픽을 다른 가상 라우터로 전송하지 않도록 하려면 유출해야 하는 경로만 유출해야 합니다. 예를 들어 인터넷에 대한 경로가 하나 있는 경우, 인터넷으로 향하는 트래픽에 대해 각 가상 라우터에서 인터넷 연결 가상 라우터로 경로가 유출되어야 합니다.

프로시저

단계 **1** **Device(**디바이스**)** > **Routing(**라우팅**)**을 선택합니다.

단계 **2** 가상 라우터의 Action(작업) 셀에서 보기 아이콘( )을 클릭하여 엽니다.

단계 **3** 다음 중 하나를 수행합니다.

- 고정 경로를 구성하려면 **Static Routing(**고정 라우팅**)** 탭을 클릭한 다음, 경로를 생성하거나 수정합니다. 자세한 내용은 고정 경로 구성, 339 페이지를 참조하십시오.
- ECMP(Equal-Cost Multi-Path) 트래픽 영역을 구성하려면 **ECMP Traffic Zones(ECMP** 트래픽 영역**)** 탭을 클릭한 다음 영역을 생성합니다. 자세한 내용은 ECMP 트래픽 영역 구성, 342 페이지를 참조하십시오.
- BGP 라우팅 프로세스를 구성하려면 **BGP** 탭을 클릭한 다음, 프로세스를 정의하는 데 필요한 Smart CLI 개체를 생성합니다. 자세한 내용은 BGP(Border Gateway Protocol), 435 페이지를 참조하십시오.

  또한 모든 가상 라우터에 적용되는 BGP에 대한 글로벌 설정도 있습니다. 이러한 속성을 구성하려면 가상 라우터 목록 페이지로 돌아가서 **BGP Global Settings(BGP** 글로벌 설정**)** 버튼을 클릭해야 합니다.
- OSPF 라우팅 프로세스를 구성하려면 **OSPF** 탭을 클릭한 다음, 최대 2개의 프로세스를 정의하는 데 필요한 Smart CLI 개체 및 그와 연관된 인터페이스 구성을 생성합니다. 자세한 내용은 OSPF(Open Shortest Path First), 393 페이지를 참조하십시오.
- (전역 가상 라우터 전용) EIGRP 라우팅 프로세스를 구성하려면 **EIGRP** 탭을 클릭한 다음, 단일 프로세스를 정의하는 데 필요한 스마트 CLI 개체를 생성합니다. 자세한 내용은 EIGRP(Enhanced Interior Gateway Routing Protocol), 415 페이지를 참조하십시오.

가상 라우터 삭제

가상 라우터가 더 이상 필요하지 않은 경우에는 삭제할 수 있습니다. 글로벌 가상 라우터는 삭제할 수 없습니다.

가상 라우터를 삭제하면 가상 라우터 내에 구성된 모든 고정 경로 및 라우팅 프로세스도 삭제됩니다.

가상 라우터에 할당된 모든 인터페이스는 글로벌 라우터에 다시 할당됩니다.

프로시저

단계 **1** **Device(**디바이스**)** > **Routing(**라우팅**)**을 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 가상 라우터 목록에서 가상 라우터의 Action(작업) 열에 있는 삭제 아이콘( )을 클릭합니다.
- 삭제할 가상 라우터를 볼 때 라우터 이름 옆의 삭제 아이콘( )을 클릭합니다.

가상 라우터를 삭제할 것인지 확인해 달라는 메시지가 표시됩니다.

단계 **3** **OK(**확인**)**를 클릭하여 삭제를 확인합니다.

가상 라우터의 예시

다음 주제에서는 가상 라우터 구현에 대한 예시를 제공합니다.

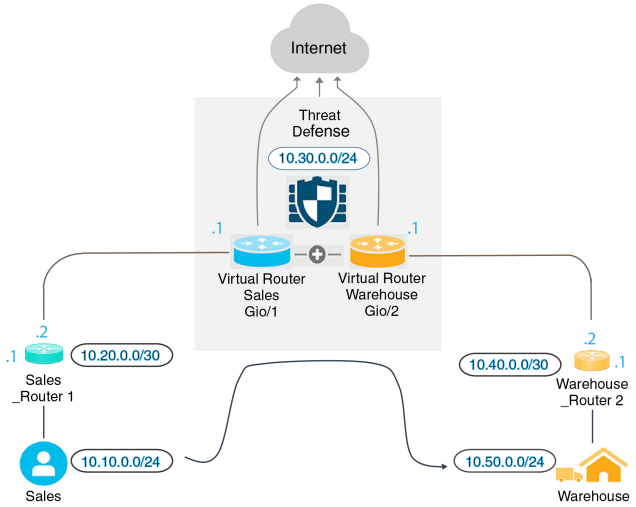
관련 항목

사이트 간 VPN을 통해 여러 가상 라우터의 네트워크에서 트래픽을 보호하는 방법, 719 페이지
RA VPN 액세스를 다른 가상 라우터의 내부 네트워크에 허용하는 방법, 799 페이지

여러 가상 라우터를 통해 원거리 서버로 라우팅하는 방법

가상 라우터를 사용할 경우, 한 가상 라우터에 있는 사용자가 별도의 가상 라우터를 통해서만 연결할 수 있는 서버에 액세스해야 하는 상황이 발생할 수 있습니다.

다음 사례를 고려하십시오. 영업 팀의 워크스테이션은 영업 가상 라우터에 연결되어 있습니다. 창고 서버는 창고 가상 라우터를 통해 연결되어 있습니다. 영업 팀이 IP 주소가 10.50.0.5/24인 창고 서버에서 정보를 조회해야 할 경우, 영업 가상 라우터의 경로를 창고 가상 라우터로 유출해야 합니다. 창고 가상 라우터는 창고 라우터 2 뒤에 멀티 홉 떨어진 창고 서버에 대한 경로도 있어야 합니다.



시작하기 전에

이 예시에서는 다음 항목을 이미 구성한 것으로 가정합니다.

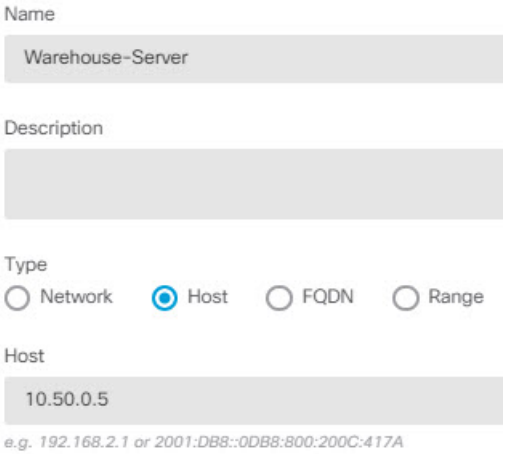
- threat defense 디바이스에서 영업 가상 라우터와 창고 가상 라우터의 경우 GigabitEthernet 0/1은 영업에 할당되고, GigabitEthernet 0/2는 창고에 할당되었습니다.
- 영업 라우터 1에는 트래픽을 10.20.0.1/30 인터페이스에서 벗어나 10.50.0.5/24로 전송하는 정적 또는 동적 경로가 있습니다.

프로시저

단계 **1** 10.50.0.5/24 또는 10.50.0.0/24에 대한 네트워크 개체를 생성합니다. 또한, 게이트웨이 10.40.0.2/30에 대한 개체를 생성합니다.

경로를 창고 서버의 단일 IP 주소로 제한하려는 경우, 호스트 개체를 사용하여 10.50.0.5를 정의합니다. 또는 영업 팀이 창고에 있는 다른 시스템에 액세스해야 하는 경우, 10.50.0.0/24 네트워크에 대한 네트워크 개체를 생성합니다. 이 예시에서는 호스트 IP 주소에 대한 경로를 생성합니다.

a) 목차에서 **Objects(**개체**)**와 **Network(**네트워크**)**를 차례로 선택합니다.
b) +를 클릭한 다음 창고 서버에 대한 개체 속성을 입력합니다.



c) **OK(**확인**)**를 클릭합니다.

d) **+**를 클릭한 다음, 창고 네트워크로 연결되는 라우터 게이트웨이에 대한 개체 속성을 입력합니다.

e) **OK(**확인**)**를 클릭합니다.

단계 **2** 창고 가상 라우터에 있는 Gi0/2 인터페이스를 가리키는 영업 가상 라우터의 경로 유출을 정의합니다.

이 예시에서는 Gi0/1의 이름이 inside로 지정되고, Gi0/2가 inside-2로 지정되었습니다.

a) **Device(**디바이스**)**를 선택한 다음 **Routing(**라우팅**)** 요약에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

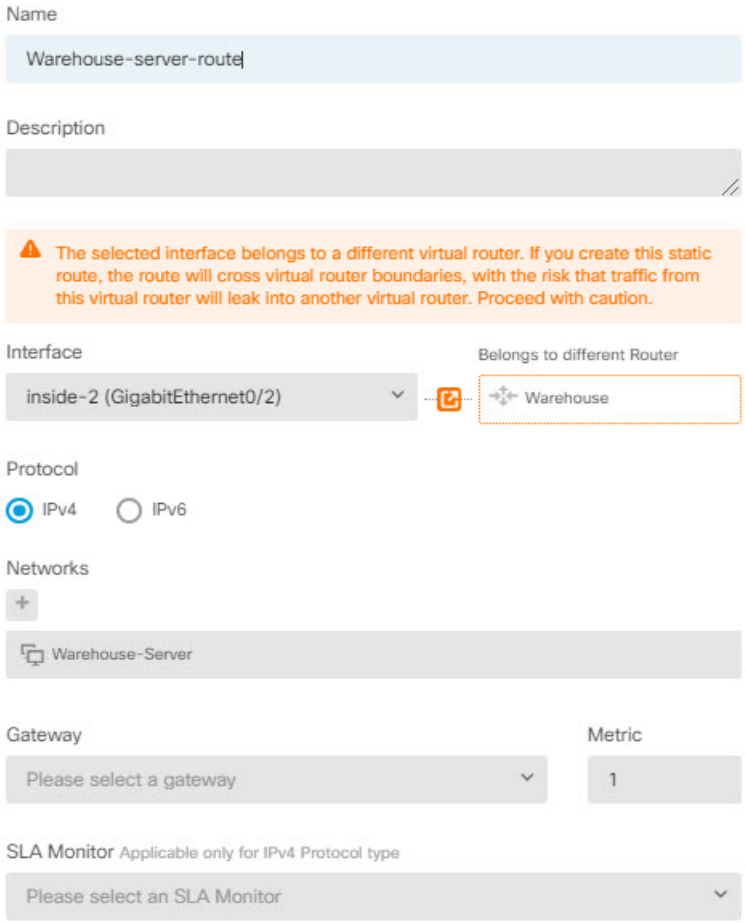
b) 가상 라우터 목록에서 영업 가상 라우터의 작업 열에 있는 보기 아이콘( )을 클릭합니다.

c) **Static Routing(**정적 라우팅**)** 탭에서 **+**를 클릭하고 다음과 같이 경로를 구성합니다.

- **Name(**이름**)** — 모든 이름을 지정할 수 있습니다(예: Warehouse-server-route).
- **Interface(**인터페이스**)** — **inside-2**를 선택합니다. 인터페이스가 다른 라우터에 있으며 경로 유출이 생성된다는 경고 메시지가 표시됩니다. 이는 사용자가 수행하려는 작업입니다.
- **Protocol(**프로토콜**)** — 이 예에서는 **IPv4**를 사용합니다. 또한 IPv6 주소를 사용하여 이 예시를 구현할 수 있습니다.

- **Networks(**네트워크**)** — Warehouse-Server 개체를 선택합니다.
- **Gateway(**게이트웨이**)** — 이 항목은 비워둡니다. 다른 가상 라우터로 경로를 유출할 경우에는 게이트웨이 주소를 선택하지 않습니다.

대화 상자가 다음과 비슷하게 표시됩니다.

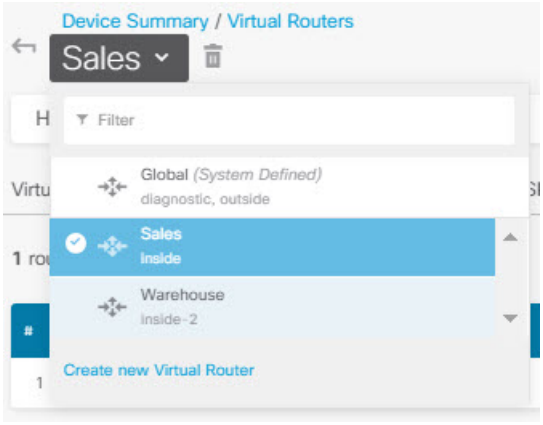


d) **OK(**확인**)**를 클릭합니다.

단계 **3** 창고 가상 라우터에서 창고 라우터 2 게이트웨이를 가리키는 경로를 정의합니다.

또는, 창고 라우터 2에서 경로를 동적으로 검색하는 라우팅 프로토콜을 구성하여 이 작업을 수행할 수 있습니다. 이 예에서는 정적 경로를 정의합니다.

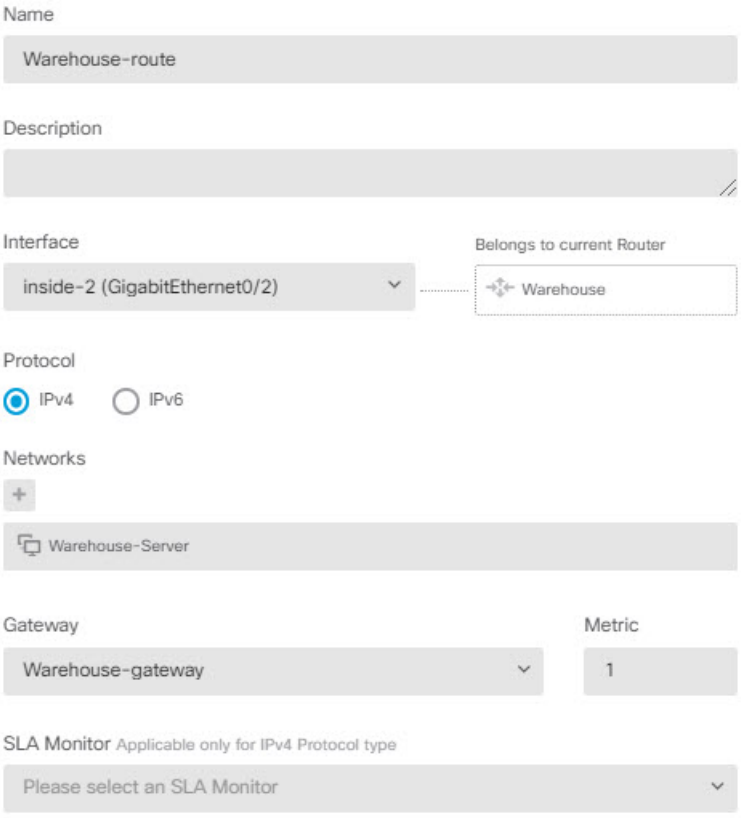
a) 현재 Sales(영업)라고 표시된 가상 라우터 드롭다운 목록에서 창고 가상 라우터를 선택하여 라우터를 전환합니다.



b) **Static Routing(**정적 라우팅**)** 탭에서 **+**를 클릭하고 다음과 같이 경로를 구성합니다.

- **Name(**이름**)** — 모든 이름을 지정할 수 있습니다(예: Warehouse-route).
- **Interface(**인터페이스**)** — **inside-2**를 선택합니다.
- **Protocol(**프로토콜**)** — **IPv4**를 선택합니다.
- **Networks(**네트워크**)** — Warehouse-Server 개체를 선택합니다.
- **Gateway(**게이트웨이**)** — Warehouse-gateway 개체를 선택합니다.

대화 상자가 다음과 비슷하게 표시됩니다.

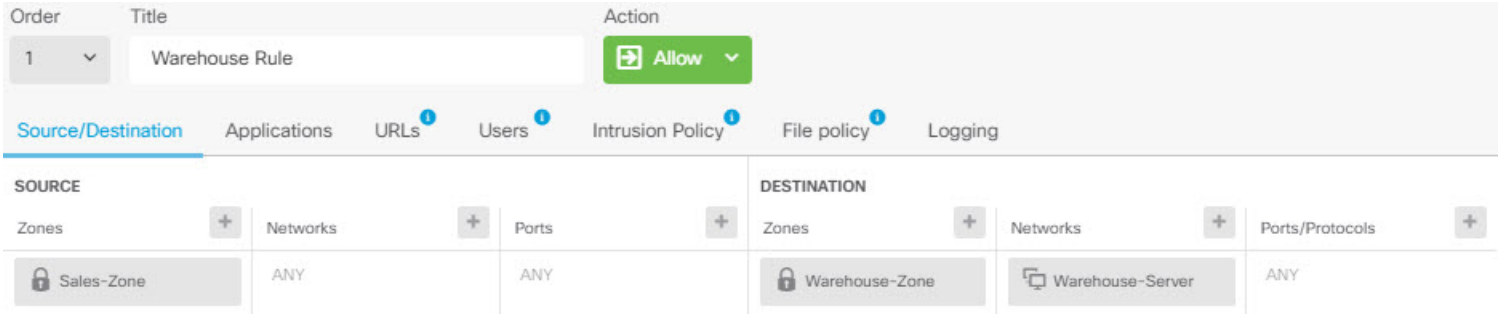


c) **OK(**확인**)**를 클릭합니다.

단계 **4** 창고 서버에 대한 액세스를 허용하는 액세스 제어 규칙이 있는지 확인합니다.

가장 단순한 규칙을 사용할 경우, 영업 가상 라우터에 있는 소스 인터페이스의 트래픽을 대상 Warehouse-Server 네트워크 개체에 대한 창고 가상 라우터에 있는 대상 인터페이스로 전송할 수 있습니다. 적절하다고 판단될 경우 침입 검사를 트래픽에 적용할 수 있습니다.

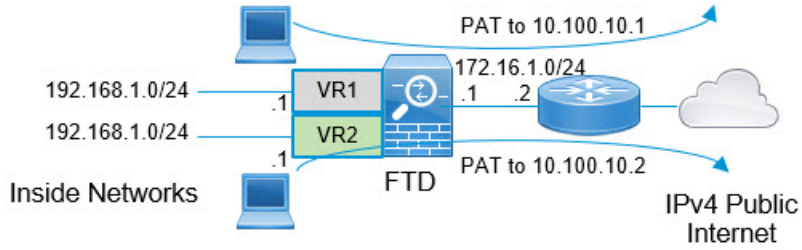
예를 들어 영업 가상 라우터에 있는 인터페이스가 Sales-Zone 보안 영역에 있을 경우, 창고 가상 라우터에 있는 해당 인터페이스는 Warehouse-Zone 보안 영역에 존재하며 액세스 제어 규칙은 다음과 유사합니다.



중복된 어드레스 스페이스가 있는 여러 가상 라우터에 인터넷 액세스를 제공하는 방법

가상 라우터를 사용할 경우, 별도의 라우터에 상주하는 인터페이스에 대해 동일한 네트워크 주소를 사용할 수 있습니다. 예를 들어 내부 및 내부-2 인터페이스를 정의하여 두 인터페이스가 모두 192.168.1.1/24라는 IP 주소를 사용하도록 하고 192.168.1.0/24 네트워크의 해당 세그먼트에서 엔드포인트를 관리할 수 있습니다. 그러나 이러한 별도의 가상 라우터에서 라우팅되는 IP 주소가 동일하므로, 반환 트래픽이 올바른 대상으로 이동하도록 하려면 가상 라우터에서 나가는 트래픽을 신중하게 처리해야 합니다.

예를 들어 동일한 어드레스 스페이스를 사용하는 두 개의 가상 라우터에서 인터넷 액세스를 허용하려면, 각 가상 라우터 내의 인터페이스에 개별적으로 NAT 규칙을 적용해야 합니다. 이 경우 별도의 NAT 또는 PAT 풀을 사용하는 것이 좋습니다. PAT를 사용하여 가상 라우터 1의 소스 주소를 10.100.10.1로 변환하고, 가상 라우터 2의 소스 주소를 10.100.10.2로 변환할 수 있습니다. 아래 그림에는 이러한 설정이 나와 있습니다. 여기서 인터넷 연결 외부 인터페이스는 전역 라우터의 일부입니다. 소스 인터페이스를 명시적으로 선택한 상태에서 NAT/PAT 규칙을 정의해야 합니다. 왜냐하면 "any"를 소스 인터페이스로 사용할 경우 2개의 서로 다른 인터페이스에 동일한 IP 주소가 존재할 수 있으므로, 시스템에서 올바른 소스를 식별하는 것이 불가능하기 때문입니다.



참고 이 예는 각 가상 라우터에 단일 인터페이스가 포함된 단순화된 예입니다. "내부" 가상 라우터에 둘 이상의 인터페이스가 있을 경우 각 "내부" 인터페이스에 대해 NAT 규칙을 생성해야 합니다. 중복된 어드레스 스페이스를 사용하지 않는 가상 라우터 내에 일부 인터페이스가 있는 경우에도 NAT 규칙의 소스 인터페이스를 명시적으로 식별하면 문제를 더 쉽게 해결할 수 있으며, 인터넷에 바인딩된 가상 라우터에서 나가는 트래픽을 더 명확하게 분리할 수 있습니다.

프로시저

단계 **1** 가상 라우터 1(VR1)에 대한 내부 인터페이스를 구성합니다.

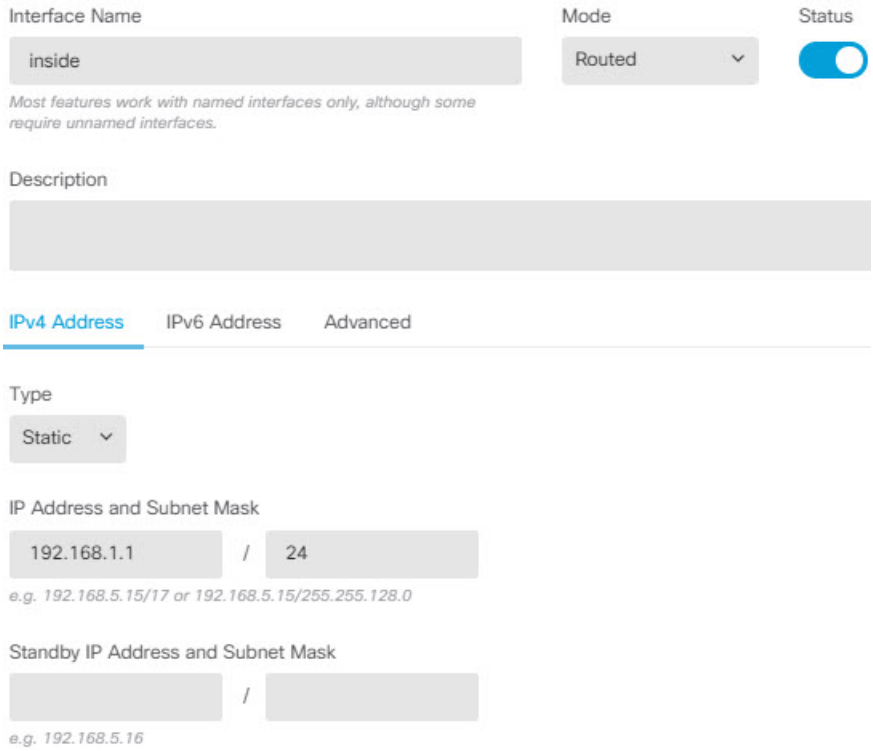
a) 디바이스를 클릭한 다음, **Interfaces(**인터페이스**)** 요약에서 **View All Interfaces(**모든 인터페이스 보기**)**를 클릭합니다.

b) VR1에 할당할 인터페이스에 대한 Action(작업) 열에서 수정 아이콘( )을 클릭합니다.

c) 다음 속성을 하나 이상 구성합니다.

- **Name(**이름**)** — 이 예에서는 **inside**로 지정합니다.

- **Mode(모드) - Routed(라우팅)**를 선택합니다.
- **Status(상태)** — 인터페이스를 활성화합니다.
- **IPv4 Address(IPv4 주소) > Type(유형)**— **Static(고정)**을 선택합니다.
- **IPv4 Address and Subnet Mask(IPv4 주소 및 서브넷 마스크)** — 192.168.1.1/24를 입력합니다.



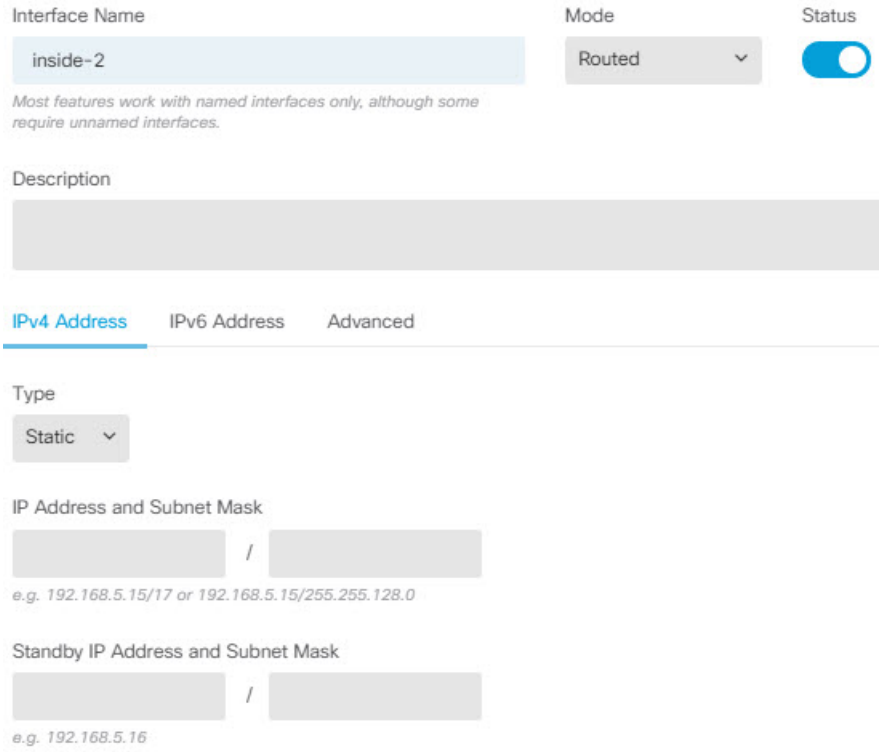
d) **OK(확인)**를 클릭합니다.

단계 **2** 가상 라우터 2(VR2)에 대한 inside-2 인터페이스를 구성하되, IP 주소는 지정하지 않습니다.

a) Interfaces(인터페이스) 목록 페이지에서 VR2에 할당할 인터페이스에 대한 Action(작업) 열에서 수정 아이콘( )을 클릭합니다.

b) 다음 속성을 하나 이상 구성합니다.

- **Name(이름)** — 이 예에서는 **inside-2**로 지정합니다.
- **Mode(모드) - Routed(라우팅)**를 선택합니다.
- **Status(상태)** — 인터페이스를 활성화합니다.
- **IPv4 Address(IPv4 주소) > Type(유형)**— **Static(고정)**을 선택합니다.
- **IPv4 Address and Subnet Mask(IPv4 주소 및 서브넷 마스크)** — 이 필드는 비워둡니다. 이 단계에서 내부 인터페이스와 동일한 주소를 구성하려고 할 경우, 시스템에 오류 메시지가 표시되며 기능 이외의 컨피그레이션을 생성할 수 없습니다. 동일한 라우터 내에서는 서로 다른 인터페이스를 통해 동일한 어드레스 스페이스로 라우팅할 수 없습니다.



c) **OK(**확인**)**를 클릭합니다.

단계 **3** 외부 인터페이스에 대한 정적 기본 경로 유출을 포함하여, 가상 라우터 VR1을 구성합니다.

a) **Device(**디바이스**)**를 선택한 다음 **Routing(**라우팅**)** 요약에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

b) Routing(라우팅) 페이지의 상단에서 **Add Multiple Virtual Routers(**여러 가상 라우터 추가**)**를 클릭합니다.

c) 설명 패널의 오른쪽 하단에서 **Create First Custom Virtual Router(**첫 번째 맞춤형 가상 라우터 생성)를 클릭합니다.

d) 가상 라우터 VR1에 대한 속성을 입력합니다.

- **Name(**이름**)** — VR1 또는 선택한 다른 이름을 입력합니다.
- **Interfaces(**인터페이스**)** — **+**를 클릭하고 **inside**를 선택한 후 **OK(**확인**)**를 클릭합니다.

e) **OK(**확인**)**를 클릭합니다.

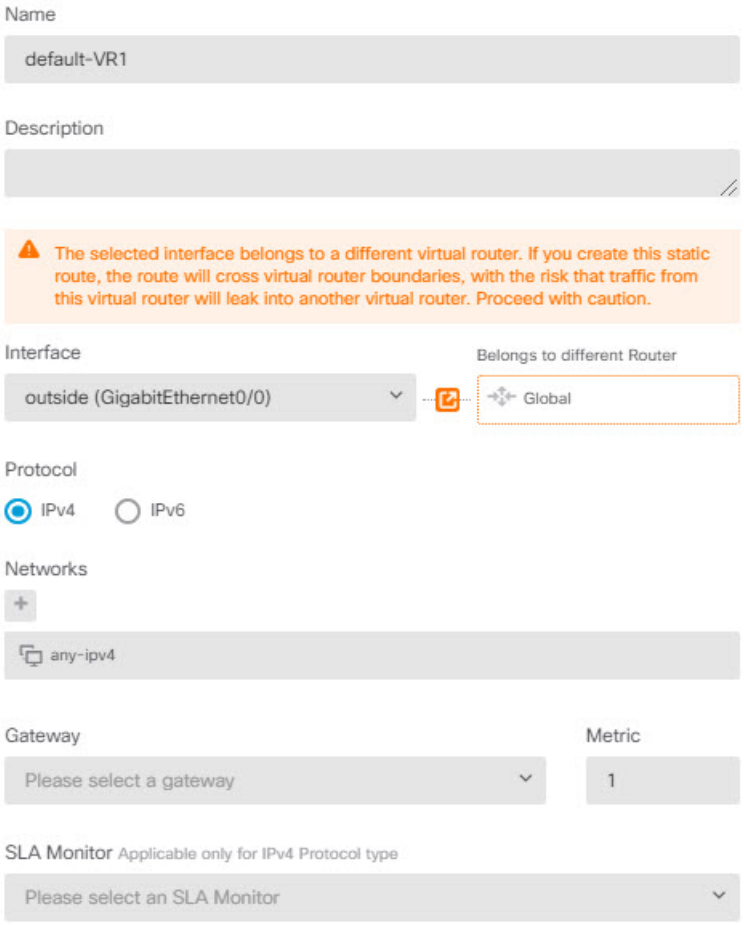
대화 상자가 닫히고 가상 라우터의 목록이 표시됩니다.

f) 가상 라우터 목록에서 VR1 가상 라우터의 작업 열에 있는 보기 아이콘()을 클릭합니다.

g) **Static Routing(**정적 라우팅**)** 탭에서 **+**를 클릭하고 다음과 같이 경로를 구성합니다.

- **Name(**이름**)** — 어떤 이름이든 가능합니다(예: **default-VR1**).
- **Interface(**인터페이스**)** — **outside**를 선택합니다. 인터페이스가 다른 라우터에 있으며 경로 유출이 생성된다는 경고 메시지가 표시됩니다. 이는 사용자가 수행하려는 작업입니다.
- **Protocol(**프로토콜**)** — 이 예에서는 **IPv4**를 사용합니다.
- **Networks(**네트워크**)** — **any-ipv4** 개체를 선택합니다. 이 경로가 VR1 내에서 라우팅될 수 없는 모든 트래픽에 대한 기본 경로가 됩니다.
- **Gateway(**게이트웨이**)** — 이 항목은 비워둡니다. 다른 가상 라우터로 경로를 유출할 경우에는 게이트웨이 주소를 선택하지 않습니다.

대화 상자가 다음과 비슷하게 표시됩니다.



h) **OK(**확인**)**를 클릭합니다.

단계 **4** 외부 인터페이스에 대한 정적 기본 경로 유출을 포함하여, 가상 라우터 VR2를 구성합니다.

a) VR1이 표시되어 있는 경우, 뒤로 버튼(⮌)을 클릭하여 가상 라우터 목록으로 돌아갑니다.

b) 목록 위쪽에 있는 +를 클릭합니다.

c) 가상 라우터 VR2에 대한 속성을 입력합니다.

- **Name(**이름**)** — VR2 또는 선택한 다른 이름을 입력합니다.
- **Interfaces(**인터페이스**)** — +를 클릭하고 **inside-2**를 선택한 후 **OK(**확인**)**를 클릭합니다.

d) **OK(**확인**)**를 클릭합니다.

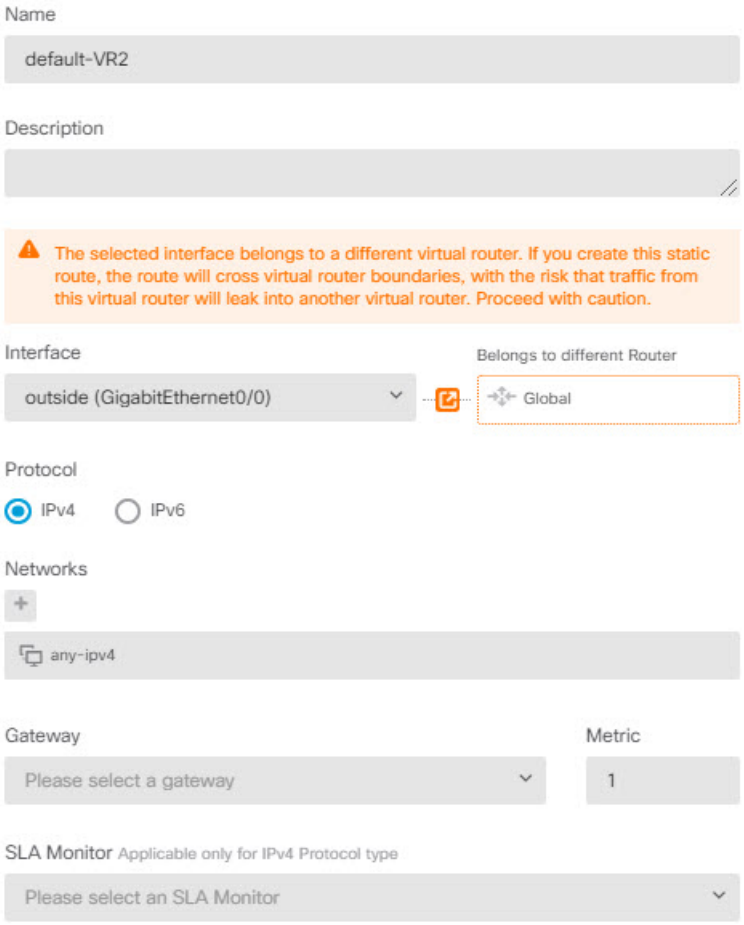
대화 상자가 닫히고 가상 라우터의 목록이 표시됩니다.

e) 가상 라우터 목록에서 VR2 가상 라우터의 작업 열에 있는 보기 아이콘( )을 클릭합니다.

f) **Static Routing(**정적 라우팅**)** 탭에서 +를 클릭하고 다음과 같이 경로를 구성합니다.

- **Name(**이름**)** — 어떤 이름이든 가능합니다(예: **default-VR2**).
- **Interface(**인터페이스**)** — **outside**를 선택합니다. 인터페이스가 다른 라우터에 있으며 경로 유출이 생성된다는 경고 메시지가 표시됩니다. 이는 사용자가 수행하려는 작업입니다.
- **Protocol(**프로토콜**)** — 이 예에서는 **IPv4**를 사용합니다.
- **Networks(**네트워크**)** — **any-ipv4** 개체를 선택합니다. 이 경로가 VR2 내에서 라우팅될 수 없는 모든 트래픽에 대한 기본 경로가 됩니다.
- **Gateway(**게이트웨이**)** — 이 항목은 비워둡니다. 다른 가상 라우터로 경로를 유출할 경우에는 게이트웨이 주소를 선택하지 않습니다.

대화 상자가 다음과 비슷하게 표시됩니다.

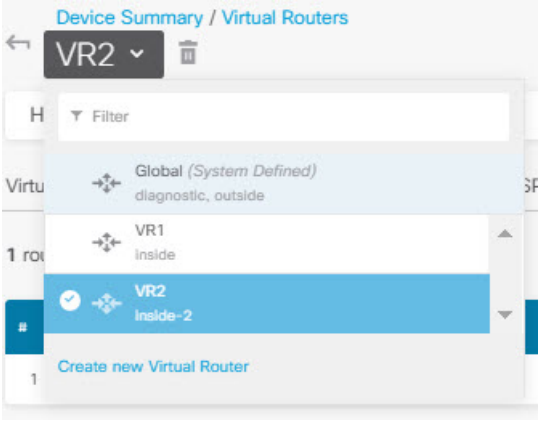


g) **OK(**확인**)**를 클릭합니다.

단계 **5** 외부 인터페이스에 대한 기본 경로를 전역 라우터에 생성합니다.

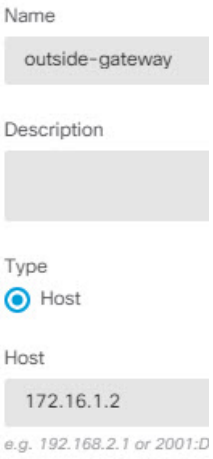
이 경로의 목적은 두 가지 가상 라우터에서 전역 라우터의 외부 인터페이스로 유출되는 트래픽에 올바른 게이트웨이를 할당하기 위한 것입니다.

a) VR2가 표시되면, 페이지 상단에 있는 VR2 이름을 클릭하여 가상 라우터 목록을 열고 전역 라우터를 선택합니다.

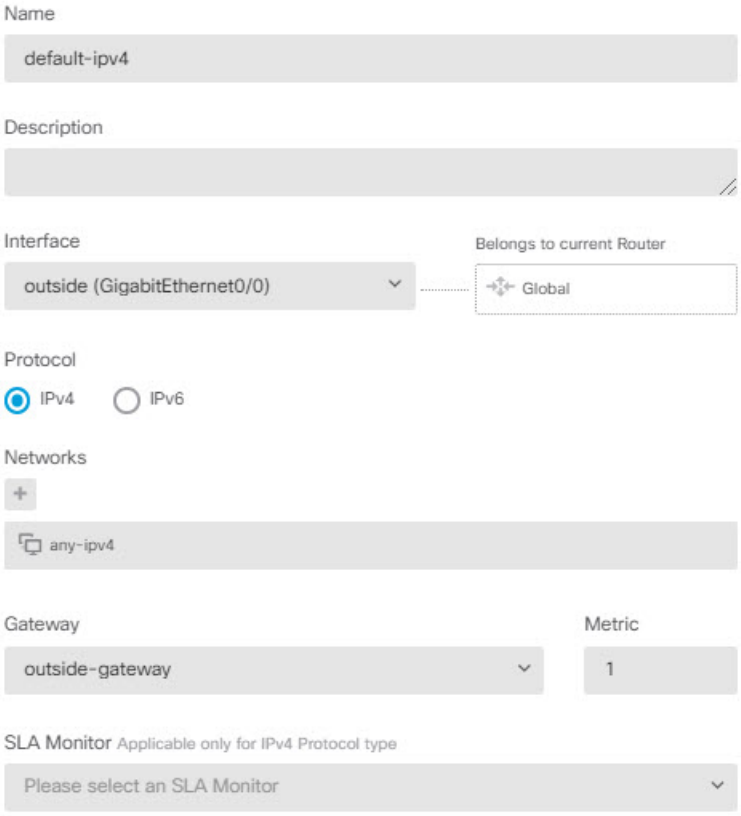


b) 전역 라우터에 대한 Static Routing(정적 라우팅) 탭에서 +를 클릭하고 다음과 같이 경로를 구성합니다.

- **Name(**이름**)** — 어떤 이름이든 가능합니다(예: default-ipv4).
- **Interface(**인터페이스**)** — **outside**를 선택합니다.
- **Protocol(**프로토콜**)** — 이 예에서는 **IPv4**를 사용합니다.
- **Networks(**네트워크**)** — **any-ipv4** 개체를 선택합니다. 이 경로가 모든 IPv4 트래픽에 대한 기본 경로가 됩니다.
- **Gateway(**게이트웨이**)** — 개체가 기존에 없다고 가정한 상태에서 **Create New Network Object(**새 네트워크 개체 생성**)**를 클릭한 다음, 외부 인터페이스에서 네트워크 링크의 다른 끝에 있는 게이트웨이의 IP 주소(이 예에서는 172.16.1.2)에 대한 호스트 개체를 정의합니다. 개체를 생성한 후, 정적 경로의 Gateway(게이트웨이) 필드에서 해당 개체를 선택합니다.



대화 상자가 다음과 비슷하게 표시됩니다.



c) **OK(**확인**)**를 클릭합니다.

단계 **6** **Interfaces(**인터페이스**)** 페이지로 돌아가 IP 주소를 inside-2에 추가합니다.

a) 디바이스를 클릭한 다음, **Interfaces(**인터페이스**)** 요약에서 **View All Interfaces(**모든 인터페이스 보기**)**를 클릭합니다.

b) VR2에 할당한 inside-2 인터페이스에 대한 Action(작업) 열에서 수정 아이콘( )을 클릭합니다.

c) **IPv4 Address(IPv4** 주소**)** 탭에 192.168.1.1/24를 IP 주소 및 서브넷 마스크로 입력합니다.

d) **OK(**확인**)**를 클릭합니다.

inside 및 inside-2 인터페이스가 현재 별도의 가상 라우터에 있으므로 이번에는 중복 IP 주소에 대한 오류가 발생하지 않습니다.

단계 **7** 외부 트래픽이 10.100.10.1로 향하도록 PAT inside에 대한 NAT 규칙을 생성합니다.

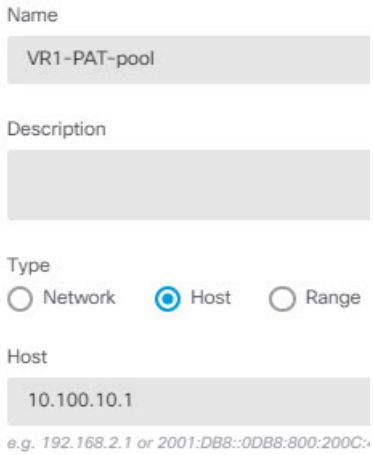
a) **Policies(**정책**)**를 선택한 다음 **NAT**를 클릭합니다.

b) 내부-외부 인터페이스에 InsideOutsideNatRule이라는 이름의 수동 NAT 규칙이 이미 있는 경우, 인터페이스 PAT를 적용하고 해당 규칙에 대해 수정 아이콘( )을 클릭합니다. 그렇지 않을 경우, **+**를 클릭하여 새 규칙을 생성합니다.

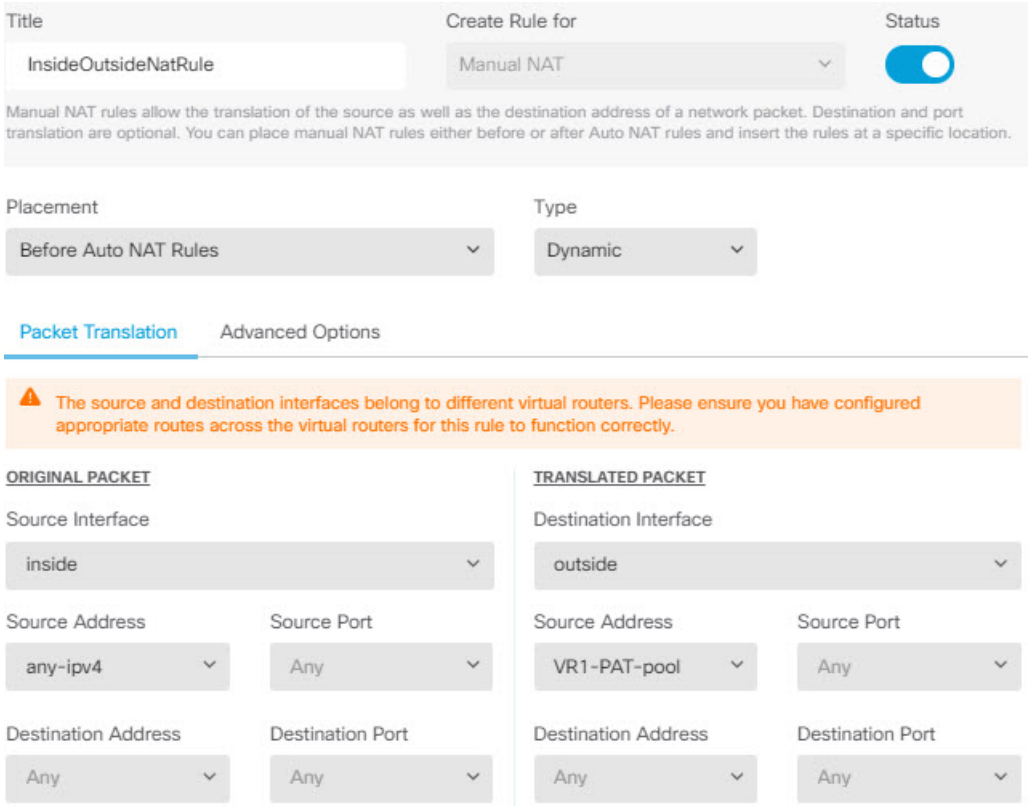
기존 규칙을 수정할 경우, 소스 및 대상 인터페이스가 서로 다른 가상 라우터에 있으며 경로를 정의해야 한다는 경고 메시지가 나타납니다. 이는 절차의 앞 단계에서 수행한 작업입니다.

c) 기존 규칙을 수정한다고 가정할 경우, **Translated Packet(**변환된 패킷**)** > **Source Address(**소스 주소**)**에서 드롭다운 화살표를 클릭하고, **Create New Network(**새 네트워크 생성**)**를 클릭합니다(10.100.10.1을 정의하는 호스트 개체가 기존에 없다고 가정).

d) PAT 주소에 대한 호스트 네트워크 개체를 구성합니다. 개체는 다음과 비슷해야 합니다.



e) 새 개체를 **Translated Packet(**변환된 패킷**)** > **Source Address(**소스 주소**)**로 선택합니다. NAT 규칙이 다음과 유사하게 표시됩니다.



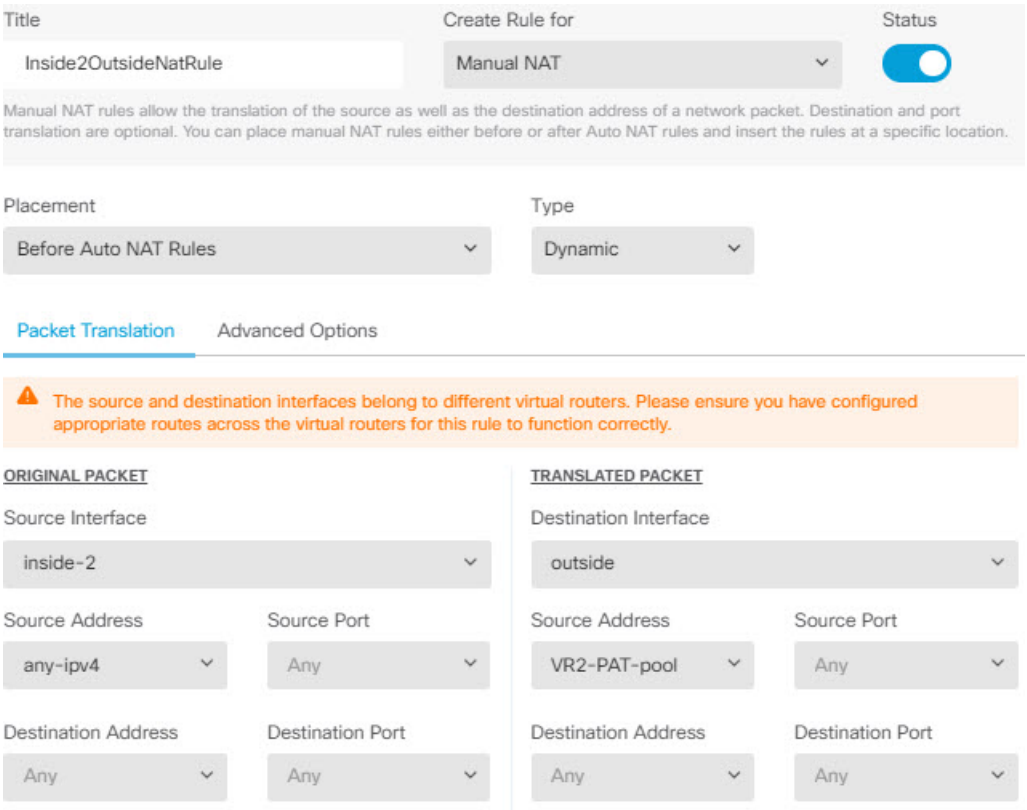
f) **OK(**확인**)**를 클릭합니다.

단계 **8** 외부 트래픽이 10.100.10.2로 향하도록 PAT inside-2에 대한 NAT 규칙을 생성합니다.

이 규칙은 다음과 같은 예외를 제외하고 VR1에 대한 규칙과 동일하게 표시됩니다.

- **Name(**이름**)** — 이는 고유해야 합니다(예: Inside2OutsideNatRule).
- **Original Packet(**원본 패킷**)** > **Source Interface(**소스 인터페이스**)** — inside-2를 선택합니다.
- **Translated Packet(**변환된 패킷**)** > **Source Address(**소스 주소**)** — 10.100.10.2에 대한 새 호스트 네트워크 개체를 생성합니다.

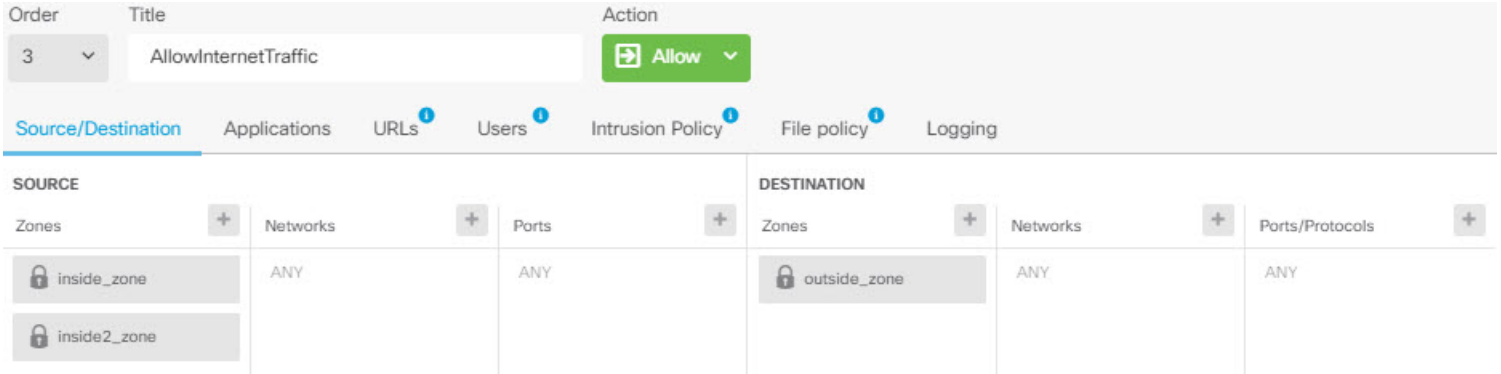
규칙이 다음과 유사하게 표시됩니다.



단계 **9** **Policies(**정책**)** > **Access Control(**액세스 제어**)**을 선택하고, 트래픽이 inside_zone 및 inside2_zone에서 outside_zone으로 향하도록 허용하는 액세스 제어 규칙을 구성합니다.

마지막으로, inside 및 inside-2 인터페이스에서 외부 인터페이스로 향하는 트래픽을 허용하는 액세스 제어 정책을 구성해야 합니다. 액세스 제어 규칙은 보안 영역을 사용해야 하므로, 이러한 각 인터페이스에 대한 영역을 생성해야 합니다. 또는 inside 및 inside-2 양쪽을 모두 보유하는 단일 영역을 생성할 수도 있지만, 이러한 라우터에서 트래픽을 처리하는 방식을 차별화하는 추가 규칙을 이 정책 또는 다른 정책에서 생성할 가능성이 높습니다.

인터페이스의 이름을 딴 영역을 생성한다고 가정할 경우, 모든 트래픽이 인터넷으로 흐르도록 허용하는 기본 규칙은 다음과 같습니다. 적합하다고 생각되는 경우 침입 정책을 이 규칙에 적용할 수 있습니다. 원치 않는 트래픽을 차단하는 추가 규칙(예: URL 필터링을 구현하는 경우)을 정의할 수 있습니다.



가상 라우터 모니터링

가상 라우터를 모니터링하고 트러블슈팅하려면 CLI 콘솔을 열거나 디바이스 CLI에 로그인하여 다음 명령을 사용합니다. Routing(라우팅) 페이지의 **Commands(**명령**)** 메뉴에서 이러한 명령 중 일부를 선택할 수도 있습니다.

- **show vrf** 시스템에 정의된 가상 라우터에 대한 정보를 표시합니다.
- **show ospf** [**vrf** *name* | **all**]

  가상 라우터의 OSPF 프로세스에 대한 정보를 표시합니다. 가상 라우터를 지정하여 해당 가상 라우터의 프로세스에 대한 정보만 볼 수도 있고, 옵션을 생략하여 모든 가상 라우터의 VRF에 대한 정보를 볼 수도 있습니다. **show ospf ?**를 사용하여 추가 옵션 목록을 확인합니다.
- **show bgp** [**vrf** *name* | **all**]

  가상 라우터의 OSPF 프로세스에 대한 정보를 표시합니다. 가상 라우터를 지정하여 해당 가상 라우터의 프로세스에 대한 정보만 볼 수도 있고, 옵션을 생략하여 모든 가상 라우터의 VRF에 대한 정보를 볼 수도 있습니다. **show bgp ?**를 사용하여 추가 옵션 목록을 확인합니다.
- **show eigrp** *option*

  EIGRP 프로세스에 대한 정보를 표시합니다. **show eigrp ?**를 사용하여 사용 가능한 옵션을 확인합니다.

14 장

경로 조정을 위한 경로 맵 및 기타 개체

다양한 라우팅 프로토콜을 통해 경로 배포 및 어그리게이션과 같은 미세 조정 활동을 할 수 있습니다. 일부 조정 기능의 경우 경로 맵 또는 기타 개체를 사용하여 조정 정책의 대상이 되어야 하는 경로를 식별합니다. 경로 맵에는 일치하는 경로에 대한 옵션을 설정하는 추가 기능이 있으므로, 다음 홉 라우터가 맞춤형 동작을 적용하는 데 사용할 수 있는 경로를 변경할 수 있습니다.

이러한 개체를 생성해야 하는지 여부는 사용자가 구현하는 라우팅 프로토콜의 동작을 미세 조정하는 데 필요한 사항에 따라 달라집니다. 먼저 요구 사항을 평가하여 구성하려는 조정 명령에 필요한 개체 유형을 결정합니다.

경로 맵 구성

다양한 용도로 경로 맵을 사용할 수 있으며, 일부 라우팅 프로토콜은 다른 프로토콜보다 더 많은 용도를 지원합니다. 가장 일반적인 용도는 경로 재분배를 다른 라우팅 프로토콜로 미세 조정하는 것입니다.

경로 맵 허용 및 거부 절

경로 맵은 하나 이상의 **permit** 또는 **deny** 절로 구성됩니다. 이러한 절의 순서는 중요하며 경로는 맵 하향식, 첫 번째 일치 항목에 대해 평가됩니다. 경로가 절과 일치하지 않으면 경로 맵과 일치하지 않는 것으로 간주됩니다.

각 허용 절은 0개 이상의 **match** 및 **set** 명령문을 포함할 수 있습니다. **match** 명령문은 절과 일치하는 경로를 결정하는 반면, **set** 명령문은 경로 메트릭과 같은 경로의 일부 특성을 수정합니다. set 명령문은 필요하지 않습니다. 경로를 변경하지 않고 재배포(또는 다른 서비스)를 위해 경로를 일치시킬 수 있습니다.

각 거부 절은 0개 이상의 match 명령문을 포함할 수 있습니다. 그러나 "거부" 경로는 단순히 경로 맵과 일치하지 않아 set 작업을 적용할 수 없으므로 set 절을 포함하는 것은 의미가 없습니다.

경로 맵 **Match** 및 **Set** 명령문

각 경로 맵 절은 두 가지 값을 갖습니다.

- 일치 값은 이 절을 적용할 경로를 선택합니다.
- set 값은 경로의 일부 특성을 수정합니다.

예를 들면, 재배포되는 각 경로에 대해 라우터는 먼저 경로 맵에 있는 절의 일치 기준을 평가합니다. 경로가 기준과 일치하면 허용 또는 거부 절에 따라 경로가 재배포되거나 거부됩니다. 허용 절에 대한 일치 항목의 경우 set 명령의 값으로 경로 특성 중 일부를 수정할 수 있습니다. 경로가 기준에 일치하지 않으면 이 절은 경로에 적용되지 않고 시스템에서 경로 맵의 다음 절에 대해 경로를 평가합니다. 절이 경로와 일치하거나 경로 맵의 끝에 도달할 때까지 경로 맵 스캔이 계속됩니다. 일치 항목이 없으면 경로는 경로 맵과 일치하지 않는 것으로 간주됩니다(거부 작업과 동일함).

단일 절의 match 및 set 명령문:

- 여러 개의 match 명령문은 AND 처리됩니다. 즉, 경로가 절과 일치하려면 각 명령문을 충족해야 합니다.
- 단일 match 명령문 내의 여러 값은 OR 처리됩니다. 즉, 경로가 해당 match 명령문 내의 어떤 값이든 일치하는 경우 이는 전체적으로 명령문과 일치하는 것으로 간주됩니다.
- match 명령문이 없으면 모든 경로가 절과 일치합니다.
- 경로 맵 허용 절에 set 명령문이 없으면 경로의 현재 특성을 수정하지 않고 경로에 기능(예: 재배포)이 적용됩니다.
- 거부 절의 모든 set 명령문은 무시됩니다. "거부" 경로는 단순히 경로 맵과 일치하지 않아 set 작업을 적용할 수 없으므로 set 절을 포함하는 것은 의미가 없습니다.
- match 또는 set 명령문이 없는 빈 절은 이전 절에서 일치하지 않은 경로와 일치합니다. 예를 들면 다음과 같습니다.
  - 빈 허용 절은 수정 없이 남은 경로의 재배포를 허용합니다.
  - 빈 거부 절은 나머지 경로의 재배포를 허용하지 않습니다. 경로 맵을 완전히 스캔했지만 정확한 일치 항목을 찾지 못한 경우의 기본 작업입니다.

경로 맵 구성

다양한 용도로 경로 맵을 사용할 수 있으며, 일부 라우팅 프로토콜은 다른 프로토콜보다 더 많은 용도를 지원합니다. 가장 일반적인 용도는 경로 재분배를 다른 라우팅 프로토콜로 미세 조정하는 것입니다.

경로 맵은 하나 이상의 **permit** 또는 **deny** 절로 구성됩니다. 이러한 절의 순서는 중요하며 경로는 맵 하향식, 첫 번째 일치 항목에 대해 평가됩니다. 경로가 절과 일치하지 않으면 경로 맵과 일치하지 않는 것으로 간주됩니다.

각 허용 절은 0개 이상의 **match** 및 **set** 명령문을 포함할 수 있습니다. **match** 명령문은 절과 일치하는 경로를 결정하는 반면, **set** 명령문은 경로 메트릭과 같은 경로의 일부 특성을 수정합니다. set 명령문은 필요하지 않습니다. 경로를 변경하지 않고 재배포(또는 다른 서비스)를 위해 경로를 일치시킬 수 있습니다.

각 거부 절은 0개 이상의 match 명령문을 포함할 수 있습니다. 그러나 "거부" 경로는 단순히 경로 맵과 일치하지 않아 set 작업을 적용할 수 없으므로 set 절을 포함하는 것은 의미가 없습니다.

match 및 set 명령문을 평가하는 방법에 대한 자세한 설명은 경로 맵 Match 및 Set 명령문, 376 페이지를 주의깊게 읽어 보십시오.

시작하기 전에

액세스 목록, AS 경로 액세스 목록, 커뮤니티 목록, 정책 목록 및 접두사 목록 등 일치 기준을 정의하기 위해 경로 맵에서 다양한 기타 개체를 사용할 수 있습니다. 경로 맵을 생성하려면 먼저 이러한 개체를 생성해야 합니다.

ACL 일치의 경우 IPv4 주소에는 표준 또는 확장 ACL을 사용할 수 있지만 IPv6에는 확장 ACL만 사용할 수 있습니다. match 절은 IPv4 또는 IPv6만 기반으로 하므로 ACL에 match 명령문에 대한 올바른 주소 체계가 있는지 확인합니다.

또한 BGP의 match 및 set 기준은 기타 라우팅 프로토콜과 비교할 때 다릅니다. 경로 맵을 사용할 라우팅 프로세스에 대해 올바른 match/set 기준을 선택해야 합니다.

프로시저

단계 **1** **Device(**디바이스**)** > **Advanced Configuration(**고급 컨피그레이션**)**에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

단계 **2** 목차에서 **Smart CLI(**스마트 **CLI)** > **Objects(**개체**)**를 선택합니다.

단계 **3** 다음 중 하나를 수행합니다.

- 개체를 생성하려면 + 버튼을 클릭합니다.
- 개체를 수정하려면 개체의 수정 아이콘()을 클릭하십시오.

참조되지 않는 개체를 삭제하려면 해당 개체의 휴지통 아이콘()을 클릭합니다.

단계 **4** **Route Map(**경로 맵**)**을 **CLI Template(CLI** 템플릿**)**으로 선택합니다.

단계 **5** 스마트 CLI 개체의 **Name(**이름**)**을 입력합니다. 이 이름은 **route-map** 명령에서 CLI 템플릿의 첫 번째 라인에 경로 맵 이름으로도 입력됩니다.

단계 **6** 첫 번째 절을 생성합니다.

a) *redistribution* 변수를 클릭하고 다음 중 하나를 선택합니다.

- **permit**—일치. 이 규칙과 일치하는 연결이 구성 중인 기능에 대해 선택됩니다.

- **deny**—일치하지 않음. 이 규칙과 일치하는 연결이 기능에서 제외됩니다. "denied" 트래픽이 삭제되는 것은 아니며 서비스만 해당 트래픽에 적용되지 않습니다. 예를 들어 이 경로 맵을 사용하여 재배포할 경로를 정의하는 경우 "거부됨" 주소 공간만 재배포되지 않습니다.

b) **sequence-number** 변수를 클릭하고 절 번호를 1~ 65535 범위에서 입력합니다.

이 번호는 경로 맵 내의 다른 번호가 지정된 절과 관련이 있습니다. 일반적인 방법은 개수를 열 개씩, 즉 10, 20, 30으로 건너뛰어 나중에 새 절을 삽입할 공간을 확보하는 것입니다.

단계 **7** **Show Disabled(**비활성화됨 표시**)**를 클릭하고 절에 대한 **match** 명령문을 구성합니다.

a) 이를 활성화하려면 **configure** *clause* 명령 옆의 + 를 클릭합니다.

b) *clause*를 클릭하고 BGP 경로 맵에 대해 **bgp-match-clause**를 선택하거나 기타 모든 라우팅 프로토콜에 대해 **match-clause**를 선택합니다.

c) (BGP 경로 맵) 이 절에서 대상으로 하는 특정 경로를 식별하도록 다음 **match** 명령문 조합을 구성합니다. 구성하지 않은 명령을 비활성화하려면 - 아이콘을 클릭해야 합니다.

- **match as-path**에 전달하는 고성능 고속 어플라이언스입니다. 변수를 클릭하고 일치시킬 자율 시스템 번호를 정의하는 AS 경로 개체를 선택합니다.
- **match community**. 변수를 클릭하고 일치시킬 커뮤니티를 정의하는 커뮤니티 목록 개체를 선택합니다.
- **match policy-list**. 변수를 클릭하고 절의 일치 기준을 정의하는 정책 목록 개체를 선택합니다.
- **match tag**. 변수를 클릭하고 일치시킬 경로 태그 값을 0~4294967295 범위에서 입력합니다.

d) (모든 기타 라우팅 프로토콜) 이 절에서 대상으로 하는 특정 경로를 식별하도록 다음 **match** 명령문 조합을 구성합니다. 구성하지 않은 명령을 비활성화하려면 **-** 아이콘을 클릭해야 합니다. 이러한 명령 중 일부를 활성화하려면 **+**를 클릭해야 할 수 있습니다.

- **match interface**. 변수를 클릭하고 일치시킬 경로의 모든 인터페이스를 선택합니다.
- **configure match ipv4/ipv6 ip address** *list-type* IP 버전에 맞는 명령을 활성화합니다. 그 다음 *list-type* 변수를 클릭하고 **access-list** 또는 **prefix-list**를 기반으로 하는 경로의 IP 주소와 일치시킬지를 선택합니다. 그러면 변수를 클릭하고 일치시킬 IP 주소를 정의하는 접두사 목록 또는 액세스 목록을 선택할 수 있는 **match ipv4/ipv6 address** 명령이 추가됩니다.
- **configure match ipv4/ipv6 ip next-hop** *list-type list-type* 변수를 클릭하고 **access-list** 또는 **prefix-list**를 기반으로 하는 경로의 다음 홉 라우터 IP 주소와 일치시킬지를 선택합니다. 그러면 변수를 클릭하고 일치시킬 IP 주소를 정의하는 접두사 목록 또는 액세스 목록을 선택할 수 있는 **match ipv4/ipv6 next-hop** 명령이 추가됩니다.
- **configure match ipv4/ipv6 ip route-source** *list-type list-type* 변수를 클릭하고 **access-list** 또는 **prefix-list**를 기반으로 하는 경로의 경로 소스 IP 주소와 일치시킬지를 선택합니다. 그러면 변수를 클릭하고 일치시킬 IP 주소를 정의하는 접두사 목록 또는 액세스 목록을 선택할 수 있는 **match ipv4/ipv6 route-source** 명령이 추가됩니다.
- **match metric**. 변수를 클릭하고 일치시킬 라우팅 메트릭을 1 ~ 4294967295 범위에서 입력합니다.

- **match route-type**. (OSPF, EIGRP) 변수를 클릭하고 경로 유형을 선택합니다.
  - **external-1**, **external-2**를 입력합니다. OSPF 또는 EIGRP 외부 유형-1 또는 유형-2 경로.
  - **internal**. OSPF 영역 간 및 영역 내 경로 또는 EIGRP 내부 경로.
  - **local**. 로컬에서 생성된 BGP 경로.
  - **nssa-external-1**, **nssa-external-2**를 입력합니다. 외부 NSSA(Not So stubby Area) 유형-1 또는 유형-2 경로.

단계 **8** (선택 사항, 허용 절 전용) 허용되는 경로, 즉 일치하는 경로의 경우 경로 특성을 수정하도록 **set** 명령문을 구성할 수 있습니다. 경로는 수정할 필요가 없습니다. 예를 들어, 변경하지 않고 재배포할 수 있습니다.

a) **...** > **Duplicate(**중복**)**(configure match-clause 또는 허용 절 내의 **configure bgp-match-clause** 명령 왼쪽)를 클릭합니다. 새 **configure** *clause* 명령은 허용 절의 끝에 추가됩니다.

b) *clause*를 클릭하고 일치 절에 대해 선택한 항목에 따라 **bgp-set-clause** 또는 **set-clause**를 선택합니다.

c) (BGP 경로 맵) 일치하는 경로의 특성을 수정하려면 다음 **set** 명령문 조합을 구성합니다. 구성하지 않은 명령을 비활성화하려면 **-** 아이콘을 클릭해야 합니다.

- **configure set as-path** *options*. *options*를 클릭하고 **properties**를 선택하면 구성해야 하는 다음 명령이 추가됩니다. 중복된 AS 번호를 포함하여 경로에 항목을 추가하면 경로가 길어지고 경로가 최적의 경로로 선택될 가능성이 적어집니다.
  - **set as-path prepend** *as-path*. *as-path*를 클릭하고 경로의 AS_PATH 특성 시작 부분이 되도록 추가할 최대 10개의 자동 시스템 번호를 입력합니다. 변경 사항은 아웃바운드 BGP 경로 맵에 적용됩니다.
  - **set as-path prepend last-as** *value*. *value*를 클릭하고 시스템이 알림 네이버의 자율 시스템 번호를 AS_PATH 변수의 시작 앞에 추가해야 하는 횟수를 입력합니다. 변경 사항은 인바운드 BGP 경로 맵에 적용됩니다.
  - **set as-path tag**. 경로의 태그를 자율 시스템 경로로 변환합니다. 경로를 BGP로 재배포할 때만 적용됩니다.
- **set community** *community-number properties*. *community-number*를 클릭하고 경로의 커뮤니티를 1~4694967295 범위에서 입력합니다. 필요에 따라 *properties*를 클릭하고 다음 중 하나를 추가할 수 있습니다.
  - **internet**—이 커뮤니티 경로가 모든 피어(내부 및 외부)에게 알려집니다.
  - **no-advertise**—이 커뮤니티 경로가 모든 피어(내부 또는 외부)에게 알려지지 않습니다.
  - **no-export**—이 커뮤니티 경로가 같은 자율 시스템 안에 있는 피어 또는 연합 내의 다른 하위 자율 시스템에만 알려집니다. 이 경로는 외부 피어에 알려지지 않습니다.

- **set local-preference**. 변수를 클릭하고 자율 시스템 경로의 기본 설정 값을 0~4294967295 범위에서 입력합니다. 전역 BGP 옵션에서 이를 변경하지 않는 한 BGP 경로의 기본 설정은 100입니다. 기본 설정 번호가 가장 높은 경로가 우선시됩니다.
- **set weight**. 변수를 클릭하고 경로의 가중치를 0~65535 범위에서 입력합니다. 라우터가 동일한 목적지에 대하여 하나 이상의 경로를 학습한 경우 가중치가 가장 높은 경로가 우선합니다.
- **set origin** *options*. BGP 경로의 원본은 주 IP 라우팅 테이블에 있는 경로의 경로 정보를 기반으로 합니다. *options*를 클릭하여 이를 변경하고 BGP 원본 코드를 설정하는 방법을 선택할 수 있습니다.
  - **igp**. 원본을 원격 IGP(Internal Gateway Gateway) 시스템으로 설정합니다.
  - **incomplete**. 원본을 알 수 없는 헤리티지로 설정합니다.
- **configure next-hop ipv4/ipv6** *options*. 이는 별도의 명령입니다. 해당 IP 버전에 대한 *options*를 클릭하고 다음 중 하나를 선택합니다. 다음 홉 게이트웨이 설정은 일반적으로 정책 기반 라우팅을 구현할 때 수행하는 작업입니다.
  - **specific-ip**. 이 경로에 대한 다음 홉 게이트웨이의 IP 주소를 명시적으로 설정하려면 이 옵션을 선택합니다. **set ip/ipv6 next-hop ip-address** 명령이 추가됩니다. 변수를 클릭하고 다음 홉 게이트웨이의 IP 주소를 입력합니다. 공백으로 구분하여 여러 IP 주소를 추가할 수 있습니다. 첫 번째 게이트웨이의 주소에 연결할 수 없는 경우 그 다음 주소가 시도됩니다.
  - **user-peer-address**. 다음 홉 게이트웨이를 BGP 피어의 IP 주소로 설정하려면 이 옵션을 선택합니다. BGP 피어의 아웃바운드 경로 맵에 있는 이 옵션을 사용하면 알려진 일치 경로의 다음 홉이 로컬 라우터의 피어링 주소로 설정되어 다음 홉 계산이 비활성화됩니다. 이 명령에 대한 추가 컨피그레이션이 필요합니다.
- **set ipv4/ipv6 address** *prefix-list* 이는 별도의 명령입니다. 선택한 접두사 목록의 내용에 따라 경로의 IP 주소를 변경합니다.
- **set automatic-tag**. 시스템이 경로에 대한 태그 값을 자동으로 계산하도록 합니다.

d) (모든 기타 라우팅 프로토콜) 일치하는 경로의 특성을 수정하려면 다음 **set** 명령문 조합을 구성합니다. 구성하지 않은 명령을 비활성화하려면 **-** 아이콘을 클릭해야 합니다.

- **set metric**. 변수를 클릭하고 메트릭 값을 0~4294967295 범위에서 입력합니다. 이 값은 EIGRP에서 사용되지 않습니다.
- **set metric-type**. 변수를 클릭하고 메트릭의 유형을 선택합니다.
  - **type-1**, **type-2**를 입력합니다. OSPF의 외부 경로 유형입니다. 유형-2가 기본값입니다.
  - **internal**. 경로의 다음 홉의 IGP(Internal Gateway Protocol) 메트릭과 일치하도록 eBGP(외부 BGP) 네이버에 알려진 접두사에 MED(Multi Exit Discriminator) 값을 설정합니다. 이는 생성된 내부 BGP(iBGP) 및 eBGP 파생 경로에 적용됩니다.

단계 **9** 허용/거부 절을 추가하여 경로 맵을 완료합니다.

절을 추가하려면 **...** > **Duplicate(**중복**)(permit** 또는 **deny** 라인 왼쪽)를 클릭합니다. Duplicate(중복) 명령을 클릭하는 절 바로 뒤에 새 *redistribution sequence-number* 절이 추가됩니다.

경로 맵 절은 개체에 표시되는 순서가 아니라 시퀀스 번호의 순서대로 평가되지만 순차적인 순서로 새 절을 삽입하는 경우에는 개체를 수정하는 것이 더 쉽습니다. 개체 내에서 절을 이동할 수 없습니다.

절을 복제하면 미리 구성된 특성이 없는 새로운 빈 절이 삽입됩니다. "중복"을 생성한 후에는 위의 설명대로 진행하여 필요에 따라 구성합니다.

단계 **10** **OK(**확인**)**를 클릭하여 개체를 저장합니다.

이제 경로 맵이 필요한 기능에 대해 라우팅 프로세스 컨피그레이션 또는 FlexConfig 개체에서 개체를 사용할 수 있습니다.

액세스 목록 구성

ACL(Access Control List)이라고도 알려진 액세스 목록 개체는 서비스를 적용할 트래픽을 선택합니다. 경로 맵과 같은 특별한 기능을 구성할 때 이러한 개체를 사용합니다. ACL에 의해 허용으로 식별된 트래픽은 서비스가 제공되는 반면 "차단된" 트래픽은 서비스에서 제외됩니다. 서비스에서 제외된 트래픽은 반드시 삭제된다는 의미는 아닙니다.

다음 유형의 ACL을 구성할 수 있습니다.

- 확장 - 소스 및 대상 주소와 포트를 기반으로한 트래픽을 식별합니다. IPv4 및 IPv6 주소를 지원합니다.
- 표준 - 대상 주소만을 기반으로 트래픽을 식별합니다. IPv4만 지원합니다.

ACL은 하나 이상의 ACE(액세스 제어 항목) 또는 규칙으로 구성됩니다. ACE의 순서는 중요합니다. ACL을 평가하여 패킷이 "permit" ACE와 일치하는지 확인할 때 패킷은 각 ACE 항목에 대해 해당 항목이 나열된 순서에 따라 테스트됩니다. 일치가 발견되면 ACE가 더 이상 점검되지 않습니다. 예를 들어 10.100.10.1과 일치시키면서 나머지 10.100.10.0/24를 제외하려는 경우 10.100.10.1에 대한 허용 항목이 10.100.10.0/24에 대한 거부 항목 앞에 와야 합니다. 일반적으로 더 구체적인 규칙이 ACL의 상단에 배치됩니다.

허용 항목과 일치하지 않는 패킷은 일치에서 거부되거나 제외된 것으로 간주됩니다.

다음 주제는 ACL 개체를 구성하는 방법을 설명합니다.

확장 액세스 목록 구성

소스, 대상 주소, 프로토콜, 포트를 기반으로 트래픽을 일치시키려고 하거나 트래픽이 IPv6인 경우 확장 ACL 개체를 사용합니다.

시작하기 전에

개체에서 생성하는 ACE에 필요한 네트워크 또는 포트 개체를 생성합니다.

프로시저

단계 **1** **Device(**디바이스**)** > **Advanced Configuration(**고급 컨피그레이션**)**에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

단계 **2** 목차에서 **Smart CLI(**스마트 **CLI)** > **Objects(**개체**)**를 선택합니다.

단계 **3** 다음 중 하나를 수행합니다.

- 개체를 생성하려면 **+** 버튼을 클릭합니다.
- 개체를 수정하려면 개체의 수정 아이콘()을 클릭하십시오.

참조되지 않는 개체를 삭제하려면 해당 개체의 휴지통 아이콘()을 클릭합니다.

단계 **4** **Standard Access List(**표준 액세스 목록**)**을 **CLI Template(CLI** 템플릿**)**으로 선택합니다.

단계 **5** 스마트 CLI 개체의 **Name(**이름**)**을 입력합니다. 이 이름은 **access list** 명령에서 CLI 템플릿의 첫 번째 라인에 ACL 이름으로도 입력됩니다.

단계 **6** ACL의 최상위 규칙이어야 하는 ACE를 생성합니다.

구축 시에 시스템이 명령을 일련의 ACE로 분할할 수 있더라도(특히 둘 이상의 네트워크 개체를 포함하는 경우) 단일 **configure access list entry** 명령 내에 포함된 각 명령 목록은 기본적으로 하나의 ACE입니다.

a) 액세스 목록 항목 구성 명령에서 *action*을 클릭하고 다음 중 하나를 선택합니다.

- **permit**—일치. 이 ACE와 일치하는 연결이 구성 중인 기능에 대해 선택됩니다.
- **deny**—일치하지 않음. 이 ACE와 일치하는 연결이 기능에서 제외됩니다. "denied" 트래픽이 삭제되는 것은 아니며 서비스만 해당 트래픽에 적용되지 않습니다. 예를 들어 경로 맵에서 이 ACL을 사용하여 재배포할 경로를 정의하는 경우 "거부됨" 주소 공간은 단순히 재배포되지 않습니다.

b) **permit/deny network** 명령에서 변수를 클릭하여 연결의 소스 IP 주소 및 대상 IP 주소를 정의하는 네트워크 개체를 선택합니다. 여러 개체를 선택할 수 있습니다. "임의" 주소를 지정하려면 any-ipv4 및 any-ipv6 개체를 선택합니다.

c) **configure permit/deny port** 명령에서 *options*을 클릭하고 다음 중 하나를 선택합니다. 그러면 템플릿에 연결된 permit/deny 명령이 추가됩니다.

- **any**—포트가 중요하지 않은 경우. 즉, 모든 유형의 IP 트래픽과 일치합니다.
- **any-source**—소스 TCP/UDP 포트가 중요하지 않지만 대상 포트를 지정하려는 경우. **permit/deny port** 명령에서 *destination-port* 변수를 클릭하고 포트 개체를 선택합니다.
- **any-destination**—대상 TCP/UDP 포트가 중요하지 않지만 소스 포트를 지정하려는 경우. **permit/deny port** 명령에서 *source-port* 변수를 클릭하고 포트 개체를 선택합니다.

- **source-destination**—소스 및 대상 TCP/UDP 포트가 모두 중요한 경우. **permit/deny port** 명령에서 *source-port* 및 *destination-port* 변수를 클릭하고 포트 개체를 선택합니다.

d) **configure logging** 명령에서 **disabled**를 선택합니다. 로깅은 액세스 제어에 사용되는 ACL에 적용되며 이러한 개체는 액세스 제어에 사용할 수 없습니다. 따라서 어떤 옵션을 선택하든 로깅 옵션이 무시됩니다.

단계 **7** ACE를 추가하여 ACL을 완료합니다.

ACE를 추가하려면 **...** > **Duplicate(**중복**)(configure access list entry** 라인 왼쪽)를 클릭합니다. Duplicate(중복) 명령을 클릭하는 ACE 바로 뒤에 새 ACE 그룹이 추가됩니다.

따라서 개체에 여러 ACE가 있는 경우 "중복"할 ACE를 현명하게 선택합니다. 개체 내에서 ACE를 이동할 수 없으므로 실수를 한 경우 올바른 위치에서 수동으로 ACE를 다시 생성해야 합니다.

ACE를 복제하면 미리 구성된 특성이 없는 새로운 빈 ACE가 삽입됩니다. "중복"을 생성한 후에는 위의 설명대로 진행하여 필요에 따라 구성합니다.

단계 **8** **OK(**확인**)**를 클릭하여 개체를 저장합니다.

이제 확장 ACL이 필요한 기능에 대해 경로 맵 개체 또는 FlexConfig 개체에서 개체를 사용할 수 있습니다.

표준 액세스 목록 구성

대상 IPv4 주소를 기준으로만 트래픽을 일치시키고 구성 중인 기능이 표준 ACL을 지원하면 표준 ACL 개체를 사용합니다. 그 외에는 확장 ACL을 사용합니다.

시작하기 전에

개체에서 생성하는 ACE에 필요한 네트워크 개체를 생성합니다.

프로시저

단계 **1** **Device(**디바이스**)** > **Advanced Configuration(**고급 컨피그레이션**)**에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

단계 **2** 목차에서 **Smart CLI(**스마트 **CLI)** > **Objects(**개체**)**를 선택합니다.

단계 **3** 다음 중 하나를 수행합니다.

- 개체를 생성하려면 + 버튼을 클릭합니다.
- 개체를 수정하려면 개체의 수정 아이콘()을 클릭하십시오.

참조되지 않는 개체를 삭제하려면 해당 개체의 휴지통 아이콘()을 클릭합니다.

단계 **4** **Standard Access List(**표준 액세스 목록**)**을 **CLI Template(CLI** 템플릿**)**으로 선택합니다.

단계 **5** 스마트 CLI 개체의 **Name(**이름**)**을 입력합니다. 이 이름은 **access list** 명령에서 CLI 템플릿의 첫 번째 라인에 ACL 이름으로도 입력됩니다.

단계 **6** ACL의 최상위 규칙이어야 하는 ACE를 생성합니다.

단일 **configure action** 명령 내에 포함된 각 명령 목록은 하나의 ACE입니다.

a) **configure action** 명령에서 *action*을 클릭하고 다음 중 하나를 선택합니다.

- **permit**—일치. 이 ACE와 일치하는 연결이 구성 중인 기능에 대해 선택됩니다.
- **deny**—일치하지 않음. 이 ACE와 일치하는 연결이 기능에서 제외됩니다. "denied" 트래픽이 삭제되는 것은 아니며 서비스만 해당 트래픽에 적용되지 않습니다. 예를 들어 경로 맵에서 이 ACL을 사용하여 재배포할 경로를 정의하는 경우 "거부됨" 주소 공간은 단순히 재배포되지 않습니다.

b) **permit/deny host** 명령에서 변수를 클릭하여 연결의 대상 IP 주소를 정의하는 네트워크 개체를 선택합니다. 개체는 네트워크 또는 호스트 주소를 지정할 수 있습니다. **permit/deny host** 명령 당 하나의 개체를 선택할 수 있습니다. 명령에서 **...** > **Duplicate(**중복**)**를 클릭하여 추가 주소를 지정합니다. 그러면 이 주소가 동일한 작업의 고유한 ACE가 됩니다. "임의" 주소를 지정하려면 any-ipv4 개체를 선택합니다.

단계 **7** ACE를 추가하여 ACL을 완료합니다.

ACE를 추가하려면 **...** > **Duplicate(**중복**)**(**configure action** 라인 왼쪽)를 클릭합니다. Duplicate(중복) 명령을 클릭하는 ACE 바로 뒤에 새 ACE 그룹이 추가됩니다.

따라서 개체에 여러 ACE가 있는 경우 "중복"할 ACE를 현명하게 선택합니다. 개체 내에서 ACE를 이동할 수 없으므로 실수를 한 경우 올바른 위치에서 수동으로 ACE를 다시 생성해야 합니다.

ACE를 복제하면 미리 구성된 특성이 없는 새로운 빈 ACE가 삽입됩니다. "중복"을 생성한 후에는 위의 설명대로 진행하여 필요에 따라 구성합니다.

단계 **8** **OK(**확인**)**를 클릭하여 개체를 저장합니다.

이제 표준 ACL이 필요한 기능에 대해 경로 맵 개체 또는 FlexConfig 개체에서 개체를 사용할 수 있습니다.

AS 경로 액세스 목록 구성

AS 경로 액세스 목록을 사용하여 업데이트의 자율 시스템 번호를 기준으로 BGP 네이버 업데이트를 필터링할 수 있습니다. 허용된 AS 번호는 업데이트를 수락하는 반면 거부된 AS 번호는 업데이트를 거부합니다. 즉, 라우팅 테이블에 추가되지 않습니다.

또한 아웃바운드 방향으로 AS 경로 필터링을 적용하고 네이버에 보내는 업데이트를 필터링할 수도 있습니다.

또한 BGP 주소 집계를 위해 경로 맵에서 AS 경로 개체를 사용할 수 있습니다.

프로시저

단계 **1** **Device(**디바이스**)** > **Advanced Configuration(**고급 컨피그레이션**)**에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

단계 **2** 목차에서 **Smart CLI(**스마트 **CLI)** > **Objects(**개체**)**를 선택합니다.

단계 **3** 다음 중 하나를 수행합니다.

- 개체를 생성하려면 **+** 버튼을 클릭합니다.
- 개체를 수정하려면 개체의 수정 아이콘( )을 클릭하십시오.

참조되지 않는 개체를 삭제하려면 해당 개체의 휴지통 아이콘( )을 클릭합니다.

단계 **4** **CLI Template(CLI** 템플릿**)**으로 **ASPath**를 선택합니다.

단계 **5** 스마트 CLI 개체의 **Name(**이름**)**을 입력합니다. 이름은 1~500 범위의 숫자여야 합니다. 이 이름은 **as-path** 명령에서 CLI 템플릿의 첫 번째 라인에 AS 경로 액세스 목록 이름으로도 입력됩니다.

단계 **6** AS 경로 항목을 구성합니다.

각 항목은 *action* 옵션으로 시작하는 단일 라인에 포함됩니다.

a) *action*을 클릭하고 다음 중 하나를 선택합니다.

- **permit**—일치. 이 규칙과 일치하는 연결이 구성 중인 기능에 대해 선택됩니다.
- **deny**—일치하지 않음. 이 규칙과 일치하는 연결이 기능에서 제외됩니다. "denied" 트래픽이 삭제되는 것은 아니며 서비스만 해당 트래픽에 적용되지 않습니다. 예를 들어 경로 맵에서 이 개체를 사용하여 재배포할 경로를 정의하는 경우 "denied" 주소 공간은 단순히 재배포되지 않습니다.

b) *regex*를 클릭하고 이 항목과 일치해야 하는 AS 번호를 정의하는 정규식을 입력합니다.

가장 간단한 형식의 정규식은 완전한 AS 경로 번호일 뿐이며, 단일 자율 시스템에서 경로 업데이트를 허용하거나 거부합니다.

AS 번호는 1~4294967295 또는 1.0~65535.65535가 될 수 있습니다. AS 번호는 인터넷에서 각 네트워크를 식별하는 고유한 할당 값입니다. 시스템은 RFC 5396에 정의된 대로 asplain 및 asplain 표기법을 지원합니다. 사용해야 하는 표기법은 BGP 전역 설정에서 **bgp asnotation dot** 명령을 활성화했는지 여부에 따라 달라집니다.

단계 **7** 항목을 추가하여 AS 경로 액세스 목록을 완성합니다.

항목을 추가하려면 **...** > **Duplicate(**중복**)**(*action* 라인 왼쪽)를 클릭합니다. Duplicate(중복) 명령을 클릭하면 항목 바로 뒤에 새 항목이 추가됩니다.

따라서 개체에 항목이 많은 경우 "중복"할 항목을 현명하게 선택합니다. 개체 내에서 항목을 이동할 수 없으므로 실수를 한 경우 올바른 위치에서 수동으로 항목을 다시 생성해야 합니다. 규칙은 하향식으로 평가되며, 첫 번째 일치 항목이 적용됩니다.

항목을 복제하면 미리 구성된 특성이 없는 새로운 빈 항목이 삽입됩니다. "중복"을 생성한 후에는 위의 설명대로 진행하여 필요에 따라 구성합니다.

단계 **8** **OK(**확인**)**를 클릭하여 개체를 저장합니다.

이제 AS 경로 액세스 목록이 필요한 기능에 대해 BGP 개체, 경로 맵 개체 또는 FlexConfig 개체에서 개체를 사용할 수 있습니다.

커뮤니티 목록 구성

BGP 프로세스에서 커뮤니티 정보를 전송하도록 활성화한 경우 커뮤니티 목록을 경로 맵에서 일치 절로 사용하여 일치하는 경로에 대한 특성을 설정할 수 있습니다. 예를 들어 특정 커뮤니티에 대한 경로 기본 설정을 변경할 수 있습니다.

커뮤니티는 공통 특성을 공유하는 대상 그룹에 대한 알려진 경로에 서비스 공급자가 연결할 선택적 특성 또는 레이블입니다. 특정 커뮤니티 번호는 ISP에서 알릴 수 있습니다. ISP에서 번호와 해당 의미를 가져온 다음 경로 맵을 사용하여 번호를 처리할 방법을 선택해야 합니다.

커뮤니티 목록은 순서가 지정되며, 일치하는 항목은 액세스 및 접두사 목록과 유사한 하향식 첫 번째 일치 항목으로 결정됩니다.

두 가지 유형의 커뮤니티 목록이 있습니다.

- 표준 — 서비스 공급자로부터 얻은 커뮤니티와 같이 잘 알려진 특정 커뮤니티를 대상으로 하려는 경우 표준 목록을 사용합니다.
- 확장 — 정규식 일치를 기반으로 커뮤니티 집합을 일치시키려는 경우 확장 목록을 사용합니다.

프로시저

단계 **1** **Device(**디바이스**)** > **Advanced Configuration(**고급 컨피그레이션**)**에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

단계 **2** 목차에서 **Smart CLI(**스마트 **CLI)** > **Objects(**개체**)**를 선택합니다.

단계 **3** 다음 중 하나를 수행합니다.

- 개체를 생성하려면 **+** 버튼을 클릭합니다.
- 개체를 수정하려면 개체의 수정 아이콘( )을 클릭하십시오.

참조되지 않는 개체를 삭제하려면 해당 개체의 휴지통 아이콘( )을 클릭합니다.

단계 **4** **CLI Template(CLI** 템플릿**)**으로 **Standard Community List(**표준 커뮤니티 목록**)** 또는 **Expanded Community List(**확장 커뮤니티 목록**)**를 선택합니다.

단계 **5** 스마트 CLI 개체의 **Name(**이름**)**을 입력합니다. 이 이름은 **community-list** 명령에서 CLI 템플릿의 첫 번째 라인에 커뮤니티 목록 이름으로도 입력됩니다.

단계 **6** (표준 목록) 커뮤니티 목록 항목을 구성합니다.

각 항목은 *action* 옵션으로 시작하는 단일 라인에 포함됩니다.

a) *action*을 클릭하고 다음 중 하나를 선택합니다.

- **permit**—일치. 이 규칙과 일치하는 연결이 구성 중인 기능에 대해 선택됩니다.
- **deny**—일치하지 않음. 이 규칙과 일치하는 연결이 기능에서 제외됩니다. "denied" 트래픽이 삭제되는 것은 아니며 서비스만 해당 트래픽에 적용되지 않습니다. 예를 들어 경로 맵에서 이 규칙을 사용하여 재배포할 경로를 정의하는 경우 "거부됨" 주소 공간은 단순히 재배포되지 않습니다.

b) *community-number*를 클릭하고 최대 10개의 커뮤니티를 공백으로 구분하여 입력합니다. 단일 규칙의 여러 커뮤니티는 AND 처리되므로 모든 커뮤니티가 경로에서 일치하는 경우에만 일치 항목이 존재합니다.

BGP 프로세스에 대해 활성화된 번호 지정 방법에 따라 10진수 형식(1-4294967295) 또는 AA:NN 형식(각 값은 1~66535)으로 커뮤니티를 입력합니다. ISP 또는 다른 BGP 네이버에서 이러한 번호를 가져옵니다.

c) (선택 사항). *properties*를 클릭하고 잘 알려진 다른 커뮤니티를 규칙에 추가합니다.

- **internet**—이 커뮤니티 경로가 모든 피어(내부 및 외부)에게 알려집니다.
- **no-advertise**—이 커뮤니티 경로가 모든 피어(내부 또는 외부)에게 알려지지 않습니다.
- **no-export**—이 커뮤니티 경로가 같은 자율 시스템 안에 있는 피어 또는 연합 내의 다른 하위 자율 시스템에만 알려집니다. 이 경로는 외부 피어에 알려지지 않습니다.

단계 **7** (확장 목록) 커뮤니티 목록 항목을 구성합니다.

a) *action*을 클릭하고 **permit** 또는 **deny**를 선택합니다. 이러한 작업은 위에 설명되어 있습니다.

b) *regex*를 클릭하고 이 항목과 일치해야 하는 커뮤니티를 정의하는 정규식을 입력합니다.

* 또는 + 문자를 사용하여 매칭할 경우 가장 긴 구성소를 가장 먼저 일치시킵니다. 중첩된 구성소는 외부에서 안쪽으로 일치시키며 연결된 구문은 왼쪽부터 일치시킵니다. 정규식이 한 입력 문자열의 서로 다른 두 부분과 매칭할 경우 가장 앞에 오는 것을 먼저 일치시킵니다. 정규식 쓰기에 대한 자세한 내용은 Cisco IOS Terminal Services 컨피그레이션 가이드의 "정규식" 부록을 참조하십시오.

단계 **8** 항목을 추가하여 커뮤니티 목록을 완성합니다.

항목을 추가하려면 **...** > **Duplicate(**중복**)**(*action* 라인 왼쪽)를 클릭합니다. Duplicate(중복) 명령을 클릭하면 항목 바로 뒤에 새 항목이 추가됩니다.

따라서 개체에 항목이 많은 경우 "중복"할 항목을 현명하게 선택합니다. 개체 내에서 항목을 이동할 수 없으므로 실수를 한 경우 올바른 위치에서 수동으로 항목을 다시 생성해야 합니다.

항목을 복제하면 미리 구성된 특성이 없는 새로운 빈 항목이 삽입됩니다. "중복"을 생성한 후에는 위의 설명대로 진행하여 필요에 따라 구성합니다.

단계 **9** **OK(**확인**)**를 클릭하여 개체를 저장합니다.

이제 경로 맵이나 라우팅 프로세스에서 또는 FlexConfig 개체에서 커뮤니티 목록이 필요한 기능에 대해 개체를 사용할 수 있습니다.

정책 목록 구성

하나 이상의 일치 절을 대체하기 위해 경로 맵의 정책 목록을 사용할 수 있습니다. 따라서 재사용하려는 일련의 일치 절이 있는 경우 정책 맵을 사용하면 컨피그레이션이 간소화되므로 각 경로 맵에서 일치 절을 반복할 필요가 없습니다. BGP의 정책 목록을 참조하는 경로 맵을 사용할 수 있습니다.

경로 맵 내에서 정책 목록 외에 다른 일치 절을 포함할 수 있습니다. 정책 목록 일치 절은 수신 특성에 대해서만 일치합니다.

정책 목록은 일치하는 IPv4 주소만 지원합니다. IPv6 주소와 일치시킬 수 없습니다.

정책 맵에 있는 일치 절의 경우:

- 여러 일치 절은 AND 처리됩니다. 즉, 경로가 정책 목록과 일치하려면 각 절을 충족해야 합니다.
- 단일 일치 절 내의 여러 값은 OR로 처리됩니다. 즉, 경로가 해당 match 명령문 내의 어떤 값이든 일치하는 경우 이는 전체적으로 명령문과 일치하는 것으로 간주됩니다.

시작하기 전에

액세스 목록, 접두사 목록 또는 AS 경로 액세스 목록에 대해 일치 절을 구성하려는 경우 정책 목록을 생성하기 전에 해당 개체를 생성해야 합니다.

프로시저

단계 **1** **Device(**디바이스**)** > **Advanced Configuration(**고급 컨피그레이션**)**에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

단계 **2** 목차에서 **Smart CLI(**스마트 **CLI)** > **Objects(**개체**)**를 선택합니다.

단계 **3** 다음 중 하나를 수행합니다.

- 개체를 생성하려면 **+** 버튼을 클릭합니다.
- 개체를 수정하려면 개체의 수정 아이콘( )을 클릭하십시오.

참조되지 않는 개체를 삭제하려면 해당 개체의 휴지통 아이콘( )을 클릭합니다.

단계 **4** **Policy List(**정책 목록**)**을 **CLI Template(CLI** 템플릿**)**으로 선택합니다.

단계 **5** 스마트 CLI 개체의 **Name(**이름**)**을 입력합니다. 이 이름은 **policy-list** 명령에서 CLI 템플릿의 첫 번째 라인에 정책 목록 이름으로도 입력됩니다.

단계 **6** **policy-list** 명령에서 *action*을 클릭하여 다음 중 하나를 선택합니다.

- **permit**—일치. 이 목록과 일치하는 연결이 구성 중인 기능에 대해 선택됩니다.

- **deny**—일치하지 않음. 이 목록과 일치하는 연결이 기능에서 제외됩니다. "denied" 트래픽이 삭제되는 것은 아니며 서비스만 해당 트래픽에 적용되지 않습니다. 예를 들어 경로 맵에서 이 개체를 사용하여 재배포할 경로를 정의하는 경우 "denied" 주소 공간은 단순히 재배포되지 않습니다.

단계 **7** 템플릿 위의 **Show Disabled(**비활성화된 항목 표시**)**를 클릭하여 일치 명령을 표시합니다. 활성화하려는 match 명령문 왼쪽에있는 **+** 아이콘을 클릭해야 합니다. 다음 match 명령문의 조합을 구성하여 대상으로 하는 경로를 정의합니다.

- **match as-path**. 변수를 클릭하고 일치시킬 자율 시스템 번호를 정의하는 AS 경로 개체를 선택합니다.
- **configure match ip address** *list-type*. *list-type* 변수를 클릭하고 **access-list** 또는 **prefix-list**를 기반으로 하는 경로의 IP 주소와 일치시킬지를 선택합니다. 그러면 변수를 클릭하고 일치시킬 IP 주소를 정의하는 IPv4 접두사 목록 또는 표준 액세스 목록을 선택할 수 있는 **match ip address** 명령이 추가됩니다.
- **configure match ip next-hop** *list-type list-type* 변수를 클릭하고 **access-list** 또는 **prefix-list**를 기반으로 하는 경로의 다음 홉 라우터 IP 주소와 일치시킬지를 선택합니다. 그러면 변수를 클릭하고 일치시킬 IP 주소를 정의하는 IPv4 접두사 목록 또는 표준 액세스 목록을 선택할 수 있는 **match ip next-hop** 명령이 추가됩니다.
- **configure match ip route-source** *list-type list-type* 변수를 클릭하고 **access-list** 또는 **prefix-list**를 기반으로 하는 경로의 경로 소스 IP 주소와 일치시킬지를 선택합니다. 그러면 변수를 클릭하고 일치시킬 IP 주소를 정의하는 IPv4 접두사 목록 또는 표준 액세스 목록을 선택할 수 있는 **match ip route-source** 명령이 추가됩니다.
- **match community** *community-list options*. *community-list*변수를 클릭하고 일치시킬 커뮤니티를 정의하는 커뮤니티 목록 개체를 선택합니다. 목록의 모든 커뮤니티가 일치하는 경우에만 경로가 커뮤니티 목록과 일치하도록 하려면 *options*를 클릭하고 **exact-match**를 선택합니다.
- **match interface**. 변수를 클릭하고 일치시킬 경로의 모든 인터페이스를 선택합니다.
- **match metric**. 변수를 클릭하고 1~4294967295 범위에서 일치시킬 라우팅 MED(Multi-Exit dicator) 메트릭을 입력합니다.
- **match tag**. 변수를 클릭하고 일치시킬 경로 태그 값을 0~4294967295 범위에서 입력합니다.

단계 **8** **OK(**확인**)**를 클릭하여 개체를 저장합니다.

이제 BGP 라우팅에 사용할 경로 맵 개체의 개체를 사용할 수 있습니다.

프리픽스 목록 구성

접두사 목록은 액세스 제어 목록과 유사합니다. 접두사 목록은 허용/거부 규칙의 순서가 지정된 목록입니다. 여기서 permit(허용)은 목록과 일치해야 하는 주소 접두사를, deny(거부)는 목록과 일치하지 않아야 하는 주소 접두사를 나타냅니다. 시스템은 일치 항목을 하향식으로 평가하고 첫 번째 일치 규

칙을 기반으로 작업을 할당하며 반드시 가장 잘 일치하는 규칙을 기반으로 하는 것은 아닙니다. 따라서 필요한 일치 항목을 얻으려면 시퀀스 번호를 신중하게 지정해야 합니다.

경로 재분배 또는 삽입 또는 BGP 네이버 필터링을 위해 OSPF 필터링 또는 BGP, OSPF 또는 EIGRP 경로 맵에 접두사 목록을 사용할 수 있습니다.

IPv4 및 IPv6 주소에 대해 별도의 접두사 목록이 있지만 목록의 구조는 동일합니다.

프로시저

단계 **1** **Device(**디바이스**)** > **Advanced Configuration(**고급 컨피그레이션**)**에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

단계 **2** 목차에서 **Smart CLI(**스마트 **CLI)** > **Objects(**개체**)**를 선택합니다.

단계 **3** 다음 중 하나를 수행합니다.

- 개체를 생성하려면 **+** 버튼을 클릭합니다.
- 개체를 수정하려면 개체의 수정 아이콘()을 클릭하십시오.

참조되지 않는 개체를 삭제하려면 해당 개체의 휴지통 아이콘()을 클릭합니다.

단계 **4** **IPv4 Prefix List(IPv4** 접두사 목록**)** 또는 **IPv6 Prefix List(IPv6** 접두사 목록**)**를 **CLI Template(CLI** 템플릿**)**으로 선택합니다.

단계 **5** 스마트 CLI 개체의 **Name(**이름**)**을 입력합니다. 이 이름은 **prefix-list** 명령에서 CLI 템플릿의 첫 번째 라인에 접두사 목록 이름으로도 입력됩니다.

단계 **6** **seq** 명령줄인 접두사 목록 항목을 구성합니다.

각 항목은 **seq** 옵션으로 시작하는 단일 라인에 포함됩니다.

a) **seq**에서 *sequence-number*를 클릭하고 이 규칙의 번호(1~4294967294)를 입력합니다. 이 번호는 다른 규칙의 시퀀스 번호와 관련이 있으며, 첫 번째로 평가되는 규칙은 1입니다. 일반적인 방법은 5, 10, 15 등으로 카운트를 건너뛰는 것입니다. 그러면 다른 규칙의 시퀀스 번호를 변경할 필요 없이 새 규칙을 삽입할 수 있습니다.

b) *action*을 클릭하고 다음 중 하나를 선택합니다.

- **permit**—일치. 이 규칙과 일치하는 연결이 구성 중인 기능에 대해 선택됩니다.
- **deny**—일치하지 않음. 이 규칙과 일치하는 연결이 기능에서 제외됩니다. "denied" 트래픽이 삭제되는 것은 아니며 서비스만 해당 트래픽에 적용되지 않습니다. 예를 들어 경로 맵에서 이 규칙을 사용하여 재배포할 경로를 정의하는 경우 "거부됨" 주소 공간은 단순히 재배포되지 않습니다.

c) *ip-address-mask*를 클릭하고 네트워크 주소 및 마스크(IPv4의 CIDR 형식) 또는 IPv6의 접두사 길이를 입력합니다. 예를 들어 10.100.10.0/24 (IPv4) 또는 2001:DB8:0:CD30::/60 (IPv6)과 같이 입력합니다.

시스템에서는 **ge** 또는 **le** 옵션 중 하나를 포함하지 않는 한 이 주소/마스크에 대해 정확히 일치하는 항목을 사용합니다. 예를 들어 규칙에 **ge 9**를 포함하지 않은 경우 10.100.10.10/8은 10.100.10.0/24와 일치하지 않습니다.

마스크 또는 접두사 길이는 다음과 같을 수 있습니다.

- IPv4 = 0-32
- IPv6 = 0-128

d) (선택 사항). **ge** 및 **le** 키워드를 사용하여 IP 주소 및 마스크/접두사 길이보다 구체적인 접두사에 대해 일치시킬 접두사 길이 범위를 지정할 수 있습니다. 이러한 키워드가 없으면 정확한 일치 항목만 규칙과 일치하는 것으로 간주됩니다.

ge *min-prefix-length*는 일치시킬 최소 접두사 길이를 지정합니다. 최소 길이는 마스크/접두사 길이보다 길어야 하며 옵션이 있는 경우 **le** 옵션에서 정의된 최대 길이와 같거나 짧아야 합니다.

le *min-prefix-length*는 일치시킬 최대 접두사 길이를 지정합니다. 최댓값은 최솟값(있는 경우)과 같거나 커야 하며 최솟값이 지정되지 않은 경우 마스크/접두사 길이보다 길어야 합니다.

위에 언급된 상대적 길이 제한 외에 이러한 옵션의 길이에는 다음과 같은 외부 제한이 있습니다.

- IPv4 = 1-32
- IPv6 = 0-128

단계 **7** 항목을 추가하여 접두사 목록을 완성합니다.

항목을 추가하려면 **...** > **Duplicate(**중복**)(seq** 라인 왼쪽)를 클릭합니다. Duplicate(중복) 명령을 클릭하면 항목 바로 뒤에 새 항목이 추가됩니다.

편의상 항목을 시퀀스 순서대로 유지하는 것이 가장 좋습니다. 그러나 구축 시 접두사 목록은 개체에서 혼합된 경우에도 사퀀스 순서로 다시 작성됩니다.

항목을 복제하면 미리 구성된 특성이 없는 새로운 빈 항목이 삽입됩니다. "중복"을 생성한 후에는 위의 설명대로 진행하여 필요에 따라 구성합니다.

단계 **8** **OK(**확인**)**를 클릭하여 개체를 저장합니다.

이제 경로 맵이나 라우팅 프로세스에서 또는 FlexConfig 개체에서 접두사 목록이 필요한 기능에 대해 개체를 사용할 수 있습니다.

예

다음은 접두사 목록을 사용하여 접두사를 일치시키는 방법에 대한 몇 가지 예입니다. 시퀀스 번호는 간소화를 위해 예제에서 제외되었습니다. 각 규칙의 실제 동작은 해당 주소 공간의 하위 집합과 일치하는 이전 규칙에 의해 순차적으로 수정됩니다.

- 기본 경로 0.0.0.0/0 거부:

```
deny 0.0.0.0/0
```

- 접두사 10.0.0.0/8 허용:

```
permit 10.0.0.0/8
```

- 접두사가 192/8 인 경로에서 길이가 최대 24 비트 길이의 마스크 허용:

```
permit 192.168.0.0/8 le 24
```

- 접두사가 192/8 인 경로에 길이가 25비트보다 긴 마스크 거부 :

```
deny 192.168.0.0/8 ge 25
```

- 모든 주소 공간에서 8~24비트의 마스크 길이 허용:

```
permit 0.0.0.0/0 ge 8 le 24
```

- 모든 주소 공간에서 길이가 25비트보다 긴 마스크 거부:

```
deny 0.0.0.0/0 ge 25
```

- 접두사가 10/8인 모든 경로 거부:

```
deny 10.0.0.0/8 le 32
```

- 접두사가 192.168.1/24인 경로에 대해 길이가 25비트보다 긴 모든 마스크 거부:

```
deny 192.168.1.0/24 ge 25
```

- 접두사가 0/0인 모든 경로 허용:

```
permit 0.0.0.0/0 le 32
```

15 장

OSPF(Open Shortest Path First)

OSPF(Open Shortest Path First)는 연결 상태 내부 게이트웨이 프로토콜입니다. OSPF 라우터에서는 네이버 라우터에 연결 상태 정보를 플러딩하여 OSPF 영역에 있는 모든 라우터에서 네트워크 토폴로지를 전체적으로 볼 수 있도록 합니다.

IP 버전에 따라 별도의 OSPF 버전(IPv4 네트워크용 OSPFv2 및 IPv6 네트워크용 OSPFv3)이 있습니다. 이러한 버전은 독립적입니다. 즉, OSPFv3는 OSPFv2를 대체하지 않습니다.

Smart CLI 개체를 사용하여 디바이스를 OSPFv2 네트워크 토폴로지에 통합하도록 OSPFv2를 구성할 수 있습니다. OSPFv3를 설정할 수 없습니다.

OSPFv2 프로세스 및 영역 구성

threat defense을 사용해 최대 2개의 OSPFv2 프로세스를 구성할 수 있습니다. 프로세스 번호는 내부 전용 표시기입니다. 자체 추적을 위해 번호를 일관되게 지정할 수는 있지만 다른 디바이스에서 사용되는 모든 프로세스 번호를 일치시킬 필요는 없습니다.

모든 내부 네트워크에 대해 192.168.1.0/24와 같은 개인 네트워크 번호 지정을 사용하는 경우, 이러한 내부 네트워크에 대한 하나의 OSPFv2 프로세스와 외부 공용 주소 지정 가능 네트워크에 대한 두 번째 프로세스를 사용하여 공용 주소와 개인 주소를 구분해야 할 수 있습니다. 개인 번호 지정을 사용하지 않는 경우에도 내부에서 하나의 프로세스를, 외부에서 다른 프로세스를 실행하고 두 프로세스 간의 경로 하위 집합을 재분배할 수 있습니다. NAT를 사용하고 OSPF가 공용 및 개인 영역에서 가동되는 경우와 주소 필터링이 필요한 경우에는 2개의 OSPF 프로세스(하나는 공용 영역에 사용되는 프로세스이고 다른 하나는 개인 영역에서 사용되는 프로세스)를 실행해야 합니다.

반대로 영역 번호는 네트워크에 존재하며, 다른 인접 라우터에서 사용하는 번호와 동일해야 합니다. 단일 영역 네트워크를 구성하는 경우에는 영역 0(백본 영역이라고도 함)을 사용합니다. 계층적 네트워크 설계를 보유한 다중 영역 네트워크의 경우, 네트워크에 정의된 영역을 이해하고 이 디바이스가 참여해야 하는 영역을 파악해야 합니다.

가상 라우터를 사용하는 경우에는 가상 라우터당 2개의 OSPFv2 프로세스를 구성할 수 있습니다.

다음 절차에서는 단일 OSPFv2 프로세스를 생성하는 방법에 대해 설명합니다. 두 번째 프로세스를 생성하려면 절차를 반복합니다.

프로시저

단계 **1** 디바이스를 클릭한 다음, **Routing(**라우팅**)** 요약을 클릭합니다.

단계 **2** 가상 라우터를 활성화한 경우 OSPF를 구성 중인 라우터의 보기 아이콘( )을 클릭합니다.

단계 **3** **OSPF** 탭을 클릭합니다.

단계 **4** 다음 중 하나를 수행합니다.

- 새 프로세스를 생성하려면 **+** > **OSPF**를 클릭하거나 **Create OSPF Object(OSPF** 개체 생성**)** > **OSPF** 버튼을 클릭합니다.
- 수정할 개체의 수정 아이콘( )을 클릭합니다. 개체를 수정할 때는 직접 구성하지 않은 줄이 표시될 수도 있습니다. 이러한 줄은 구성 중인 기본값을 표시하기 위해 노출됩니다.

프로세스가 더 이상 필요하지 않은 경우 해당 개체의 휴지통 아이콘을 클릭하여 프로세스를 삭제합니다.

단계 **5** 개체의 이름 및 설명(선택 사항)을 입력합니다.

단계 **6** 기본 프로세스 속성을 구성합니다.

- **router ospf** *process-id*. *process-id*를 클릭하고 1과 65535 사이의 숫자를 입력합니다. 이 숫자는 이 디바이스 내에서만 의미가 있으며 다른 라우터에 구성된 프로세스 번호와 일치하지 않아도 됩니다. 숫자는 가상 라우터 내에서 고유해야 합니다.
- **log-adj-changes** *log-state*. *log-state*를 클릭하고 다음 옵션 중 하나를 선택합니다.
  - **enable** (권장) - OSPFv2 네이버가 작동 또는 중단될 경우 syslog 메시지가 생성됩니다. 이 옵션을 선택하면 **log-adj-changes** *log-type* 줄이 개체에 추가됩니다. 네이버가 작동 또는 중단되는 경우뿐만 아니라 각 상태 변경에 대해서도 syslog 메시지를 생성하려면 *log-type*을 클릭하고 **detail**을 선택합니다.

    자세한 메시지를 원하지 않을 경우, *log-type*을 옵션으로 그대로 두면 됩니다. 개체에서 이 줄을 삭제하지 마십시오.
  - **disable**- syslog 메시지가 생성되지 않습니다. **no log-adj-changes** 줄이 개체에 추가됩니다. 이 줄을 삭제하지 마십시오.

단계 **7** 개체 본문 위에 있는 **Show Disabled(**비활성화된 항목 표시**)** 링크를 클릭하여 가능한 다른 모든 구성 줄을 추가합니다.

단계 **8** 영역 번호를 구성합니다.

a) 명령을 활성화하려면 **area** *area-id* 줄 왼쪽의 **+**를 클릭합니다. 명령을 활성화할 때까지는 이를 구성할 수 있습니다.

b) *area-id*를 클릭하고 영역 번호를 입력합니다. 이 영역 번호는 OSPFv2 영역을 정의하는 다른 라우터에서 사용하는 번호와 동일해야 합니다. 영역 ID는 십진수 또는 IP 주소로 지정할 수 있습니다. 유효한 십진수 값의 범위는 0~4294967295입니다.

단계 **9** 영역 내에서 라우팅해야 하는 네트워크 및 인터페이스를 구성합니다.

a) **configure area** *area-id options* 줄 왼쪽의 +를 클릭합니다.

b) *area-id*를 클릭하고 **area** 명령의 동일한 영역 번호를 입력합니다.

c) *options*를 클릭하고 **properties**를 선택합니다. 이 작업을 수행하면 기본적으로 활성화되어 있는 줄(**network** 명령)을 비롯하여 여러 개의 줄이 추가됩니다.

d) **network** 명령에서 *network-object*를 클릭하고 이 영역에 포함되어야 하는 네트워크를 정의하는 개체를 선택합니다. 일반적으로 이는 직접 연결된 네트워크입니다. 예를 들어, 내부 인터페이스의 IP 주소가 192.168.1.1/24인 경우 이 명령에 대해 연결된 네트워크 개체에는 192.168.1.0/24가 포함됩니다. 개체가 아직 없는 경우 **Create New Network(**새 네트워크 생성**)**를 클릭하여 바로 생성합니다.

e) (선택 사항) **network** 명령에서 *tag-interface*를 클릭하고 네트워크를 호스팅하거나 네트워크로 라우팅되는 인터페이스를 선택합니다. 인터페이스를 선택하면 해당 인터페이스가 라우팅 프로세스에서 사용되기 때문에 인터페이스의 주소가 변경되는 것을 방지할 수 있습니다. 이를 통해 인터페이스 주소 지정을 변경할 경우 라우팅 구성에 영향을 줄 수 있다는 점을 다시 한 번 확인할 수 있습니다.

   여기서 인터페이스를 선택하는 경우 인터페이스에서 주소를 변경하려면 먼저 라우팅 프로세스에서 해당 주소를 제거해야 합니다. 그런 다음, IP 주소를 변경하고 나서 여기로 돌아와 새 네트워크 및 인터페이스를 선택하여 올바르게 구성된 라우팅 프로세스를 확인해야 합니다.

f) 다른 모든 새 영역 줄은 선택 사항이며 기본적으로 비활성화되어 있습니다. 이러한 서비스가 필요한 경우에만 이를 구성합니다. 자세한 내용은 OSPF 프로세스 및 영역 특성 맞춤설정, 395 페이지를 참고하십시오.

단계 **10** 다중 영역 네트워크에 대한 프로세스를 구성 중인 경우, **area** 및 **configure area** 줄에서 원으로 표시된 **-**의 왼쪽 영역 위에 마우스를 올리고 **...** > **duplicate(**중복**)**을 클릭합니다. 그런 다음 위의 설명대로 새 영역 및 해당 네트워크를 구성합니다. 이 라우팅 프로세스가 참여해야 하는 모든 영역을 정의할 때까지 이 프로세스를 반복합니다.

단계 **11** **OK(**확인**)**를 클릭합니다.

OSPF 프로세스 및 영역 특성 맞춤설정

OSPF에는 기본값이 설정된 여러 옵션이 포함되어 있습니다. 이러한 값은 여러 네트워크에서 원활하게 작동합니다. 그러나 필요한 정확한 동작을 얻기 위해 하나 이상의 설정을 조정해야 할 수 있습니다. 다음 주제에서는 OSPFv2 라우팅 프로세스를 맞춤설정할 수 있는 다양한 방법에 대해 설명합니다.

OSPF 프로세스에 대한 고급 설정 구성

거리 메트릭, 타이머, Graceful Restart, 링크 상태 광고 및 기타 라우팅 업데이트 전송에 사용되는 라우터 ID 등 OSPFv2 프로세스의 전반적인 동작을 제어하는 여러 가지 설정을 구성할 수 있습니다. 이러한 많은 설정에는 대부분의 네트워크에 적합한 기본값이 설정되어 있습니다.

프로시저

단계 **1** 디바이스를 클릭한 다음, **Routing(**라우팅**)** 요약을 클릭합니다.

단계 **2** 가상 라우터를 활성화한 경우 OSPF를 구성 중인 라우터의 보기 아이콘( )을 클릭합니다.

단계 **3** **OSPF** 탭을 클릭합니다.

단계 **4** OSPF 프로세스 개체를 추가하거나 수정합니다.

단계 **5** **setup ospf** 줄을 찾습니다.

개체를 추가할 경우, **Show Disabled(**비활성화된 항목 표시**)** 링크를 클릭하여 해당 줄을 표시해야 합니다. 그런 다음, 명령의 +를 클릭하여 이를 활성화하고 *configuration*을 클릭한 후 **advanced**를 선택합니다. 기본적으로 활성화되는 명령은 기본값으로 이미 활성화되어 있습니다.

개체를 수정할 경우, 해당 줄이 이미 활성화됩니다.

이 절차의 나머지 부분에서는 **Show Disabled(**비활성화된 항목 표시**)**를 클릭한 것으로 가정합니다. 명령이 표시되지 않을 경우, 비활성화된 명령을 표시해야 합니다.

단계 **6** (선택 사항). 라우터 ID를 구성합니다.

+를 클릭하여 **router-id** 명령을 활성화한 다음, 변수를 클릭하고 이 디바이스에서 라우터 업데이트를 전송할 때 사용해야 할 IPv4 주소를 입력합니다. OSPF 시스템에서는 두 개의 라우터가 동일한 라우터 ID를 가질 수 없으므로, 이는 해당 영역에서 고유해야 합니다.

프로세스에 대한 라우터 ID를 명시적으로 지정하지 않으면 시스템에서는 활성 인터페이스에 할당된 최상위 IP 주소를 사용합니다. 따라서 선택한 인터페이스를 비활성화하거나 해당 주소를 변경할 경우 라우터 ID가 변경될 수 있습니다. 라우터 ID를 명시적으로 할당하면 프로세스의 일관성을 보장할 수 있습니다.

단계 **7** (선택 사항). 요약 경로 비용을 계산할 경우 RFC 1583 호환성을 구성합니다.

+를 클릭하여 **configure summary-route-cost** 명령을 활성화한 다음, 변수를 클릭하고 RFC 1583 호환성을 끄는 **any**를 선택하거나 이를 켜는 **rfc1583**을 선택합니다.

이 명령은 OSPF 개체에서 기본적으로 활성화되어 있지 않지만, RFC 1583 호환성은 요약 경로 비용을 계산할 때 실제로 사용되는 기본 방법입니다. CLI에 정의된 컨피그레이션을 검토할 경우 비활성화된 설정만 표시됩니다.

RFC 1583 호환성이 활성화된 라우팅 루프가 발생할 수 있습니다. 라우팅 루프를 방지하기 위해 비활성화합니다. OSPF 라우팅 도메인의 모든 OSPF 라우터에서 RFC 1583 호환성을 동일하게 설정했는지 확인합니다.

단계 **8** (선택 사항). 멀티캐스트 OSPF(MOSPF) 링크 상태 광고(LSA)에 대한 시스템 로그 메시지를 억제합니다.

+를 클릭하여 **ignore lsa mospf** 명령을 활성화합니다.

시스템에서는 LSA Type 6 MOSPF 패킷을 지원하지 않습니다. 시스템에서 이러한 패킷을 수신할 때 시스템 로그 메시지를 전송하지 않도록 이 명령을 활성화하면 시스템 로그 서버의 노이즈를 줄일 수 있습니다.

단계 **9** 거리 메트릭을 구성합니다.

다음 **distance** 명령은 기본적으로 활성화되어 있습니다. 경로 유형을 기준으로 OSPF 경로 관리 거리를 변경할 수 있습니다. 거리는 1~255이며, 높은 숫자는 낮은 숫자보다 신뢰성이 떨어집니다. 이러한 메트릭은 서로 다른 프로세스에서 유사한 경로를 비교할 때 학습된 경로의 상대적인 값을 판단하는 데 사용됩니다.

- **distance ospf inter-area 110**. 숫자를 클릭하고 한 영역에서 다른 영역까지의 모든 경로에 대한 거리를 설정합니다.
- **distance ospf intra-area 110**. 숫자를 클릭하고 한 영역 내의 모든 경로에 대한 거리를 설정합니다.
- **distance ospf external 110**. 숫자를 클릭하고 재배포를 통해 학습된 다른 라우팅 도메인의 경로에 대한 거리를 설정합니다.

단계 **10** OSPF 프로세스의 경로 계산 타이머를 구성합니다.

다음 타이머 명령은 이러한 기본값을 사용하여 활성화됩니다.

- **timers lsa arrival 1000**. 숫자를 클릭하고, 시스템이 OSPF 네이버에서 동일한 LSA(Link-State Advertisement)를 수락하는 최소 간격(0~600000 밀리초)을 설정합니다. 이 명령을 사용하여 네이버에서 수신되는 동일한 LSA를 허용하기 위해 경과해야 하는 최소 간격을 나타낼 수 있습니다. 이 최소 시간 전에 수신되는 LSA는 무시됩니다.
- **timers pacing flood 33**. 숫자를 클릭하고, 플러딩 대기열의 LSA가 업데이트 간격 사이에서 속도 조절되는 시간(5~100 밀리초)을 설정합니다.
- **timers pacing lsp-group 240**. 숫자를 클릭하고 OSPF LSA(Link-State Advertisement)를 그룹으로 수집하고 새로 고치거나, 체크섬하거나, 기간 경과로 설정할 간격(10~1800초)을 설정합니다.
- **timers pacing retransmission 66**. 숫자를 클릭하고 재전송 대기열에서 LSA가 속도 조절되는 시간 간격(5~200 밀리초)을 설정합니다. OSPF 패킷 플러딩 요구 사항을 충족하는 다른 옵션을 모두 사용하지 않은 한 패킷 재전송 속도 조절 타이머를 변경하지 않는 것이 좋습니다. 특히, 기본 플러딩 타이머를 변경하기 전에 요약, 스텁 영역 사용, 대기열 조정 및 버퍼 조정을 먼저 구성하십시오.
- **timers throttle lsa 0 5000 5000**. 숫자를 클릭하고 OSPF(Open Shortest Path First) LSA(Link-State Advertisement) 생성을 위한 속도 제한 값을 설정합니다. LSA 및 SPF 제한은 네트워크가 불안정한 동안 OSPF에서 LSA 업데이트 속도를 늦추는 동적 메커니즘을 제공하며, OSPF를 보다 빠르게 통합할 수 있도록 합니다. 해당 값은 다음과 같습니다.
  - **Start Interval(**시작 간격**)(**첫 번째 숫자) — LSA의 첫 번째 발생을 생성하는 데 걸리는 최소 지연 시간(1~600000 밀리초)입니다. LSA의 첫 번째 인스턴스는 로컬 OSPF 토폴로지가 변

경된 즉시 생성됩니다. 다음 LSA는 이 시작 간격 이후에만 생성됩니다. 지연 없이 LSA를 생성하려면 0을 지정합니다.

- **Hold Time(**보류 시간**)**(두 번째 숫자) — LSA를 다시 생성하는 데 걸리는 최소 지연 시간(1~600000 밀리초)입니다. 이 값은 LSA 생성을 위해 이후의 속도 제한 시간을 계산하는 데 사용됩니다.
- **Maximum Interval(**최대 간격**)**(세 번째 숫자) — LSA를 다시 생성하는 데 걸리는 최대 지연 시간(1~600000 밀리초)입니다.

- **timers throttle spf 5000 10000 10000**. 숫자를 클릭하고 SPF(Shortest Path First) 생성을 위한 속도 제한 값을 설정합니다. 해당 값은 다음과 같습니다.
  - **Start Interval(**시작 간격**)**(첫 번째 숫자) — SPF 계산의 변경 사항을 수신하는 데 걸리는 지연 시간(1~600000 밀리초)입니다.
  - **Hold Time(**보류 시간**)**(두 번째 숫자) — 첫 번째 SPF 계산과 두 번째 SPF 계산 간의 지연 시간(1~600000 밀리초)입니다.
  - **Maximum Interval(**최대 간격**)**(세 번째 숫자) — SPF 계산을 위한 최대 대기 시간(1~600000 밀리초)입니다.

단계 **11** (선택 사항). OSPF 라우팅 도메인에 이르는 기본 외부 경로를 생성합니다.

+를 클릭하여 **default-information originate** 명령을 활성화합니다. 선택에 따라 다음 명령을 활성화 및 구성하여 기능을 세부적으로 조정할 수 있습니다.

- **default-information originate always**. 기본 경로가 없는 경우에도 항상 기본 경로를 광고합니다.
- **default-information originate metric 1 metric-type** *metric-type-value*. 기본 경로를 생성하는 데 사용되는 메트릭 유형 및 값입니다.
  - **metric** 숫자를 클릭하고 OSPF 기본 메트릭 값(0~16777214)을 입력합니다. 필요한 다른 값을 아는 경우를 제외하고는 10을 입력합니다.
  - **metric-type** 숫자를 클릭하고 1 또는 2를 OSPF 라우팅 도메인으로 광고되는 기본 경로와 연결된 외부 링크 유형으로 선택합니다. 기본값은 2입니다.
- **default-information originate route-map** *route-map*. 경로 맵이 충족될 경우 기본 경로를 생성하는 라우팅 프로세스를 지정하는 경로 맵을 선택합니다.

단계 **12** (선택 사항). 디바이스에 고가용성(HA)이 구성된 경우 NSF(Non-Stop Forwarding) Graceful Restart를 구성합니다.

시스템에 몇 가지 알려진 오류가 발생할 수 있으며, 이러한 상황은 스위칭 플랫폼 전반의 패킷 포워딩에 영향을 미치지 않아야 합니다. NSF(Non-Stop Forwarding) 기능을 사용하면 알려진 경로를 계속 사용하여 데이터를 전달하는 동시에 라우팅 프로토콜 정보를 복원할 수 있습니다. 이 기능은 구성 요소에 오류가 발생하거나(예: HA 모드에서 액티브 유닛이 스탠바이 유닛에 페일오버를 수행하거나, 클러스터 모드의 기본 유닛에서 새 기본으로 선택된 보조 유닛에 장애가 발생한 경우), 무중단 소프트웨어 업그레이드가 예약된 경우 유용합니다.

NSF Cisco(RFC 4811 및 RFC 4812) 또는 NSF IETF(RFC 3623)를 사용하여 OSPFv2에서 Graceful Restart를 구성할 수 있습니다.

디바이스를 NSF 지원 또는 NSF 인식 디바이스로 구성할 수 있습니다. NSF 지원 디바이스는 해당 디바이스의 재시작 작업을 네이버에 나타낼 수 있으며, NSF 인식 디바이스는 네이버를 초기화하도록 지원할 수 있습니다.

- 현재 작동 중인 모드에 관계없이 디바이스를 NSF 인식 디바이스로 구성할 수 있습니다.
- 디바이스를 NSF 지원 디바이스로 구성하려면 디바이스가 고가용성(페일오버) 또는 Spanned Etherchannel(L2) 클러스터 모드에 있어야 합니다.

참고 Graceful Restart를 구성할 경우에도 fast hello 패킷을 사용하도록 OSPF 프로세스를 구성하면 안 됩니다. 액티브 유닛과 스탠바이 유닛 간의 역할 변경에 소요된 시간이 구성된 dead 간격을 초과하므로, fast hello 패킷으로 Graceful Restart를 실행할 수 없습니다.

Graceful Restart를 구성하려면

a) +를 클릭하여 **configure nsf graceful-restart** 명령을 활성화합니다.
b) *mechanism* 변수를 클릭하고 다음 중 하나를 선택합니다.
   - **cisco** - Cisco RFC 4811 및 RFC 4812에 따라 NSF 지원 디바이스를 구성합니다.
   - **ietf** - IETF RFC 3623에 따라 NSF 지원 디바이스를 구성합니다.
   - **both** - 디바이스를 NSF 지원 디바이스 대신 NSF 인식 헬퍼로 구성합니다.
   - **none** - 이전에 구성한 경우 Graceful Restart를 비활성화합니다.
c) 이전 단계에서 선택한 항목을 기준으로 사양에 따라 Graceful Restart를 구현하는 데 필요한 명령이 추가됩니다. 이러한 명령을 비활성화하지 마십시오. 선택적으로 추가 구성이 필요한 명령은 하나밖에 없습니다. 다음은 추가된 명령에 대한 설명입니다. **no** 형식으로 된 명령은 관련 기능을 끕니다.
   - **nsf cisco helper**. Cisco NSF(Nonstop Forwarding) 헬퍼 모드를 활성화합니다. NSF 지원 threat defense 디바이스가 Graceful Restart를 수행하면 헬퍼 threat defense 디바이스는 무중단 포워딩 복구 프로세스를 지원합니다.
   - **nsf ietf helper** *mode-option*. IETF NSF(Nonstop Forwarding) 헬퍼 모드를 활성화합니다. NSF 지원 threat defense 디바이스가 Graceful Restart를 수행하면 헬퍼 threat defense 디바이스는 무중단 포워딩 복구 프로세스를 지원합니다. 선택에 따라, *mode-option*을 클릭하고 엄격한 LSA(Link-State Advertisement) 확인을 활성화할 수 있습니다. 엄격한 LSA 확인이 활성화된 상태에서, 다시 시작 시스템으로 플러딩되는 LSA에서 변경 사항이 감지되거나, Graceful Restart 프로세스가 시작되었을 때 다시 시작 시스템의 재전송 목록에 변경된 LSA가 있는 경우 헬퍼 시스템은 다시 시작 시스템의 지원 프로세스를 중단합니다.
   - **capability lls**. Cisco Graceful Restart에 필요한 LLS(Link Local Signaling)를 활성화합니다.
   - **capability opaque**. IETF Graceful Restart에 필요한 링크 상태 광고(LSA)를 활성화합니다.

단계 **13** **OK(**확인**)**를 클릭합니다.

OSPF 영역 속성 구성

일부 OSPF 영역 매개변수를 구성할 수 있습니다. 영역에서 광고할 네트워크를 정의하고, 필터링 및 가상 링크를 추가할 수 있습니다. 또한, 이러한 영역 파라미터에는 인증 설정, 스텁 영역 정의, 기본 요약 경로에 특정 비용 할당이 포함됩니다. 인증에서는 영역에 무단 액세스를 차단하는 비밀번호 기반의 보호 기능을 제공합니다.

영역 파라미터를 구성할 경우 해당 영역 내에서 시스템이 작동하는 방식을 알고 있어야 합니다.

여러 영역에 인터페이스가 있는 라우터는 ABR(영역 경계선 라우터)라고 합니다. OSPF를 사용하는 라우터와 다른 라우팅 프로토콜을 사용하는 라우터 간에 트래픽을 재분배하는 게이트웨이 역할을 수행하는 라우터를 ASBR(자동 시스템 경계 라우터)이라고 합니다.

ABR에서는 LSA(Link-State Advertisement)를 사용하여 사용 가능한 경로에 대한 정보를 다른 OSPF 라우터로 전송합니다. ABR 유형 3 LSA 필터링을 사용할 경우, ABR 역할을 수행하는 시스템을 통해 별도의 사설 및 공용 영역을 확보할 수 있습니다. 유형 3 LSA(영역 간 경로)는 한 영역에서 다른 영역으로 필터링할 수 있으며, 이렇게 하면 사설 네트워크를 알리지 않고도 NAT와 OSPF를 함께 사용할 수 있습니다.

프로시저

단계 **1** 디바이스를 클릭한 다음, **Routing(**라우팅**)** 요약을 클릭합니다.

단계 **2** 가상 라우터를 활성화한 경우 OSPF를 구성 중인 라우터의 보기 아이콘( )을 클릭합니다.

단계 **3** **OSPF** 탭을 클릭합니다.

단계 **4** OSPF 프로세스 개체를 추가하거나 수정합니다.

단계 **5** 영역 번호를 구성합니다.

a) 명령을 활성화하려면 **area** *area-id* 줄 왼쪽의 +를 클릭합니다. 명령을 활성화할 때까지는 이를 구성할 수 있습니다.

b) *area-id*를 클릭하고 영역 번호를 입력합니다. 이 영역 번호는 OSPFv2 영역을 정의하는 다른 라우터에서 사용하는 번호와 동일해야 합니다. 영역 ID는 십진수 또는 IP 주소로 지정할 수 있습니다. 유효한 십진수 값의 범위는 0~4294967295입니다.

단계 **6** 영역 내에서 라우팅해야 하는 네트워크 및 인터페이스를 구성합니다.

a) **configure area** *area-id options* 줄 왼쪽의 +를 클릭합니다.

b) *area-id*를 클릭하고 **area** 명령의 동일한 영역 번호를 입력합니다.

c) *options*를 클릭하고 **properties**를 선택합니다. 이 작업을 수행하면 기본적으로 활성화되어 있는 줄(**network** 명령)을 비롯하여 여러 개의 줄이 추가됩니다.

d) **network** 명령에서 *network-object*를 클릭하고 이 영역에 포함되어야 하는 네트워크를 정의하는 개체를 선택합니다. 일반적으로 이는 직접 연결된 네트워크입니다. 예를 들어, 내부 인터페이스의 IP 주소가 192.168.1.1/24인 경우 이 명령에 대해 연결된 네트워크 개체에는 192.168.1.0/24가 포함

됩니다. 개체가 아직 없는 경우 **Create New Network(**새 네트워크 생성**)**를 클릭하여 바로 생성합니다.

e) (선택 사항) **network** 명령에서 *tag-interface*를 클릭하고 네트워크를 호스팅하거나 네트워크로 라우팅되는 인터페이스를 선택합니다. 인터페이스를 선택하면 해당 인터페이스가 라우팅 프로세스에서 사용되기 때문에 인터페이스의 주소가 변경되는 것을 방지할 수 있습니다. 이를 통해 인터페이스 주소 지정을 변경할 경우 라우팅 구성에 영향을 줄 수 있다는 점을 다시 한 번 확인할 수 있습니다.

여기서 인터페이스를 선택하는 경우 인터페이스에서 주소를 변경하려면 먼저 라우팅 프로세스에서 해당 주소를 제거해야 합니다. 그런 다음, IP 주소를 변경하고 나서 여기로 돌아와 새 네트워크 및 인터페이스를 선택하여 올바르게 구성된 라우팅 프로세스를 확인해야 합니다.

단계 **7** (선택 사항). 스텁 영역 또는 NSSA(Not-so-stubby Area)로 전송되는 기본 요약 경로에 대한 비용을 구성합니다.

이 옵션은 아래에 설명된 것처럼 영역을 스텁 또는 NSSA로 구성하는 경우에만 의미가 있습니다. 영역 속성에서 +를 클릭하여 다음 명령을 활성화합니다.

area *area_id* **default-cost 1**

필요한 경우 올바른 영역 ID를 입력합니다. 그런 다음, 숫자를 클릭하고 경로의 상대적 비용(0~16777214)을 입력합니다. 기본값은 1입니다. 숫자가 커질수록 대상에 적용되는 다른 경로에서 해당 경로가 사용될 가능성이 낮아집니다.

단계 **8** (선택 사항). 영역의 접두사 필터링을 구성합니다.

ABR(Area Border Router)의 OSPFv2 영역 사이에 있는 Type 3 LSA(Link-State Advertisement)에서 광고되는 접두사를 필터링할 수 있습니다. 접두사 필터링은 OSPF 영역 간의 경로 배포 제어 기능을 개선합니다. 접두사 필터링은 지정된 접두사만 한 영역에서 다른 영역으로 전송되도록 허용하며 다른 모든 접두사는 제한합니다. 이러한 유형의 영역 필터링은 특정 OSPF 영역의 외부 또는 특정 OSPF 영역의 내부에 적용하거나, 동일한 OSPF 영역의 내부와 외부에 동시에 적용할 수 있습니다.

이 명령을 구성하려면 우선 **Device(**디바이스**)** > **Advanced Configuration(**디바이스 고급 컨피그레이션**)** 페이지에서 스마트 CLI 개체인 접두사 목록을 생성해야 합니다. 인바운드 또는 아웃바운드 광고에 대해 필터 방향 파라미터의 방향을 선택하여 별도의 접두사 목록을 구성할 수 있습니다.

area *area-id* **filter-list prefix** *prefix-list filter-direction*

단계 **9** (선택 사항). 영역을 스텁 영역으로 구성합니다.

스텁 영역은 외부 경로에 대한 정보가 전송되지 않는 영역입니다. 그 대신, 스텁 영역에는 ABR에서 생성된 기본 외부 경로가 있으며 이는 자동 시스템 외부의 목적지를 위한 경로입니다. 정상적으로 작동하려면 스텁 영역에서 기본 라우팅을 사용해야 합니다. 스텁 영역에 전송되는 LSA의 수를 더 줄이려면, ABR에서 **area stub** 명령의 **no-summary** 키워드를 사용하여 요약 링크 광고(LSA Type 3)가 스텁 영역에 전송되지 않도록 할 수 있습니다.

영역을 스텁으로 구성하려면 다음을 수행합니다.

a) setup area-id as type 줄 왼쪽의 +를 클릭합니다.
b) *type*을 클릭하고 **stub**을 선택합니다. 이렇게 하면 설정 줄 뒤에 area stub 명령이 추가됩니다.
c) 선택에 따라, **area stub** 명령에서 *stub-parameters*를 클릭하고 **no-summary**를 선택합니다.

단계 **10** (선택 사항). 영역을 NSSA(Not-so-stubby Area)로 구성합니다.

NSSA(Not-so-stubby Area)는 스텁 영역과 유사합니다. NSSA의 경우 코어의 Type 5 외부 LSA를 영역으로 플러딩하지 않으나, 제한된 방식을 통해 자동 시스템 외부 경로를 영역 내로 가져올 수 있습니다.

NSSA는 재분배를 통해 Type 7 자동 시스템 외부 경로를 NSSA 영역 내로 가져옵니다. 이러한 Type 7 LSA는 NSSA ABR(Area Border Router)에 의해 Type 5 LSA로 변환되며, 이는 전체 라우팅 도메인에 걸쳐 플러딩됩니다. 변환이 이루어지는 동안 요약 및 필터링이 지원됩니다.

OSPFv2를 사용하는 중앙 사이트를 다른 라우팅 프로토콜을 사용하는 원격 사이트에 연결해야 하는 ISP 또는 네트워크 관리자의 경우 연결 영역을 NSSA로 실행하여 관리 작업을 간소화할 수 있습니다. 원격 사이트의 경로는 스텁 영역으로 재배포할 수 없고 2개의 라우팅 프로토콜을 유지해야 하므로 기업 사이트 경계선 라우터와 원격 라우터 간의 연결을 OSPFv2 스텁 영역으로 실행할 수 없습니다. 일반적으로 RIP 같은 단순 프로토콜을 실행하여 재배포를 처리하게 됩니다. NSSA를 활용할 경우, 기업 라우터와 원격 라우터 간의 영역을 NSSA로 정의함으로써 OSPFv2를 확장하여 원격 연결을 지원할 수 있습니다.

이 기능을 사용하기 전에 다음 지침을 고려하십시오.

- 외부 목적지에 도착하는 데 사용할 Type 7 기본 경로를 설정할 수 있습니다. 구성된 경우, 라우터에서는 Type 7 기본값을 NSSA 또는 NSSA 영역 경계 라우터에 생성합니다.
- 동일한 영역 내의 모든 라우터는 해당 영역을 NSSA로 인식해야 합니다. 그렇지 않을 경우 라우터 간에 서로 통신을 수행할 수 없습니다.

영역을 NSSA로 구성하려면 다음을 수행합니다.

a) **setup** *area-id* **as** *type* 줄 왼쪽의 +를 클릭합니다.

b) *type*을 클릭하고 **nssa**를 선택합니다. 이렇게 하면 설정 줄 뒤에 **area nssa** 명령을 포함한 몇 가지 명령이 추가되는데, 이러한 명령은 활성화된 상태로 두어야 합니다.

c) (선택 사항). NSSA에 대한 Type 7 기본 경로를 생성하려면 +를 클릭하여 다음 명령을 활성화합니다.

area *area_id* **nssa default-information-originate metric 1 metric-type 2**

선택에 따라 다음 값을 조정할 수 있습니다.

- **metric** 숫자를 클릭하고 OSPF 기본 메트릭 값(0~16777214)을 입력합니다. 필요한 다른 값을 아는 경우를 제외하고는 10을 입력합니다.
- **metric-type** 숫자를 클릭하고 1 또는 2를 OSPF 라우팅 도메인으로 광고되는 기본 경로와 연결된 외부 링크 유형으로 선택합니다. 기본값은 2입니다.

d) (선택 사항). 시스템이 ABR이고 다른 라우팅 프로토콜에서 재배포하여 NSSA가 아닌 일반 영역으로만 경로를 가져오려면 +를 클릭하여 다음 명령을 활성화합니다.

area *area_id* **nssa no-redistribution**

e) (선택 사항). NSSA에 요약 경로를 삽입하지 않으려면 +를 클릭하여 다음 명령을 활성화합니다.

area *area_id* **nssa no-summary**

단계 **11** (선택 사항). 영역에 대한 가상 링크를 구성합니다.

OSPF에서는 모든 영역이 백본 영역에 연결되어야 합니다. 백본과의 연결이 끊길 경우 가상 링크를 설정하여 복구할 수 있습니다. 백본 영역에 연결된 라우터에 대한 가상 링크를 구성할 수 있습니다.

a) **configure area** *area-id* **virtual-link** *ip_address option* 줄 왼쪽의 +를 클릭합니다.
b) *ip_address*를 클릭하고 가상 링크를 설정할 라우터의 라우터 ID를 입력합니다.
c) (선택 사항). *option*을 클릭하고 **properties**를 선택하여 대부분의 네트워크에 적합하도록 기본값이 설정되어 있는 다음 속성을 조정합니다. 이러한 명령의 첫 부분은 동일한 명령의 파라미터이므로 생략합니다.

- **authentication** *auth-type*. +를 클릭하여 명령을 활성화한 다음, *auth-type*을 클릭하고 **none**, **password** 또는 **message-digest**를 클릭합니다. none 이외의 항목을 선택할 경우 주요 옵션을 구성합니다. 옵션은 OSPFv2 인터페이스 설정 및 OSPF 인증 구성, 409 페이지에 설명된 것처럼, OSPF 인터페이스에서 구성하는 옵션과 동일합니다. 다른 라우터에서 인증을 사용할 경우에만 인증을 구성합니다.
- **hello-interval 10**. 숫자를 클릭하고 인터페이스에서 전송된 hello 패킷 간의 간격(1~65535초)을 입력합니다.
- **retransmit-interval 5**. 숫자를 클릭하고 가상 링크에 대한 LSA 재전송 간의 시간(1~65535초)을 입력합니다.
- **transmit-delay 1**. 숫자를 클릭하고, OSPF가 토폴로지 변경 사항을 받은 때부터 SPF(최단 경로 우선) 계산을 시작할 때까지의 지연 시간(1~65535초)을 입력합니다.

d) **...** > **Duplicate(중복)(configure area virtual-link** 명령 옆)를 클릭하여 다른 가상 링크를 정의할 수 있습니다. 필요한 개수만큼 정의합니다.

단계 **12** (선택 사항). 시스템이 ABR(Area Border Router)인 경우, 범위를 구성하여 영역에 대한 경로를 통합하거나 요약할 수 있습니다.

area range 명령을 구성하면 ABR에서 단일 요약 경로를 다른 영역에 광고합니다. 라우팅 정보는 영역 경계에서 압축됩니다. 영역의 외부에서는 단일 경로가 각 어드레스 레인지에 대해 광고됩니다. 이러한 동작을 경로 요약이라고 합니다. 하나의 영역에 대해 여러 **area range** 명령을 구성할 수 있습니다. 이런 방법으로 OSPF는 각기 다른 여러 어드레스 레인지 세트에 대해 주소를 요약할 수 있습니다.

경로 요약을 구성하려면 다음을 수행합니다.

a) **area** *area-id* **range** *network-object range-parameters* 줄의 왼쪽에 있는 +를 클릭합니다.
b) *network-object*를 클릭하고 요약할 경로가 있는 어드레스 레인지를 정의하는 네트워크 개체를 선택합니다.
c) (선택 사항). *range-parameters*를 클릭하고 다음 속성 중 하나를 선택합니다.

- **advertise**. Type 3 요약 LSA(Link-State Advertisement)를 광고하고 생성하기 위해 주소 범위 상태를 설정합니다. 옵션을 선택하지 않을 경우 이 값이 기본값입니다.
- **not-advertise**. 어드레스 레인지 상태를 DoNotAdvertise로 설정합니다. Type 3 요약 LSA가 억제되고, 구성 요소 네트워크는 다른 네트워크에 숨겨진 상태로 유지됩니다.

d) **...** > **Duplicate(**중복**)**(**area range** 명령 옆)를 클릭하여 다른 경로 요약을 정의할 수 있습니다. 필요한 개수만큼 정의합니다.

단계 **13** 다중 영역 네트워크에 대한 프로세스를 구성 중인 경우, **area** 및 **configure area** 줄에서 원으로 표시된 - 왼쪽 영역 위에 마우스를 올리고 **...** > **Duplicate(**중복**)**를 클릭합니다. 그런 다음 위의 설명대로 새 영역 및 해당 네트워크와 다른 설정을 구성합니다. 이 라우팅 프로세스가 참여해야 하는 모든 영역을 정의할 때까지 이 프로세스를 반복합니다.

단계 **14** **OK(**확인**)**를 클릭합니다.

정적 **OSPF** 네이버 구성

정적 OSPF 네이버를 정의하여 포인트 투 포인트 비 브로드캐스트 네트워크 즉, VPN 터널을 통해 OSPF 경로를 광고할 수 있습니다.

이러한 라우터는 스스로 인접성을 형성할 수 있으므로, 일반 브로드캐스트 네트워크에 있는 정적 네이버를 정의하지 않아도 됩니다.

시작하기 전에

시스템이 네이버에 연결해야 할 때 통과하는 인터페이스를 결정합니다. 네이버 라우터를 정의하려면 먼저 이 인터페이스의 OSPF 설정을 구성해야 합니다.

프로시저

단계 **1** 디바이스를 클릭한 다음, **Routing(**라우팅**)** 요약을 클릭합니다.

단계 **2** 가상 라우터를 활성화한 경우 OSPF를 구성 중인 라우터의 보기 아이콘( )을 클릭합니다.

단계 **3** **OSPF** 탭을 클릭합니다.

단계 **4** OSPF 인터페이스 개체를 추가 또는 수정하고, 선택한 인터페이스에 대해 **ospf network point-to-point non-broadcast** 명령을 활성화합니다. 변경 내용을 저장합니다.

단계 **5** OSPF 프로세스 개체를 추가하거나 수정합니다.

단계 **6** **Show Disabled(**비활성화된 항목 표시**)**를 클릭하여 모든 명령을 표시한 다음, **+**를 클릭하여 **neighbor** 명령을 활성화합니다.

단계 **7** 네이버 주소를 구성합니다.

neighbor *ip-address* **interface** *interface*

- *ip-address*를 클릭하고 네이버 라우터의 IP 주소를 입력합니다.
- *interface*를 클릭하고 시스템이 라우터에 연결할 수 있을 때 통과하는 인터페이스를 선택합니다.

단계 **8** 필요한 경우 네이버 라우터에 대한 정적 경로를 구성합니다.

라우터의 IP 주소가 선택한 인터페이스와 같은 네트워크에 있는 경우, 정적 경로는 필요하지 않습니다. 예를 들어 IP 주소가 10.100.10.1/24이고, 네이버 주소가 10.100.10.2/24인 인터페이스를 선택할 경우 정적 경로가 필요하지 않습니다.

단계 **9** **...** > **Duplicate(**중복**)(neighbor**명령 옆)를 클릭하여 다른 정적 네이버를 정의할 수 있습니다. 필요한 개수만큼 정의합니다.

단계 **10** **OK(**확인**)**를 클릭합니다.

OSPF 요약 주소 구성

다른 프로토콜의 경로가 OSPF에 재분배될 경우, 각 경로는 외부 LSA에 개별적으로 광고됩니다. 그러나 시스템을 구성하여 지정된 네트워크 주소 및 마스크에 포함되는 모든 재배포된 경로에 대한 단일 경로를 광고할 수 있습니다. 이렇게 구성하면 OSPF 링크 상태 데이터베이스의 크기가 줄어듭니다. 지정된 IP 주소 마스크 쌍과 일치하는 경로를 억제할 수 있습니다. 태그 값을 일치 값으로 사용하여 경로 맵을 통한 재배포를 제어할 수 있습니다.

경로 요약은 광고된 주소를 통합하는 작업입니다. 다른 라우팅 프로토콜에서 학습된 경로를 요약할 수 있습니다. 요약 광고에 사용되는 메트릭은 특정 경로 중에서도 가장 작은 메트릭입니다. 요약 경로는 라우팅 테이블의 크기를 줄이는 데 도움이 됩니다.

OSPF에 요약 경로를 사용하면 OSPF ASBR에서는 단일한 외부 경로를 해당 주소에서 다루는 모든 재분배 경로의 취합본으로 광고하게 됩니다. OSPF로 재분배되는 다른 라우팅 프로토콜의 경로만 요약할 수 있습니다.

시작하기 전에

요약하려는 모든 주소에 대한 네트워크 개체를 생성합니다.

프로시저

단계 **1** 디바이스를 클릭한 다음, **Routing(**라우팅**)** 요약을 클릭합니다.

단계 **2** 가상 라우터를 활성화한 경우 OSPF를 구성 중인 라우터의 보기 아이콘( )을 클릭합니다.

단계 **3** **OSPF** 탭을 클릭합니다.

단계 **4** OSPF 프로세스 개체를 추가하거나 수정합니다.

단계 **5** **Show Disabled(**비활성화된 항목 표시**)**를 클릭하여 모든 명령을 표시한 다음, **+**를 클릭하여 **configure** *network-object* **as** *option* **summary-address** 명령을 활성화합니다.

단계 **6** *network-object*를 클릭하고 요약할 어드레스 스페이스를 정의하는 개체를 선택합니다.

단계 **7** *options*를 클릭하고 다음 중 하나를 선택합니다.

- **advertising**. 주소와 일치하는 경로를 광고합니다.
- **non-advertising**. 주소와 일치하는 경로를 억제합니다.

단계 **8** (선택 사항). 요약된 경로에 태그 값을 추가하려면 **+**를 클릭하여 **summary-address tag** 명령을 활성화하고, *tag-number* 변수를 클릭하고, 태그 번호(0~4294967295)를 입력합니다.

이 값은 OSPF 자체에서는 사용되지 않지만, ASBR(Autonomous System Boundary Router) 간에 정보를 교환하는 데 사용될 수 있습니다. 아무것도 지정하지 않으면 BGP 및 EGP의 경로에 원격 자동 시스템 번호가 사용됩니다. 다른 프로토콜에는 영(0)이 사용됩니다.

태그 값을 사용하는 주요 이유는 태그 번호를 기반으로 재배포를 제어하기 위해서입니다. 태그 값을 재배포 경로 맵에서 사용하지 않을 경우 여기에서 구성하지 않아도 됩니다.

단계 **9** **...** > **Duplicate(**중복**)(configure summary-address** 명령 옆)를 클릭하여 다른 경로 요약을 정의할 수 있습니다. 필요한 개수만큼 정의합니다.

단계 **10** **OK(**확인**)**를 클릭합니다.

OSPF 필터 규칙 구성

각 필터 규칙에 필요한 스마트 CLI 표준 액세스 목록 개체를 생성합니다. 거부 액세스 제어 항목(ACE)을 사용하여 항목과 일치하는 경로를 필터링하고, 업데이트해야 하는 경로에 대한 ACE를 허용합니다.

시작하기 전에

지정된 접두사만 한 영역에서 다른 영역으로 전송되도록 허용하고 다른 모든 접두사를 제한하도록 ABR(Area Border Rouer) Type 3 LSA 필터를 구성할 수 있습니다. 이러한 유형의 영역 필터링은 특정 OSPF 영역의 외부 또는 특정 OSPF 영역의 내부에 적용하거나, 동일한 OSPF 영역의 내부와 외부에 동시에 적용할 수 있습니다. OSPF ABR Type 3 LSA 필터링은 OSPF 영역 간의 경로 재분배 제어 기능을 개선합니다.

프로시저

단계 **1** 디바이스를 클릭한 다음, **Routing(**라우팅**)** 요약을 클릭합니다.

단계 **2** 가상 라우터를 활성화한 경우 OSPF를 구성 중인 라우터의 보기 아이콘( )을 클릭합니다.

단계 **3** **OSPF** 탭을 클릭합니다.

단계 **4** OSPF 프로세스 개체를 추가하거나 수정합니다.

단계 **5** **Show Disabled(**비활성화된 항목 표시**)**를 클릭하여 모든 명령을 표시한 다음, **+**를 클릭하여 **configure filter-rules** *direction* 명령을 활성화합니다.

단계 **6** *direction*을 클릭하고 수신 업데이트 필터링에 **in**을 선택하거나, 아웃바운드 업데이트 필터링에 **out**을 선택합니다.

단계 **7** 인바운드 필터의 경우, 업데이트를 필터링할 인터페이스를 선택적으로 지정할 수 있습니다. 인터페이스를 지정하지 않으면 인터페이스에서 수신된 모든 업데이트에 필터가 적용됩니다.

a) **+**를 클릭하여 **distribute-list** *acl-name* **in interface** *interface* 명령을 활성화합니다.

b) *interface* 변수를 클릭하고 인터페이스를 선택합니다.

단계 **8** 아웃바운드 필터의 경우 프로토콜을 선택적으로 지정하여, 해당 라우팅 프로세스로 광고되는 경로로 필터를 제한할 수 있습니다.

distribute-list out 명령은 두 가지 형식이 있습니다. 하나는 *protocol* 변수 뒤에 *identifier* 변수가 있는 형식이고, 다른 하나는 식별자가 없는 형식입니다. 다음과 같은 프로토콜을 선택할 수 있지만, 이러한 프로토콜은 추가 식별자 정보를 제공해야 하는지 여부에 따라 아래와 같은 명령 버전으로 나뉩니다.

- **connected**. 시스템의 인터페이스에 직접 연결된 네트워크에 대해 설정된 경로의 경우.
- **static**. 수동으로 생성한 정적 경로의 경우.
- **rip**. RIP에 광고된 경로의 경우.
- **bgp** *automonous-system*. BGP에 광고된 경로의 경우. *identifier*를 클릭하고 시스템에 정의된 BGP 프로세스에 대한 자동 시스템 번호를 입력합니다.
- **eigrp** *automonous-system*. EIGRP에 광고된 경로의 경우. *identifier*를 클릭하고 시스템에 정의된 EIGRP 프로세스에 대한 자동 시스템 번호를 입력합니다.
- **ospf** *process-id*. OSPF에 광고된 경로의 경우. *identifier*를 클릭하고 시스템에 정의된 다른 OSPF 프로세스에 대한 프로세스 ID를 입력합니다.

단계 **9** **...** > **Duplicate(**중복**)(configure filter-rules** 명령 옆)를 클릭하여 다른 필터 규칙을 정의할 수 있습니다. 필요한 개수만큼 정의합니다.

단계 **10** **OK(**확인**)**를 클릭합니다.

OSPF 재배포 구성

다른 라우팅 프로토콜, 연결된 경로, 정적 경로에서 OSPF 프로세스로 경로를 재배포하는 작업을 제어할 수 있습니다.

시작하기 전에

OSPF에 재배포를 구성하기 전에, 경로를 재배포할 라우팅 프로세스를 구성하고 변경 사항을 구축하는 것이 좋습니다.

경로 맵을 적용하여 재배포되는 경로를 세부적으로 조정하려면 스마트 CLI 경로 맵 개체를 생성합니다. 경로 맵과 일치하는 경로가 재배포되며, 일치하지 않는 모든 경로는 재배포되지 않습니다.

프로시저

단계 **1** 디바이스를 클릭한 다음, **Routing(**라우팅**)** 요약을 클릭합니다.

단계 **2** 가상 라우터를 활성화한 경우 OSPF를 구성 중인 라우터의 보기 아이콘()을 클릭합니다.

단계 **3** **OSPF** 탭을 클릭합니다.

단계 **4** OSPF 프로세스 개체를 추가하거나 수정합니다.

단계 **5** **Show Disabled(**비활성화된 항목 표시**)**를 클릭하여 모든 명령을 표시한 다음, **+**를 클릭하여 **configure redistribution** 명령을 활성화합니다.

단계 **6** *protocol* 변수를 클릭하고 경로를 재배포할 소스 프로세스를 선택합니다. **connected** 및 **static** 경로를 재배포하거나 **bgp**, **eigrp**, **isis**, **ospf** 또는 **rip**에 의해 생성된 경로를 재배포할 수 있습니다.

단계 **7** 라우팅 프로세스를 선택할 경우, *identifier* 변수를 클릭하고 필요한 값, 즉

- **bgp**, **eigrp**를 입력합니다. 자동 시스템 번호를 입력합니다.
- **ospf**. 프로세스 ID 번호를 입력합니다.
- **connected**, **static**, **isis**, **rip**. **none**을 입력합니다. 다른 값을 입력할 경우 해당 값은 무시됩니다.

단계 **8** (선택 사항, IS-IS 전용.) **redistribute isis level-2** 명령에서 **level-2**를 클릭하고 학습한 경로를 IS-IS 영역(**level-1**) 내에서만 재배포할지, IS-IS 영역(**level-2**) 간에 재배포할지, 또는 두 영역 모두(**level-1-2**)에서 재배포할지 선택합니다.

단계 **9** (선택 사항, 모든 프로토콜.) 재배포를 제어하기 위해 경로에 태그를 적용할 경우 **+**를 클릭하여 **redistribute tag** *tag-number* 명령을 활성화한 다음, 변수를 클릭하고 재배포할 경로와 연관된 태그를 입력합니다. 태그 번호의 범위는 0~4294967295입니다.

단계 **10** (선택 사항, 모든 프로토콜.) 표준 클래스를 준수하는 서브넷뿐만 아니라 모든 서브넷에 대한 경로를 재배포하려면 **+**를 클릭하여 **redistribute subnets** 명령을 활성화합니다.

예를 들어 이 명령을 활성화하지 않을 경우 10.100.10.0/24에 대한 특정 경로가 재배포되지 않습니다. 그 대신, 10.0.0.0/8에 대한 경로만 재배포됩니다.

단계 **11** (선택 사항, 모든 프로토콜.) 경로 맵을 기준으로 재배포되는 경로를 세부적으로 조정하려면 **+**를 클릭하여 **redistribute** *route-map* 명령을 활성화하고 변수를 클릭한 후 제한 사항을 정의하는 경로 맵을 선택합니다.

경로 맵을 적용하지 않을 경우, 해당 프로세스에 대한 모든 경로(재배포를 위해 구성된 다른 명령에 적합함)가 재배포됩니다.

단계 **12** (선택 사항, 모든 프로토콜.) 재배포된 경로에 대한 메트릭을 세부적으로 조정하려면 **+**를 클릭하여 다음 명령을 활성화하고 옵션을 구성합니다.

redistribute *protocol* **metric** *metric-value* **metric-type** *metric-type-value*

변수를 클릭하고 다음을 구성합니다.

- **metric**. 배포되는 경로의 메트릭 값은 0~16777214입니다. 하나의 OSPF 프로세스에서 동일한 디바이스의 다른 OSPF 프로세스로 재배포할 경우, 메트릭 값을 지정하지 않으면 한 프로세스에서 다른 프로세스로 메트릭이 이동됩니다. OSPF 프로세스에 다른 프로세스를 재배포할 경우 기본 메트릭은 20입니다.
- **metric-type**. 메트릭 유형은 OSPF 라우팅 도메인으로 광고되는 기본 경로와 연결된 외부 링크 유형입니다. 사용 가능한 옵션은 Type 1 외부 경로는 1, Type 2 외부 경로는 2입니다. 기본값은 2입니다.

단계 **13** (선택 사항, OSPF 전용.) 다음 명령은 다른 OSPF 프로세스에서 경로를 재배포할 때 기본적으로 활성화됩니다. **-**를 클릭하여 원치 않는 명령을 비활성화할 수 있습니다.

이러한 명령은 OSPF 경로가 다른 라우팅 도메인에 재배포되는 기준을 지정합니다.

- **redistribute ospf match external 1**. 자동 시스템의 외부에 있지만, OSPF에 Type 1 외부 경로로서 가져온 경로입니다.
- **redistribute ospf match external 2**. 자동 시스템의 외부에 있지만, OSPF에 Type 2 외부 경로로서 가져온 경로입니다.
- **redistribute ospf match internal**. 특정 자동 시스템의 내부에 있는 경로입니다.
- **redistribute ospf match nssa-external 1**. 자동 시스템의 외부에 있지만, OSPF에 Type 1 외부 경로로서 가져온 경로이며 NSSA(Not-So-Stubby-Area)로만 표시됩니다.
- **redistribute ospf match nssa-external 2**. 자동 시스템의 외부에 있지만, OSPF에 Type 2 외부 경로로서 가져온 경로이며 NSSA(Not-So-Stubby-Area)로만 표시됩니다.

단계 **14** **...** > **Duplicate(**중복**)(configure redistribution** 명령 옆)를 클릭하여 다른 프로토콜에 대한 재배포를 구성할 수 있습니다. 해당 네트워크에 적합한 각 프로토콜에 대해 재배포를 구성합니다.

단계 **15** **OK(**확인**)**를 클릭합니다.

OSPFv2 인터페이스 설정 및 OSPF 인증 구성

네이버 OSPF 라우터를 향하는 모든 인터페이스는 hello 패킷 및 기타 방법을 사용해 라우터와 통신함으로써 네이버의 상태를 확인하고 라우팅 업데이트를 공유합니다. 이러한 특성 중 일부에는 기본 설정이 있지만 OSPF 인터페이스 설정 개체를 사용하여 옵션을 명시적으로 설정하는 것이 가장 좋습니다. OSPF 네이버 라우터에 인접한 각 인터페이스에 대한 개체를 생성합니다.

참고 특정 네트워크의 라우터는 인증 및 분실 네이버 탐지 hello 및 dead 간격에 대해 동일한 값을 가져야 합니다.

프로시저

단계 **1** 디바이스를 클릭한 다음, **Routing(**라우팅**)** 요약을 클릭합니다.

단계 **2** 가상 라우터를 활성화한 경우 OSPF를 구성 중인 라우터의 보기 아이콘( )을 클릭합니다.

단계 **3** **OSPF** 탭을 클릭합니다.

단계 **4** 다음 중 하나를 수행합니다.

- 새 개체를 생성하려면 + > **OSPF Interface Settings(OSPF** 인터페이스 설정**)**를 클릭하거나 **Create OSPF Object(OSPF** 개체 생성**)** > **OSPF Interface Settings(OSPF** 인터페이스 설정**)** 버튼을 클릭합니다.
- 수정할 개체의 수정 아이콘( )을 클릭합니다. 개체를 수정할 때는 직접 구성하지 않은 줄이 표시될 수도 있습니다. 이러한 줄은 구성 중인 기본값을 표시하기 위해 노출됩니다.

인터페이스 설정 개체가 더 이상 필요하지 않은 경우 해당 개체의 휴지통 아이콘을 클릭하여 해당 개체를 삭제합니다.

단계 **5** 개체의 이름 및 설명(선택 사항)을 입력합니다.

단계 **6** 인터페이스에 대한 인증을 구성합니다.

configure authentication *auth_type*

OSPF 인증을 구성하려면 각 OSPF 인터페이스에서 비밀번호 또는 인증 키를 구성한 다음, 해당 영역 자체에서 인증을 활성화해야 합니다. 인터페이스와 영역에서 동일한 인증 방법을 선택해야 합니다.

*auth-type*을 클릭하여 다음 옵션을 선택할 수 있습니다.

- **none**- OSPF 인증은 사용하지 마십시오. 링크에서 작동하는 모든 OSPF 라우터에서는 이 라우터와의 인접성을 설정할 수 있습니다. 다음 명령이 **ospf authentication null** 개체에 추가됩니다.
- **password**- 공유 비밀번호를 사용하여 OSPF 연결을 인증합니다. 인터페이스별로 각 네트워크에 별도의 비밀번호를 구성할 수 있습니다. 그러나 동일한 네트워크에 있는 모든 네이버 라우터에는 OSPF 정보를 교환할 수 있도록 동일한 비밀번호가 있어야 합니다.

  이 옵션을 선택하면 두 가지 명령(**ospf authentication** 및 **ospf authentication-key** *key*)이 추가됩니다. 변수를 클릭하여 다음을 구성합니다.

  - *key* - 비밀번호를 비롯한 비밀 키 개체를 선택합니다. 비밀번호는 최대 8자까지 입력할 수 있습니다. 두 문자 사이에 공백을 포함할 수 있습니다. 비밀번호 맨 앞이나 맨 뒤의 공백은 무시됩니다. 개체가 아직 없는 경우 목록 하단에서 **Create New Secret Key(**새 비밀 키 생성**)**를 클릭하여 바로 생성합니다.

- **message-digest**- 메시지 다이제스트(MD5)를 사용하여 OSPF 연결을 인증합니다. MD5 인증에서는 통신의 무결성을 확인하고, 발신지를 인증하며, 적시성을 점검합니다. 동일한 MD5 키를 사용하도록 두 라우터를 모두 구성해야 합니다.

  이 옵션을 선택하면 두 가지 명령(**ospf authentication message-digest** 및 **ospf message-digest-key** *key-id* **md5** *key*)이 추가됩니다. 변수를 클릭하여 다음을 구성합니다.

  - *key-id* - 1부터 255까지의 인증 키 ID 번호입니다. 동일한 키 ID 및 관련 MD5 키를 사용하여 네이버 라우터를 구성해야 합니다.
  - *key* - MD5 키를 포함하는 비밀 키 개체를 선택합니다. 키는 최대 16자의 영숫자 비밀번호입니다. 문자 사이에 공백을 포함할 수 있습니다. 키 맨 앞이나 맨 뒤의 공백은 무시됩니다. 개체가 아직 없는 경우 목록 하단에서 **Create New Secret Key(**새 비밀 키 생성**)**를 클릭하여 바로 생성합니다.

단계 **7** (선택 사항) LSA(연결 상태 알림) 타이머를 구성합니다.

이러한 타이머에는 기본값이 있으므로 네트워크에 다른 설정이 필요한 경우에만 기본값을 변경해야 합니다. 다음 명령을 구성합니다.

- **ospf retransmit interval 5**- OSPF 인터페이스에 속하는 인접성에 대해 LSA를 재전송하는 동안의 시간(초 단위)입니다. 시간(초 단위)은 연결된 네트워크에 있는 두 라우터 간의 예상 왕복 지연

시간보다 길어야 합니다. 범위는 1초 ~ 8192초입니다. 기본값은 5초입니다. 5를 클릭하고 새 숫자를 입력하여 값을 변경합니다.

- **ospf transmit-delay 1**- OSPF 인터페이스에서 연결 상태 업데이트 패킷을 전송하는 데 필요한 예상 시간(초 단위, 1에서 8192초 사이)입니다. 기본값은 1초입니다. 1을 클릭하고 새 숫자를 입력하여 값을 변경합니다.

단계 **8** (선택 사항) 기타 모든 설정은 기본값이거나 선택 사항입니다. 다른 동작이 필요한 경우에만 이를 변경하거나 활성화합니다. **Show Disabled(**비활성화된 항목 표시**)** 링크를 클릭하여 옵션을 표시합니다.

다음은 추가 인터페이스 설정입니다. 설정을 활성화하려면 명령의 왼쪽에 있는 **+**를 클릭한 다음, 명령을 구성합니다(필요한 경우).

- **ospf cost** *value* - OSPF 인터페이스에서 패킷을 전송하는 비용(연결 상태 메트릭)으로 1에서 65535 사이의 값입니다. 값 1은 인터페이스에 직접 연결된 네트워크를 나타냅니다. 변수를 클릭하고 네트워크에서 사용 중인 숫자를 기준으로 인터페이스의 기능을 나타내는 비용을 입력합니다.

  값을 결정할 때, 인터페이스 대역폭이 클수록 해당 인터페이스 전반에서 패킷을 전송하는 관련 비용이 낮습니다. 다시 말해, 큰 비용 값은 낮은 대역폭 인터페이스를 나타내며, 작은 비용 값은 높은 대역폭 인터페이스를 나타냅니다. 선택하는 특정 숫자에는 고유한 의미가 없습니다. 이 값은 OSPF 영역 전체에서 인터페이스에 대해 구성하는 다른 값에 상대적입니다. 이러한 값은 대상에 대한 최적의 경로 계산에 영향을 미칩니다.

  threat defense 디바이스의 OSPF 인터페이스 기본 비용은 10입니다. 이 기본값은 Cisco IOS 소프트웨어와 다릅니다. 고속 이더넷과 기가비트 이더넷의 기본 비용은 1이고 10BaseT의 기본 비용은 10입니다. 네트워크에서 ECMP를 사용 중인 경우 이 차이를 고려해야 합니다.

- **ospf database-filter all out**- 동기화 및 플러딩 중에 OSPF 인터페이스로 발신되는 모든 LSA를 필터링합니다.

- **ospf mtu-ignore**- 수신 데이터베이스 패킷에 대한 OSPF MTU(최대 전송 단위) 불일치 탐지를 비활성화합니다. OSPF에서는 인접 디바이스가 공통 인터페이스에서 동일한 MTU를 사용하고 있는지 여부를 확인합니다. 이 확인은 네이버에서 DBD(Database Descriptor) 패킷을 교환할 때 이루어집니다. DBD 패킷에 수신되는 MTU가 수신 인터페이스에 구성된 MTU보다 크면 OSPF 인접성이 설정되지 않습니다. 인터페이스의 MTU 값을 동일하게 수정할 수 없는 경우에는 MTU 확인을 비활성화할 수 있습니다.

- **ospf network point-to-point non-broadcast**- OSPF 인터페이스를 포인트 투 포인트 비 브로드캐스트 네트워크로 구성합니다. 그러면 VPN 터널을 통해 OSPF 경로를 전송할 수 있습니다. 이 옵션을 구성하는 경우 네이버의 동적 검색을 수행할 수 없습니다. 또한 다음 작업을 수행해야 합니다.

  - OSPF 프로세스 개체를 업데이트하여 이 인터페이스에 대한 단일 고정 네이버를 정의합니다. 또한 네이버 라우터의 OSPF 프로세스를 업데이트하여 이 디바이스를 고정 네이버로 정의합니다.

  - 네이버 라우터를 가리키는 고정 경로를 각 라우터에서 생성합니다.

- **ospf priority** *value* - 네트워크의 다른 라우터에 상대적인 라우터의 우선순위(0~255)입니다. 기본 우선순위는 1입니다. 네트워크에 연결된 두 라우터가 모두 전용 라우터가 되려고 시도하는 경우 라우터 우선순위가 더 높은 라우터가 전용 라우터가 됩니다. 우선순위가 동일한 경우 라우

터 ID 값이 더 큰 라우터가 전용 라우터가 됩니다. 라우터 우선순위가 0으로 설정된 라우터는 전용 라우터 또는 백업 전용 라우터가 될 수 없습니다. 변수를 클릭하고 네트워크에서 사용하는 상대 번호 지정 시스템을 기준으로 우선순위를 선택합니다.

- **ospf lost-neighbor-detection** *detection-mechanism* - 시스템에서 네이버 라우터의 작동 중지 여부를 확인하는 방법을 정의합니다. OSPF 라우터가 중단됨으로 선언될 때마다 OSPF에서 경로를 다시 계산해야 합니다. 분실 네이버 탐지 구성에 대한 자세한 정보는 OSPFv2 손실된 네이버 탐지 및 Fast Hello 패킷(OSPF 인터페이스 설정) 구성, 412 페이지의 내용을 참조하십시오.

단계 **9** **OK(**확인**)**를 클릭합니다.

OSPFv2 손실된 네이버 탐지 및 Fast Hello 패킷(OSPF 인터페이스 설정) 구성

OSPF 프로세스에서는 각 네이버 라우터에 hello 패킷을 정기적으로 전송하여 네이버가 계속 응답할 수 있는지 확인합니다. 응답에 계속해서 실패하면 네이버 라우터(전체 또는 인접 인터페이스만)를 라우팅에 사용할 수 없고, OSPF에서는 경로를 다시 계산해야 하며, OSPF 시스템은 업데이트된 라우팅 테이블에서 통합해야 하는 것입니다.

다음 값을 조정하여 네트워크를 세밀하게 조정할 수 있습니다. 네이버가 중단됨으로 선언되고 경로가 다시 계산되는 빈도를 최소화하는 것이 가장 좋습니다. 한편, OSPF 라우터(또는 인터페이스)가 실제로 중단되었을 때 네트워크가 양호한 라우팅 테이블에서 재통합되는 데 걸리는 시간을 최소화할 수도 있습니다.

- Hello 간격 - 이는 hello 패킷이 전송되는 간격의 시간입니다. 기본값은 10초마다입니다. 원하는 경우 fast hello 패킷을 구성할 수 있습니다. 그러면 hello가 1초 미만의 간격으로 전송됩니다. fast hello 패킷을 사용하면 중단된 네이버가 가장 빠르게 탐지되고 라우팅 테이블이 재통합됩니다.
- Dead 간격 - 네이버에서 hello 패킷이 표시되지 않는 경우 네이버가 dead로 선언된 시간입니다. fast hello 패킷을 사용하는 경우를 제외하고 기본값은 40초(기본 hello 간격의 4배)입니다.이 경우 dead 간격은 항상 1초입니다. dead 간격을 더 작게 지정하면 네이버의 작동 중단을 더 빠르게 탐지하여 통합 기능을 개선할 수 있지만, 라우팅이 더 불안정해질 수 있습니다. 어떤 경우든 dead 간격을 hello 간격보다 더 크게 구성해야 합니다. 네트워크의 모든 OSPF 라우터에서 dead 간격을 동일하게 설정해야 합니다.

OSPF Interface Settings(OSPF 인터페이스 설정) 개체에서 손실된 네이버터 탐지를 구성합니다.

프로시저

단계 **1** 디바이스를 클릭한 다음, **Routing(**라우팅**)** 요약을 클릭합니다.

단계 **2** 가상 라우터를 활성화한 경우 OSPF를 구성 중인 라우터의 보기 아이콘( )을 클릭합니다.

단계 **3** **OSPF** 탭을 클릭합니다.

단계 **4** 다음 중 하나를 수행합니다.

- 새 개체를 생성하려면 + > **OSPF Interface Settings(OSPF** 인터페이스 설정**)**를 클릭하거나 **Create OSPF Object(OSPF** 개체 생성**)** > **OSPF Interface Settings(OSPF** 인터페이스 설정**)** 버튼을 클릭합니다.
- 수정할 개체의 수정 아이콘()을 클릭합니다. 개체를 수정할 때는 직접 구성하지 않은 줄이 표시될 수도 있습니다. 이러한 줄은 구성 중인 기본값을 표시하기 위해 노출됩니다.

단계 **5** **ospf lost-neighbor-detection** *detection-mechanism* 명령이 표시되지 않으면 **Show Disabled(**비활성화된 항목 표시**)** 링크를 클릭합니다.

단계 **6** 이를 활성화하려면 명령 왼쪽의 **+**를 클릭합니다.

단계 **7** *detection-mechanism*을 클릭하고 구현하려는 메커니즘을 선택합니다.

- **dead-interval-** 표준 hello 간격을 초 단위로 구성하려는 경우 다음과 같은 명령이 추가되었습니다. 필요에 따라 해당 값을 조정하십시오.
  - **ospf hello-interval 10-** Hello 간격(1~8192초)입니다. 기본값은 10입니다. 이 값은 dead 간격보다 작아야 합니다. 원하는 숫자를 입력하려면 값을 클릭합니다.
  - **ospf dead-interval 40-** dead 간격(1~8192초)입니다. 권장 값은 hello 간격의 4배이지만 더 빠른 통합을 위해 시간을 더 짧게 구성할 수 있습니다.
- **hello-multiplier-** 1초 미만의 fast hello 패킷을 구성하려는 경우 다음과 같은 명령이 추가되었습니다. 값을 구성해야 합니다.
  - **ospf dead-interval minimal hello-multiplier** *value* - 변수를 클릭하고 각 초마다 전송해야 하는 hello 패킷의 수를 3에서 20 사이의 값으로 입력합니다. dead 간격은 **minimal** 키워드를 사용하여 1초로 설정됩니다.

단계 **8** **OK(**확인**)**를 클릭합니다.

OSPF 모니터링

OSPF를 모니터링하고 트러블슈팅하려면 CLI 콘솔을 열거나 디바이스 CLI에 로그인하여 다음 명령을 사용합니다. Routing(라우팅) 페이지의 **Commands(**명령**)** 메뉴에서 이러한 명령 중 일부를 선택할 수도 있습니다.

show ospf ?를 사용하여 추가 옵션 목록을 가져옵니다. 예를 들어, 프로세스 ID, 영역 ID 및 가상 라우터를 지정하여 표시되는 정보를 제한할 수 있으며 원하는 정보만 대상으로 하는 기타 옵션을 지정할 수 있습니다. 다음 목록은 요약입니다.

- **show ospf**

  OSPFv2 라우팅 프로세스에 대한 일반적인 정보가 표시됩니다.

- **show ospf border-routers**

  ABR 및 ASBR에 대한 내부 OSPFv2 라우팅 테이블 항목이 표시됩니다.

- **show ospf database**

  특정 라우터에 대해 OSPFv2 데이터베이스에 관련된 정보 목록이 표시됩니다.

- **show ospf events**

  OSPF 내부 이벤트 정보가 표시됩니다.

- **show ospf flood-list**

  인터페이스를 통해 플러딩되기를 대기 중인 LSA 목록이 표시됩니다(OSPF v2packet 속도 확인). OSPFv2 업데이트 패킷은 자동으로 속도를 조절하여 33밀리초 미만의 속도로는 전송되지 않도록 합니다. 속도가 조절되지 않을 경우 일부 업데이트 패킷은 링크 속도가 느려지거나, 업데이트가 네이버에 빠른 속도로 수신되지 않거나, 라우터의 버퍼 용량이 부족해질 수 있습니다.

  효율성을 높이고 재전송 손실을 최소화하기 위해서는 재발송하는 동안에도 속도 조절을 사용해야 합니다. 또한 인터페이스 외부로 전송하기 위해 대기 중인 LSA를 표시할 수도 있습니다. 속도 조절을 사용하면 OSPFv2 업데이트 및 재전송 패킷을 더욱 효율적으로 전송할 수 있습니다.

- **show ospf interface**

  OSPFv2 관련 인터페이스 정보가 표시됩니다.

- **show ospf neighbor**

  인터페이스당 OSPFv2 네이버 정보가 표시됩니다.

- **show ospf nsf**

  OSPFv2 관련 NSF(Non-Stop Forwarding) 정보를 표시합니다.

- **show ospf request-list**

  라우터에서 요청한 모든 LSA 목록이 표시됩니다.

- **show ospf retransmission-list**

  재전송 대기 중인 모든 LSA 목록을 표시합니다.

- **show ospf rib**

  OSPF RIB(Router Information Base)를 표시합니다.

- **show ospf statistics**

  SPF가 실행된 횟수, 이유 및 지속 시간 같이 다양한 OSPFv3 통계를 표시합니다.

- **show ospf summary-addresses**

  OSPFv2 프로세스에 따라 구성된 모든 요약 주소 재분배 정보의 목록이 표시됩니다.

- **show ospf traffic**

  특정 OSPFv2 인스턴스에 의해 전송되거나 수신된 다양한 유형의 패킷 목록이 표시됩니다.

- **show ospf virtual-links**

  OSPFv2 관련 가상 링크 정보가 표시됩니다.

16 장

EIGRP(Enhanced Interior Gateway Routing Protocol)

EIGRP(Enhanced Interior Gateway Routing Protocol)는 하이브리드 동적 거리 벡터 및 링크 상태 내부 게이트웨이 라우팅 프로토콜입니다. 이는 원래 Cisco에서 개발한 독점 프로토콜로 이제는 RFC 7868에 정의된 개방형 표준입니다. 자율 시스템 내에서 내부 경로를 관리하기 위해 EIGRP를 구성할 수 있습니다.

EIGRP의 모범 사례

다음은 EIGRP 구성을 위한 몇 가지 팁입니다.

- 기존 EIGRP 자율 시스템에 디바이스를 삽입하는 경우 자율 시스템에 있는 다른 라우터의 컨피그레이션을 검사하여 시스템 번호 및 기타 맞춤화를 확인합니다. 추가하는 threat defense 디바이스에서 동일하거나 최소한 일관된 맞춤화를 구현해야 합니다.
- 전체 EIGRP 프로세스를 구성할지 아니면 스텁 프로세스를 구성할지 결정합니다.
  - threat defense 디바이스가 둘 이상의 다른 EIGRP 라우터에 연결된 자율 시스템의 중간에 있는 경우 전체 EIGRP 프로세스가 필요할 수 있습니다. 전체 라우팅을 위한 EIGRP 프로세스 구성, 418 페이지를 참조하십시오.
  - threat defense 디바이스가 한 개의 다른 EIGRP 라우터에만 연결되는 자율 시스템의 엣지에 있고, 그렇지 않으면 연결된 네트워크만 호스팅하는 경우 스텁 라우터로 구성하는 것이 가장 적합할 수 있습니다. threat defense 디바이스가 연결된 경로에 대한 정보를 EIGRP 네이버에 전송하도록 스텁을 구성하여 자율 시스템의 다른 EIGRP 라우터가 threat defense 디바이스의 연결된 네트워크에 대한 경로를 가져오도록 할 수 있습니다. 스텁 라우팅을 위한 EIGRP 프로세스 구성, 420 페이지의 내용을 참조하십시오.

- 기본 설정은 대부분의 네트워크에서 작동하므로 자율 시스템의 다른 EIGRP 라우터에서 조정한 경우에만 조정합니다. 자율 시스템 번호를 구성하고 라우팅할 네트워크를 지정하기만 하면 완전한 기능의 EIGRP 프로세스를 수행할 수 있습니다.
- 라우터를 식별하기 위해 안정적인 주소를 사용하도록 라우터 ID를 구성합니다. 이렇게 하면 라우팅 문제를 보다 쉽게 트러블슈팅할 수 있습니다. EIGRP 고급 설정 구성, 422 페이지의 내용을 참조하십시오.
- 라우팅 루프를 생성하지 않고 네트워크에 어떤 이점을 제공할 것으로 판단하지 않는 한 자동 경로 요약(**auto-summary** 명령)을 활성화하지 마십시오. 네트워크에서 자동 요약이 작동하는지 여부를 확인하는 방법은 이 문서의 범위를 벗어납니다.

EIGRP 소개

EIGRP(Enhanced Interior Gateway Routing Protocol)는 하이브리드 동적 거리 벡터 및 링크 상태 내부 게이트웨이 라우팅 프로토콜입니다. EIGRP는 동일한 자율 시스템 내에서 라우터로 라우팅 업데이트를 전송합니다. 일반적으로 EIGRP는 멀티캐스트 업데이트를 사용하여 네이버 라우터를 검색하지만, 멀티캐스트 경계 외부에 있는 정적 네이버를 구성할 수 있으며 이러한 정적 네이버는 유니캐스트 업데이트를 가져옵니다.

EIGRP의 통합 기술은 DUAL(Diffusing Update Algorithm)이라는 알고리즘을 기반으로 합니다. 이 알고리즘은 경로 계산 전반에 걸쳐 모든 순간에 루프 프리(loop-free) 작동을 보장하며 토폴로지 변경과 관련된 모든 디바이스의 동기화를 허용합니다. 토폴로지 변경의 영향을 받지 않는 디바이스는 재계산에 포함되지 않습니다.

라우팅 메트릭을 조정하여 경로 선택 방법을 제어할 수 있습니다. 다음 주제에서는 이러한 고급 개념에 대한 몇 가지 배경 정보를 제공합니다.

참고 이러한 메트릭을 조정하는 경우 자율 시스템 내의 모든 라우터를 동일하게 조정해야 합니다. 그렇지 않으면 라우팅 루프가 발생할 수 있습니다.

이중 FSM(Finite State Machine)

이중 FSM(Finite State Mchine)은 모든 경로 계산을 위한 결정 프로세스를 구현합니다. 모든 네이버가 알리는 모든 경로를 추적합니다. DUAL은 효율적인 루프 없는 경로를 선택하기 위해 거리 정보(메트릭이라고 함)를 사용합니다.

DUAL은 실행 가능한 successor를 기반으로 라우팅 테이블에 삽입할 경로를 선택합니다. successor는 라우팅 루프의 일부가 아님을 보증하는 대상에 대한 최저 비용 경로를 가진 네이버 라우터(패킷 전달에 사용됨)입니다.

토폴로지 변경이 발생하면 DUAL은 실행 가능한 successor를 테스트합니다. 실행 가능한 successor가 있는 경우 DUAL은 불필요한 재계산을 방지하기 위해 실행 가능한 모든 successor를 사용합니다.

실행 가능한 successor가 없고 대상을 광고하는 네이버만 있는 경우에는 새 successor를 확인하려면 재계산을 수행해야 합니다. 경로를 재계산하는 데 필요한 시간은 통합 시간에 영향을 줍니다.

EIGRP 메트릭 가중치

EIGRP는 라우팅 및 메트릭 계산에서 K 값이라고 하는 메트릭 가중치를 사용합니다. EIGRP 메트릭 기본값은 대부분의 네트워크에서 최적의 성능을 제공하도록 신중하게 선택되었습니다.

IOS 라우터와 달리 threat defense 디바이스에서 실행 중인 EIGRP에 대해 이러한 기본 K 값을 조정할 수 없습니다. 자율 네트워크 내 모든 시스템에서 동일한 K 값을 사용해야 하므로 threat defense 디바이스가 포함된 자율 시스템 내의 라우터에서는 값을 변경해서는 안 됩니다.

K 값이 사용되는 방식에 대한 설명은 EIGRP 비용 메트릭, 417 페이지를 참조하십시오.

EIGRP 비용 메트릭

EIGRP는 링크 특성 외에 메트릭 가중치(K 값)를 사용하여 복합 비용 메트릭을 계산합니다. 링크 특성의 변경으로 인한 네트워크 변동을 방지하기 위해 이 계산에 사용된 일부 값을 조정할 수 있습니다.

실제 계산은 5개의 K 값(승수)과 5개의 벡터 특성을 사용하여 매우 복잡합니다. 그러나 3개의 K 값은 기본적으로 0이며, K 값의 기본값을 변경할 수 없으므로 실제 계산이 크게 간소화됩니다.

비용 메트릭 = 256 * (대역폭 + 지연)

변경할 수 있는 값은 EIGRP 프로세스에서 또는 EIGRP 프로세스로 재배포되는 경로의 대역폭 및 지연 값입니다. 특히 **default-metric** 명령(재배포된 모든 경로 유형에 대한 기본값을 설정) 또는 **redistribute metric** 명령(특정 경로 유형에 대한 메트릭을 설정)에서 이러한 값을 조정할 수 있습니다. 다음에 유의하십시오.

- 대역폭은 경로의 최소 대역폭(초당 킬로 비트)입니다. 초당 1~4294967295 킬로바이트가 될 수 있습니다. 공식의 대역폭은 다음 공식에 따라 조정되고 전환됩니다.

  $(10^7$/최소 대역폭(초당 킬로 비트))

- 지연은 10마이크로초 단위의 경로 지연입니다.

threat defense에서 사용되지 않는 다른 특성으로는 지연 안정성, 경로의 유효로드 및 경로의 최소 MTU(최대 전송 단위)가 있습니다. 값이 사용되지 않더라도 이러한 명령을 조정하는 경우에는 값을 구성해야 합니다.

EIGRP가 비용 메트릭을 계산하는 방법에 대한 자세한 내용은 *IP Routing: EIGRP Configuration Guide(IP 라우팅: EIGRP 컨피그레이션 가이드)*를 참조하십시오. 예를 들어 https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_eigrp/configuration/xe-16-7/ire-xe-16-8-book/ire-enhanced-igrp.html입니다.

EIGRP를 위한 지침

IPv6 지침

IPv6를 지원하지 않습니다.

추가 지침

- 최대 하나의 EIGRP 프로세스가 지원됩니다.
- EIGRP 프로세스의 자율 시스템 번호는 변경할 수 없습니다. 대신, 프로세스를 삭제하고 변경 사항을 구축한 다음 새로운 자율 시스템 번호를 사용하여 새 프로세스를 구성합니다.
- BVI(Bridge Virtual Interface)에 속하는 EIGRP 프로세스에 네트워크를 포함할 수 없습니다.
- 구성 변경 사항이 적용될 때마다 EIGRP 인접성 플랩이 발생하며, 이로 인해 특히 배포 목록, 오프셋 목록 및 요약 변경 사항에서 네이버로부터 전송 또는 수신된 라우팅 정보가 수정됩니다. 라우터를 동기화한 후 EIGRP는 네이버 간에 인접성을 재설정합니다. 인접성이 해제되고 재설정되면 네이버 간에 확인한 모든 경로가 지워지고, 새 배포 목록을 통해 네이버 간의 전체 동기화가 새로 수행됩니다.

코어 EIGRP 프로세스 구성

다음 주제에서는 EIGRP를 가동하고 디바이스에서 실행하는 방법을 설명합니다. 전체 라우팅 프로세스를 구성하거나, 자율 네트워크에 EIGRP 라우터로 완전히 참여해서는 안되는 시스템에 대한 스텁 프로세스로 구성할 수 있습니다.

전체 라우팅을 위한 EIGRP 프로세스 구성

하나의 EIGRP 프로세스를 구성할 수 있습니다. 여러 가상 라우터를 구성하는 경우 EIGRP는 전역 가상 라우터에서만 지원됩니다.

다음 절차에서는 EIGRP 라우팅에 대한 모든 기본값을 사용하여 네트워크 집합에 대한 기본 EIGRP 라우팅을 설정합니다. 이 절차를 완료하면 디바이스에서 EIGRP를 활성화할 수 있습니다. 필요에 따라 다른 절차를 완료하여 EIGRP 프로세스를 미세 조정할 수 있습니다.

시작하기 전에

네트워크에서 EIGRP에 사용할 자율 시스템 번호를 확인합니다.

EIGRP 자율 시스템 내에서 라우팅할 각 네트워크를 정의하는 네트워크 개체를 생성합니다. 예를 들어 192.168.1.0/24 및 192.168.2.0/24 네트워크에 EIGRP를 사용하려는 경우 각 네트워크에 하나씩 두 개의 네트워크 개체를 생성합니다.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음, **Routing(**라우팅**)** 요약을 클릭합니다.

단계 **2** 가상 라우터를 활성화한 경우 전역 가상 라우터의 보기 아이콘( )을 클릭합니다.

단계 **3** **EIGRP** 탭을 클릭합니다.

단계 **4** 다음 중 하나를 수행합니다.

- 새 프로세스를 생성하려면 +를 클릭하거나 **Create EIGRP Object(EIGRP** 개체 생성**)** 버튼을 클릭합니다.
- 수정할 개체의 수정 아이콘( )을 클릭합니다. 개체를 수정할 때는 직접 구성하지 않은 줄이 표시될 수도 있습니다. 이러한 줄은 구성 중인 기본값을 표시하기 위해 노출됩니다.

프로세스가 더 이상 필요하지 않은 경우 해당 개체의 휴지통 아이콘을 클릭하여 프로세스를 삭제합니다.

단계 **5** 스마트 CLI 개체의 **Name(**이름**)** 및 설명(선택 사항)을 입력합니다.

단계 **6** 기본 프로세스 속성을 구성합니다.

router eigrp *autonomous-system*

변수를 클릭하고 1~65535 범위의 숫자를 입력합니다. 이 디바이스와 동일한 라우팅 도메인 내에서 작동해야 하는 네트워크의 다른 라우터에서 사용되는 것과 동일한 자율 시스템 번호를 사용합니다.

단계 **7** EIGRP 자동 시스템 내에서 라우팅해야 하는 네트워크 및 인터페이스를 구성합니다.

a) 개체 본문 위에 있는 **Show Disabled(**비활성화된 항목 표시**)** 링크를 클릭하여 가능한 다른 모든 구성 줄을 추가합니다.

b) **network** *network-object* 라인의 왼쪽에 있는 +를 클릭합니다.

c) **network** 명령에서 변수를 클릭하고 이 자율 시스템에 포함되어야 하는 네트워크를 정의하는 개체를 선택합니다.

일반적으로 이는 직접 연결된 네트워크입니다. 예를 들어, 내부 인터페이스의 IP 주소가 192.168.1.1/24인 경우 이 명령에 대해 연결된 네트워크 개체에는 192.168.1.0/24가 포함됩니다. 개체가 아직 없는 경우 **Create New Network(**새 네트워크 생성**)**를 클릭하여 바로 생성합니다.

정의된 네트워크 안에 해당하는 직접 연결된 네트워크와 정적 네트워크를 프로세스에서 알립니다. 또한 정의된 네트워크에 해당하는 IP 주소를 가진 인터페이스만 EIGRP 라우팅 프로세스에 참여합니다.

EIGRP 라우팅에 참여를 원하지 않지만 알리고 싶은 네트워크에 연결된 인터페이스가 있다면 EIGRP 패시브 라우팅 인터페이스 구성, 425 페이지를 참조하십시오.

d) 라우팅할 추가 네트워크가 있는 경우 **...** > **Duplicate(**중복**)(network** 명령 왼쪽**)**를 클릭하여 새 네트워크를 추가합니다. 라우팅할 모든 네트워크를 구성할 때까지 **network** 라인을 계속 추가합니다.

단계 **8** (선택 사항). 필요한 경우 초기에 비활성화된 다른 명령의 설정을 조정합니다. EIGRP 프로세스 맞춤화, 422 페이지의 내용을 참조하십시오.

단계 **9** **OK(**확인**)**를 클릭합니다.

스텁 라우팅을 위한 **EIGRP** 프로세스 구성

디바이스를 EIGRP 스텁 라우터로 구성할 수 있습니다. 스텁 라우팅은 시스템에 대한 메모리 및 처리 능력 요구 사항을 낮춥니다. 스텁 라우터인 시스템은 모든 로컬이 아닌 트래픽을 배포 라우터로 전달하기 때문에 전체 EIGRP 라우팅 테이블을 유지할 필요가 없습니다. 일반적으로 배포 라우터는 기본 경로 외에 아무것도 stub 라우터로 보낼 필요가 없습니다.

지정된 경로만 stub 라우터에서 배포 라우터로 전파됩니다. 스텁 라우터인 시스템은 요약, 연결 경로, 재배포된 정적 경로, 외부 경로, 내부 경로에 대한 모든 쿼리에 "액세스 불가" 메시지로 응답합니다. 시스템에서 모든 인접한 라우터에 특별한 피어 정보 패킷을 보내 자신의 상태가 스텁 라우터임을 알립니다. stub 상태를 알려주는 패킷 정보를 수신하는 모든 네이버는 경로에 대해 일체 stub 라우터에 쿼리하지 않고 stub 피어가 있는 라우터는 피어에 쿼리하지 않습니다. stub 라우터는 올바른 업데이트를 모든 피어에 전송하기 위해 배포 라우터에 의지합니다.

시작하기 전에

네트워크에서 EIGRP에 사용할 자율 시스템 번호를 확인합니다.

EIGRP 자율 시스템 내에서 라우팅할 각 네트워크를 정의하는 네트워크 개체를 생성합니다. 예를 들어 192.168.1.0/24 및 192.168.2.0/24 네트워크에 EIGRP를 사용하려는 경우 각 네트워크에 하나씩 두 개의 네트워크 개체를 생성합니다.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음, **Routing(**라우팅**)** 요약을 클릭합니다.

단계 **2** 가상 라우터를 활성화한 경우 전역 가상 라우터의 보기 아이콘( )을 클릭합니다.

단계 **3** **EIGRP** 탭을 클릭합니다.

단계 **4** 다음 중 하나를 수행합니다.

- 새 프로세스를 생성하려면 +를 클릭하거나 **Create EIGRP Object(EIGRP** 개체 생성**)** 버튼을 클릭합니다.
- 수정할 개체의 수정 아이콘( )을 클릭합니다. 개체를 수정할 때는 직접 구성하지 않은 줄이 표시될 수도 있습니다. 이러한 줄은 구성 중인 기본값을 표시하기 위해 노출됩니다.

프로세스가 더 이상 필요하지 않은 경우 해당 개체의 휴지통 아이콘을 클릭하여 프로세스를 삭제합니다.

단계 **5** 스마트 CLI 개체의 **Name(**이름**)** 및 설명(선택 사항)을 입력합니다.

단계 **6** 기본 프로세스 속성을 구성합니다.

router eigrp *autonomous-system*

변수를 클릭하고 1~65535 범위의 숫자를 입력합니다. 이 디바이스와 동일한 라우팅 도메인 내에서 작동해야 하는 네트워크의 다른 라우터에서 사용되는 것과 동일한 자율 시스템 번호를 사용합니다.

단계 **7** EIGRP 자동 시스템 내에서 라우팅해야 하는 네트워크 및 인터페이스를 구성합니다.

a) 개체 본문 위에 있는 **Show Disabled(**비활성화된 항목 표시**)** 링크를 클릭하여 가능한 다른 모든 구성 줄을 추가합니다.

b) **network** *network-object* 라인의 왼쪽에 있는 +를 클릭합니다.

c) **network** 명령에서 변수를 클릭하고 이 자율 시스템에 포함되어야 하는 네트워크를 정의하는 개체를 선택합니다.

일반적으로 이는 직접 연결된 네트워크입니다. 예를 들어, 내부 인터페이스의 IP 주소가 192.168.1.1/24인 경우 이 명령에 대해 연결된 네트워크 개체에는 192.168.1.0/24가 포함됩니다. 개체가 아직 없는 경우 **Create New Network(**새 네트워크 생성**)**를 클릭하여 바로 생성합니다.

정의된 네트워크 안에 해당하는 직접 연결된 네트워크와 정적 네트워크를 프로세스에서 알립니다. 또한 정의된 네트워크에 해당하는 IP 주소를 가진 인터페이스만 EIGRP 라우팅 프로세스에 참여합니다.

EIGRP 라우팅에 참여를 원하지 않지만 알리고 싶은 네트워크에 연결된 인터페이스가 있다면 EIGRP 패시브 라우팅 인터페이스 구성, 425 페이지를 참조하십시오.

d) 라우팅할 추가 네트워크가 있는 경우 **...** > **Duplicate(**중복**)(network** 명령 왼쪽)를 클릭하여 새 네트워크를 추가합니다. 라우팅할 모든 네트워크를 구성할 때까지 **network** 라인을 계속 추가합니다.

단계 **8** 스텁 설정을 구성합니다.

a) **setup eigrp** *configuration* 라인 왼쪽의 +를 클릭합니다.

b) 변수를 클릭하고 **advanced**를 선택합니다.

c) **setup eigrp stub** *stub-options* 명령의 왼쪽에 있는 +를 클릭합니다.

d) 디바이스가 자율 시스템의 다른 라우터와 경로를 공유하는 것을 제한하여 EIGRP 네이버 라우터에서만 업데이트를 수신하도록 *stub-options*를 클릭하고 **receive**를 선택합니다. 그런 다음, 다음 명령을 구성합니다.

eigrp stub *stub-parameters*

변수를 클릭하고 **receive-only**를 선택합니다.

e) 디바이스가 EIGRP 네이버 라우터에 대한 경로를 알릴 수 있도록 허용하려면 *stub-options*를 클릭하고 **other**를 선택합니다. 그런 다음, 다음 명령을 구성하여 알려야 할 경로 유형을 선택합니다.

eigrp stub *connected-parameter redistributed-parameter static-parameter summary-parameter*

변수를 클릭하여 선택합니다. 하나 이상의 경로 유형을 선택해야 하지만 모두 또는 임의의 조합을 선택할 수 있습니다.

- *connected-parameter*. 연결된 경로를 알리려면 **connected**를 선택합니다. 연결된 경로가 **network** 명령문으로 적용되지 않는 경우 EIGRP 프로세스에서 연결된 경로에 대한 재배포를 구성해야 할 수 있습니다.
- *redistributed-parameter*. 다른 라우팅 프로토콜에서 EIGRP 라우팅 프로세스로 재배포된 경로를 알리려면 **redistributed**를 선택합니다.

- *static-parameter*. 정적 경로를 알리려면 **static**을 선택합니다. 또한 **configure redistribution** 명령을 활성화하고 정적 경로의 재배포를 구성해야 합니다.
- *summary-parameter*. 요약 경로를 알리려면 **summary**를 선택합니다.

단계 **9** (선택 사항). 필요한 경우 초기에 비활성화된 다른 명령의 설정을 조정합니다. EIGRP 프로세스 맞춤화, 422 페이지의 내용을 참조하십시오.

단계 **10** **OK(**확인**)**를 클릭합니다.

EIGRP 프로세스 맞춤화

EIGRP에는 기본값이 설정된 여러 옵션이 포함되어 있습니다. 이러한 값은 여러 네트워크에서 원활하게 작동합니다. 그러나 필요한 정확한 동작을 얻기 위해 하나 이상의 설정을 조정해야 할 수 있습니다. 다음 주제에서는 EIGRP 라우팅 프로세스를 맞춤화할 수 있는 다양한 방법에 대해 설명합니다.

EIGRP 고급 설정 구성

자동 경로 요약, 거리 메트릭, 로깅 및 링크 상태 알림과 기타 라우팅 업데이트 전송에 사용되는 라우터 ID 등을 비롯한 EIGRP 프로세스의 전반적인 동작을 제어하는 여러 가지 설정을 구성할 수 있습니다. 이러한 많은 설정에는 대부분의 네트워크에 적합한 기본값이 설정되어 있습니다.

시작하기 전에

이 절차에서는 EIGRP 프로세스를 이미 구성했다고 가정합니다. 코어 EIGRP 프로세스 구성, 418 페이지를 참조하십시오.

프로세스를 생성하면 특정 고급 옵션이 기본적으로 활성화됩니다. EIGRP 개체를 수정하면 이러한 활성화된 옵션이 표시됩니다.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음, **Routing(**라우팅**)** 요약을 클릭합니다.

단계 **2** 가상 라우터를 활성화한 경우 전역 가상 라우터의 보기 아이콘()을 클릭합니다.

단계 **3** **EIGRP** 탭을 클릭합니다.

단계 **4** EIGRP 개체의 수정 아이콘()을 클릭합니다.

개체를 수정할 때는 직접 구성하지 않은 줄이 표시될 수도 있습니다. 이러한 줄은 구성 중인 기본값을 표시하기 위해 노출됩니다.

단계 **5** 개체 본문 위에 있는 **Show Disabled(**비활성화된 항목 표시**)**를 클릭하여 가능한 다른 모든 컨피그레이션 라인을 추가합니다.

단계 **6** **setup eigrp** *configuration* 라인은 이미 **setup eigrp advanced**로 활성화되어 있어야 합니다. 그렇지 않은 경우, 라인 왼쪽의 +를 클릭하여 활성화한 다음, 변수를 클릭하고 **advanced**를 선택합니다.

단계 **7** (선택 사항, 권장하지 않음) 네트워크 번호 경계의 경로를 자동으로 요약하려면 **auto-summary** 명령 옆의 +를 클릭합니다.

불연속 네트워크를 가진 경우 라우팅 문제가 발생할 수 있습니다.

예를 들어 네트워크 172.16.1.0, 172.16.2.0 및 172.16.3.0이 연결된 라우터가 있고 이러한 네트워크가 모두 EIGRP에 참여하는 경우 EIGRP 라우팅 프로세스에서 해당 경로에 대해 요약 주소 172.16.0.0이 생성됩니다. 네트워크 172.16.10.0 및 172.16.11.0가 있는 네트워크에 라우터가 추가되고 해당 네트워크가 EIGRP에 참여할 경우에도 172.16.0.0으로 요약됩니다. 따라서 경로를 자동으로 요약하면 잘못된 라우터로 트래픽이 라우팅됩니다.

단계 **8** (선택 사항, 권장함) 라우터 ID를 구성합니다.

+를 클릭하여 **router-id** 명령을 활성화한 다음, 변수를 클릭하고 이 디바이스에서 라우터 업데이트를 전송할 때 사용해야 할 IPv4 주소를 입력합니다. EIGRP 자율 시스템에서는 두 개의 라우터가 동일한 라우터 ID를 가질 수 없으므로 이는 시스템에서 고유해야 합니다.

프로세스에 대한 라우터 ID를 명시적으로 지정하지 않으면 시스템에서는 활성 인터페이스에 할당된 최상위 IP 주소를 사용합니다. 따라서 선택한 인터페이스를 비활성화하거나 해당 주소를 변경할 경우 라우터 ID가 변경될 수 있습니다. 라우터 ID를 명시적으로 할당하면 프로세스의 일관성을 보장할 수 있습니다.

단계 **9** (선택 사항). 내부 및 외부 EIGRP 경로에 대한 관리 거리를 구성합니다.

다음 명령은 프로세스를 구성할 때 기본적으로 활성화되어 있습니다. 새 개체를 구성하는 경우 +를 클릭해야 명령을 활성화할 수 있습니다.

distance eigrp 90 170

모든 라우팅 프로토콜은 다른 라우팅 프로토콜과 구별되는 알고리즘을 기반으로 한 메트릭을 갖기 때문에 서로 다른 라우팅 프로토콜에서 생성된 동일 대상의 경로 2개 중에서 최적의 경로를 결정하는 것이 가능하지 않을 수도 있습니다. 관리 영역은 서로 다른 두 라우팅 프로토콜로부터 동일한 대상의 서로 다른 경로가 2개 이상 나올 경우 최적의 경로를 선택하기 위해 시스템에서 사용하는 경로 매개변수입니다.

EIGRP의 관리 거리는 1~255입니다. 이러한 숫자는 시스템에서 최상의 경로를 선택할 때 다른 라우팅 프로세스에 할당된 관리 값을 기준으로 합니다. 일반적으로 이 값이 클수록 신뢰 등급이 낮습니다. 기본값은 대부분의 네트워크에서 작동합니다. EIGRP 경로를 우선적으로 사용하도록 하거나 EIGRP 경로 사용 가능성을 줄이려는 경우에는 기본값을 조정합니다.

숫자는 다음을 의미합니다.

- 첫 번째 값(90): 내부 거리. EIGRP 내부 경로에 대한 AD(Administrative Distance)입니다. 내부 경로는 동일한 자율 시스템 내의 다른 엔티티로부터 학습된 것입니다.
- 두 번째 값(170): 외부 거리. EIGRP 외부 경로에 대한 AD(Administrative Distance)입니다. 외부 경로는 자율 시스템의 외부에 있는 네이버로부터 최상의 경로가 학습된 경로입니다.

단계 **10** **default-metric** 명령은 다른 라우팅 프로세스에서 경로를 재배포할 때 사용됩니다. 또한 재배포를 구성하는 경우에만 이를 구성하십시오. 자세한 내용은 EIGRP 경로 재배포 구성, 430 페이지를 참조해 주십시오.

단계 **11** 네이버 로깅을 구성합니다.

다음 명령은 프로세스를 구성할 때 기본적으로 활성화되어 있습니다. 새 개체를 구성하는 경우 +를 클릭해야 명령을 활성화할 수 있습니다. 로깅을 비활성화하려면 -를 클릭하여 명령을 비활성화합니다.

- **eigrp log-neighbor-changes** EIGRP 네이버 인접성 변경 사항의 로깅을 활성화합니다.
- **eigrp log-neighbor-warnings 10** EIGRP 네이버 경고 메시지의 로깅을 비활성화합니다. 이 숫자는 반복되는 네이버 경고 메시지 간의 시간 간격(1~65535초)입니다. 반복 경고가 이 간격 중 발생할 경우 로깅되지 않습니다.

단계 **12** **setup stub** 명령을 구성하려면 스텁 라우팅을 위한 EIGRP 프로세스 구성, 420 페이지를 참조하십시오.

단계 **13** **OK(**확인**)**를 클릭합니다.

EIGRP에서 알릴 네트워크 구성

network 명령을 사용하여 EIGRP 라우팅에 포함되어야 하는 네트워크 및 인터페이스를 식별합니다. 인터페이스가 EIGRP 라우팅에 참여하려면 네트워크 엔트리에 의해 정의된 주소 범위에 해당해야 합니다. 직접 연결 및 고정 네트워크를 알리려면 네트워크 엔트리 범위에 해당해야 합니다.

시작하기 전에

이 절차에서는 EIGRP 프로세스를 이미 구성했다고 가정합니다. 코어 EIGRP 프로세스 구성, 418 페이지를 참조하십시오.

광고할 네트워크를 정의하는 네트워크 개체를 생성합니다.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음, **Routing(**라우팅**)** 요약을 클릭합니다.

단계 **2** 가상 라우터를 활성화한 경우 전역 가상 라우터의 보기 아이콘( )을 클릭합니다.

단계 **3** **EIGRP** 탭을 클릭합니다.

단계 **4** EIGRP 개체의 수정 아이콘( )을 클릭합니다.

개체를 수정할 때는 직접 구성하지 않은 줄이 표시될 수도 있습니다. 이러한 줄은 구성 중인 기본값을 표시하기 위해 노출됩니다.

단계 **5** 개체 본문 위에 있는 **Show Disabled(**비활성화된 항목 표시**)**를 클릭하여 가능한 다른 모든 컨피그레이션 라인을 추가합니다.

단계 **6** 이미 네트워크를 구성했다고 가정하고, **...** > **Duplicate(**중복**)(network** 라인 옆)를 클릭하여 빈 명령을 새로 만듭니다.

아직 네트워크를 정의하지 않은 경우, 빈 **network** *network-object* 라인 옆의 +를 클릭합니다.

단계 **7** **network** 명령에서 변수를 클릭하고 이 자율 시스템에 포함되어야 하는 네트워크를 정의하는 개체를 선택합니다.

일반적으로 이는 직접 연결된 네트워크입니다. 예를 들어, 내부 인터페이스의 IP 주소가 192.168.1.1/24인 경우 이 명령에 대해 연결된 네트워크 개체에는 192.168.1.0/24가 포함됩니다. 개체가 아직 없는 경우 **Create New Network(**새 네트워크 생성**)**를 클릭하여 바로 생성합니다.

정의된 네트워크 안에 해당하는 직접 연결된 네트워크와 정적 네트워크를 프로세스에서 알립니다. 또한 정의된 네트워크에 해당하는 IP 주소를 가진 인터페이스만 EIGRP 라우팅 프로세스에 참여합니다.

EIGRP 라우팅에 참여를 원하지 않지만 알리고 싶은 네트워크에 연결된 인터페이스가 있다면 EIGRP 패시브 라우팅 인터페이스 구성, 425 페이지를 참조하십시오.

단계 **8** 라우팅할 추가 네트워크가 있는 경우 **...** > **Duplicate(**중복**)(network** 명령 왼쪽)를 클릭하여 새 네트워크를 추가합니다. 라우팅할 모든 네트워크를 구성할 때까지 **network** 라인을 계속 추가합니다.

단계 **9** **OK(**확인**)**를 클릭합니다.

EIGRP 패시브 라우팅 인터페이스 구성

EIGRP 라우팅에 참여하는 것은 원치 않지만, 알리고 싶은 네트워크에 연결된 인터페이스가 있는 경우 이 인터페이스가 연결된 네트워크를 포함하는 **network** 명령을 구성하고 **passive-interface** 명령을 사용하여 이 인터페이스가 EIGRP 업데이트를 보내거나 받지 않게 할 수 있습니다.

기본적으로 시스템은 EIGRP 업데이트를 전송 및 수신하는 모든 인터페이스를 액티브로 설정하는 **no passive-interface default** 명령을 활성화합니다.

다음 절차에서는 인터페이스를 패시브로 변경하는 방법을 설명합니다.

시작하기 전에

이 절차에서는 EIGRP 프로세스를 이미 구성했다고 가정합니다. 코어 EIGRP 프로세스 구성, 418 페이지를 참조하십시오.

프로세스를 생성할 때 **network** 명령을 추가하여 EIGRP를 사용하여 라우팅해야 하는 네트워크를 나타냅니다. 라우팅할 추가 네트워크를 구성하려면 EIGRP에서 알릴 네트워크 구성, 424 페이지를 참조하십시오.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음, **Routing(**라우팅**)** 요약을 클릭합니다.

단계 **2** 가상 라우터를 활성화한 경우 전역 가상 라우터의 보기 아이콘()을 클릭합니다.

단계 **3** **EIGRP** 탭을 클릭합니다.

단계 **4** EIGRP 개체의 수정 아이콘( )을 클릭합니다.

개체를 수정할 때는 직접 구성하지 않은 줄이 표시될 수도 있습니다. 이러한 줄은 구성 중인 기본값을 표시하기 위해 노출됩니다.

단계 **5** 개체 본문 위에 있는 **Show Disabled(**비활성화된 항목 표시**)**를 클릭하여 가능한 다른 모든 컨피그레이션 라인을 추가합니다.

단계 **6** 개체를 수정하는 경우 **configure interface passive** 명령 및 해당 하위 항목 **no passive-interface default**가 활성화됩니다.

새 개체의 경우 **+**를 클릭하여 **configure routing-interface** *parameters* 명령을 활성화합니다.

단계 **7** 인터페이스를 기본적으로 액티브 상태로 구성한 다음, 선택적으로 인터페이스를 패시브 상태로 설정하려면 다음을 수행합니다.

a) **configure routing-interface** 명령에서 변수를 클릭하고 **passive**를 선택합니다.

이 작업은 EIGRP 인터페이스를 기본적으로 액티브로 설정하는 **no passive-interface default** 명령을 활성화합니다.

b) **passive-interface** 인터페이스 명령 옆의 **+**를 클릭하고 변수를 클릭한 다음 EIGRP 라우팅 업데이트에 참여하지 않아야 하고 패시브 상태여야 하는 인터페이스를 선택합니다.

c) 추가 패시브 인터페이스를 구성해야 하는 경우 **...** > **Duplicate(**중복**)(passive-interface** *interface* 명령 옆**)**를 클릭합니다. 패시브 상태여야 하는 각 인터페이스에 대해 **passive-interface** 명령이 표시될 때까지 계속 진행합니다.

단계 **8** 인터페이스를 기본적으로 패시브 상태로 구성한 다음, 선택적으로 인터페이스를 액티브 상태로 설정하려면 다음을 수행합니다.

a) **configure routing-interface** 명령에서 변수를 클릭하고 **active**를 선택합니다.

이 작업은 기본적으로 EIGRP 인터페이스를 패시브 상태로 만드는 **passive-interface default** 명령을 활성화합니다.

b) **no passive-interface** *interface* 명령 옆의 **+**를 클릭하고 변수를 클릭한 다음 EIGRP 라우팅 업데이트에 액티브 상태로 참여해야 하는 인터페이스를 선택합니다.

c) 추가 액티브 인터페이스를 구성해야 하는 경우 **...** > **Duplicate(**중복**)(no passive-interface** *interface* 명령 옆**)**를 클릭합니다. 액티브 상태여야 하는 각 인터페이스에 대해 **no passive-interface** 명령이 표시될 때까지 계속 진행합니다.

단계 **9** 인터페이스를 기본 동작(패시브 또는 액티브)으로 다시 전환하려면 해당 인터페이스를 패시브 또는 액티브로 설정하는 명령 옆의 **-**를 클릭합니다. 이렇게 하면 예외가 삭제되고 사용자가 설정한 기본 작업에 따라 인터페이스가 작동합니다.

단계 **10** **OK(**확인**)**를 클릭합니다.

정적 EIGRP 네이버 구성

EIGRP hello 패킷은 멀티캐스트 패킷으로 전송됩니다. EIGRP 네이버가 VPN 터널과 같이 브로드캐스트가 아닌 네트워크에 위치한 경우 해당 네이버를 수동으로 정의해야 합니다. EIGRP 네이버를 수동으로 정의할 경우 hello 패킷은 유니캐스트 메시지로 해당 네이버에 전송됩니다.

이러한 라우터는 스스로 인접성을 형성할 수 있으므로, 일반 브로드캐스트 네트워크에 있는 정적 네이버를 정의하지 않아도 됩니다.

시작하기 전에

이 절차에서는 EIGRP 프로세스를 이미 구성했다고 가정합니다. 코어 EIGRP 프로세스 구성, 418 페이지를 참조하십시오.

시스템이 네이버에 연결해야 할 때 통과하는 인터페이스를 결정합니다.

EIGRP 고급 설정 구성, 422 페이지에서 설명한대로 네이버에 대한 로깅 설정을 구성할 수도 있습니다.

프로시저

단계 **1** 디바이스를 클릭한 다음, **Routing(**라우팅**)** 요약을 클릭합니다.

단계 **2** 가상 라우터를 활성화한 경우 전역 가상 라우터의 보기 아이콘()을 클릭합니다.

단계 **3** **EIGRP** 탭을 클릭합니다.

단계 **4** EIGRP 개체의 수정 아이콘()을 클릭합니다.

개체를 수정할 때는 직접 구성하지 않은 줄이 표시될 수도 있습니다. 이러한 줄은 구성 중인 기본값을 표시하기 위해 노출됩니다.

단계 **5** **Show Disabled(**비활성화된 항목 표시**)**를 클릭하여 모든 명령을 표시한 다음, **+**를 클릭하여 **neighbor** 명령을 활성화합니다.

단계 **6** 네이버 주소를 구성합니다.

neighbor *ip-address* **interface** *interface*

- *ip-address*를 클릭하고 네이버 라우터의 IP 주소를 입력합니다.
- *interface*를 클릭하고 시스템이 라우터에 연결할 수 있을 때 통과하는 인터페이스를 선택합니다.

단계 **7** 필요한 경우 네이버 라우터에 대한 정적 경로를 구성합니다.

라우터의 IP 주소가 선택한 인터페이스와 같은 네트워크에 있는 경우, 정적 경로는 필요하지 않습니다. 예를 들어 IP 주소가 10.100.10.1/24이고, 네이버 주소가 10.100.10.2/24인 인터페이스를 선택할 경우 정적 경로가 필요하지 않습니다.

단계 **8** **...** > **Duplicate(**중복**)(neighbor** 명령 옆**)**를 클릭하여 다른 정적 네이버를 정의할 수 있습니다. 필요한 개수만큼 정의합니다.

단계 **9** **OK(**확인**)**를 클릭합니다.

제어 EIGRP 후보 기본 경로 전파

EIGRP 프로세스에서 기본 경로 후보의 전송 또는 수신을 제어할 수 있습니다. 기본적으로 모든 후보 경로는 경로 필터링 및 재배포 설정에 따라 알려지거나 수락됩니다.

기본 경로의 전송 또는 수신을 직접 끌 수는 없습니다. EIGRP에서 기본 경로 전파를 방지하려면 any-ipv4 네트워크를 거부하는 표준 ACL을 사용하여 이러한 명령을 구성하십시오.

시작하기 전에

이 절차에서는 EIGRP 프로세스를 이미 구성했다고 가정합니다. 코어 EIGRP 프로세스 구성, 418 페이지를 참조하십시오.

각 필터 규칙에 필요한 스마트 CLI 표준 액세스 목록 개체를 생성합니다. 거부 액세스 제어 항목(ACE)을 사용하여 항목과 일치하는 경로를 필터링하고, 업데이트해야 하는 경로에 대한 ACE를 허용합니다.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음, **Routing(**라우팅**)** 요약을 클릭합니다.

단계 **2** 가상 라우터를 활성화한 경우 전역 가상 라우터의 보기 아이콘( )을 클릭합니다.

단계 **3** **EIGRP** 탭을 클릭합니다.

단계 **4** EIGRP 개체의 수정 아이콘( )을 클릭합니다.

개체를 수정할 때는 직접 구성하지 않은 줄이 표시될 수도 있습니다. 이러한 줄은 구성 중인 기본값을 표시하기 위해 노출됩니다.

단계 **5** 개체 본문 위에 있는 **Show Disabled(**비활성화된 항목 표시**)**를 클릭하여 가능한 다른 모든 컨피그레이션 라인을 추가합니다.

단계 **6** **+**를 클릭하여 다음 명령 중 하나 또는 둘 다를 활성화합니다.

- 후보 기본 경로의 수신을 제어하기 위한 **default-information in** *acl*.
- 후보 기본 경로의 전송을 제어하기 위한 **default-information out** *acl*.

단계 **7** 변수를 클릭하고 필터를 적용하는 표준 ACL을 선택합니다.

단계 **8** **OK(**확인**)**를 클릭합니다.

EIGRP 필터 규칙 구성

표준 액세스 제어 목록에 정의된 네트워크 접두사를 기준으로 수신 또는 발신 라우팅 업데이트를 필터링할 수 있습니다. 필터링을 사용하면 경로 배포에 대한 제어를 EIGRP 자율 시스템 또는 다른 라우팅 프로세스로의 아웃바운드 제어로 향상할 수 있습니다.

시작하기 전에

이 절차에서는 EIGRP 프로세스를 이미 구성했다고 가정합니다. 코어 EIGRP 프로세스 구성, 418 페이지를 참조하십시오.

각 필터 규칙에 필요한 스마트 CLI 표준 액세스 목록 개체를 생성합니다. 거부 액세스 제어 항목(ACE)을 사용하여 항목과 일치하는 경로를 필터링하고, 업데이트해야 하는 경로에 대한 ACE를 허용합니다.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음, **Routing(**라우팅**)** 요약을 클릭합니다.

단계 **2** 가상 라우터를 활성화한 경우 전역 가상 라우터의 보기 아이콘( )을 클릭합니다.

단계 **3** **EIGRP** 탭을 클릭합니다.

단계 **4** EIGRP 개체의 수정 아이콘( )을 클릭합니다.

개체를 수정할 때는 직접 구성하지 않은 줄이 표시될 수도 있습니다. 이러한 줄은 구성 중인 기본값을 표시하기 위해 노출됩니다.

단계 **5** **Show Disabled(**비활성화된 항목 표시**)**를 클릭하여 모든 명령을 표시한 다음, +를 클릭하여 **configure filter-rules** *direction* 명령을 활성화합니다.

단계 **6** *direction*을 클릭하고 수신 업데이트 필터링에 **in**을 선택하거나, 아웃바운드 업데이트 필터링에 **out**을 선택합니다.

이 작업은 **distribute-list** 명령을 개체에 추가합니다.

단계 **7** 인바운드 필터의 경우, 업데이트를 필터링할 인터페이스를 선택적으로 지정할 수 있습니다. 인터페이스를 지정하지 않으면 인터페이스에서 수신된 모든 업데이트에 필터가 적용됩니다. +를 클릭하여 다음 옵션 중 하나를 활성화합니다.

- **distribute-list** *acl-name* **in**

  표준 ACL 개체를 선택합니다.

- **distribute-list** *acl-name* **in interface** *interface*

  표준 ACL 개체 및 수신 업데이트를 필터링할 인터페이스를 선택합니다.

단계 **8** 아웃바운드 필터의 경우 프로토콜을 선택적으로 지정하여, 라우팅 프로세스 및 업데이트를 필터링할 인터페이스로 생성되는 경로로 필터를 제한할 수 있습니다. +를 클릭하여 다음 옵션 중 하나를 활성화합니다.

- **distribute-list** *acl-name* **out**

  표준 ACL 개체를 선택합니다.

- **distribute-list** *acl-name* **out interface** *interface*

  표준 ACL 개체 및 발신 업데이트를 필터링할 인터페이스를 선택합니다.

- **distribute-list** *acl-name* **out** *protocol*

  표준 ACL 개체 및 다음 경로 유형 중 하나를 선택합니다.

  - **connected**. 시스템의 인터페이스에 직접 연결된 네트워크에 대해 설정된 경로의 경우.
  - **static**. 수동으로 생성한 정적 경로의 경우.
  - **rip**. RIP에서 생성된 경로용.

- **distribute-list** *acl-name* **out** *interface identifier*

  표준 ACL 개체 및 다음 경로 유형 중 하나를 선택합니다.

  - **ospf** *process-id*. OSPF에서 생성된 경로용. identifier를 클릭하고 시스템에 정의된 OSPF 프로세스에 대한 프로세스 ID를 입력합니다.
  - **bgp** *automonous-system*. BGP에서 생성된 경로용. identifier를 클릭하고 시스템에 정의된 BGP 프로세스에 대한 자동 시스템 번호를 입력합니다.

단계 **9** **...** > **Duplicate(**중복**)(configure filter-rules** 명령 옆)를 클릭하여 다른 필터 규칙을 정의할 수 있습니다. 필요한 개수만큼 정의합니다.

단계 **10** **OK(**확인**)**를 클릭합니다.

EIGRP 경로 재배포 구성

다른 라우팅 프로토콜, 연결된 경로, 정적 경로에서 EIGRP 프로세스로 경로를 재배포하는 작업을 제어할 수 있습니다.

시작하기 전에

EIGRP에 재배포를 구성하기 전에, 경로를 재배포할 라우팅 프로세스를 구성하고 변경 사항을 구축하는 것이 좋습니다.

경로 맵을 적용하여 재배포되는 경로를 세부적으로 조정하려면 스마트 CLI 경로 맵 개체를 생성합니다. 경로 맵과 일치하는 경로가 재배포되며, 일치하지 않는 모든 경로는 재배포되지 않습니다.

이 절차에서는 EIGRP 프로세스를 이미 구성했다고 가정합니다. 코어 EIGRP 프로세스 구성, 418 페이지를 참조하십시오.

프로시저

단계 1 **Device(**디바이스**)**를 클릭한 다음, **Routing(**라우팅**)** 요약을 클릭합니다.

단계 2 가상 라우터를 활성화한 경우 전역 가상 라우터의 보기 아이콘( )을 클릭합니다.

단계 3 **EIGRP** 탭을 클릭합니다.

단계 4 EIGRP 개체의 수정 아이콘( )을 클릭합니다.

개체를 수정할 때는 직접 구성하지 않은 줄이 표시될 수도 있습니다. 이러한 줄은 구성 중인 기본값을 표시하기 위해 노출됩니다.

단계 5 **Show Disabled(**비활성화된 항목 표시**)**를 클릭하여 모든 명령을 표시합니다.

단계 6 (선택 사항). +를 클릭하여 **setup eigrp advanced** 명령 그룹에 있는 **default-metric** 명령을 활성화합니다.

경로 유형에 대해 특정 **redistribute metric** 명령을 구성하지 않은 경우 **default-metric** 명령은 재배포된 경로에 사용할 메트릭을 설정합니다.

default-metric *bandwidth-metric delay-metric reliability-metric effective-bandwidth path-MTU*

변수를 클릭하고 다음을 구성합니다. 모든 메트릭 변수를 구성해야 합니다.

- *bandwidth-metric* 변수를 클릭하고 이 경로의 연결 대역폭을 1~4294967295킬로바이트/초로 입력합니다.
- *delay-metric* 변수를 클릭하고 경로의 연결 지연을 0~4294967295 범위에서 10ms 단위로 입력합니다.
- *reliability-metric* 변수를 클릭하고 경로에 대한 EIGRP 신뢰도 메트릭을 0~255 범위에서 입력합니다. 여기서 255는 100% 신뢰도를 나타냅니다. 이 메트릭은 무시되지만 여전히 구성해야 합니다.
- *effective-bandwidth* 변수를 클릭하고 경로에 대한 EIGRP 유효 대역폭을 1~255 범위에서 입력합니다. 여기서 255는 100% 로드되었음을 나타냅니다. 이 메트릭은 무시되지만 여전히 구성해야 합니다.
- *path-MTU* 변수를 클릭하고 경로의 MTU(평균 전송 단위)를 1~65535 범위에서 입력합니다. 이 메트릭은 무시되지만 여전히 구성해야 합니다.

단계 7 +를 클릭하여 **configure redistribution** 명령을 활성화합니다.

단계 8 *protocol* 변수를 클릭하고 경로를 재배포할 소스 프로세스를 선택합니다. **connected** 및 **static** 경로를 재배포하거나 **bgp**, **isis**, **ospf** 또는 **rip**에 의해 생성된 경로를 재배포할 수 있습니다.

단계 9 라우팅 프로세스를 선택할 경우, *identifier* 변수를 클릭하고 필요한 값을 입력합니다.

- **bgp**. 자동 시스템 번호를 입력합니다.
- **ospf**. 프로세스 ID 번호를 입력합니다.
- **connected**, **static**, **isis**, **rip**. **none**을 입력합니다. 다른 값을 입력할 경우 해당 값은 무시됩니다.

단계 **10** (선택 사항, IS-IS 전용.) **redistribute isis route-level** *route-level* 명령에서 변수를 클릭하고 학습한 경로를 IS-IS 영역(**level-1**) 내에서만 재배포할지, IS-IS 영역(**level-2**) 간에 재배포할지, 또는 두 영역 모두(**level-1-2**)에서 재배포할지 선택합니다.

단계 **11** (선택 사항, 모든 프로토콜.) 경로 맵을 기준으로 재배포되는 경로를 세부적으로 조정하려면 **+**를 클릭하여 **redistribute** *route-map* 명령을 활성화하고 변수를 클릭한 후 제한 사항을 정의하는 경로 맵을 선택합니다.

경로 맵을 적용하지 않을 경우, 해당 프로세스에 대한 모든 경로(재배포를 위해 구성된 다른 명령에 적합함)가 재배포됩니다.

단계 **12** (선택 사항, 모든 프로토콜.) 재배포된 경로에 대한 메트릭을 세부적으로 조정하려면 **+**를 클릭하여 다음 명령을 활성화하고 옵션을 구성합니다.

redistribute *protocol* **metric** *bandwidth-metric delay-metric reliability-metric effective-bandwidth path-MTU*

변수를 클릭하고 위의 **default-metric** 명령에서 설명하는 값을 구성합니다. 모든 메트릭 변수를 구성해야 합니다.

단계 **13** (선택 사항, OSPF 전용.) 다음 명령은 OSPF 프로세스에서 경로를 재배포할 때 기본적으로 활성화됩니다. **-**를 클릭하여 원치 않는 명령을 비활성화할 수 있습니다.

이러한 명령은 OSPF 경로가 다른 라우팅 도메인에 재배포되는 기준을 지정합니다.

- **redistribute ospf match external 1**. 자동 시스템의 외부에 있지만, OSPF에 Type 1 외부 경로로서 가져온 경로입니다.
- **redistribute ospf match external 2**. 자동 시스템의 외부에 있지만, OSPF에 Type 2 외부 경로로서 가져온 경로입니다.
- **redistribute ospf match internal**. 특정 자동 시스템의 내부에 있는 경로입니다.
- **redistribute ospf match nssa-external 1**. 자동 시스템의 외부에 있지만, OSPF에 Type 1 외부 경로로서 가져온 경로이며 NSSA(Not-So-Stubby-Area)로만 표시됩니다.
- **redistribute ospf match nssa-external 2**. 자동 시스템의 외부에 있지만, OSPF에 Type 2 외부 경로로서 가져온 경로이며 NSSA(Not-So-Stubby-Area)로만 표시됩니다.

단계 **14** **...** > **Duplicate(**중복**)(configure redistribution** 명령 옆)를 클릭하여 다른 프로토콜에 대한 재배포를 구성할 수 있습니다. 해당 네트워크에 적합한 각 프로토콜에 대해 재배포를 구성합니다.

단계 **15** **OK(**확인**)**를 클릭합니다.

EIGRP 모니터링

다음 명령을 사용하여 EIGRP 라우팅 프로세스를 모니터링할 수 있습니다. 명령 출력의 예와 설명은 명령 참조를 참고하십시오.

- **show eigrp events** [{*start end*} | **type**]

EIGRP 이벤트 로그를 표시합니다.

- **show eigrp interfaces** [*if-name*] [**detail**]

  EIGRP 라우팅에 참여하는 인터페이스를 표시합니다.

- **show eigrp neighbors** [**detail** | **static**] [*if_name*]

  EIGRP 네이버 테이블을 표시합니다.

- **show eigrp topology** [*ip_addr* [*mask*] | **active** | **all-links** | **pending** | **summary** | **zero-successors**]

  EIGRP 토폴로지 테이블을 표시합니다.

- **show eigrp traffic**

  EIGRP 트래픽 통계를 표시합니다.

17 장

BGP(Border Gateway Protocol)

BGP는 인터넷을 위한 라우팅 정보 교환에 사용되며 인터넷 서비스 제공자(ISP) 간에 사용되는 프로토콜입니다. 시스템이 통신 사업자 네트워크에 대한 게이트웨이인 경우 BGP를 구현해야 할 수 있습니다. 단일 자율 시스템에 대해 디바이스에서 하나의 BGP 프로세스를 구성할 수 있습니다.

BGP 소개

BGP는 자율 시스템 간 라우팅 프로토콜과 자율 시스템 내부 라우팅 프로토콜입니다. 자율 시스템은 공통 관리와 공통 라우팅 정책에 따르는 네트워크 또는 네트워크 그룹입니다. BGP는 인터넷을 위한 라우팅 정보 교환에 사용되며 인터넷 서비스 제공자(ISP) 간에 사용되는 프로토콜입니다.

라우팅 테이블 변경 사항

네이버 간 TCP 연결이 처음 설정되면 BGP 네이버가 전체 라우팅 정보를 교환합니다. 라우팅 테이블 변경 사항이 감지되면 BGP 라우터가 변경된 경로만 네이버로 전송합니다. BGP 라우터는 주기적인 라우팅 업데이트를 전송하지 않고 BGP 라우팅 업데이트는 목적지 네트워크로의 최적의 경로만 알립니다.

참고 AS 루프 탐지는 전체 AS 경로를 검사하고(AS_PATH 특성에 지정된대로) 로컬 시스템의 AS 번호가 AS 경로에 나타나지 않는지 확인하여 수행됩니다. 기본적으로 EBGP는 학습된 경로를 동일한 피어에 알려서 루프 확인을 수행하는 데 있어 ASA의 추가 CPU 주기를 방지하고 기존 발신 업데이트 작업의 지연을 방지합니다.

BGP를 통해 학습된 경로에는 특정 목적지로 향하는 경로가 여럿일 때 최적의 경로를 결정하는 데 사용되는 속성이 포함되어 있습니다. 이러한 속성을 BGP 속성이라고 하며 경로 선택 과정에서 사용됩니다.

- Weight — 이는 Cisco가 정의한 라우터에 대한 로컬 속성입니다. 가중치 속성은 주변의 라우터에 알려지지 않습니다. 라우터가 동일한 목적지에 대하여 하나 이상의 경로를 학습한 경우 가중치가 가장 높은 경로가 우선합니다.
- Local preference — 로컬 기본 설정 속성은 로컬 AS로부터 출구 지점을 선택하는 데 사용됩니다. 가중치 속성과 달리 로컬 우선 속성은 로컬 AS 전체에 걸쳐 전파됩니다. AS에서 출구 지점이 여럿인 경우 로컬 우선 속성이 가장 높은 출구 지점이 특정 경로에 대한 출구 지점으로 사용됩니다.
- Multi-exit discriminator — MED(multi-exit discriminator) 또는 메트릭 속성은 메트릭에 알려지는 AS로의 우선 경로에 관한 외부 AS에 대한 제안으로 사용됩니다. MED를 수신하는 외부 AS가 경로 선택을 위해 다른 BGP 속성을 사용할 수도 있기 때문에 제안이라고 하는 것입니다. MED 메트릭이 낮은 경로가 우선합니다.
- Origin — 발신지 속성은 BGP가 특정 경로에 관해 어떻게 확인하는지 나타냅니다. 발신지 속성은 3가지 값을 가질 수 있으며 경로 선택에 사용됩니다.
  - IGP — 경로가 발신 AS 내부에 있습니다. 이 값은 경로를 BGP로 삽입하기 위해 네트워크 라우터 구성 명령을 사용할 때 설정됩니다.
  - EGP — 경로는 EBGP(Exterior Border Gateway Protocol)를 통해 확인됩니다.
  - Incomplete — 경로의 발신지가 알 수 없거나 확인되지 않았습니다. 경로가 BGP로 재배포되면 불완전한 발신지가 됩니다.
- AS_path — 경로 알림이 자율 시스템을 통과할 때 경로가 전달된 AS 번호의 주문 목록에 AS 번호가 추가됩니다. 가장 짧은 AS_path 목록을 가진 경로만 IP 라우팅 테이블에 설치됩니다.
- Next hop — EBGP next-hop 속성은 전달되는 라우터에 도달하기 위해 사용되는 IP 주소입니다. EBGP 피어의 경우 next-hop 주소는 피어 간 연결의 IP 주소입니다. IBGP의 경우 EBGP next-hop 주소가 로컬 AS로 전달됩니다.
- Community — 커뮤니티 속성은 라우팅 결정(허용, 우선, 재배포)을 적용할 수 있는 커뮤니티라는 대상 그룹화 방법을 제공합니다. 경로 맵은 커뮤니티 속성을 설정하는 데 사용됩니다. 미리 정의된 커뮤니티 속성은 다음과 같습니다.
  - no-export — 이 경로를 EBGP 피어에게 알리지 않습니다.
  - no-advertise — 이 경로를 어느 피어에게도 알리지 않습니다.
  - internet — 이 경로를 인터넷 커뮤니티에 알립니다. 네트워크의 모든 라우터가 여기 포함됩니다.

BGP를 사용해야 하는 시기

대학 및 기업과 같은 고객 네트워크는 일반적으로 네트워크 내 라우팅 정보 교환을 위해 OSPF와 같은 IGP(Interior Gateway Protocol)를 활용합니다. 고객은 ISP에 연결하고 ISP는 BGP를 사용하여 고객 및 ISP 경로를 교환합니다. AS(autonomous system) 사이에서 BGP가 사용될 때 이 프로토콜을 EBGP(External BGP)라고 합니다. 서비스 공급자가 AS 내에서 경로 교환을 위해 BGP를 사용할 때의 프로토콜은 IBGP(Interior BGP)라고 합니다.

BGP를 IPv6 네트워크를 통해 IPv6 접두사를 위한 라우팅 정보를 전달하는 데도 사용할 수 있습니다.

BGP 경로 선택

BGP는 같은 경로에 대해 서로 다른 소스로부터 여러 공지를 수신할 수 있습니다. BGP는 최적의 경로로 하나의 경로만 선택합니다. 이 경로가 선택된 경우 BGP는 선택된 경로를 IP 라우팅 테이블에 놓고 네이버에 전파합니다. BGP는 제시된 순서대로 다음 기준에 따라 목적지에 대한 경로를 선택합니다.

- 경로가 접근할 수 없는 next hop을 지정하면 업데이트를 삭제합니다.
- 가중치가 가장 높은 경로가 우선합니다.
- 가중치가 동일한 경우 로컬 우선이 가장 높은 경로가 우선합니다.
- 로컬 우선이 동일한 경우 이 라우터에서 실행 중인 BGP에서 발생한 경로가 우선합니다.
- 경로가 시작되지 않은 경우 AS_path가 가장 짧은 경로가 우선합니다.
- 모든 경로의 AS_path 길이가 같은 경우 발신지 유형이 가장 낮은 경로(IGP가 EGP보다 낮고 EGP가 incomplete보다 낮은 경로)가 우선합니다.
- 발신지 코드가 동일한 경우 MED 속성이 가장 낮은 경로가 우선합니다.
- MED가 같은 경로의 경우 내부 경로보다 외부 경로가 우선합니다.
- 그래도 경로가 동일한 경우 가장 가까운 IGP 네이버를 통한 경로가 우선합니다.
- 여러 경로에 BGP 다중 경로, 437 페이지에 대한 라우팅 테이블에서의 설치 작업이 필요한지 결정합니다.
- 두 경로 모두 외부인 경우 먼저 수신된 경로가 우선합니다(오래된 경로).
- BGP 라우터 ID가 지정한 대로 IP 주소가 가장 낮은 경로가 우선합니다.
- 여러 경로의 발신자 또는 라우터 ID가 동일할 경우 클러스터 목록 길이가 가장 짧은 경로가 우선합니다.
- 가장 낮은 네이버 주소에서 시작하는 경로가 우선합니다.

BGP 다중 경로

BGP 다중 경로를 사용하면 동일한 대상 접두사에 대해 비용이 동일한 여러 BGP 경로의 IP 라우팅 테이블에 설치할 수 있습니다. 그러면 대상 접두사에 대한 트래픽이 모든 설치된 경로에서 공유됩니다.

이러한 경로는 로드 공유에 최적의 경로와 함께 테이블에 설치됩니다. BGP 다중 경로는 최적의 경로를 선택할 때는 영향을 주지 않습니다. 예를 들어, 라우터는 알고리즘에 따라 경로 중 하나를 계속해서 최적의 경로로 지정하고 BGP 피어에 이 최적의 경로를 알립니다.

다중 경로의 후보가 되려면 동일한 대상에 대한 경로에 최적의 경로 특성과 동일한 다음 특성이 있어야 합니다.

- 무게

- 로컬 기본 설정
- AS-PATH 길이
- 출처 코드
- MED(Multi Exit Discriminator)
- 다음 중 하나입니다.
  - 네이버 AS 또는 하위-AS(BGP 다중 경로 추가 전)
  - AS-PATH(BGP 다중 경로 추가 후)

일부 BGP 다중 경로 기능은 다중 경로 후보에게 다음과 같은 추가 요구 사항을 제시합니다.

- 경로는 외부 또는 연합-외부 네이버(eBGP)에서 확인되어야 합니다.
- BGP next hop에 대한 IGP 메트릭은 최적의 경로 IGP 메트릭과 동일해야 합니다.

다음은 내부 BGP(iBGP) 다중 경로 후보에 대한 추가 요구 사항입니다.

- 경로는 내부 네이버(iBGP)에서 확인되어야 합니다.
- 라우터가 동일하지 않은 비용의 iBGP 다중 경로에 대해 구성되지 않은 경우 BGP next hop에 대한 IGP 메트릭은 최적의 경로 IGP 메트릭과 동일해야 합니다.

BGP는 다중 경로 후보에서 가장 최근에 수신한 경로를 최대 *n*개까지 IP 라우팅 테이블에 삽입합니다. 이때 *n*은 라우팅 테이블에 설치할 경로의 수이며 BGP 다중 경로를 구성할 때 지정된 수입니다. 다중 경로가 비활성화된 경우 기본값은 1입니다.

비용이 동일하지 않은 로드 밸런싱에 BGP 링크 대역폭을 사용할 수도 있습니다.

참고 동일한 next-hop-self는 내부 피어에 전달되기 전에 eBGP 다중 경로 중에서 선택된 최적의 경로에서 수행됩니다.

BGP 구성

다음 주제에서는 BGP를 구성하는 방법을 설명합니다.

BGP 전역 설정 구성

BGP를 구성할 경우, 가상 라우터를 사용하면 전역 설정이 모든 가상 라우터에 적용됩니다. BGP 프로세스를 정의하도록 구성하는 추가 BGP 설정이 있습니다. 가상 라우터를 사용하는 경우에는 각 가상 라우터당 별도의 BGP 프로세스를 구성할 수 있습니다.

시작하기 전에

BGP 전역 설정 개체를 생성한 후에 더 이상 필요하지 않은 경우 해당 개체를 삭제할 수 있습니다. 이 절차에 따라 개체를 수정하기만 하면 되지만, 대화 상자의 맨 아래에 있는 **Delete BGP Global Settings Object(BGP** 전역 설정 개체 삭제**)** 버튼을 클릭하십시오.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음, **Routing(**라우팅**)** 요약을 클릭합니다.

단계 **2** 기본 라우팅 또는 가상 라우터 페이지에서 **BGP Global Settings(BGP** 전역 설정**)** 버튼을 클릭합니다.

가상 라우터를 보려는 경우 가상 라우터의 기본 목록으로 돌아가야 합니다.

단계 **3** BGP 전역 설정 개체를 아직 구성하지 않은 경우 **Create BGP Global Settings Object(BGP** 전역 설정 개체 생성**)**를 클릭합니다.

단계 **4** (선택 사항). 개체 이름을 변경하거나 개체에 대한 설명을 입력할 수 있습니다. 기본 개체 이름은 BgpGeneralSettings입니다.

단계 **5** 최소한 다음 기본 설정을 구성합니다.

- **router bgp** *as-number*. *as-number*를 클릭하고 BGP 프로세스에 대한 자동 시스템(AS) 번호를 입력합니다. AS 번호는 1~4294967295 또는 1.0~65535.65535가 될 수 있습니다. AS 번호는 인터넷에서 각 네트워크를 식별하는 고유한 할당 값입니다. 시스템은 RFC 5396에 정의된 대로 asplain 및 asplain 표기법을 지원합니다.
- **log-neighbor-changes** *state*. *state*를 클릭하고 enable 또는 disable을 선택합니다. 이를 활성화한 경우(권장 사항), BGP 네이버가 변경되고(위로 또는 아래로) 재설정이 로깅됩니다. 이는 네트워크 연결 문제 해결과 네트워크 안정성 측정에 도움이 됩니다.
- **transport path-mtu-discovery** *state*. *state*를 클릭하고 enable 또는 disable을 선택합니다. 이를 활성화한 경우(권장 사항), 시스템에서는 두 IP 호스트 간의 네트워크 경로에서 최대 전송 단위(MTU) 크기를 확인한 다음, 최상위 MTU 경로를 사용합니다. 이는 IP 단편화를 방지합니다.
- **fast-external-fallover** *state*. *state*를 클릭하고 enable 또는 disable을 선택합니다. 이를 활성화한 경우(권장 사항), 시스템에서는 직접 연결된 외부 피어와 함께 BGP 피어링 세션에 대해 빠른 외부 페일오버를 사용합니다. 링크가 다운되면 즉시 세션이 재설정됩니다. BGP 빠른 외부 페일오버를 비활성화할 경우, BGP 라우팅 프로세스는 기본 대기 타이머(keepalive 3개)가 만료될 때까지 기다렸다가 피어링 세션을 재설정합니다.
- **enforce-first-as** *state*. *state*를 클릭하고 enable 또는 disable을 선택합니다. 이를 활성화한 경우(권장 사항), 시스템에서는 자동 시스템 번호를 AS_PATH 속성의 첫 번째 세그먼트로 나열하지 않는 eBGP 피어에서 받은 수신 업데이트를 거부합니다. 이 명령을 활성화하면 잘못 구성되었거나 허가받지 않은 피어가 다른 자동 시스템에서 보낸 경로처럼 광고함으로써 트래픽을 잘못된 방향으로 전달하는, 즉 로컬 라우터를 스푸핑하는 것을 막을 수 있습니다.

단계 **6** (선택 사항). 개체 본문 위에 있는 **Show Disabled(**비활성화된 항목 표시**)** 링크를 클릭하여 가능한 다른 모든 구성 줄을 추가합니다.

옵션 왼쪽의 +를 클릭하여 다음 옵션을 활성화할 수 있습니다.

- **bgp asnotation dot**. BGP 4바이트 자동 시스템 번호의 기본 표시 및 정규식 일치 형식을 asplain(10진수)에서 asdot(점 표기법)으로 바꿉니다. 시스템에서는 자동 시스템 번호에 대해 asplain을 자동 시스템 번호의 기본 표시 형식으로 사용합니다. 그러나 이 명령을 활성화하지 않는 경우에도 asplain 및 asdot 형식 모두로 4바이트 자동 시스템 번호를 구성할 수 있습니다.

  또한 정규식에서 4바이트 자동 시스템 번호를 일치시킬 때 기본 형식도 asplain입니다. 따라서 이 명령을 활성화하지 않을 경우, 4바이트 자동 시스템 번호를 일치시켜야 하는 모든 정규식은 asplain 형식으로 작성해야 합니다.

- **bgp scan time 60**. 숫자를 클릭하고 다음 홉 검증을 위한 BGP 라우터의 스캔 간격을 5~60초 단위로 입력합니다. 기본값은 60초입니다.

- **configure nexthop trigger** *state*. *state*를 클릭하고 **enable** 또는 **disable**을 선택합니다. BGP next-hop 주소 추적은 이벤트 기반입니다. 피어링 세션이 설정되면 BGP 접두사가 자동으로 추적됩니다. Next-hop 변경 사항은 RIB(Routing Information Base)에서 업데이트되는 대로 신속하게 BGP에 보고됩니다. 이러한 최적화를 통해 RIB에 설치된 경로의 next-hop 변경에 대한 응답 시간을 단축함으로써 전반적인 BGP 통합이 향상됩니다. BGP 검사 주기 사이에 최적 경로 계산이 실행될 경우 변경 사항만 처리되고 추적됩니다. 다음 홉 주소 추적을 활성화할 경우 다음 명령이 추가됩니다. 새 개체에서 일반 옵션을 구성하지 않은 경우, 기본값은 이 기능을 활성화하는 것입니다.

  - **bgp nexthop trigger enable**. BGP next-hop 주소 추적으로 BGP 응답 시간이 크게 향상됩니다. 그러나 불안정한 IGP(Interior Gateway Protocol) 피어로 인해 BGP가 불안정해질 수 있습니다. BGP에 미칠 영향을 줄이기 위해 불안정한 IGP 피어링 세션을 강력하게 억제하는 것이 좋습니다.

  - **bgp nexthop trigger delay 5**. 이 숫자를 클릭하여 BGP next-hop 주소 추적을 위한 라우팅 테이블 검사 간의 지연 간격을 변경합니다. 전체 라우팅 테이블 검사의 지연 간격을 IGP 조정 파라미터와 일치하도록 조정함으로써 BGP next-hop 주소 추적의 성능을 높일 수 있습니다. 기본 지연 간격은 5초이며, 이는 고속 조정된 IGP에 적합한 값입니다. 컨버전스 속도가 더 느린 IGP의 경우, IGP 통합 시간에 따라 지연 간격을 20초 이상으로 바꿀 수 있습니다. 지연을 0~100초 범위로 설정할 수 있습니다.

- **bgp aggregate-timer 30**. 숫자를 클릭하여 BGP 경로가 어그리게이션되는 간격(6~60초)을 설정합니다. 기본값은 30초입니다.

- **bgp router-id** *router-id*. *router-id*를 클릭하고 전역 라우터 ID로 사용해야 할 IPv4 주소를 입력합니다. 이 ID는 스스로 라우터 ID를 지정하지 않는 가상 라우터의 모든 BGP 프로세스에 사용됩니다. 이 명령을 활성화하지 않으면 라우터 ID가 가상 라우터에 할당된 물리적 인터페이스의 최상위 IP 주소로 설정됩니다. 이 명령을 사용하여 라우터 ID가 안정적인 상태를 유지하도록 합니다.

- **bgp maxas-limit** *value*. *value*를 클릭하고 BGP 업데이트 메시지의 AS-path 속성에 있는 자동 시스템 번호의 최대 개수(1~254 범위)를 입력합니다. AS-path 속성은 소스와 대상 라우터 간 중간 AS 번호 시퀀스로, 패킷이 이동할 방향을 형성합니다. 시스템은 지정된 값을 초과하는 AS-path에 있는 여러 개의 자동 시스템을 가진 경로를 무시합니다. 이 명령은 AS-path 세그먼트에 있는 자동 시스템 번호의 개수를 제한할 뿐만 아니라 AS-path 세그먼트의 수도 10개로 제한합니다. 이 명령을 활성화하지 않으면 어떤 경로도 삭제되지 않습니다.

단계 **7** (선택 사항). BGP 고급 옵션을 구성합니다.

필요한 경우 **Show Disabled(**비활성화된 항목 표시**)** 링크를 클릭하여 다음 명령을 표시합니다. 설정을 수정할 경우, **timers** 및 **bestpath** 옵션 집합이 모두 표시됩니다. 이러한 옵션은 몇 가지 기본값이 활성화되어 있기 때문이며, 이를 명시적으로 설정하지 않은 경우에도 마찬가지입니다.

configure bgp advanced *advanced-option*

*advanced-option*을 클릭하고 다음 중 하나를 선택합니다. 왼쪽 열의 ...를 클릭하고 **Duplicate(**중복**)**를 선택하여 이러한 모든 옵션을 구성할 수 있습니다.

- **timers**. BGP 네이버 라우터와 통신할 때 사용하는 타이머를 구성합니다.

  timers bgp 60 180 0

  - 첫 번째 값(기본값 60): **Keepalive** 간격. 숫자를 클릭하고 시스템이 keepalive 메시지를 BGP 네이버에 전송하는 빈도(0~65535초)를 입력합니다. 빈도는 20 이하로 지정하지 않는 것이 좋습니다. 이렇게 할 경우 경로에 불필요하게 플래핑이 발생할 수 있습니다.
  - 두 번째 값(기본값 180): 보류 시간. 숫자를 클릭하고, 시스템에서 keepalive 메시지를 수신한 후 BGP 네이버를 dead를 선언하기 전까지 기다려야 하는 시간(0~65535초)을 입력합니다.
  - 세 번째 값(기본값 0): 최소 보류 시간. 숫자를 클릭하고 BGP 네이버에 구성된 허용되는 최소 보류 시간을 지정합니다. 허용되는 최소 보류 시간은 이 시스템의 보류 시간으로 지정된 간격보다 작거나 같아야 합니다. 범위는 0~65535초입니다.

- **bestpath**. BGP 최적 경로 선택 알고리즘에서 사용되는 옵션을 구성합니다. **bgp default local-preference** 명령은 기본적으로 구성되지만, 명령의 **+**를 클릭하여 다른 명령을 추가할 수 있습니다.
  - **bgp default local-preference 100**. 숫자를 클릭하고, BGP AS에 있는 다른 라우터에 대한 이 시스템의 환경설정을 나타내는 값(0~4294967295)을 입력합니다. 기본값은 100입니다. 값이 높을수록 우선순위가 높습니다. 이 우선 값은 로컬 자율 시스템의 모든 라우터와 액세스 서버로 전송됩니다. 이 속성은 iBGP 피어끼리만 교환하며 로컬 정책을 결정하는 데 사용됩니다.
  - **bgp always-compare-med**. 서로 다른 자동 시스템에 있는 네이버의 경로에 대한 MED(Multi Exit Discriminator)를 비교할 수 있도록 합니다. 기본적으로 시스템은 서로 다른 자동 시스템에 있는 네이버의 경로에 대한 MED를 비교하지 않습니다.
  - **bgp bestpath compare-routerid**. 두 개의 서로 다른 피어에서 두 개의 동일한 경로를 수신한 경우(라우터 ID를 제외한 모든 속성 동일), 라우터 ID를 최적 경로 선택을 위한 기준으로 사용하십시오. 이 명령이 활성화된 경우, 다른 모든 속성이 동일하다면 라우터 ID가 가장 낮은 것이 최적 경로로 선택됩니다. 그렇지 않으면 수신된 첫 번째 경로가 사용됩니다.
  - **bgp deterministic-med**. 주변의 AS에서 광고된 최적의 MED 경로를 선택합니다.
  - **bgp bestpath med missing-as-worst**. MED 속성이 누락된 경로를 우선순위가 가장 낮은 경로로 설정합니다. 기본적으로 시스템은 누락된 MED가 있는 경로를 최적의 경로로 간주합니다.

- **graceful-restart**. 고가용성 또는 클러스터 컨피그레이션에서 시스템에 대한 Graceful Restart를 구성합니다.

- **bgp graceful-restart**. 무중단 포워딩을 위한 Graceful Restart를 활성화합니다. Graceful Restart를 사용할 경우, 시스템은 재시작 중에 주소 그룹의 포워딩 상태를 유지 관리하는 기능을 광고할 수 있습니다.
- **bgp graceful-restart restart-time 120**. 숫자를 클릭하고 graceful-restart-capable 네이버가 재시작 이벤트 발생 후 정상 작업으로 복귀하기까지 시스템이 대기할 최대 시간(1~3600초)을 입력합니다. 기본값은 120초입니다.
- **bgp graceful-restart stalepath-time 360**. 숫자를 클릭하고 시스템이 피어 재시작을 위해 오래된 경로를 보유할 최대 시간(1~3600초)을 입력합니다. 모든 오래된 경로가 이 시간 이후 삭제됩니다. 기본값은 360초입니다.

단계 **8** **OK(**확인**)**를 클릭합니다.

BGP 프로세스 구성

BGP 전역 설정을 구성한 후 BGP 프로세스를 구성할 수 있습니다. 가상 라우터를 사용하는 경우에는 각 가상 라우터당 별도의 프로세스를 구성할 수 있습니다. 시스템에 대해 또는 가상 라우터당 최대 한 개의 BGP 프로세스를 구성할 수 있습니다.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음, **Routing(**라우팅**)** 요약을 클릭합니다.

단계 **2** 가상 라우터를 활성화한 경우 BGP를 구성 중인 라우터의 보기 아이콘( )을 클릭합니다.

단계 **3** **BGP** 탭을 클릭합니다.

단계 **4** 다음 중 하나를 수행합니다.

- 새 프로세스를 생성하려면 +를 클릭하거나 **Create BGP Object(BGP** 개체 생성**)** 버튼을 클릭합니다.
- 수정할 개체의 수정 아이콘( )을 클릭합니다. 개체를 수정할 때는 직접 구성하지 않은 줄이 표시될 수도 있습니다. 이러한 줄은 구성 중인 기본값을 표시하기 위해 노출됩니다.

프로세스가 더 이상 필요하지 않은 경우 해당 개체의 휴지통 아이콘을 클릭하여 프로세스를 삭제합니다.

단계 **5** 개체의 이름과 설명(선택 사항)을 입력합니다.

단계 **6** 프로세스에 대한 최소 설정을 구성합니다.

- **router bgp** *as-number*. *as-number*를 클릭하고 전역 설정에 지정한 BGP 프로세스에 동일한 자동 시스템(AS) 번호를 입력합니다. AS 번호는 1~4294967295 또는 1.0~65535.65535가 될 수 있습니다. AS 번호는 인터넷에서 각 네트워크를 식별하는 고유한 할당 값입니다. 시스템은 RFC 5396에 정의된 대로 asplain 및 asplain 표기법을 지원합니다.

- **configure address-family** *ip-protocol*. *ip-protocol*을 클릭하고 IPv4 또는 IPv6을 선택합니다. 가상 라우터를 사용할 경우 전역 라우터에만 IPv6을 구성할 수 있습니다. 임의의 가상 라우터에 대해 IPv4를 구성할 수 있습니다. 옵션을 선택하면 **address-family ipv4 unicast** 또는 **address-family ipv6 unicast** 명령이 추가되며, 다음 명령이 추가되어 이를 구성해야 합니다.
  - **configure address-family {ipv4 | ipv6}** *settings*. settings를 클릭하고 **general** 또는 **advanced**를 클릭합니다. 이 옵션 아래에 있는 하나 이상의 명령을 구성하여 최소 프로세스를 사용해야 하지만, 중요한 프로세스의 경우 이것으로 충분하지 않습니다.

단계 **7** **Show Disabled(**비활성화된 항목 표시**)**를 클릭하고 프로세스를 맞춤 설정하여 네트워크에서 올바르게 작동하도록 합니다.

따라서 위의 설명대로 최소 명령 세트를 구성할 경우, 개체를 저장한 후 나중에 프로세스 설정을 맞춤설정할 수 있습니다. 다음 주제에서는 다양한 옵션에 대해 설명합니다. 최소한 네트워크 설정을 구성하여 프로세스가 경로를 배포할 네트워크를 식별해야 합니다. 일반 설정 및 고급 설정 두 가지 모두 대부분의 사례에 적합한 명령 기본값이 있습니다.

- SNMP 일반 설정 구성, 444 페이지
- BGP 고급 설정 구성, 445 페이지
- BGP에서 광고할 네트워크 구성, 446 페이지
- BGP 경로 삽입 구성, 447 페이지
- BGP 집계 주소 설정, 448 페이지
- IPv4에 대한 BGP 필터 설정 구성, 450 페이지
- BGP 네이버 구성, 452 페이지
- 다른 라우팅 프로토콜에서 BGP 경로 재배포 구성, 459 페이지

단계 **8** (선택 사항). 이 프로세스에 대한 라우터 ID를 구성합니다.

BGP 전역 설정에서 BGP 프로세스에 사용할 라우터 ID를 구성할 수 있습니다. 프로세스 개체에서도 선택적으로 이를 구성할 수 있습니다. 프로세스 개체에 구성된 라우터 ID는 전역 라우터 ID를 재정의합니다. 이렇게 하면 특정 가상 라우터에 대한 전역 값을 쉽게 재정의할 수 있습니다.

다음 명령이 표시되지 않을 경우 **Show Disabled(**비활성화된 항목 표시**)**를 클릭하고 옆에 있는 **+**를 클릭하여 명령을 활성화합니다.

- **bgp router-id** *router-id*. *router-id*를 클릭하고 이 프로세스의 라우터 ID로 사용해야 할 IPv4 주소를 입력합니다. 이 명령을 활성화하지 않으면 라우터 ID가 전역 라우터 ID로 설정되거나, 가상 라우터에 할당된 물리적 인터페이스의 최상위 IP 주소로 설정됩니다. 이 명령을 사용하여 라우터 ID가 안정적인 상태를 유지하도록 합니다.

단계 **9** **OK(**확인**)**를 클릭합니다.

SNMP 일반 설정 구성

일반 설정은 관리 거리, 타이머, 다음 홉 주소 추적(IPv4의 경우에만 해당)을 정의합니다. 이러한 옵션에는 대부분의 네트워크에 적합한 기본값이 설정되어 있습니다.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음, **Routing(**라우팅**)** 요약을 클릭합니다.

단계 **2** 가상 라우터를 활성화한 경우 BGP를 구성 중인 라우터의 보기 아이콘()을 클릭합니다.

단계 **3** **BGP** 탭을 클릭합니다.

단계 **4** BGP 프로세스 개체를 추가하거나 수정합니다.

단계 **5** **configure address-family ipv4** 또는 **ipv6** 줄을 찾습니다. **general** 옵션이 이미 선택되어 있는 경우 다음 단계로 이동합니다. 하지만 다음 경우를 고려하십시오.

- *settings* 변수가 계속 표시되면 이를 클릭하고 **general**를 선택합니다.
- 고급 옵션을 이미 구성한 경우, 명령의 왼쪽에 있는 **...** 버튼을 클릭하고 **Duplicate(**중복**)**를 선택합니다. 그런 다음, *settings*를 클릭하고 **general**을 선택합니다.

단계 **6** 다음 명령을 구성합니다.

- **distance bgp 20 200 200**. BGP에 대한 관리 거리(1~255)를 구성합니다. 이러한 숫자는 시스템에서 최상의 경로를 선택할 때 다른 라우팅 프로세스에 할당된 관리 값을 기준으로 합니다. 일반적으로 이 값이 클수록 신뢰 등급이 낮습니다. 다른 프로토콜이 eBGP(external BGP)를 통해 학습하는 것보다 우수한 노드 경로를 제공할 수 있거나 BGP가 일부 내부 경로를 우선적으로 사용해야 할 경우 이 명령을 사용합니다. 거리가 255인 경로는 라우팅 테이블에 설치되지 않습니다. 숫자는 다음을 의미합니다.
  - 첫 번째 값(기본값 20): 외부 거리. 숫자를 클릭하고 외부 BGP 경로에 대한 관리 거리를 입력합니다. 외부 자동 시스템에서 학습한 경로는 외부 경로입니다.
  - 두 번째 값(기본값 200): 내부 거리. 숫자를 클릭하고 내부 BGP 경로에 대한 관리 거리를 입력합니다. 로컬 자동 시스템의 피어에서 학습한 경로는 내부 경로입니다. 내부 BGP 경로의 관리 거리를 변경하는 것은 위험하므로 권장되지 않습니다. 잘못된 컨피그레이션 때문에 라우팅 테이블이 일관성을 잃고 라우팅이 중단될 수 있습니다.
  - 세 번째 값(기본값 200): 로컬 거리. 숫자를 클릭하고 로컬 BGP 경로에 대한 관리 거리를 입력합니다. 로컬 경로는 BGP 라우팅 프로세스의 **network** 명령을 통해 나열된 네트워크(즉, 프로세스에서 광고하는 네트워크) 또는 다른 프로세스에서 BGP에 재배포 중인 네트워크용입니다.

단계 **7** **OK(**확인**)**를 클릭합니다.

BGP 고급 설정 구성

특수한 상황에서만 필요한 다양한 옵션을 구성하려면 고급 설정을 사용합니다. 이러한 대부분의 옵션은 기본적으로 비활성화되어 있습니다.

시작하기 전에

table-map 명령을 구성하려면, 우선 **Device(**디바이스**)** > **Advanced Configuration(**고급 컨피그레이션**)** 페이지로 이동한 후 명령에 필요한 스마트 CLI 경로 맵 개체를 생성합니다.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음, **Routing(**라우팅**)** 요약을 클릭합니다.

단계 **2** 가상 라우터를 활성화한 경우 BGP를 구성 중인 라우터의 보기 아이콘( )을 클릭합니다.

단계 **3** **BGP** 탭을 클릭합니다.

단계 **4** BGP 프로세스 개체를 추가하거나 수정합니다.

단계 **5** **configure address-family ipv4** 또는 **ipv6** 줄을 찾습니다. **advanced** 옵션이 이미 선택되어 있는 경우 다음 단계로 이동합니다. 하지만 다음 경우를 고려하십시오.

- *settings* 변수가 계속 표시되면 이를 클릭하고 **advanced**를 선택합니다.
- 일반 옵션을 이미 구성한 경우, 명령의 왼쪽에 있는 **...** 버튼을 클릭하고 **Duplicate(**중복**)**를 선택합니다. 그런 다음, *settings*를 클릭하고 **advanced**를 선택합니다.

단계 **6** 다음 명령을 구성합니다. 개체를 처음 생성할 때 첫 번째 명령 이외의 모든 항목을 표시하려면 **Show Disabled(**비활성화된 항목 표시**)**를 클릭해야 합니다.

명령의 +를 사용하여 이를 활성화합니다.

- **bgp redistribute-internal**. EIGRP 또는 OSPF 같은 IGP(Interior Gateway Protocol)로의 iBGP 재배포를 구성합니다. IGP에 iBGP를 재배포할 때 각별히 주의해야 합니다. 재배포되는 접두사의 수를 제한하기 위해 IP 접두사 목록 및 경로 맵 구문을 사용합니다. 필터링되지 않은 BGP 라우팅 테이블을 IGP에 재배포하면 정상적인 IGP 네트워크 작업에 지장을 줄 수 있습니다. 이 명령은 기본적으로 활성화되어 있으므로 이를 해제하려면 해당 명령의 - 버튼을 클릭해야 합니다.
- **bgp suppress-inactive**. RIB(비활성 경로)에 설치되지 않은 경로가 피어에 광고되지 않도록 합니다. 기본적으로 BGP는 비활성 경로를 광고합니다. BGP는 RIB에 설치되지 않은 경로에 RIB-failure 플래그를 표시합니다. 이 플래그는 **show bgp** 명령의 출력에도 나타납니다. 이를테면 Rib-Failure (17)이라고 표시됩니다. 이 플래그는 경로 또는 RIB에 대한 오류나 문제를 의미하지 않습니다.
- **auto-summary**. (IPv4 전용) 서브넷 경로를 네트워크 레벨 경로로 자동으로 요약합니다. 경로를 요약하면 라우팅 테이블에서 라우팅 정보의 양이 줄어듭니다. 연결되지 않은 서브넷 간의 라우팅을 수행해야 하는 경우 자동 요약을 비활성화합니다. 자동 요약이 비활성화되면 서브넷이 알려집니다.
- **synchronization**. BGP와 IGP(Interior Gateway Protocol) 시스템(예: OSPF) 간 동기화를 활성화합니다. 일반적으로 BGP 스피커는 경로가 로컬이거나 IGP에 존재하지 않는 한 외부 네이버에 경

로를 전달하지 않습니다. 이 기능을 사용하면 자동 시스템 내의 라우터 및 액세스 서버가 BGP에서 다른 자동 시스템에 사용할 수 있도록 지정하기 전에 경로를 가질 수 있습니다. 자동 시스템의 다른 라우터가 BGP를 발신하지 않는 경우 이 명령을 사용합니다.

- **table-map** *route-map options*. (IPv4 전용) BGP 라우팅 테이블에서 업데이트되는 경로에 대한 메트릭, 태그 값 또는 트래픽 색인을 설정하는 경로 맵을 적용하거나, 경로가 RIB에 다운로드되는지 여부를 제어합니다. *route-map*을 클릭하고 경로 맵을 정의하는 스마트 CLI 개체를 선택합니다. 경로 맵에서 IP 액세스 목록, 자동 시스템 경로, 커뮤니티, 접두사 목록, 다음 홉에 대한 일치 절을 사용할 수 있습니다.

  *options*를 클릭하고 공백 또는 **filter**를 선택하여 경로 맵을 사용하는 방법을 결정할 수 있습니다.

  - **filter**를 선택하지 않을 경우, 시스템은 경로를 RIB에 설치하기 전에 경로 맵을 사용하여 경로의 특정 속성을 설정합니다. 경로 맵에서 해당 경로를 허용하거나 거부하는지 여부에 관계없이, 경로는 항상 다운로드됩니다.
  - **filter**를 선택할 경우, 경로 맵은 BGP 경로를 RIB에 다운로드할지 여부도 제어합니다. 경로 맵에서 허용된 경로만 다운로드되며, 거부된 경로는 다운로드되지 않습니다.

- **default-information originate**. 기본 경로(네트워크 0.0.0.0)를 광고하도록 BGP를 구성합니다. **default-information originate** 명령의 컨피그레이션은 **network** 명령의 컨피그레이션과 유사합니다. 그러나 **default-information originate** 명령을 사용하려면 경로 0.0.0.0을 명시적으로 재배포해야 하며, 이는 이 개체에서도 구성해야 합니다. **network** 명령을 사용하려면 OSPF 같은 IGP(Interior Gateway Protocol) 라우팅 테이블에 경로 0.0.0.0만 있어야 합니다. 따라서 기본 경로를 배포하려면 **network** 명령을 사용하는 것이 좋습니다.
- **maximum paths 1**. 라우팅 테이블에 설치할 수 있는 병렬 BGP 경로의 최대 수(1~8개)를 제어합니다. 이 명령을 사용하여 BGP 피어링 세션에 대해 equal-cost 또는 unequal-cost 다중 경로 로드 공유를 구성합니다. BGP 라우팅 테이블에 다중 경로로서 경로를 설치하려는 경우 해당 경로는 이미 설치된 다른 경로와 동일한 다음 홉을 가질 수 없습니다. BGP 다중 경로 로드 공유가 구성되어도 BGP 라우팅 프로세스에서는 여전히 BGP 피어에 대한 최적의 경로를 광고합니다. equal-cost 경로의 경우 최저 라우터 ID가 있는 네이버의 경로가 최적의 경로로서 광고됩니다.

  BGP equal-cost 다중 경로 로드 공유를 구성하려면 모든 경로 속성이 동일해야 합니다. 경로 속성에는 가중치, 로컬 우선, 자동 시스템 경로(길이만이 아니라 전체 속성), 발신지 코드, MED(Multi Exit Discriminator) 및 IGP(Interior Gateway Protocol) 거리가 포함됩니다.
- **maximum paths ibgp 1**. 라우팅 테이블로 설치할 수 있는 내부 BGP 경로의 최대 수(1~8개)를 제어합니다. 다중 경로 iBGP에 대한 고려 사항은 위의 **maximum paths** 명령에 설명된 것과 동일합니다.

단계 **7** **OK(**확인**)**를 클릭합니다.

BGP에서 광고할 네트워크 구성

BGP 라우팅 프로세스로 광고할 네트워크를 정의해야 합니다.

시작하기 전에

광고할 네트워크를 정의하는 네트워크 개체를 생성합니다. BGP에 대해 구성하는 주소 패밀리에 따라 IPv4 네트워크 또는 IPv6 네트워크를 정의하거나, 두 가지를 모두 정의할 수 있습니다.

네트워크 개체가 대규모 네트워크 공간을 지정할 경우, 네트워크 개체에 적용할 경로 맵을 생성하여 광고하지 않을 더 큰 공간 내에서 서브넷을 필터링할 수 있습니다. 경로 맵 사양과 일치하는 경로만 광고됩니다. 스마트 CLI를 사용하여 경로 맵 개체를 생성합니다.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음, **Routing(**라우팅**)** 요약을 클릭합니다.

단계 **2** 가상 라우터를 활성화한 경우 BGP를 구성 중인 라우터의 보기 아이콘( )을 클릭합니다.

단계 **3** **BGP** 탭을 클릭합니다.

단계 **4** BGP 프로세스 개체를 추가하거나 수정합니다.

네트워크 명령은 **configure address family ipv4** 또는 **ipv6** 명령 아래에 있는 명령 세트 내에 있습니다. 광고할 네트워크를 구성하려면 주소 패밀리를 구성해야 합니다.

각 주소 그룹 내의 **network** 명령은 구성하려는 주소 패밀리와 일치하는 주소를 지정해야 합니다.

단계 **5** **Show Disabled(**비활성화된 항목 표시**)**를 클릭하여 모든 명령을 표시한 다음, **+**를 클릭하여 **network** 또는 **network route-map** 명령을 활성화하고, 다음 옵션을 구성합니다.

- *network-object*. 변수를 클릭하고 광고할 네트워크를 정의하는 네트워크 개체인 IPv4 네트워크 주소 및 마스크 또는 IPv6 네트워크 주소 및 접두사를 선택합니다.
- **route-map** *map-tag*. 변수를 클릭하고, 네트워크 개체에 적용해야 하는 경로 맵을 선택하여 해당 범위 내에서 광고해야 할 주소를 필터링합니다.
- (선택 사항, IPv6 전용.) *prefix-name*. 변수를 클릭하고 접두사를 광고할 DHCPv6 접두사의 이름을 입력합니다. 이 옵션을 구성할 경우 네트워크 개체가 접두사에 대한 서브넷 역할을 합니다. 이 옵션을 사용하려면 DHCPv6 접두사 위임 클라이언트를 활성화해야 합니다. 이렇게 하려면 FlexConfig를 사용하여 **ipv6 dhcp client pd** 명령을 인터페이스 컨피그레이션 모드의 인터페이스에 추가해야 합니다.

단계 **6** **...** > **Duplicate(**중복**)(network** 또는 **network route-map** 명령 옆**)**를 클릭하여 광고할 추가 네트워크를 구성합니다.

단계 **7** **OK(**확인**)**를 클릭합니다.

BGP 경로 삽입 구성

조건부 경로 삽입을 구성하여 BGP 라우팅 테이블로 더 많은 특정 경로를 삽입할 수 있습니다. 조건부 경로 삽입을 통해 더 특정한 접두사를 일치 없이 BGP 라우팅 테이블에 넣을 수 있습니다. 모든 삽입된 접두사에 대해 유효한 상위 경로가 있어야 합니다. 어그리게이트 경로(기존 접두사)와 같거나 더 특정한 접두사만 삽입할 수 있습니다.

시작하기 전에

접두사를 정의하는 데 필요한 경로 맵을 생성해야 합니다. 이러한 경로 맵은 절차에 설명된 요건을 충족해야 합니다.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음, **Routing(**라우팅**)** 요약을 클릭합니다.

단계 **2** 가상 라우터를 활성화한 경우 BGP를 구성 중인 라우터의 보기 아이콘()을 클릭합니다.

단계 **3** **BGP** 탭을 클릭합니다.

단계 **4** BGP 프로세스 개체를 추가하거나 수정합니다.

경로 삽입 명령은 **configure address family ipv4** 또는 **ipv6** 명령 아래에 있는 명령 세트 내에 있습니다. 광고할 네트워크를 구성하려면 주소 패밀리를 구성해야 합니다.

단계 **5** **Show Disabled(**비활성화된 항목 표시**)**를 클릭하여 모든 명령을 표시한 다음, **+**를 클릭하여 **bgp inject-map** 명령을 활성화합니다.

단계 **6** 다음 명령 속성을 구성합니다.

- **inject-map** *inject-map*. 변수를 클릭하고 라우팅 테이블에 생성 및 설치할 접두사를 정의하는 경로 맵을 선택합니다. 삽입된 접두사는 로컬 BGP RIB에 설치됩니다. 유효한 상위 경로가 있어야 합니다. 어그리게이트 경로(기존 접두사)와 같거나 더 특정한 접두사만 삽입할 수 있습니다. 경로 맵은 접두사 목록을 사용하여 삽입할 경로를 지정해야 합니다.
- **exist-map** *exist-map*. 변수를 클릭하고 BGP 스피커가 추적할 접두사를 정의하는 경로 맵을 선택합니다. 이 경로 맵은 접두사 목록을 사용하여 어그리게이트 접두사를 지정하고 경로 소스도 지정해야 합니다. 경로 소스는 서브넷이 아닌 라우터입니다(예: 10.2.1.1/32).
- *options*. 선택에 따라, 변수를 클릭하고 **copy-attributes**를 선택합니다. 이 옵션은 어그리게이트 경로와 동일한 속성을 상속하도록 삽입된 접두사를 구성합니다. 이 키워드를 선택하지 않으면 삽입된 접두사는 로컬에서 시작한 경로의 기본 속성을 사용합니다.

단계 **7** **...** > **Duplicate(**중복**)(bgp inject-map** 명령 옆**)**를 클릭하여 추가 경로 삽입 규칙을 구성합니다.

단계 **8** **OK(**확인**)**를 클릭합니다.

BGP 집계 주소 설정

BGP 네이버는 라우팅 정보를 저장하고 교환하며 더 많은 BGP 스피커가 구성되면 라우팅 정보의 양이 증가합니다. 경로 어그리게이션은 여러 경로의 속성을 결합하여 하나의 경로만 알리는 프로세스입니다. 종합 접두사는 CIDR(Classless Interdomain Routing) 원칙을 사용하여 연속 네트워크를 라우팅 테이블에 요약할 수 있는 하나의 클래스리스 IP 주소 집합으로 결합합니다. 결과적으로 더 적은 경로를 알리게 됩니다.

명령에서 키워드 없이 어그리게이트 경로를 구성하면 지정된 범위 내에 속하는 더 구체적인 BGP 경로를 사용할 수 있는 경우 시스템은 BGP 라우팅 테이블에서 어그리게이트 항목을 생성합니다. (어그

리게이트와 일치하는 더 긴 접두사가 RIB(Routing Information Base)에 있어야 합니다.) 어그리게이트 경로는 자동 시스템에서 오는 것으로 광고되며, 정보가 누락될 수 있음을 보여주는 원자성 어그리게이트 속성 세트를 갖습니다. **as-set** 키워드를 지정하지 않는 한 원자성 어그리게이트 속성이 설정됩니다.

다음 절차에서는 특정 경로의 어그리게이션을 하나의 경로로 구성하는 방법에 대해 설명합니다.

시작하기 전에

경로 맵을 적용하여 어그리게이트되는 경로 또는 어그리게이트 경로의 속성 세트를 세부적으로 조정하려면 스마트 CLI 경로 맵 개체를 생성합니다.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음, **Routing(**라우팅**)** 요약을 클릭합니다.

단계 **2** 가상 라우터를 활성화한 경우 BGP를 구성 중인 라우터의 보기 아이콘( )을 클릭합니다.

단계 **3** **BGP** 탭을 클릭합니다.

단계 **4** BGP 프로세스 개체를 추가하거나 수정합니다.

어그리게이션 명령은 **configure address family ipv4** 또는 **ipv6** 명령 아래에 있는 명령 세트 내에 있습니다. 어그리게이션을 구성하려면 주소 패밀리를 구성해야 합니다.

단계 **5** **Show Disabled(**비활성화된 항목 표시**)**를 클릭하여 모든 명령을 표시한 다음, **+**를 클릭하여 **configure aggregate-address** 명령을 활성화합니다.

단계 **6** *map-type* 변수를 클릭하고 이 특정 어그리게이트 경로에 적용할 경로 맵 유형을 선택합니다.

이 옵션에 따라 개체에 추가되는 **aggregate-address** 명령에 포함되는 파라미터가 결정됩니다. 총 3개의 개별 경로 맵을 적용하여 어그리게이션에서 경로를 억제하고, 경로를 광고하고, 어그리게이트 경로에 적용할 속성을 정의할 수 있습니다.

- 경로 맵을 적용할 필요가 없는 경우 **no-map**을 선택합니다
- 모든 세 가지 옵션에 경로 맵을 적용하려면 **all**을 선택합니다.
- 전체가 아닌 하나 또는 두 가지 맵을 적용하려면 **suppress-map**, **advertise-map**, **attribute-map**, **suppress-advertise**, **suppress-attribute**, **advertise-attribute** 중에서 적절한 키워드 조합을 선택합니다.

단계 **7** 어그리게이트할 경로의 속성을 구성합니다.

다음은 속성의 전체 목록입니다. 표시되는 내용은 맵 유형 선택 사항에 따라 달라집니다.

- *network-object*. 변수를 클릭하고 어그리게이트할 어드레스 스페이스를 정의하는 네트워크 개체를 선택합니다. 개체는 구성할 주소 유형과 일치하는 IPv4 또는 IPv6 주소를 사용해야 합니다. 예를 들어 모든 10.0.0.0/8 서브넷에 대한 경로를 어그리게이트할 수 있습니다.
- **suppress-map** *suppress-route-map*. 변수를 클릭하고 경로 맵을 선택하여 지정된 경로의 광고를 억제합니다. 경로 맵의 일치 절을 사용하여 일부 더 구체적인 어그리게이트 경로를 선택적으로

억제하고 나머지는 억제하지 않을 수 있습니다. 경로 맵은 액세스 목록 및 자동 시스템 경로를 기준으로 한 경로와 일치할 수 있습니다.

- **advertise-map** *advertise-route-map*. 변수를 클릭하고, 어그리게이트 경로의 다른 구성 요소(예: AS_SET 또는 커뮤니티)를 빌드하는 데 사용할 특정 경로를 선택하는 경로 맵을 선택합니다. 이는 어그리게이트의 구성 요소가 별도의 자동 시스템에 있는 상태에서 AS_SET로 어그리게이트를 만들고 이를 동일한 자동 시스템 중 일부에 다시 광고하려는 경우에 유용합니다. 어그리게이트가 수신 라우터에서 BGP 루프 탐지 메커니즘에 의해 삭제되지 않도록 AS_SET에서 특정 자동 시스템 번호를 생략해야 합니다. 경로 맵은 액세스 목록 및 자동 시스템 경로를 기준으로 한 경로와 일치할 수 있습니다.
- **attribute-map** *attribute-route-map*. 변수를 클릭하고 어그리게이트 경로의 속성을 변경하는 경로 맵을 선택합니다. 이는 AS_SET를 구성하는 경로 중 하나가 community no-export 속성과 같이 어그리게이트 경로가 내보내지지 않도록 하는 속성으로 구성된 경우에 유용합니다.
- *options*. 변수를 클릭하고 다음 옵션에서 하나 또는 전체를 선택하거나 아무것도 선택하지 않습니다.
  - **as-set**. 어그리게이트 경로에 대한 자동 시스템 세트 경로 정보를 생성합니다. 이 경로에 대해 알려지는 경로는 요약되는 모든 경로에 포함된 모든 요소로 구성된 AS_SET가 됩니다. 여러 경로를 어그리게이트할 때는 이 키워드를 사용하지 마십시오. 이 경로는 요약된 경로에 대한 자동 시스템 경로 도달 정보가 변경될 때마다 계속해서 취소 및 업데이트해야 합니다.
  - **summary-only**. 모든 네이버에 대한 더 구체적인 경로의 광고를 억제합니다.

단계 **8** **...** > **Duplicate(**중복**)(configure aggregate-address** 명령 옆)를 클릭하여 어그리게이트할 추가 경로를 구성합니다.

단계 **9** **OK(**확인**)**를 클릭합니다.

IPv4에 대한 BGP 필터 설정 구성

필터 규칙을 생성하여 시스템이 다른 라우팅 프로토콜로부터 학습하거나 다른 라우팅 프로토콜에 광고하는 라우팅 정보를 제한할 수 있습니다.

여기에 설명된 컨피그레이션은 모든 로컬 프로세스 및 모든 BGP 네이버에 대한 업데이트를 필터링하는 데 적용됩니다. neighbor 설정에서 neighbor마다 서로 다른 필터링 규칙을 구성할 수 있습니다.

시작하기 전에

각 필터 규칙에 필요한 스마트 CLI 표준 액세스 목록 개체를 생성합니다. 거부 액세스 제어 항목(ACE)을 사용하여 항목과 일치하는 경로를 필터링하고, 업데이트해야 하는 경로에 대한 ACE를 허용합니다.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음, **Routing(**라우팅**)** 요약을 클릭합니다.

단계 **2** 가상 라우터를 활성화한 경우 BGP를 구성 중인 라우터의 보기 아이콘( )을 클릭합니다.

단계 **3** **BGP** 탭을 클릭합니다.

단계 **4** BGP 프로세스 개체를 추가하거나 수정합니다.

필터링 명령은 **configure address family ipv4** 명령 아래에 있는 명령 세트 내에 있습니다. 필터링을 구성하려면 주소 패밀리를 구성해야 합니다. 이러한 규칙은 IPv6에 사용할 수 없습니다.

단계 **5** **Show Disabled(**비활성화된 항목 표시**)**를 클릭하여 모든 명령을 표시한 다음, **+**를 클릭하여 **configure filter-rules** *direction* 명령을 활성화합니다.

단계 **6** *direction*을 클릭하고 수신 업데이트 필터링에 **in**을 선택하거나, 아웃바운드 업데이트 필터링에 **out**을 선택합니다.

단계 **7** 인바운드 필터의 경우, 업데이트를 필터링할 인터페이스를 선택적으로 지정할 수 있습니다. 인터페이스를 지정하지 않으면 인터페이스에서 수신된 모든 업데이트에 필터가 적용됩니다.

a) **+**를 클릭하여 **distribute-list** *acl-name* **in interface** *interface* 명령을 활성화합니다.

b) *interface* 변수를 클릭하고 인터페이스를 선택합니다.

단계 **8** 아웃바운드 필터의 경우 프로토콜을 선택적으로 지정하여, 해당 라우팅 프로세스로 광고되는 경로로 필터를 제한할 수 있습니다.

distribute-list out 명령은 두 가지 형식이 있습니다. 하나는 *protocol* 변수 뒤에 *identifier* 변수가 있는 형식이고, 다른 하나는 식별자가 없는 형식입니다. 다음과 같은 프로토콜을 선택할 수 있지만, 이러한 프로토콜은 추가 식별자 정보를 제공해야 하는지 여부에 따라 아래와 같은 명령 버전으로 나뉩니다.

- **connected**. 시스템의 인터페이스에 직접 연결된 네트워크에 대해 설정된 경로의 경우.
- **static**. 수동으로 생성한 정적 경로의 경우.
- **rip**. RIP에 광고된 경로의 경우.
- **bgp** *automonous-system*. BGP에 광고된 경로의 경우. *identifier*를 클릭하고 시스템에 정의된 BGP 프로세스에 대한 자동 시스템 번호를 입력합니다.
- **eigrp** *automonous-system*. EIGRP에 광고된 경로의 경우. *identifier*를 클릭하고 시스템에 정의된 EIGRP 프로세스에 대한 자동 시스템 번호를 입력합니다.
- **ospf** *process-id*. OSPF에 광고된 경로의 경우. *identifier*를 클릭하고 시스템에 정의된 OSPF 프로세스에 대한 프로세스 ID를 입력합니다.

단계 **9** **...** > **Duplicate(**중복**)(configure filter-rules** 명령 옆**)**를 클릭하여 다른 필터 규칙을 정의할 수 있습니다. 필요한 개수만큼 정의합니다.

단계 **10** **OK(**확인**)**를 클릭합니다.

BGP 네이버 구성

BGP가 라우팅 업데이트를 교환하는 네이버를 정의해야 합니다.

시작하기 전에

여러 선택적인 명령에는 경로 맵, 접두사 목록 등에 대한 스마트 CLI 개체가 필요합니다. 개체가 필요한지 확인하려면 구성해야 하는 옵션을 검토합니다. 연결된 BGP 명령을 구성하려면 먼저 스마트 CLI 개체를 생성해야 합니다.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음, **Routing(**라우팅**)** 요약을 클릭합니다.

단계 **2** 가상 라우터를 활성화한 경우 BGP를 구성 중인 라우터의 보기 아이콘()을 클릭합니다.

단계 **3** **BGP** 탭을 클릭합니다.

단계 **4** BGP 프로세스 개체를 추가하거나 수정합니다.

네이버 명령은 **configure address family ipv4** 또는 **ipv6** 명령 아래에 있는 명령 세트 내에 있습니다. 각 주소 패밀리에 대해 개별적으로 네이버를 구성해야 합니다.

단계 **5** **Show Disabled(**비활성화된 항목 표시**)**를 클릭하여 모든 명령을 표시한 다음, **+**를 클릭하여 **configure neighbor** 명령을 활성화합니다.

단계 **6** 네이버 명령에서 기본 네이버 파라미터를 구성합니다.

- **neighbor** *neighbor-address*. 변수를 클릭한 후, 구성하려는 주소 그룹에 알맞게 BGP 네이버 라우터의 IPv4 또는 IPv6 주소를 입력합니다.
- **remote-as** *as-number*. 변수를 클릭하고 BGP 네이버 라우터의 자동 시스템 번호를 입력합니다.
- *config-options*. 변수를 클릭하고 **properties**를 선택합니다. 기본적으로 구성되는 속성만 네이버를 활성화합니다. 이 절차에 설명된 대로 다른 옵션을 조정할 수 있습니다.

단계 **7** (선택 사항). 네이버 일반 설정을 구성합니다.

a) **+**를 클릭하여 **configure neighbor** *neighbor-address* **remote-as** *settings* 명령을 활성화합니다. 명령을 볼 수 없는 경우 **Show Disabled(**비활성화된 항목 표시**)**를 클릭합니다.

b) *settings*를 클릭하고 **general**를 선택합니다.

c) **configure neighbor description** 명령에서 변수를 클릭하고 네이버에 대한 설명(네이버의 위치 또는 목적 등)을 최대 80자까지 입력하거나, 설명을 원하지 않을 경우 **-**를 클릭하여 명령을 비활성화합니다. 설명에는 공백 또는 물음표를 포함할 수 없습니다.

d) (IPv4 전용) **configure neighbor shutdown** 명령은 초기에 활성화되어 있습니다. 이 명령은 이러한 BGP 네이버와의 통신을 비활성화하여 활성 세션을 종료하고, 모든 연결된 라우팅 정보를 제거합니다. 이러한 네이버와 활발하게 통신하려면 **-**를 클릭하여 이 명령을 비활성화합니다.

e) **configure neighbor fall-over bfd** 명령에서 *option*을 클릭하고 **single-hop** 또는 **multi-hop**(BFD 컨피그레이션에 따라)을 선택하거나, **-**를 클릭하여 명령을 비활성화합니다.

이 명령은 BGP를 등록하여 BFD(Bidirectional Forwarding Detection)에서 포워딩 경로 탐지 오류 메시지를 수신하도록 합니다. 단일 홉 또는 멀티 홉 선택 여부는 사용자가 생성한 후 이 네이버와 접하는 인터페이스에 연결한 BFD 템플릿의 유형에 따라 좌우됩니다. 여기서 선택한 사항이 BFD 템플릿과 일치하는지 확인합니다. FlexConfig를 사용하여 BFD 템플릿을 작성하고 적용해야 합니다.

단계 **8** (선택 사항). 네이버 고급 설정을 구성합니다.

a) 이미 구성한 경우 **...** > **Duplicate(**중복**)(configure neighbor** *neighbor-address* **remote-as** *settings* 명령의 경우)를 클릭하거나 아직 사용 중이 아닌 경우 **+**를 클릭하여 활성화합니다. 명령을 볼 수 없는 경우 **Show Disabled(**비활성화된 항목 표시**)**를 클릭합니다.

b) *settings*를 클릭하고 **advanced**를 선택합니다.

c) **neighbor password** 명령에서 *secret* 변수를 클릭하고 네이버를 인증할 때 사용할 비밀번호가 포함된 비밀 키 개체를 선택하거나, MD5(Message Digest 5) 인증을 사용하지 않으려는 경우 **-**를 클릭하여 명령을 비활성화합니다. BGP 개체를 수정하는 동안에는 키 개체를 생성할 수 있습니다.

비밀 키 개체는 대/소문자를 구분하는 키 비밀번호를 최대 25자까지 포함해야 합니다. 문자열은 공백 및 특수 문자(` ~ ! @ # $ % ^ & * ( ) - _ = + | \ } ] { [ " ` : ; / > <.,?)를 포함하여 모든 영문숫자 문자를 포함할 수 있습니다. 그러나 number-space-anything 형식의 비밀번호는 지정할 수 없습니다. 숫자 뒤에 공백이 오면 인증이 실패할 수 있습니다.

네이버가 동일한 비밀번호를 사용하도록 구성되어 있는지 확인합니다.

d) **configure neighbor hops** 명령에서 *options* 변수를 클릭하고 다음 중 하나를 선택하거나, 피어가 멀티 홉과 떨어져 있지 않은 경우(즉, 이 시스템에 직접 연결되지 않은 경우) **-**를 클릭하여 명령을 비활성화합니다. 라우팅 루프와 반복 경로가 발생할 수 있으므로 이러한 옵션은 신중하게 사용하십시오. 직접 연결된 피어만 구성하는 것이 좋습니다.

- **ebgp-multihop**. 직접 연결되지 않은 네트워크에 상주하는 외부 피어로의 BGP 연결을 승인 및 시도합니다. 이 옵션을 선택하면 다음 명령이 추가됩니다.
  - **neighbor ebgp-multihop 255**. 255를 클릭하고 TTL(Time-to-Live) 값을 홉 수(1~255)로 입력합니다.
  - **neighbor disable-connected-check**. **+**를 클릭하여 이 명령을 활성화하고 연결 확인을 비활성화하여 루프백 인터페이스를 사용하는 단일 홉 피어로 eBGP 피어링 세션을 설정합니다. 이 명령이 없으면 피어가 동일한 네트워크 세그먼트에 직접 연결되어 있지 않은 경우 연결 확인을 수행하면 피어링 세션의 연결이 차단됩니다.
- **ttl-security-hop**. BGP 피어링 세션을 보안하고 두 외부 BGP(eBGP) 피어를 분리는 최대 홉 개수를 구성합니다. 이 옵션을 선택하면 다음 명령이 추가됩니다.

  neighbor ttl-security hops *hop-count*. 변수를 클릭하고 피어를 분리하는 최대 홉 수(1~254)를 입력합니다.

  neighbor ttl-security 명령은 CPU 사용률 기반 공격으로부터 BGP 피어링 세션을 보호하기 위해 경량 보안 메커니즘을 제공합니다. 이러한 유형의 공격은 일반적으로 패킷 헤더에 위조된 소스 및 수신 IP 주소가 포함된 IP 패킷을 네트워크에 집중적으로 보내 네트워크를 무력화하려는 DoS(Denial of Service) 무차별 대입(brute force) 공격입니다.

이 기능은 TTL 수가 로컬에서 구성한 값보다 크거나 같은 IP 패킷만 허용하는 IP 패킷의 기본 동작을 활용합니다. IP 패킷에서 TTL 수를 정확하게 위조하는 것은 일반적으로 불가능한 것으로 간주됩니다. 소스 또는 대상 네트워크에 내부적으로 액세스하지 않고는, 신뢰 피어의 TTL 수와 일치하도록 패킷을 정확히 위조하는 것이 불가능합니다.

이 기능의 효과를 최대화하려면 로컬 네트워크와 외부 네트워크 간 홉(hop) 수가 일치하도록 hop-count 값을 엄격하게 구성해야 합니다. 그러나 멀티 홉(multihop) 피어링 세션에 대해 이 기능을 구성할 경우 경로 변경 가능성을 고려해야 합니다. 네트워크의 모든 라우터에서 이 기능을 구성하십시오.

e) **neighbor version** 명령에서 *version-number* 변수를 클릭하고 4를 입력하여 소프트웨어에서 BGP 버전 4를 사용하도록 하거나, **-**를 클릭하여 명령을 비활성화합니다. 기본적으로 버전 4가 사용되며, 필요한 경우 버전 2로 동적으로 다운되도록 협상됩니다. 이 명령에서 4를 구성하면 버전 협상이 방지됩니다.

f) **neighbor transport connection-mode** 명령에서 *options* 변수를 클릭하고 TCP 연결이 **active** 또는 **passive**인지 선택하거나, **-**를 클릭하여 명령을 비활성화하고 모드를 기본값으로 그대로 둡니다.

g) **neighbor transport path-mtu-discovery** 명령에서 *options* 변수를 클릭하고 **blank**를 선택하여 경로 MTU 검색을 활성화하거나, **disable**을 선택하여 비활성화합니다. 기본적으로 경로 MTU 검색이 수행되므로, blank를 선택하는 것은 **-**를 클릭하여 명령을 비활성화하는 것과 같습니다. 경로 MTU 검색을 수행하면 BGP 세션에서 대규모 MTU 링크를 활용할 수 있습니다.

단계 **9** (선택 사항). 네이버 마이그레이션 설정을 구성합니다.

마이그레이션 설정은 **neighbor local-as** 명령을 구성합니다. **neighbor local-as** 명령은 eBGP 네이버에서 수신하는 경로에 대한 자동 시스템 번호를 추가 및 제거하여 AS_PATH 특성을 사용자 지정하는 데 사용됩니다. 이 명령의 컨피그레이션은 라우터가 자동 시스템 번호 마이그레이션을 위해 외부 피어에 또 다른 자동 시스템의 멤버로서 표시되도록 허용합니다. 이 기능은 기존 피어링 정돈 작업을 방해하지 않은 채 네트워크 운영자가 고객을 새로운 컨피그레이션으로 마이그레이션하도록 허용함으로써 BGP 네트워크에서 자동 시스템 번호를 변경하는 프로세스를 간소화합니다.

이 마이그레이션은 진정한 eBGP 피어링 세션에 대해서만 수행할 수 있습니다. 이 명령은 연합의 서로 다른 하위 자동 시스템에 있는 두 개의 피어에 대해 작동하지 않습니다.

주의 BGP는 네트워크 도달 정보를 유지하고 라우팅 루프를 예방하기 위해 경로가 이동하는 각 BGP 네트워크에서 자동 시스템을 접두사로 추가합니다. 이 명령은 자동 시스템 마이그레이션에만 구성하고, 이전이 완료된 후에는 구성을 해제하십시오. 이 절차는 숙련된 네트워크 운영자만 시도해야 합니다. 부적절한 컨피그레이션을 통해 라우팅 루프가 생성될 수 있습니다.

a) 이미 구성한 경우 **...** > **Duplicate(**중복**)(configure neighbor** *neighbor-address* **remote-as** *settings* 명령의 경우)를 클릭하거나 아직 사용 중이 아닌 경우 **+**를 클릭하여 활성화합니다. 명령을 볼 수 없는 경우 **Show Disabled(**비활성화된 항목 표시**)**를 클릭합니다.

b) *settings*를 클릭하고 **migration**를 선택합니다. 그러면 다음과 같은 명령이 추가됩니다.

configure *neighbor-address* **local-as** *local-as-number options*

c) *local-as-number* 변수를 클릭하고 AS_PATH 속성 앞에 추가할 로컬 자동 시스템(AS) 번호를 입력합니다. 입력할 범위는 1~4294967295(asplain 표기법) 또는 1.0~65535.65535(asdot 표기법)입니다.

로컬 BGP 라우팅 프로세스 또는 원격 피어의 네트워크에서 자동 시스템 번호를 지정할 수 없습니다.

d) *options* 변수를 클릭하고 다음 중 하나를 선택합니다. 이 목록(**none** 이외)에서 항목을 선택할 경우 목록의 상위에 있는 모든 옵션도 선택됩니다. 이는 정상적인 결과로, 옵션은 완전히 독립적이지 않습니다.

- **none**. 다음 옵션은 구성하지 마십시오.
- **no-prepend**. 로컬 자동 시스템 번호를 eBGP 네이버에서 수신한 경로 앞에 추가하지 않습니다.
- **replace-as**. 실제 자동 시스템 번호를 eBGP 업데이트의 로컬 자동 시스템 번호로 교체합니다. 로컬 BGP 라우팅 프로세스에서의 자동 시스템 번호는 접두사로 추가되지 않습니다.
- **dual-as**. eBGP 네이버가 실제 자동 시스템 번호(로컬 BGP 라우팅 프로세스)를 사용하거나 로컬 자동 시스템 번호를 사용하여 피어링 세션을 설정하도록 eBGP 네이버를 구성합니다.

단계 **10** (선택 사항, IPv4 전용.) 네이버 고가용성(HA) 설정을 구성합니다.

HA 모드 설정은 **neighbor ha-mode graceful-restart** 명령을 구성합니다. 이 명령은 개별 BGP 네이버에 대한 Graceful Restart 기능을 활성화 또는 비활성화합니다. Graceful Restart가 이전에 BGP 피어에 대해 활성화된 경우 Graceful Restart 기능을 비활성화하려면 disable 키워드를 사용합니다.

Graceful Restart 기능은 세션 설정 중에 OPEN 메시지에서 NSF(Nonstop Forwarding) 지원 피어 및 NSF 인식 피어 간에 협상됩니다. BGP 세션이 설정된 후 Graceful Restart 기능을 활성화할 경우, 소프트 또는 하드 리셋으로 세션을 다시 시작해야 합니다.

HA 모드 설정은 개별 네이버에 대한 Graceful Restart를 구성합니다. 그 대신, BGP 전역 설정을 사용하여 모든 네이버에 대한 Graceful Restart를 활성화할 수 있습니다.

a) 이미 구성한 경우 **...** > **Duplicate(**중복**)(configure neighbor** *neighbor-address* **remote-as** *settings* 명령의 경우)를 클릭하거나 아직 사용 중이 아닌 경우 **+**를 클릭하여 활성화합니다. 명령을 볼 수 없는 경우 **Show Disabled(**비활성화된 항목 표시**)**를 클릭합니다.

b) *settings*를 클릭하고 **ha-mode**를 선택합니다.

c) Graceful Restart를 비활성화하려면 **neighbor ha-mode graceful-restart** 명령에서 *options*를 클릭하고 **disable**을 선택합니다. 이전의 비활성화 작업을 취소하려면 blank를 선택합니다.

단계 **11** (선택 사항). 네이버 활성화 옵션을 구성합니다.

새 네이버를 구성할 경우 기본적으로 활성화됩니다. 처음부터 네이버를 비활성화하려면, 활성화 설정을 활성화하거나 다른 활성화 설정을 구성해야 합니다.

a) **+**를 클릭하여 **configure neighbor** *neighbor-address* **activate** *activate-options* 명령을 활성화합니다. 명령을 볼 수 없는 경우 **Show Disabled(**비활성화된 항목 표시**)**를 클릭합니다.

b) *activate-options*를 클릭하고 **properties**를 선택합니다.

c) **neighbor** *neighbor-address* **activate** 명령은 활성화된 상태로 추가됩니다. **-**를 클릭하여 명령을 비활성화하고 네이버를 초기에 비활성화된 상태로 구성합니다. 네이버와 통신할 준비가 되면 이 개체를 수정하여 네이버를 활성화해야 합니다.

단계 **12** (선택 사항). 네이버 활성화 설정에서 필터링을 구성합니다.

a) 이미 구성한 경우 **...** > **Duplicate(**중복**)**(**configure neighbor** *neighbor-address* **activate** *settings* 명령의 경우)를 클릭하거나 아직 사용 중이 아닌 경우 **+**를 클릭하여 활성화합니다. 명령을 볼 수 없는 경우 **Show Disabled(**비활성화된 항목 표시**)**를 클릭합니다.

b) *settings*를 클릭하고 **filtering**를 선택합니다.

c) 다음과 같은 네이버 명령의 조합을 사용하여 이 네이버를 통해 수신되거나 이 네이버로 전송된 접두사를 제어할 수 있는 필터링을 구성합니다. **-**를 클릭하여 사용하지 않을 항목을 비활성화합니다. 이러한 모든 명령은 인바운드 및 아웃바운드 방향 양쪽에서 필터링을 허용합니다. 양쪽 방향을 모두 구성하려면 명령에 대해 **...** > **Duplicate(**중복**)**를 클릭합니다.

neighbor distribute-list 및 **neighbor prefix-list** 명령 두 가지 모두를 같은 방향의 네이버에 적용하지 마십시오. 이러한 두 가지 명령은 함께 사용할 수 없으며, 둘 중 하나만 각 인바운드 또는 아웃바운드 방향에 적용할 수 있습니다.

- **distribute-list** *acl options*. (IPv4 전용) 선택한 표준 액세스 목록(ACL)을 기준으로 접두사를 필터링합니다. 그런 다음, *options*를 클릭하고 필터를 **in** 방향으로 적용할지 또는 **out** 방향으로 적용할지 선택합니다.
- **route-map** *route-map options*. 선택한 경로 맵을 기준으로 접두사를 필터링합니다. 그런 다음, *options*를 클릭하고 필터를 **in** 방향으로 적용할지 또는 **out** 방향으로 적용할지 선택합니다. 경로 맵 내에서 액세스 목록, AS 경로, 접두사, 배포 목록을 기준으로 필터링을 구성할 수 있습니다.
- **prefix-list** *prefix-list options*. 선택한 IPv4 또는 IPv6 접두사 목록을 기준으로 접두사를 필터링합니다. 그런 다음, *options*를 클릭하고 필터를 **in** 방향으로 적용할지 또는 **out** 방향으로 적용할지 선택합니다.
- **filter-list** *as-path options*. 선택한 AS 경로 필터 개체를 기준으로 접두사를 필터링합니다. 그런 다음, *options*를 클릭하고 필터를 **in** 방향으로 적용할지 또는 **out** 방향으로 적용할지 선택합니다.

d) **configure prefix-limit neighbor** *neighbor-address limit-options* 명령에서 *limit-options*를 클릭하고 다음 중 하나를 선택하거나, **-**를 클릭하여 명령을 비활성화합니다. 옵션을 선택하면 구성해야 할 추가 옵션과 함께 일부 **neighbor maximum-prefix** 명령 형식이 추가됩니다. 이 명령을 사용하여 네이버에서 수신할 수 있는 접두사 수를 제어합니다.

- **none**. 추가 파라미터 없이 명령의 기본 형식을 구성합니다. 변수를 클릭하고 다음 값을 구성합니다.
  - max-prefix-limit. 이 네이버에서 허용되는 최대 접두사 수(1~2147483647)입니다. 다른 옵션을 선택할 경우에도 이 변수를 구성해야 합니다.
  - **75** (임계값). 라우터가 경고 메시지 생성을 시작할 최대 비율(1~100)입니다. 기본값은 75%입니다.
- **restart**. 한계에 도달하면 네이버와의 피어링 세션을 중지합니다. *restart-interval* 변수를 클릭하고, 세션을 다시 시작하기 전까지 시스템이 대기해야 하는 시간(1~65535분)을 구성합니다.
- **warning-only**. 한계에 도달해도 세션을 중지하지 않습니다. 그 대신, 경고 시스템 로그 메시지를 표시하고 세션을 계속 진행합니다.

단계 **13** (선택 사항). 네이버 활성화 설정에서 경로를 구성합니다.

a) 이미 구성한 경우 **...** > **Duplicate(**중복**)(configure neighbor** *neighbor-address* **activate** *settings* 명령의 경우)를 클릭하거나 아직 사용 중이 아닌 경우 **+**를 클릭하여 활성화합니다. 명령을 볼 수 없는 경우 **Show Disabled(**비활성화된 항목 표시**)**를 클릭합니다.

b) *settings*를 클릭하고 **routes**를 선택합니다.

c) **neighbor advertisement-interval** 명령에서 *value* 변수를 클릭하고 경로 업데이트를 이 네이버로 전송하는 최소 경로 광고 간격(0~600초)을 입력합니다. 또는 **-**를 클릭하여 명령을 비활성화하고 가상 라우터에 있는 iBGP 및 eBGP 세션에 대해 해당 간격을 기본값 0으로 두거나, 가상 라우터에 없는 eBGP 세션에 대해 30으로 설정합니다. 값 0은 라우팅 테이블이 변경될 때마다 빈도에 상관없이 시스템에서 업데이트를 전송한다는 것을 의미합니다.

d) **neighbor advertise-map** 명령에서 다음 옵션을 구성하여 선택한 경로를 네이버에 조건부로 광고하도록 하거나, **-**를 클릭하여 명령을 비활성화하여 모든 경로 업데이트를 네이버에 조건 없이 전송하도록 합니다.

조건부로 광고할 경로(접두사)는 두 개의 경로 맵(advertise map 및 exist map 또는 non-exist map)에서 정의됩니다.

exist map 또는 non-exist map과 연결된 경로 맵은 BGP 스피커가 추적하는 접두사를 지정합니다.

advertise map과 연결된 경로 맵은 조건이 충족될 때 지정된 네이버로 광고할 접두사를 지정합니다.

exist map을 구성하면, advertise map과 exist map에 모두 접두사가 존재하는 경우 조건이 충족됩니다.

non-exist map을 구성하면, advertise map에는 접두사가 존재하지만 non-exist map에는 존재하지 않는 경우 조건이 충족됩니다.

조건이 충족되지 않으면 경로가 취소되고 조건부 광고가 발생하지 않습니다. 조건부 광고가 발생하려면 동적으로 광고 여부를 결정할 수 있는 모든 경로가 BGP 라우팅 테이블에 존재해야 합니다.

- *advertise-route-map*. 이 변수를 클릭하고 exist map 또는 non-exist map의 조건이 충족된 경우 어떤 경로를 광고할지 정의하는 경로 맵을 선택합니다.
- *options condition-route-map*. options를 클릭하고 다음 중 하나를 선택합니다.
  - **exist-map**. 변수를 클릭하고 exist 경로 맵을 선택합니다.
  - **non-exist-map**. 변수를 클릭하고 non-exist 경로 맵을 선택합니다.

e) **neighbor** *neighbor-address* **remove-private-as** 명령은 활성화된 상태로 추가됩니다. 명령을 비활성화하려면 **-**를 클릭합니다. 이 명령은 eBGP 아웃바운드 라우팅 업데이트에서 비공개 자동 시스템 번호를 제거합니다. 비공개 AS 값의 범위는 64512~65535입니다.

f) **configure neighbor default-originate** 명령에서 *options*를 클릭하고 다음 중 하나를 선택하거나, **-**를 클릭하여 명령을 비활성화합니다.

- **none**. 시스템에서 네이버에 기본 경로를 조건 없이 전송하도록 허용합니다.

- **route-map**. 시스템에서 네이버에 기본 경로를 조건부로 전송하도록 합니다. 경로 맵과 함께 사용할 경우, 경로 맵에 일치하는 IP 주소 구문이 포함되어 있고 IP 액세스 목록과 정확히 일치하는 경로가 있으면 기본 경로가 삽입됩니다. 경로 맵에서 표준 또는 확장 액세스 목록을 사용하여 기본 경로를 정의할 수 있습니다. **neighbor default-originate** 명령에서 개체에 추가된 *route-map* 변수를 클릭하고 경로 맵을 선택해야 합니다.

단계 **14** (선택 사항). 네이버 활성화 설정에서 타이머를 구성합니다.

네이버에 대한 타이머를 구성할 경우, 설정은 전역 BGP 설정의 모든 BGP 네이버에 구성된 타이머를 재정의합니다.

a) 이미 구성한 경우 **...** > **Duplicate(**중복**)**(**configure neighbor** *neighbor-address* **activate** *settings* 명령의 경우)를 클릭하거나 아직 사용 중이 아닌 경우 **+**를 클릭하여 활성화합니다. 명령을 볼 수 없는 경우 **Show Disabled(**비활성화된 항목 표시**)**를 클릭합니다.

b) *settings*를 클릭하고 **timers**를 선택합니다.

c) **neighbors timers** 명령에서 다음 변수를 구성합니다.

- *keepalive-interval*. 시스템이 keepalive 메시지를 이 네이버에 전송하는 빈도(0~65535초)입니다. 이 명령을 구성하지 않으면 기본값은 60초입니다.
- *hold-time*. keepalive 메시지를 수신하지 않아 시스템에서 이 네이버를 dead로 선언하는 간격(0~65535초)입니다. 이 명령을 구성하지 않으면 기본값은 180초입니다.
- **0** (최소 보류 시간). 이 네이버에서 구성할 수 있는 최소 허용 보류 시간(0~65535초)입니다. 이 값은 이 시스템에 구성된 보류 시간보다 작거나 같아야 합니다. 네이버의 보류 시간이 이 값보다 작을 경우, 시스템에서 네이버에 BGP 세션을 설정하지 않습니다.

단계 **15** (선택 사항). 고급 네이버 활성화 설정을 구성합니다.

a) 이미 구성한 경우 **...** > **Duplicate(**중복**)**(**configure neighbor** *neighbor-address* **activate** *settings* 명령의 경우)를 클릭하거나 아직 사용 중이 아닌 경우 **+**를 클릭하여 활성화합니다. 명령을 볼 수 없는 경우 **Show Disabled(**비활성화된 항목 표시**)**를 클릭합니다.

b) *settings*를 클릭하고 **advanced**를 선택합니다.

c) 다음 **neighbor** 명령 중 활성화된 상태로 유지할 명령을 결정합니다. 원치 않는 옵션을 비활성화하려면 **-**를 클릭합니다.

- **send-community**. 커뮤니티 속성을 네이버에 전송합니다.
- **weight** *value*. 변수를 클릭하여 초기 가중치(0~65535초)를 이 네이버에서 학습된 경로에 할당합니다. 이 명령을 구성하지 않을 경우, 또 다른 BGP 피어를 통해 학습된 경로의 기본 가중치는 0이고, 로컬 라우터에서 소싱된 경로의 기본 가중치는 32768입니다. 그러나 경로 맵을 사용하여 설정된 경로 가중치는 이 명령을 사용하여 구성된 가중치를 재정의합니다.
- **next-hop-self**. 라우터를 BGP 발신 네이버에 대한 다음 홉으로 구성합니다. 이 명령은 BGP 네이버가 동일한 IP 서브넷의 다른 모든 네이버에 직접 액세스하지 못할 수 있는 unmeshed 네트워크(예: Frame Relay 또는 X.25)에서 유용합니다.

단계 **16** **...** > **Duplicate(**중복**)**(**configure neighbor** 명령 옆)를 클릭하여 다른 네이버를 정의할 수 있습니다. 필요한 개수만큼 정의합니다.

단계 **17** **OK(**확인**)**를 클릭합니다.

다른 라우팅 프로토콜에서 **BGP** 경로 재배포 구성

다른 라우팅 프로토콜, 연결된 경로, 정적 경로에서 BGP 프로세스로 경로를 재배포하는 작업을 제어할 수 있습니다.

시작하기 전에

BGP에 재배포를 구성하기 전에, 경로를 재배포할 라우팅 프로세스를 구성하고 변경 사항을 구축하는 것이 좋습니다.

경로 맵을 적용하여 재배포되는 경로를 세부적으로 조정하려면 스마트 CLI 경로 맵 개체를 생성합니다. 경로 맵과 일치하는 경로가 재배포되며, 일치하지 않는 모든 경로는 재배포되지 않습니다.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음, **Routing(**라우팅**)** 요약을 클릭합니다.

단계 **2** 가상 라우터를 활성화한 경우 BGP를 구성 중인 라우터의 보기 아이콘( )을 클릭합니다.

단계 **3** **BGP** 탭을 클릭합니다.

단계 **4** BGP 프로세스 개체를 추가하거나 수정합니다.

재배포 명령은 **configure address family ipv4** 또는 **ipv6** 명령 아래에 있는 명령 세트 내에 있습니다. 재배포를 구성하려면 주소 패밀리를 구성해야 합니다.

단계 **5** **Show Disabled(**비활성화된 항목 표시**)**를 클릭하여 모든 명령을 표시한 다음, **+**를 클릭하여 **configure ipv4/ipv6 redistribution** 명령을 활성화합니다.

단계 **6** *protocol* 변수를 클릭하고 경로를 재배포할 소스 프로세스를 선택합니다. **connected** 및 **static** 경로를 재배포하거나 **eigrp**(IPv4 전용), **isis**, **ospf** 또는 **rip**(IPv4 전용)에 의해 생성된 경로를 재배포할 수 있습니다.

단계 **7** 라우팅 프로세스를 선택할 경우, *identifier* 변수를 클릭하고 필요한 값을 입력합니다.

- **eigrp**. 자동 시스템 번호를 입력합니다.
- **ospf**. 프로세스 ID 번호를 입력합니다.
- **connected**, **static**, **isis**, **rip**. **none**을 입력합니다. 다른 값을 입력할 경우 해당 값은 무시됩니다.

단계 **8** (선택 사항, IS-IS 전용.) **redistribute isis level-2** 명령에서 **level-2**를 클릭하고 학습한 경로를 IS-IS 영역(**level-1**) 내에서만 재배포할지, IS-IS 영역(**level-2**) 간에 재배포할지, 또는 두 영역 모두(**level-1-2**)에서 재배포할지 선택합니다.

단계 **9** (선택 사항, 모든 프로토콜.) 재배포된 경로에 대한 메트릭을 세부적으로 조정하려면 **+**를 클릭하여 다음 명령을 활성화하고 옵션을 구성합니다.

redistribute *protocol* **metric** *metric-value*

변수를 클릭하고 배포할 경로의 메트릭 값(0~4294967295)을 입력합니다.

단계 **10** (선택 사항, 모든 프로토콜.) 경로 맵을 기준으로 재배포되는 경로를 세부적으로 조정하려면 **+**를 클릭하여 **redistribute route-map** 명령을 활성화하고 변수를 클릭한 후 제한 사항을 정의하는 경로 맵을 선택합니다.

경로 맵을 적용하지 않을 경우, 해당 프로세스에 대한 모든 경로(재배포를 위해 구성된 다른 명령에 적합함)가 재배포됩니다.

단계 **11** (선택 사항, OSPF 전용.) 다음 명령은 OSPF 프로세스에서 경로를 재배포할 때 기본적으로 활성화됩니다. **-**를 클릭하여 원치 않는 명령을 비활성화할 수 있습니다.

이러한 명령은 OSPF 경로가 다른 라우팅 도메인에 재배포되는 기준을 지정합니다.

- **redistribute ospf match external 1**. 자동 시스템의 외부에 있지만, OSPF에 Type 1 외부 경로로서 가져온 경로입니다.
- **redistribute ospf match external 2**. 자동 시스템의 외부에 있지만, OSPF에 Type 2 외부 경로로서 가져온 경로입니다.
- **redistribute ospf match internal**. 특정 자동 시스템의 내부에 있는 경로입니다.
- **redistribute ospf match nssa-external 1**. 자동 시스템의 외부에 있지만, OSPF에 Type 1 외부 경로로서 가져온 경로이며 NSSA(Not-So-Stubby-Area)로만 표시됩니다.
- **redistribute ospf match nssa-external 2**. 자동 시스템의 외부에 있지만, OSPF에 Type 2 외부 경로로서 가져온 경로이며 NSSA(Not-So-Stubby-Area)로만 표시됩니다.

단계 **12** **...** > **Duplicate(**중복**)(configure redistribution** 명령 옆)를 클릭하여 다른 프로토콜에 대한 재배포를 구성할 수 있습니다. 해당 네트워크에 적합한 각 프로토콜에 대해 재배포를 구성합니다.

단계 **13** **OK(**확인**)**를 클릭합니다.

BGP 모니터링

BGP를 모니터링하고 트러블슈팅하려면 CLI 콘솔을 열거나 디바이스 CLI에 로그인하여 다음 명령을 사용합니다. Routing(라우팅) 페이지의 **Commands(**명령**)** 메뉴에서 이러한 명령 중 일부를 선택할 수도 있습니다.

show bgp ?를 사용하여 추가 옵션 목록을 가져옵니다. 예를 들어, 자율 시스템 번호 및 가상 라우터를 지정하여 표시되는 정보를 제한할 수 있으며 원하는 정보만 대상으로 하는 기타 옵션을 지정할 수 있습니다. 다음 목록은 요약입니다.

- **show bgp**

  BGP 라우팅 테이블의 엔트리를 표시합니다.

- **show bgp cidr-only**

  비자연 네트워크 마스크가 있는 경로(CIDR, 즉 Classless Interdomain Routing)를 표시합니다.

- **show bgp community**

  지정된 BGP 커뮤니티에 속하는 경로를 표시합니다.

- **show bgp community-list**

  BGP 커뮤니티 목록에서 허용하는 경로를 표시합니다.

- **show bgp filter-list** *access-list-number*

  지정된 필터 목록에 순응하는 경로를 표시합니다.

- **show bgp injected-paths**

  BGP 라우팅 테이블의 모든 삽입된 경로를 표시합니다.

- **show bgp ipv4 unicast**

  유니캐스트 세션에 대한 IPv4(IP version 4) BGP 라우팅 테이블의 엔트리를 표시합니다.

- **show bgp ipv6 unicast**

  IPv6 BGP 라우팅 테이블의 항목을 표시합니다.

- **show bgp neighbors**

  네이버에 대한 BGP 및 TCP 연결에 관한 정보를 표시합니다.

- **show bgp paths**

  데이터베이스의 모든 BGP 경로를 표시합니다.

- **show bgp prefix-list**

  접두사 목록 또는 접두사 목록 항목에 대한 정보를 표시합니다.

- **show bgp regexp** *regexp*

  자율 시스템 경로 정규식과 일치하는 경로를 표시합니다.

- **show bgp rib-failure**

  RIB(Routing Information Base) 테이블에서 설치에 실패한 BGP 경로를 표시합니다.

- **show bgp summary**

  모든 BGP 연결의 상태를 표시합니다.

- **show bgp update-group**

  BGP 업데이트 그룹에 대한 정보를 표시합니다.

V 부

보안 정책

18 장

SSL 암호 해독

HTTPS와 같은 일부 프로토콜은 SSL(Secure Sockets Layer) 또는 그 후속 버전인 TLS(Transport Layer Security)를 사용하여 안전한 전송을 위해 트래픽을 암호화합니다. 시스템에서는 암호화된 연결을 검사할 수 없으므로 상위 레이어의 트래픽 특성을 고려하여 액세스 의사 결정을 내리는 액세스 규칙을 적용하려면 암호를 해독해야 합니다.

SSL 암호 해독 정보

일반적으로 연결은 액세스 제어 정책을 통해 허용되는지 아니면 차단되는지가 결정됩니다. 그러나 SSL 암호 해독 정책을 활성화하는 경우에는 암호화된 연결이 가장 먼저 SSL 암호 해독 정책을 통해 암호가 해독되어야 하는지 아니면 차단되어야 하는지가 결정됩니다. 암호 해독 여부와 관계없이 차단 해제된 연결은 모두 액세스 제어 정책을 통해 최종 허용/차단 여부가 결정됩니다.

참고 ID 정책에서 활성 인증 규칙을 구현하려면 SSL 암호 해독 정책을 활성화해야 합니다. SSL 암호 해독을 활성화하여 ID 정책을 활성화하되 다른 방법으로는 SSL 암호 해독을 구현하지 않으려는 경우에는 Do Not Decrypt(암호 해독 안 함)를 기본 작업으로 선택하고 추가 SSL 암호 해독 규칙을 생성하지 마십시오. ID 정책은 필요한 규칙이라면 무엇이든 자동으로 생성합니다.

다음 주제에서는 암호화된 트래픽 플로우 관리 및 암호 해독에 대해 자세히 설명합니다.

SSL 암호 해독을 구현하는 이유

HTTPS 연결과 같이 암호화된 트래픽은 검사할 수 없습니다.

은행 및 기타 금융 기관에 대한 연결 등 많은 연결이 합법적으로 암호화되어 있으며, 많은 웹 사이트에서 암호화를 사용하여 개인 정보 또는 민감한 데이터를 보호합니다. 예를 들어 device manager에 대한 연결은 암호화됩니다.

그러나 사용자는 암호화된 연결 내에서 부적절한 트래픽을 숨길 수도 있습니다.

SSL 암호 해독을 구현함으로써 연결을 암호 해독하고, 연결에 위협 또는 다른 부적절한 트래픽이 포함되어 있지 않은지 검사한 다음, 연결을 계속하도록 허용하기 전에 재암호화할 수 있습니다. 암호 해독된 트래픽은 액세스 제어 정책을 통과하고 암호 해독된 연결의 검사받은 특성(암호화된 특성 아님)을 기반으로 하는 규칙과 일치합니다. 따라서 액세스 제어 정책을 적용해야 하는 필요와 민감한 정보를 보호해야 하는 사용자의 필요 간의 균형을 유지할 수 있습니다.

또한, 네트워크에 원하지 않는 유형의 암호화된 트래픽을 차단하기 위해 SSL 암호 해독 규칙을 구성할 수 있습니다.

트래픽을 암호 해독한 다음 재암호화하면 디바이스의 처리 부하가 증가하므로 전체 시스템 성능이 감소된다는 점에 유의하십시오.

암호화된 트래픽에 적용할 수 있는 작업

SSL 암호 해독 규칙을 구성할 때 다음 주제에 설명된 작업을 적용할 수 있습니다. 이러한 작업은 명시적인 규칙과 일치하지 않는 모든 트래픽에 적용되는 기본 작업에도 사용할 수 있습니다.

참고 SSL 암호 해독 정책을 통과하는 모든 트래픽은 이후에 액세스 제어 정책을 통과해야 합니다. SSL 암호 해독 정책에서 삭제하는 트래픽을 제외하고는 액세스 제어 정책에 따라 최종 허용/삭제 여부가 결정됩니다.

재서명 암호 해독

트래픽 암호 해독 및 재서명을 선택하는 경우, 시스템이 MITM(Man-In-The-Middle) 역할을 합니다.

브라우저에서 https://www.cisco.com의 사용자 유형을 예로 들 수 있습니다. 트래픽이 threat defense 디바이스에 도달하면 디바이스에서는 규칙에 지정된 CA 인증서를 사용하는 사용자와 협상하며 사용자와 threat defense 디바이스 간에 SSL 터널을 구축합니다. 동시에 이 디바이스에서는 https://www.cisco.com에 접속하여 서버와 threat defense 디바이스 간에 SSL 터널을 생성합니다.

따라서 사용자는 www.cisco.com에서 인증서 대신 SSL 암호 해독 규칙에 대해 구성된 CA 인증서를 보게 됩니다. 연결을 완료하려면 사용자가 인증서를 신뢰해야 합니다. 그러면 threat defense 디바이스에서는 사용자와 대상 서버 간의 양방향 트래픽에서 암호 해독/재암호화를 수행합니다.

참고 클라이언트가 서버 인증서 재서명에 쓰이는 CA를 신뢰하지 않을 경우 신뢰할 수 없는 인증서임을 사용자에게 경고합니다. 이를 방지하려면 클라이언트가 신뢰하는 CA 저장소에 CA 인증서를 가져오십시오. 또는 조직에 개인 PKI가 있을 경우, 조직의 모든 클라이언트가 자동으로 신뢰하는 루트 CA에 의해 서명된 중간 CA 인증서를 발급한 다음 그 CA 인증서를 디바이스에 업로드할 수 있습니다.

재서명 암호 해독 작업으로 규칙을 구성할 경우 이 규칙은 구성된 규칙 조건과 더불어 참조된 내부 CA 인증서의 서명 알고리즘 유형을 기반으로 트래픽을 일치시킵니다. SSL 암호 해독 정책용 단일 재서명 인증서를 선택할 수 있으므로 이 경우 재서명 규칙에 대한 트래픽 일치를 제한할 수 있습니다.

예를 들어, 재서명 인증서가 EC(Elliptic Curve) 기반 CA 인증서인 경우에만 EC 알고리즘을 사용하여 암호화된 발신 트래픽이 재서명 암호 해독 규칙과 일치합니다. 이와 유사하게 글로벌 재서명 인증서가 RSA인 경우에만 RSA 알고리즘을 사용하여 암호화된 트래픽이 재서명 암호 해독 규칙과 일치합니다. 즉, 구성된 다른 모든 규칙 조건이 일치하더라도 EC 알고리즘을 사용하여 암호화된 발신 트래픽은 이 규칙과 일치하지 않습니다.

알려진 키 암호 해독

목적지 서버를 소유하고 있는 경우 알려진 키를 사용하여 암호 해독을 구현할 수 있습니다. 이 경우 사용자가 https://www.cisco.com에 대한 연결을 열면 인증서를 제시하는 threat defense 디바이스인 경우에도 www.cisco.com에 대한 실제 인증서가 사용자에게 표시됩니다.

소속된 조직은 도메인 및 인증서의 소유자여야 합니다. cisco.com을 예로 드는 경우, 엔드 유저가 Cisco 인증서를 확인할 수 있으려면 실제로 cisco.com 도메인을 소유(즉, 엔드 유저가 Cisco Systems)하고 공용 CA에서 서명한 cisco.com 인증서의 소유권을 갖고 있어야만 합니다. 조직이 소유한 사이트에 대해 알려진 키를 사용해야만 암호를 해독할 수 있습니다.

알려진 키로 암호 해독을 수행하는 주요 목적은 HTTPS 서버로 향하는 트래픽을 암호 해독하여 외부 공격으로부터 서버를 보호하는 것입니다. 외부 HTTPS 사이트에 대한 클라이언트 측 트래픽을 검사하기 위해서는 서버를 소유하고 있지 않으므로 재서명 암호 해독을 사용해야 합니다.

참고 알려진 키 암호 해독을 사용하려면 서버 인증서 및 키를 내부 ID 인증서로 업로드한 다음 SSL 암호 해독 정책 설정에서 알려진 키 인증서 목록에 추가해야 합니다. 그러면 서버 주소를 대상 주소로 사용하여 알려진 키 암호 해독에 대한 규칙을 작성할 수 있습니다. SSL 암호 해독 정책에 인증서를 추가하는 데 대한 자세한 내용은 알려진 키 및 재서명 암호 해독을 위한 인증서 구성, 483 페이지를 참조하십시오.

암호 해독 안 함

특정 유형의 트래픽은 암호 해독을 우회하도록 선택하는 경우, 해당 트래픽에는 처리 작업이 수행되지 않습니다. 암호화된 트래픽은 일치하는 액세스 제어 규칙을 기반으로 허용 또는 차단되는 액세스 제어 정책으로 계속 진행됩니다.

차단

SSL 암호 해독 규칙과 일치하는 암호화된 트래픽을 간단하게 차단할 수 있습니다. SSL 암호 해독 정책에서 차단 기능을 사용하면 액세스 제어 정책에 연결할 수 없게 됩니다.

HTTPS 연결을 차단하는 경우 사용자에게 시스템 기본 차단 응답 페이지가 표시되지 않습니다. 대신 보안 연결 실패를 나타내는 브라우저의 기본 페이지가 표시됩니다. 오류 메시지는 사이트가 정책으로 인해 차단되었음을 나타내지 않습니다. 대신 일반적인 암호화 알고리즘이 없다는 오류가 표시될 수 있습니다. 이 메시지만으로는 연결이 의도적으로 차단되었는지를 명확하게 파악할 수 없습니다.

자동 생성된 **SSL** 암호 해독 규칙

SSL 암호 해독 정책의 활성화 여부와 관계없이, 시스템은 활성 인증을 구현하는 각 ID 정책 규칙에 대해 재서명 암호 해독 규칙을 자동으로 생성합니다. 이 작업은 HTTPS 연결에 대한 활성 인증을 활성화하는 데 필요합니다.

SSL 암호 해독 정책을 활성화하면 Identity Policy Active Authentication Rules(ID 정책 활성 인증 규칙) 머리글 아래에서 이 규칙을 확인할 수 있습니다. 이러한 규칙은 SSL 암호 해독 정책 상단에 읽기 전용으로 그룹화되어 있습니다. ID 정책을 변경해야만 규칙을 변경할 수 있습니다.

암호 해독이 불가능한 트래픽 처리

연결의 암호 해독이 불가능하게 만드는 몇 가지 특성이 있습니다. 연결에 다음 특성이 있는 경우, 연결이 다른 방법으로 일치할 수 있는 어떤 규칙과도 관계없이 기본 작업이 연결에 적용됩니다. 암호 해독 안 함 대신 차단을 기본 작업으로 선택하는 경우, 합법적인 트래픽의 과도한 삭제를 포함한 문제가 발생할 수 있습니다.

- 압축된 세션 — 데이터 압축이 연결에 적용되었습니다.
- SSLv2 세션 — 지원되는 최소 SSL 버전은 SSLv3입니다.
- 알려지지 않은 암호 그룹 — 시스템에서 연결에 대한 암호 그룹을 인식하지 않습니다.

- 지원되지 않는 암호 그룹 — 시스템에서 탐지된 암호 그룹을 기반으로 암호 해독을 지원하지 않습니다.
- 세션이 캐시되지 않음 — SSL 세션에서 세션 재사용이 활성화되었고 클라이언트 및 서버가 세션 식별자로 세션을 재설정했으며 시스템에서 해당 세션 식별자를 캐시하지 않았습니다.
- 핸드셰이크 오류 — SSL 핸드셰이크 협상 중에 오류가 발생했습니다.
- 암호 해독 오류 — 암호 해독 작업 중에 오류가 발생했습니다.
- 패시브 인터페이스 트래픽 — 패시브 인터페이스(패시브 보안 영역)의 모든 트래픽은 암호 해독할 수 없습니다.

SSL 암호 해독을 위한 라이선스 요건

SSL 암호 해독 정책을 사용하는 데에는 특수 라이선스가 필요하지 않습니다.

그러나 URL 카테고리 및 평판을 일치 기준으로 사용하는 규칙을 생성하려면 **URL** 라이선스가 필요합니다. 라이선스 구성에 대한 자세한 내용은 선택 가능한 라이선스 활성화 또는 비활성화, 98 페이지를 참조하십시오.

SSL 암호 해독에 대한 지침

SSL 암호 해독 정책을 구성하고 모니터링할 때는 다음 사항에 유의하십시오.

- 액세스 제어 규칙이 다음에 해당할 때 신뢰 또는 차단으로 설정된 규칙과 일치하는 연결의 경우 SSL 암호 해독 정책이 우회됩니다.
  - 보안 영역, 네트워크, 지리위치 및 포트를 트래픽 일치 기준으로만 사용하는 경우.
  - 검사가 필요한 다른 규칙(예: 애플리케이션이나 URL을 기준으로 하는 연결과 일치하는 규칙) 앞에 오거나 침입 또는 파일 검사를 적용하는 규칙을 허용하는 경우.
- URL 카테고리 일치를 사용할 때는 사이트의 로그인 페이지가 사이트 자체의 카테고리와 다른 카테고리에 포함되는 경우가 있음을 고려해야 합니다. 예를 들어 Gmail은 "웹 기반 이메일" 카테고리에 포함되지만 로그인 페이지는 "인터넷 포털" 카테고리에 포함됩니다. 이러한 사이트에 대한 연결을 암호 해독하려면 두 카테고리를 모두 규칙에 포함해야 합니다.
- VDB(Vulnerability Database) 업데이트에서 사용되지 않는 애플리케이션을 제거하는 경우, 삭제된 애플리케이션을 사용하는 SSL 암호 해독 규칙 또는 애플리케이션 필터를 변경해야 합니다. 이러한 규칙을 수정할 때까지는 변경 사항을 구축할 수 없습니다. 또한 문제를 해결하기 전에는 시스템 소프트웨어 업데이트를 설치할 수 없습니다. Application Filters(애플리케이션 필터) 개체 페이지 또는 규칙의 Application(애플리케이션) 탭에서는 이러한 애플리케이션 이름 뒤에 "(사용되지 않음)"이라고 표시됩니다.

- 활성 인증 규칙이 있는 경우에는 SSL 암호 해독 정책을 비활성화할 수 없습니다. SSL 암호 해독 정책을 비활성화하려면 ID 정책을 비활성화하거나 활성 인증을 사용하는 ID 규칙을 삭제해야 합니다.

SSL 암호 해독 정책을 구현 및 유지 관리하는 방법

SSL 암호 해독 정책을 사용하여 암호화된 트래픽을 일반 텍스트 트래픽으로 전환할 수 있으므로 URL 필터링, 침입 및 악성코드 제어 그리고 기타 서비스(DPI(Deep Packet Inspection)를 필요로 함)를 적용할 수 있습니다. 정책에서 트래픽을 허용하는 경우, 트래픽은 디바이스를 떠나기 전에 다시 암호화됩니다.

SSL 암호 해독 정책은 암호화된 트래픽에만 적용됩니다. 암호화되지 않은 연결은 SSL 암호 해독 규칙을 기준으로 평가되지 않습니다.

일부 다른 보안 정책과 달리 SSL 암호 해독 정책은 인증서가 만료되거나 목적지 서버에서 변경될 수 있기 때문에 적극적으로 모니터링하고 유지 관리해야 합니다. 또한, MITM(Man-In-The-Middle) 공격과 재서명 암호 해독 작업은 구분할 수 없기 때문에 클라이언트 소프트웨어의 변경 사항에 따라 특정 연결을 암호 해독하는 능력이 변경될 수 있습니다.

다음 절차에서는 SSL 암호 해독 정책을 구현하고 유지 관리하는 엔드 투 엔드 프로세스에 대해 설명합니다.

프로시저

단계 **1** 재서명 암호 해독 규칙을 구현할 경우 필요한 내부 CA 인증서를 생성합니다.

내부 CA(인증 기관) 인증서를 사용해야 합니다. 다음과 같은 옵션이 있습니다. 사용자가 인증서를 신뢰해야 하므로 클라이언트 브라우저가 이미 신뢰하도록 구성되어 있는 인증서를 업로드하거나 업로드하는 인증서가 브라우저의 신뢰 저장소에 추가되어 있는지 확인합니다.

- 디바이스 자체에서 서명한 자체 서명 내부 CA 인증서를 생성합니다. 자체 서명 내부 및 내부 CA 인증서 생성, 167 페이지의 내용을 참조하십시오.
- 외부 신뢰 CA 또는 조직 내부의 CA에서 서명한 키와 내부 CA 인증서를 업로드합니다. 내부 및 내부 CA 인증서 업로드, 165 페이지의 내용을 참조하십시오.

단계 **2** 알려진 키 암호 해독 규칙을 구현할 경우, 각 내부 서버에서 인증서와 키를 수집합니다.

서버에서 인증서와 키를 얻어야 하므로 알려진 키 암호 해독은 제어하고 있는 서버에만 사용할 수 있습니다. 이러한 인증서와 키를 내부 인증서(내부 CA 인증서 아님)로 업로드합니다. 내부 및 내부 CA 인증서 업로드, 165 페이지의 내용을 참조하십시오.

단계 **3** SSL 암호 해독 정책 활성화, 473 페이지.

정책을 활성화하는 경우 몇 가지 기본 설정도 구성합니다.

단계 **4** 기본 SSL 암호 해독 작업 구성, 474 페이지.

의심스러운 경우에는 **Do Not Decrypt(**암호 해독 안 함**)**를 기본 동작으로 선택합니다. 액세스 제어 정책은 여전히 필요한 경우 기본 SSL 암호 해독 규칙과 일치하는 트래픽을 삭제할 수 있습니다.

단계 **5** SSL 암호 해독 규칙 구성, 475 페이지.

암호 해독할 트래픽과 적용할 암호 해독 유형을 확인합니다.

단계 **6** 알려진 키 암호 해독을 구성하는 경우 SSL 암호 해독 정책 설정을 편집하여 해당 인증서를 포함합니다. 알려진 키 및 재서명 암호 해독을 위한 인증서 구성, 483 페이지의 내용을 참조하십시오.

단계 **7** 필요시 재서명 암호 해독 규칙에 사용된 CA 인증서를 다운로드하고 클라이언트 워크스테이션에서 브라우저에 업로드합니다.

인증서를 다운로드하고 클라이언트에게 배포하는 데 대한 자세한 내용은 재서명 암호 해독 규칙을 위한 CA 인증서 다운로드, 484 페이지를 참조하십시오.

단계 **8** 주기적으로 재서명 및 알려진 키 인증서를 업데이트합니다.

- 재서명 인증서 - 만료되기 전에 이 인증서를 업데이트합니다. device manager를 통해 인증서를 생성하는 경우, 유효 기간은 5년입니다. 인증서의 유효 기간을 확인하려면 **Objects(**개체**)** > **Certificates(**인증서**)**를 선택하고 목록에서 인증서를 찾은 다음 Actions(작업) 열에서 이에 대한 정보 아이콘( )을 클릭합니다. 정보 대화 상자에는 유효 기간 및 몇 가지 기타 특성이 표시됩니다. 이 페이지에서 대체 인증서를 업로드할 수도 있습니다.
- 알려진 키 인증서 - 모든 알려진 키 암호 해독 규칙의 경우, 목적지 서버의 현재 인증서와 키를 업로드했는지 확인해야 합니다. 또한, 지원되는 서버에서 인증서와 키가 변경될 때마다 새 인증서와 키를 내부 인증서로 업로드하고 새 인증서를 사용하도록 SSL 암호 해독 설정을 업데이트해야 합니다.

단계 **9** 외부 서버에 대해 누락된, 신뢰할 수 있는 CA 인증서를 업로드합니다.

시스템에는 신뢰할 수 있는 CA 루트 및 중간 인증서(서드파티에서 발급)가 다양하게 포함되어 있습니다. 이러한 항목은 암호 해독 재서명 규칙에 대해 threat defense과(와) 대상 서버 간의 연결을 협상할 때 필요합니다.

루트 CA의 트러스트 체인 내의 모든 인증서를 신뢰할 수 있는 CA 인증서 목록에 업로드하며, 여기에는 루트 CA 인증서 및 모든 중간 CA 인증서가 포함됩니다. 이렇게 하지 않으면 중간 CA가 발급한 신뢰할 수 있는 인증서를 탐지하는 것이 더 어려워집니다. **Objects(**개체**)** > **Certificates(**인증서**)** 페이지에서 인증서를 업로드합니다. 신뢰할 수 있는 CA 인증서 업로드, 169 페이지의 내용을 참조하십시오.

SSL 암호 해독 정책 구성

SSL 암호 해독 정책을 사용하여 암호화된 트래픽을 일반 텍스트 트래픽으로 전환할 수 있으므로 URL 필터링, 침입 및 악성코드 제어 그리고 기타 서비스(DPI(Deep Packet Inspection)를 필요로 함)를 적용할 수 있습니다. 정책에서 트래픽을 허용하는 경우, 트래픽은 디바이스를 떠나기 전에 다시 암호화됩니다.

SSL 암호 해독 정책은 암호화된 트래픽에만 적용됩니다. 암호화되지 않은 연결은 SSL 암호 해독 규칙을 기준으로 평가되지 않습니다.

참고 VPN 터널은 SSL 암호 해독 정책이 평가되기 전에 암호 해독되므로 정책은 터널에 적용되지 않습니다. 그러나 터널 내의 암호화된 연결은 모두 SSL 암호 해독 정책을 기준으로 평가받습니다.

다음 절차에서는 SSL 암호 해독 정책을 구성하는 방법에 대해 설명합니다. SSL 암호 해독 생성 및 관리의 엔드 투 엔드 프로세스에 대한 설명은 SSL 암호 해독 정책을 구현 및 유지 관리하는 방법, 470 페이지를 참조하십시오.

시작하기 전에

SSL 암호 해독 규칙 테이블에는 다음과 같이 두 가지 섹션이 있습니다.

- **Identity Policy Active Authentication Rules(ID** 정책 활성 인증 규칙**)** - ID 정책을 활성화하고 활성 인증을 사용하는 규칙을 생성하는 경우, 시스템에서는 정책이 작동하도록 설정하는 데 필요한 SSL 암호 해독 규칙을 자동으로 생성합니다. 이러한 규칙은 항상 직접 생성하는 SSL 암호 해독 규칙보다 먼저 평가됩니다. 또한, 이러한 규칙은 ID 정책을 변경하는 방식으로 간접적으로만 변경할 수 있습니다.
- **SSL Native Rules(SSL** 기본 규칙**)** - 이미 구성한 규칙입니다. 규칙은 이 섹션에만 추가할 수 있습니다.

프로시저

단계 **1** **Policies(**정책**)** > **SSL Decryption(SSL** 암호 해독**)**을 선택합니다.

정책을 아직 활성화하지 않은 경우 **Enable SSL Decryption(SSL** 암호 해독 활성화**)**을 클릭하여 SSL 암호 해독 정책 활성화, 473 페이지에 설명된 대로 정책 설정을 구성합니다.

단계 **2** 정책의 기본 작업을 구성합니다.

가장 안전한 방법은 **Do Not Decrypt(**암호 해독 안 함**)**를 선택하는 것입니다. 자세한 내용은 기본 SSL 암호 해독 작업 구성, 474 페이지의 내용을 참고하십시오.

단계 **3** SSL 암호 해독 정책을 관리합니다.

SSL 암호 해독 설정을 구성하고 나면 이 페이지에 모든 규칙이 순서대로 나열됩니다. 목록의 맨 위에서부터 규칙과 트래픽의 일치 여부를 확인하며, 첫 번째로 일치하는 규칙에 따라 적용할 작업이 결정됩니다. 이 페이지에서는 다음을 수행할 수 있습니다.

- 정책을 비활성화하려면 **SSL Decryption Policy(SSL** 암호 해독 정책**)** 토글을 클릭합니다. **Enable SSL Decryption(SSL** 암호 해독 활성화**)**을 클릭하여 다시 활성화할 수 있습니다.
- 정책에서 사용된 인증서의 목록을 포함한 정책 설정을 수정하려면 **SSL Decryption Settings(SSL** 암호 해독 설정**)** 버튼(⚙)을 클릭하십시오. 또한, 클라이언트에게 배포할 수 있도록 재서명 암호 해독 규칙에 사용되는 인증서를 다운로드할 수 있습니다. 다음 주제를 참조하십시오.

- 알려진 키 및 재서명 암호 해독을 위한 인증서 구성, 483 페이지
- 재서명 암호 해독 규칙을 위한 CA 인증서 다운로드, 484 페이지

- 규칙을 구성하려면 다음을 수행합니다.
  - 새 규칙을 생성하려면 + 버튼을 클릭합니다. SSL 암호 해독 규칙 구성, 475 페이지의 내용을 참조하십시오.
  - 기존 규칙을 수정하려면 Actions(작업) 열에서 해당 규칙의 수정 아이콘()을 클릭합니다. 테이블에서 속성을 클릭하여 규칙 속성을 선택적으로 수정할 수도 있습니다.
  - 더 이상 필요하지 않은 규칙을 삭제하려면 Actions(작업) 열에서 해당 규칙의 삭제 아이콘()을 클릭합니다.
- 규칙을 이동하려면 규칙을 수정하고 **Order(**순서**)** 드롭다운 목록에서 새 위치를 선택합니다.
- 예를 들어 제거 또는 변경된 URL 카테고리 때문에 어떤 규칙에 문제가 생긴 경우에는 검색 상자 옆에 있는 **See Problem Rules(**문제 규칙 참조**)** 링크를 클릭하여 해당 규칙만 표시하도록 테이블을 필터링합니다. 이러한 규칙에서 필요한 서비스를 제공하도록 수정 및 교정(또는 삭제)하십시오.

SSL 암호 해독 정책 활성화

SSL 암호 해독 규칙을 구성하기 전에 정책을 활성화하고 몇 가지 기본 설정을 구성해야 합니다. 다음 절차에서는 정책을 직접 활성화하는 방법에 대해 설명합니다. ID 정책을 활성화하는 경우에도 정책을 활성화할 수 있습니다. ID 정책의 경우 SSL 암호 해독 정책을 활성화해야 합니다.

시작하기 전에

SSL 암호 해독 정책이 없는 릴리스에서 업그레이드했지만 활성 인증 규칙이 있는 ID 정책을 구성한 경우에는 SSL 암호 해독 정책이 이미 활성화되어 있습니다. 사용할 재서명 암호 해독 인증서를 선택하고 선택적으로 사전 정의된 규칙을 활성화합니다.

프로시저

단계 **1** **Policies(**정책**)** > **SSL Decryption(SSL** 암호 해독**)**을 선택합니다.

단계 **2** 정책 설정을 구성하려면 **Enable SSL Decryption(SSL** 암호 해독 활성화**)**을 클릭합니다.

- 처음으로 정책을 활성화한 경우, SSL Decryption Configuration(SSL 암호 해독 컨피그레이션) 대화 상자가 열립니다. 다음 단계를 계속 진행합니다.
- 이미 한 번 정책을 구성했다가 비활성화한 경우, 간단히 이전 설정 및 규칙을 사용하여 정책을 다시 활성화할 수 있습니다. **SSL Decryption Settings(SSL** 암호 해독 설정**)** 버튼()을 클릭하여

알려진 키 및 재서명 암호 해독을 위한 인증서 구성, 483 페이지에 설명된 대로 설정을 컨피그레이션할 수 있습니다.

단계 3 **Decrypt Re-Sign Certificate(**재서명 암호 해독 인증서**)**에서 재서명된 인증서를 이용하여 암호 해독을 구현하는 규칙에 사용할 내부 CA 인증서를 선택합니다.

사전 정의된 NGFW-Default-InternalCA 인증서를 사용하거나, 생성 또는 업로드한 인증서를 사용할 수 있습니다. 인증서가 아직 없으면 **Create Internal CA(**내부 **CA** 생성**)**를 클릭하여 생성합니다.

클라이언트 브라우저에서 인증서를 아직 설치하지 않은 경우, 다운로드 버튼( )을 클릭하여 복사본을 획득합니다. 인증서 설치 방법에 대한 자세한 내용은 각 브라우저에 대한 설명서를 참조하십시오. 재서명 암호 해독 규칙을 위한 CA 인증서 다운로드, 484 페이지도 참조하십시오.

단계 4 (선택 사항). **Trusted CA Certificates(**신뢰할 수 있는 **CA** 인증서**)** 아래에서 **+**를 클릭하고 정책에서 신뢰할 인증서 또는 인증서 그룹을 선택합니다.

기본 그룹인 CTA(Cisco-Trusted-Authorities)에는 시스템 정의된 신뢰할 수 있는 CA 인증서가 모두 포함됩니다. 추가 인증서를 업로드한 경우 여기서 인증서를 추가하거나 사용자의 그룹에서 이를 수집하여 여기에서 그룹을 선택할 수 있습니다. CTA(Cisco-Trusted-Authorities) 그룹을 교체하거나 사용자의 그룹을 추가하기만 하면 됩니다. 인증서의 서명 기관이 이 목록에 없는 사이트에 대한 인증서를 수락하라는 메시지가 사용자에게 표시됩니다. 인증서를 신뢰할 수 없다는 이유 만으로 사이트에 대한 액세스가 차단되지는 않습니다.

목록을 비워 두거나 빈 인증서 그룹만 선택하면 SSL 암호 해독 정책에서 모든 인증서를 신뢰합니다.

단계 5 초기 SSL 암호 해독 규칙을 선택합니다.

시스템에는 다음과 같이 유용하게 활용할 수 있는, 사전 정의된 규칙이 있습니다.

- **Sensitive_Data** - 이 규칙은 금융 서비스 또는 보건 및 의료 URL 카테고리(은행, 의료 서비스 등 포함)에 있는 웹 사이트와 일치하는 트래픽을 암호 해독하지 않습니다. 이 규칙을 구현하려면 URL 라이선스를 활성화해야 합니다.

단계 6 **Enable(**활성화**)**을 클릭합니다.

기본 SSL 암호 해독 작업 구성

특정 SSL 암호 해독 규칙과 일치하지 않는 암호화된 연결은 SSL 암호 해독 정책의 기본 작업에 의해 처리됩니다.

프로시저

단계 1 **Policies(**정책**)** > **SSL Decryption(SSL** 암호 해독**)**을 선택합니다.

단계 2 **Default Action(**기본 작업**)** 필드에서 아무 곳이나 클릭합니다.

단계 3 일치하는 트래픽에 적용할 작업을 선택합니다.

- **Do Not Decrypt(**암호 해독 안 함**)** - 암호화된 연결을 허용합니다. 그러면 액세스 제어 정책이 암호화된 연결을 평가하고 액세스 제어 규칙을 기반으로 삭제 또는 허용합니다.
- **Block(**차단**)** - 연결을 즉시 삭제합니다. 연결은 액세스 제어 정책으로 전달되지 않습니다.

단계 **4** (선택 사항). 기본 작업에 대한 로깅을 구성합니다.

기본 작업과 일치하는 트래픽에 대한 로깅을 활성화해야 대시보드 데이터 또는 이벤트 뷰어에 해당 트래픽이 포함됩니다. 다음 옵션 중에서 선택합니다.

- **At End of Connection(**연결 종료 시**)** — 연결 종료 시 이벤트를 생성합니다.
  - **Send Connection Events To(**다음으로 연결 이벤트 보내기**)** — 외부 syslog 서버로 이벤트의 복사본을 전송하려는 경우, syslog 서버를 정의하는 서버 개체를 선택합니다. 필요한 개체가 아직 없으면 **Create New Syslog Server(**새 **Syslog** 서버 생성**)**를 클릭하여 개체를 생성합니다. syslog 서버에 대한 로깅을 비활성화하려면 서버 목록에서 **Any(**모두**)**를 선택합니다.

    디바이스의 이벤트 스토리지는 제한되어 있으므로 외부 syslog 서버로 이벤트를 전송하면 더 장기적으로 저장할 수 있으며 이벤트 분석 성능이 개선됩니다.
- **No Logging(**로깅 없음**)** — 이벤트를 생성하지 않습니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

SSL 암호 해독 규칙 구성

SSL 암호 해독 규칙을 사용하여 암호화된 연결 처리 방법을 결정합니다. SSL 암호 해독 정책의 규칙은 위에서부터 아래로 평가됩니다. 트래픽에 적용되는 규칙은 모든 트래픽 기준이 일치하는 첫 번째 규칙입니다.

SSL 기본 규칙 섹션에서만 규칙을 생성하고 편집할 수 있습니다.

참고 VPN 연결(사이트 대 사이트 및 원격 액세스 모두)에 대한 트래픽은 SSL 암호 해독 정책이 연결을 평가하기 전에 암호 해독됩니다. 따라서 SSL 암호 해독 규칙은 VPN 연결에 적용되지 않으며 이러한 규칙을 생성할 때 VPN 연결을 고려할 필요가 없습니다. 그러나 VPN 터널 내에서 사용된 암호화된 연결은 모두 평가됩니다. 예를 들어, RA VPN 연결을 통과하는 내부 서버에 대한 HTTPS 연결은 SSL 암호 해독 규칙을 기준으로 평가됩니다. 단, RA VPN 터널 자체는 이미 암호 해독되어 있으므로 이를 통과하는 경우에는 평가되지 않습니다.

시작하기 전에

알려진 키 암호 해독 규칙을 생성하는 경우, 목적지 서버(내부 인증서 역할)의 인증서 및 키를 업로드하고, SSL 암호 해독 정책 설정을 편집하여 이 인증서를 사용합니다. 알려진 키 규칙은 일반적으로 규칙의 대상 네트워크 기준에서 목적지 서버를 지정합니다. 자세한 내용은 알려진 키 및 재서명 암호 해독을 위한 인증서 구성, 483 페이지의 내용을 참고하십시오.

프로시저

단계 1 **Policies(정책)** > **SSL Decryption(SSL 암호 해독)**을 선택합니다.

SSL 암호 해독 규칙(활성 인증 ID 규칙에 대해 자동으로 생성된 규칙 제외)을 구성하지 않은 경우, **Add Pre-Defined Rules(사전 정의된 규칙 추가)**를 클릭하여 사전 정의된 규칙을 추가할 수 있습니다. 원하는 규칙을 선택하라는 프롬프트가 표시됩니다.

단계 2 다음 중 하나를 수행합니다.

- 새 규칙을 생성하려면 + 버튼을 클릭합니다.
- 기존 규칙을 수정하려면 해당 규칙의 수정 아이콘()을 클릭합니다.

더 이상 필요하지 않은 규칙을 삭제하려면 해당 규칙의 삭제 아이콘()을 클릭합니다.

단계 3 **Order(순서)**에서 순서가 지정된 규칙 목록에 규칙을 삽입할 위치를 선택합니다.

SSL Native Rules(SSL 기본 규칙) 섹션에만 규칙을 삽입할 수 있습니다. Identity Policy Active Authentication Rules(ID 정책 활성 인증 규칙)가 ID 정책에서 자동으로 생성되며, 이 규칙은 읽기 전용입니다.

규칙은 처음 일치하는 항목을 기준으로 적용되므로, 매우 구체적인 트래픽 일치 기준이 포함된 규칙이 보다 일반적인 기준이 포함된 정책(규칙이 일치하지 않는 경우 일치하는 트래픽에 적용됨) 위에 표시되도록 삽입해야 합니다.

기본적으로는 규칙이 목록의 끝에 추가됩니다. 나중에 규칙의 위치를 변경하려는 경우 이 옵션을 수정합니다.

단계 4 **Tile(제목)**에서 규칙의 이름을 입력합니다.

이름에는 공백을 포함할 수 없지만, 영숫자 및 특수 문자(+, ., _, -)는 사용할 수 있습니다.

단계 5 일치하는 트래픽에 적용할 작업을 선택합니다.

각 옵션에 대한 자세한 내용은 다음을 참조하십시오.

- 재서명 암호 해독, 466 페이지
- 알려진 키 암호 해독, 467 페이지
- 암호 해독 안 함, 468 페이지
- 차단, 468 페이지

단계 6 다음 탭을 적절하게 조합하여 트래픽 일치 기준을 정의합니다.

- **Source/Destination(소스/대상)** - 트래픽이 통과하는 보안 영역(인터페이스), IP 주소/IP 주소의 국가나 대륙(지리적 위치) 또는 트래픽에서 사용되는 TCP 포트입니다. 기본값은 영역, 주소, 지리적 위치 및 TCP 포트입니다. SSL 암호 해독 규칙에 대한 소스/대상 기준, 478 페이지의 내용을 참조하십시오.

- **Application(**애플리케이션**)** - 유형, 범주, 태그, 위험, 사업 타당성에 따라 애플리케이션을 정의하는 필터 또는 애플리케이션입니다. 기본값은 암호화된 애플리케이션입니다. SSL 암호 해독 규칙에 대한 애플리케이션 기준, 479 페이지를 참조하십시오.
- **URL** - 웹 요청의 URL 카테고리입니다. 기본값은 일치를 위해 고려되지 않은 URL 카테고리와 평판입니다. SSL 암호 해독 규칙에 대한 URL 기준, 480 페이지의 내용을 참조하십시오.
- **Users(**사용자**)** - ID 소스, 사용자 또는 사용자 그룹입니다. ID 정책에 따라 트래픽 일치에 사용자 및 그룹 정보를 사용할 수 있는지가 결정됩니다. 이 기준을 사용하려면 ID 정책을 구성해야 합니다. SSL 암호 해독 규칙에 대한 사용자 기준, 481 페이지의 내용을 참조하십시오.
- **Advanced(**고급**)** - SSL/TLS 버전 및 인증서 상태와 같이 연결에서 사용하는 인증서에서 파생된 특성입니다. SSL 암호 해독 규칙에 대한 고급 기준, 482 페이지의 내용을 참조하십시오.

조건을 수정하려면 해당 조건 내의 **+** 버튼을 클릭하고 필요한 개체나 요소를 선택한 후에 팝업 대화상자에서 **OK(**확인**)**를 클릭합니다. 기준에 개체가 필요한데 필요한 개체가 없는 경우에는 새 개체 생성을 클릭하면 됩니다. 개체 또는 요소의 **x**를 클릭하면 정책에서 해당 개체나 요소를 제거할 수 있습니다.

SSL 암호 해독 규칙에 조건을 추가하는 경우 다음 팁을 고려하십시오.

- 규칙마다 여러 조건을 구성할 수 있습니다. 규칙을 트래픽에 적용하려면 트래픽이 규칙의 모든 조건과 일치해야 합니다. 예를 들어, URL 카테고리를 기반으로 트래픽을 암호 해독하는 단일 규칙을 사용할 수 있습니다.
- 규칙의 각 조건에 대해 최대 50개의 기준을 추가할 수 있습니다. 조건의 기준 중 어느 것이든 모두 일치하는 트래픽은 조건을 만족합니다. 예를 들어, 최대 50개의 애플리케이션 또는 애플리케이션 필터에 대해 애플리케이션 제어를 적용하는 단일 규칙을 사용할 수 있습니다. 따라서 단일 조건의 항목 간 관계는 OR이고 조건 유형 간의 관계(예: 소스/대상과 애플리케이션 간의 관계)는 AND가 됩니다.
- 일치하는 URL 카테고리에는 URL 필터링 라이선스가 필요합니다.

단계 **7** (선택 사항). 규칙에 대해 로깅을 구성합니다.

대시보드 데이터 또는 이벤트 뷰어에 포함될 규칙과 일치하는 트래픽에 대한 로깅을 활성화해야 합니다. 다음 옵션 중에서 선택합니다.

- **At End of Connection(**연결 종료 시**)** — 연결 종료 시 이벤트를 생성합니다.
  - **Send Connection Events To(**다음으로 연결 이벤트 보내기**)** — 외부 syslog 서버로 이벤트의 복사본을 전송하려는 경우, syslog 서버를 정의하는 서버 개체를 선택합니다. 필요한 개체가 아직 없으면 **Create New Syslog Server(**새 **Syslog** 서버 생성**)**를 클릭하여 개체를 생성합니다. syslog 서버에 대한 로깅을 비활성화하려면 서버 목록에서 Any(모두)를 선택합니다.

    디바이스의 이벤트 스토리지는 제한되어 있으므로 외부 syslog 서버로 이벤트를 전송하면 더 장기적으로 저장할 수 있으며 이벤트 분석 성능이 개선됩니다.
- **No Logging(**로깅 없음**)** — 이벤트를 생성하지 않습니다.

단계 **8** **OK(**확인**)**를 클릭합니다.

SSL 암호 해독 규칙에 대한 소스/대상 기준

SSL 암호 해독 규칙의 소스/대상 기준은 트래픽이 통과하는 보안 영역(인터페이스), IP 주소/IP 주소의 국가나 대륙(지리적 위치) 또는 트래픽에서 사용되는 TCP 포트를 정의합니다. 기본값은 영역, 주소, 지리적 위치 또는 TCP 포트입니다. TCP는 SSL 암호 해독 규칙과 일치되는 유일한 프로토콜입니다.

조건을 수정하려면 해당 조건 내의 **+** 버튼을 클릭하고 필요한 개체나 요소를 선택한 후에 **OK(**확인**)**를 클릭합니다. 기준에 개체가 필요한데 필요한 개체가 없는 경우에는 새 개체 생성을 클릭하면 됩니다. 개체 또는 요소의 **x**를 클릭하면 정책에서 해당 개체나 요소를 제거할 수 있습니다.

다음 기준을 사용하여 규칙과 일치하는 소스 및 대상을 식별할 수 있습니다.

소스 영역**,** 대상 영역

트래픽이 통과하는 인터페이스를 정의하는 보안 영역 개체입니다. 기준은 하나 또는 둘 다 정의할 수도 있고 둘 다 정의하지 않을 수도 있습니다. 지정되지 않은 기준은 임의 인터페이스의 트래픽에 적용됩니다.

- 영역 내 인터페이스의 디바이스에서 나가는 트래픽에 일치시키기 위해서는 대상 영역에 해당 영역을 추가합니다.
- 영역 내 인터페이스를 통해 디바이스로 들어오는 트래픽에 일치시키기 위해서는 소스 영역에 해당 영역을 추가합니다.
- 규칙에 소스와 대상 영역 조건을 모두 추가한 경우, 일치하는 트래픽은 반드시 지정된 소스 영역 중 하나에서 발생해야 하며 대상 영역 중 하나를 통해 전송되어야 합니다.

트래픽이 디바이스로 들어오거나 디바이스에서 나가는 위치를 기준으로 규칙을 적용해야 하는 경우 이 기준을 사용해야 합니다. 예를 들어 외부 호스트에서 내부 호스트로 이동하는 모든 트래픽을 암호 해독하려는 경우에는 외부 영역을 **Source Zones(**소스 영역**)**로, 내부 영역을 **Destination Zones(**대상 영역**)**로 선택합니다.

소스 네트워크**,** 대상 네트워크

트래픽의 네트워크 주소나 위치를 정의하는 네트워크 개체 또는 지리적 위치입니다.

- 특정 IP 주소 또는 지리적 위치에서 나오는 트래픽을 일치시키려면 소스 네트워크를 구성합니다.
- 특정 IP 주소 또는 지리적 위치로 향하는 트래픽을 일치시키려면 대상 네트워크를 구성합니다.
- 규칙에 소스와 대상 네트워크 조건을 모두 추가한 경우, 일치하는 트래픽은 반드시 지정된 IP 주소 중 하나에서 발생해야 하며 그 목적지가 대상 IP 주소 중 하나여야 합니다.

이 기준을 추가할 때는 다음 탭에서 선택합니다.

- 네트워크 - 제어하려는 트래픽의 소스 또는 대상 IP 주소를 정의하는 네트워크 개체 또는 그룹을 선택합니다.

참고 알려진 키 암호 해독 규칙의 경우 업로드한 인증서와 키를 사용하는 목적지 서버의 IP 주소를 사용하는 개체를 선택합니다.

- 지리위치 - 소스 또는 대상 국가나 대륙을 기준으로 트래픽을 제어하려면 지리적 위치를 선택합니다. 대륙을 선택하면 대륙 내의 모든 국가가 선택됩니다. 규칙에서 지리적 위치를 직접 선택하는 방법 외에, 위치를 정의하기 위해 생성한 지리위치 개체를 선택할 수도 있습니다. 지리적 위치를 사용하면 특정 국가에서 사용될 수 있는 모든 IP 주소를 몰라도 해당 국가에 대한 액세스를 쉽게 제한할 수 있습니다.

소스 포트**,** 대상 포트/프로토콜

트래픽에 사용되는 프로토콜을 정의하는 포트 개체입니다. TCP 프로토콜 및 포트는 SSL 암호 해독 규칙에 대해서만 지정할 수 있습니다.

- TCP 포트에서 발생하는 트래픽을 일치시키려면 **Source Ports(**소스 포트**)**를 구성합니다.
- TCP 포트로 향하는 트래픽을 일치시키려면 **Destination Ports/Protocols(**대상 포트/프로토콜**)**를 구성합니다.
- 특정 TCP 포트에서 발생하는 트래픽과 특정 TCP 포트로 향하는 트래픽을 모두 일치시키려면 두 포트를 모두 구성합니다. 예를 들어 포트 TCP/80에서 포트 TCP/8080으로 이동하는 트래픽을 대상으로 지정할 수 있습니다.

SSL 암호 해독 규칙에 대한 애플리케이션 기준

SSL 암호 해독 규칙의 애플리케이션 기준은 유형, 카테고리, 태그, 위험 또는 사업 타당성에 따라 애플리케이션을 정의하는 필터 또는 IP 연결에 사용되는 애플리케이션을 정의합니다. 기본값은 SSL 프로토콜 태그가 있는 모든 애플리케이션입니다. SSL 암호 해독 규칙은 어떤 암호화되지 않은 애플리케이션과도 일치시킬 수 없습니다.

규칙에서 개별 애플리케이션을 지정할 수 있으나 애플리케이션 필터를 사용하면 정책 생성 및 관리가 간소화됩니다. 예를 들어, 위험도가 높고 사업 타당성이 낮은 모든 애플리케이션을 암호 해독하거나 차단하는 SSL 암호 해독 규칙을 생성할 수 있습니다. 사용자가 이러한 애플리케이션 중 하나를 사용하려고 할 경우, 세션은 암호 해독되거나 차단됩니다.

이와 더불어 Cisco에서는 시스템 및 VDB(Vulnerability Database)를 통해 추가 애플리케이션 탐지기를 자주 업데이트하고 추가합니다. 따라서 규칙을 수동으로 업데이트하지 않아도 위험도가 높은 애플리케이션에 대한 규칙이 새 애플리케이션에 자동으로 적용될 수 있습니다.

규칙에서 애플리케이션 및 필터를 직접 지정하거나 이러한 특성을 정의하는 애플리케이션 필터 개체를 생성할 수 있습니다. 이 두 가지 경우의 사양은 동일하지만, 개체를 사용하면 복잡한 규칙을 생성할 때에도 시스템 제한(기준당 항목 50개)을 유지하기가 더욱 쉽습니다.

애플리케이션 및 필터 목록을 수정하려면 조건 내에서 **+** 버튼을 클릭하고 개별 탭에 나열된 원하는 애플리케이션 또는 애플리케이션 필터 개체를 선택한 후에 팝업 대화 상자에서 **OK(**확인**)**를 클릭합니다. 탭 중 하나에서 **Advanced Filter(**고급 필터**)**를 클릭하면 필터 기준을 선택하거나 특정 애플리케이션을 검색할 수 있습니다. 애플리케이션, 필터 또는 개체에 대해 **x**를 클릭하면 정책에서 해당 항목

을 제거할 수 있습니다. **Save As Filter(**필터로 저장**)** 링크를 클릭하면 아직 개체가 아닌 결합된 기준을 새 애플리케이션 필터 개체로 저장할 수 있습니다.

애플리케이션 기준과 고급 필터를 구성하고 애플리케이션을 선택하는 방법에 대한 자세한 내용은 애플리케이션 필터 개체 구성, 153 페이지를 참조하십시오.

SSL 암호 해독 규칙에서 애플리케이션 기준을 사용할 때 다음 팁을 고려하십시오.

- 시스템은 StartTLS를 사용하여 암호화되는 해독된 애플리케이션을 식별할 수 있습니다. 여기에는 SMTPS, POPS, FTPS, TelnetS, IMAPS 같은 애플리케이션이 포함됩니다. 또한, 시스템은 TLS ClientHello 메시지 내 서버 이름 지표 또는 서버 인증서 주체 고유 이름 값에 따라 암호화된 특정 애플리케이션을 식별할 수 있습니다.
- 시스템은 서버 인증서 교환 이후에만 애플리케이션을 식별할 수 있습니다. SSL 핸드셰이크 중에 교환된 트래픽이 애플리케이션 조건을 포함하는 SSL 규칙의 다른 모든 조건과 일치하지만 식별이 완료되지 않은 경우, SSL 정책을 사용하여 패킷을 통과하도록 할 수 있습니다. 이러한 동작을 통해 핸드셰이크가 완료되므로 애플리케이션을 식별할 수 있습니다. 시스템에서 식별을 완료하면, 애플리케이션 조건과 매칭되는 나머지 세션 트래픽에 SSL 규칙 작업을 적용합니다.
- 선택한 애플리케이션을 VDB 업데이트를 통해 제거한 경우 애플리케이션 이름 뒤에 "(Depredcated(사용되지 않음))"이라고 표시됩니다. 이러한 애플리케이션은 필터에서 제거해야 합니다. 그렇지 않으면 후속 구축 및 시스템 소프트웨어 업그레이드가 차단됩니다.

SSL 암호 해독 규칙에 대한 URL 기준

SSL 암호 해독 규칙의 URL 기준은 웹 요청의 URL이 속하는 카테고리를 정의합니다. 또한, 암호 해독, 차단 또는 암호 해독 없이 허용할 사이트의 상대적인 평판을 지정할 수 있습니다. 기본값은 URL 카테고리를 기반으로 하는 연결과 일치하지 않습니다.

예를 들어, 암호화된 모든 게임 사이트를 차단하거나 신뢰할 수 없는 소셜 네트워킹 사이트를 암호 해독할 수 있습니다. 사용자가 해당 카테고리 및 평판 조합을 가진 URL을 찾아보려고 시도하는 경우, 세션이 차단 또는 암호 해독됩니다. URL 카테고리 일치에 대한 자세한 정보는 카테고리 및 평판을 기준으로 URL 필터링, 519 페이지의 내용을 참조하십시오.

범주 탭

+를 클릭하고 원하는 범주를 선택한 후에 **OK(**확인**)**를 클릭합니다. 카테고리의 **x**를 클릭하면 정책에서 해당 카테고리를 제거할 수 있습니다.

기본적으로는 평판과 관계없이 선택한 각 범주의 모든 URL에 규칙을 적용합니다. 평판을 기준으로 하여 규칙을 제한하려면 각 범주의 아래쪽 화살표를 클릭하고 임의 체크 박스 선택을 취소한 후에 평판 슬라이더를 사용하여 평판 레벨을 선택합니다. 평판 슬라이더의 왼쪽에는 암호 해독 없이 허용할 사이트가, 오른쪽에는 암호 해독하거나 차단할 사이트가 표시됩니다. 평판 사용 방식은 규칙 작업에 따라 달라집니다.

- 규칙이 연결을 암호 해독하거나 차단하는 경우 평판 레벨을 선택하면 해당 레벨보다 심각도가 높은 평판도 모두 선택됩니다. 예를 들어, **Questionable sites(**의심스러운 사이트**)**(레벨 2)를 암호 해독하거나 차단하는 규칙을 구성하는 경우, **Untrusted(**신뢰할 수 없음**)**(레벨 1) 사이트도 자동으로 암호 해독되거나 차단됩니다.

- 규칙이 연결을 암호 해독 없이 허용(암호 해독 안 함)하는 경우 평판 레벨을 선택하면 해당 레벨보다 심각도가 낮은 평판도 모두 선택됩니다. 예를 들어, **Favorable sites(**선호 사이트**)**(레벨 4)를 암호 해독하지 않는 규칙을 구성하는 경우, **Trusted(**신뢰할 수 있음**)**(레벨 5) 사이트도 자동으로 암호 해독되지 않습니다.

평판을 알 수 없는 URL을 평판 일치에 포함하려면 **Include Sites with Unknown Reputation(**평판을 알 수 없는 사이트 포함**)** 옵션을 선택합니다. 새 사이트는 일반적으로 등급이 지정되지 않으며, 사이트의 평판을 알 수 없거나 확인할 수 없는 다른 이유가 있을 수 있습니다.

URL의 카테고리 확인

특정 URL의 카테고리 및 평판을 확인할 수 있습니다. **URL to Check(**확인할 **URL)** 상자에서 URL을 입력하고 **Go(**이동**)**를 클릭하십시오. 결과를 볼 수 있는 외부 웹 사이트로 연결됩니다. 분류에 동의하지 않는 경우 **Submit a URL Category Dispute(URL** 카테고리 이의 제출**)** 링크를 클릭하고 저희에게 알려주십시오.

SSL 암호 해독 규칙에 대한 사용자 기준

SSL 암호 해독 규칙의 사용자 기준은 IP 연결의 사용자 또는 사용자 그룹을 정의합니다. 규칙에 사용자 또는 사용자 그룹 기준을 포함하려면 ID 정책 및 관련 디렉터리 서버를 구성해야 합니다.

ID 정책에 따라 특정 연결에 대해 사용자 ID가 수집되는지가 결정됩니다. ID가 설정된 경우에는 호스트의 IP 주소가 식별된 사용자와 연결됩니다. 그러므로 해당 소스 IP 주소가 사용자에 매핑된 트래픽은 해당 사용자가 보내는 것으로 간주됩니다. IP 패킷 자체는 사용자 ID 정보를 포함하지 않으므로 이 IP 주소에서 사용자로의 매핑은 가능한 최적의 근사치입니다.

규칙에는 최대 50개의 사용자나 그룹을 추가할 수 있으므로 일반적으로는 개별 사용자를 선택하는 것보다 그룹을 선택하는 것이 더 효율적입니다. 예를 들어 외부 네트워크에서 오는 엔지니어링 그룹에 대한 트래픽을 해독하는 규칙을 생성하고 이 그룹에서 나오는 발신 트래픽의 암호를 해독하지 않는 별도의 규칙을 만들 수 있습니다. 그러면 신규 엔지니어에 대해 규칙을 적용하려는 경우 디렉터리 서버의 엔지니어링 그룹에 해당 엔지니어를 추가하기만 하면 됩니다.

해당 소스 내 모든 사용자에게 적용할 ID 소스도 선택할 수 있습니다. 따라서 여러 Active Directory 도메인을 지원하는 경우, 도메인에 근거하여 차등 암호 해독을 제공할 수 있습니다.

사용자 목록을 수정하려면 조건 내의 **+** 버튼을 클릭하고 다음 기술 중 하나를 사용하여 원하는 사용자 또는 사용자 그룹을 선택합니다. 사용자 또는 그룹의 **x**를 클릭하면 정책에서 해당 사용자나 그룹을 제거할 수 있습니다.

- **Identity Sources(ID** 소스**)** - 선택한 소스에서 얻은 모든 사용자에게 규칙을 적용하려면 AD 영역 또는 로컬 사용자 데이터베이스 같은 ID 소스를 선택합니다. 필요한 영역이 아직 없는 경우, **Create New Identity Realm(**새 **ID** 영역 생성**)**을 클릭하여 바로 생성합니다.
- **Groups(**그룹**)** - 원하는 사용자 그룹을 선택합니다. 그룹은 디렉터리 서버에서 그룹을 구성하는 경우에만 사용할 수 있습니다. 그룹을 선택하면 하위 그룹을 포함하여 그룹의 모든 멤버에게 규칙이 적용됩니다. 하위 그룹을 다르게 처리하려는 경우에는 하위 그룹용으로 별도의 액세스 규칙을 생성한 다음 액세스 제어 정책에서 상위 그룹용 규칙 위에 배치해야 합니다.
- **Users(**사용자**)** - 개별 사용자를 선택합니다. 사용자 이름에는 Realm\username과 같은 ID 소스가 접두사로 붙습니다.

Special-Identities-Realm에서 일부 사용자는 기본으로 제공됩니다.

- **Failed Authentication(**실패한 인증**)** - 사용자에게 인증하라는 메시지가 표시되었는데 사용자가 허용되는 최대 횟수 이내에 유효한 사용자 이름/비밀번호 쌍을 입력하지 못했습니다. 인증에 실패해도 사용자의 네트워크 액세스가 차단되지는 않지만, 이러한 사용자의 네트워크 액세스를 제한하는 액세스 규칙을 작성할 수 있습니다.
- **Guest(**게스트**)** - 게스트 사용자는 ID 규칙이 이러한 사용자를 게스트로 지칭하도록 구성된다는 점을 제외하면 실패한 인증 사용자와 비슷합니다. 즉, 게스트 사용자 역시 인증하라는 메시지가 표시되었지만, 최대 시도 횟수 이내에 인증하지 못한 사용자입니다.
- **No Authentication Required(**인증 필요 없음**)** - 사용자의 연결이 인증을 지정하지 않은 ID 규칙과 일치하여 인증하라는 메시지가 표시되지 않았습니다.
- **Unknown(**알 수 없음**)** - IP 주소에 대한 사용자 매핑이 없으며 아직 실패한 인증 기록이 없습니다. 이는 일반적으로 해당 주소에서 HTTP 트래픽이 아직 전송되지 않았음을 의미합니다.

SSL 암호 해독 규칙에 대한 고급 기준

고급 트래픽 일치 기준은 연결에 사용되는 인증서에서 파생된 특성과 관련이 있습니다. 다음 옵션 중 하나 또는 모두를 구성할 수 있습니다.

인증서 속성

선택한 속성 중 하나와 일치하는 트래픽은 규칙의 인증서 속성 옵션과 일치합니다. 다음을 구성할 수 있습니다.

인증서 상태

인증서 상태가 **Valid(**유효함**)** 또는 **Invalid(**유효하지 않음**)**인지 여부입니다. 인증서 상태가 중요하지 않은 경우, **Any(**모두**)**(기본값)를 선택합니다.

인증서는 다음 조건을 모두 충족하는 경우 유효한 것으로 간주되며, 그렇지 않은 경우에는 유효하지 않습니다.

- 정책이 인증서를 발급한 CA를 신뢰합니다.
- 인증서의 내용에 대해 인증서의 서명을 제대로 검증할 수 있습니다.
- 발급자 CA 인증서가 정책의 신뢰할 수 있는 CA 인증서 목록에 저장됩니다.
- 정책의 신뢰할 수 있는 CA가 인증서를 취소하지 않음
- 현재 날짜가 인증서의 유효 시작일과 유효 만료일 사이에 해당합니다.

자체 서명

서버 인증서에 동일한 주체 및 발급자 고유 이름이 포함되어 있는지 여부입니다. 다음 중 하나를 선택합니다.

- **Self-Signing(**자체 서명**)** — 서버 인증서가 자체 서명되었습니다.

- **CA-Signing(CA** 서명**)** — 서버 인증서가 CA(인증 기관)에 의해 서명되었습니다. 즉, 발급자와 주체가 동일하지 않습니다.
- **Any(**모두**)** — 인증서가 일치 기준으로 자체 서명되었는지를 신경 쓰지 않습니다.

지원되는 버전

일치하는 SSL/TLS 버전입니다. 규칙은 선택한 버전 중 하나를 사용하는 트래픽에 적용됩니다. 기본값은 모든 버전입니다. **SSL 3.0**, **TLS 1.0**, **TLS 1.1**, **TLS 1.2** 중에서 선택합니다.

예를 들어 TLSv1.2 연결만 허용하려는 경우 하위 버전에 대한 차단 규칙을 생성할 수 있습니다.

나열되지 않은 버전(예: SSL v2.0)을 사용하는 트래픽은 SSL 암호 해독 정책에 대한 기본 작업에 의해 처리됩니다.

알려진 키 및 재서명 암호 해독을 위한 인증서 구성

재서명하거나 알려진 키를 사용하여 암호 해독을 구현하는 경우, SSL 암호 해독 규칙에서 사용할 수 있는 인증서를 식별해야 합니다. 모든 인증서가 유효하고 만료되지 않았는지 확인합니다.

특히 알려진 키 암호 해독의 경우, 암호 해독 중인 연결을 지닌 각 목적지 서버의 현재 인증서 및 키가 시스템에 있는지 확인해야 합니다. 알려진 키 암호 해독 규칙과 함께 암호 해독을 위해 목적지 서버의 실제 인증서와 키를 사용합니다. 따라서 threat defense 디바이스에는 항상 현재 인증서 및 키가 있어야 합니다. 그러지 않으면 암호 해독에 실패합니다.

알려진 키 규칙으로 목적지 서버에서 인증서 또는 키를 변경할 때마다 새로운 내부 인증서와 키를 업로드합니다. 단, 내부 CA 인증서가 아니라 내부 인증서로 업로드합니다. 다음 절차를 통해 인증서를 업로드하거나 **Objects(**개체**)** > **Certificates(**인증서**)** 페이지로 이동하여 인증서를 업로드할 수 있습니다.

프로시저

단계 **1** **Policies(**정책**)** > **SSL Decryption(SSL** 암호 해독**)**을 선택합니다.

단계 **2** **SSL Decryption Settings(SSL** 암호 해독 설정**)** 버튼(⚙)을 클릭합니다.

단계 **3** **Decrypt Re-Sign Certificate(**재서명 암호 해독 인증서**)**에서 재서명된 인증서를 이용하여 암호 해독을 구현하는 규칙에 사용할 내부 CA 인증서를 선택합니다.

사전 정의된 NGFW-Default-InternalCA 인증서를 사용하거나, 생성 또는 업로드한 인증서를 사용할 수 있습니다. 인증서가 아직 없으면 **Create Internal CA(**내부 **CA** 생성**)**를 클릭하여 생성합니다.

클라이언트 브라우저에서 인증서를 아직 설치하지 않은 경우, 다운로드 버튼(⬇)을 클릭하여 복사본을 획득합니다. 인증서 설치 방법에 대한 자세한 내용은 각 브라우저에 대한 설명서를 참조하십시오. 재서명 암호 해독 규칙을 위한 CA 인증서 다운로드, 484 페이지도 참조하십시오.

단계 **4** 알려진 키를 사용하여 암호를 해독하는 각 규칙의 경우 목적지 서버의 내부 인증서 및 키를 업로드합니다.

a) **Decrypt Known-Key Certificates(**알려진 키 암호 해독 인증서**)** 아래에서 +를 클릭합니다.

b) 내부 ID 인증서를 선택하거나 **Create New Internal Certificate(**새 내부 인증서 생성**)**를 클릭하여 바로 업로드합니다.

c) **OK(**확인**)**를 클릭합니다.

단계 **5** (선택 사항). **Trusted CA Certificates(**신뢰할 수 있는 **CA** 인증서**)** 아래에서 +를 클릭하고 정책에서 신뢰할 인증서 또는 인증서 그룹을 선택합니다.

기본 그룹인 CTA(Cisco-Trusted-Authorities)에는 시스템 정의된 신뢰할 수 있는 CA 인증서가 모두 포함됩니다. 이 설정을 변경할 수 있는 주요 사례는 다음과 같습니다.

- 기본 그룹에 없는 신뢰할 수 있는 CA 인증서를 사용하고자 합니다. 그러면 SSL 암호 해독 정책 설정에서 기본 그룹과 새 그룹을 모두 선택합니다. 신뢰할 수 있는 추가 CA 인증서를 업로드한 경우 이 작업을 수행할 수 있습니다.
- 기본 그룹에 있는 것보다 더욱 제한된 신뢰할 수 있는 CA 인증서 목록을 사용하고자 합니다. 그러면 델타 뿐 아니라 신뢰할 수 있는 인증서의 전체 목록이 포함된 그룹을 생성하고 이를 SSL 암호 해독 정책 설정에서 단독 그룹으로 선택합니다.

인증서의 서명 기관이 이 목록에 없는 사이트에 대한 인증서를 수락하라는 메시지가 사용자에게 표시됩니다. 인증서를 신뢰할 수 없다는 이유 만으로 사이트에 대한 액세스가 차단되지는 않습니다.

목록을 비워 두거나 빈 인증서 그룹만 선택하면 SSL 암호 해독 정책에서 모든 인증서를 신뢰합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

재서명 암호 해독 규칙을 위한 **CA** 인증서 다운로드

트래픽을 암호 해독하려는 경우, 사용자는 TLS/SSL을 사용하는 애플리케이션에서 신뢰할 수 있는 루트 인증 기관으로 정의된 암호화 프로세스에 사용되는 내부 CA 인증서를 보유하고 있어야 합니다. 일반적으로 인증서를 생성하거나 인증서를 하나 가져오게 되는 경우, 해당 인증서는 아직 이러한 애플리케이션에서 신뢰할 수 있는 인증서로 정의되어 있지 않습니다. 기본적으로 대부분의 웹 브라우저에서는 사용자가 HTTPS 요청을 전송할 때 클라이언트 애플리케이션에서 웹 사이트의 보안 인증서에 문제가 있음을 알려주는 경고 메시지를 표시합니다. 일반적으로 오류 메시지는 신뢰할 수 있는 인증 기관에서 웹 사이트의 보안 인증서를 발행한 것이 아니거나 알 수 없는 기관에서 웹 사이트를 인증했음을 나타냅니다. 하지만 경고는 MITM(Man-In-The-Middle) 공격이 진행 중일 수 있다는 점을 나타낼 수도 있습니다. 일부 다른 클라이언트 애플리케이션은 사용자에게 이 경고 메시지를 표시하지 않으며 사용자가 인식할 수 없는 인증서를 수락하도록 허용하지도 않습니다.

사용자에게 필수 인증서를 제공하는 데에는 다음과 같은 옵션이 있습니다.

루트 인증서를 수락하도록 사용자에게 알림

조직의 사용자에게 회사의 새로운 정책에 대해 알리고 조직에서 제공하는 루트 인증서를 신뢰할 수 있는 소스로 수락하도록 통지할 수 있습니다. 사용자는 다음에 사이트에 액세스할 때 다시 프롬프트가 나타나지 않도록 인증서를 수락하고 신뢰할 수 있는 루트 인증 기관 보관 영역에 저장해야 합니다.

참고 사용자는 대체 인증서를 생성한 CA 인증서를 수락하고 신뢰해야 합니다. 대신 사용자가 대체 서버 인증서를 신뢰하는 경우, 사용자는 방문하는 서로 다른 각 HTTPS 사이트에 대해 계속 경고를 보게 됩니다.

클라이언트 디바이스에 루트 인증서 추가

신뢰할 수 있는 루트 인증 기관으로 네트워크에 있는 모든 클라이언트 디바이스에 루트 인증서를 추가할 수 있습니다. 이렇게 하면 클라이언트 애플리케이션이 루트 인증서를 포함하는 트랜잭션을 자동으로 수락합니다.

인증서를 이메일 발송하거나 공유 사이트에 배치하는 방식을 통해 사용자가 인증서를 사용할 수 있게 하거나 인증서를 기업 워크스테이션 이미지에 통합하고 애플리케이션 업데이트 시설을 사용하여 사용자에게 자동으로 배포되게 할 수 있습니다.

다음 절차에서는 내부 CA 인증서를 다운로드하고 Windows 클라이언트에 설치하는 방법에 대해 설명합니다.

프로시저

단계 **1** device manager에서 인증서를 다운로드합니다.

a) **Policies(**정책**)** > **SSL Decryption(SSL** 암호 해독**)**을 선택합니다.

b) **SSL Decryption Settings(SSL** 암호 해독 설정**)** 버튼( )을 클릭합니다.

c) 다운로드 버튼( )을 클릭합니다.

d) 다운로드 위치를 선택하고 선택적으로 파일 이름(확장자 제외)을 변경한 다음 **Save(**저장**)**를 클릭합니다.

이제 SSL Decryption Settings(SSL 암호 해독 설정) 대화 상자에서 취소 작업을 할 수 있습니다.

단계 **2** 클라이언트 시스템의 웹 브라우저에서 신뢰할 수 있는 루트 인증 기관 보관 영역에 인증서를 설치하거나 클라이언트가 직접 인증서를 설치할 수 있도록 합니다.

프로세스는 운영 체제 및 브라우저의 유형에 따라 달라집니다. 예를 들어, Windows에서 실행 중인 Internet Explorer 및 Chrome에는 다음과 같은 프로세스를 사용할 수 있습니다. Firefox의 경우, **Tools(**도구**)** > **Options(**옵션**)** > **Advanced(**고급**)** 페이지를 통해 설치합니다.

a) 시작 메뉴에서 제어판 > 인터넷 옵션을 선택합니다.

b) 내용 탭을 선택합니다.

c) 인증서 버튼을 클릭하여 인증서 대화 상자를 엽니다.

d) 신뢰할 수 있는 루트 인증 기관 탭을 선택합니다.

e) 가져오기를 클릭하고 마법사를 따라 다운로드한 파일(<uuid>_internalCA.crt)을 찾아 선택한 다음 신뢰할 수 있는 루트 인증 기관 보관 영역에 추가합니다.

f) 마침을 클릭합니다.

성공적으로 가져왔음을 알리는 메시지가 표시됩니다. 잘 알려진 서드파티 인증 기관에서 인증서를 얻는 대신 자체 서명 인증서를 생성한 경우 Windows에서 인증서를 검증할 수 없다는 중간 대화 상자 경고가 표시될 수 있습니다.

이제 인증서 및 인터넷 옵션 대화 상자를 닫으면 됩니다.

예: 네트워크에서 이전 SSL/TLS 버전 차단

일부 조직에서는 정부 규제 또는 회사 정책에 따라 이전 버전의 SSL 또는 TLS를 사용하지 못하도록 해야 합니다. SSL 암호 해독 정책을 사용하여 금지한 SSL/TLS 버전을 사용하는 트래픽을 차단할 수 있습니다. 금지된 트래픽을 즉시 파악할 수 있도록 SSL 암호 해독 정책의 맨 위에 이 규칙을 배치해 보십시오.

다음 예에서는 모든 SSL 3.0 및 TLS 1.0 연결을 차단합니다.

시작하기 전에

이 절차에서는 SSL 암호 해독 정책 활성화, 473 페이지에 설명된 대로 SSL 암호 해독 정책을 이미 활성화한 것으로 가정합니다.

프로시저

단계 **1** **Policies(**정책**)** > **SSL Decryption(SSL** 암호 해독**)**을 선택합니다.

단계 **2** + 버튼을 클릭하여 새 규칙을 생성합니다.

단계 **3** Order(순서)에서 **1**을 선택하여 규칙을 정책의 맨 위에 배치하거나 네트워크에 가장 적합한 숫자를 선택합니다.

기본적으로 규칙은 정책의 끝에 추가됩니다.

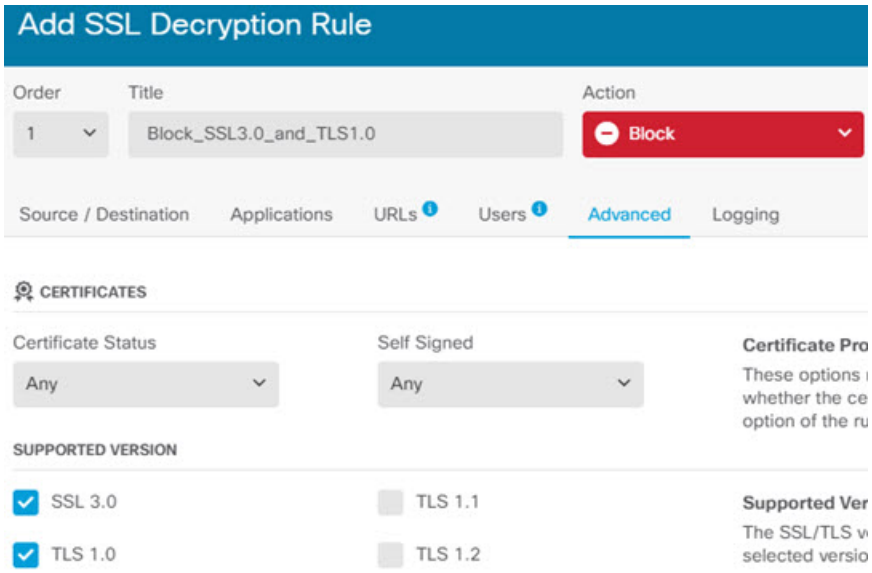
단계 **4** **Title(**제목**)**에서 규칙의 이름(예: Block_SSL3.0_and_TLS1.0)을 입력합니다.

단계 **5** **Action(**작업**)**에서 **Block(**차단**)**을 선택합니다. 그러면 규칙과 일치하는 모든 트래픽이 즉시 삭제됩니다.

단계 **6** **Source/Destination(**소스/대상**)**, **Applications(**애플리케이션**)**, **URL**, **Users(**사용자**)** 탭의 모든 옵션에 대한 기본값은 그대로 둡니다.

단계 **7** **Advanced(**고급**)** 탭을 클릭한 다음, **Supported Versions(**지원되는 버전**)**에서 SSL3.0 및 TLS1.0을 선택하고 TLS1.1 및 TLS1.2은 선택 취소합니다.

정책은 다음과 같이 표시되어야 합니다.



단계 **8** (선택 사항) 차단된 연결을 반영하는 대시보드 및 이벤트가 필요한 경우 **Logging(**로깅**)** 탭을 클릭하고 **At End of Connection(**연결 종료 시**)**을 선택합니다. 외부 syslog 서버를 사용 중인 경우, 해당 서버를 선택할 수도 있습니다.

단계 **9** **OK(**확인**)**를 클릭합니다.

이제 정책을 구축할 수 있습니다. 정책이 구축되면 시스템을 통과하는 SSL 3.0 또는 TLS 1.0 연결이 끊어집니다.

참고 SSL 2.0 연결은 정책에 대한 기본 작업에 의해 처리됩니다. 이 연결도 끊어지게 하려면 기본 작업을 Block(차단)으로 변경합니다.

다음에 수행할 작업

이 규칙을 구현하는 경우 권장 사항은 다음과 같습니다.

- 모든 유형의 암호 해독 규칙에 대해 모든 SSL/TLS 옵션이 선택되어 있는 Advanced(고급) 탭의 기본 설정을 그대로 둡니다. 이를 모든 버전에 적용하면 핸드셰이크 프로세스가 간소화됩니다. 그러나 초기 차단 규칙에서는 계속 SSL 3.0 및 TLS 1.0 연결을 방지합니다.
- 일반적으로 정책에 대한 기본 작업으로 Do Not Decrypt(암호 해독 안 함)를 사용하는 것이 좋습니다. 그러나 SSL 2.0 연결은 항상 기본 작업에 의해 처리되므로 Block(차단)을 대신 사용할 수 있습니다. 그러나 모든 해독 가능 트래픽에 대한 기본 작업으로 Do Not Decrypt(암호 해독 안 함)를 적용하려면, 트래픽 일치 기준에 대한 모든 기본값을 허용하는 정책의 끝에서 Do Not Decrypt(암호 해독 안 함) 규칙을 생성합니다. 이 규칙은 지원되는 TLS 연결 중 테이블의 이전 규칙과 일치하지 않는 연결과 일치하며 해당 TLS 버전에 대해 기본값 역할을 합니다.

SSL 암호 해독 모니터링 및 트러블슈팅

다음 주제에서는 SSL 암호 해독 정책을 모니터링하고 트러블슈팅하는 방법을 설명합니다.

SSL 암호 해독 모니터링

대시보드에서 암호 해독에 대한 정보와 로깅을 활성화한 규칙(또는 기본 작업)과 일치하는 트래픽에 대한 이벤트를 확인할 수 있습니다.

SSL 암호 해독 대시보드

전체 암호 해독 통계를 평가하려면 **Monitoring(**모니터링**)** > **SSL Decryption(SSL** 암호 해독**)** 대시보드를 확인합니다. 이 대시보드에는 다음과 같은 정보가 표시됩니다.

- 암호화된 텍스트 트래픽과 일반 텍스트 트래픽의 백분율 비교
- SSL 규칙별로 암호 해독된 암호화된 트래픽의 양

Events(이벤트)

대시보드뿐만 아니라 이벤트 뷰어(**Monitoring(**모니터링**)** > **Events(**이벤트**)**)에도 암호화된 트래픽에 대한 SSL 정보가 포함됩니다. 다음은 이벤트 평가 시 활용할 수 있는 몇 가지 팁입니다.

- 일치하는 트래픽을 차단한 SSL 규칙(또는 기본 작업)과 일치하기 때문에 삭제된 연결의 경우, **Action(**작업**)**은 "차단"이어야 하며 **Reason(**이유**)**은 "SSL 차단"을 나타내야 합니다.
- **SSL Actual Action(SSL** 실제 작업**)** 필드는 시스템이 연결에 적용한 실제 작업을 나타냅니다. 이는 일치하는 규칙에 정의된 작업을 나타내는 **SSL Expected Action(SSL** 예상 작업**)** 과 다를 수 있습니다. 예를 들어 연결이 암호 해독을 적용하는 규칙과 일치할 수 있으나, 어떠한 이유로든 암호 해독되지 않을 수 있습니다.

재서명 암호 해독이 브라우저에서는 작동하지만 앱에서는 작동하지 않는 웹 사이트 처리(SSL 또는 인증 기관 피닝)

스마트폰 및 기타 디바이스용 일부 앱은 SSL(또는 인증 기관) 피닝이라는 기술을 사용합니다. SSL 피닝 기술은 원래 서버 인증서의 해시를 앱 자체에 포함합니다. 따라서 앱이 threat defense 디바이스에서 재서명된 인증서를 받으면 해시 검증에 실패하고 연결이 중단됩니다.

이때 기본적인 증상은 사용자가 사이트 앱을 사용해서는 웹 사이트에 연결할 수 없지만 웹 브라우저를 사용하면 연결할 수 있다는 것입니다(앱으로 연결에 실패한 디바이스에서 브라우저를 사용할 때도 연결 가능). 사용자가 Facebook iOS 또는 Android 앱은 사용할 수 없지만 Safari나 Chrome에서 https://www.facebook.com을 입력하면 연결할 수 있는 경우를 예로 들 수 있습니다.

SSL 피닝은 특별히 메시지 가로채기(man-in-the-middle) 공격을 차단하는 데 사용되므로 이러한 현상을 해결하는 방법은 없습니다. 다음 옵션 중에서 선택해야 합니다.

- 앱 사용자를 지원합니다. 이 경우 사이트로의 트래픽을 암호 해독할 수 없습니다. SSL Decryption(SSL 암호 해독) 규칙의 Application(애플리케이션) 탭에서 사이트 애플리케이션용 Do Not Decrypt(암호 해독 안 함) 규칙을 생성하고, 이 규칙을 연결에 적용할 Decrypt Re-sign(재서명 암호 해독) 규칙 앞에 배치합니다.
- 사용자들이 브라우저만 사용하도록 강제합니다. 사이트로의 트래픽을 암호 해독해야 하는 경우에는 사용자에게 네트워크를 통해 연결할 때 사이트 앱을 사용할 수 없으며 브라우저만 사용해야 함을 알려야 합니다.

기타 세부정보

특정 사이트가 브라우저에서는 작동하는데 동일 디바이스의 앱에서는 작동하지 않는 경우 SSL 피닝 인스턴스를 살펴봐야 합니다. 하지만 심층적으로 확인하려면 연결 이벤트를 사용해 브라우저 테스트와 더불어 SSL 피닝을 확인할 수 있습니다.

앱은 두 가지 방식으로 해시 검증 장애를 처리할 수 있습니다.

- Facebook 등의 그룹 1 앱은 서버에서 SH, CERT, SHD 메시지를 받는 즉시 SSL ALERT 메시지를 보냅니다. Alert는 보통 SSL 피닝을 나타내는 "Unknown CA (48)(알 수 없는 CA(48))" 알림입니다. 알림 메시지 후에는 TCP Reset(TCP 재설정)이 전송됩니다. 이벤트 세부사항에는 다음 증상이 표시됩니다.
  - SSL Flow Flag(SSL 플로우 플래그)에는 ALERT_SEEN이 포함되어 있습니다.
  - SSL Flow Flag(SSL 플로우 플래그)에는 APP_DATA_C2S 또는 APP_DATA_S2C가 포함되어 있지 않습니다.
  - SSL Flow Message(SSL 플로우 메시지)는 보통 CLIENT_HELLO, SERVER_HELLO, SERVER_CERTIFICATE, SERVER_KEY_EXCHANGE, SERVER_HELLO_DONE입니다.
- Dropbox 등의 그룹 2 앱은 알림을 보내지 않습니다. 대신 핸드셰이크가 완료될 때까지 기다렸다가 TCP Reset(TCP 재설정)을 전송합니다. 이벤트에는 다음 증상이 표시됩니다.
  - SSL Flow Flag(SSL 플로우 플래그)에는 ALERT_SEEN, APP_DATA_C2S 또는 APP_DATA_S2C가 포함되어 있지 않습니다.
  - SSL Flow Message(SSL 플로우 메시지)는 보통 CLIENT_HELLO, SERVER_HELLO, SERVER_CERTIFICATE, SERVER_KEY_EXCHANGE, SERVER_HELLO_DONE, CLIENT_KEY_EXCHANGE, CLIENT_CHANGE_CIPHER_SPEC, CLIENT_FINISHED, SERVER_CHANGE_CIPHER_SPEC, SERVER_FINISHED입니다.

재서명 암호 해독이 브라우저에서는 작동하지만 앱에서는 작동하지 않는 웹 사이트 처리**(SSL** 또는 인증 기관 피닝**)**

19 장

ID 정책

연결에서 사용자 ID 정보를 수집하기 위해 ID 정책을 사용할 수 있습니다. 그런 다음 대시보드에서 사용자 ID를 기준으로 사용량을 보고 사용자 또는 사용자 그룹을 기준으로 액세스 제어를 구성할 수 있습니다.

ID 정책 개요

ID 정책을 사용하여 연결과 연계된 사용자를 탐지할 수 있습니다. 사용자를 식별하면 위협, 엔드포인트 및 네트워크 인텔리전스를 사용자 ID 정보와 연결할 수 있습니다. 시스템에서 네트워크 행동, 트래픽 및 이벤트를 개별 사용자와 직접 연결하므로 정책 위반, 공격 또는 네트워크 취약점의 소스를 손쉽게 식별할 수 있습니다.

예를 들어 침입 이벤트의 대상인 호스트를 소유한 사용자와 내부 공격 또는 포트 스캔을 시작한 사용자를 식별할 수 있습니다. 부적절한 웹 사이트 또는 애플리케이션에 액세스하는 사용자 및 대역폭을 많이 사용하는 사용자도 식별할 수 있습니다.

사용자 탐지에서는 분석용 데이터 수집 이외의 작업도 수행할 수 있습니다. 사용자 이름 또는 사용자 그룹 이름을 기준으로 액세스 규칙을 작성하여 사용자 ID를 기준으로 리소스에 대한 액세스를 선택적으로 허용하거나 차단할 수도 있습니다.

다음 방법을 통해 사용자 ID를 획득할 수 있습니다.

- 패시브 인증 - 모든 유형의 연결에 대해, 사용자 이름과 비밀번호를 입력하라는 메시지를 표시하지 않고 다른 인증 서비스를 통해 사용자 ID를 획득합니다.
- 액티브 인증 - HTTP 연결에만 사용자 이름과 비밀번호를 입력하라는 메시지를 표시하고, 소스 IP 주소의 사용자 ID를 획득하기 위해 지정된 ID 소스를 통해 인증을 수행합니다.

다음 주제에서는 사용자 ID에 대해 자세히 설명합니다.

패시브 인증을 통한 사용자 **ID** 설정

패시브 인증은 사용자에게 사용자 이름 및 비밀번호를 요구하지 않고 사용자 ID를 수집합니다. 시스템은 지정된 ID 소스에서 매핑을 가져옵니다.

다음 소스에서 패시브 방식으로 사용자-IP 주소 매핑을 획득할 수 있습니다.

- 원격 액세스 VPN 로그인. 패시브 ID에 대해 지원되는 사용자 유형은 다음과 같습니다.
  - 외부 인증 서버에 정의된 사용자 어카운트.
  - device manager에 정의된 로컬 사용자 어카운트.
- Cisco ISE(Identity Services Engine), Cisco ISE PIC(Identity Services Engine Passive Identity Connector)

지정된 사용자가 둘 이상의 소스를 통해 식별되는 경우에는 RA VPN ID가 우선적으로 사용됩니다.

활성 인증을 통한 사용자 **ID** 설정

인증은 사용자의 ID를 확인하는 작업입니다.

활성 인증을 사용하는 경우, 시스템에 사용자-ID 매핑이 없는 IP 주소에서 HTTP 트래픽 흐름이 유입되는 경우 시스템에 구성된 디렉터리에 대해 트래픽 흐름을 시작한 사용자를 인증할지를 결정할 수 있습니다. 사용자가 정상적으로 인증하면 해당 IP 주소는 인증된 사용자의 ID를 포함하는 것으로 간주됩니다.

인증이 실패해도 사용자의 네트워크 액세스는 차단되지 않습니다. 최종적으로는 액세스 규칙에 따라 이러한 사용자에게 제공할 액세스 권한이 결정됩니다.

알 수 없는 사용자 처리

ID 정책에 대해 디렉터리 서버를 구성할 때 시스템은 디렉터리 서버에서 사용자 및 그룹 멤버십 정보를 다운로드합니다. 이 정보는 24시간마다 자정에 또는 디렉터리 컨피그레이션을 수정하고 저장할 때마다 새로 고침됩니다. 정보를 변경하지 않는 경우에도 마찬가지입니다.

사용자가 활성 인증 ID 규칙에 따라 인증에 성공했으나 사용자 이름이 다운로드된 사용자 ID 정보에 없으면 해당 사용자는 알 수 없음으로 표시됩니다. 사용자 ID와 사용자 일치 그룹 규칙은 ID 관련 대시보드에 표시되지 않습니다.

그러나 알 수 없음 사용자에 대한 모든 액세스 제어 규칙은 적용됩니다. 예를 들어 알 수 없음 사용자에 대한 연결을 차단하는 경우, 해당 사용자는 인증에 성공하더라도(즉, 디렉터리 서버에서 사용자와 비밀번호를 유효한 것으로 인식하더라도) 차단됩니다.

그러므로 사용자를 추가 또는 삭제하거나 그룹 멤버십을 변경하는 등 디렉터리 서버를 변경하면 시스템이 디렉터리에서 업데이트를 다운로드할 때까지는 해당 변경 사항이 정책 시행에 반영되지 않습니다.

매일 자정 업데이트가 수행될 때까지 기다리지 않으려면 디렉터리 영역 정보를 수정하여(**Objects(**개체**)** > **Identity Sources(ID** 소스**)**에서 해당 영역 수정) 업데이트를 강제로 수행할 수 있습니다. **Save(**저장**)**를 클릭한 다음 변경 사항을 구축합니다. 그러면 시스템이 업데이트를 즉시 다운로드합니다.

참고 **Policies(**정책**)** > **Access Control(**액세스 제어**)**로 이동하여 **Add Rule (+)(**규칙 추가**(+))** 버튼을 클릭하고 **Users(**사용자**)** 탭에서 사용자 목록을 확인하여 새 사용자 정보 또는 삭제된 사용자 정보가 시스템에 있는지를 확인할 수 있습니다. 새 사용자를 찾을 수 없거나 삭제된 사용자를 찾을 수 있으면 시스템의 정보는 오래된 것입니다.

ID 정책을 구현하는 방법

IP 주소와 연결된 사용자를 알 수 있도록 사용자 ID 획득을 활성화하려면 여러 항목을 구성해야 합니다. 이러한 항목을 정확하게 구성하면 모니터링 대시보드 및 이벤트에서 사용자 이름을 확인할 수 있습니다. 또한 액세스 제어 및 SSL 암호 해독 규칙에서 사용자 ID를 트래픽 일치 기준으로 사용할 수도 있습니다.

다음 절차에서는 ID 정책이 작동하도록 하려면 구성해야 하는 항목의 개요를 제공합니다.

프로시저

단계 **1** AD ID 영역을 구성합니다.

사용자 인증 프롬프트를 표시하여 사용자 ID를 활성 방식으로 수집하든 아니면 패시브 방식으로 수집하든 관계없이 사용자 ID 정보가 포함된 AD(Active Directory) 서버를 구성해야 합니다. AD ID 영역 구성, 177 페이지의 내용을 참조하십시오.

패시브 ID를 구성하는 경우, 두 개 이상의 AD 영역에 있는 ID에서 시스템을 가져올 수 있는 AD 영역 시퀀스를 생성할 수 있습니다. 이는 네트워크에 여러 AD 도메인이 있는 경우 유용합니다.

단계 **2** 패시브 인증 ID 규칙을 사용하려는 경우 패시브 ID 소스를 구성합니다.

디바이스에서 구현하는 서비스와 네트워크에서 사용 가능한 서비스를 기준으로 하여 다음 중 원하는 소스를 구성할 수 있습니다.

- 원격 액세스 VPN - 디바이스에 대한 원격 액세스 VPN 연결을 지원하려는 경우 사용자 로그인은 device manager 내에 정의된 로컬 사용자 또는 AD 서버를 기준으로 하여 ID를 제공할 수 있습니다. RA VPN 구성에 대한 정보는 원격 액세스 VPN 구성, 733 페이지의 내용을 참조하십시오.
- Cisco ISE(Identity Services Engine) 또는 Cisco ISE PIC(Identity Services Engine Passive Identity Connector) - 이러한 제품을 사용하는 경우에는 디바이스를 pxGrid 서브스크라이버로 구성하고 ISE에서 사용자 ID를 획득할 수 있습니다. ISE(Identity Services Engine) 구성, 187 페이지의 내용을 참조하십시오.

단계 **3** **Policies(**정책**)** > **Identity(ID)**를 선택하고 ID 정책을 활성화합니다. ID 정책 구성, 495 페이지의 내용을 참조하십시오.

단계 **4** ID 정책 설정 구성, 496 페이지.

패시브 ID 소스는 시스템에서 구성한 소스를 기준으로 하여 자동으로 선택됩니다. 활성 인증을 구성하려는 경우 종속 포털 및 SSL 재서명 암호 해독(SSL 암호 해독 정책을 아직 활성화하지 않은 경우)용 인증서를 구성해야 합니다.

단계 **5** ID 정책 기본 작업 구성, 498 페이지.

패시브 인증만 사용하려는 경우에는 기본 작업을 패시브 인증으로 설정할 수 있으며, 구체적인 규칙을 생성할 필요가 없습니다.

단계 **6** ID 규칙 구성, 498 페이지.

관련 네트워크에서 패시브 또는 액티브 사용자 ID를 수집할 규칙을 생성합니다.

활성 인증 모범 사례

ID 규칙에서 사용자에 대한 액티브 인증을 요구하는 경우 사용자는 연결 시에 사용한 인터페이스의 캡티브 포털 포트로 리디렉션되며, 그리고 나면 인증하라는 메시지가 표시됩니다.

이 리디렉션은 인터페이스 IP 주소에 대한 것이므로 ID 정책 인증서가 정확하게 일치하지 않으며, 사용자에게 신뢰할 수 없는 인증서 오류가 발생합니다. 사용자가 인증서를 수락해야 디바이스를 계속 인증할 수 있습니다. 이 동작은 중간자(man-in-the-middle) 공격과 유사하므로 사용자는 신뢰할 수 없는 인증서를 수락하지 않습니다.

이 문제를 방지하기 위해 디바이스에서 한 인터페이스의 정규화된 도메인 이름(FQDN)을 사용하도록 활성 인증을 구성할 수 있습니다. 올바르게 구성된 인증서를 사용하면 신뢰할 수 없는 인증서 오류가 발생하지 않으며, 인증이 더 원활하고 안전해집니다.

시작하기 전에

활성 인증은 HTTP 트래픽에 대해서만 발생하며, 디바이스에 사용자의 워크스테이션 또는 다른 클라이언트 디바이스에 대한 현재 사용자 매핑이 없는 경우 최종 사용자에게 중단이 발생합니다. 수동 인증을 대신 구현하여 중단을 방지할 수 있습니다.

프로시저

단계 **1** DNS 서버에서 활성 인증 수집에 사용할 인터페이스의 인터페이스 IP 주소에 대한 정규화된 도메인 이름(FQDN)을 정의합니다.

종속 포털이라고도 하는 이 인터페이스는 라우팅 인터페이스여야 합니다.

단계 **2** CA(Certificate Authority)를 사용하여 이 FQDN에 대한 인증서를 가져옵니다.

ftd1.captive-port.example.com과 같은 특정 FQDN에 대한 인증서를 생성할 수 있습니다. 또는 다음을 수행할 수 있습니다.

- 여러 디바이스의 종속 포털 인터페이스에 적용할 수 있는 와일드카드 인증서를 가져옵니다(예: *.captive-port.example.com). 와일드카드는 더 광범위할 수 있으며, 넓은 범위의 엔드포인트 클래스에 적용할 수 있습니다(예: *.eng.example.com 또는 even *.example.com).
- 인증서에 여러 SAN(Subject Alternate Name)을 포함합니다.

단계 **3** **Objects(**개체**)** > **Certificates(**인증서**)**를 선택하고 인증서를 업로드합니다.

단계 **4** **Objects(**개체**)** > **Network(**네트워크**)**를 선택하고 DNS 이름에 대한 FQDN 네트워크 개체를 생성합니다.

단계 **5** **Policies(**정책**)** > **Identity(ID)** 페이지에서 인증서 및 FQDN 개체로 ID 정책 설정을 업데이트합니다.

단계 **6** 활성 인증을 사용하는 ID 정책에서 규칙을 생성합니다.

ID 정책 구성

연결에서 사용자 ID 정보를 수집하기 위해 ID 정책을 사용할 수 있습니다. 그런 다음 대시보드에서 사용자 ID를 기준으로 사용량을 보고 사용자 또는 사용자 그룹을 기준으로 액세스 제어를 구성할 수 있습니다.

아래에서는 ID 정책을 통해 사용자 ID를 가져오는 데 필요한 요소를 구성하는 방법을 간략하게 설명합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Identity(ID)**를 선택합니다.

ID 정책을 아직 정의하지 않은 경우 **ID** 정책 활성화를 클릭하여 ID 정책 설정 구성, 496 페이지에서 설명하는 대로 설정을 구성합니다.

단계 **2** ID 정책을 관리합니다.

ID 설정을 구성하고 나면 이 페이지에 모든 규칙이 순서대로 나열됩니다. 목록의 맨 위에서부터 규칙과 트래픽의 일치 여부를 확인하며, 첫 번째로 일치하는 규칙에 따라 적용할 작업이 결정됩니다. 이 페이지에서는 다음을 수행할 수 있습니다.

- ID 정책을 활성화하거나 비활성화하려면 **ID** 정책 토글을 클릭합니다.
- ID 정책 설정을 변경하려면 **Identity Policy Configuration(ID** 정책 컨피그레이션**)** 버튼()을 클릭하십시오.
- **Default Action(**기본 작업**)**을 변경하려면 작업을 클릭하고 원하는 작업을 선택합니다. ID 정책 기본 작업 구성, 498 페이지의 내용을 참조하십시오.
- 규칙을 이동하려면 규칙을 수정하고 **Order(**순서**)** 드롭다운 목록에서 새 위치를 선택합니다.
- 규칙을 구성하려면 다음을 수행합니다.

- 새 규칙을 생성하려면 + 버튼을 클릭합니다.
- 기존 규칙을 수정하려면 Actions(작업) 열에서 해당 규칙의 수정 아이콘()을 클릭합니다. 테이블에서 속성을 클릭하여 규칙 속성을 선택적으로 수정할 수도 있습니다.
- 더 이상 필요하지 않은 규칙을 삭제하려면 Actions(작업) 열에서 해당 규칙의 삭제 아이콘()을 클릭합니다.

ID 규칙 생성 및 수정에 대한 자세한 내용은 ID 규칙 구성, 498 페이지를 참조하십시오.

ID 정책 설정 구성

ID 정책이 작동하려면 사용자 ID 정보를 제공하는 소스를 구성해야 합니다. 구성해야 하는 설정은 구성할 규칙의 유형(패시브, 액티브 또는 모두)에 따라 다릅니다.

Settings(설정) 대화 상자에서는 이러한 설정이 개별 섹션에 표시됩니다. 대화 상자에 액세스하는 방법에 따라 두 섹션이 모두 표시될 수도 있고 한 섹션만 표시될 수도 있습니다. 필수 설정을 사전에 구성하지 않은 상태로 인증 유형에 대한 규칙을 생성하려고 하면 대화 상자가 자동으로 나타납니다.

다음 절차에서는 전체 대화 상자에 대해 설명합니다.

시작하기 전에

디렉터리 서버, threat defense 디바이스 및 클라이언트에서 시간 설정이 서로 일치하는지 확인합니다. 이러한 디바이스 간에 시간이 바뀌면 사용자가 정상적으로 인증하지 못할 수 있습니다. 여기서 "일치"란 여러 표준 시간대를 사용할 수는 있지만 이러한 표준 시간대를 기준으로 할 때 시간이 동일해야 한다는 의미입니다. 예를 들어 PST로 오전 10시는 EST로 오후 1시에 해당합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Identity(ID)**를 선택합니다.

단계 **2** **Identity Policy Configuration(ID** 정책 컨피그레이션**)** 버튼()을 클릭하십시오.

단계 **3** **Passive Authentication(**패시브 인증**)** 옵션을 구성합니다.

대화 상자에는 이미 구성한 패시브 인증 소스가 표시됩니다.

필요한 경우 이 대화 상자를 통해 ISE를 구성할 수 있습니다. ISE 개체를 아직 구성하지 않은 경우 **Integrate ISE(ISE** 통합**)** 링크를 클릭하여 바로 ISE 개체를 생성할 수 있습니다. 개체가 있는 경우 해당 상태와 함께 나열됩니다. 상태는 Enabled(활성화됨) 또는 Disabled(비활성화됨)입니다.

패시브 인증 규칙을 생성하려면 하나 이상의 활성화된 패시브 ID 소스를 구성한 상태여야 합니다.

단계 **4** 액티브 인증 옵션을 구성합니다.

ID 규칙에서 사용자에 대한 활성 인증을 요구하는 경우 사용자는 종속 포털 포트로 리디렉션되며, 이후에는 인증하라는 메시지가 표시됩니다. 이러한 설정을 구성하기 전에 활성 인증 모범 사례, 494 페이지 항목을 읽어보십시오.

- **Server Certificate(**서버 인증서**)** — 활성 인증 중에 사용자에게 제공할 내부 인증서를 선택합니다. 필요한 인증서를 아직 생성하지 않은 경우 드롭다운 목록 하단에서 **Create New Internal Certificate(**새 내부 인증서 생성**)**를 클릭합니다.

  사용자의 브라우저에서 이미 신뢰하는 인증서를 업로드하지 않으면 사용자가 인증서를 허용해야 합니다.

- **Redirect to Host Name(**호스트 이름으로 리디렉션**)**(Snort 3.0만 해당) — 활성 인증 요청에 대한 종속 포털로 사용해야 하는 인터페이스의 정규화된 호스트 이름을 정의하는 네트워크 개체를 선택합니다. 개체가 없는 경우, **Create New Network(**새 네트워크 생성**)**를 클릭합니다.

  FQDN은 디바이스에 있는 인터페이스 중 하나의 IP 주소로 확인되어야 합니다. FQDN을 사용하면 클라이언트가 인식할 활성 인증에 대한 인증서를 할당할 수 있으므로, IP 주소로 리디렉션될 때 신뢰할 수 없는 인증서 경고가 표시되지 않습니다. 인증서는 인증서의 SAN(Subject Alternate Name)에 FQDN, 와일드카드 FQDN 또는 여러 FQDN을 지정할 수 있습니다.

  ID 규칙에서 사용자에 대한 활성 인증을 요구하지만 리디렉션 FQDN을 지정하지 않는 경우 사용자는 연결 시 사용한 인터페이스의 종속 포털 포트로 리디렉션됩니다.

- **Port(**포트**)** - 종속 포털 포트입니다. 기본값은 885(TCP)입니다. 다른 포트를 구성하는 경우에는 포트가 1025-65535 범위에 포함되어야 합니다.

  참고 호스트 이름으로 리디렉션 FQDN을 제공하지 않는 경우 HTTP 기본, HTTP 응답 페이지 및 NTLM 인증 방법에서 인터페이스의 IP 주소를 사용하여 사용자를 종속 포털로 리디렉션합니다. 그러나 HTTP 협상의 경우에는 사용자가 정규화된 DNS 이름 *firewall-hostname.AD-domain-name*을 사용하여 리디렉션됩니다. 호스트 이름으로 리디렉션 FQDN 없이 HTTP 협상을 사용하려는 경우에는 DNS 서버도 업데이트하여 활성 인증을 수행해야 하는 모든 내부 인터페이스의 IP 주소에 이 이름을 매핑해야 합니다. 이렇게 하지 않으면 리디렉션을 완료할 수 없으며 사용자가 인증할 수 없습니다. 인증 방법과 무관하게 일관된 동작을 보장하기 위해 항상 호스트 이름으로 리디렉션 FQDN을 제공하는 것이 좋습니다.

단계 **5** (활성 인증에만 해당됨) **Decrypt Re-Sign Certificate(**재서명 암호 해독 인증서**)**에서 재서명된 인증서를 이용하여 암호 해독을 구현하는 규칙에 사용할 내부 CA 인증서를 선택합니다.

사전 정의된 NGFW-Default-InternalCA 인증서를 사용하거나, 생성 또는 업로드한 인증서를 사용할 수 있습니다. 인증서가 아직 없으면 **Create Internal CA(**내부 **CA** 생성**)**를 클릭하여 생성합니다.

클라이언트 브라우저에서 인증서를 아직 설치하지 않은 경우, 다운로드 버튼( )을 클릭하여 복사본을 획득합니다. 인증서 설치 방법에 대한 자세한 내용은 각 브라우저에 대한 설명서를 참조하십시오. 재서명 암호 해독 규칙을 위한 CA 인증서 다운로드, 484 페이지도 참조하십시오.

참고 SSL 암호 해독 정책을 아직 구성하지 않은 경우에만 SSL 암호 해독 설정에 대한 프롬프트가 표시됩니다. ID 정책을 활성화한 후에 이러한 설정을 변경하려면 SSL 암호 해독 정책 설정을 편집합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

ID 정책 기본 작업 구성

ID 정책은 개별 ID 규칙과 일치하지 않는 모든 연결에 대해 구현되는 기본 작업입니다.

실제로 규칙이 없는 것도 정책에 대해 유효한 컨피그레이션입니다. 모든 트래픽 소스에서 패시브 인증을 사용하려는 경우에는 기본 작업으로 패시브 인증을 구성하면 됩니다.

프로시저

단계 **1** **Policies(**정책**)** > **Identity(ID)**를 선택합니다.

단계 **2** **Default Action(**기본 작업**)**을 클릭하고 다음 중 하나를 선택합니다.

- **Passive Auth (Any Identity Source)(**패시브 인증**(**모든 **ID** 소스**))** - ID 규칙과 일치하지 않는 연결에 대해 구성된 모든 패시브 ID 소스를 사용하여 사용자 ID가 결정됩니다. 패시브 ID 소스를 구성하지 않는 경우 Passive Auth(패시브 인증)를 기본값으로 사용하는 것은 No Auth(인증 없음)를 사용하는 것과 같습니다.
- **No Auth (No Authentication Required)(**인증 없음**(**인증 필요 없음**))** - ID 규칙과 일치하지 않는 연결에 대해서는 사용자 ID가 확인되지 않습니다.

ID 규칙 구성

ID 규칙은 일치하는 트래픽에 대해 사용자 ID 정보를 수집할지 여부를 결정합니다. 일치하는 트래픽에 대해 사용자 ID 정보를 가져오지 않으려는 경우에는 인증 없음을 구성할 수 있습니다.

규칙 컨피그레이션에 관계없이 액티브 인증은 HTTP 트래픽에 대해서만 수행됩니다. 따라서 액티브 인증에서 비 HTTP 트래픽을 제외하는 규칙을 생성할 필요가 없습니다. 모든 HTTP 트래픽에 대해 사용자 ID 정보를 가져오려면 모든 소스와 대상에 대해 활성 인증 규칙만 적용하면 됩니다.

참고 인증에서 장애가 발생해도 네트워크 액세스에는 아무 영향이 없습니다. ID 정책은 사용자 ID 정보만 수집합니다. 인증 시에 장애가 발생한 사용자의 네트워크 액세스를 차단하려는 경우에는 액세스 규칙을 사용해야 합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Identity(ID)**를 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 새 규칙을 생성하려면 + 버튼을 클릭합니다.
- 기존 규칙을 수정하려면 해당 규칙의 수정 아이콘()을 클릭합니다.

더 이상 필요하지 않은 규칙을 삭제하려면 해당 규칙의 삭제 아이콘()을 클릭합니다.

단계 **3** **Order(**순서**)**에서 순서가 지정된 규칙 목록에 규칙을 삽입할 위치를 선택합니다.

규칙은 처음 일치하는 항목을 기준으로 적용되므로, 매우 구체적인 트래픽 일치 기준이 포함된 규칙이 보다 일반적인 기준이 포함된 정책(규칙이 일치하지 않는 경우 일치하는 트래픽에 적용됨) 위에 표시되도록 삽입해야 합니다.

기본적으로는 규칙이 목록의 끝에 추가됩니다. 나중에 규칙의 위치를 변경하려는 경우 이 옵션을 수정합니다.

단계 **4** **Tile(**제목**)**에서 규칙의 이름을 입력합니다.

단계 **5** **Action(**작업**)**을 선택하고 필요한 경우 **AD Identity Source(AD ID** 소스**)**를 선택합니다.

패시브 및 활성 인증 규칙용 사용자 어카운트를 포함하는 AD ID 영역을 선택해야 합니다. 필요한 영역이 아직 없는 경우, **Create New Identity Realm(**새 **ID** 영역 생성**)**을 클릭하여 바로 생성합니다. 패시브 인증의 경우 단일 AD 영역 개체 대신 AD 영역 시퀀스를 선택할 수 있습니다.

- **Passive Auth(**패시브 인증**)** - 패시브 인증을 통해 사용자 ID를 확인합니다. 구성된 모든 ID 소스가 표시됩니다. 규칙은 구성된 모든 소스를 자동으로 사용합니다.
- **Active Auth(**활성 인증**)** - 활성 인증을 통해 사용자 ID를 확인합니다. 액티브 인증은 HTTP 트래픽에만 적용됩니다. 다른 트래픽 유형이 액티브 인증을 요구하거나 허용하는 ID 정책과 일치하는 경우에는 액티브 인증을 시도하지 않습니다.
- **No Auth(**인증 없음**)** - 사용자 ID를 가져오지 않습니다. 이 트래픽에는 ID 기반 액세스 규칙이 적용되지 않습니다. 이러한 사용자는 인증 필요 없음으로 표시됩니다.

단계 **6** (액티브 인증에만 해당됨) 디렉터리 서버에서 지원하는 인증 방법(유형)을 선택합니다.

- **HTTP** 기본 - 암호화되지 않은 HTTP BA(기본 인증) 연결을 통해 사용자를 인증합니다. 사용자는 브라우저의 기본 인증 팝업 창을 통해 네트워크에 로그인합니다. 이는 기본값입니다.
- **NTLM** - NTLM(NT LAN Manager) 연결을 통해 사용자를 인증합니다. 이 선택 사항은 AD 영역을 선택할 때만 사용 가능합니다. 사용자가 브라우저의 기본 인증 팝업 창을 통해 네트워크에 로그인합니다. 그러나 사용자가 Windows 도메인 로그인을 통해 투명하게 인증을 하도록 IE 및 Firefox 브라우저를 구성할 수 있습니다(투명 사용자 인증 활성화, 502 페이지 참조).
- **HTTP** 협상 - 디바이스가 사용자 에이전트(사용자가 트래픽 흐름을 시작하는 데 사용 중인 애플리케이션)와 Active Directory 서버 간에 방법을 협상할 수 있도록 합니다. 협상 시에는 일반적으로 지원되는 가장 강력한 방법이 순서대로 사용됩니다(NTLM -> 기본). 사용자는 브라우저의 기본 인증 팝업 창을 통해 네트워크에 로그인합니다.
- **HTTP** 대응 페이지 - 시스템 제공 웹 페이지를 통해 인증하라는 메시지를 사용자에게 표시합니다. 이 방법은 일종의 HTTP 기본 인증입니다.

참고 호스트 이름으로 리디렉션 FQDN을 제공하지 않는 경우 HTTP 기본, HTTP 응답 페이지 및 NTLM 인증 방법에서 인터페이스의 IP 주소를 사용하여 사용자를 종속 포털로 리디렉션합니다. 그러나 HTTP 협상의 경우에는 사용자가 정규화된 DNS 이름 *firewall-hostname.AD-domain-name*을 사용하여 리디렉션됩니다. 호스트 이름으로 리디렉션 FQDN 없이 HTTP 협상을 사용하려는 경우에는 DNS 서버도 업데이트하여 활성 인증을 수행해야 하는 모든 내부 인터페이스의 IP 주소에 이 이름을 매핑해야 합니다. 이렇게 하지 않으면 리디렉션을 완료할 수 없으며 사용자가 인증할 수 없습니다. 인증 방법과 무관하게 일관된 동작을 보장하기 위해 항상 호스트 이름으로 리디렉션 FQDN을 제공하는 것이 좋습니다.

단계 **7** (활성 인증에만 해당됨) 활성 인증에서 장애가 발생하는 사용자에게 게스트 사용자 레이블을 지정할지를 결정하려면 **Fall Back as Guest(**게스트로 폴백**)** > **On/Off(**켜기/끄기**)**를 선택합니다.

사용자에게는 3번의 인증 기회가 제공됩니다. 인증에서 장애가 발생하면 이 옵션의 선택 여부에 따라 사용자 표시 방법이 결정됩니다. 이러한 값을 기준으로 액세스 규칙을 작성할 수 있습니다.

- **Fall Back as Guest(**게스트로 폴백**)** > **On(**켜기**)** - 사용자가 게스트로 표시됩니다.
- **Fall Back as Guest(**게스트로 폴백**)** > **Off(**끄기**)** - 사용자가 실패한 인증으로 표시됩니다.

단계 **8** **Source/Destination(**소스/대상**)** 탭에서 트래픽 일치 기준을 정의합니다.

HTTP 트래픽에 대해서만 액티브 인증을 시도합니다. 그러므로 비 HTTP 트래픽에 대해서는 인증 없음 규칙을 구성할 필요가 없으며 액티브 인증 규칙을 생성할 필요도 없습니다. 그러나 패시브 인증은 모든 유형의 트래픽에 유효합니다.

ID 규칙의 소스/대상 기준은 트래픽이 통과하는 보안 영역(인터페이스), IP 주소나 IP 주소의 국가나 대륙(지리적 위치) 또는 트래픽에서 사용되는 프로토콜과 포트를 정의합니다. 기본값은 모든 영역, 주소, 지리적 위치, 프로토콜 및 포트입니다.

조건을 수정하려면 해당 조건 내의 **+** 버튼을 클릭하고 필요한 개체나 요소를 선택한 후에 팝업 대화상자에서 **OK(**확인**)**를 클릭합니다. 기준에 개체가 필요한데 필요한 개체가 없는 경우에는 새 개체 생성을 클릭하면 됩니다. 개체 또는 요소의 **x**를 클릭하면 정책에서 해당 개체나 요소를 제거할 수 있습니다.

다음과 같은 트래픽 일치 기준을 구성할 수 있습니다.

소스 영역**,** 대상 영역

트래픽이 통과하는 인터페이스를 정의하는 보안 영역 개체입니다. 기준은 하나 또는 둘 다 정의할 수도 있고 둘 다 정의하지 않을 수도 있습니다. 지정되지 않은 기준은 임의 인터페이스의 트래픽에 적용됩니다.

- 영역 내 인터페이스의 디바이스에서 나가는 트래픽에 일치시키기 위해서는 대상 영역에 해당 영역을 추가합니다.
- 영역 내 인터페이스를 통해 디바이스로 들어오는 트래픽에 일치시키기 위해서는 소스 영역에 해당 영역을 추가합니다.
- 규칙에 소스와 대상 영역 조건을 모두 추가한 경우, 일치하는 트래픽은 반드시 지정된 소스 영역 중 하나에서 발생해야 하며 대상 영역 중 하나를 통해 전송되어야 합니다.

트래픽이 디바이스로 들어오거나 디바이스에서 나가는 위치를 기준으로 규칙을 적용해야 하는 경우 이 기준을 사용해야 합니다. 예를 들어 내부 네트워크에서 생성되는 모든 트래픽에서 사용자 ID를 수집하려는 경우 내부 영역을 소스 영역으로 선택하고 대상 영역은 비워 둡니다.

참고 단일 규칙에서 패시브 보안 영역과 라우팅 보안 영역을 함께 사용할 수는 없습니다. 또한 패시브 보안 영역은 소스 영역으로만 지정할 수 있으며 대상 영역으로 지정할 수는 없습니다.

소스 네트워크**,** 대상 네트워크

트래픽의 네트워크 주소나 위치를 정의하는 네트워크 개체 또는 지리적 위치입니다.

- 특정 IP 주소 또는 지리적 위치에서 나오는 트래픽을 일치시키려면 소스 네트워크를 구성합니다.
- 특정 IP 주소 또는 지리적 위치로 향하는 트래픽을 일치시키려면 대상 네트워크를 구성합니다.
- 규칙에 소스와 대상 네트워크 조건을 모두 추가한 경우, 일치하는 트래픽은 반드시 지정된 IP 주소 중 하나에서 발생해야 하며 그 목적지가 대상 IP 주소 중 하나여야 합니다.

이 기준을 추가할 때는 다음 탭에서 선택합니다.

- 네트워크 - 제어하려는 트래픽의 소스 또는 대상 IP 주소를 정의하는 네트워크 개체 또는 그룹을 선택합니다.
- 지리위치 - 소스 또는 대상 국가나 대륙을 기준으로 트래픽을 제어하려면 지리적 위치를 선택합니다. 대륙을 선택하면 대륙 내의 모든 국가가 선택됩니다. 규칙에서 지리적 위치를 직접 선택하는 방법 외에, 위치를 정의하기 위해 생성한 지리위치 개체를 선택할 수도 있습니다. 지리적 위치를 사용하면 특정 국가에서 사용될 수 있는 모든 IP 주소를 몰라도 해당 국가에 대한 액세스를 쉽게 제한할 수 있습니다.

  참고 최신 지리적 위치 데이터를 사용하여 트래픽을 필터링하려면 GeoDB(geolocation database)를 정기적으로 업데이트하는 것이 좋습니다.

소스 포트**,** 대상 포트/프로토콜

트래픽에 사용되는 프로토콜을 정의하는 포트 개체입니다. TCP/UDP의 경우 여기에는 포트가 포함될 수 있습니다.

- 특정 프로토콜이나 포트에서 나오는 트래픽을 일치시키려면 소스 포트를 구성합니다. 소스 포트는 TCP/UDP 전용일 수 있습니다.
- 특정 프로토콜이나 포트로 향하는 트래픽을 일치시키려면 대상 포트/프로토콜을 구성합니다.
- 특정 TCP/UDP 포트에서 발생하는 트래픽과 특정 TCP/UDP 포트로 향하는 트래픽을 모두 일치시키려면 두 포트를 모두 구성합니다. 조건에 소스 및 대상 포트를 모두 추가한 경우, 단일 전송 프로토콜(TCP 또는 UDP)을 공유하는 포트만 추가할 수 있습니다. 예를 들어 포트 TCP/80에서 포트 TCP/8080으로 이동하는 트래픽을 대상으로 지정할 수 있습니다.

단계 **9** **OK(**확인**)**를 클릭합니다.

투명 사용자 인증 활성화

액티브 인증을 허용하도록 ID 정책을 구성하는 경우 다음 인증 방법을 통해 사용자 ID를 가져올 수 있습니다.

HTTP 기본

HTTP 기본 인증을 사용하는 경우 사용자에게 디렉터리 사용자 이름과 비밀번호를 사용하여 인증하라는 메시지가 항상 표시됩니다. 비밀번호는 일반 텍스트로 전송됩니다. 그러므로 기본 인증은 안전한 인증 형식으로 간주되지 않습니다.

기본은 기본적으로 사용되는 인증 메커니즘입니다.

HTTP 대응 페이지

사용자에게 로그인 브라우저 페이지가 표시되는 HTTP 기본 인증 유형입니다.

NTLM, HTTP 협상**(Active Directory**용 **Windows** 통합 인증**)**

Windows 통합 인증을 사용할 때는 사용자가 워크스테이션을 사용하기 위해 도메인에 로그인하는 방식을 활용합니다. 브라우저는 서버에 액세스할 때 이 도메인 로그인 사용을 시도합니다(활성 인증 중의 threat defense 종속 포털 포함). 비밀번호는 전송되지 않습니다. 인증이 성공하면 사용자는 투명 방식으로 인증되므로 인증 과정이 수행되었는지 또는 처리되었는지를 알 수 없습니다.

브라우저가 도메인 로그인 크리덴셜을 사용하여 인증 요청을 처리할 수 없으면 사용자에게 사용자 이름과 비밀번호를 입력하라는 메시지가 표시됩니다. 이러한 방식은 기본 인증과 동일한 사용자 환경입니다. 따라서 Windows 통합 인증을 구성하는 경우에는 사용자가 같은 도메인의 네트워크나 서버에 액세스할 때 크리덴셜을 입력해야 할 필요가 감소합니다.

HTTP 협상은 Active Directory 서버와 사용자 에이전트에서 모두 지원하는 가장 강력한 방법을 선택합니다. 협상에서 인증 방법으로 HTTP 기본을 선택하는 경우에는 투명 인증 기능이 제공되지 않습니다. 강도의 순서는 NTLM, 기본입니다. 투명 인증을 수행하려면 협상에서 NTLM을 선택해야 합니다.

투명 인증을 활성화하려면 클라이언트 브라우저가 Windows 통합 인증을 지원하도록 구성해야 합니다. 다음 섹션에서는 Windows 통합 인증을 지원하는 흔히 사용되는 몇 가지 브라우저에 대한 Windows 통합 인증의 일반적인 요건 및 기본 컨피그레이션에 대해 설명합니다. 사용되는 기술은 소프트웨어 릴리스 간에 변경될 수 있으므로, 사용자는 사용 중인 브라우저나 다른 사용자 에이전트의 도움말을 참조해야 합니다.

팁 모든 브라우저에서 Windows 통합 인증을 지원하는 것은 아닙니다. 예를 들어 이 문서를 작성하는 시점의 버전을 기준으로 할 때 Chrome 및 Safari와 같은 브라우저는 해당 인증을 지원하지 않습니다. 이러한 브라우저의 경우 사용자에게 사용자 이름과 비밀번호를 입력하라는 메시지가 표시됩니다. 브라우저 설명서를 참조하여 사용 중인 버전에서 지원되는지 확인하십시오.

투명 인증 요구사항

사용자는 투명 인증을 구현하도록 브라우저 또는 사용자 에이전트를 구성해야 합니다. 이 작업은 사용자가 개별적으로 수행할 수도 있고, 관리자가 사용자를 위해 브라우저 또는 사용자 에이전트를 구성한 다음 소프트웨어 배포 툴을 사용해 클라이언트 워크스테이션으로 해당 컨피그레이션을 푸시할 수도 있습니다. 사용자가 이 작업을 직접 수행하도록 하는 경우 네트워크에서 사용되는 특정 컨피그레이션 파라미터를 제공해야 합니다.

브라우저 또는 사용자 에이전트와 관계없이 다음과 같은 일반 컨피그레이션을 구현해야 합니다.

- 사용자가 네트워크에 연결하는 데 사용하는 threat defense 리디렉션 호스트 이름 또는 인터페이스를 신뢰할 수 있는 사이트 목록에 추가합니다. 리디렉션 호스트 이름을 사용하지 않는 경우 IP 주소를 사용할 수도 있고, 사용 가능한 경우 inside.example.com과 같은 정규화된 호스트 이름(FQDN)을 사용할 수도 있습니다. 와일드카드 또는 부분 주소를 사용하여 일반화된 신뢰할 수 있는 사이트를 생성할 수도 있습니다. 예를 들어, 일반적으로 *.example.com 또는 단순히 example.com을 사용하여 모든 내부 사이트를 포함하면 네트워크의 모든 서버를 신뢰할 수 있습니다(자신의 도메인 이름을 사용). 인터페이스의 특정 주소를 추가하는 경우에는 모든 사용자 액세스 포인트가 네트워크를 가리키도록 신뢰할 수 있는 사이트에 여러 주소를 추가해야 할 수 있습니다.
- Windows 통합 인증은 프록시 서버를 통해 작동하지 않습니다. 따라서 프록시를 사용하지 않거나, 프록시를 통과하지 않도록 제외되는 주소에 threat defense 리디렉션 호스트 이름 또는 인터페이스를 추가해야 합니다. 프록시를 사용해야 하도록 결정하는 경우에는 NTLM을 사용하더라도 사용자에게 인증하라는 메시지가 표시됩니다.

팁 투명 인증은 반드시 구성해야 하는 것은 아니며 엔드 유저의 편의를 위해 구성하는 기능입니다. 투명 인증을 구성하지 않으면 모든 인증 방법에서 사용자에게 로그인 과정이 제공됩니다.

투명 인증을 위해 **Internet Explorer** 구성

NTLM 투명 인증을 위해 Internet Explorer를 구성하려면 다음 단계를 수행합니다.

프로시저

단계 **1** **Tools(**도구**) > Internet Options(**인터넷 옵션**)**을 선택합니다.

단계 **2** **Security(**보안**)** 탭과 **Local Intranet(**로컬 인트라넷**)** 영역을 차례로 선택하고 다음을 수행합니다.

a) **Sites(**사이트**)** 버튼을 클릭하여 신뢰할 수 있는 사이트 목록을 엽니다.

b) 다음 옵션 중 하나 이상이 선택되어 있는지 확인합니다.

- **Automatically detect intranet network(**인트라넷 네트워크를 자동으로 검색**)**. 이 옵션을 선택하면 다른 옵션은 모두 비활성화됩니다.
- **Include all sites that bypass the proxy(**프록시 서버를 건너뛰는 사이트를 모두 포함**)**

c) **Advanced(**고급**)**를 클릭하여 로컬 인트라넷 사이트 대화 상자를 열고 신뢰하려는 URL을 **Add Site(**사이트 추가**)** 상자에 붙여넣은 후에 **Add(**추가**)**를 클릭합니다.

URL이 두 개 이상인 경우 이 프로세스를 반복합니다. 부분 URL을 지정하려면 와일드카드를 사용합니다. 예를 들어 **`http://*.example.com`**과 같이 입력할 수도 있고 **`*.example.com`**만 입력할 수도 있습니다.

대화 상자를 닫고 인터넷 옵션 대화 상자로 돌아옵니다.

d) **Local Intranet(**로컬 인트라넷**)**을 계속 선택한 상태로 **Custom Level(**맞춤형 레벨**)**을 클릭하여 보안 설정 대화 상자를 엽니다. **User Authentication(**사용자 인증**)** > **Logon(**로그온**)** 설정을 찾아서 인트라넷 영역에서만 자동으로 로그온을 선택합니다. **OK(**확인**)**를 클릭합니다.

단계 **3** 인터넷 옵션 대화 상자에서 **Connections(**연결**)** 탭을 클릭한 다음 **LAN Settings(LAN** 설정**)**를 클릭합니다.

Use a proxy server for your LAN(LAN에 프록시 서버 사용**)**이 선택되어 있으면 threat defense 인터페이스가 프록시를 우회하는지 확인해야 합니다. 이렇게 하려면 다음 중 적절한 작업을 수행합니다.

- 로컬 주소에 프록시 서버 건너뛰기를 선택합니다.
- **Advanced(**고급**)**를 클릭하고 다음으로 시작하는 주소에는 프록시 서버 사용 안 함 상자에 주소를 입력합니다. **`*.example.com`**과 같은 와일드카드를 사용할 수 있습니다.

투명 인증을 위해 **Firefox** 구성

NTLM 투명 인증을 위해 Firefox를 구성하려면 다음 단계를 수행합니다.

프로시저

단계 **1** **about:config**를 엽니다. 필터 막대를 사용하여 수정해야 하는 기본 설정을 찾습니다.

단계 **2** NTLM을 지원하려면 다음 기본 설정을 수정합니다(network.automatic으로 필터링).

- **network.automatic-ntlm-auth.trusted-uris** - 기본 설정을 더블 클릭하고 URL을 입력한 후에 **OK(**확인**)**를 클릭합니다. URL이 여러 개이면 쉼표로 구분하여 입력할 수 있습니다. 프로토콜은 원하는 경우 입력하면 됩니다. 예를 들면 다음과 같습니다.

```
http://host.example.com, http://hostname, myhost.example.com
```

부분 URL을 사용할 수도 있습니다. Firefox는 임의 하위 문자열이 아닌 문자열 끝이 일치하는지를 확인합니다. 그러므로 도메인 이름만 지정하여 전체 내부 네트워크를 포함할 수 있습니다. 예를 들면 다음과 같습니다.

```
example.com
```

- **network.automatic-ntlm-auth.allow-proxies** - 값이 기본값인 **true**인지 확인합니다. 값이 현재 false인 경우 더블 클릭하여 값을 변경합니다.

단계 **3** HTTP 프록시 설정을 확인합니다. **Tools(**툴**)** > **Options(**옵션**)**를 선택한 다음 옵션 대화 상자의 **Network(**네트워크**)** 탭을 클릭하여 이러한 옵션을 찾을 수 있습니다. 연결 그룹에서 **Settings(**설정**)** 버튼을 클릭합니다.

- **No Proxy(**프록시 없음**)**이 선택되어 있으면 구성할 항목이 없는 것입니다.
- **Use System Proxy Settings(**시스템 프록시 설정 사용**)**이 선택되어 있으면 about:config에서 **network.proxy.no_proxies_on** 속성을 수정하여 **network.automatic-ntlm-auth.trusted-uris**에 포함한 신뢰할 수 있는 URI를 추가해야 합니다.
- **Manual Proxy Configuration(**수동 프록시 컨피그레이션**)**이 선택되어 있으면 이러한 신뢰할 수 있는 URI가 포함되도록 프록시 없음 목록을 업데이트합니다.
- 다른 옵션 중 하나가 선택되어 있으면 해당 컨피그레이션에 사용되는 속성에서 동일한 신뢰할 수 있는 URI가 제외되는지를 확인합니다.

ID 정책 모니터링

인증이 필요한 ID 정책이 올바르게 작동하는 경우 **Monitoring(**모니터링**)** > **Users(**사용자**)** 대시보드와 사용자 정보를 포함하는 기타 대시보드에 사용자 정보가 표시됩니다.

또한, **Monitoring(**모니터링**)** > **Events(**이벤트**)**에 표시되는 이벤트에 사용자 정보가 포함됩니다.

사용자 정보가 표시되지 않으면 디렉터리 서버가 올바르게 작동하고 있는지 확인하십시오. 연결을 확인하려면 디렉터리 서버 컨피그레이션 대화 상자의 **Test(**테스트**)** 버튼을 사용합니다.

디렉터리 서버가 작동 중이며 사용 가능한 경우 활성 인증이 필요한 ID 규칙의 트래픽 일치 기준이 사용자를 일치시키는 방식으로 작성되어 있는지 확인합니다. 예를 들어 사용자 트래픽이 디바이스에 진입하는 경로로 사용되는 인터페이스가 소스 영역에 포함되어 있는지 확인합니다. 활성 인증 ID 규칙은 HTTP 트래픽만 일치시키므로 사용자는 디바이스를 통해 이 트래픽 유형을 전송해야 합니다.

패시브 인증의 경우 해당 소스를 사용 중이라면 ISE 개체에서 **Test(**테스트**)** 버튼을 사용합니다. 원격 액세스 VPN을 사용 중이라면 서비스가 정상 작동하며 사용자가 VPN 연결을 할 수 있는지 확인합니다. 문제 파악 및 해결에 대한 자세한 정보는 이러한 기능의 트러블슈팅 주제를 참조하십시오.

ID 정책의 예시

사용 사례 장에는 ID 정책을 구현하는 예시가 포함되어 있습니다. 네트워크 트래픽을 파악하는 방법, 49 페이지의 내용을 참조하십시오.

20 장

보안 인텔리전스

보안 인텔리전스 정책을 사용하면 소스/대상 IP 주소 또는 대상 URL을 기준으로 원치 않는 트래픽을 미리 삭제할 수 있습니다. 다음 주제에서는 보안 인텔리전스를 구현하는 방법에 대해 설명합니다.

보안 인텔리전스 정보

보안 인텔리전스 정책을 사용하면 소스/대상 IP 주소 또는 대상 URL을 기준으로 원치 않는 트래픽을 미리 삭제할 수 있습니다. 시스템은 액세스 제어 정책을 사용하여 이 원치 않는 트래픽을 평가 전에 삭제하며, 이에 따라 사용된 시스템 리소스의 양이 줄어듭니다.

다음을 기반으로 트래픽을 차단할 수 있습니다.

- Cisco Talos Intelligence Group(Talos) 피드 - Talos에서는 정기적으로 업데이트되는 보안 인텔리전스 피드에 액세스할 수 있도록 지원합니다. 악성코드, 스팸, 봇넷, 피싱과 같은 보안 위협을 나타내는 사이트는 맞춤형 컨피그레이션을 업데이트하고 구축하는 속도보다 빠르게 나타났다 사라질 수 있습니다. 시스템에서는 피드 업데이트를 정기적으로 다운로드하므로 컨피그레이션을 재구축하지 않아도 새로운 위협 인텔리전스를 사용할 수 있습니다.

참고 Talos 피드는 기본적으로 1시간마다 업데이트됩니다. **Device(**디바이스**)** > **Updates(**업데이트**)** 페이지에서 업데이트 빈도를 변경할 수 있으며, 요구에 따라 피드를 업데이트할 수도 있습니다.

- 네트워크 및 URL 개체 — 차단하고 싶은 특정 IP 주소 또는 URL을 알고 있는 경우, 이에 대한 개체를 생성하여 차단 목록 또는 예외 목록에 추가할 수 있습니다. FQDN 또는 범위 사양을 갖춘 네트워크 개체는 사용할 수 없다는 점에 유의하십시오.

IP 주소(네트워크) 및 URL에 대한 별도의 목록을 생성합니다.

참고 HTTP/HTTPS 요청이 호스트 이름 대신 IP 주소를 사용하는 URL에 대한 요청인 경우, 시스템에서는 네트워크 주소 목록에서 IP 주소 평판을 조회합니다. 네트워크 및 URL 목록에서 IP 주소를 복제할 필요가 없습니다.

차단 목록에 대한 예외 설정

각 차단 목록에 대해 do not block list(차단 안 함 목록)이라고도 하는 관련 예외 목록을 생성할 수 있습니다. 예외 목록을 사용하는 유일한 목적은 차단 목록에 표시되는 IP 주소 또는 URL을 제외하는 것입니다. 즉, 사용해야 하고 안전하다고 알고 있는데 차단 목록에 구성된 피드에 있는 주소 또는 URL을 찾은 경우, 차단 목록에서 범주를 완전히 제거하지 않고도 네트워크/URL을 제외할 수 있습니다.

제외된 트래픽은 나중에 액세스 제어 정책을 기준으로 평가됩니다. 연결의 최종 허용/삭제 여부는 연결과 일치하는 액세스 제어 규칙에 따라 결정됩니다. 또한, 액세스 규칙에 따라 연결에 침입 또는 악성코드 검사를 적용할지도 결정됩니다.

보안 인텔리전스 피드 카테고리

다음 표에서는 Cisco Talos Intelligence Group(Talos) 피드에서 사용할 수 있는 카테고리에 대해 설명합니다. 이러한 범주는 네트워크와 URL 차단에 모두 사용할 수 있습니다.

이러한 범주는 시간이 지남에 따라 변경될 수 있으므로 새로 다운로드한 피드에 범주 변경 사항이 포함될 수 있습니다. 보안 인텔리전스를 구성할 때 범주 이름 옆의 정보 아이콘을 클릭하여 설명을 볼 수 있습니다.

표 ***9: Cisco Talos Intelligence Group(Talos)*** 피드 카테고리

보안인텔리전스카테고리	설명
Attackers	아웃바운드의 악의적 활동으로 알려진 액티브 스캐너 및 호스트
Banking_fraud	전자 뱅킹과 관련된 사기성 활동을 수행하는 사이트
Bogon	bogon 네트워크 및 할당되지 않은 IP 주소
Bots	바이너리 악성코드 드로퍼를 호스팅하는 사이트
CnC	봇넷용 CnC(Command-and-Control) 서버를 호스팅하는 사이트
Cryptomining	크립토마이닝 마이닝을 위해 풀 및 월렛에 대한 원격 액세스를 제공하는 호스트
Dga	CnC 서버에서 RP(Rendezvous Point) 역할을 하는 많은 수의 도메인 이름을 생성하는 데 사용되는 악성코드 알고리즘
Exploitkit	클라이언트에서 소프트웨어 취약성을 식별하도록 설계된 소프트웨어 킷

보안 인텔리전스 카테고리	설명
High_risk	보안 그래프의 OpenDNS 예측 보안 알고리즘과 일치하는 도메인 및 호스트 이름
Ioc	IOC(Indicator of Compromise)에 관련된 것으로 관찰된 호스트
Link_sharing	저작권이 있는 파일을 허가 없이 공유하는 웹사이트
Malicious	반드시 더 세부적인 또 다른 위협 범주에 해당하지는 않지만 악의적인 행동을 보이는 사이트
Malware	악성코드 바이너리 또는 익스플로잇 킷을 호스팅하는 사이트
Newly_seen	최근에 등록되었거나 텔레메트리를 통해 아직 확인되지 않은 도메인
Open_proxy	익명의 웹 브라우징을 허용하는 오픈 프록시
Open_relay	스팸에 사용되는 것으로 알려진 오픈 메일 릴레이
Phishing	피싱 페이지를 호스팅하는 사이트
Response	악성 활동 또는 의심스러운 활동에 적극적으로 참여하고 있는 IP 주소 및 URL
Spam	스팸을 전송하는 것으로 알려진 메일 호스트
Spyware	스파이웨어 및 애드웨어 활동을 포함, 제공 또는 지원하는 것으로 알려진 사이트
Suspicious	알려진 악성코드와 유사한 특성을 지니고 있으며 의심스러워 보이는 파일
tor_exit_node	Tor Anonymizer 네트워크에 대한 종료 노드 서비스를 제공하는 것으로 알려진 호스트

보안 인텔리전스를 위한 라이선스 요건

보안 인텔리전스를 사용하려면 위협 라이선스를 활성화해야 합니다. 선택 가능한 라이선스 활성화 또는 비활성화, 98 페이지의 내용을 참조하십시오.

보안 인텔리전스 구성

보안 인텔리전스 정책을 사용하면 소스/대상 IP 주소 또는 대상 URL을 기준으로 원치 않는 트래픽을 미리 삭제할 수 있습니다. 모든 허용된 연결은 계속해서 액세스 제어 정책을 통해 평가되고 결과적으로 삭제될 수도 있습니다. 보안 인텔리전스를 사용하려면 IPS 라이선스를 활성화해야 합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Security Intelligence(**보안 인텔리전스**)**를 선택합니다.

단계 **2** 정책이 활성화되지 않은 경우 **Enable Security Intelligence(**보안 인텔리전스 활성화**)** 버튼을 클릭합니다.

Security Intelligence(보안 인텔리전스**)** 토글을 클릭하여 **Off(**끄기**)**로 전환하면 언제든지 정책을 비활성화할 수 있습니다. 컨피그레이션은 보존되므로 정책을 다시 활성화할 때 다시 구성할 필요가 없습니다.

단계 **3** 보안 인텔리전스를 구성합니다.

네트워크(IP 주소) 및 URL에 대한 별도의 차단 목록이 있습니다.

a) **Network(**네트워크**)** 또는 **URL** 탭을 클릭하여 구성할 목록을 표시합니다.

b) 차단/드롭 목록에서 +를 클릭하여 연결을 즉시 삭제할 개체 또는 피드를 선택합니다.

개체 선택기는 유형별로 별도의 탭에서 개체 및 피드를 구성합니다. 원하는 개체가 아직 없는 경우 목록 하단에서 **Create New Object(**새 개체 생성**)** 링크를 클릭하여 바로 생성합니다. Cisco Talos Intelligence Group(Talos) 피드에 대한 설명을 보려면 피드 옆에 있는 **i** 버튼을 클릭합니다. 보안 인텔리전스 피드 카테고리, 508 페이지도 참조하십시오.

참고 보안 인텔리전스는 /0 넷마스크를 사용하는 IP 주소 블록을 무시합니다. 여기에는 any-ipv4 및 any-ipv6 네트워크 개체가 포함됩니다. 네트워크 차단용으로 이러한 개체를 선택하지 마십시오.

c) Do Not Block(차단 안 함) 목록에서 +를 클릭하고 차단 목록에 예외 사항을 선택합니다.

이러한 목록을 구성하는 유일한 이유는 차단 목록에 있는 IP 주소 또는 URL에 대한 예외 사항을 만드는 것입니다. 제외된 연결은 나중에 액세스 제어 정책을 기준으로 평가되고 어떤 식으로든 삭제될 수 있습니다.

d) 다른 차단 목록을 구성하려면 이 프로세스를 반복합니다.

단계 **4** (선택 사항). **Edit Logging Settings(**기록 설정 수정**)** 버튼(⚙)을 클릭하여 기록을 컨피그레이션합니다.

로깅을 활성화하면 차단 목록 항목과 일치하는 항목이 로깅됩니다. 로깅이 활성화된 상태에서 제외된 연결이 액세스 제어 규칙과 일치하는 경우에는 로그 메시지를 받더라도 예외 항목과 일치하는 항목은 로깅되지 않습니다.

다음 설정을 구성합니다.

- **Connection Events Logging(**연결 이벤트 로깅**)** - 로깅을 활성화 또는 비활성화하려면 토글을 클릭합니다.
- **Syslog** - 외부 syslog 서버로 이벤트의 복사본을 전송하려는 경우 이 옵션을 선택하고 syslog 서버를 정의하는 서버 개체를 선택합니다. 필요한 개체가 아직 없으면 **Add Syslog Server(Syslog** 서버 추가**)**를 클릭하여 개체를 생성합니다.

디바이스의 이벤트 스토리지는 제한되어 있으므로 외부 syslog 서버로 이벤트를 전송하면 더 장기적으로 저장할 수 있으며 이벤트 분석 성능이 개선됩니다.

보안 인텔리전스 모니터링

보안 인텔리전스 정책에 대해 로깅을 활성화한 경우 시스템에서는 차단 목록의 항목과 일치하는 각 연결에 대해 보안 인텔리전스 이벤트를 생성합니다. 이러한 연결에는 일치하는 연결 이벤트가 있습니다.

삭제된 연결에 대한 통계가 Monitoring(모니터링) 페이지에서 사용할 수 있는 다양한 대시보드에 표시됩니다.

Monitoring(모니터링**)** > **Access and SI Rules(**액세스 및 **SI** 규칙**)** 대시보드에는 트래픽과 가장 많이 일치하는 액세스 규칙 및 보안 인텔리전스 규칙에 상응하는 규칙이 표시됩니다.

또한, **Monitoring(**모니터링**)** > **Events(**이벤트**)**를 선택한 다음 **Security Intelligence(**보안 인텔리전스**)** 보기를 선택하여 **Connection(**연결**)** 탭에서 관련 연결 이벤트뿐만 아니라 보안 인텔리전스 이벤트를 볼 수 있습니다.

- 이벤트의 SI 범주 ID 필드는 네트워크 또는 URL 개체나 피드와 같이 차단 목록에서 일치하는 개체를 나타냅니다.
- 연결 이벤트의 Reason(이유) 필드에서는 이벤트에 표시된 작업이 적용된 이유에 대해 설명합니다. 예를 들어 IP 차단 또는 URL 차단과 같이 이유와 페어링된 차단 작업은 보안 인텔리전스가 연결을 삭제했음을 나타냅니다.

보안 인텔리전스의 예시

사용 사례 장에는 보안 인텔리전스 정책을 구현하는 예시가 포함되어 있습니다. 위협을 차단하는 방법, 57 페이지의 내용을 참조하십시오.

21 장

액세스 제어

다음 주제에서는 액세스 제어 규칙에 대해 설명합니다. 이러한 규칙은 디바이스를 통과할 수 있는 트래픽을 제어하며 침입 검사와 같은 고급 서비스를 트래픽에 적용합니다.

액세스 제어의 모범 사례

액세스 제어 정책은 내부 네트워크를 보호하고 부적절한 웹 사이트와 같은 바람직하지 않은 외부 네트워크 리소스에 사용자가 액세스하는 것을 방지하기 위한 기본 도구입니다. 따라서 이 정책에 각별한 주의를 기울이고 필요한 보호 및 연결성 수준을 얻도록 세밀하게 조정하는 것이 좋습니다.

다음 절차에서는 액세스 제어 정책을 사용하여 수행해야 하는 기본 작업에 대한 개요를 제공합니다. 이는 개요이며 각 작업을 수행하기 위한 전체 단계를 제공하지는 않습니다.

액세스 제어 정책에 접근하려면 **Policies(**정책**)** > **Access Control(**액세스 제어**)**을 선택합니다.

프로시저

단계 **1** 정책의 기본 작업을 구성합니다.

기본 작업은 정책의 특정 규칙과 일치하지 않는 연결을 처리합니다. 기본적으로 이 작업은 **Block(**차단**)**이므로 규칙에서 누락된 사항은 모두 차단됩니다. 따라서 원하는 트래픽을 허용하는 액세스 제어 규칙만 작성하면 됩니다. 이는 액세스 제어 정책을 구성하는 기존의 방법입니다.

기본적으로 트래픽을 허용하는 반대의 작업을 수행할 수 있으며, 원하지 않는 알려진 트래픽을 삭제하는 규칙을 작성할 수 있으므로 허용하려는 모든 항목에 대한 규칙이 필요하지는 않습니다. 이렇게

하면 신규 서비스를 쉽게 사용할 수 있지만, 원하지 않는 새 트래픽이 발견되기 전에 통과할 위험이 있습니다.

단계 **2** **Access Policy Settings(**액세스 정책 설정**)(**⚙**)** 버튼을 클릭하고, **TLS Server Identity Discovery(TLS** 서버 **ID** 검색**)** 옵션을 활성화합니다.

이 옵션을 활성화하지 않으면 TLS 1.3 트래픽이 원하는 규칙과 일치하지 않습니다.

단계 **3** 가능한 한 소수의 액세스 제어 규칙을 생성합니다.

기존 방화벽에서는 IP 주소와 포트의 다양한 조합에 대한 수만 개의 규칙을 생성하게 될 수 있습니다. 차세대 방화벽에서는 고급 검사를 사용하여 이러한 세부 규칙을 피할 수 있습니다. 규칙이 적을수록 시스템에서 트래픽을 더욱 빠르게 평가할 수 있으며 규칙 세트 내에서 문제를 보다 쉽게 발견하고 수정할 수 있습니다.

단계 **4** 액세스 제어 규칙에서 로깅 활성화합니다.

로깅을 활성화한 경우에만 일치하는 트래픽에 대한 통계가 수집됩니다. 로깅을 활성화하지 않으면 모니터링 대시보드가 정확하지 않습니다.

단계 **5** 매우 구체적인 규칙을 정책의 맨 위에 두고, 특정 규칙이 일치하는 연결과 일치하는 보다 일반적인 규칙보다 위에 있는지 확인합니다.

정책은 하향식으로 평가되며, 첫 번째 일치 항목이 적용됩니다. 따라서 특정 서브넷에 대한 모든 트래픽을 차단하는 규칙을 설정한 다음, 서브넷 내에서 단일 IP 주소에 대한 액세스를 허용하는 규칙을 따르면 첫 번째 규칙이 이를 차단하므로 해당 주소에 대한 트래픽은 허용되지 않습니다.

또한 기존 기준(예: 인그레스/이그레스 인터페이스, 소스/대상 IP 주소, 포트 또는 지리위치)만을 기반으로 트래픽을 대상으로 하는 규칙을 심층 검사가 필요한 규칙(예 : 사용자 기준, URL 필터링 또는 애플리케이션 필터링에 적용되는 규칙)보다 먼저 배치해야 합니다. 이러한 규칙은 검사가 필요하지 않으므로 규칙을 조기에 추가하면 일치하는 연결에 대한 액세스 제어 결정을 더욱 빨리 내릴 수 있습니다.

자세한 내용은 액세스 제어 규칙 순서에 대한 모범 사례, 526 페이지를 참조하십시오.

단계 **6** 차단 및 허용 규칙을 트래픽의 대상 하위 세트에 페어링합니다. 규칙입니다.

예를 들어, 대량의 HTTP / HTTPS 트래픽은 허용하되 음란물이나 도박과 같은 바람직하지 않은 사이트에 대한 액세스는 차단해야 할 경우가 많습니다. 그런 경우, 다음 규칙을 생성하고 정책 내에서 순차적으로 유지하여 이를 수행할 수 있습니다.(예 : 규칙 11 및 12)

- 내부 보안 영역(소스) 및 외부 보안 영역(대상), 그리고 모든 IP 주소, 포트 또는 지리위치에 적용되는, 바람직하지 않은 URL 범주를 대상으로 하는 URL 필터링 차단 규칙. 예를 들어 봇넷 차단, 아동 학대 콘텐츠, 암호 해독, DNS 터널링, 온라인 뱅킹 사기, 익스플로잇, 익스트림, 필터 회피, 도박, 해킹, 혐오 표현, 고위험 사이트 및 위치, 불법 활동, 불법 다운로드, 불법 약물, 악성 사이트, 악성 코드 사이트, 모바일 위협, P2P 악성 코드 노드, 피싱, 음란물, 스팸, 스파이웨어 및 애드웨어 등을 차단합니다.
- 내부 보안 영역(소스) 및 외부 보안 영역(대상) 그리고 모든 IP 주소, 포트 또는 지리위치에 적용되는, HTTP 및 HTTPS 애플리케이션에 대한 애플리케이션 필터링 허용 규칙. URL 필터링 규칙이 원치 않는 웹 리소스에 대한 액세스를 차단한 후 이 규칙은 다른 모든 HTTP/HTTPS 액세스를 허용합니다.

단계 **7** IP 주소 또는 포트에 관계없이 트래픽을 대상으로 하는 차세대 고급 방화벽 기능을 사용합니다.

공격자 또는 기타 악의적인 사용자는 기존의 액세스 제어 트래픽 일치 기준을 회피하기 위해 IP 주소 및 포트를 자주 변경할 수 있습니다. 대신 다음과 같은 차세대 기능을 사용하십시오.

- 사용자 기준 — 트래픽을 시작하는 사용자에 대한 정보를 얻으려면 ID 정책을 구성합니다. Active Directory 서버는 사용자를 그룹으로 구성하며, 사용자 그룹 멤버십을 기반으로 트래픽을 허용하거나 차단하는 액세스 제어 규칙을 생성할 수 있습니다. 예를 들어 엔지니어가 개발 서브넷에 액세스하도록 허용하면서 엔지니어 그룹에 속하지 않은 사람은 암묵적으로 차단할 수 있습니다. 개별 사용자 이름 대신 그룹을 사용하면 사람들이 네트워크에 추가될 때 규칙을 계속 업데이트할 필요가 없습니다.
- 애플리케이션 기준 — 애플리케이션 필터링 기준을 사용하여 애플리케이션 유형을 허용하거나 차단합니다. 따라서 사용자가 HTTP 연결에 대한 포트를 변경하면 시스템에서는 포트 80으로 이동하지 않더라도 HTTP임을 인식할 수 있습니다. 자세한 내용은 애플리케이션 필터링에 대한 모범 사례, 518 페이지를 참조하십시오.
- URL 범주 및 평판 기준 — 범주를 기반으로 URL 필터링을 사용하여 사이트 유형에 따라 사이트를 동적으로 허용하거나 차단합니다. 사이트 유형 또는 범주 내에서 사이트의 평판이 좋은 수행자인지 나쁜 수행자인지에 따라 규칙을 세밀하게 조정할 수 있습니다. 범주 및 평판을 사용하면 사이트가 URL을 변경할 때 규칙을 지속적으로 조정할 필요가 없습니다. URL을 기준으로 사이트를 수동으로 차단하려는 경우 이 작업을 수행해야 합니다. 자세한 내용은 효과적인 URL 필터링에 대한 모범 사례, 522 페이지를 참조하십시오.

  URL 범주/평판 필터링 규칙을 DNS 조회 요청의 FQDN에 적용할 수도 있습니다. 시스템은 차단된 범주/평판에 대한 DNS 회신을 방지하여 사용자의 연결 시도를 효과적으로 차단할 수 있습니다. 자세한 내용은 URL 범주 및 평판을 기준으로 DNS 요청 필터링, 525 페이지 섹션을 참조해 주십시오.

단계 **8** 모든 허용 규칙에 침입 검사를 적용합니다.

차세대 방화벽의 강력한 측면 중 하나는 동일한 디바이스를 사용하여 침입 검사 및 액세스 제어를 적용할 수 있다는 점입니다. 각 허용 규칙에 침입 정책을 적용합니다. 그러면 공격이 일반적으로 정상적인 경로를 통해 네트워크에 침입하는 경우 이를 탐지하여 공격 연결을 삭제할 수 있습니다.

기본 작업이 Allow(허용)인 경우 기본 작업과 일치하는 트래픽에 대해 침입 방지를 적용할 수도 있습니다.

단계 **9** 또한 원치 않는 IP 주소 및 URL을 차단하도록 보안 인텔리전스 정책을 구성합니다.

보안 인텔리전스 정책은 액세스 제어 정책보다 먼저 적용되므로 액세스 제어 규칙이 평가받기 전에 원치 않는 연결을 차단할 수 있습니다. 이를 통해 초기 차단을 제공하고 액세스 제어 규칙의 복잡성을 줄일 수 있습니다.

단계 **10** SSL 암호 해독 정책 구현을 고려하십시오.

시스템은 암호화된 트래픽에서 심층 검사를 수행할 수 없습니다. SSL 암호 해독 정책을 구성할 경우 액세스 제어 정책이 암호 해독된 트래픽 버전에 적용됩니다. 따라서 심층 검사에는 침입 정책을 사용하여 공격을 식별할 수 있으며, 애플리케이션 및 URL 필터링을 더욱 효과적으로 적용할 수 있으므로

규칙 일치가 보다 효율적입니다. 액세스 제어 정책에서 허용하는 모든 트래픽은 디바이스에서 전송되기 전에 다시 암호화되므로 최종 사용자의 암호화 보호는 손실되지 않습니다.

액세스 제어 개요

다음 항목에서는 액세스 제어 정책에 대해 설명합니다.

액세스 제어 규칙 및 기본 작업

액세스 제어 정책을 사용하여 네트워크 리소스에 대한 액세스를 허용하거나 차단합니다. 이 정책은 하향식으로 평가되는 순서가 지정된 규칙 집합으로 구성됩니다. 트래픽에 적용되는 규칙은 모든 트래픽 기준이 일치하는 첫 번째 규칙입니다.

다음을 기준으로 하여 액세스를 제어할 수 있습니다.

- 소스 및 대상 IP 주소, 프로토콜, 포트 및 인터페이스와 같은 기존 네트워크 특성(보안 영역 형식)
- 네트워크 개체 형식의 소스 또는 대상의 FQDN(Fully Qualified Domain Name). 트래픽 일치는 DNS 조회에서 이름에 대해 반환되는 IP 주소를 기준으로 합니다.
- Cisco Identity Services Engine(ISE)에서 소스 또는 대상에 할당한 SGT(Security Group Tag).
- 사용 중인 애플리케이션. 특정 애플리케이션을 기반으로 액세스를 제어할 수도 있고, 애플리케이션의 범주, 특정 특성으로 태그가 지정된 애플리케이션, 애플리케이션의 유형(클라이언트, 서버, 웹) 또는 애플리케이션의 위험이나 사업 타당성 등급을 포함하는 규칙을 생성할 수도 있습니다.
- 일반화된 URL 범주를 포함한 웹 요청의 대상 URL. 대상 사이트의 공개 평판에 따라 일치하는 범주를 세분화할 수 있습니다.
- DNS 조회 요청에서 FQDN의 URL 범주 및 평판. 원치 않는 범주 또는 좋지 않은 평판의 DNS 응답을 차단하여 후속 연결 시도를 효과적으로 방지할 수 있습니다.
- 요청을 하는 사용자 또는 사용자가 속한 사용자 그룹

허용한 암호화되지 않은 트래픽에 대해 IPS 검사를 적용하여 위협을 확인하고 공격으로 보이는 트래픽을 차단할 수 있습니다. 또한 파일 정책을 사용하여 금지된 파일이나 악성코드를 확인할 수도 있습니다.

액세스 규칙과 일치하지 않는 모든 트래픽은 액세스 제어 기본 작업에 의해 처리됩니다. 기본적으로 트래픽을 허용하는 경우 트래픽에 침입 검사를 적용할 수 있습니다. 그러나 기본 작업에 의해 처리되는 트래픽에 대해서는 파일 또는 악성코드 검사를 수행할 수 없습니다.

애플리케이션 필터링

액세스 제어 규칙을 사용하여 연결에 사용되는 애플리케이션을 기반으로 트래픽을 필터링할 수 있습니다. 시스템은 수많은 애플리케이션을 인식할 수 있으므로 모든 웹 애플리케이션을 차단하지 않고 웹 애플리케이션 하나만 차단하는 방법을 알아낼 필요가 없습니다.

널리 사용되는 몇 가지 애플리케이션의 경우 애플리케이션의 여러 측면을 필터링할 수 있습니다. 예를 들어 Facebook 전체를 차단하지 않고 Facebook Games만 차단하는 규칙을 생성할 수 있습니다.

일반 애플리케이션 특성을 기반으로 하는 규칙을 생성할 수도 있습니다. 그러면 위험 또는 사업 타당성, 유형, 범주 또는 태그를 선택하여 전체 애플리케이션 그룹을 차단하거나 허용할 수 있습니다. 그러나 애플리케이션 필터에서 범주를 선택할 때는 원치 않는 애플리케이션이 포함되지 않도록 일치하는 애플리케이션 목록을 확인해야 합니다**.** 가능한 그룹화에 대한 자세한 설명은 애플리케이션 기준, 536 페이지를 참조하십시오.

암호화된 트래픽과 암호 해독된 트래픽에 대한 애플리케이션 제어

애플리케이션이 암호화를 사용하는 경우에는 시스템이 애플리케이션을 식별하지 못할 수도 있습니다.

시스템은 SMTPS, POPS, FTPS, TelnetS, IMAPS를 비롯하여 StartTLS로 암호화된 애플리케이션 트래픽을 탐지할 수 있습니다. 또한, TLS ClientHello 메시지 내 서버 이름 지표 또는 서버 인증서의 주체 고유 이름 값에 따라 암호화된 특정 애플리케이션을 식별할 수 있습니다.

애플리케이션 필터 대화 상자를 사용하여 다음 태그를 선택한 후에 애플리케이션 목록을 검사하여 애플리케이션에서 암호 해독이 필요한지 확인합니다.

- **SSL** 프로토콜 - SSL 프로토콜로 태그가 지정된 트래픽은 암호를 해독할 필요가 없습니다. 시스템은 이 트래픽을 인식할 수 있으며 액세스 제어 작업을 적용할 수 있습니다. 나열된 애플리케이션에 대한 액세스 제어 규칙이 필요한 연결과 일치하는지를 확인해야 합니다.
- 암호 해독된 트래픽 - 트래픽을 먼저 암호 해독해야 시스템이 해당 트래픽을 인식할 수 있습니다. 이 트래픽에 대한 SSL 암호 해독 규칙을 구성합니다.

CIP(Common Industrial Protocol) 및 Modbus 애플리케이션(ISA 3000)에서 필터링

Cisco ISA 3000 디바이스에서 CIP(Common Industrial Protocol) 및 Modbus 전처리기를 활성화하고 액세스 제어 규칙에서 CIP 및 Modbus 애플리케이션을 필터링할 수 있습니다. 모든 CIP 애플리케이션 이름은 CIP Write와 같이 "CIP"로 시작합니다. Modbus용 애플리케이션은 하나뿐입니다.

전처리기를 활성화하려면 CLI 세션(SSH 또는 콘솔)에서 전문가 모드로 이동하고 다음 명령을 실행하여 이러한 SCADA(Supervisory Control and Data Acquisition) 애플리케이션 중 하나 또는 둘 다를 활성화해야 합니다.

sudo /usr/local/sf/bin/enable_scada.sh {cip | modbus | both}

예를 들어, 전처리기를 모두 활성화하려면 다음을 수행합니다.

```
> expert
admin@firepower:~$ sudo /usr/local/sf/bin/enable_scada.sh both
```

참고 이 명령은 모든 구축을 완료한 후에 실행해야 합니다. 이러한 전처리기는 구축 시 비활성화됩니다.

애플리케이션 필터링에 대한 모범 사례

애플리케이션 필터링 액세스 제어 규칙을 설계할 때 다음 권장 사항에 유의하십시오.

- 광고물 트래픽과 같이 웹 서버에서 참조된 트래픽을 처리하려면 참조하는 애플리케이션이 아닌 참조되는 애플리케이션의 일치 여부를 확인합니다.
- 애플리케이션 및 URL 기준을 동일한 규칙으로 결합하지 마십시오(특히 암호화된 트래픽의 경우).
- 태그가 지정된 **Decrypted Traffic(**암호 해독된 트래픽**)**에 대해 규칙을 작성하는 경우, 일치하는 트래픽을 암호 해독하는 SSL 암호 해독 규칙이 있는지 확인합니다. 이러한 애플리케이션은 암호 해독된 연결에서만 식별 가능합니다.
- TLS 1.3 인증서가 암호화됩니다. 애플리케이션 또는 URL 필터링을 사용하는 액세스 규칙과 일치하도록 TLS 1.3으로 암호화된 트래픽의 경우 시스템은 TLS 1.3 인증서를 암호 해독해야 합니다. 암호화된 연결이 올바른 액세스 컨트롤 규칙과 일치하는지 확인하려면 액세스 컨트롤 설정에서 **TLS 1.3** 인증서 가시성을 활성화할 것을 권장합니다. 설정은 인증서만 암호 해독합니다. 연결은 암호화된 상태로 유지됩니다.
- 시스템은 Skype 애플리케이션 트래픽의 여러 유형을 탐지할 수 있습니다. Skype 트래픽을 제어하려면 개별 애플리케이션을 선택하는 대신 애플리케이션 필터 목록에서 Skype 태그를 선택합니다. 이렇게 하면 시스템이 동일한 방법으로 모든 Skype 트래픽을 탐지하고 제어할 수 있도록 할 수 있습니다.
- Zoho 메일에 대한 액세스를 제어하려면 Zoho 및 Zoho Mail 애플리케이션을 모두 선택합니다.

URL 필터링

액세스 제어 규칙을 사용하여 HTTP 또는 HTTPS 연결에 사용되는 URL을 기반으로 트래픽을 필터링할 수 있습니다. HTTPS는 암호화되어 있으므로 HTTPS보다 HTTP에 대한 URL 필터링이 더 간단합니다.

다음 기술을 사용하여 URL 필터링을 구현할 수 있습니다.

- 범주 및 평판 기반 URL 필터링 - URL 필터링 라이선스를 사용하면 URL의 일반 분류(범주) 및 위험 레벨(평판)을 기준으로 웹 사이트에 대한 액세스를 제어할 수 있습니다. 이는 원치 않는 사이트를 차단하는 단연 가장 쉽고 효과적인 방법입니다.
- 수동 URL 필터링 - 임의의 라이선스를 사용하여 개별 URL과 URL 그룹을 수동으로 지정해 웹 트래픽을 맞춤형 방식으로 더 상세하게 제어할 수 있습니다. 수동 필터링의 주요 목적은 카테고리 기반 차단 규칙에 대한 예외를 생성하는 것이지만 다른 목적으로도 수동 규칙을 사용할 수 있습니다.

다음 항목에서는 URL 필터링에 대해 자세히 설명합니다.

카테고리 및 평판을 기준으로 URL 필터링

URL 필터링 라이선스가 있으면 요청한 URL의 카테고리 및 평판을 기준으로 웹 사이트에 대한 액세스를 제어할 수 있습니다.

- 범주 - URL의 일반 분류입니다. 예를 들어 ebay.com은 경매 범주에 속하고 monster.com은 구직 범주에 속합니다. 하나의 URL이 여러 카테고리에 속할 수 있습니다.
- 평판 - URL이 사용자가 속한 조직의 보안 정책에 어긋나는 용도로 사용될 가능성입니다. 평판의 범위는 Untrusted(신뢰할 수 없음)(레벨 1)부터 Trusted(신뢰할 수 있음)(레벨 5)까지입니다.

URL 범주 및 평판을 사용하면 URL 필터링을 빠르게 구성할 수 있습니다. 예를 들어, 액세스 제어를 사용해 Illegal Drugs(불법 약물) 카테고리에서 신뢰할 수 없는 URL을 차단할 수 있습니다.

카테고리에 대한 설명은 https://www.talosintelligence.com/categories를 참조하십시오.

범주 및 평판 데이터를 사용하면 정책 생성 및 관리도 간소화됩니다. 보안 위협을 나타내거나 부적절한 콘텐츠를 제공하는 사이트가 나타나고 사라지는 속도는 새 정책을 업데이트하고 구축하는 속도보다 빠를 수 있습니다. Cisco는 새로운 사이트, 변경된 분류 및 변경된 평판이 있는 URL 데이터베이스를 업데이트하므로 규칙이 새로운 정보에 맞게 자동으로 조정됩니다. 따라서 새로운 사이트를 처리하기 위해 규칙을 편집할 필요가 없습니다.

일반 URL 데이터베이스 업데이트를 활성화하는 경우 시스템에서 URL 필터링에 최신 정보를 사용할 수 있습니다. 또한, Cisco CSI(Collective Security Intelligence)와의 통신을 활성화하여 알려지지 않은 카테고리 및 평판을 지닌 URL에 대한 최신 위협 인텔리전스를 얻을 수 있습니다. 자세한 내용은 URL Filtering(URL 필터링) 기본 설정 컨피그레이션, 843 페이지의 내용을 참고하십시오.

참고 이벤트 및 애플리케이션 세부사항에서 URL 범주 및 평판 정보를 확인하려면 URL 조건을 사용하여 규칙을 하나 이상 생성해야 합니다.

URL의 카테고리 및 평판 조회

특정 URL의 카테고리 및 평판을 확인할 수 있습니다. 액세스 제어 규칙 또는 SSL 암호 해독 규칙의 URL 탭으로 이동하거나 **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **URL Filtering Preferences(URL** 필터링 기본 설정**)**로 이동할 수 있습니다. 거기에서 **URL to Check(**확인할 **URL)** 필드에 URL을 입력하고 **Go(**이동**)**를 클릭하면 됩니다.

그러면 조회 결과를 표시하는 웹 사이트로 이동합니다. 이 정보를 이용하여 카테고리 및 평판 기준 URL 필터링 규칙의 동작을 확인할 수 있습니다.

분류에 동의하지 않는 경우, device manager에서 **Submit a URL Category Dispute(URL** 카테고리 이의 제기 제출**)**를 클릭하여 저희에게 의견을 알려주시면 됩니다.

수동 **URL** 필터링

개별 URL 또는 URL 그룹을 수동으로 필터링하여 카테고리 및 평판 기반 URL 필터링을 보완하거나 선택적으로 재정의할 수 있습니다. 이러한 유형의 URL 필터링을 수행하는 데는 특별한 라이선스가 필요하지 않습니다.

예를 들어 액세스 제어를 사용하여 조직에 적합하지 않은 웹 사이트 카테고리를 차단할 수 있습니다. 그러나 해당 카테고리에 액세스 권한을 제공하려는 적합한 웹 사이트가 포함된 경우에는 해당 사이트에 수동 허용 규칙을 생성하여 해당 카테고리에 대한 차단 규칙 앞에 배치하면 됩니다.

수동 URL 필터링을 구성하려면 대상 URL을 사용하는 URL 개체를 생성합니다. 이 URL이 해석되는 방식은 다음 규칙을 기반으로 합니다.

- 경로를 포함하지 않는 경우(즉, URL에 / 문자가 없음), 이 일치는 서버의 호스트 이름만을 기준으로 합니다. 호스트 이름은 :// 구분자 뒷부분 또는 호스트 이름의 의 뒷부분이 같아야 일치하는 것으로 간주됩니다. 예를 들어 ign.com은 ign.com 및 www.ign.com과 일치하지만 verisign.com과는 일치하지 않습니다.
- 하나 이상의 / 문자를 포함하는 경우, 전체 URL 문자열이 서버 이름, 경로 및 쿼리 파라미터를 비롯한 부분 문자열 일치에 사용됩니다. 그러나 서버가 재구성되고 페이지가 새 경로로 이동될 수 있으므로 개별 웹 페이지 또는 사이트 일부를 차단하거나 허용하기 위해 수동 URL 필터링은 사용하지 않는 것이 좋습니다. 부분 문자열 일치는 예기치 않은 일치로 이어질 수도 있으며, 이 경우에는 URL 개체에 포함하는 문자열도 쿼리 파라미터 내부에 있는 의도하지 않은 서버 또는 문자열의 경로와 일치됩니다.
- 시스템에서는 암호화 프로토콜(HTTP 대 HTTPS)을 무시합니다. 다시 말해, 특정 웹 사이트를 차단하는 경우 애플리케이션 조건을 사용하여 특정 프로토콜을 대상으로 하지 않는 한 해당 웹 사이트에 대한 HTTP 및 HTTPS 트래픽이 모두 차단됩니다. URL 개체를 생성할 때에는 개체 생성 시 프로토콜을 지정할 필요가 없습니다. 이를테면 http://example.com 대신 example.com을 사용하십시오.
- URL 개체를 사용하여 액세스 제어 규칙에서 HTTPS 트래픽을 매칭하려는 경우, 트래픽 암호화에 사용되는 공개 키 인증서에서 주체 CN을 사용하여 개체를 생성합니다. 또한 주체 CN에 포함된 하위 도메인은 무시되므로 하위 도메인 정보를 포함하지 마십시오. 이를테면 www.example.com 대신 example.com을 사용하십시오.

  그러나 인증서의 주체 일반 이름은 웹 사이트의 도메인 이름과 아무런 관련도 없을 수 있습니다. 예를 들어, youtube.com 인증서의 주체 일반 이름은 *.google.com입니다(언제든 변경 가능). URL 필터링 규칙이 암호 해독된 트래픽에서 작동하도록 SSL 암호 해독 정책을 사용하여 HTTPS 트래픽을 암호 해독하면 더 일관성 있는 결과를 얻게 됩니다.

참고 인증서 정보를 더 이상 사용할 수 없어 브라우저에서 TLS 세션을 다시 시작하는 경우에는 URL 개체가 HTTPS 트래픽과 일치되지 않습니다. 따라서 URL 개체를 주의하여 구성하더라도 HTTPS 연결에 대해 일관성 없는 결과를 얻을 수 있습니다.

HTTPS 트래픽 필터링

HTTPS 트래픽은 암호화되어 있기 때문에 HTTPS 트래픽에서 직접 URL 필터링을 수행하는 것은 HTTP 트래픽에서 그렇게 하는 것만큼 간단하지 않습니다. 따라서 SSL 암호 해독 정책을 사용하여 필터링하려는 모든 HTTPS 트래픽을 암호 해독하는 방법을 고려해야 합니다. 그래야 URL 필터링 액세스 제어 정책이 암호 해독된 트래픽에서 작동하며 일반 HTTP 트래픽을 대상으로 할 때 얻는 결과와 동일한 결과를 얻을 수 있습니다.

그러나 일부 HTTPS 트래픽을 암호 해독되지 않은 상태로 액세스 제어 정책에 전달하는 것을 허용하려면 규칙이 HTTP 트래픽과 일치하는 것과는 다른 방법으로 HTTPS 트래픽과 일치한다는 점을 이해해야 합니다. 시스템은 암호화된 트래픽을 필터링하기 위해 SSL 핸드셰이크 중에 전달된 정보(트래픽을 암호화하는 데 사용된 공개 키 인증서의 주체 공용 이름)를 기준으로 요청된 URL을 확인합니다. URL의 웹 사이트 호스트 이름과 주체 일반 이름 간에는 관련성이 적거나 없을 수 있습니다.

DNS 요청 필터링을 활성화하면 범주/평판 규칙에 대한 HTTPS 일치를 개선할 수 있습니다. 시스템은 사용자가 HTTPS 연결 시도를 시작하기 전에 DNS 확인 단계 도중 범주 및 평판을 확인하고 원치 않는 조합에 대한 DNS 응답을 차단할 수 있습니다. 허용되는 DNS 응답의 경우 시스템은 후속 HTTPS 연결에 사용할 수 있는 범주/평판 정보를 보유하게 됩니다. DNS 요청 필터링, 524 페이지의 내용을 참조하십시오.

HTTP 필터링과 달리, HTTPS 필터링은 주체 공용 이름 내의 서브도메인을 무시합니다. 수동으로 HTTPS URL을 필터링할 경우 하위 도메인 정보를 포함하지 마십시오. 이를테면 www.example.com 대신 example.com을 사용하십시오. 또한, 사이트에서 사용하는 인증서의 콘텐츠를 검토하여 가지고 있는 도메인이 주체 일반 이름에서 사용된 적절한 도메인인지 그리고 이 이름이 다른 규칙과 충돌하지 않는지(예: 차단하려는 사이트의 이름이 허용하려는 이름과 중복될 수 있음) 확인합니다. 예를 들어, youtube.com 인증서의 주체 일반 이름은 *.google.com입니다(언제든 변경 가능).

참고 인증서 정보를 더 이상 사용할 수 없어 브라우저에서 TLS 세션을 다시 시작하는 경우에는 URL 개체가 HTTPS 트래픽과 일치되지 않습니다. 따라서 URL 개체를 주의하여 구성하더라도 HTTPS 연결에 대해 일관성 없는 결과를 얻을 수 있습니다.

암호화 프로토콜을 통해 트래픽 제어

시스템에서는 URL 필터링을 수행할 때 암호화 프로토콜(HTTP 대 HTTPS)을 무시합니다. 이는 수동 및 평판 기반 URL 조건 모두에 해당됩니다. 즉, URL 필터링에서는 다음 웹 사이트에 대한 트래픽을 똑같이 처리합니다.

- http://example.com
- https://example.com

HTTP 또는 HTTPS 트래픽 중 하나에만 일치하는 규칙을 구성하려면 대상 조건에서 TCP 포트를 지정하거나 규칙에 애플리케이션 조건을 추가합니다. 예를 들어 각각 TCP 포트/애플리케이션 및 URL 조건을 갖춘 2개의 액세스 제어 규칙을 작성하여 어떤 사이트에 대한 HTTPS 액세스를 허용하되 HTTP 액세스는 허용하지 않을 수 있습니다.

첫 번째 규칙은 웹 사이트에 대한 HTTPS 트래픽을 허용합니다.

작업: Allow(허용)
TCP 포트 또는 애플리케이션: HTTPS(TCP 포트 443)
URL: example.com

두 번째 규칙은 동일한 웹 사이트에 대한 HTTP 액세스를 차단합니다.

작업: Block(차단)
TCP 포트 또는 애플리케이션: HTTP(TCP 포트 80)
URL: example.com

URL 및 애플리케이션 필터링 비교

URL 및 애플리케이션 필터링에는 유사한 점이 있습니다. 하지만 다음과 같이 매우 뚜렷한 목적을 위해 필터링 기능을 사용해야 합니다.

- URL 필터링은 전체 웹 서버에 대한 액세스를 차단하거나 허용하는 데 사용되는 가장 좋은 방법입니다. 예를 들어, 네트워크에서 모든 유형의 도박을 허용하지 않으려는 경우 URL 필터링 규칙을 생성하여 도박 카테고리를 차단할 수 있습니다. 이 규칙을 사용하면 사용자는 카테고리 내 모든 웹 서버의 모든 페이지에 액세스할 수 없습니다.
- 애플리케이션 필터링은 호스팅 사이트와 관계없이 특정 애플리케이션을 차단하거나 기타 허용 가능한 웹 사이트의 특정 기능을 차단하는 데 유용합니다. 예를 들어, 모든 Facebook을 차단하지 않고 Facebook의 게임 애플리케이션만 차단할 수 있습니다.

애플리케이션과 URL 기준을 결합하면 예기치 않은 결과가 발생할 수 있기 때문에(특히 암호화된 트래픽의 경우) 이는 URL 및 애플리케이션 기준에 대한 별도의 규칙을 생성하기에 좋은 정책입니다. 애플리케이션과 URL 기준을 단일 규칙에서 결합해야 하는 경우, 애플리케이션 및 URL 결합 규칙이 더 일반적인 애플리케이션 전용 또는 URL 전용 규칙에 대한 예외 역할을 하지 않는 한, 이러한 규칙은 간단한 애플리케이션 전용 또는 URL 전용 규칙 이후에 배치해야 합니다. URL 필터링 차단 규칙은 애플리케이션 필터링보다 더 광범위하기 때문에 애플리케이션 전용 규칙보다 상위에 배치해야 합니다.

애플리케이션과 URL 기준을 결합하는 경우, 원치 않는 사이트 및 애플리케이션에 대한 액세스를 허용하지 않으려면 네트워크를 더 신중하게 모니터링해야 할 수 있습니다.

효과적인 URL 필터링에 대한 모범 사례

URL 필터링 액세스 제어 규칙을 설계할 때 다음 권장 사항에 유의하십시오.

- 가능한 경우 항상 카테고리 및 평판 차단 기능을 사용합니다. 이렇게 하면 새 사이트가 카테고리에 추가될 때 자동으로 차단되며, 사이트의 평판이 높아지거나 낮아지는 경우 평판을 기반으로 하는 차단 기능이 조정됩니다.
- URL 카테고리 일치를 사용할 때는 사이트의 로그인 페이지가 사이트 자체의 카테고리와 다른 카테고리에 포함되는 경우가 있음을 고려해야 합니다. 예를 들어 Gmail은 Web-based Email(웹 기반 이메일) 카테고리에 포함되지만 로그인 페이지는 Search Engines and Portals(검색 엔진 및 포털) 카테고리에 포함됩니다. 카테고리에 대해 여러 작업이 포함된 각기 다른 규칙이 있는 경우 의도하지 않은 결과가 발생할 수 있습니다.

- URL 개체를 사용하여 전체 웹 사이트를 대상으로 하고 카테고리 차단 규칙에 대한 예외를 설정합니다. 즉, 예외를 설정하지 않는다면 카테고리 규칙에서 차단될 특정 사이트를 허용합니다.
- URL 개체를 사용하여 웹 서버를 수동으로 차단하려는 경우 보안 인텔리전스 정책에서 차단하는 것이 훨씬 더 효과적입니다. 보안 인텔리전스 정책은 액세스 제어 규칙이 평가되기 전에 연결을 삭제하므로 더욱 빠르고 효율적인 차단을 가능하게 합니다.
- HTTPS 연결을 가장 효과적으로 필터링하려면 SSL 암호 해독 규칙을 구현하여 액세스 제어 규칙을 작성 중인 대상 트래픽의 암호를 해독합니다. 암호 해독된 HTTPS 연결은 액세스 제어 정책에서 HTTP 연결로 필터링되므로 HTTPS 필터링에 대한 모든 제한을 피할 수 있습니다.
- TLS 1.3 인증서가 암호화됩니다. 애플리케이션 또는 URL 필터링을 사용하는 액세스 규칙과 일치하도록 TLS 1.3으로 암호화된 트래픽의 경우 시스템은 TLS 1.3 인증서를 암호 해독해야 합니다. 암호화된 연결이 올바른 액세스 컨트롤 규칙과 일치하는지 확인하려면 액세스 컨트롤 설정에서 **TLS 1.3** 인증서 가시성을 활성화할 것을 권장합니다. 설정은 인증서만 암호 해독합니다. 연결은 암호화된 상태로 유지됩니다.
- URL 필터링은 전체 웹 서버를 차단하는 반면, 애플리케이션 필터링은 웹 서버와 관계없이 특정 애플리케이션 사용을 대상으로 하므로 애플리케이션 필터링 규칙보다 URL 차단 규칙을 먼저 배치합니다.
- 카테고리를 알 수 없는 고위험 사이트를 차단하려면 Uncategorized(카테고리가 지정되지 않음) 카테고리를 선택하고 평판 슬라이더를 Questionable(의심스러움) 또는 Untrusted(신뢰할 수 없음)으로 조정합니다.
- DNS 요청 필터링도 활성화하여 전반적인 URL 필터링 효율성을 높일 수 있습니다. DNS 요청 필터링을 사용하는 경우 시스템에서 DNS 조회 시간에 FQDN의 URL 범주 및 평판을 결정하므로, 후속 HTTP/HTTPS 요청이 동일한 대상으로 향하는 경우 이 정보를 사용할 수 있습니다. 추가로 범주/평판을 차단하는 경우 웹 세션 설정 단계가 아닌 DNS 요청 단계에서 연결 시도가 중단됩니다. DNS 요청 필터링, 524 페이지의 내용을 참조하십시오.

웹 사이트를 차단할 때 사용자에게 표시되는 내용

URL 필터링 규칙을 사용하여 웹 사이트를 차단할 때 사용자에게 표시되는 내용은 사이트가 암호화되어 있는지에 따라 달라집니다.

- HTTP 연결 - 사용자에게는 시간이 초과되거나 재설정된 연결의 경우에 표시되는 일반적인 브라우저 페이지가 아닌 시스템 기본 차단 응답 페이지가 표시됩니다. 이 페이지에서는 연결이 의도적으로 차단되었다는 내용이 명확하게 표시됩니다.
- HTTPS(암호화된) 연결 - 사용자에게 시스템 기본 차단 응답 페이지가 표시되지 않습니다. 대신 보안 연결 실패를 나타내는 브라우저의 기본 페이지가 표시됩니다. 오류 메시지는 사이트가 정책으로 인해 차단되었음을 나타내지 않습니다. 대신 일반적인 암호화 알고리즘이 없다는 오류가 표시될 수 있습니다. 이 메시지만으로는 연결이 의도적으로 차단되었는지를 명확하게 파악할 수 없습니다.

또한, 명시적 URL 필터링 규칙이 아닌 다른 액세스 제어 규칙이나 기본 작업에 의해 웹 사이트가 차단될 수도 있습니다. 예를 들어 전체 네트워크 또는 지리위치를 차단하는 경우 해당 네트워크나 지리

위치의 웹 사이트도 모두 차단됩니다. 이러한 규칙으로 인해 차단된 사용자에게는 아래 제한에서 설명하는 응답 페이지가 표시될 수도 있고 표시되지 않을 수도 있습니다.

URL 필터링을 구현할 때는 사이트가 의도적으로 차단될 때 표시될 수 있는 내용 및 차단 대상 사이트 유형을 엔드 유저에게 설명하는 것이 좋습니다. 그렇지 않으면 엔드 유저가 차단된 연결의 트러블슈팅을 수행하는 데 오랜 시간을 쓸 수 있습니다.

HTTP 대응 페이지의 제한

시스템에서 웹 트래픽을 차단할 때 HTTP 대응 페이지가 항상 표시되는 것은 아닙니다.

- 승격된 액세스 제어 규칙(단순한 네트워크 조건만 사용하여 초기에 배치된 차단 규칙)으로 인해 웹 트래픽이 차단될 때는 시스템에서 응답 페이지를 표시하지 않습니다.
- 시스템에서 요청된 URL을 식별하기 전에 웹 트래픽이 차단되면 시스템은 응답 페이지를 표시하지 않습니다.
- 액세스 제어 규칙에 의해 차단되는 암호화된 연결에 대해서는 시스템이 응답 페이지를 표시하지 않습니다.

DNS 요청 필터링

HTTP/HTTPS가 아닌 연결 시도에도 DNS 조회 요청에 URL 범주 및 평판 데이터베이스를 적용할 수 있습니다.

예를 들어 사용자가 www.example.com에 대한 FTP 연결을 시도하는 경우, 해당 FQDN(Fully Qualified Domain Name)에 대한 DNS 조회 요청이 표시될 때 www.example.com의 범주 및 평판을 조회하도록 시스템을 설정할 수 있습니다. 반환된 범주/평판에 대한 DNS/URL 필터링 규칙이 차단 규칙인 경우 시스템은 DNS 회신을 차단합니다. 따라서 사용자는 FQDN에 대한 IP 주소를 가져오지 않으며, 연결 시도는 실패합니다.

DNS 조회 요청 필터링을 활성화하면 URL 필터링 규칙을 HTTP/HTTPS 이외의 프로토콜로 확장하고, FTP, TFTP, SCP, ICMP 및 기타 프로토콜에서 웹 액세스를 위해 차단하는 사이트에 대한 연결을 설정하는 것을 방지할 수 있습니다. 이는 사용자가 FQDN 이름을 사용하는 한 작동하므로 DNS 조회가 필요합니다. 사용자가 IP 주소를 사용하는 경우 DNS 요청이 없으므로 DNS 요청 차단이 불가능합니다.

HTTP/HTTPS 트래픽의 경우 DNS 요청 시간에 범주/평판 조회를 수행하면 웹 세션을 설정하기 전에 연결을 방지할 수 있으므로 시스템 성능이 향상될 수 있습니다. 이는 암호화된 HTTPS에 특히 유용할 수 있습니다. DNS 요청 단계에서 거부함으로써 시스템에서 HTTPS 연결을 확인할 수 없으므로 암호 해독 규칙을 평가할 필요가 없고, 암호화된 세션을 올바른 액세스 제어 규칙과 일치시키는 더욱 어려운 작업을 수행할 필요도 없습니다.

DNS 요청 필터링 지침

DNS 요청 필터링을 설정할 때는 다음 사항에 유의하십시오.

- DNS 요청 필터링은 DNS 세션에서만 작동합니다. DNS 회신을 허용하는 경우(즉, URL 필터링 규칙 작업이 Allow(허용)임), 사용자가 반환한 IP 주소로 설정하는 후속 연결은 액세스 제어 규칙

과 별도로 일치됩니다. 연결이 다른 규칙과 일치될 수 있으므로 다른 이유로 차단 또는 허용될 수 있습니다. 예를 들어, FTP에서 DNS 조회를 통해 IP 주소를 가져오도록 허용하는 경우 FTP 연결을 금지하는 또 다른 액세스 제어 규칙이 있을 수 있으며, 그 결과 연결이 차단됩니다.

- URL/DNS 요청 필터링 규칙 이전의 액세스 제어 규칙과 일치하는 DNS 조회 요청은 일치하는 규칙에 따라 허용되거나 차단됩니다. 이러한 연결에 대해서는 범주/평판 조회가 이루어지지 않습니다.
- 이 기능을 사용하려면 범주/평판을 기반으로 URL 필터링을 구현해야 합니다. 이 유형의 URL 필터링에 대한 URL 필터링 라이선스가 있어야 합니다. 범주/평판을 기반으로 하는 URL 필터링 규칙이 없는 경우, DNS 요청 필터링이 적합하지 않으므로 이를 활성화해서는 안 됩니다.
- DNS 필터링에 의해 생성되는 연결 이벤트에는 DNS Query(DNS 쿼리), URL Category(URL 범주) 및 URL Reputation(URL 평판)과 같은 특수 관심 필드가 포함됩니다. DNS Query(DNS 쿼리) 필드에는 조회 요청에 대한 FQDN(Fully Qualified Domain Name)이 표시됩니다. DNS 필터링 이벤트의 경우 URL 필드가 비어 있습니다.
- DNS 요청 필터링은 URL 범주 및 평판 데이터베이스만 사용합니다. 일치하는 액세스 제어 규칙에서 정의된 URL 개체 또는 기타 수동 URL 필터링은 무시됩니다. 수동 DNS 이름 차단을 구현하려면 보안 인텔리전스 DNS 정책을 사용합니다.

URL 범주 및 평판을 기준으로 DNS 요청 필터링

다음 절차에서는 DNS 조회 요청 필터링을 구현하는 방법을 설명합니다.

시작하기 전에

아직 활성화되지 않은 경우 URL 라이선스를 활성화해야 합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)**을 선택합니다.

단계 **2** 필요한 경우 **Access Policy Settings(**액세스 정책 설정**)**( ) 버튼을 클릭하고, **Reputation Enforcement on DNS Traffic(DNS** 트래픽에 대한 평판 시행**)** 옵션을 선택한 다음 **OK(**확인**)**를 클릭합니다.

이 옵션은 액세스 제어 정책에 대한 DNS 요청 필터링을 활성화합니다. 이 옵션은 기본적으로 활성화되어 있습니다.

단계 **3** DNS 요청에도 적용되는 URL 범주 및 평판을 기반으로 필터링을 구현하려면 기존 URL 필터링 규칙을 평가하거나 새 규칙을 생성합니다.

URL 필터링은 일반적으로 HTTP/HTTPS 트래픽에만 적용되므로 애플리케이션 또는 포트를 기준으로 이러한 규칙을 제한할 이유가 없습니다. 하지만 이러한 제한이 있는 경우 규칙을 DNS 요청에도 적용할 수 있는지 확인합니다.

- **Source/Destination(**소스/대상**)** 탭에서 **Destination Ports(**대상 포트**)** 필드가 **Any(**모두**)**인 경우 변경할 필요가 없습니다. 포트를 지정한 경우 **DNS over UDP** 및 **DNS over TCP**를 목록에 추가합니다.

- **Applications(**애플리케이션**)** 탭에서 애플리케이션 목록이 **Any(**모두**)**인 경우 변경할 필요가 없습니다. 애플리케이션 또는 애플리케이션 필터를 지정한 경우 **DNS** 애플리케이션을 목록 또는 필터에 추가합니다. 다른 DNS 관련 옵션은 이 목적과 관련이 없습니다.

액세스 제어 규칙 생성에 대한 자세한 내용은 액세스 제어 규칙 구성, 532 페이지를 참조하십시오.

단계 **4** 이전 규칙을 평가하여 DNS 요청이 해당 규칙과 일치하지 않는지 확인합니다.

DNS 요청이 범주 및 평판 사양이 있는 URL 필터링 규칙과 일치하는 경우에만 범주 및 평판이 결정됩니다. URL 필터링 규칙이 DNS 요청 필터링을 우회하는 것보다 이전에 액세스 제어 정책의 규칙과 일치하는 DNS 요청. 이러한 DNS 요청은 차단 또는 허용되는 일치 규칙에 따라 처리됩니다.

침입, 파일 및 악성코드 검사

침입 정책 및 파일 정책은 트래픽이 원하는 대상에 도달하도록 허용하기 전에 최종 방어선으로 함께 사용됩니다.

- 침입 정책은 시스템의 침입 방지 기능을 제어합니다.
- 파일 정책은 시스템의 파일 제어 및 악성코드 방어 기능을 제어합니다.

기타 모든 트래픽 처리는 네트워크 트래픽에서 침입, 금지된 파일 및 악성코드를 검사하기 전에 수행됩니다. 침입 또는 파일 정책을 액세스 제어 규칙과 연결하여 시스템이 액세스 제어 규칙의 조건과 일치하는 트래픽을 통과시키기 전에 침입 정책이나 파일 정책 또는 두 정책을 모두 사용하여 트래픽을 먼저 검사하도록 명령할 수 있습니다.

트래픽을 허용하는 규칙에 대해서만 침입 및 파일 정책을 구성할 수 있습니다. 트래픽을 **trust(**신뢰**)** 또는 **block(**차단**)**하도록 설정된 규칙에 대해서는 검사가 수행되지 않습니다. 또한, 액세스 제어 정책의 기본 작업이 허용이면 침입 정책은 구성할 수 있지만 파일 정책은 구성할 수 없습니다.

액세스 제어 규칙으로 처리되는 단일한 연결의 경우, 침입 검사 전에 파일 검사가 이루어집니다. 즉, 시스템에서는 파일 정책 또는 침입에 의해 차단된 파일은 검사하지 않습니다. 파일 검사 내에서 유형을 기준으로 한 간단한 차단은 악성코드 검사 및 차단보다 우선합니다. 세션에서 파일이 탐지되고 차단될 때까지, 세션의 패킷은 침입 검사 대상이 될 수 있습니다.

참고 기본적으로, 시스템에서는 암호화된 페이로드의 침입 및 파일 검사를 비활성화합니다. 이는 암호화 연결이 침입 및 파일 검사가 구성된 액세스 제어 규칙과 일치하는 경우 오탐을 줄이고 성능을 높이는 데 도움이 됩니다. 검사는 암호화되지 않은 트래픽에 대해서만 작동합니다.

액세스 제어 규칙 순서에 대한 모범 사례

규칙은 처음 일치하는 항목을 기준으로 적용되므로, 매우 구체적인 트래픽 일치 기준이 포함된 규칙이 보다 일반적인 기준이 포함된 정책(규칙이 일치하지 않는 경우 일치하는 트래픽에 적용됨) 위에 표시되도록 삽입해야 합니다. 다음 권장 사항을 참고하십시오.

- 구체적인 규칙은 일반적인 규칙보다 먼저 배치해야 합니다(특히, 구체적인 규칙이 일반적인 규칙에 대한 예외인 경우).
- IP 주소, 보안 영역, 포트 번호 등 레이어-3/4 기준만을 기반으로 하여 트래픽을 삭제하는 규칙은 가능한 한 먼저 배치해야 합니다. 레이어-3/4 기준은 검사하지 않고 신속하게 평가될 수 있기 때문에 이러한 규칙은 검사(예: 애플리케이션 또는 URL 기준을 사용하는 검사)가 필요한 규칙보다 먼저 배치하는 것이 좋습니다. 물론 이러한 규칙에 대한 예외는 해당 규칙보다 상위에 배치해야 합니다.
- 구체적인 삭제 규칙은 가능한 경우 항상 정책 상위에 둡니다. 이렇게 하면 부적절한 트래픽에 대해 가능한 한 빠른 결정을 내릴 수 있습니다.
- 애플리케이션 및 URL 기준을 모두 포함하는 규칙은 애플리케이션 및 URL 기준이 결합된 규칙이 더 일반적인 애플리케이션 전용 또는 URL 전용 규칙에 대한 예외 역할을 하지 않는 한, 간단한 애플리케이션 전용 또는 URL 전용 규칙 이후에 배치해야 합니다. 애플리케이션과 URL 기준을 결합하면 예기치 않은 결과가 발생할 수 있기 때문에(특히 암호화된 트래픽의 경우) 가능한 경우 항상 URL 및 애플리케이션 필터링에 대해 별도의 규칙을 생성하는 것이 좋습니다.

NAT 및 액세스 규칙

NAT를 구성한 경우라도, 액세스 규칙은 액세스 규칙 일치를 확인할 때 항상 실제 IP 주소를 사용합니다. 예를 들어 내부 서버 10.1.1.5가 외부에서 공개적으로 라우팅 가능한 IP 주소 209.165.201.5를 갖도록 NAT를 구성할 경우, 외부 트래픽이 내부 서버에 액세스하는 것을 허용하는 액세스 규칙은 서버의 매핑된 주소(209.165.201.5)가 아니라 실제 IP 주소(10.1.1.5)를 참조해야 합니다.

기타 보안 정책이 액세스 제어에 영향을 미치는 방식

기타 보안 정책은 액세스 제어 규칙이 작동하고 연결과 일치하는 방식에 영향을 미칠 수 있습니다. 액세스 규칙을 구성할 때 다음 사항에 유의하십시오.

- **SSL Decryption(SSL** 암호 해독**)** 정책 — SSL 암호 해독 규칙은 액세스 제어보다 먼저 평가됩니다. 따라서 암호화된 연결이 일부 유형의 암호 해독을 적용하는 SSL 암호 해독 규칙과 일치하는 경우, 이 연결은 액세스 제어 정책에서 평가되는 일반 텍스트(암호 해독됨) 연결입니다. 액세스 규칙은 연결의 암호화된 버전을 확인하지 않습니다. 또한, 트래픽을 삭제하는 SSL 암호 해독 규칙과 일치하는 모든 연결은 액세스 제어 정책에서 확인되지 않습니다. 마지막으로, 암호 해독 안 함 규칙과 일치하는 모든 암호화된 연결은 암호화된 상태에서 평가됩니다.
- **Identity(ID)** 정책 — 연결은 소스 IP 주소에 대한 사용자 매핑이 있는 경우에만 사용자(및 사용자 그룹)와 일치됩니다. 사용자 또는 그룹 멤버십의 핵심인 액세스 규칙은 ID 정책에 의해 사용자 ID가 수집된 연결하고만 일치할 수 있습니다.
- **Security Intelligence(**보안 인텔리전스**)** 정책 — 삭제된 연결은 액세스 제어 정책에서 확인되지 않습니다. 차단 안 함 목록과 일치하는 연결은 이후에 액세스 제어 규칙과 일치되며, 궁극적으로 연결을 처리하는 방법(허용 또는 삭제)을 결정하는 액세스 제어 규칙입니다.
- **VPN**(사이트 대 사이트 또는 원격 액세스) — VPN 트래픽은 항상 액세스 제어 정책을 대상으로 평가되며 연결은 일치 규칙에 기초하여 허용 또는 삭제됩니다. 그러나 VPN 터널 자체는 액세스

제어 정책이 평가되기 전에 암호 해독됩니다. 액세스 제어 정책은 터널 자체가 아니라 VPN 터널 내부에 임베드된 연결을 평가합니다.

액세스 제어를 위한 라이선스 요건

액세스 제어 정책을 사용하는 데에는 특수 라이선스가 필요하지 않습니다.

그러나 액세스 제어 정책에 포함된 특수 기능에 대해서는 다음과 같은 라이선스가 필요합니다. 라이선스 구성에 대한 자세한 내용은 선택 가능한 라이선스 활성화 또는 비활성화, 98 페이지를 참조하십시오.

- **URL** 라이선스 - URL 카테고리 및 평판을 일치 기준으로 사용하는 규칙을 생성하는 데 필요합니다.
- 위협 라이선스 - 액세스 규칙 또는 기본 작업에서 침입 정책을 구성하는 데 필요합니다. 파일 정책을 사용하려면 이 라이선스도 필요합니다(악성코드 라이선스도 필요함).
- 악성코드 라이선스 - 액세스 규칙에서 파일 정책을 구성하는 데 필요합니다. 위협은 파일 정책에도 필요합니다.

액세스 제어 정책에 대한 지침 및 제한 사항

다음은 액세스 제어에 대한 몇 가지 추가적인 제한 사항입니다. 규칙에서 예상된 결과를 얻고 있는지 평가할 때 이 제한 사항을 고려하십시오.

- URL 데이터베이스 업데이트에 추가되거나(신규, 수신), 사용되지 않거나(발신) 삭제된 카테고리가 포함된 경우, 영향을 받는 액세스 제어 규칙을 변경할 수 있는 유예 기간이 있습니다. 영향을 받는 규칙에는 규칙에 영향을 미치는 문제에 대한 설명과 카테고리 변경에 대한 자세한 내용을 참조할 수 있는 Cisco Talos Intelligence Group(Talos) 웹 사이트의 링크가 있는 정보 메시지가 표시되어 있습니다. 규칙을 업데이트하여 최신 URL 데이터베이스에서 사용할 수 있는 적절한 범주를 사용하도록 해야 합니다.

  유예 기간을 수용하려면 새로 추가된 수신 카테고리를 적절한 규칙에 추가하되 사용하지 않는 발신 카테고리를 제거하지 마십시오. 이때 규칙에는 신규 및 기존 카테고리가 포함되어야 합니다. 새 카테고리는 기존 카테고리에 삭제 표시가 된 경우에 적용됩니다. 기존 범주가 최종 삭제된 경우, 규칙을 수정하여 삭제된 카테고리를 제거하고 컨피그레이션을 재구축해야 합니다. 삭제된 카테고리를 사용하는 규칙을 모두 수정할 때까지는 컨피그레이션을 구축하지 못하도록 차단됩니다. 주의해야 하는 규칙을 기준으로 필터링하려면 테이블 위쪽에 있는 문제 규칙 참조 링크를 클릭하십시오.

- Device Manager는 디렉터리 서버에서 최대 50,000명의 사용자에 대한 정보를 다운로드할 수 있습니다. 디렉터리 서버에 50,000개가 넘는 사용자 계정이 포함되어 있으면 액세스 규칙에서 사용자를 선택할 때 또는 사용자 기반 대시보드 정보를 확인할 때 가능한 이름이 모두 표시되지 않으며, 다운로드한 이름에 대해서만 규칙을 작성할 수 있습니다.

이 50,000명 제한은 그룹과 연결된 이름에도 적용됩니다. 그룹의 구성원이 50,000명보다 많으면 다운로드한 50,000개의 이름에 대해서만 그룹 구성원 자격과의 일치 여부를 확인할 수 있습니다.

- VDB(Vulnerability Database) 업데이트에서 사용되지 않는 애플리케이션을 제거하는 경우, 삭제된 애플리케이션을 사용하는 액세스 제어 규칙 또는 애플리케이션 필터를 변경해야 합니다. 이러한 규칙을 수정할 때까지는 변경 사항을 구축할 수 없습니다. 또한 문제를 해결하기 전에는 시스템 소프트웨어 업데이트를 설치할 수 없습니다. Application Filters(애플리케이션 필터) 개체 페이지 또는 규칙의 Application(애플리케이션) 탭에서는 이러한 애플리케이션 이름 뒤에 "(사용되지 않음)"이라고 표시됩니다.

- FQDN(Fully Qualified Domain Name) 네트워크 개체를 소스 또는 대상 기준으로 사용하려면 **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **DNS Server(DNS** 서버**)**에서 데이터 인터페이스용 DNS도 구성해야 합니다. 시스템은 관리 DNS 서버 설정을 사용하여 액세스 제어 규칙에 사용되는 FQDN 개체 조회를 수행하지 않습니다. FQDN 확인 트러블슈팅에 대한 정보는 일반 DNS 문제 문제 해결, 829 페이지의 내용을 참조하십시오.

  FQDN으로 액세스를 제어하는 방식은 최선형 메커니즘이라는 점에 유의하십시오. 다음과 같은 점을 고려하십시오.

  - DNS 회신은 스푸핑될 수 있기 때문에 완전히 신뢰할 수 있는 내부 DNS 서버만 사용하십시오.
  - 특히 아주 인기 있는 서버에 대한 일부 FQDN에는 자주 변경되는 IP 주소가 여러 개 있을 수 있습니다. 시스템에서는 캐시된 DNS 조회 결과를 사용하므로 사용자는 캐시에는 아직 없는 새 주소를 가져올 수 있습니다. 따라서 FQDN에서 인기 사이트를 차단하여 일관성 없는 결과가 나올 수 있습니다.
  - 인기 있는 FQDN의 경우, 다양한 DNS 서버에서 일련의 다양한 IP 주소를 반환할 수 있습니다. 따라서 컨피그레이션한 것이 아닌 다른 DNS 서버를 사용자가 사용하는 경우, FQDN 기반 액세스 제어 규칙은 클라이언트에서 사용하는 사이트의 모든 IP 주소에 적용되지 않을 수 있으며 규칙에 대해 원하는 결과를 얻지 못할 수 있습니다.
  - 일부 FQDN DNS 항목의 경우에는 TTL(Time to Live) 값이 매우 짧습니다. 이로 인해 조회 테이블이 다시 컴필레이션되는 일이 자주 발생하여 전체 시스템 성능에 영향을 미칠 수 있습니다.

- 활발하게 사용 중인 규칙을 수정하는 경우 더 이상 Snort가 검사하지 않는 설정된 연결에는 변경 사항이 적용되지 않습니다. 새 규칙은 이후 연결의 일치 여부를 확인하는 데 사용됩니다. 또한 Snort가 활발하게 특정 연결을 검사하는 중인 경우, 변경된 일치 기준 또는 작업 기준을 기존 연결에 적용할 수 있습니다. 변경 사항이 모든 현재 연결에 적용되게 해야 하는 경우, 디바이스 CLI에 로그인한 다음 **clear conn** 명령을 사용하여 설정된 연결을 종료하면 됩니다. 이 경우 연결의 소스에서 연결 재설정을 시도하므로 새 규칙과 적절하게 일치한다고 가정합니다.

- 시스템은 연결에서 애플리케이션 또는 URL을 식별하기 위해 3~5개의 패킷을 사용합니다. 따라서 올바른 액세스 제어 규칙이 지정된 연결에 대해 즉시 일치되지 않을 수 있습니다. 그러나 애플리케이션/URL이 확인되고 나면 일치 규칙을 기반으로 연결이 처리됩니다. 암호화된 연결의 경우, 이는 SSL 핸드셰이크에서 서버 인증서 교환 이후에 발생합니다.

- 시스템은 애플리케이션이 식별된 연결에서 페이로드가 없는 패킷에 기본 정책 작업을 적용합니다.
- 특히 보안 영역, 네트워크 개체 및 포트 개체에 대한 일치 기준은 가능한 경우 항상 비워 둡니다. 예를 들어, 모든 인터페이스가 포함된 영역을 생성하는 대신 보안 영역 기준을 비워 두기만 하면 시스템에서 모든 인터페이스에 대한 트래픽을 더 효율적으로 일치시킬 수 있습니다. 여러 기준을 지정하는 경우 시스템에서는 지정된 기준의 모든 콘텐츠 조합에 대해 일치시켜야 합니다.
- 소스 또는 대상 기준에 대해 IP 주소를 지정하는 경우 동일한 규칙에서 IPv4 및 IPv6 주소를 혼합하지 마십시오. IPv4 및 IPv6 주소에 대해 별도의 규칙을 생성하십시오.
- 관련 Rfc를 위반하는 GRE 터널은 삭제 됩니다. 예를 들어, GRE 터널이 RFC와 달리 예약된 비트에 0이 아닌 값을 포함하는 경우 이는 삭제 됩니다. 비규격 GRE 터널을 허용해야 하는 경우 원격 관리자를 사용하고 세션을 신뢰하는 사전 필터 규칙을 구성해야 합니다. device manager를 사용하여 사전 필터 규칙을 구성할 수 없습니다.

액세스 제어 정책 구성

액세스 제어 정책을 사용하여 네트워크 리소스에 대한 액세스를 제어합니다. 이 정책은 하향식으로 평가되는 순서가 지정된 규칙 집합으로 구성됩니다. 트래픽에 적용되는 규칙은 모든 트래픽 기준이 일치하는 첫 번째 규칙입니다. 트래픽과 일치하는 규칙이 없으면 페이지 맨 아래에 표시된 기본 작업이 적용됩니다.

액세스 제어 정책을 구성하려면 **Policies(**정책**)** > **Access Control(**액세스 제어**)**을 선택합니다.

액세스 제어 테이블에는 모든 규칙이 순서대로 나열됩니다. 각 규칙에 대해 다음을 수행합니다.

- 맨 왼쪽 열의 규칙 번호 옆에 있는 > 버튼을 클릭하여 규칙 다이어그램을 엽니다. 다이어그램을 통해 규칙이 어떻게 트래픽을 제어하는지 시각화할 수 있습니다. 버튼을 다시 클릭하여 다이어그램을 닫습니다.
- 대부분의 셀에서는 인라인 수정이 허용됩니다. 예를 들어, 작업을 클릭하여 다른 작업을 선택하거나 소스 네트워크 개체를 클릭하여 소스 기준을 추가 또는 변경할 수 있습니다.
- 규칙을 이동하려면 규칙 위에 마우스를 올려놓고 이동 아이콘( )이 나타나면 이를 클릭하여 규칙을 새 위치로 끌어 놓습니다. 규칙을 수정하고 순서 목록에서 새 위치를 선택하여 규칙을 이동할 수도 있습니다. 규칙은 처리할 순서대로 배치해야 합니다. 특정 규칙, 특히 더 일반적인 규칙에 대한 예외를 정의하는 규칙은 목록 위쪽에 있어야 합니다.
- 맨 오른쪽 열에는 규칙의 작업 버튼이 포함되어 있습니다. 셀 위에 마우스를 올려 놓으면 버튼이 표시됩니다. 규칙은 수정( )하거나 삭제( )할 수 있습니다.
- 액세스 컨트롤 설정 ( ) 버튼을 클릭하여 정책 내 특정 규칙이 아닌 액세스 컨트롤 정책에 적용되는 설정을 구성합니다.
- 테이블에서 적중 횟수 열을 추가 또는 제거하려면 테이블 위쪽에 있는 **Toggle Hit Counts(**적중 횟수 토글**)** 아이콘( )을 클릭합니다. 적중 횟수 열은 규칙에 대한 총 적중 횟수와 최종 적중 날

짜 및 시간과 함께 이름 열의 오른쪽에 표시됩니다. 적중 횟수 정보는 토글 버튼을 클릭하면 가져올 수 있습니다. 최신 정보를 얻으려면 **refresh(**새로고침**)** 아이콘()을 클릭하십시오.

- 예를 들어 제거 또는 변경된 URL 카테고리 때문에 어떤 규칙에 문제가 생긴 경우에는 검색 상자 옆에 있는 **See Problem Rules(**문제 규칙 참조**)** 링크를 클릭하여 해당 규칙만 표시하도록 테이블을 필터링합니다. 이러한 규칙에서 필요한 서비스를 제공하도록 수정 및 교정(또는 삭제)하십시오.

다음 항목에서는 정책을 구성하는 방법을 설명합니다.

기본 작업 구성

특정 액세스 규칙과 일치하지 않는 연결은 액세스 제어 정책의 기본 작업에 의해 처리됩니다.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)**을 선택합니다.

단계 **2** **Default Action(**기본 작업**)** 필드에서 아무 곳이나 클릭합니다.

단계 **3** 일치하는 트래픽에 적용할 작업을 선택합니다.

- **Trust(**신뢰**)** - 어떤 종류든 추가 검사 없이 트래픽을 허용합니다.
- **Allow(**허용**)** - 침입 정책이 적용되는 트래픽을 허용합니다.
- **Block(**차단**)** - 트래픽을 무조건 삭제합니다. 트래픽은 검사되지 않습니다.

단계 **4** 작업이 **Allow(**허용**)**인 경우 침입 정책을 선택합니다.

정책 옵션에 대한 설명은 침입 정책 설정, 540 페이지를 참조하십시오.

단계 **5** (선택 사항). 기본 작업에 대한 로깅을 구성합니다.

기본 작업과 일치하는 트래픽에 대한 로깅을 활성화해야 대시보드 데이터 또는 이벤트 뷰어에 해당 트래픽이 포함됩니다. 로깅 설정, 541 페이지의 내용을 참조하십시오.

단계 **6** **OK(**확인**)**를 클릭합니다.

액세스 컨트롤 정책 설정 구성

정책 내 특정 규칙이 아닌 액세스 컨트롤 정책에 적용되는 설정을 구성할 수 있습니다.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 컨트롤**)**을 선택합니다.

단계 **2** **Access Policy Settings(**액세스 정책 설정**)** () 버튼을 클릭합니다.

단계 **3** 설정을 구성합니다.

- **TLS Server Identity Discovery(TLS** 서버 **ID** 검색**)** - TLS 1.3 인증서가 암호화됩니다. 애플리케이션 또는 URL 필터링을 사용하는 액세스 규칙과 일치하도록 TLS 1.3으로 암호화된 트래픽의 경우 시스템은 TLS 1.3 인증서를 암호 해독해야 합니다. 암호화된 연결이 올바른 액세스 제어 규칙과 일치하는지 확인하려면 이 옵션을 활성화하는 것이 좋습니다. 설정은 인증서만 암호 해독합니다. 연결은 암호화된 상태로 유지됩니다. 이 옵션을 활성화하면 TLS 1.3 인증서를 해독할 수 있습니다. 해당 SSL 암호 해독 규칙을 생성할 필요가 없습니다.
- **Reputation Enforcement on DNS Traffic(DNS** 트래픽에 대한 평판 시행**)** - URL 필터링 범주 및 평판 규칙을 DNS 조회 요청에 적용하려면 이 옵션을 활성화합니다. 조회 요청의 FQDN(Fully Qualified Domain Name)에 차단 중인 범주 및 평판이 있는 경우 시스템은 DNS 응답을 차단합니다. 사용자는 DNS 확인을 받지 않으므로 연결을 완료할 수 없습니다. 웹 이외의 트래픽에 URL 범주 및 평판 필터링을 적용하려면 이 옵션을 사용합니다. 자세한 내용은 DNS 요청 필터링, 524 페이지를 참고하십시오.

단계 **4** **OK(**확인**)**를 클릭합니다.

액세스 제어 규칙 구성

액세스 제어 규칙을 사용하여 네트워크 리소스에 대한 액세스를 제어합니다. 액세스 제어 정책의 규칙은 위에서부터 아래로 평가됩니다. 트래픽에 적용되는 규칙은 모든 트래픽 기준이 일치하는 첫 번째 규칙입니다.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)**을 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 새 규칙을 생성하려면 **+** 버튼을 클릭합니다.
- 기존 규칙을 수정하려면 해당 규칙의 수정 아이콘( )을 클릭합니다.

더 이상 필요하지 않은 규칙을 삭제하려면 해당 규칙의 삭제 아이콘( )을 클릭합니다.

단계 **3** **Order(**순서**)**에서 순서가 지정된 규칙 목록에 규칙을 삽입할 위치를 선택합니다.

규칙은 처음 일치하는 항목을 기준으로 적용되므로, 매우 구체적인 트래픽 일치 기준이 포함된 규칙이 보다 일반적인 기준이 포함된 정책(규칙이 일치하지 않는 경우 일치하는 트래픽에 적용됨) 위에 표시되도록 삽입해야 합니다.

기본적으로는 규칙이 목록의 끝에 추가됩니다. 나중에 규칙의 위치를 변경하려는 경우 이 옵션을 수정합니다.

단계 **4** **Tile(**제목**)**에서 규칙의 이름을 입력합니다.

이름에는 공백을 포함할 수 없지만, 영숫자 및 특수 문자(+, ., _, -)는 사용할 수 있습니다.

단계 **5** 일치하는 트래픽에 적용할 작업을 선택합니다.

- **Trust(**신뢰**)** - 어떤 종류든 추가 검사 없이 트래픽을 허용합니다.
- **Allow(**허용**)** - 정책에서 침입 및 기타 검사 설정이 적용되는 트래픽을 허용합니다.
- **Block(**차단**)** - 트래픽을 무조건 삭제합니다. 트래픽은 검사되지 않습니다.

단계 **6** 다음 탭을 적절하게 조합하여 트래픽 일치 기준을 정의합니다.

- **Source/Destination(**소스/대상**)** — 트래픽이 통과하는 보안 영역(인터페이스), IP 주소/IP 주소의 국가나 대륙(지리적 위치), 주소에 할당된 SGT(Security Group Tag) 또는 트래픽에서 사용되는 프로토콜과 포트입니다. 기본값은 모든 영역, 주소, 지리적 위치, SGT, 프로토콜 및 포트입니다. 소스/대상 기준, 534 페이지의 내용을 참조하십시오.
- **Application(**애플리케이션**)** - 유형, 범주, 태그, 위험, 사업 타당성에 따라 애플리케이션을 정의하는 필터 또는 애플리케이션입니다. 기본값은 모든 애플리케이션입니다. 애플리케이션 기준, 536 페이지의 내용을 참조하십시오.
- **URL** - 웹 또는 DNS 조회 요청의 URL 또는 URL 범주입니다. 기본값은 모든 URL입니다. URL 기준, 538 페이지의 내용을 참조하십시오.
- **Users(**사용자**)** - ID 소스, 사용자 또는 사용자 그룹입니다. ID 정책에 따라 트래픽 일치에 사용자 및 그룹 정보를 사용할 수 있는지가 결정됩니다. 이 기준을 사용하려면 ID 정책을 구성해야 합니다. 사용자 기준, 539 페이지의 내용을 참조하십시오.

조건을 수정하려면 해당 조건 내의 **+** 버튼을 클릭하고 필요한 개체나 요소를 선택한 후에 팝업 대화상자에서 **OK(**확인**)**를 클릭합니다. 기준에 개체가 필요한데 필요한 개체가 없는 경우에는 새 개체 생성을 클릭하면 됩니다. 개체 또는 요소의 **x**를 클릭하면 정책에서 해당 개체나 요소를 제거할 수 있습니다.

조건을 액세스 제어 규칙에 추가할 경우 다음 팁을 고려하십시오.

- 규칙마다 여러 조건을 구성할 수 있습니다. 규칙을 트래픽에 적용하려면 트래픽이 규칙의 모든 조건과 일치해야 합니다. 예를 들어, 특정 호스트 또는 네트워크에 대해 URL 필터링을 수행하는 단일 규칙을 사용할 수 있습니다.
- 규칙의 각 조건에 대해 최대 50개의 기준을 추가할 수 있습니다. 조건의 기준 중 어느 것이든 모두 일치하는 트래픽은 조건을 만족합니다. 예를 들어, 최대 50개의 애플리케이션 또는 애플리케이션 필터에 대해 애플리케이션 제어를 적용하는 단일 규칙을 사용할 수 있습니다. 따라서 단일 조건의 항목 간 관계는 OR이고 조건 유형 간의 관계(예: 소스/대상과 애플리케이션 간의 관계)는 AND가 됩니다.
- 일부 기능을 사용하려면 적절한 라이선스를 활성화해야 합니다.

단계 **7** (선택 사항). 허용 작업을 사용하는 정책의 경우 암호화되지 않은 트래픽에 대한 추가 검사를 구성할 수 있습니다. 다음 링크 중 하나를 클릭합니다.

- **Intrusion Policy(**침입 정책**)** — **Intrusion Policy(**침입 정책**)** > **On(**켜기**)**을 선택하고 트래픽에서 침입과 익스플로잇을 검사할 침입 검사 정책을 선택합니다. 침입 정책 설정, 540 페이지의 내용을 참조하십시오.
- **File Policy(**파일 정책**)** - 트래픽에서 차단해야 하는 파일과 악성코드가 포함된 파일을 검사하기 위한 파일 정책을 선택합니다. 파일 정책 설정, 540 페이지의 내용을 참조하십시오.

단계 **8** (선택 사항). 규칙에 대해 로깅을 구성합니다.

기본적으로 규칙과 일치하는 트래픽에 대해서는 연결 이벤트가 생성되지 않습니다. 단, 파일 정책을 선택하면 파일 이벤트가 기본적으로 생성됩니다. 이 행동은 변경할 수 있습니다. 정책과 일치하는 트래픽에 대한 로깅을 활성화해야 대시보드 데이터 또는 이벤트 뷰어에 해당 트래픽이 포함됩니다. 로깅 설정, 541 페이지의 내용을 참조하십시오.

침입 이벤트는 항상 일치하는 액세스 규칙의 로깅 컨피그레이션과 관계없이 삭제하거나 알리도록 설정된 침입 규칙에 대해 생성됩니다.

단계 **9** **OK(**확인**)**를 클릭합니다.

소스/대상 기준

액세스 규칙의 Source/Destination(소스/대상) 기준은 트래픽이 통과하는 보안 영역(인터페이스), IP 주소/IP 주소의 국가나 대륙(지리적 위치), 주소에 할당된 SGT(Security Group Tag) 또는 트래픽에서 사용되는 프로토콜과 포트를 정의합니다. 기본값은 모든 영역, 주소, 지리적 위치, SGT, 프로토콜 및 포트입니다.

조건을 수정하려면 해당 조건 내의 **+** 버튼을 클릭하고 필요한 개체나 요소를 선택한 후에 **OK(**확인**)**를 클릭합니다. 기준에 개체가 필요한데 필요한 개체가 없는 경우에는 새 개체 생성을 클릭하면 됩니다. 개체 또는 요소의 **x**를 클릭하면 정책에서 해당 개체나 요소를 제거할 수 있습니다.

다음 기준을 사용하여 규칙과 일치하는 소스 및 대상을 식별할 수 있습니다.

소스 영역**,** 대상 영역

트래픽이 통과하는 인터페이스를 정의하는 보안 영역 개체입니다. 기준은 하나 또는 둘 다 정의할 수도 있고 둘 다 정의하지 않을 수도 있습니다. 지정되지 않은 기준은 임의 인터페이스의 트래픽에 적용됩니다.

- 영역 내 인터페이스의 디바이스에서 나가는 트래픽에 일치시키기 위해서는 대상 영역에 해당 영역을 추가합니다.
- 영역 내 인터페이스를 통해 디바이스로 들어오는 트래픽에 일치시키기 위해서는 소스 영역에 해당 영역을 추가합니다.
- 규칙에 소스와 대상 영역 조건을 모두 추가한 경우, 일치하는 트래픽은 반드시 지정된 소스 영역 중 하나에서 발생해야 하며 대상 영역 중 하나를 통해 전송되어야 합니다.

트래픽이 디바이스로 들어오거나 디바이스에서 나가는 위치를 기준으로 규칙을 적용해야 하는 경우 이 기준을 사용해야 합니다. 예를 들어 내부 호스트로 이동하는 모든 트래픽에서 침입을 검사하려는 경우에는 내부 영역을 **Destination Zones(**대상 영역**)**로 선택하고 소스 영역은 비워 둡니다. 규칙에서 침입 필터링을 구현하려면 규칙 작업이 **Allow(**허용**)**여야 하며 규칙에서 침입 정책을 선택해야 합니다.

참고 단일 규칙에서 패시브 보안 영역과 라우팅 보안 영역을 함께 사용할 수는 없습니다. 또한 패시브 보안 영역은 소스 영역으로만 지정할 수 있으며 대상 영역으로 지정할 수는 없습니다.

소스 네트워크, 대상 네트워크

트래픽의 네트워크 주소나 위치를 정의하는 네트워크 개체 또는 지리적 위치입니다.

- 특정 IP 주소 또는 지리적 위치에서 나오는 트래픽을 일치시키려면 소스 네트워크를 구성합니다.
- 특정 IP 주소 또는 지리적 위치로 향하는 트래픽을 일치시키려면 대상 네트워크를 구성합니다.
- 규칙에 소스와 대상 네트워크 조건을 모두 추가한 경우, 일치하는 트래픽은 반드시 지정된 IP 주소 중 하나에서 발생해야 하며 그 목적지가 대상 IP 주소 중 하나여야 합니다.

이 기준을 추가할 때는 다음 탭에서 선택합니다.

- 네트워크 - 제어하려는 트래픽의 소스 또는 대상 IP 주소를 정의하는 네트워크 개체 또는 그룹을 선택합니다. FQDN(Fully Qualified Domain Name)을 사용하여 주소를 정의하는 개체를 사용할 수 있습니다. 주소는 DNS 조회를 통해 확인됩니다.
- 지리위치 - 소스 또는 대상 국가나 대륙을 기준으로 트래픽을 제어하려면 지리적 위치를 선택합니다. 대륙을 선택하면 대륙 내의 모든 국가가 선택됩니다. 규칙에서 지리적 위치를 직접 선택하는 방법 외에, 위치를 정의하기 위해 생성한 지리위치 개체를 선택할 수도 있습니다. 지리적 위치를 사용하면 특정 국가에서 사용될 수 있는 모든 IP 주소를 몰라도 해당 국가에 대한 액세스를 쉽게 제한할 수 있습니다.

참고 최신 지리적 위치 데이터를 사용하여 트래픽을 필터링하려면 GeoDB(geolocation database)를 정기적으로 업데이트하는 것이 좋습니다.

소스 포트, 대상 포트/프로토콜

트래픽에 사용되는 프로토콜을 정의하는 포트 개체입니다. TCP/UDP의 경우 여기에는 포트가 포함될 수 있습니다. ICMP의 경우에는 코드와 유형이 포함될 수 있습니다.

- 특정 프로토콜이나 포트에서 나오는 트래픽을 일치시키려면 소스 포트를 구성합니다. 소스 포트는 TCP/UDP 전용일 수 있습니다.
- 특정 프로토콜이나 포트로 향하는 트래픽을 일치시키려면 대상 포트/프로토콜을 구성합니다. 조건에 대상 포트만 추가할 경우, 다른 전송 프로토콜을 사용하는 포트를 추가할 수 있습니다. ICMP 및 기타 비TCP/UDP 사양은 대상 포트에서만 허용되며 소스 포트에서는 허용되지 않습니다.

- 특정 TCP/UDP 포트에서 발생하는 트래픽과 특정 TCP/UDP 포트로 향하는 트래픽을 모두 일치시키려면 두 포트를 모두 구성합니다. 조건에 소스 및 대상 포트를 모두 추가한 경우, 단일 전송 프로토콜(TCP 또는 UDP)을 공유하는 포트만 추가할 수 있습니다. 예를 들어 포트 TCP/80에서 포트 TCP/8080으로 이동하는 트래픽을 대상으로 지정할 수 있습니다.

소스 **SGT** 그룹**,** 대상 **SGT** 그룹

ISE(Identity Services Engine)에서 다운로드되는 트래픽에 할당된 SGT를 식별하는 SGT(Security Group Tag) 그룹 개체입니다. ISE ID 소스를 정의하는 경우에만 이러한 개체를 사용할 수 있습니다. 그렇지 않으면 이 섹션은 나타나지 않습니다. 엑세스 제어를 위한 SGT 사용 방법에 대한 자세한 내용은 TrustSec SGT(Security Group Tag)를 사용하여 네트워크 액세스를 제어하는 방법, 546 페이지를 참조하십시오.

- 소스에 그룹에 정의된 SGT 중 하나가 있는 트래픽을 일치시키려면 소스 **SGT** 그룹을 구성합니다.
- 그룹에 정의된 SGT 중 하나를 포함하는 대상에 트래픽을 일치시키려면 대상 **SGT** 그룹을 구성합니다.
- 규칙에 소스와 대상 SGT 조건을 모두 추가한 경우 일치하는 트래픽은 반드시 지정된 태그 중 하나를 가진 소스에서 발생해야 하며 대상 태그 중 하나로 대상이 지정되어 있어야 합니다.

애플리케이션 기준

액세스 규칙의 애플리케이션 기준은 IP 연결 또는 필터에 사용되는 애플리케이션을 정의하며 유형, 범주, 태그, 위험 또는 사업 타당성에 따라 애플리케이션을 정의합니다. 기본값은 모든 애플리케이션입니다.

규칙에서 개별 애플리케이션을 지정할 수 있으나 애플리케이션 필터를 사용하면 정책 생성 및 관리가 간소화됩니다. 예를 들어, 위험도가 높고 비즈니스 관련성이 낮은 모든 애플리케이션을 식별하여 차단하는 액세스 제어 규칙을 만들 수 있습니다. 사용자가 이러한 애플리케이션 중 하나를 사용하려고 할 경우, 세션은 차단됩니다.

이와 더불어 Cisco에서는 시스템 및 VDB(Vulnerability Database)를 통해 추가 애플리케이션 탐지기를 자주 업데이트하고 추가합니다. 따라서 규칙을 수동으로 업데이트하지 않아도 위험도가 높은 애플리케이션을 차단하는 규칙이 새 애플리케이션에 자동으로 적용될 수 있습니다.

규칙에서 애플리케이션 및 필터를 직접 지정하거나 이러한 특성을 정의하는 애플리케이션 필터 개체를 생성할 수 있습니다. 이 두 가지 경우의 사양은 동일하지만, 개체를 사용하면 복잡한 규칙을 생성할 때에도 시스템 제한(기준당 항목 50개)을 유지하기가 더욱 쉽습니다.

애플리케이션 및 필터 목록을 수정하려면 조건 내에서 **+** 버튼을 클릭하고 개별 탭에 나열된 원하는 애플리케이션 또는 애플리케이션 필터 개체를 선택한 후에 팝업 대화 상자에서 **OK(**확인**)**를 클릭합니다. 탭 중 하나에서 **Advanced Filter(**고급 필터**)**를 클릭하면 필터 기준을 선택하거나 특정 애플리케이션을 검색할 수 있습니다. 애플리케이션, 필터 또는 개체에 대해 **x**를 클릭하면 정책에서 해당 항목을 제거할 수 있습니다. **Save As Filter(**필터로 저장**)** 링크를 클릭하면 아직 개체가 아닌 결합된 기준을 새 애플리케이션 필터 개체로 저장할 수 있습니다.

참고 선택한 애플리케이션을 VDB 업데이트를 통해 제거한 경우 애플리케이션 이름 뒤에 "(Depredcated(사용되지 않음))"이라고 표시됩니다. 이러한 애플리케이션은 필터에서 제거해야 합니다. 그렇지 않으면 후속 구축 및 시스템 소프트웨어 업그레이드가 차단됩니다.

다음과 같은 고급 필터 기준을 사용하여 규칙과 일치하는 애플리케이션이나 필터를 식별할 수 있습니다. 이러한 애플리케이션 또는 필터는 애플리케이션 필터 개체에서 사용되는 것과 같은 요소입니다.

참고 단일 필터 기준으로 여러 선택 항목이 OR 관계를 갖습니다. 예를 들어, 위험은 높음 OR 매우 높음입니다. 반면 필터 간의 관계는 AND입니다. 즉, 위험은 높음 OR 매우 높음 AND 사업 타당성은 낮음 OR 매우 낮음과 같습니다. 필터를 선택하면 디스플레이의 애플리케이션 목록이 업데이트되어 기준을 충족하는 애플리케이션만 표시됩니다. 이러한 필터를 사용하여 개별적으로 추가하려는 애플리케이션을 찾거나, 규칙에 추가할 적절한 필터를 선택하고 있는지를 확인할 수 있습니다.

위험

애플리케이션이 조직의 보안 정책과 상반되는 용도로 사용될 가능성(매우 낮음~매우 높음)

사업 타당성

조직의 비즈니스 운영(레크리에이션과 반대) 컨텍스트 내에서 애플리케이션이 사용될 가능성(매우 낮음~매우 높음)

유형

애플리케이션 유형:

- 애플리케이션 프로토콜 - 호스트 간의 통신을 나타내는 HTTP, SSH 등의 애플리케이션 프로토콜
- 클라이언트 프로토콜 - 호스트에서 실행 중인 소프트웨어를 나타내는 웹 브라우저, 이메일 클라이언트 등의 클라이언트
- 웹 애플리케이션 - HTTP 트래픽의 요청 URL 또는 콘텐츠를 나타내는 MPEG 비디오, Facebook 등의 웹 애플리케이션

범주

가장 중요한 기능을 설명하는 일반 애플리케이션 분류

태그

애플리케이션에 대한 추가 정보로, 범주와 비슷합니다.

암호화된 트래픽의 경우, 시스템은 **SSL** 프로토콜 태그가 지정된 애플리케이션만 사용하여 트래픽을 식별하고 필터링할 수 있습니다. 이 태그가 없는 애플리케이션은 암호화되지 않은 트래픽 또는 해독된 트래픽에서만 탐지할 수 있습니다. 또한 암호화된 트래픽 또는 암호화되지 않은 트

래픽이 아닌 암호 해독된 트래픽에서만 탐지할 수 있는 애플리케이션에는 암호 해독된 트래픽 태그가 할당됩니다.

애플리케이션 목록(디스플레이 하단)

이 목록은 목록 위의 옵션에서 필터를 선택하면 업데이트되므로 현재 필터와 일치하는 애플리케이션을 확인할 수 있습니다. 이 목록을 사용하여 규칙에 필터 기준을 추가하려는 경우 필터가 적절한 애플리케이션을 대상으로 하는지를 확인할 수 있습니다. 특정 애플리케이션을 추가하려는 경우 이 목록에서 선택합니다.

URL 기준

액세스 규칙의 URL 기준은 웹 요청에 사용되는 URL 또는 요청된 URL이 속하는 범주를 정의합니다. 범주가 일치하는 경우 허용하거나 차단할 사이트의 상대적 평판을 지정할 수도 있습니다. 기본적으로는 모든 URL이 허용됩니다.

DNS 조회 요청 필터링을 활성화하면 범주 및 평판 설정이 조회 요청의 FQDN(Fully Qualified Domain Name)에도 적용됩니다. 범주 및 평판 설정만 DNS 요청 필터링에 적용됩니다. 수동 URL 필터링은 무시됩니다.

URL 카테고리 및 평판을 통해 액세스 제어 규칙의 URL 조건을 신속하게 만들 수 있습니다. 예를 들어, 모든 게임 사이트 또는 신뢰할 수 없는 소셜 네트워킹 사이트를 차단할 수 있습니다. 사용자가 해당 카테고리 및 평판 조합을 가진 URL 검색을 시도하는 모든 경우, 세션이 차단됩니다.

범주 및 평판 데이터를 사용하면 정책 생성 및 관리도 간소화됩니다. 이를 통해 시스템이 웹 트래픽을 예상대로 제어할 수 있습니다. 마지막으로, Cisco의 위협 인텔리전스는 새로운 URL, 새로운 범주 및 기존 URL의 새로운 범주와 위험이 적용되어 지속적으로 업데이트되므로 시스템은 최신 정보를 사용하여 요청된 URL을 필터링할 수 있습니다. 악성코드, 스팸, 봇넷, 피싱과 같은 보안 위협을 나타내는 악성 사이트는 새로운 정책을 업데이트하고 구축하는 것보다 빠르게 나타났다 사라질 수 있습니다.

URL 목록을 수정하려면 조건 내의 **+** 버튼을 클릭하고 다음 기술 중 하나를 사용하여 원하는 범주 또는 URL을 선택합니다. 범주 또는 개체의 **x**를 클릭하면 정책에서 해당 범주나 개체를 제거할 수 있습니다.

URL 탭

+를 클릭하고 URL 개체 또는 그룹을 선택한 후에 **OK(**확인**)**를 클릭합니다. 필요한 개체가 없는 경우에는 **Create New URL(**새 **URL** 생성**)**을 클릭하면 됩니다.

참고 특정 사이트를 대상으로 하도록 URL 개체를 구성하기 전에 수동 URL 필터링에 대한 정보를 자세히 확인하십시오.

범주 탭

+를 클릭하고 원하는 범주를 선택한 후에 **OK(**확인**)**를 클릭합니다.

카테고리에 대한 설명은 https://www.talosintelligence.com/categories를 참조하십시오.

기본적으로는 평판과 관계없이 선택한 각 범주의 모든 URL에 규칙을 적용합니다. 평판을 기준으로 하여 규칙을 제한하려면 각 범주의 아래쪽 화살표를 클릭하고 임의 체크 박스 선택을 취소한 후에 평판 슬라이더를 사용하여 평판 레벨을 선택합니다. 평판 슬라이더의 왼쪽은 허용할 사이트를, 오른쪽은 차단할 사이트를 나타냅니다. 평판 사용 방식은 규칙 작업에 따라 달라집니다.

- 규칙이 웹 액세스를 차단하거나 모니터링하는 경우 평판 레벨을 선택하면 해당 레벨보다 심각도가 높은 모든 평판도 선택됩니다. 예를 들어, **Questionable sites(**의심스러운 사이트**)**(레벨 2)를 차단하거나 모니터링하는 규칙을 구성하는 경우, **Untrusted(**신뢰할 수 없음**)**(레벨 1) 사이트도 자동으로 차단되거나 모니터링됩니다.
- 규칙이 웹 액세스를 허용하는 경우 평판 레벨을 선택하면 해당 레벨보다 심각도가 낮은 모든 평판도 선택됩니다. 예를 들어, **Favorable sites(**선호 사이트**)**(레벨 4)를 허용하는 규칙을 구성하는 경우, **Trusted(**신뢰할 수 있음**)(**레벨 **5)** 사이트도 자동으로 허용됩니다.

평판을 알 수 없는 URL을 평판 일치에 포함하려면 **Include Sites with Unknown Reputation(**평판을 알 수 없는 사이트 포함**)** 옵션을 선택합니다. 새 사이트는 일반적으로 등급이 지정되지 않으며, 사이트의 평판을 알 수 없거나 확인할 수 없는 다른 이유가 있을 수 있습니다.

URL의 카테고리 확인

특정 URL의 카테고리 및 평판을 확인할 수 있습니다. **URL to Check(**확인할 **URL)** 상자에서 URL을 입력하고 **Go(**이동**)**를 클릭하십시오. 결과를 볼 수 있는 외부 웹 사이트로 연결됩니다. 분류에 동의하지 않는 경우 **Submit a URL Category Dispute(URL** 카테고리 이의 제출**)** 링크를 클릭하고 저희에게 알려주십시오.

사용자 기준

액세스 규칙의 사용자 기준은 IP 연결의 사용자 또는 사용자 그룹을 정의합니다. 액세스 규칙에 사용자 또는 사용자 그룹 기준을 포함하려면 ID 정책 및 연관된 디렉터리 서버를 구성해야 합니다.

ID 정책에 따라 특정 연결에 대해 사용자 ID가 수집되는지가 결정됩니다. ID가 설정된 경우에는 호스트의 IP 주소가 식별된 사용자와 연결됩니다. 그러므로 해당 소스 IP 주소가 사용자에 매핑된 트래픽은 해당 사용자가 보내는 것으로 간주됩니다. IP 패킷 자체는 사용자 ID 정보를 포함하지 않으므로 이 IP 주소에서 사용자로의 매핑은 가능한 최적의 근사치입니다.

규칙에는 최대 50개의 사용자나 그룹을 추가할 수 있으므로 일반적으로는 개별 사용자를 선택하는 것보다 그룹을 선택하는 것이 더 효율적입니다. 예를 들어 엔지니어링 그룹의 개발 네트워크 액세스를 허용하는 규칙을 생성한 다음 네트워크에 대한 기타 모든 액세스를 거부하는 후속 규칙을 생성할 수 있습니다. 그러면 신규 엔지니어에 대해 규칙을 적용하려는 경우 디렉터리 서버의 엔지니어링 그룹에 해당 엔지니어를 추가하기만 하면 됩니다.

해당 소스 내 모든 사용자에게 적용할 ID 소스도 선택할 수 있습니다. 따라서 여러 Active Directory 도메인을 지원하는 경우, 도메인에 근거하여 리소스에 대한 차등 액세스를 제공할 수 있습니다.

사용자 목록을 수정하려면 조건 내의 **+** 버튼을 클릭하고 다음 기법 중 하나를 사용하여 원하는 ID를 선택하십시오. ID의 **x**를 클릭하면 정책에서 제거할 수 있습니다.

- **Identity Sources(ID** 소스**)** - 선택한 소스에서 얻은 모든 사용자에게 규칙을 적용하려면 AD 영역 또는 로컬 사용자 데이터베이스 같은 ID 소스를 선택합니다. 필요한 영역이 아직 없는 경우, **Create New Identity Realm(**새 **ID** 영역 생성**)**을 클릭하여 바로 생성합니다.

- **Groups(**그룹**)** - 원하는 사용자 그룹을 선택합니다. 그룹은 디렉터리 서버에서 그룹을 구성하는 경우에만 사용할 수 있습니다. 그룹을 선택하면 하위 그룹을 포함하여 그룹의 모든 멤버에게 규칙이 적용됩니다. 하위 그룹을 다르게 처리하려는 경우에는 하위 그룹용으로 별도의 액세스 규칙을 생성한 다음 액세스 제어 정책에서 상위 그룹용 규칙 위에 배치해야 합니다.
- **Users(**사용자**)** - 개별 사용자를 선택합니다. 사용자 이름에는 Realm\username과 같은 ID 소스가 접두사로 붙습니다.

  Special-Identities-Realm에서 일부 사용자는 기본으로 제공됩니다.

  - **Failed Authentication(**실패한 인증**)** - 사용자에게 인증하라는 메시지가 표시되었는데 사용자가 허용되는 최대 횟수 이내에 유효한 사용자 이름/비밀번호 쌍을 입력하지 못했습니다. 인증에 실패해도 사용자의 네트워크 액세스가 차단되지는 않지만, 이러한 사용자의 네트워크 액세스를 제한하는 액세스 규칙을 작성할 수 있습니다.
  - **Guest(**게스트**)** - 게스트 사용자는 ID 규칙이 이러한 사용자를 게스트로 지칭하도록 구성된다는 점을 제외하면 실패한 인증 사용자와 비슷합니다. 즉, 게스트 사용자 역시 인증하라는 메시지가 표시되었지만, 최대 시도 횟수 이내에 인증하지 못한 사용자입니다.
  - **No Authentication Required(**인증 필요 없음**)** - 사용자의 연결이 인증을 지정하지 않은 ID 규칙과 일치하여 인증하라는 메시지가 표시되지 않았습니다.
  - **Unknown(**알 수 없음**)** - IP 주소에 대한 사용자 매핑이 없으며 아직 실패한 인증 기록이 없습니다. 이는 일반적으로 해당 주소에서 HTTP 트래픽이 아직 전송되지 않았음을 의미합니다.

침입 정책 설정

Cisco는 방화벽 시스템에서 여러 침입 정책을 제공합니다. Cisco Cisco Talos Intelligence Group(Talos)이 제공하는 여러 침입 정책은 Cisco에서 설계하였습니다. Talos는 침입 및 전처리기 규칙 상태와 고급 설정을 설정했습니다. 트래픽을 허용하는 액세스 제어 규칙의 경우 침입 정책을 선택하여 트래픽에서 침입 및 익스플로잇을 검사할 수 있습니다. 침입 정책은 패턴을 기반으로 디코딩된 패킷에서 공격을 검사하며 악의적인 트래픽을 차단하거나 변경할 수 있습니다.

Snort 2를 실행할 때는 이러한 정책만 사용할 수 있으며 수정할 수 없습니다. 그러나 침입 규칙 작업 변경(Snort 2), 582 페이지의 설명대로 특정 규칙에 대해 취할 조치를 변경할 수 있습니다.

Snort 3을 실행할 때 이러한 정책 중 하나를 선택하거나 자체 침입 정책을 생성할 수 있습니다.

침입 검사를 활성화하려면 **Intrusion Policy(**침입 정책**)** > **On(**켜기**)**을 선택하고 원하는 정책을 선택합니다. 각 정책에 대한 설명을 보려면 드롭다운 목록에서 정책의 정보 아이콘을 클릭합니다.

사전 정의된 정책에 대한 자세한 내용은 시스템 정의 네트워크 분석 및 침입 정책, 554 페이지의 내용을 참조하십시오.

파일 정책 설정

악성코드 방어를 사용해 악의적인 소프트웨어 또는 악성코드를 탐지하기 위해 파일 정책을 사용합니다. 파일 제어를 수행하는 데에도 파일 정책을 사용할 수 있습니다. 그러면 파일에 악성코드가 있는지와 관계없이 특정 유형의 모든 파일에 대한 제어가 가능합니다.

악성코드 방어는 Secure Malware Analytics Cloud를 사용하여 네트워크 트래픽에서 탐지될 가능성이 있는 악성코드의 상태를 검색하고 로컬 악성코드 분석 및 파일 사전 분류 업데이트를 가져옵니다. 관리 인터페이스에는 Secure Malware Analytics Cloud에 연결하고 악성코드 조회를 수행하기 위한 인터넷으로 연결되는 경로가 있어야 합니다. 디바이스는 적합한 파일을 탐지하면 파일의 SHA-256 해시 값을 사용하여 Secure Malware Analytics Cloud에서 파일의 상태를 쿼리합니다. 가능한 상태는 다음과 같습니다.

- Malware(악성코드) - Secure Malware Analytics Cloud가 파일을 악성코드로 분류했습니다. 아카이브 파일(예: zip 파일)은 해당 파일 내에 악성코드인 파일이 있으면 악성코드로 표시됩니다.
- Clean(정상) - Secure Malware Analytics Cloud가 파일을 악성코드가 포함되어 있지 않은 정상 파일로 분류했습니다. 아카이브 파일은 해당 파일 내의 모든 파일이 정상이면 정상으로 표시됩니다.
- Unknown(알 수 없음) - Secure Malware Analytics Cloud가 파일에 상태를 아직 할당하지 않았습니다. 아카이브 파일은 해당 파일 내에 알 수 없는 상태의 파일이 있으면 알 수 없음으로 표시됩니다.
- Unavailable(사용할 수 없음) - 시스템이 Secure Malware Analytics Cloud를 쿼리하여 파일의 상태를 확인하지 못했음을 나타냅니다. 이 속성을 통해 이벤트의 일부를 확인할 수 있습니다. 이는 예상된 작업입니다. "사용할 수 없음" 이벤트가 연속하여 여러 개 표시되는 경우에는 관리 주소에 대한 인터넷 연결이 정상적으로 작동하는지 확인하십시오.

사용 가능한 파일 정책

다음 파일 정책 중 하나를 선택할 수 있습니다.

- **None(**없음**)** - 전송된 파일에서 악성코드를 평가하지 않으며 파일별 차단을 수행하지 않습니다. 파일 전송을 신뢰할 수 있거나 거의 또는 전혀 수행될 가능성이 없는 규칙 또는 애플리케이션이나 URL 필터링이 네트워크를 적절하게 보호한다고 확신할 수 있는 규칙의 경우 이 옵션을 선택합니다.
- **Block Malware All(**악성코드 모두 차단**)** - 네트워크를 지나는 파일이 악성코드를 포함하는지 확인한 다음 위협이 되는 파일을 차단하기 위해 Secure Malware Analytics Cloud에 쿼리합니다.
- **Cloud Lookup All(**모두 클라우드 조회**)** - 네트워크를 지나는 파일의 전송을 허용하되 그 파일의 속성을 확인하고 로깅하기 위해 Secure Malware Analytics Cloud에 쿼리합니다.
- **(Custom File Policy(**맞춤형 파일 정책**))** - threat defense API filepolicies 리소스 및 기타 FileAndMalwarePolicies 리소스(예: filetypes, filetypecategories, ampcloudconfig, ampservers, 및 ampcloudconnections)를 사용하여 고유한 파일 정책을 생성할 수 있습니다. 정책을 생성하고 변경 사항을 구축한 후에는 device manager에서 액세스 제어 규칙을 수정할 때 정책을 선택할 수 있습니다. 정책 설명은 정책을 선택하면 해당 정책 아래에 표시됩니다.

로깅 설정

액세스 규칙의 로깅 설정에 따라 규칙과 일치하는 트래픽에 대해 연결 이벤트가 생성되는지가 결정됩니다. 이벤트 뷰어에서 규칙과 관련된 이벤트를 확인하려면 로깅을 활성화해야 합니다. 또한, 시스

템을 모니터링하는 데 사용할 수 있는 여러 대시보드에 일치하는 트래픽을 반영하려는 경우에도 로깅을 활성화해야 합니다.

조직의 보안 및 규정 준수 필요에 따라 연결을 로깅해야 합니다. 사용자가 생성하고 기능을 향상시키는 이벤트의 수를 제한하는 것이 사용자의 목표라면 사용자의 분석에 중요한 연결에 대한 로깅만 사용 설정합니다. 그러나, 자료 수집을 목적으로 사용자의 네트워크 트래픽에 대한 광범위한 견해를 원할 경우, 추가 연결에 대한 로깅을 사용 설정할 수 있습니다.

주의 DoS(서비스 거부) 공격 중에 차단된 TCP 연결을 로깅하는 경우 시스템 성능에 영향을 미칠 수 있으며, 데이터베이스가 유사한 다수의 이벤트로 가득 찰 수 있습니다. 차단 규칙에 대한 로깅을 활성화하기 전에 이 규칙이 인터넷 연결 인터페이스 또는 DoS 공격에 취약한 다른 인터페이스용인지를 고려하십시오.

다음과 같은 로깅 작업을 구성할 수 있습니다.

로그 작업 선택

다음 작업 중 하나를 선택할 수 있습니다.

- 연결 시작 및 종료 시 로깅 - 연결 시작 및 종료 시에 이벤트를 생성합니다. 연결 종료 이벤트는 연결 시작 이벤트에 포함된 모든 항목과 연결 중에 수집되었을 수 있는 모든 정보를 포함하므로 허용하는 트래픽에 대해서는 이 옵션을 선택하지 않는 것이 좋습니다. 두 이벤트를 모두 로깅하면 시스템 성능에 영향을 줄 수 있습니다. 하지만 차단된 트래픽의 경우에는 이 옵션만 사용할 수 있습니다.
- 연결 종료 시 로깅 - 연결 종료 시에 연결 로깅을 활성화하려면 이 옵션을 선택합니다. 허용되는 트래픽이나 신뢰하는 트래픽의 경우 이 옵션을 선택하는 것이 좋습니다.
- 연결 시 로깅하지 않음 - 규칙에 대해 로깅을 비활성화하려면 이 옵션을 선택합니다. 이는 기본값입니다.

참고 액세스 제어 규칙이 호출한 침입 정책이 침입을 탐지하고 침입 이벤트를 생성하면, 시스템은 규칙의 로깅 컨피그레이션에 상관없이 침입이 발생한 연결의 종료를 자동으로 로깅합니다. 침입이 차단된 연결을 위한 연결 로그 내 연결 작업은 **Block(**차단**)**입니다. 그 이유는 **Intrusion Block(**침입 차단**)**이며, 침입 탐지 수행을 위해서라면 반드시 Allow(허용) 규칙을 사용해야 합니다.

파일 이벤트

금지된 파일 또는 악성코드 이벤트 로깅을 활성화하려면 **Log Files(**로그 파일**)**를 선택합니다. 이 옵션을 구성하려면 규칙에서 파일 정책을 선택해야 합니다. 규칙에 대해 파일 정책을 선택하는 경우 기본값으로 이 옵션을 활성화합니다. 이 옵션은 활성화된 상태로 유지하는 것이 좋습니다.

시스템은 금지된 파일을 탐지하면 다음과 같은 유형의 이벤트 중 하나를 자동으로 로깅합니다.

- 파일 이벤트 - 악성코드 파일을 포함하여 탐지되거나 차단된 파일을 나타냅니다.

- 악성코드 이벤트 - 탐지되거나 차단된 악성코드 파일만 나타냅니다.
- 소급 적용되는 악성코드 이벤트 - 이전에 탐지된 파일에 대한 악성코드 상태가 변경되는 경우 생성됩니다.

파일이 차단된 경우의 연결을 위한 연결 로그 내 연결 작업은 **Block(**차단**)**입니다. 파일 또는 악성코드 탐지를 수행하려는 경우에도 Allow(허용) 규칙을 사용해야 합니다. 연결하는 이유는 파일 모니터링(파일 유형 또는 악성코드가 탐지된 경우), 악성코드 차단 또는 파일 차단(파일이 차단된 경우)입니다.

다음으로 연결 이벤트 보내기

외부 syslog 서버로 이벤트의 복사본을 전송하려는 경우 syslog 서버를 정의하는 서비스 개체를 선택합니다. 필요한 개체가 아직 없으면 **Create New Syslog Server(**새 **Syslog** 서버 생성**)**를 클릭하여 개체를 생성합니다. syslog 서버에 대한 로깅을 비활성화하려면 서버 목록에서 **Any(**모두**)**를 선택합니다.

디바이스의 이벤트 스토리지는 제한되어 있으므로 외부 syslog 서버로 이벤트를 전송하면 더 장기적으로 저장할 수 있으며 이벤트 분석 성능이 개선됩니다.

이 설정은 연결 이벤트에만 적용됩니다. Syslog에 침입 이벤트를 전송하려면 침입 정책 설정에서 서버를 컨피그레이션하십시오. syslog에 파일/악성코드 이벤트를 전송하려면 **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Logging Settings(**기록 설정**)**에서 서버를 컨피그레이션하십시오.

액세스 제어 정책 모니터링

다음 주제에서는 액세스 제어 정책을 모니터링하는 방법에 대해 설명합니다.

대시보드에서 액세스 제어 통계 모니터링

모니터링 대시보드에 있는 대부분의 데이터는 액세스 제어 정책과 직접적으로 관련되어 있습니다. 트래픽 및 시스템 대시보드 모니터링, 113 페이지의 내용을 참조하십시오.

- **Monitoring(**모니터링**)** > **Access And SI Rules(**액세스 및 **SI** 규칙**)**에는 가장 많이 적중한 액세스 규칙, 보안 인텔리전스 규칙에 상응하는 규칙 및 관련 통계가 표시됩니다.
- 일반적인 통계는 **Network Overview(**네트워크 개요**)**, **Destinations(**대상**)**, **Zones(**영역**)**, 대시보드에서 확인할 수 있습니다.
- URL 필터링 결과는 **URL Categories(URL** 카테고리**)** 및 **Destinations(**대상**)** 대시보드에서 확인할 수 있습니다. **URL Categories(URL** 카테고리**)** 대시보드에서 정보를 확인하려면 하나 이상의 URL 필터링 정책이 있어야 합니다.
- 애플리케이션 필터링 결과는 **Applications(**애플리케이션**)** 및 **Web Applications(**웹 애플리케이션**)** 대시보드에서 확인할 수 있습니다.
- 사용자 기반 통계는 **Users(**사용자**)** 대시보드에서 확인할 수 있습니다. 사용자 정보를 수집하려면 ID 정책을 구현해야 합니다.

- 침입 정책 통계는 **Attackers(**공격자**)** 및 **Targets(**대상**)** 대시보드에서 확인할 수 있습니다. 이러한 대시보드에서 정보를 확인하려면 하나 이상의 액세스 제어 규칙에 침입 정책을 적용해야 합니다.
- 파일 정책 및 악성코드 필터링 통계는 **File Logs(**파일 로그**)** 및 **Malware(**악성코드**)** 대시보드에서 확인할 수 있습니다. 이러한 대시보드에서 정보를 확인하려면 하나 이상의 액세스 제어 규칙에 파일 정책을 적용해야 합니다.
- **Monitoring(**모니터링**)** > **Events(**이벤트**)**에는 액세스 제어 규칙과 관련된 데이터 및 연결에 대한 이벤트도 표시됩니다.

규칙 적중 횟수 검토

각 액세스 제어 규칙에 대한 적중 횟수를 볼 수 있습니다. 적중 횟수는 연결이 규칙과 얼마나 자주 일치했는지 나타냅니다. 이 정보를 사용해 가장 많이 활성화된 규칙과 덜 활성화된 규칙을 식별할 수 있습니다.

리부팅 및 업그레이드 시에도 개수가 유지됩니다.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)**을 선택합니다.

단계 **2** **Toggle Hit Counts(**적중 횟수 토글**)** 아이콘( )을 클릭합니다.

적중 횟수 열은 규칙에 대한 총 적중 횟수와 최종 적중 날짜 및 시간과 함께 이름 열의 오른쪽에 표시됩니다. 적중 횟수 정보는 토글 버튼을 클릭하면 가져올 수 있습니다.

적중 횟수 정보로 할 수 있는 작업은 다음과 같습니다.

- 버튼 왼쪽에 적중 횟수가 마지막으로 업데이트된 시각에 관한 정보가 표시됩니다. 최신 횟수를 얻으려면 **refresh(**새로고침**)** 아이콘( )을 클릭하십시오.
- 특정 규칙에 대한 적중 횟수 자세히 보기를 열려면 테이블에 있는 적중 횟수 번호를 클릭하여 적중 횟수 대화 상자를 여십시오. 적중 횟수 정보에는 적중 횟수와 규칙과 일치한 마지막 연결의 날짜 및 시간이 포함됩니다. 카운터를 0으로 재설정하려면 **Reset(**재설정**)** 링크를 클릭하십시오.

  한 번에 모든 규칙에 대한 적중 횟수를 재설정하려면 디바이스에 대한 SSH 세션을 열고 **clear rule hits** 명령을 실행하십시오.
- 테이블에서 적중 횟수 열을 제거하려면 **Toggle Hit Counts(**적중 횟수 토글**)** 아이콘( )을 다시 클릭합니다.

액세스 제어에 대한 **Syslog** 메시지 모니터링

이벤트 뷰어에서 이벤트를 확인하는 것 외에도 액세스 제어 규칙, 침입 정책, 파일/악성코드 정책 및 보안 인텔리전스 정책을 컨피그레이션하여 syslog 서버로 이벤트를 전송할 수 있습니다. 이벤트에서는 다음 메시지 ID를 사용합니다.

- 430001 — 침입 이벤트
- 430002 — 연결 시작 시 기록된 연결 이벤트
- 430003 — 연결 종료 시 기록된 연결 이벤트
- 430004 — 파일 이벤트
- 430005 — 악성코드 이벤트

CLI에서 액세스 제어 정책 모니터링

CLI 콘솔을 열거나 디바이스 CLI에 로그인한 후에 다음 명령을 사용하여 액세스 제어 정책과 통계에 대한 상세 정보를 가져올 수도 있습니다.

- **show access-control-config** 액세스 제어 규칙에 대한 요약 정보를 규칙별 적중 횟수와 함께 표시합니다.
- **show access-list** 액세스 제어 규칙에서 생성된 ACL(Access Control Lists)을 표시합니다. ACL은 초기 필터를 제공하며 가능한 경우 항상 빠른 결정 제공을 시도하므로, 삭제해야 하는 연결을 검사할 필요가 없어 리소스가 불필요하게 사용되지 않습니다. 이 정보에는 적중 횟수가 포함됩니다.
- **show rule hits**에서는 **show access-control-config** 및 **show access-list**와 함께 표시된 횟수보다 더 정확한 통합 적중 횟수를 표시합니다. 적중 횟수를 재설정하려는 경우, **clear rule hits** 명령을 사용하십시오.
- **show snort statistics** 기본 검사기인 Snort 검사 엔진에 대한 정보를 표시합니다. Snort는 애플리케이션 필터링, URL 필터링, 침입 차단, 파일 및 악성코드 필터링을 구현합니다.
- **show conn** 인터페이스를 통해 현재 설정되어 있는 연결에 대한 정보를 표시합니다.
- **show traffic** 각 인터페이스를 통과하는 트래픽에 대한 통계를 표시합니다.
- **show ipv6 traffic** 디바이스를 통과하는 IPv6 트래픽에 대한 통계를 표시합니다.

액세스 제어의 예시

사용 사례 장에는 액세스 제어 규칙을 구현하는 몇 가지 예시가 포함되어 있습니다. 다음 예시를 참조하십시오.

- 네트워크 트래픽을 파악하는 방법, 49 페이지. 이 예시는 전반적인 연결 및 사용자 정보 수집을 위한 몇 가지 기본적인 개념을 보여줍니다.

- 위협을 차단하는 방법, 57 페이지. 이 예시는 침입 정책을 적용하는 방법을 보여줍니다.
- 악성코드를 차단하는 방법, 62 페이지. 이 예시는 파일 정책을 적용하는 방법을 보여줍니다.
- 사용 제한 정책(URL 필터링)을 구현하는 방법, 65 페이지. 이 예시는 URL 필터링을 수행하는 방법을 보여줍니다.
- 애플리케이션 사용량을 제어하는 방법, 70 페이지. 이 예시는 애플리케이션 필터링을 수행하는 방법을 보여줍니다.
- 서브넷을 추가하는 방법, 74 페이지. 이 예시는 트래픽 플로우를 허용하는 데 필요한 액세스 규칙을 비롯하여 전체 네트워크에 새 서브넷을 통합하는 방법을 보여줍니다.
- 네트워크에서 트래픽을 능동적으로 모니터링하는 방법, 79 페이지

추가 예는 다음과 같습니다.

TrustSec SGT(Security Group Tag)를 사용하여 네트워크 액세스를 제어하는 방법

Cisco ISE(Identity Services Engine)를 사용하여 Cisco TrustSec 네트워크에서 트래픽을 분류하기 위해 SGT(Security Group Tag)를 정의하고 사용하는 경우, SGT를 일치 기준으로 사용하는 액세스 제어 규칙을 작성할 수 있습니다. 따라서 IP 주소가 아니라 보안 그룹 멤버십을 기준으로 직접 액세스를 차단하거나 허용할 수 있습니다.

SGT(Security Group Tag) 정보

Cisco ISE(Identity Services Engine)에서는 SGT(Security Group Tag)를 생성하고 각 태그에 호스트 또는 네트워크 IP 주소를 할당할 수 있습니다. 또한 사용자 어카운트에 SGT를 할당할 수 있으며, SGT는 사용자의 트래픽에 할당됩니다. 네트워크의 스위치와 라우터가 이 작업을 수행하도록 구성된 경우, 이러한 태그는 ISE, Cisco TrustSec 클라우드로 제어되는 네트워크에 진입할 때 패킷에 할당됩니다.

device manager에서 ISE ID 소스를 구성하면 threat defense 시스템에서는 ISE에서 SGT 목록을 자동으로 다운로드합니다. 그러면 액세스 제어 규칙에서 SGT를 트래픽 일치 조건으로 사용할 수 있습니다.

예를 들어, 프로덕션 사용자 태그를 생성하고 192.168.7.0/24 네트워크를 태그에 연결할 수 있습니다. 이는 노트북 컴퓨터, Wi-Fi 클라이언트 등의 사용자 엔드포인트에 해당 네트워크를 사용하는 경우에 적합합니다. 프로덕션 서버에 대한 별도의 태그를 생성하고 관련 서버 또는 서브넷의 IP 주소를 태그에 할당할 수 있습니다. 그런 다음에는, threat defense에서 태그를 기반으로 사용자 네트워크에서 프로덕션 서버로의 액세스를 허용하거나 차단할 수 있습니다. 나중에 ISE의 태그와 연결된 호스트 또는 네트워크 주소를 변경하는 경우에는 threat defense 디바이스에 대해 정의된 액세스 제어 규칙을 변경할 필요가 없습니다.

threat defense에서는 SGT를 액세스 제어 규칙에 대한 트래픽 일치 기준으로 평가하는 경우, 다음 우선순위를 사용합니다.

1. 패킷에 정의된 소스 SGT 태그(있는 경우). SGT 태그를 패킷에 포함하려면 네트워크의 스위치와 라우터를 추가하도록 구성해야 합니다. 이 메서드를 구현하는 방법에 대한 자세한 내용은 ISE 설명서를 참조하십시오.

2. ISE 세션 디렉토리에서 다운로드된 대로 사용자 세션에 할당된 SGT. 이러한 유형의 SGT 일치에 대한 세션 디렉토리 정보를 수신 대기하려면 해당 옵션을 활성화해야 합니다. 그러나 이 옵션은 처음에 ISE ID 소스를 생성할 때 기본적으로 켜집니다. SGT는 소스 또는 대상과 일치할 수 있습니다. 필수 사항은 아니지만 일반적으로 사용자 ID 정보를 수집하기 위해 AD 영역과 함께 ISE ID 소스를 사용하여 패시브 인증 ID 규칙도 설정합니다.

3. SXP를 사용하여 다운로드한 SGT-IP 주소 매핑. IP 주소가 SGT 범위 내에 있는 경우 트래픽은 SGT를 사용하는 액세스 제어 규칙과 일치합니다. SGT는 소스 또는 대상과 일치할 수 있습니다.

   ISE에서는 SXP(Security-group eXchange Protocol)를 사용하여 IP-SGT 매핑 데이터베이스를 네트워크 디바이스에 전파합니다. ISE 서버를 사용하도록 threat defense 디바이스를 구성하는 경우 ISE에서 SXP 항목을 수신 대기하려면 해당 옵션을 켜야 합니다. 따라서 threat defense 디바이스에서는 ISE에서 바로 SGT(Security Group Tag) 및 매핑에 대해 학습하며, ISE에서 업데이트된 SGT(Security Group Tag) 및 매핑을 게시할 때마다 알림을 받습니다. 이렇게 하면 SGT(Security Group Tag) 및 매핑 목록이 디바이스에서 최신 상태로 유지되므로 threat defense에서 ISE에 정의된 정책을 효과적으로 적용할 수 있습니다.

SGT(Security Group Tag)를 기반으로 액세스 제어 구성

SGT(Security Group Tag)를 일치 기준으로 사용하는 액세스 제어 규칙을 구성하려면 먼저 ISE 서버에서 SGT 매핑을 가져오도록 디바이스를 구성해야 합니다.

다음 절차에서는 SXP를 통해 게시된 SGT-IP 주소 매핑을 비롯하여 ISE에 정의되어 있는 모든 매핑을 가져오려고 한다는 가정 하에 엔드 투 엔드 프로세스에 대해 설명합니다. 다른 방법은 다음과 같습니다.

- 패킷에서만 SGT 정보를 사용하고 ISE에서 다운로드한 매핑을 사용하지 않으려면 SGT 그룹 동적 개체를 간단하게 생성하여 액세스 제어 규칙에서 소스 SGT 기준으로 사용하면 됩니다. 이 경우에는 SGT 태그를 소스 조건으로만 사용할 수 있으며 이러한 태그는 대상 기준과 일치하지 않습니다.
- 패킷에 있는 SGT를 사용자 세션 SGT 매핑하고만 사용하려는 경우 ISE ID 소스의 SXP 항목을 구독하도록 옵션을 설정할 필요가 없으며 SXP 매핑을 게시하도록 ISE를 구성할 필요도 없습니다. 소스 및 대상 일치 조건 둘 다에 이 정보를 사용할 수 있습니다.

시작하기 전에

이 섹션에서는 네트워크에서 이미 Cisco TrustSec을 구성했으며 단순하게 정책 적용 시점으로 threat defense 디바이스를 추가하는 것으로 가정합니다. Cisco TrustSec을 구축하지 않은 경우 ISE로 시작하여 네트워크를 구성한 다음, 이 절차로 돌아오십시오. Cisco TrustSec에 대한 설명은 이 문서에 포함되어 있지 않습니다.

프로시저

단계 **1** SGT가 정의되었는지, ISE가 SXP 주제를 게시하도록 올바르게 구성되었는지, 필요한 정적 매핑이 있는지 확인합니다.

ISE에서 보안 그룹 및 SXP 게시 구성, 549 페이지의 내용을 참조하십시오.

단계 **2** SXP 주제를 수신하도록 Identity Services Engine 개체를 업데이트합니다.

ISE를 사용하여 사용자 세션 SGT 매핑, SXP를 통한 정적 SGT-IP 주소 매핑 또는 둘 다를 가져올 수 있습니다. 기본적으로 ISE ID 소스를 구성하면 사용자 세션 매핑만 가져오게 됩니다. ISE에서 SXP 항목을 수신 대기하려면 해당 옵션을 켜야 합니다.

a) **Objects(**개체**)** > **Identity Sources(ID** 소스**)**를 선택합니다.
b) ISE 개체를 수정합니다. 아직 이를 구성하지 않은 경우 **+** > **Identity Services Engine**을 클릭하여 ISE(Identity Services Engine) 구성, 187 페이지를 확인합니다.
c) **Subscribe To(**구독 대상**)**에서 **SXP Topic(SXP** 주제**)**을 선택합니다.

패시브 인증을 사용하거나 user-to-SGT 매핑을 원하는 경우 **Session Directory Topic(**세션 디렉토리 주제**)**도 선택했는지 확인합니다.

d) **OK(**확인**)**를 클릭합니다.

단계 **3** 변경 사항을 구축하고 시스템이 ISE에서 태그 및 매핑을 다운로드할 때까지 기다립니다.

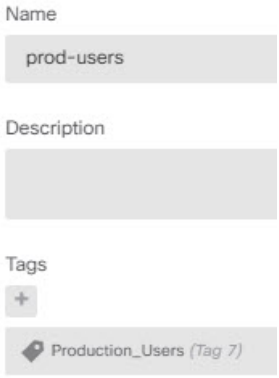
ISE ID 소스를 구성하고 변경 사항을 구축하고 나면 시스템에서는 ISE 서버에서 SGT(Security Group Tag) 정보를 검색합니다. 변경 사항을 구축할 때까지는 다운로드가 수행되지 않습니다.

단계 **4** 액세스 제어 규칙에 필요한 SGT 그룹 개체를 생성합니다.

ISE에서 검색된 정보는 액세스 제어 규칙에서 바로 사용할 수 없습니다. 대신, 다운로드한 SGT 정보를 참조하는 SGT 그룹을 생성해야 합니다. SGT 그룹에서는 둘 이상의 SGT를 참조할 수 있으므로 적절한 경우 관련된 태그 컬렉션을 기준으로 정책을 적용할 수 있습니다.

개체의 수와 내용은 작성하려는 액세스 제어 규칙에 따라 달라집니다. 필요한 모든 개체를 생성하려면 다음 프로세스를 반복합니다.

a) **Objects(**개체**)** > **SGT Group(SGT** 그룹**)**을 선택합니다.
b) **+**를 클릭하여 새 개체를 추가하거나 기존 개체를 수정합니다.
c) 새 개체의 이름을 입력하고 필요한 경우 설명을 입력합니다.
d) **Tags(**태그**)**에서 **+**를 클릭하고 그룹에 포함해야 하는 모든 태그를 선택합니다.



e) **OK(**확인**)**를 클릭합니다.

단계 **5** SGT 그룹 개체를 사용하는 액세스 제어 규칙을 생성합니다.

예를 들면, 아래의 규칙에서는 프로덕션 사용자에게서 프로덕션 서버로 향하는 트래픽을 허용합니다. 이 규칙은 전적으로 SGT에 달려 있으며, 소스/대상 인터페이스 또는 기타 기준으로 제한되지 않습니다. 따라서 규칙은 서로 다른 인터페이스에서 오는 경우 및 ISE에서 보안 그룹 멤버십을 변경하는 경우 트래픽에 동적으로 적용됩니다. 패킷에 소스 SGT가 명시적으로 포함되지 않은 경우, 소스/대상 일치는 사용자 세션 정보 또는 SXP에서 게시된 매핑에서 가져온 SGT-IP 주소 매핑과 비교하여 패킷 IP 주소를 기반으로 합니다.

a) **Policies(**정책**)** > **Access Control(**액세스 제어**)**을 선택합니다.
b) 새 규칙을 생성하거나 기존 규칙을 수정하려면 +를 클릭합니다.
c) 규칙 이름을 입력하고 작업으로 **Allow(**허용**)**를 선택합니다.
d) **Source/Destination(**소스/대상**)** 탭에서 **Source(**소스**)** > **SGT Groups(SGT** 그룹**)**아래에서 +를 클릭하고 프로덕션 사용자 용으로 생성한 개체를 선택합니다.
e) **Source/Destination(**소스/대상**)** 탭의 **Destination(**대상**)** > **SGT Groups(SGT** 그룹**)**아래에서 +를 클릭하고 프로덕션 서버용으로 생성한 개체를 선택합니다.
f) 필요에 따라 다른 옵션을 구성합니다. 예를 들어 로깅을 활성화하고 침입 정책을 적용할 수 있습니다.
g) **OK(**확인**)**를 클릭합니다.

단계 **6** 컨피그레이션을 구축합니다.

ISE에서 보안 그룹 및 SXP 게시 구성

TrustSec 정책 및 SGT(Security Group Tag)를 생성하려면 Cisco ISE(Identity Services Engine)에서 수행해야 할 구성이 많이 있습니다. TrustSec을 구현하는 방법에 대한 더 자세한 내용은 ISE 설명서를 참조하십시오.

다음 절차에서는 ISE에서 threat defense 디바이스에 대해 구성해야 하는 핵심 설정의 중요 사항을 골라서 설명하므로 이를 따라 정적 SGT-IP 주소 매핑을 다운로드하고 적용할 수 있습니다. 그러면 이 매핑을 액세스 제어 규칙에서 소스 및 대상 SGT 일치에 사용할 수 있습니다. 자세한 내용은 ISE 설명서를 참조하십시오.

이 절차의 스크린 샷은 ISE 2.4를 기준으로 합니다. 이러한 기능에 대한 정확한 경로는 이후 릴리스에서 변경될 수 있지만 개념 및 요구 사항은 동일합니다. ISE 2.4 이상 및 2.6 이상 버전이 권장되더라도 구성은 ISE 2.2 패치 1부터 작동해야 합니다.

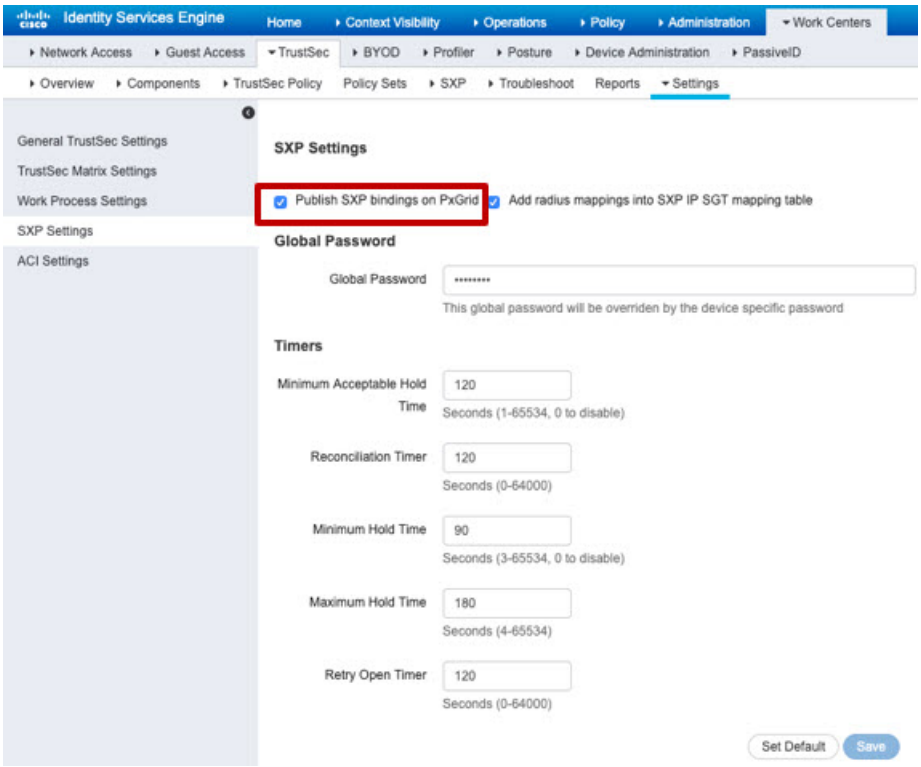
시작하기 전에

SGT-IP 주소 정적 매핑을 게시하고, 사용자 세션-SGT 매핑을 가져와 threat defense 디바이스가 이를 수신할 수 있도록 하려면 ISE Plus 라이선스가 있어야 합니다.

프로시저

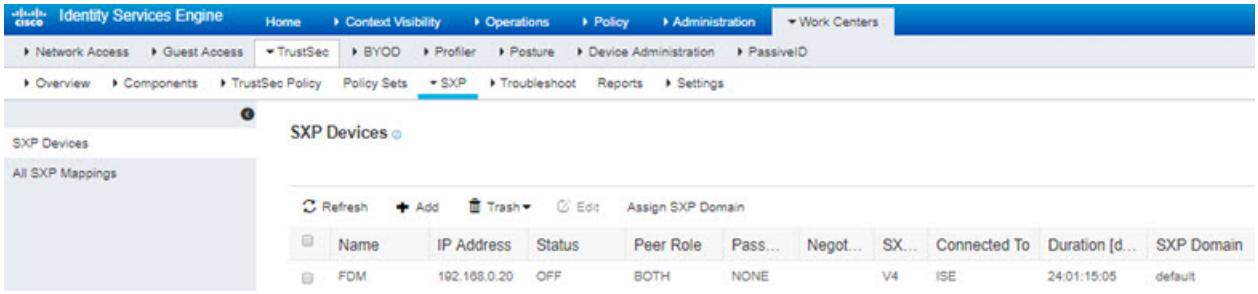
단계 **1** **Work Center(**작업 센터**)** > **TrustSec** > **Settings(**설정**)** > **SXP Settings(SXP** 설정**)**를 선택하고 **Publish SXP Bindings on PxGrid(PxGrid**에서 **SXP** 바인딩 게시**)** 옵션을 선택합니다.

이 옵션을 선택하면 ISE에서 SXP를 사용하여 SGT 매핑을 전송합니다. threat defense 디바이스에서 SXP 항목에 대한 목록의 내용을 "수신 대기"하도록 설정하려면 이 옵션을 선택해야 합니다. 정적 SGT-IP 주소 매핑에 대한 정보를 가져오려면 threat defense 디바이스에 대해 이 옵션을 선택해야 합니다. 단순히 패킷에 정의된 SGT 태그 또는 사용자 세션에 할당된 SGT를 사용하려는 경우에는 이 옵션이 필수 사항이 아닙니다.

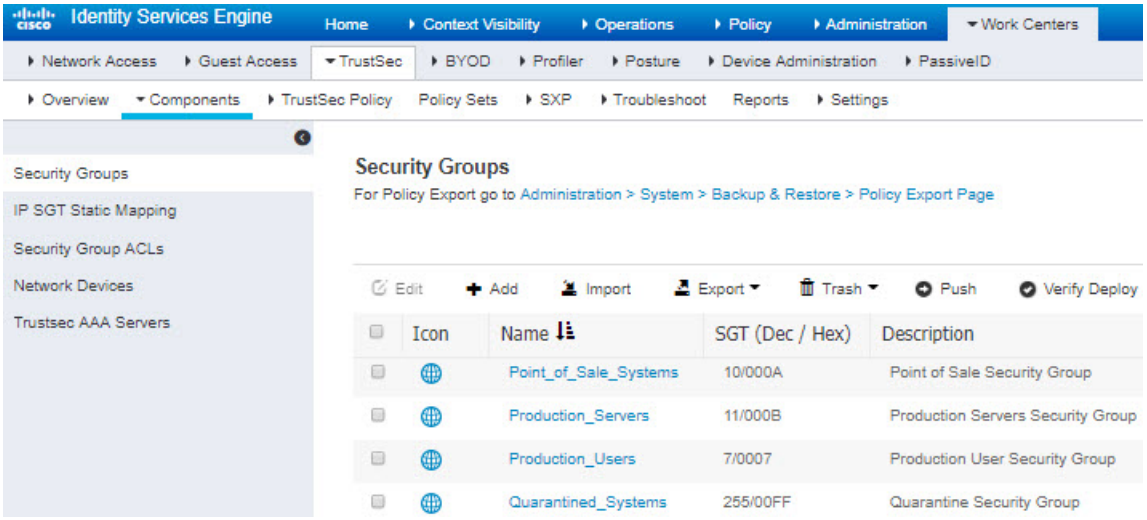


단계 **2** **Work Centers(**작업 센터**)** > **TrustSec** > **SXP** > **SXP Devices(SXP** 디바이스**)**를 선택하고 디바이스를 추가합니다.

이 디바이스가 실제 디바이스일 필요는 없으며, threat defense 디바이스의 관리 IP 주소를 사용할 수도 있습니다. 이 표에는 ISE에서 정적 SGT-IP 주소 매핑을 게시하도록 유도하는 디바이스가 하나 이상 필요합니다. 단순히 패킷에 정의된 SGT 태그 또는 사용자 세션에 할당된 SGT를 사용하려는 경우에는 이 단계가 필수 사항이 아닙니다.

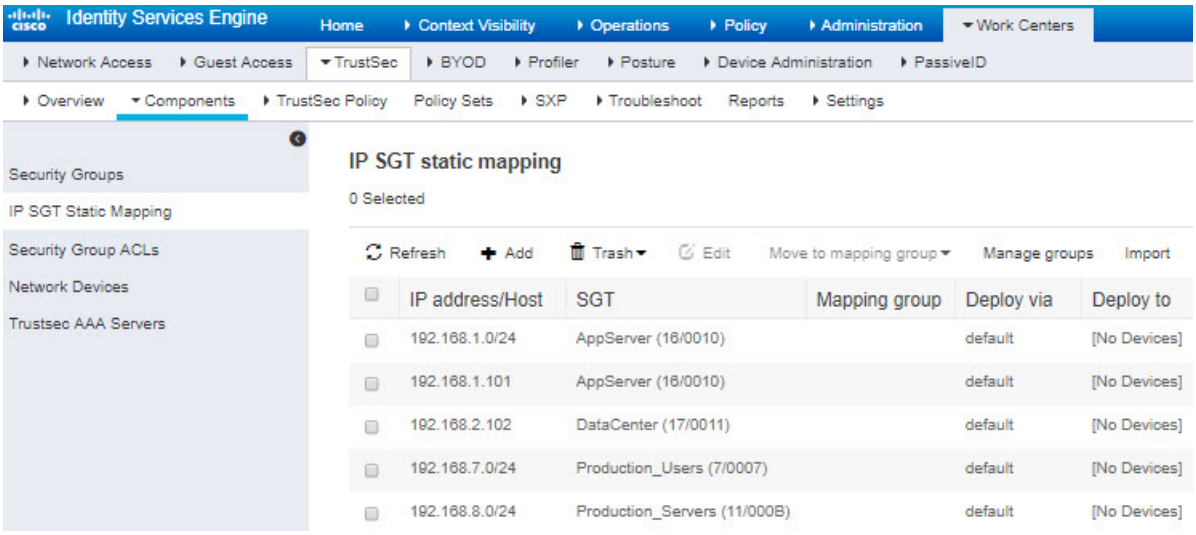


단계 **3** **Work Centers(**작업 센터**)** > **TrustSec** > **Components(**구성 요소**)** > **Security Groups(**보안 그룹**)**를 선택하고 SGT(Security Group Tag)가 정의되어 있는지 확인합니다. 필요에 따라 새로 생성합니다.



단계 **4** **Work Centers(**작업 센터**)** > **TrustSec** > **Components(**구성 요소**)** > **IPSGT Static Mapping(IPSGT** 정적 매핑**)**을 선택하고 호스트 및 네트워크 IP 주소를 SGT(Security Group Tag)에 매핑합니다.

단순히 패킷에 정의된 SGT 태그 또는 사용자 세션에 할당된 SGT를 사용하려는 경우에는 이 단계가 필수 사항이 아닙니다.


Identity Services Engine
Home
Context Visibility
Operations
Policy
Administration
Work Centers
Network Access
Guest Access
TrustSec
BYOD
Profiler
Posture
Device Administration
PassiveID
Overview
Components
TrustSec Policy
Policy Sets
SXP
Troubleshoot
Reports
Settings
Security Groups
IP SGT Static Mapping
Security Group ACLs
Network Devices
Trustsec AAA Servers
IP SGT static mapping
0 Selected
Refresh
Add
Trash
Edit
Move to mapping group
Manage groups
Import
IP address/Host
SGT
Mapping group
Deploy via
Deploy to
192.168.1.0/24
AppServer (16/0010)
default
[No Devices]
192.168.1.101
AppServer (16/0010)
default
[No Devices]
192.168.2.102
DataCenter (17/0011)
default
[No Devices]
192.168.7.0/24
Production_Users (7/0007)
default
[No Devices]
192.168.8.0/24
Production_Servers (11/000B)
default
[No Devices]

22 장

침입 정책

다음 주제에서는 침입 정책 및 밀접하게 연관된 NAP(네트워크 분석 정책)에 대해 설명합니다. 침입 정책에는 위협에 대한 트래픽을 확인하고 공격으로 표시되는 트래픽을 차단하는 규칙이 포함됩니다. 네트워크 분석 정책은 트래픽을 정규화하고 프로토콜 이상 징후를 확인하여 트래픽의 추가 검사를 준비하는 트래픽 전처리를 제어합니다.

전처리 및 침입 검사는 매우 밀접하게 연관되어 있기 때문에, 단일 패킷을 검사하는 네트워크 분석 및 침입 정책은 반드시 서로 보완해야 합니다.

침입 및 네트워크 분석 정책 정보

네트워크 분석 및 침입 정책은 침입 위협을 탐지 및 방지하기 위해 함께 작동합니다.

- NAP(네트워크 분석 정책)는 트래픽을 디코딩하고 전처리하는 방법을 제어합니다. 이 정책의 목적은 향후 평가를 위함이며, 특히 침입 시도의 신호가 될 수 있는 변칙 트래픽의 경우 유효합니다.
- 침입 정책은 침입 및 전처리 규칙(침입 규칙으로 총칭함)을 사용하여 패턴 기반의 공격에 대한 디코딩된 패킷을 검사합니다. 규칙은 위협 트래픽을 방지(삭제)하고 이벤트를 생성하거나, 단순히 이를 탐지(알림)만 하고 이벤트를 생성할 수 있습니다.

시스템이 트래픽을 분석하기 때문에, 네트워크 분석 디코딩 및 전처리 단계는 침입 방지 단계보다 이전에 또는 별도로 발생합니다. 네트워크 분석 및 침입 정책은 폭넓고 심층적인 패킷 검사를 제공합니

다. 이 둘을 함께 사용하면 호스트 및 호스트 데이터의 가용성, 무결성 및 기밀성을 위협할 수 있는 네트워크 트래픽을 탐지하고 알리고 방지할 수 있습니다.

시스템 정의 네트워크 분석 및 침입 정책

시스템에는 상호 보완하고 함께 작동하는 동일한 이름의 네트워크 분석 및 침입 정책 쌍이 여러 개 포함되어 있습니다. 예를 들어, "Balanced Security and Connectivity(보안과 연결의 균형 유지)"라는 이름으로 NAP 및 침입 정책이 모두 있으며 이 두 정책은 함께 사용해야 합니다. 시스템 제공 정책은 Cisco Talos Intelligence Group(Talos)에서 구성합니다. Talos에서는 이러한 정책에 대해 침입 및 전처리기 규칙 상태를 설정하고 전처리기 및 다른 고급 설정에 대한 초기 구성을 제공합니다.

새로운 취약성이 알려지면 Talos에서 침입 규칙 업데이트를 릴리스합니다. 이 규칙 업데이트는 모든 시스템 제공 네트워크 분석 또는 침입 정책을 수정할 수 있고 새롭게 업데이트된 침입 규칙 및 전처리기 규칙, 기존 규칙을 위한 수정된 상태, 그리고 수정된 기본 정책 설정을 제공할 수 있습니다. 규칙 업데이트는 또한 시스템 제공 정책에서 규칙을 삭제할 수 있고, 새로운 규칙 카테고리를 제공할 수 있으며, 기본 변수 집합을 수정할 수 있습니다.

규칙 데이터베이스를 수동으로 업데이트하거나 정기 업데이트 일정을 구성할 수 있습니다. 업데이트를 적용하려면 업데이트를 구축해야 합니다. 시스템 데이터베이스 업데이트에 대한 자세한 내용은 시스템 데이터베이스 업데이트, 857 페이지를 참조하십시오.

시스템 제공 정책은 다음과 같습니다.

Balanced Security and Connectivity(보안과 연결의 균형 유지**)** 네트워크 분석 및 침입 정책

이 정책은 속도 및 탐지 모두에 구축됩니다. 두 정책을 함께 사용하는 것은 대부분의 네트워크 및 구축 유형에 대해 좋은 시작점이 됩니다. 시스템에서는 Balanced Security and Connectivity(보안과 연결의 균형 유지) 네트워크 분석 정책을 기본값으로 사용합니다.

Connectivity Over Security(연결이 보안에 우선함**)** 네트워크 분석 및 침입 정책

이러한 정책은 연결(모든 리소스에 접근할 수 있는 기능)이 네트워크 인프라 보안보다 우선하는 네트워크에 구축됩니다. 침입 정책은 Security Over Connectivity(보안이 연결에 우선함)에서 활성화된 것보다 훨씬 더 적은 규칙을 활성화합니다. 트래픽을 차단하는 가장 중요한 규칙만 사용 설정됩니다.

Security Over Connectivity(보안이 연결에 우선함**)** 네트워크 분석 및 침입 정책

이러한 정책은 네트워크 인프라 보안이 사용자 편의보다 우선하는 네트워크에 구축됩니다. 침입 정책은 적합한 트래픽에 대해 경계하거나 중단할 수 있는 다양한 네트워크 이상 침입 규칙을 활성화합니다.

Maximum Detection(최대 탐지**)** 네트워크 분석 및 침입 정책

이러한 정책은 Security over Connectivity(연결보다 보안 우선) 정책에서보다 네트워크 인프라 보안이 강조되는 네트워크에 구축되며, 운영에 더 큰 영향을 미칠 수 있습니다. 예를 들어 이 침입 정책에서는 악성코드, 익스플로잇 킷, 오래된 일반적인 취약점, 통제되지 않은 알려진 익스플로잇 등 다수의 위협 범주에서 규칙을 활성화합니다.

검사 모드: 방지 및 탐지

기본적으로 모든 침입 정책은 Prevention(차단) 모드에서 작동하여 IPS(침입 방지 시스템)를 구현합니다. Prevention(차단) 검사 모드에서 연결이 트래픽을 삭제하는 작업을 수행하는 침입 규칙과 일치하는 경우 연결이 능동적으로 차단됩니다.

대신 네트워크에서 침입 정책의 영향을 테스트하려는 경우, 모드를 IDS(침입 탐지 시스템)를 구현하는 모드를 Detection(탐지)로 변경할 수 있습니다. 이 검사 모드에서 삭제 규칙은 일치하는 연결에 대한 알림을 받는 알림 규칙처럼 처리되지만, 작업 결과는 Would Have Blocked(차단되었을 수 있음)가 되고 연결은 실제로 차단되지 않습니다.

침입 정책에 따라 검사 모드를 변경하면 차단 및 탐지를 혼합하여 사용할 수 있습니다.

Snort 3 네트워크 분석 정책(NAP)에도 검사 모드가 있습니다. 침입 정책과 달리 NAP 정책은 전역 정책이므로 모든 NAP 처리를 방지 또는 탐지 모드에서 실행해야 합니다. 침입 정책에 사용하는 것과 동일한 모드를 사용해야 합니다. 방지 및 탐지 정책이 혼합된 경우 가장 제한적인 침입 정책과 일치하도록 Prevention(방지)을 선택합니다.

침입 및 전처리기 규칙

침입 규칙은 시스템이 네트워크에서 취약점을 익스플로잇하려는 시도를 탐지하는 데 사용하는 키워드와 인수의 지정된 집합입니다. 시스템에서 네트워크 트래픽을 분석하면서 각 규칙에 지정된 조건과 패킷을 비교하고 데이터 패킷이 규칙에 지정된 모든 조건을 충족하는 경우 규칙을 트리거합니다.

시스템에는 Cisco Talos Intelligence Group(Talos)가 생성한 다음 유형의 규칙이 포함됩니다.

- 침입 규칙(공유 개체 규칙 및 표준 텍스트 규칙으로 세분화됨)
- 전처리기 규칙(네트워크 분석 정책에서 전처리기 및 패킷 디코더 탐지 옵션과 관련된 규칙). 대부분의 전처리기 규칙은 기본적으로 비활성화되어 있습니다.

다음 주제에서는 침입 규칙에 대해 자세히 설명합니다.

침입 규칙 특성

침입 정책을 확인하면 위협을 식별하는 데 사용할 수 있는 모든 침입 규칙 목록이 표시됩니다.

각 정책에 대한 규칙 목록은 동일합니다. 차이점은 각 규칙에 대해 구성된 작업에 있습니다. 30,000개 이상의 규칙이 있으므로, 목록을 스크롤하는 데 시간이 걸립니다. 목록을 스크롤하면 규칙이 표시됩니다.

다음은 각 규칙을 정의하는 특성입니다.

> (서명 설명)

왼쪽 열의 > 버튼을 클릭하여 서명 설명을 엽니다. 설명은 트래픽을 규칙과 일치시키기 위해 Snort 검사 엔진에서 사용하는 실제 코드입니다. 코드에 대한 설명은 이 문서의 범위를 벗어나지만 *Management Center* 컨피그레이션 가이드에는 자세히 설명되어 있습니다. http://www.cisco.com/c/en/us/support/security/defense-center/products-installation-and-configuration-guides-list.html에서 해당하는 소프트웨어 버전의 문서를 선택하십시오. 침입 규칙 수정에 대한 정보를 찾아봅니다.

서명에는 특정 항목에 대한 변수가 포함됩니다. 자세한 내용은 기본 침입 변수 집합, 556 페이지를 참고하십시오.

GID

생성기 식별자(ID). 이 번호는 어떤 시스템 구성 요소가 규칙을 평가하고 이벤트를 생성하는지 나타냅니다. 1은 표준 텍스트 침입 규칙을 나타내고, 3은 공유 개체 침입 규칙을 나타냅니다. (이러한 규칙 유형의 차이점은 device manager 사용자에게 크게 중요하지 않습니다.) 이러한 규칙은 침입 정책을 구성할 때 관심을 가져야 할 주요 규칙입니다. 기타 GID에 대한 자세한 내용은 생성기 식별자, 557 페이지를 참조하십시오.

SID

SID(Snort 식별자)는 서명 ID라고도 합니다. 1000000보다 낮은 Snort ID는 Cisco Talos Intelligence Group(Talos)에서 생성했습니다.

Action(작업)

선택한 침입 정책에 있는 이 규칙의 상태입니다. 규칙마다 "(Default(기본값))"가 작업에 추가되며, 이는 이 정책에 있는 규칙의 기본 작업입니다. 기본 설정으로 규칙을 되돌리려면 이 작업을 선택합니다. 가능한 작업은 다음과 같습니다.

- **Alert(알림)** — 이 규칙이 트래픽과 일치할 경우 이벤트를 생성하지만 연결을 삭제하지는 않습니다.
- **Drop(삭제)** — 이 규칙이 트래픽과 일치할 경우 이벤트를 생성하고 연결도 삭제합니다.
- **Disabled(비활성화됨)** — 트래픽을 이 규칙과 일치시키지 않습니다. 아무런 이벤트도 생성되지 않습니다.

Status(상태)

Snort 2 규칙의 경우 상태는 별도의 열에 표시됩니다. 규칙에 대한 기본 작업을 변경할 경우, 이 열에 "Overridden(재정의됨)"이 표시됩니다. 그렇지 않을 경우, 열이 비어 있습니다.

Snort 3 규칙의 경우 "Overridden(재정의됨)" 상태를 변경했으면 Action 특성의 맨 아래에 표시됩니다.

Message(메시지)

이는 규칙의 이름이며, 해당 규칙으로 트리거된 이벤트에도 표시됩니다. 메시지는 일반적으로 서명이 일치하는 위협을 식별합니다. 각 위협에 대한 자세한 내용은 인터넷을 검색하여 참조할 수 있습니다.

기본 침입 변수 집합

침입 규칙 서명에는 특정 항목에 대한 변수가 포함됩니다. 아래에는 변수의 기본값이 나와 있으며, $HOME_NET 및 $EXTERNAL_NET이 가장 일반적으로 사용되는 변수입니다. 프로토콜은 포트 번호와 별도로 지정되므로, 포트 변수는 번호로만 존재합니다.

- $DNS_SERVERS = $HOME_NET(임의의 IP 주소 의미)
- $EXTERNAL_NET = 임의의 IP 주소

- $FILE_DATA_PORTS = $HTTP_PORTS, 143, 110
- $FTP_PORTS = 21, 2100, 3535
- $GTP_PORTS = 3386, 2123, 2152
- $HOME_NET = 임의의 IP 주소
- $HTTP_PORTS = 144개의 포트 번호가 지정됨: 36, 80-90, 311, 383, 443, 555, 591, 593, 631, 666, 801, 808, 818, 901, 972, 1158, 1212, 1220, 1414, 1422, 1533, 1741, 1830, 1942, 2231, 2301, 2381, 2578, 2809, 2980, 3029, 3037, 3057, 3128, 3443, 3507, 3702, 4000, 4343, 4848, 5000, 5117, 5222, 5250, 5450, 5600, 5814, 6080, 6173, 6767, 6988, 7000, 7001, 7005, 7071, 7080, 7144, 7145, 7510, 7770, 7777-7779, 8000, 8001, 8008, 8014, 8015, 8020, 8028, 8040, 8060, 8080-8082, 8085, 8088, 8118, 8123, 8161, 8180-8182, 8222, 8243, 8280, 8300, 8333, 8344, 8400, 8443, 8500, 8509, 8787, 8800, 8888, 8899, 8983, 9000, 9002, 9060, 9080, 9090, 9091, 9111, 9290, 9443, 9447, 9710, 9788, 9999, 10000, 11371, 12601, 13014, 15489, 19980, 23472, 29991, 33300, 34412, 34443, 34444, 40007, 41080, 44449, 50000, 50002, 51423, 53331, 55252, 55555, 56712
- $HTTP_SERVERS = $HOME_NET(임의의 IP 주소 의미)
- $ORACLE_PORTS = 임의로 지정됨
- $SHELLCODE_PORTS = 180
- $SIP_PORTS = 5060, 5061, 5600
- $SIP_SERVERS = $HOME_NET(임의의 IP 주소 의미)
- $SMTP_SERVERS = $HOME_NET(임의의 IP 주소 의미)
- $SNMP_SERVERS = $HOME_NET(임의의 IP 주소 의미)
- $SQL_SERVERS = $HOME_NET(임의의 IP 주소 의미)
- $SSH_PORTS = 22
- $SSH_SERVERS = $HOME_NET(임의의 IP 주소 의미)
- $TELNET_SERVERS = $HOME_NET(임의의 IP 주소 의미)

생성기 식별자

GID(생성기 식별자)는 침입 규칙을 평가하고 이벤트를 생성하는 하위 시스템을 식별합니다. 표준 텍스트 침입 규칙에는 생성기 ID 1이 있으며 공유 개체 침입 규칙에는 생성기 ID 3이 있습니다. 또한, 다양한 전처리기에 대한 여러 가지 규칙 집합이 있습니다. 다음 표에서는 GID에 대해 설명합니다.

표 ***10:*** 생성기 ***ID***

ID	**Component(**구성 요소**)**
1	표준 텍스트 규칙

ID	Component(구성 요소)
2	태그가 지정된 패킷 (태그가 지정된 세션에서 패킷을 생성하는 태그 생성기에 대한 규칙)
3	공유 개체 규칙
102	HTTP 디코더
105	Back Orifice 탐지기
106	RPC 디코더
116	패킷 디코더
119, 120	HTTP 검사 전처리기 (GID 120 규칙은 서버별 HTTP 트래픽과 관련이 있음)
122	포트스캔 탐지기
123	IP 조각 모음기
124	SMTP 디코더 (SMTP 동사를 대상으로 익스플로잇)
125	FTP 디코더
126	텔넷 디코더
128	SSH 전처리기
129	스트림 전처리기
131	DNS 전처리기
133	DCE/RPC 전처리기
134	규칙 레이턴시, 패킷 레이턴시 (규칙 레이턴시가 침입 규칙의 그룹을 일시 중지(SID 1)하거나 다시 활성화(SID 2)하는 경우 또는 패킷 레이턴시 임계값이 초과되어 시스템이 패킷 검사를 중지하는 경우(SID 3), 이러한 규칙에 대한 이벤트가 생성됨)
135	속도 기반 공격 탐지기 (네트워크의 호스트에 대한 과도한 연결)
137	SSL 전처리기
138, 139	민감한 데이터 전처리기

ID	Component(구성 요소)
140	SIP 전처리기
141	IMAP 전처리기
142	POP 전처리기
143	GTP 전처리기
144	Modbus 전처리기
145	DNP3 전처리기

네트워크 분석 정책

네트워크 분석 정책은 트래픽 전처리를 제어합니다. 전처리기는 트래픽을 정규화하고 프로토콜 이상 징후를 확인하여 트래픽의 추가 검사를 준비합니다. 네트워크 분석 관련 전처리는 보안 인텔리전스 삭제 및 SSL 암호 해독 후, 그리고 액세스 제어 및 침입/파일 검사 전에 발생합니다.

기본적으로 시스템에서는 Balanced Security and Connectivity(보안과 연결의 균형 유지) 네트워크 분석 정책을 사용하여 액세스 제어 정책에 의해 처리된 모든 트래픽을 전처리합니다. 그러나 액세스 제어 규칙에 대해 침입 정책을 구성하는 경우 시스템에서는 적용된 가장 적극적인 침입 정책과 일치하는 네트워크 분석 정책을 사용합니다. 예를 들어 액세스 제어 규칙에서 Security over Connectivity(보안이 연결에 우선함) 및 Balanced(보안과 연결의 균형 유지) 정책을 모두 사용하는 경우 시스템에서는 모든 트래픽에 대해 Security over Connectivity(보안이 연결에 우선함) NAP를 사용합니다. Snort 3 맞춤형 침입 정책의 경우 이러한 할당은 침입 정책에 할당된 기본 템플릿 정책에 따라 수행됩니다.

Snort 3을 사용하는 경우 정책을 명시적으로 선택하고 선택적으로 설정을 사용자 지정할 수 있습니다. 침입 정책을 직접 사용하거나 사용자 지정 침입 정책의 기본 정책으로 사용하는 경우 디바이스를 통과하는 대부분의 트래픽에 사용하는 침입 정책과 일치하는 이름의 정책을 선택하는 것이 좋습니다. 그런 다음 검사 모드를 변경하거나 네트워크의 트래픽을 고려하여 특정 검사기 또는 바인더 설정을 조정할 수 있습니다.

또한 침입 정책에서 전처리기 규칙을 활성화했는지 여부도 고려하십시오. 전처리기가 필요한 규칙을 활성화하는 경우 NAP에서 해당 검사기를 활성화해야 합니다. 각 검사기에 대해 검사한 포트(바인더)를 포함하여 검사기의 속성을 조정하여 네트워크에 대한 검사기 동작을 사용자 지정할 수도 있습니다.

참고 Snort 2를 사용하는 경우 시스템은 액세스 제어 규칙에서 적용하는 가장 제한적인 침입 정책과 동일한 이름의 NAP 정책을 사용하며, 검사기 또는 바인더 설정을 편집할 수 없습니다.

침입 정책을 위한 라이선스 요건

액세스 제어 규칙에 침입 정책을 적용하려면 위협라이선스를 활성화해야 합니다. 라이선스 구성에 대한 자세한 내용은 선택 가능한 라이선스 활성화 또는 비활성화, 98 페이지를 참조하십시오.

네트워크 분석 정책의 경우 추가 라이선스가 필요하지 않습니다.

액세스 제어 규칙에서 침입 정책 적용

침입 정책을 네트워크 트래픽에 적용하려면 트래픽을 허용하는 액세스 제어 규칙 내에서 정책을 선택하고 침입 정책을 직접 할당하지는 마십시오.

서로 다른 침입 정책을 할당하여 보호 중인 네트워크의 상대적인 위험도를 기반으로 다양한 침입 보호 기능을 제공할 수 있습니다. 예를 들어, 내부 네트워크와 외부 네트워크 간의 트래픽에 대해서는 더 엄격한 Security over Connectivity(연결보다 보안 우선) 정책을 사용하는 반면, 내부 네트워크 간의 트래픽에 대해서는 덜 엄격한 Connectivity over Security(연결이 보안에 우선함) 정책을 적용할 수 있습니다.

모든 네트워크에 대해 동일한 정책을 사용하여 컨피그레이션을 간소화할 수도 있습니다. 예를 들어, Balanced Security and Connectivity(보안과 연결의 균형 유지) 정책은 연결에 지나치게 영향을 미치지 않고 우수한 보호 기능을 제공하도록 설계되었습니다.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)**을 선택합니다.

단계 **2** 트래픽을 허용하도록 새 규칙을 생성하거나 기존 규칙을 수정합니다.

기본 작업이 허용인 경우, 기본 작업에서 침입 정책을 지정할 수도 있습니다.

트래픽을 신뢰하거나 차단하는 규칙에는 침입 정책을 적용할 수 없습니다.

단계 **3** **Intrusion Policy(**침입 정책**)** 탭을 클릭합니다.

단계 **4** **Intrusion Policy(**침입 정책**)** > **On(**켜기**)**을 선택하고 일치하는 트래픽에서 사용할 침입 검사 정책을 선택합니다.

Snort 2와 Snort 3 간 전환

Snort는 제품에 대한 기본 검사 엔진입니다. Snort 버전을 자유롭게 전환할 수는 있지만, Snort 2.0의 일부 침입 규칙은 Snort 3.0에는 없을 수 있으며 그 반대의 경우도 마찬가지입니다. 이러한 규칙 중 하나에 대한 규칙 동작을 변경한 경우에는 해당 변경 사항이 유지되지 않습니다. 해당 변경 사항은 Snort 3으로 전환했다가 다시 Snort 2로 전환하거나 Snort 3으로 다시 전환하는 경우에는 유지되지 않습니다. 두 버전에 모두 있는 규칙의 규칙 동작에 대한 변경 사항은 유지됩니다. Snort 3과 Snort 2의 규칙

간 매핑은 일대일 또는 일대 다수가 될 수 있으므로 변경 사항을 가장 효과적으로 유지할 수 있습니다.

Snort 버전을 변경하는 경우 시스템에서는 자동 구축을 수행하여 변경을 구현합니다. 작업 목록에서 진행률을 확인할 수 있습니다. 작업은 'Snort 버전 변경' 및 '자동 구축-Snort 버전 전환'입니다. 새 버전을 시작할 수 있도록 Snort를 중지해야 하므로 일시적인 트래픽 손실이 발생합니다.

참고 Snort 버전을 전환하려고 하는데 스위치에 장애가 발생하면 취소할 수 없는 변경 사항을 보류하게 되며, 이후의 전환 시도는 허용되지 않습니다. 이 경우 API Explorer에서 사용할 수 있는 ToggleInspectionEngine API를 사용하여 스위치를 완료해야 합니다. bypassPendingChangeValidation 특성을 TRUE로 설정해야 합니다.

시작하기 전에

현재 어떤 Snort 버전이 활성화되어 있는지 확인하려면 이 절차를 사용하거나 **Policies(**정책**)** > **Intrusion(**침입**)**을 선택합니다. 테이블 위의 **Snort Version(Snort** 버전**)** 라인을 찾습니다. 현재 버전은 전체 버전 번호의 첫 번째 번호입니다. 예를 들어 2.9.17-95는 Snort 2 버전입니다.

디바이스가 에어 갭(air-gapped) 네트워크에 있는 경우 전환하기 전에 새 버전의 최신 규칙 패키지를 수동으로 업로드하는 것이 좋습니다.

2.0으로 다운그레이드하는 경우, 생성한 맞춤형 침입 정책이 맞춤형 정책에 사용된 기본 정책으로 변환됩니다. 가능한 한 규칙 작업 재정의가 유지됩니다. 둘 이상의 맞춤형 정책이 동일한 기본 정책을 사용하는 경우, 대부분의 액세스 제어 정책에 사용되는 맞춤형 정책의 재정의는 유지되며 다른 맞춤형 정책의 재정의는 손실됩니다. 이러한 "중복" 정책을 사용하는 액세스 제어 규칙은 이제 가장 많이 사용되는 맞춤형 정책에서 생성된 기본 정책을 사용합니다. 모든 맞춤형 정책이 삭제됩니다. 나중에 가져올 수 있도록 맞춤형 정책을 유지하려는 경우 Snort 3으로 다시 전환한 후 threat defense API를 사용하여 컨피그레이션을 내보냅니다.

또한 2.0으로 다운그레이드하면 NAP 사용자 지정이 제거되고, 시스템은 액세스 제어 규칙에 사용되는 침입 정책에 따라 가장 적합한 NAP를 사용하도록 전환됩니다.

활성 인증의 호스트 이름 리디렉션에도 Snort 3이 필요하며, Snort 2로 전환하면 제거됩니다.

보류 중인 변경 사항을 구축해야 Snort 버전을 전환할 수 있습니다.

프로시저

단계 **1** 디바이스를 선택한 다음 Updates(업데이트) 요약에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

Intrusion Rule(침입 규칙**)** 그룹을 확인합니다. 현재 Snort 버전이 표시됩니다.

단계 **2** **Intrusion Rule(**침입 규칙**)** 그룹에서 **Upgrade to Snort 3.0(Snort 3.0**으로 업그레이드**)** 또는 **Downgrade to Snort 2.0(Snort 2.0**으로 다운그레이드**)**을 클릭하여 Snort 버전을 변경할 수 있습니다.

단계 **3** 작업을 확인하라는 프롬프트가 표시되면 최신 침입 규칙 패키지를 가져오는 옵션을 선택한 다음 **Yes(**예**)**를 클릭합니다.

최신 규칙 패키지를 받는 것이 좋습니다. 시스템은 액티브 Snort 버전용 패키지만 다운로드하므로 전환하려는 Snort 버전용 최신 패키지가 설치되어 있지 않을 가능성이 높습니다.

버전 전환 작업이 완료될 때까지 기다려야 침입 정책을 수정할 수 있습니다.

침입 이벤트를 위한 **Syslog** 구성

침입 정책에 외부 syslog 서버를 구성하여 침입 이벤트를 syslog 서버에 전송할 수 있습니다. 서버에 침입 이벤트를 전송하려면 침입 정책에서 syslog 서버를 구성해야 합니다. 액세스 규칙에서 syslog 서버를 구성하면 syslog 서버에 연결 이벤트만 전송되고 침입 이벤트는 전송되지 않습니다.

여러 시스템 로그 서버를 선택하면 각 서버로 이벤트가 전송됩니다.

침입 이벤트의 메시지 ID는 430001입니다.

프로시저

단계 **1** **Policies(**정책**)** > **Intrusion(**침입**)**을 선택합니다.

단계 **2** **Intrusion Policy Settings(**침입 정책 설정**)** 버튼(⚙)을 클릭하여 syslog를 구성합니다.

단계 **3** **Send Intrusion Events To(**다음으로 침입 이벤트 전송**)** 아래의 **+** 버튼을 클릭하고 시스템 로그 서버를 정의하는 서버 개체를 선택합니다. 필요한 개체가 아직 없으면 **Create New Syslog Server(**새 시스템 로그 서버 생성**)**를 클릭하여 개체를 생성합니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

네트워크 분석 정책 구성**(Snort 3)**

네트워크 분석 정책(NAP)은 디바이스에서 허용되는 모든 연결에 적용됩니다. NAP는 활성화된 검사기 및 검사기에서 사용하는 속성의 값을 결정합니다. 바인더는 다양한 검사기와 연결해야 할 포트 및 프로토콜을 결정합니다.

액세스 제어 규칙에서 적용하는 침입 정책에 따라 NAP를 조정합니다.

- 액세스 제어 규칙에서 단일 침입 정책을 사용하는 경우 동일한 이름의 NAP를 선택합니다. 그런 다음 침입 정책의 설정을 기반으로 검사기와 속성을 조정합니다. 예를 들어 CIP와 같은 특정 검사기에 대해 침입 규칙을 활성화하는 경우, NAP에서 해당 검사기를 활성화해야 합니다.
- 여러 침입 정책을 사용하는 경우 가장 엄격한 침입 정책과 일치하는 NAP를 선택합니다.
- 사용자 지정 침입 정책을 사용하는 경우 사용자 지정 침입 정책에 대한 기본 침입 정책을 기반으로 NAP를 선택합니다.

- 검사기 또는 바인더를 사용자 지정할 필요가 없는 경우, 침입 정책 사용을 기반으로 가장 적합한 NAP를 자동으로 선택하도록 시스템을 구성하는 것이 좋습니다. 이것이 기본 옵션입니다.

시작하기 전에

이를 방지하지 않는 한 시스템은 LSP 업데이트를 정기적으로 검사 규칙에 다운로드합니다. 이러한 업데이트는 검사기와 속성을 추가 또는 제거하고, 속성의 기본 설정을 변경할 수 있습니다. 제거된 검사기를 재정의한 경우, 이러한 재정의가 유지되며 검사기가 더 이상 지원되지 않는다는 경고가 표시됩니다. 이 경우 검사기를 삭제하고 NAP가 완전히 유효한지 확인하기 위해 플래그가 지정된 다른 조정을 수행합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Intrusion(**침입**)**을 선택합니다.

표 위에 표시된 Snort 버전이 3.x인지 확인합니다.

단계 **2** **Intrusion Policy Settings(**침입 정책 설정**)** 버튼(⚙)을 클릭합니다.

단계 **3** **Default Network Analysis Policy(**기본 네트워크 분석 정책**)**에서 다음 중 하나를 선택합니다.

- **Auto(**자동**)** - 액세스 제어 규칙에 적용된 가장 많이 사용되는 침입 정책(또는 사용자 지정 규칙의 기본 정책)과 일치하는 NAP를 자동으로 선택합니다. 침입 정책을 적용하지 않으면 Balanced Security and Connectivity NAP(균형 잡힌 보안 및 연결성 NAP)가 사용됩니다. NAP는 Prevention(방지) 모드에서 실행되며 침입 또는 바인더 설정을 사용자 지정할 수 없습니다. 이 절차의 나머지 부분은 자동 모드에서 실행할 때 적용되지 않습니다.
- **Custom(**사용자 지정**)** - 사용해야 할 NAP를 명시적으로 선택합니다. 다른 정책을 선택하려면 정책 이름 옆에 있는 **Edit(**편집**)** 링크를 클릭합니다. 그런 다음 검사 모드를 선택하고 다음 단계에서 설명하는 것과 같이 검사기 및 바인더 설정을 사용자 지정할 수 있습니다.

단계 **4** Edit Network Analysis Policy(네트워크 분석 정책 편집) 대화 상자에서 정책을 선택하고 해당 설정을 구성합니다.

a) **Network Analysis Policy(**네트워크 분석 정책**)**에서 허용되는 모든 연결에 전역으로 적용해야 하는 정책을 선택합니다.

b) **Inspection Mode(**검사 모드**)**를 선택합니다.

검사 모드에 따라 규정 미준수 트래픽을 처리하는 방법이 결정됩니다. 최적의 결과를 얻으려면 침입 정책에서 사용하는 것과 동일한 검사 모드를 사용하십시오.

- **Prevention(**방지**)** - 정책의 설정에 따라 모든 디코더, 정규화 또는 프로토콜 변칙을 차단합니다. SSL 암호 해독 정책을 활성화하거나 액세스 제어 정책 설정에서 **TLS Server Identity Discovery(TLS** 서버 **ID** 검색**)** 옵션을 활성화하는 경우 이 옵션을 사용해야 합니다.
- **Detection(**탐지**)** - 디코더, 정규화 또는 프로토콜 변칙에 대한 알림만 제공합니다. 어떤 트래픽도 차단하지 않습니다.

c) (선택 사항). 검사기 및 바인더에 대한 재정의를 구성하고 관리합니다.

- 재정의를 편집하려면 검사기 및 바인더 재정의 구성, 564 페이지 항목을 참조하십시오.
- 스키마 또는 재정의를 다운로드하려면 재정의 및 스키마 다운로드, 566 페이지 항목을 참조하십시오.
- 재정의를 업로드하려면 재정의 업로드, 567 페이지 항목을 참조하십시오.
- 모든 재정의를 재설정하려면 NAP 파일 위의 **Reset Inspector / Binder Overrides(**검사기/바인더 재정의 재설정**)** 링크를 클릭합니다. 재설정을 확인하라는 메시지가 나타납니다. 명령 이름에 표시된 대로 삭제는 검사기 또는 바인더로 제한됩니다. 예를 들어, 모든 바인더 재정의를 삭제해도 검사기 재정의는 변경되지 않습니다.
- 선택한 검사기의 모든 변경 사항을 취소하려면 **Reset *Inspector* to Defaults(**검사기를 기본값으로 재설정**)**를 클릭합니다.
- 재정의가 있는 검사기만 볼 수 있도록 보기를 필터링하려면 **Show Only Overrides(**재정의만 표시**)**를 클릭합니다. **Show All Inspectors(**모든 검사기 표시**)**를 클릭하여 필터를 제거합니다.

d) **OK(**확인**)**를 클릭합니다.

검사기 및 바인더 재정의 구성

기본 NAP를 선택하면 해당 베이스라인 정책에 포함된 관리자 설정을 선택하게 됩니다. 대부분의 경우에는 적절한 설정입니다.

하지만 선택한 NAP의 설정을 재정의할 수 있습니다. 예를 들어 개별 검사기를 활성화 또는 비활성화하거나 속성 또는 바인더에 대한 값을 변경할 수 있습니다.

다음 절차에서는 재정의를 직접 구성하는 방법을 설명합니다. 또는 스키마를 다운로드하고 오프라인에서 변경한 다음 재정의를 업로드할 수 있습니다. 다른 디바이스에서 다운로드한 재정의를 업로드할 수도 있습니다.

시작하기 전에

각 검사기, 바인더 및 속성에 대한 설명은 이 문서의 범위를 벗어납니다. 예시를 포함한 세부 정보는 https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/snort3-inspectors/snort-3-inspector-reference.html에서 *Snort 3* 검사기 참조에서 확인하십시오.

프로시저

단계 **1** **Policies(**정책**)** > **Intrusion(**침입**)**을 선택한 다음 **Intrusion Policy Settings(**침입 정책 설정**)** 버튼(⚙)을 클릭하고, NAP 설정에 대해 **Custom(**맞춤형**)**을 선택한 다음 정책 이름 옆에 있는 **Edit(**편집**)** 링크를 클릭합니다.

단계 **2** 변경할 설정이 포함된 탭을 클릭합니다.

- **Inspector(**검사기**)** - 검사기는 FTP와 같은 특정 유형의 트래픽에서 프로토콜 변칙을 검사합니다.

- **Binders(**바인더**)** - 바인더 검사기는 트래픽을 검사하기 위해 서비스 검사기를 사용해야 하는 시기를 결정합니다. 바인딩 검사기의 구성에는 포트, 호스트, CIDR 및 네트워크 분석 정책의 다른 검사기가 트래픽을 검사해야 하는 시기를 정의하는 서비스가 포함됩니다.

단계 **3** 필요에 따라 설정을 편집합니다.

- 다음을 사용하여 JSON 편집기에서 보기를 제어합니다.
  - JSON 파일의 전체 텍스트 검색을 수행하려면 **Filter(**필터**)** 편집 상자를 사용합니다.
  - JSON 파일의 모든 폴더를 열려면 **Expand All Fields(**모든 필드 확장**)(**  **)** 버튼을 클릭합니다.
  - JSON 파일의 모든 폴더를 닫으려면 **Collapse All Fields(**모든 필드 축소**)(**  **)** 버튼을 클릭합니다.
  - 최근 변경 사항을 취소하려면 **Undo Last Action(**마지막 작업 실행 취소**)(**  **)** 버튼을 클릭합니다
  - 마지막으로 되돌린 변경 사항을 다시 적용하려면 **Redo(**다시 실행**)(**  **)** 버튼을 클릭합니다.
  - 작업 메뉴, 오류 플래그 및 편집을 안내하는 기타 기능이 포함된 JSON 파일의 형식이 지정된 보기를 보려면 **Tree(**트리**)**를 선택합니다.
  - 원시 JSON 파일을 보려면 **Code(**코드**)**를 선택합니다.
- 트리 보기에서 **Menu(**메뉴**)(****)** 버튼을 클릭하여 파일의 내용을 조작합니다 다음 작업을 수행할 수 있습니다.
  - 속성을 삽입합니다. 편집기를 사용하여 적절한 데이터 유형을 결정하도록 하려면 Auto(자동)를 사용합니다. 그렇지 않으면 배열, 개체 또는 문자열을 추가합니다. 유효하지 않은 속성을 추가하는 경우 시스템은 검사기 또는 바인더를 해결해야 하는 문제가 있는 것으로 표시합니다.
  - 속성을 추가합니다. 이 작업은 삽입과 동일하지만 섹션 끝에 속성을 배치합니다.
  - 선택한 속성을 복제합니다.
  - 선택한 속성을 제거(삭제)합니다. 속성을 편집할 때 팝업 메시지에 삭제 명령이 제공될 수도 있습니다.
- 현재 비활성화된 검사기를 활성화하거나 부울 속성의 설정을 변경하려면 속성 값 앞에 있는 확인란을 클릭합니다. 예를 들어, 검사기를 활성화하려면 **enabled : false** 속성을 다음과 같이 변경합니다.

- 문자열 또는 숫자 속성의 값을 변경하려면 속성을 클릭하고 필요에 따라 값을 편집합니다. 항목이 필드의 규칙을 위반할 경우, 오류 메시지에서 불일치를 설명합니다. 예를 들어, 범위를 벗어난 값을 입력하는 경우 숫자 값에 유효한 값 범위가 표시됩니다.

- 재정의 재설정:
  - **Reset Inspector/Binder Overrides(**검사기/바인더 재정의 재설정**)**를 클릭하여 모든 검사기 또는 바인더에 대한 모든 변경 사항을 제거하고 기본값으로 되돌립니다. 명령 이름에 표시된 대로 삭제는 검사기 또는 바인더로 제한됩니다. 예를 들어, 모든 바인더 재정의를 삭제해도 검사기 재정의는 변경되지 않습니다.
  - **Reset *Inspector* to Defaults(**검사기를 기본값으로 재설정**)**를 클릭하여 선택한 검사기의 모든 변경 사항만 되돌립니다.
- 재정의가 있는 검사기만 볼 수 있도록 보기를 필터링하려면 **Show Only Overrides(**재정의만 표시**)**를 클릭합니다. **Show All Inspectors(**모든 검사기 표시**)**를 클릭하여 필터를 제거합니다.
- 검사기가 더 이상 지원되지 않으면 검사기는 메시지와 함께 플래그가 지정됩니다. 메시지에서 **Delete Inspector(**검사기 삭제**)** 링크를 클릭하여 검사기를 제거합니다.

단계 **4** 완료되면**OK(**확인**)**를 클릭합니다.

재정의 및 스키마 다운로드

NAP 스키마를 다운로드하거나 정책에 대해 구성한 재정의를 다운로드할 수 있습니다.

기본 NAP를 변경할 때마다 이전 설정으로 돌아가려면 재정의를 다운로드하는 것이 좋습니다. 또한 한 디바이스에서 JSON 편집기를 사용하여 모든 디바이스에서 사용할 재정의를 구현하고, 재정의를 다운로드한 다음 해당 재정의 파일을 다른 디바이스에 업로드할 수 있습니다.

오프라인으로 파일을 편집한 다음 이 디바이스 또는 여러 디바이스에 재정의를 업로드하려는 경우 스키마를 다운로드하면 유용합니다. 변경 사항만 재정의로 간주되도록 하려면 전체 파일을 업로드하는 대신 변경해야 하는 섹션만 복사/붙여넣기해야 합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Intrusion(**침입**)**을 선택한 다음 **Intrusion Policy Settings(**침입 정책 설정**)** 버튼(⚙)을 클릭하고, NAP 설정에 대해 **Custom(**맞춤형**)**을 선택한 다음 정책 이름 옆에 있는 **Edit(**편집**)** 링크를 클릭합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 현재 선택한 NAP의 스키마를 다운로드하려면 기어 아이콘(⚙)을 클릭하고 **Download(**다운로드**)** > **Policy Schema(**정책 스키마**)**를 선택합니다
- 현재 편집 세션 이전에 있었던 것처럼 저장된 재정의 세트를 다운로드하려면 기어 아이콘(⚙)을 클릭하고 **Download(**다운로드**)** > **Last Saved Overrides(**마지막으로 저장된 재정의**)**를 선택합니다. 파일에는 재정의된 속성과 해당 속성에 포함된 개체가 있습니다.

- 현재 편집 세션에서 생성한 재정의를 다운로드하려면 기어 아이콘(⚙)을 클릭하고 **Download(**다운로드**)** > **Current Unsaved Overrides(**현재 저장되지 않은 재정의**)**를 선택합니다. 파일에는 재정의된 속성과 해당 속성에 포함된 개체가 있습니다.

재정의 업로드

임베디드 JSON 편집기를 사용하여 속성을 편집하는 대신 NAP 정책 스키마를 다운로드하고 파일을 오프라인에서 편집한 다음 파일을 업로드할 수 있습니다. 그러면 업로드된 파일에 구성된 모든 재정의가 선택한 NAP에 적용됩니다.

다른 디바이스에서 재정의를 구성한 후 다운로드한 파일을 업로드할 수도 있습니다.

재정의를 업로드하면 동일한 파일을 여러 디바이스에 업로드하고 동일한 재정의를 쉽게 적용할 수 있습니다.

시작하기 전에

네트워크 분석 정책에서 검사기 구성을 재정의하려면 필요한 변경 사항만 업로드해야 합니다. 전체 구성을 업로드해서는 안 됩니다. 이렇게 하면 재정의가 고정되어 이후에 LSP 업데이트의 일부로 포함되는 기본값 또는 구성 변경 사항이 적용되지 않습니다. 업로드한 재정의는 변경하려는 속성에만 집중해야 합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Intrusion(**침입**)**을 선택한 다음 **Intrusion Policy Settings(**침입 정책 설정**)** 버튼(⚙)을 클릭하고, NAP 설정에 대해 **Custom(**맞춤형**)**을 선택한 다음 정책 이름 옆에 있는 **Edit(**편집**)** 링크를 클릭합니다.

단계 **2** 기어 아이콘(⚙)을 클릭하고 **Upload(**업로드**)** > **Overrides(**재정의**)**를 선택합니다.

단계 **3** (선택 사항). **Download(**다운로드**)** 링크 중 하나를 클릭하여 기존 재정의 사본을 저장합니다.

마지막으로 저장한 재정의(현재 편집 세션 전에 수행한 재정의) 또는 현재 저장되지 않은 재정의(현재 편집 세션 중에 수행한 재정의)를 다운로드할 수 있습니다.

단계 **4** Confirm Upload Overrides(업로드 재정의 확인) 대화 상자에서 **Yes(**예**)**를 클릭하여 계속할 것임을 확인합니다.

단계 **5** **Browse(**찾아보기**)**를 클릭하거나 드래그 앤 드롭하여 재정의가 포함된 JSON 파일을 선택하고 **OK(**확인**)**를 클릭합니다.

침입 정책 관리(Snort 3)

Snort 3를 검사 엔진으로 사용하는 경우 고유한 침입 정책을 생성하여 원하는 대로 맞춤화할 수 있습니다. 시스템은 동일한 이름의 Cisco Talos Intelligence Group(Talos) 정의된 정책을 기반으로 하는 사전 정의된 정책과 함께 제공됩니다. 이러한 정책을 수정할 수는 있지만, 기본 Talos 정책을 기반으로 고유한 정책을 생성하고 규칙 작업을 조정해야 하는 경우 변경하는 것이 좋습니다.

이러한 사전 정의된 각 정책에는 동일한 침입 규칙(서명이라고도 함) 목록이 포함되지만, 각 규칙에 수행되는 조치가 다릅니다. 예를 들어 어떤 규칙은 어떤 정책에서는 활성화되지만, 다른 정책에서는 비활성화될 수 있습니다.

특정 규칙이 차단하지 말아야 할 트래픽을 차단하여 오탐(False Positive)이 지나치게 많이 발생하고 있다는 사실을 알게 될 경우, 보안이 더 낮은 침입 정책으로 전환하지 않고도 규칙을 비활성화할 수 있습니다. 또는 트래픽을 삭제하지 않고 일치 항목에 대해 알리도록 규칙을 변경할 수 있습니다.

이와 반대로, 특정 공격을 차단해야 하지만 선택한 침입 정책에서 관련 규칙이 비활성화된 경우, 보안이 더 높은 정책으로 변경하지 않고도 규칙을 활성화할 수 있습니다.

침입 관련 대시보드 및 이벤트 뷰어(두 가지 모두 **Monitoring(모니터링)** 페이지에서 제공)를 사용하여 침입 규칙이 트래픽에 어떤 영향을 미치는지 평가하십시오. 침입 이벤트와 침입 데이터는 알리거나 삭제하도록 설정된 침입 규칙과 일치하는 트래픽에 대해서만 표시됩니다. 즉, 비활성화된 규칙은 평가되지 않습니다.

참고 Snort 2로 전환하면 맞춤형 정책을 생성할 수 없으며, 침입 정책이 약간 다르게 사용됩니다. 이 항목 대신 침입 정책 관리(Snort 2), 581 페이지를 참조하십시오.

프로시저

단계 **1** **Policies(정책)** > **Intrusion(침입)**을 선택합니다.

표 위에 표시된 Snort 버전이 3.x인지 확인합니다.

단계 **2** 다음 중 하나를 수행합니다.

- **Search/Filter(검색/필터)** 상자를 사용하여 정책을 찾습니다. 이름으로만 검색할 수 있습니다.
- 기어 아이콘(⚙)을 클릭하여 시스템 로그 서버에 로깅을 활성화합니다. 침입 이벤트를 위한 Syslog 구성, 562 페이지의 내용을 참조하십시오.
- 기어 아이콘(⚙)을 클릭하여 네트워크 분석 정책(NAP)을 구성합니다. 네트워크 분석 정책 구성(Snort 3), 562 페이지의 내용을 참조하십시오.
- 새 정책을 생성하려면 +를 클릭합니다. 맞춤형 침입 정책 구성(Snort 3), 569 페이지의 내용을 참조하십시오.

- 정책에서 속성과 규칙을 확인하고 수정하려면 수정 아이콘()을 클릭합니다. 침입 정책 속성 보기 또는 수정(Snort 3), 570 페이지의 내용을 참조하십시오.
- 정책을 삭제하려면 삭제 아이콘()을 클릭합니다.

맞춤형 침입 정책 구성(Snort 3)

사전 정의된 정책이 요구 사항에 맞지 않을 경우 새 침입 정책을 생성하여 규칙 동작을 맞춤설정할 수 있습니다. 일반적으로, 이러한 정책을 변경하는 대신 미리 정의된 정책을 기반으로 맞춤형 정책을 생성하는 것이 좋습니다. 그러면 맞춤화로 필요한 결과를 얻지 못하는 경우에 Cisco Talos 정의 정책 중 하나를 쉽게 구현할 수 있습니다.

프로시저

단계 **1** **Policies(**정책**)** > **Intrusion(**침입**)**을 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 새 정책을 생성하려면 **+**를 클릭합니다.
- 기존 정책을 편집하려면, 정책에 대한 편집 아이콘()을 클릭합니다. 정책 상세정보가 표시되면 페이지 상단의 정책 속성 섹션에서 **Edit(**수정**)** 링크를 클릭합니다.

단계 **3** 정책의 **Name(**이름**)**을 입력하고 필요한 경우 설명을 입력합니다.

단계 **4** 정책을 위한 **Inspection Mode(**검사 모드**)** 구성

- **Prevention(**차단**)** - 침입 규칙 작업이 항상 적용됩니다. 삭제 규칙과 일치하는 연결이 차단됩니다.
- **Detection(**탐지**)** - 침입 규칙에서 알림만 생성합니다. 삭제 규칙과 일치하는 연결을 통해 알림 메시지가 생성되지만 연결은 차단되지 않습니다.

단계 **5** 정책의 **Base Template(**기본 템플릿**)**을 선택합니다.

기본 템플릿은 Cisco Talos에서 제공합니다. 각각에 대한 정보 아이콘을 클릭하면 정책에 대한 추가 정보를 확인할 수 있습니다. 새 규칙 패키지가 설치되면 정책 이름이 변경될 수 있으며 새 정책이 표시됩니다.

- **Maximum Detection(**최대 탐지**) (Cisco Talos)** — 이 정책은 오로지 보안에 중점을 둡니다. 네트워크 연결 및 처리량을 보장하지 않으며 오탐이 발생할 수 있습니다. 이 정책은 강력한 보안이 필요한 영역에만 사용해야 하며, 알림을 조사하여 유효성을 확인할 보안 모니터를 마련해야 합니다.

- **Security Over Connectivity(**보안이 연결에 우선함**) (Cisco Talos)** — 이 정책은 가급적 네트워크 연결 및 처리량 대신 보안에 중점을 둡니다. 트래픽을 더 자세히 검사하고 더 많은 규칙을 평가하지만 합당한 수준 내에서 오탐이 발생하고 레이턴시가 증가합니다.
- **Balanced Security and Connectivity(**보안과 연결의 균형 유지**) (Cisco Talos)** — (기본값) 이 정책은 네트워크 연결 및 처리량과 보안 요구 사항의 사이에서 절묘한 균형을 유지하려 합니다. 이 정책은 연결성보다 보안 우선 정책만큼 엄격하지는 않지만 정상적인 트래픽을 가급적 방해하지 않으면서 사용자의 안전을 유지하려 합니다.
- **Connectivity Over Security(**연결이 보안에 우선함**) (Cisco Talos)** — 이 정책은 가급적 보안 대신 네트워크 연결성 및 처리량에 중점을 둡니다. 트래픽을 자세히 검사하지 않으며 평가하는 규칙도 더 적습니다.
- **No Rules Active(**활성 규칙 없음**) (Cisco Talos)** — 이 정책은 일반적인 전 처리기 설정을 지정하는 기본 정책이지만 규칙 또는 기본 제공 알림을 활성화하지 않습니다. 적용하려는 정책만 활성화되도록 하려면 이 정책을 기본으로 사용합니다.

단계 **6** **OK(**확인**)**를 클릭합니다.

침입 정책 목록으로 돌아갑니다. 이제 새 정책을 보고 필요에 따라 규칙 작업을 조정할 수 있습니다.

침입 정책 속성 보기 또는 수정(Snort 3)

Intrusion Policy(침입 정책) 페이지에는 사전 정의된 정책과 사용자 정의 정책을 포함하는 정책 목록과 해당 설명이 표시됩니다. 정책을 수정하려면 먼저 정책의 속성을 확인해야 합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Intrusion(**침입**)**을 선택합니다.

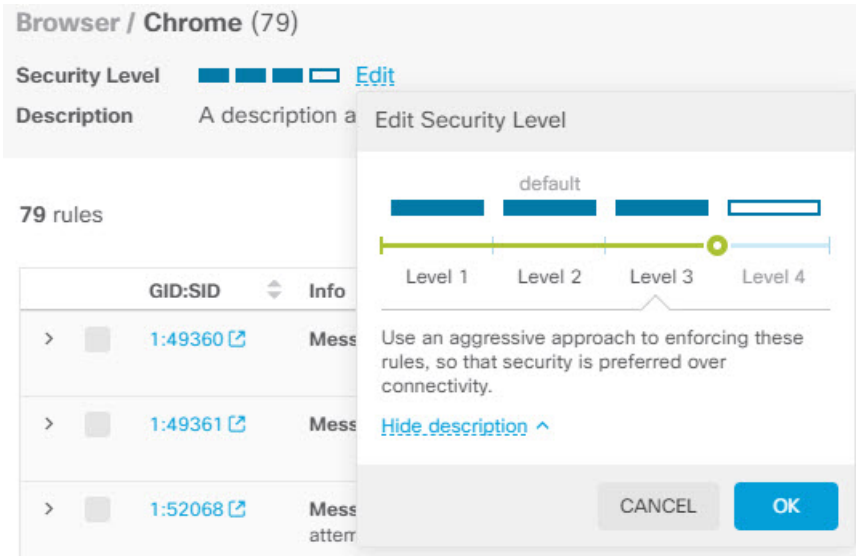
단계 **2** 정책의 편집 아이콘()을 클릭합니다.

정책에는 다음 섹션이 포함되어 있습니다.

- **Policy Name(**정책 이름**)** 드롭다운 목록
  - 드롭다운 목록에서 다른 정책을 선택하여 쉽게 전환하거나 뒤로 버튼()을 클릭하여 정책 목록으로 돌아갈 수 있습니다.
  - 정책 이름() 옆에 있는 삭제 아이콘을 클릭하여 이 정책을 삭제할 수 있습니다.
- **General properties(**일반 속성**)** 이 섹션에서는 침입 모드, 기본 정책 및 설명을 보여줍니다. **Edit(**수정**)**를 클릭하여 이러한 속성 또는 정책 이름을 변경합니다.
- 규칙 그룹 목차. 이 목록에는 정책에 액티브 규칙이 있는 모든 규칙 그룹이 표시됩니다. 그룹에는 더 큰 상위 그룹 내에서 규칙의 하위 세트를 구성하는 하위 그룹을 포함한 상위 그룹을 가진

계층 구조가 있습니다. 각 그룹은 규칙의 논리적 모음이며 지정된 규칙이 둘 이상의 그룹에 표시될 수 있습니다.

- 현재 정책에 액티브 규칙이 없는 그룹을 추가하려면 + > **Add Existing Rule Group**(기존 규칙 그룹 추가)을 클릭하여 그룹을 선택합니다. 침입 정책에서 규칙 그룹 추가 또는 제거(Snort 3), 572 페이지의 내용을 참조하십시오.
- 그룹의 보안 레벨을 변경하려면 목록에서 하위 그룹을 선택합니다. 규칙 목록이 아래에 나열된 그룹의 규칙과 함께 맨 위에 보안 레벨을 표시하도록 변경됩니다. 보안 레벨 옆에 있는 **Edit**(수정) 링크를 클릭하여 새 레벨을 선택합니다. 수정할 때는 **View Description**(설명 보기)을 클릭하여 각 보안 레벨에 대한 정보를 가져옵니다. 레벨을 변경하면 액티브 상태인 규칙이 변경될 수 있으며, 보다 많은 액티브 규칙 및 삭제 작업을 가진 보다 많은 규칙을 사용하는 경향이 있는 안전한 레벨을 사용하여 지정된 규칙에 대한 작업도 변경될 수 있습니다. **OK**(확인)를 클릭하여 변경을 확인합니다. (보안 수준은 맞춤형 규칙 그룹에 적용되지 않습니다.)



- 그룹의 모든 규칙을 제거하려면 목록에서 하위 그룹을 선택합니다. 그 다음 그룹 이름의 맨 오른쪽에 있는 **Exclude**(제외) 링크를 클릭하고 그룹을 제외할 것임을 확인합니다. 그룹을 제외하면 그룹의 모든 규칙이 간단히 비활성화됩니다. 그룹은 삭제되지 않습니다.

  그러나 활성화된 다른 그룹과 공유하는 규칙이 그룹에 포함된 경우 공유 규칙은 여전히 액티브 상태인 그룹에서 적용한 모든 작업을 유지합니다. 모든 경우, 그룹 구성원 자격에 관계없이 개별 규칙에 대해 가장 적극적인 설정을 유지합니다.
- 맞춤형 규칙의 새 맞춤형 규칙 그룹을 추가하려면 + > **Upload Custom Rules**(맞춤형 규칙 업로드)를 클릭합니다. 자세한 내용은 맞춤형 침입 규칙 업로드, 577 페이지 섹션을 참조해 주십시오.
- 맞춤형 규칙 그룹의 이름 또는 설명을 변경하려면 **Edit**(편집)를 클릭합니다.
- 맞춤형 규칙 그룹을 삭제하려면 **Delete**(삭제)를 클릭합니다. 자세한 내용은 맞춤형 침입 규칙 및 규칙 그룹 관리, 576 페이지를 참고하십시오.

- 맞춤형 규칙 그룹에 새 맞춤형 규칙을 추가하려면 규칙 테이블 위에 있는 +를 클릭합니다. 개별 맞춤형 침입 규칙 설정, 580 페이지의 내용을 참조하십시오.
- 맞춤형 규칙에 대한 그룹 멤버십을 편집, 복제, 삭제 또는 관리하려면 규칙 오른쪽에 마우스를 두고 해당 버튼 또는 명령을 클릭합니다. 자세한 내용은 개별 맞춤형 침입 규칙 설정, 580 페이지를 참고하십시오.

- **List of rules(**규칙 목록**)**. 전체 텍스트 검색을 사용하여 규칙을 찾으려면 검색 필드를 이용하십시오. GID 또는 SID의 조합에서 검색할 필터링 항목을 선택하거나 (추가한) 사용자 정의 규칙만 표시하거나,작업이 재정의된 규칙만 표시하거나, 해당 작업(비활성, 알림, 삭제)을 기준으로 간단히 규칙을 표시할 수도 있습니다. 규칙은 느리게 로드되므로 필터링되지 않은 전체 목록을 스크롤하려면 시간이 조금 걸립니다. 목록을 필터링할 때 새로 고침 버튼을 클릭하여 필터링된 보기를 다시 로드합니다.
  - 규칙에 대한 작업을 변경하려면 해당 규칙에 대한 **Action(**작업**)** 셀을 클릭하고 새 작업, 즉 **Alert(**알림**)** 전용, 일치하는 트래픽 **Block(**차단**)** 또는 규칙 **Disable(**비활성화**)**을 선택합니다. 각 규칙에 대한 기본 작업이 표시됩니다.
  - 한 번에 두 개 이상의 규칙에 대한 작업을 변경하려면 변경할 규칙의 왼쪽 열에 있는 체크박스를 클릭한 다음 규칙 테이블 위의 **Action(**작업**)** 드롭다운 목록에서 새 작업을 선택합니다. GID:SID 헤더의 체크 박스를 클릭하여 목록의 모든 규칙을 선택합니다. 한 번에 최대 5,000개의 규칙을 변경할 수 있습니다.
  - 맞춤형 규칙 그룹 내에서 규칙을 업데이트하려면 **Upload Rule File(**규칙 파일 업로드**)**을 클릭합니다. 자세한 내용은 맞춤형 침입 규칙 업로드, 577 페이지를 참고하십시오.
  - 규칙에 대한 자세한 정보를 얻으려면 **GID:SID** 셀의 링크를 클릭합니다. 링크를 클릭하면 Snort.org로 이동됩니다.
  - 나열된 규칙을 변경하려면 규칙 그룹 목차에서 상위 그룹이 아닌 하위 그룹을 클릭하면 됩니다. 규칙 그룹 목록의 맨 위에 있는 **ALL RULES(**모든 규칙**)**를 클릭하여 모든 규칙 목록으로 돌아갈 수 있습니다.
  - 정렬 순서를 변경하려면 열의 테이블 헤더를 클릭합니다. 규칙의 기본 정렬은 재정의된 규칙, 삭제 규칙, 알림 규칙 순입니다.
  - 침입 규칙(LSP) 업데이트의 변경 사항을 확인하려면 필터 필드에서 **LSP Update(LSP** 업데이트**)**를 선택한 다음 변경 사항을 확인하려는 업데이트를 선택하고, 모든 변경 사항을 볼지 아니면 규칙에 대한 추가 또는 변경 사항만 표시할지를 지정합니다.

침입 정책에서 규칙 그룹 추가 또는 제거(Snort 3)

침입 규칙은 로컬 그룹에서 구성됩니다. 그룹에는 계층 구조가 있으며 관련 하위 그룹을 포함하는 상위 그룹이 있습니다. 규칙 자체는 하위 그룹에만 나타납니다. 상위 그룹은 단순한 조직 구조입니다. 지정된 규칙은 둘 이상의 그룹에 나타날 수 있습니다.

생성하는 모든 맞춤형 규칙 그룹은 User Defined Groups 폴더에 있습니다. 맞춤형 규칙 그룹에는 계층 구조가 없습니다.

침입 정책에 규칙을 추가하거나 제거하는 가장 쉬운 방법은 그룹을 추가하거나 제거하는 것입니다. 그룹의 규칙은 논리적으로 관련되어 있으므로 지정된 그룹 내의 모든 규칙은 아니더라도 대부분을 사용해야 할 가능성이 높습니다.

다음 절차에서는 그룹을 추가하고 그룹의 보안 레벨을 변경하는 방법에 대해 설명합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Intrusion(**침입**)**을 선택합니다.

단계 **2** 변경할 정책의 편집 아이콘()을 클릭합니다.

단계 **3** (그룹 추가) 그룹이 규칙 그룹 목록에 표시되지 않으면 + > **Add Existing Rule Group(**기존 규칙 그룹 추가**)**을 클릭하고 다음을 수행합니다.

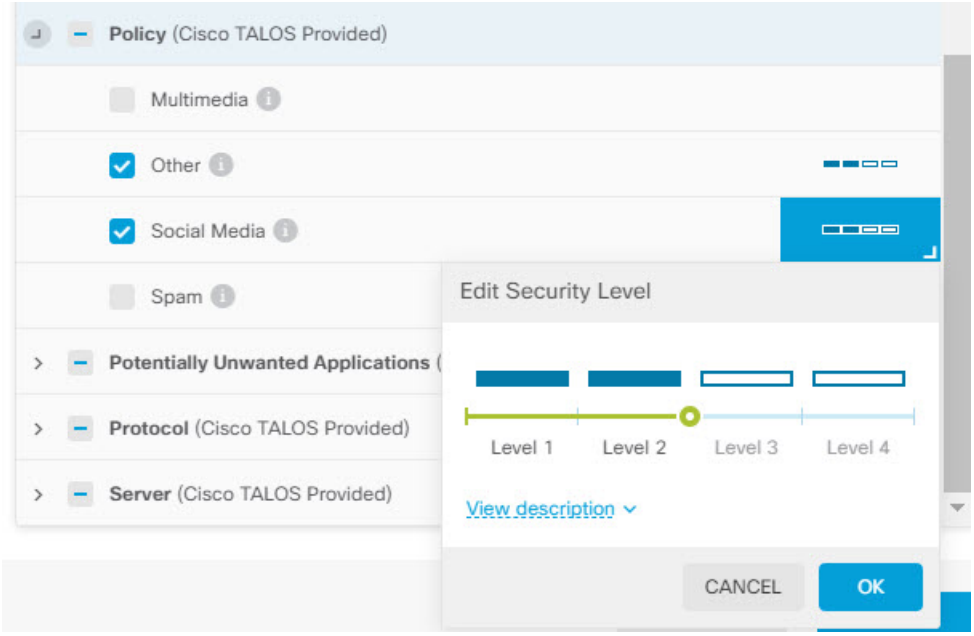
a) 하위 그룹을 찾습니다.

- 상위 그룹 이름 옆의 확인 표시는 상위 그룹의 모든 하위 그룹이 이미 선택되었음을 나타냅니다.
- 상위 그룹 이름 옆의 빼기 표시는 하나 이상의 하위 그룹에 이 정책에 대해 활성화된 규칙이 없음을 나타냅니다. 이들은 추가할 수 있는 그룹입니다.
- 하위 그룹 이름 옆의 확인 표시는 그룹이 이미 선택되었음을 나타냅니다.

b) 추가할 그룹을 선택합니다(즉, 체크 박스 선택).

c) (선택 사항으로, 맞춤형 규칙 그룹에 적용되지 않습니다.) 각 그룹에는 맞춤형 정책에 사용되는 기본 정책에 따라 기본 보안 레벨이 있습니다. 변경하려면 보안 레벨 아이콘을 클릭하여 새 레벨을 선택한 후 **OK(**확인**)**를 클릭합니다.

레벨 1은 보안보다 연결을 강조하는 가장 덜 안전한 상태이며, 레벨 4는 최대한의 보안을 제공하는 가장 적극적인 보안 상태입니다. **View Description(**설명 보기**)**을 클릭하여 각 레벨에 대한 설명을 선택하여 볼 수 있습니다.



d) 모든 변경 사항을 적용할 때까지 그룹을 계속 선택하거나 선택을 취소합니다.

e) **OK(**확인**)**를 클릭합니다.

단계 **4** (그룹 제거) 그룹 내의 모든 규칙을 비활성화하려는 경우 다음 방법 중 하나를 사용할 수 있습니다.

- 그룹을 선택한 다음, 규칙 목록 위의 그룹 이름 맨 오른쪽에 있는 **Exclude(**제외**)** 링크를 클릭합니다.
- 그룹을 추가하는 방법을 사용합니다. 대신 원치 않는 그룹을 선택 취소하고(즉, 체크 박스 선택을 취소) **OK(**확인**)**를 클릭합니다.
- 맞춤형 규칙 그룹을 삭제하여 시스템 및 이를 사용하는 모든 침입 정책에서 완전히 제거할 수 있습니다. 그룹을 선택한 다음 **Delete(**삭제**)**를 클릭합니다.

침입 규칙 작업 변경(Snort 3)

각 침입 정책의 규칙은 동일합니다. 차이점은 각 규칙에 수행되는 작업이 정책마다 다를 수 있다는 점입니다.

규칙 작업을 변경하면 오탐이 지나치게 많이 발생하는 규칙을 비활성화하거나, 규칙에서 일치하는 트래픽을 알리거나 삭제할지 여부를 변경할 수 있습니다. 또한 비활성화된 규칙을 활성화하여 일치하는 트래픽을 알리거나 삭제할 수 있습니다.

규칙 작업을 변경하는 가장 쉬운 방법은 규칙 그룹의 보안 레벨을 변경하는 것입니다. 그룹의 보안 레벨을 변경하면 그룹 내 규칙의 작업이 변경됩니다. 즉, 선택한 보안 상태에 따라 일부 규칙이 활성화(또는 비활성화)되거나 작업이 알림과 삭제 간에 변경될 수 있습니다. 그러나 필요한 경우 개별 규칙 작업을 변경할 수 있습니다.

참고 지정된 규칙에 대한 기본 작업은 선택된 그룹 및 심각도 전체를 기반으로 합니다. 그룹의 심각도를 변경하거나 그룹을 제외하면 규칙에 대한 기본 작업이 변경될 수 있습니다.

시작하기 전에

맞춤형 규칙 그룹에는 보안 레벨이 없습니다. 보안 레벨 기술을 사용하여 맞춤형 규칙에 대한 규칙 작업을 변경할 수 없습니다.

프로시저

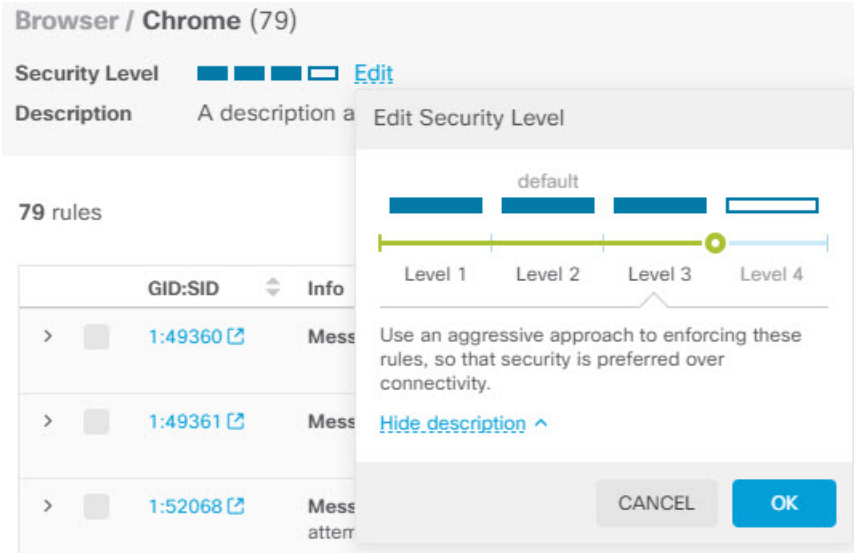
단계 **1** **Policies(**정책**)** > **Intrusion(**침입**)**을 선택합니다.

단계 **2** 변경하려는 규칙 작업이 있는 정책의 보기 아이콘( )을 클릭합니다.

단계 **3** (권장 방법) 규칙 그룹의 보안 레벨을 변경합니다.

a) 규칙 그룹 목록에서 하위 규칙 그룹을 클릭합니다.

b) 규칙 목록 위에서 그룹의 보안 레벨 옆에 있는 **Edit(**수정**)**를 클릭합니다.



참고 그룹의 모든 규칙을 비활성화하려면 **Edit(**수정**)**를 클릭하지 마십시오. 대신 **Exclude(**제외**)**를 클릭하여 그룹을 제외할 것임을 확인합니다. 그룹은 삭제되지 않으며 해당 규칙은 단순히 비활성화됩니다. 나머지 단계를 건너 뜁니다.

c) 그룹의 새 레벨을 선택합니다. **View Description(**설명 보기**)**을 클릭하여 각 레벨에 대한 설명을 선택하여 볼 수 있습니다.

레벨 1은 보안보다 연결을 강조하는 가장 덜 안전한 상태이며, 레벨 4는 최대한의 보안을 제공하는 가장 적극적인 보안 상태입니다.

d) **OK(**확인**)**를 클릭합니다.

단계 **4** (수동 방법) 하나 이상의 규칙에 대한 작업을 변경합니다.

a) 변경하려는 작업이 있는 규칙을 찾습니다.

Search/Filter(검색/필터**)** 상자를 사용하여 규칙 정보 내의 문자열을 검색합니다. GID 또는 SID의 조합에서 검색할 필터링 항목을 선택하거나 해당 작업(비활성, 알림, 삭제)을 기준으로 간단히 규칙을 표시할 수도 있습니다. 규칙은 느리게 로드되므로 필터링되지 않은 전체 목록을 스크롤하려면 시간이 조금 걸립니다. 목록을 필터링할 때 새로 고침 버튼을 클릭하여 필터링된 보기를 다시 로드합니다.

문제 해결 작업을 수행 중인 경우, 이벤트 또는 Cisco Technical Support를 통해 SID(Snort 식별자) 및 GID(생성기 식별자)를 제공받는 것이 가장 좋습니다. 그러면 규칙을 정확하게 검색할 수 있습니다.

b) 작업을 변경하려면 다음 중 하나를 수행합니다.

- 한 번에 하나의 규칙 변경 — 규칙의 **Action(**작업**)** 열을 클릭하고 필요한 작업을 선택합니다.
  - **Alert(**알림**)** — 이 규칙이 트래픽과 일치할 경우 이벤트를 생성하지만 연결을 삭제하지는 않습니다.
  - **Drop(**삭제**)** — 이 규칙이 트래픽과 일치할 경우 이벤트를 생성하고 연결도 삭제합니다.
  - **Disabled(**비활성화됨**)** — 트래픽을 이 규칙과 일치시키지 않습니다. 아무런 이벤트도 생성되지 않습니다.
- 한 번에 여러 규칙 변경 — 변경하려는 규칙의 체크 박스를 클릭한 다음, 테이블 위의 **Bulk(**대량**)** 드롭다운을 클릭하여 원하는 작업을 선택합니다. GID:SID 헤더의 체크 박스를 클릭하여 목록의 모든 규칙을 선택합니다. 한 번에 최대 5,000개의 규칙을 변경할 수 있습니다.

맞춤형 침입 규칙 및 규칙 그룹 관리

시스템에는 Cisco Talos Intelligence Group(Talos)에서 정의한 수천 개의 침입 규칙이 제공됩니다. 추가 공격에 대해 알고 있는 경우 맞춤형 침입 규칙을 생성 및 업로드하여 해당 공격을 차단하고 알림을 보내거나 삭제할 수 있습니다. 규칙을 한 번에 하나씩 생성, 편집 및 삭제할 수도 있습니다.

업로드된 규칙의 경우 텍스트 편집기를 사용하여 오프라인으로 규칙을 생성합니다. 업로드하는 각 텍스트 파일에 맞춤형 규칙 그룹을 포함하는 것이 좋습니다. 그런 다음 규칙에 변경 사항을 쉽게 업로드하고, 새 규칙을 맞춤형 규칙 그룹에 병합하거나, 규칙을 편집된 새 복사본으로 교체할 수 있습니다.

이러한 규칙을 생성하는 방법을 설명하는 것은 이 문서의 범위를 벗어납니다. Snort 2 규칙을 Snort 3 형식으로 변환하는 방법을 포함하여 Snort에 대한 침입 규칙을 작성하는 방법에 대한 자세한 내용은 https://snort.org/documents 가이드를 참조하십시오. https://snort.org/documents/rules-writers-guide-to-snort-3-rules의 규칙 작성자를 위한 *Snort 3* 규칙 작성 소개를 예로 들 수 있습니다.

시작하기 전에

맞춤형 침입 규칙 업로드, 577 페이지에서 설명하는 것과 같이 맞춤형 규칙을 업로드하는 프로세스 도중 또는 개별 규칙을 생성하거나 규칙 구성원 자격을 관리할 때 맞춤형 규칙 그룹을 생성합니다. 그룹을 생성한 후에는 그룹 및 그룹의 콘텐츠를 관리할 수 있습니다.

맞춤형 그룹은 그룹을 생성할 때 편집한 정책뿐만 아니라 모든 침입 정책에 사용할 수 있습니다. 따라서 그룹에 대한 변경 사항은 모든 정책에 적용됩니다. 예를 들어, 맞춤형 규칙 그룹을 삭제하면 모든 정책에서 삭제되며 더 이상 사용할 수 없습니다.

프로시저

단계 **1** **Policies(**정책**)** > **Intrusion(**침입**)**을 선택합니다.

단계 **2** 정책의 편집 아이콘()을 클릭합니다.

기본 제공 정책 중 하나가 아닌 맞춤형 침입 정책에 사용자 지정 규칙을 추가하는 것이 좋습니다.

단계 **3** 다음 중 하나를 수행합니다.

- 그룹을 생성하려면 **+** > **Upload Custom Rules(**맞춤형 규칙 업로드**)**를 클릭합니다. 맞춤형 침입 규칙 업로드, 577 페이지의 내용을 참조하십시오.
- 그룹의 이름 또는 설명을 편집하려면 User Defined Groups 폴더의 그룹 콘텐츠 테이블에서 그룹을 선택합니다. 이후 **Edit(**편집**)**를 클릭하고 변경합니다.
- 정책에서 그룹 및 그룹의 규칙을 제외하려면 User Defined Groups 폴더의 그룹 콘텐츠 테이블에서 그룹을 선택합니다. 이후 **Exclude(**제외**)**를 클릭하여 그룹을 제거할 수 있습니다.
- 시스템과 그룹을 사용하는 모든 정책에서 그룹을 삭제하려면 User Defined Groups 폴더의 그룹 콘텐츠 테이블에서 그룹을 선택합니다. 그런 다음 **Delete(**삭제**)**를 클릭합니다. 규칙이 삭제된 그룹에만 있는 경우 시스템에서도 삭제됩니다. 하지만 삭제하지 않은 다른 맞춤형 규칙 그룹에도 규칙이 있는 경우 규칙은 해당 그룹에서 그대로 유지됩니다.
- 그룹에서 규칙을 대량으로 교체하거나 업데이트하려면 User Defined Groups 폴더의 그룹 콘텐츠 테이블에서 그룹을 선택합니다. 그런 다음 그룹의 규칙 테이블 위에 있는 Action(작업) 드롭다운 목록에서 **Upload Rule File(**규칙 파일 업로드**)**을 클릭합니다. 해당 프로세스는 맞춤형 침입 규칙 업로드, 577 페이지에서 설명한 것과 동일합니다.
- 개별 규칙과 그룹에 대한 규칙 할당을 생성 및 관리하려면 개별 맞춤형 침입 규칙 설정, 580 페이지의 내용을 참조하십시오.

맞춤형 침입 규칙 업로드

현재 다른 규칙에서 처리하지 않는 공격에 대해 알고 있는 경우 맞춤형 침입 규칙을 생성 및 업로드하여 해당 공격을 차단하고 알림을 보내거나 삭제할 수 있습니다. 가져온 규칙의 작업은 알림 또는 삭제여야 하며, 규칙의 기본 작업은 가져온 파일의 작업에 의해 정의됩니다. 가져온 후에는 규칙 작업을 변경하고 필요한 경우 규칙을 비활성화할 수 있습니다.

이러한 규칙은 오프라인으로 생성해야 합니다. device manager에서는 단순히 규칙 파일을 업로드하는 것이며, 규칙을 직접 설정하지 않습니다. 규칙 파일은 텍스트 파일이어야 합니다. 줄바꿈을 사용하여 읽을 수 있도록 규칙의 형식을 지정하거나 한 줄에 규칙을 배치할 수 있으며, 빈 줄이 허용됩니다. 규칙 형식은 snort.org에서 설명합니다.

예를 들어 세 가지 규칙의 업로드 파일은 다음과 같이 표시될 수 있습니다.

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (
   msg: "My Custom Rule: EXPLOIT-KIT Styx exploit kit landing page request";
   flow:to_server,established;
   http_raw_uri;
   bufferlen:>100;
   http_uri;
   content:"/i.html?",depth 8; pcre:"/\/i\.html\?[a-z0-9]+\=[a-zA-Z0-9]{25}/";
   flowbits:set,styx_landing;
   metadata: copied from talos sid 29452;
   service:http;
   classtype:trojan-activity;
   gid:1;
   sid:1000000;
   rev:1;
)

alert tcp $HOME_NET 8811 -> $EXTERNAL_NET any (
   msg:"My Custom rule: MALWARE-BACKDOOR fear1.5/aciddrop1.0 runtime detection - initial
connection";
   flow:to_client,established;
   flowbits:isset,Fear15_conn.2;
   content:"Drive",nocase;
   metadata:copied from talos sid 7710;
   classtype:trojan-activity;
   gid:1;
   sid:1000001;
   rev:1;
)

alert tcp $EXTERNAL_NET $FILE_DATA_PORTS -> $HOME_NET any (
   msg:"My Custom Rule: INDICATOR-COMPROMISE download of a Office document with embedded
PowerShell";
   flow:to_client,established;
   flowbits:isset,file.doc;
   file_data;
   content:"powershell.exe",fast_pattern,nocase;
   metadata:copied from talos sid 37244;
   classtype:trojan-activity;
   gid:1;
   sid:1000002;
   rev:1;
)
```

프로시저

단계 **1** **Policies(**정책**)** > **Intrusion(**침입**)**을 선택합니다.

단계 **2** 정책의 편집 아이콘()을 클릭합니다.

기본 제공 정책 중 하나가 아닌 맞춤형 침입 정책에 사용자 지정 규칙을 추가하는 것이 좋습니다.

단계 **3** 다음 중 하나를 수행합니다.

- 그룹 목록 위에서 **+** > **Upload Custom Rules(**맞춤형 규칙 업로드**)**를 클릭합니다.
- 이미 생성한 맞춤형 규칙 그룹에 규칙을 업로드하는 경우 맞춤형 규칙 그룹을 선택하고 그룹의 규칙 테이블 위에 있는 **Action(**작업**)** 드롭다운 목록 옆에서 **Upload Rule File(**규칙 파일 업로드**)**을 클릭할 수 있습니다.

단계 **4** **Browse(**찾아보기**)**를 클릭하고 맞춤형 규칙 파일을 선택하거나 파일을 Upload File(파일 업로드) 대화상자에 끌어다 놓습니다.

업로드가 완료될 때까지 기다립니다.

단계 **5** 충돌을 처리할 방법을 선택합니다.

추가하는 규칙이 시스템에 이미 있는 규칙과 동일한 경우 충돌이 발생합니다. 이전에 업로드한 것과 동일한 규칙 또는 수정된 버전의 규칙을 업로드하는 경우에만 충돌이 발생합니다.

다음 옵션 중 하나를 선택합니다.

참고 **Merge(**병합**)**와 **Replace(**바꾸기**)**는 기본적으로 동일합니다. 기존 규칙을 변경하려면 업로드한 규칙의 개정 번호가 이전에 업로드한 규칙보다 높아야 합니다. 유일한 차이점은 업로드 파일에 대상 맞춤형 규칙 그룹에 있는 규칙이 없는 경우 **Replace(**바꾸기**)** 옵션은 규칙 그룹에서 해당 규칙을 삭제한다는 것입니다. **Merge(**병합**)** 옵션은 이러한 "없는" 규칙을 그대로 둡니다.

- **Merge(**병합**)** - 업로드된 파일에서 변경된 규칙이 선택한 그룹에도 있는 경우 업로드한 파일의 규칙이 개정 번호가 높다면 변경 사항이 병합됩니다. 변경되지 않은 규칙 또는 업로드에 해당 규칙이 없는 그룹의 규칙은 변경되지 않습니다. 업로드 시 모든 새 규칙이 추가됩니다. 이것이 기본 옵션입니다.
- **Replace(**바꾸기**)** - 업로드한 파일의 규칙이 개정 번호가 더 높은 경우 선택한 그룹의 규칙을 바꿉니다. 업로드된 파일에 없는 기존 규칙은 그룹에서 삭제됩니다. 업로드된 버전의 개정 번호가 같거나 낮은 기존 규칙은 변경되지 않습니다. 업로드 시 모든 새 규칙이 추가됩니다.

단계 **6** **+**를 클릭하고 업로드된 규칙에 대한 맞춤형 규칙 그룹을 선택합니다.

사용하고자 하는 맞춤형 규칙 그룹이 없는 경우 **Create New Group(**새 그룹 생성**)**을 클릭하여 바로 생성합니다. 새 그룹에는 이름과 설명(필요한 경우)이 필요합니다. 이후 새 그룹을 선택할 수 있습니다.

규칙을 바꾸는 경우 단일 그룹만 선택할 수 있습니다. 병합하는 경우 여러 그룹을 선택할 수 있습니다.

단계 **7** **OK(**확인**)**를 클릭합니다.

파일이 업로드되고 새 그룹에 배치됩니다. 업로드된 규칙 수와 업데이트, 삭제 또는 무시된 규칙 수에 대한 요약이 표시됩니다.

파일에 오류가 있으면 업로드가 실패합니다. 오류에 대한 자세한 정보를 보려면 **Download Error File(**다운로드 오류 파일**)** 링크를 클릭할 수 있습니다.

이 침입 정책에서 그룹이 자동으로 활성화됩니다. 그룹 및 새 규칙을 다른 정책에 추가할 수는 있지만 그룹 및 규칙은 다른 정책에서 자동으로 활성화되지 않습니다. 다른 정책에 그룹을 추가하는 방법

에 대한 자세한 내용은 침입 정책에서 규칙 그룹 추가 또는 제거(Snort 3), 572 페이지의 내용을 참고하십시오.

개별 맞춤형 침입 규칙 설정

맞춤형 침입 규칙은 대량 파일 업로드 대신 한 번에 하나씩 설정할 수 있습니다. 이 방법은 규칙을 빠르게 조정해야 하거나 한 번에 몇 개의 규칙만 만들거나 수정해야 하는 경우에 유용합니다.

침입 규칙을 설정할 때는 다음 사항에 유의하십시오.

- 모든 맞춤형 규칙의 GID는 1이어야 합니다.
- 규칙의 SID는 시스템의 모든 규칙에서 고유해야 합니다. 또한 1,000,000 이상이어야 합니다.
- 규칙을 편집하는 경우 규칙 버전을 변경해야 합니다. 일반적으로 버전 번호는 1 단위로 증가합니다.
- 고유한 버전의 규칙을 생성하기 위해 Cisco Talos Intelligence Group(Talos) 규칙을 복제할 수는 있지만 복제본의 SID를 고유하게 변경해야 합니다.

시스템에서 규칙의 형식이 올바른지 확인하기 위해 유효성 검사를 수행하며, 문제에 대한 오류 메시지가 표시됩니다. 하지만 규칙이 적절한지 여부는 시스템에서 확인할 수 없습니다.

Snort 2 규칙을 Snort 3 형식으로 변환하는 방법을 포함하여 Snort에 대한 침입 규칙을 작성하는 방법에 대한 자세한 내용은 https://snort.org/documents 가이드를 참조하십시오. https://snort.org/documents/rules-writers-guide-to-snort-3-rules의 규칙 작성자를 위한 *Snort 3* 규칙 작성 소개를 예로 들 수 있습니다.

프로시저

단계 **1** **Policies(**정책**)** > **Intrusion(**침입**)**을 선택합니다.

단계 **2** 정책의 편집 아이콘( )을 클릭합니다.

기본 제공 정책 중 하나가 아닌 맞춤형 침입 정책에 사용자 지정 규칙을 추가하는 것이 좋습니다.

단계 **3** 다음 중 하나를 수행합니다.

- 침입 규칙을 추가하려면 규칙 테이블 위에 있는 **Add Intrusion Rule(**침입 규칙 추가**)** 버튼(+)을 클릭합니다. 규칙을 추가할 때 새 규칙을 포함할 하나 이상의 맞춤형 규칙 그룹을 선택해야 합니다. 필요한 경우 규칙을 추가하면서 새 그룹을 생성할 수 있습니다.
- 기존 규칙을 복제하고 편집하여 규칙을 추가하려면 규칙의 오른쪽 끝에 마우스를 두고 Duplicate(복제) ( ) 버튼을 클릭합니다. 마우스를 올려둔 경우에만 버튼이 표시됩니다. 맞춤형 규칙의 경우 **Duplicate(**복제**)** 명령은 추가 옵션(**...**) 버튼에 있습니다.

- 맞춤형 규칙을 편집하려면 맞춤형 규칙 그룹에서 규칙을 찾고 편집() 버튼을 클릭합니다. 편집한 사항은 규칙이 있는 모든 그룹에 적용됩니다. 변경 시 규칙 버전 번호를 1 이상으로 늘려야 합니다.
- 맞춤형 규칙을 삭제하려면 해당 규칙의 삭제() 버튼을 클릭합니다. 규칙이 포함된 모든 규칙 그룹에서 규칙이 삭제됩니다. 그룹에서 규칙을 제거하려는 경우 규칙을 삭제하는 대신 **Manage Group Assignments(**그룹 할당 관리**)** 옵션을 사용합니다.
- 규칙을 포함하는 그룹을 변경하려면 추가 옵션(**...**) 버튼을 클릭하고 **Manage Group Assignment(**그룹 할당 관리**)**를 선택합니다. 그런 다음 그룹을 추가하거나 제거할 수 있습니다. 변경 사항은 그룹 구성원 자격에만 영향을 미치며, 규칙을 변경하거나 삭제하지 않습니다.

단계 **4** 새 규칙 및 그룹의 경우 정책에 규칙을 추가합니다.

새 규칙을 생성하거나 기존 규칙을 편집할 때 새 그룹을 생성하면 해당 그룹이 정책에 자동으로 추가되지 않으며 규칙이 자동으로 활성화되지도 않습니다. 편집 중인 정책에 그룹을 추가하라는 메시지가 표시됩니다. 규칙을 추가하거나 편집하는 동안 그룹을 추가하지 않는 경우 다음 프로세스를 사용하여 나중에 그룹을 추가할 수 있습니다.

a) 그룹 콘텐츠 테이블에서 + > **Add Existing Rule Group(**기존 규칙 그룹 추가**)**을 클릭합니다.
b) User Defined Groups 폴더에서 그룹을 찾고 선택한 다음 **OK(**확인**)**를 클릭합니다.
c) 콘텐츠 테이블에서 그룹을 선택하고 새 규칙이 그룹에 있으며 원하는 작업이 있는지 확인합니다.

침입 정책 관리(Snort 2)

사전 정의된 침입 정책을 적용할 수 있습니다. 이러한 각 정책에는 동일한 침입 규칙(서명이라고도 함) 목록이 포함되지만, 각 규칙에 시행되는 조치가 다릅니다. 예를 들어 어떤 규칙은 한 정책에서 활성 상태이지만, 다른 정책에서는 비활성 상태일 수 있습니다.

특정 규칙이 차단하지 말아야 할 트래픽을 차단하여 오탐(False Positive)이 지나치게 많이 발생하고 있다는 사실을 알게 될 경우, 보안이 더 낮은 침입 정책으로 전환하지 않고도 규칙을 비활성화할 수 있습니다. 또는 트래픽을 삭제하지 않고 일치 항목에 대해 알리도록 규칙을 변경할 수 있습니다.

이와 반대로, 특정 공격을 차단해야 하지만 선택한 침입 정책에서 관련 규칙이 비활성화된 경우, 보안이 더 높은 정책으로 변경하지 않고도 규칙을 활성화할 수 있습니다.

침입 관련 대시보드 및 이벤트 뷰어(두 가지 모두 **Monitoring(**모니터링**)** 페이지에서 제공)를 사용하여 침입 규칙이 트래픽에 어떤 영향을 미치는지 평가하십시오. 침입 이벤트와 침입 데이터는 알리거나 삭제하도록 설정된 침입 규칙과 일치하는 트래픽에 대해서만 표시됩니다. 즉, 비활성화된 규칙은 평가되지 않습니다.

다음 주제에서는 침입 정책 및 규칙 조정에 대해 자세히 설명합니다.

침입 정책을 위한 검사 모드 구성(Snort 2)

기본적으로 모든 침입 정책은 Prevention(차단) 모드에서 작동하여 IPS(침입 방지 시스템)를 구현합니다. Prevention(차단) 검사 모드에서 연결이 트래픽을 삭제하는 작업을 수행하는 침입 규칙과 일치하는 경우 연결이 능동적으로 차단됩니다.

대신 네트워크에서 침입 정책의 영향을 테스트하려는 경우, 모드를 IDS(침입 탐지 시스템)를 구현하는 모드를 Detection(탐지)로 변경할 수 있습니다. 이 검사 모드에서 삭제 규칙은 일치하는 연결에 대한 알림을 받는 알림 규칙처럼 처리되지만, 작업 결과는 Would Have Blocked(차단되었을 수 있음)가 되고 연결은 실제로 차단되지 않습니다.

침입 정책에 따라 검사 모드를 변경하면 차단 및 탐지를 혼합하여 사용할 수 있습니다.

프로시저

단계 **1** **Policies(**정책**)** > **Intrusion(**침입**)**을 선택합니다.

단계 **2** 검사 모드를 변경할 침입 정책의 탭을 클릭합니다.

Inspection Mode(검사 모드**)**는 규칙 테이블 위에 표시됩니다.

단계 **3** 검사 모드 옆의 **Edit(**수정**)** 링크를 클릭하고 정책에 대한 모드를 변경한 다음 **OK (**확인**)**를 클릭합니다.

옵션은 다음과 같습니다.

- **Prevention(**차단**)** - 침입 규칙 작업이 항상 적용됩니다. 삭제 규칙과 일치하는 연결이 차단됩니다.
- **Detection(**탐지**)** - 침입 규칙에서 알림만 생성합니다. 삭제 규칙과 일치하는 연결을 통해 알림 메시지가 생성되지만 연결은 차단되지 않습니다.

침입 규칙 작업 변경(Snort 2)

각각의 사전 정의된 침입 정책에는 동일한 규칙이 있습니다. 차이점은 각 규칙에 수행되는 작업이 정책마다 다를 수 있다는 점입니다.

규칙 작업을 변경하면 오탐이 지나치게 많이 발생하는 규칙을 비활성화하거나, 규칙에서 일치하는 트래픽을 알리거나 삭제할지 여부를 변경할 수 있습니다. 또한 비활성화된 규칙을 활성화하여 일치하는 트래픽을 알리거나 삭제할 수 있습니다.

프로시저

단계 **1** **Policies(**정책**)** > **Intrusion(**침입**)**을 선택합니다.

단계 **2** 변경하려는 규칙 작업이 있는 침입 정책의 탭을 클릭합니다.

사전 정의된 정책:

- Connectivity over Security(연결이 보안에 우선함)
- Balanced Security and Connectivity(균형 잡힌 보안 및 연결성)
- Security over Connectivity(보안이 연결에 우선함)
- Maximum Detection(최대 탐지)

단계 **3** 변경하려는 작업이 있는 규칙을 찾습니다.

규칙은 재정의된 규칙이 먼저 나열되고 재정의된 규칙의 그룹 내에 작업별로 정렬됩니다. 그렇지 않은 경우, 규칙은 GID별로 정렬된 다음 SID별로 정렬됩니다.

검색 상자를 사용하여 변경하려는 규칙을 찾습니다. 문제 해결 작업을 수행 중인 경우, 이벤트 또는 Cisco Technical Support를 통해 SID(Snort 식별자) 및 GID(생성기 식별자)를 제공받는 것이 가장 좋습니다.

각 규칙의 요소에 대한 자세한 내용은 침입 규칙 특성, 555 페이지의 내용을 참조하십시오.

목록을 검색하려면 다음을 수행합니다.

a) **Search(**검색**)** 상자를 클릭하여 검색 특성 대화 상자를 엽니다.
b) 생성기 ID(**GID**), Snort ID(**SID**) 또는 규칙 **Action(**작업**)**을 조합하여 입력하고 **Search(**검색**)**를 클릭합니다.

   예를 들어 **Action = Drop(**작업 = 삭제**)**을 선택하여 일치하는 연결을 삭제하는 정책 내의 모든 규칙을 볼 수 있습니다. 검색 상자 옆의 텍스트는 기준과 일치하는 규칙의 수를 나타내며, 이는 예를 들어 “8937 of 9416 rules found(9416개의 규칙 중 8937개 검색됨)”와 같이 표시됩니다.

   검색 기준을 지우려면 검색 상자에서 해당 기준의 x를 클릭합니다.

단계 **4** 규칙의 **Action(**작업**)** 열을 클릭하고 필요한 작업을 선택합니다.

- **Alert(**알림**)** — 이 규칙이 트래픽과 일치할 경우 이벤트를 생성하지만 연결을 삭제하지는 않습니다.
- **Drop(**삭제**)** — 이 규칙이 트래픽과 일치할 경우 이벤트를 생성하고 연결도 삭제합니다.
- **Disabled(**비활성화됨**)** — 트래픽을 이 규칙과 일치시키지 않습니다. 아무런 이벤트도 생성되지 않습니다.

규칙의 기본 작업은 작업에 추가되는 "(Default)(기본값)"으로 표시됩니다. 기본값을 변경하면 상태 열에 해당 규칙이 "Overridden(재정의됨)"으로 표시됩니다.

침입 정책 모니터링

침입 정책 통계는 **Monitoring(**모니터링**)** 페이지의 **Attackers(**공격자**)** 및 **Targets(**대상**)** 대시보드에서 확인할 수 있습니다. 이러한 대시보드에서 정보를 확인하려면 하나 이상의 액세스 제어 규칙에 침입 정책을 적용해야 합니다. 트래픽 및 시스템 대시보드 모니터링, 113 페이지의 내용을 참조하십시오.

침입 이벤트를 보려면 **Monitoring(**모니터링**)** > **Events(**이벤트**)**를 선택한 다음 **Intrusion(**침입**)** 탭을 클릭합니다. 이벤트에 마우스를 올려놓고 **View Details(**세부사항 보기**)** 링크를 클릭하면 더 자세한 정보를 얻을 수 있습니다. 세부 사항 페이지에서 **View IPS Rule(IPS** 규칙 보기**)**을 클릭하면 관련 침입 정책의 규칙으로 이동하여 규칙 작업을 변경할 수 있습니다. 이렇게 하면 작업을 삭제에서 알림으로 변경하여 규칙으로 인해 양호한 연결이 너무 많이 차단되는 오탐의 영향을 줄일 수 있습니다. 이와 반대로 규칙에 대한 공격 트래픽이 많이 표시되는 경우에는 알림 규칙을 삭제 규칙으로 변경할 수 있습니다.

침입 정책에 대한 syslog 서버를 컨피그레이션하는 경우, 침입 이벤트의 메시지 ID는 430001입니다.

침입 정책의 예시

사용 사례 장에는 침입 정책을 구현하는 다음의 예시가 포함되어 있습니다.

- 위협을 차단하는 방법, 57 페이지
- 네트워크에서 트래픽을 능동적으로 모니터링하는 방법, 79 페이지

23 장

NAT(네트워크 주소 변환)

다음 주제에서는 NAT(Network Address Tranlation)에 대한 내용 및 NAT를 구성하는 방법을 설명합니다.

NAT를 사용해야 하는 이유

IP 네트워크 내의 각 컴퓨터와 디바이스에는 호스트를 식별하는 고유한 IP 주소가 할당됩니다. 공용 IPv4 주소의 부족 때문에 이러한 IP 주소는 대부분 사설이며, 사설 회사 네트워크 외부로 라우팅되지 않습니다. RFC 1918의 정의에 따르면 사설 IP 주소는 내부적으로 사용할 수 있지만 외부에 알려서는 안 되는 주소입니다.

- 10.0.0.0~10.255.255.255
- 172.16.0.0 ~ 172.31.255.255
- 192.168.0.0~192.168.255.255

NAT의 주요 기능 중 하나는 사설 IP 네트워크가 인터넷에 연결되도록 하는 것입니다. NAT는 사설 IP 주소를 공용 IP 주소로 교체하여, 내부 사설 네트워크의 사설 주소를 공용 인터넷에서 사용할 수 있는 합법적이고 라우팅 가능한 주소로 전환합니다. 이렇게 하여 NAT는 공용 주소를 절약합니다. 전체 네트워크에 대해 최소 하나의 공용 주소만 외부에 알리도록 구성할 수 있기 때문입니다.

NAT의 기타 기능은 다음과 같습니다.

- 보안 - 직접 공격을 피할 수 있도록 내부 IP 주소를 숨깁니다.
- IP 라우팅 솔루션 - NAT를 사용하는 경우 중첩 IP 주소 문제가 발생하지 않습니다.

- 유연성 - 외부적으로 사용 가능한 공용 주소에 영향을 주지 않고 내부 IP 주소 지정 방식을 변경할 수 있습니다. 예를 들어 인터넷에 액세스할 수 있는 서버의 경우, 인터넷용으로는 고정 IP 주소를 유지하고 내부적으로는 서버 주소를 변경할 수 있습니다.
- IPv4와 IPv6 간 변환(라우팅된 방식 전용) - IPv6 네트워크를 IPv4 네트워크에 연결하려는 경우 NAT를 이용하면 두 가지 주소 유형 간에 변환할 수 있습니다.

참고 NAT는 필수 항목이 아닙니다. 특정 트래픽에 대해 NAT를 구성하지 않으면 해당 트래픽은 변환되지 않지만, 모든 보안 정책은 정상적으로 적용됩니다.

NAT 기본 사항

다음 주제에서는 NAT의 기본 사항 일부를 설명합니다.

NAT 용어

이 설명서는 다음과 같은 용어를 사용합니다.

- 실제 주소/호스트/네트워크/인터페이스 - 실제 주소는 변환되기 전 호스트에서 정의된 주소입니다. 외부에 액세스할 때 내부 네트워크를 변환하는 일반적인 NAT 시나리오에서는 내부 네트워크가 "실제" 네트워크일 수 있습니다. 내부 네트워크뿐 아니라 디바이스에 연결된 모든 네트워크를 변환할 수 있습니다. 따라서 외부 주소를 변환하도록 NAT를 구성하는 경우 "실제"는 내부 네트워크에 액세스하는 외부 네트워크를 지칭할 수 있습니다.
- 매핑된 주소/호스트/네트워크/인터페이스 - 매핑된 주소는 실제 주소가 변환되는 주소입니다. 외부에 액세스할 때 내부 네트워크를 변환하는 일반적인 NAT 시나리오에서는 외부 네트워크가 "매핑된" 네트워크일 수 있습니다.

참고 주소 변환 중에 디바이스 인터페이스용으로 구성된 IP 주소는 변환되지 않습니다.

- 양방향 시작 - 고정 NAT에서는 연결이 양방향으로 시작될 수 있습니다(호스트에서 나가기도 하고 호스트로 들어오기도 함).
- 소스 및 대상 NAT - 모든 패킷에 대해 소스 및 대상 IP 주소를 NAT 규칙과 비교하며, 하나 또는 둘 모두를 변환하거나 변환하지 않을 수 있습니다. 고정 NAT의 경우에는 규칙이 양방향이므로, 이 가이드 전체에서 명령 및 설명에 "source(소스)"와 "destination(대상)"이 사용됩니다. 특정 연결이 "destination(대상)" 주소에서 시작되는 경우에도 마찬가지입니다.

NAT 유형

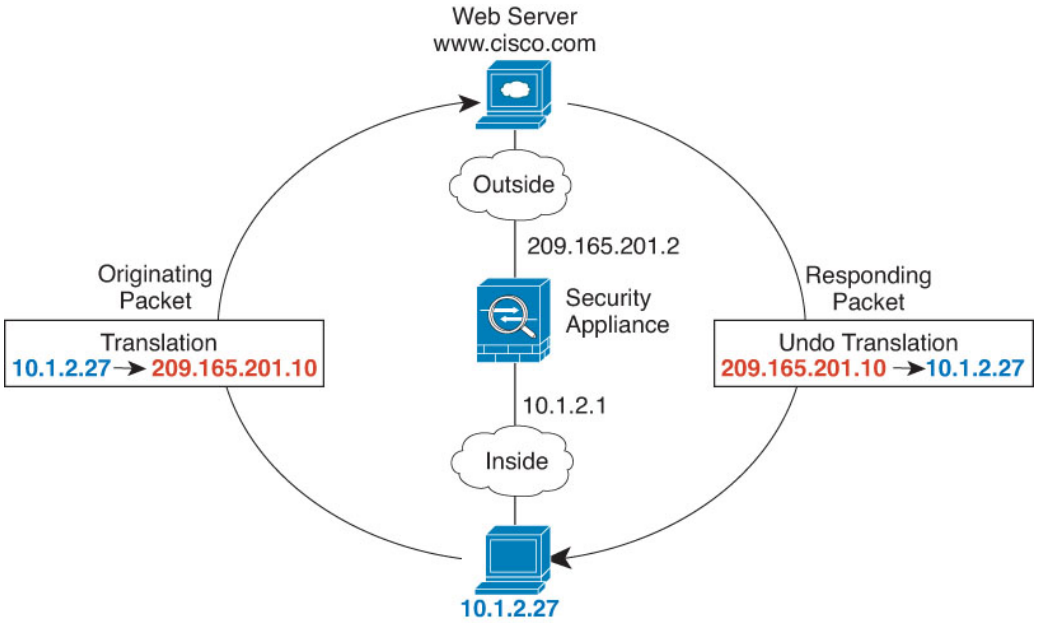
다음 방법을 사용하여 NAT를 구현할 수 있습니다.

- 동적 NAT - 실제 IP 주소의 그룹이 매핑된 IP 주소의 그룹(대개 더 작음)에 선착순으로 매핑됩니다. 실제 호스트만 트래픽을 시작할 수 있습니다. 동적 NAT, 599 페이지의 내용을 참조하십시오.
- 동적 PAT(동적 포트 주소 변환) - 실제 IP 주소의 그룹이 해당 IP 주소의 고유한 소스 포트를 사용하여 단일 IP 주소로 매핑됩니다. 동적 PAT, 604 페이지의 내용을 참조하십시오.
- 고정 NAT - 실제 IP 주소와 매핑된 IP 주소 간의 일관된 매핑입니다. 양방향 트래픽 시작이 허용됩니다. 고정 NAT, 609 페이지의 내용을 참조하십시오.
- ID NAT - 실제 주소가 기본적으로 NAT를 우회하여 자신에게 고정으로 변환됩니다. 대규모 주소 그룹을 변환하되 좀 더 작은 규모의 주소 하위 집합을 제외하고자 할 경우 이 방법으로 NAT를 구성할 수 있습니다. ID NAT, 618 페이지의 내용을 참조하십시오.

라우팅 모드의 NAT

다음 그림은 내부에 사설 네트워크가 있는 라우팅된 모드의 일반적인 NAT 예를 보여줍니다.

그림 ***33: NAT*** 예*:* 라우팅된 모드



1. 10.1.2.27의 내부 호스트가 웹 서버로 패킷을 전송하면, 패킷의 실제 소스 주소 10.1.2.27이 매핑된 주소 209.165.201.10으로 변환됩니다.
2. 서버가 응답하면 해당 호스트는 응답을 매핑된 주소 209.165.201.10으로 전송하며 위협 방지 디바이스에서 패킷을 수신합니다. 이는 위협 방지 디바이스에서 프록시 ARP를 수행하여 패킷을 신청하기 때문입니다.

3. 그런 다음 위협 방지 디바이스에서는 호스트로 전송하기 전에, 매핑된 주소 209.165.201.10에서 다시 실제 주소 10.1.2.27로의 변환을 변경합니다.

자동 **NAT** 및 수동 **NAT**

자동 *NAT* 및 수동 *NAT* 두 가지 방법으로 주소 변환을 구현할 수 있습니다.

수동 NAT에서 제공하는 추가 기능이 필요한 경우가 아니면 자동 NAT를 사용하는 것이 좋습니다. 자동 NAT가 컨피그레이션이 더 쉽고, VoIP(Voice over IP) 등의 애플리케이션에서 좀 더 안정적일 수 있습니다. VoIP의 경우 규칙에서 사용되는 개체 중 하나에 속하지 않는 간접 주소를 변환할 때 오류가 발생할 수 있습니다.

자동 **NAT**

네트워크 개체의 파라미터로 컨피그레이션되는 모든 NAT 규칙은 자동 *NAT* 규칙으로 간주됩니다. NAT 규칙을 사용하면 네트워크 개체에 대해 NAT를 빠르고 쉽게 구성할 수 있습니다. 그러나 그룹 개체에 대해서는 이러한 규칙을 생성할 수 없습니다.

이러한 규칙은 개체 자체의 일부분으로 구성되지만, 개체 관리자를 통해 개체 정의에서 NAT 컨피그레이션을 확인할 수는 없습니다.

패킷이 인터페이스로 들어가면 소스 및 대상 IP 주소 둘 다에서 자동 NAT 규칙을 확인합니다. 별도의 일치를 만든 경우 별도의 규칙을 통해 패킷의 소스 및 대상 주소를 변환할 수 있습니다. 이러한 규칙은 서로 연결되어 있지 않습니다. 트래픽에 따라 규칙의 서로 다른 조합을 사용할 수 있습니다.

규칙은 쌍을 이루지 않으므로 소스A/대상A가 소스A/대상B 이외의 다른 변환을 갖도록 지정할 수 없습니다. 이러한 종류의 기능이 필요한 경우 수동 NAT를 사용하십시오. 그러면 한 가지 규칙에서 소스 및 대상 주소를 식별할 수 있습니다.

수동 **NAT**

수동 NAT 한 가지 규칙에서 소스 및 대상 주소를 모두 식별할 수 있습니다. 소스 주소와 대상 주소를 모두 지정하면 소스A/대상A가 소스A/대상B 이외의 다른 변환을 갖도록 지정할 수 있습니다.

참고 고정 NAT의 경우에는 규칙이 양방향이므로, 이 가이드 전체에서 명령 및 설명에 "source(소스)"와 "destination(대상)"이 사용됩니다. 특정 연결이 "destination(대상)" 주소에서 시작되는 경우에도 마찬가지입니다. 예를 들어 포트 주소 변환 고정 NAT를 구성하고, 소스 주소를 텔넷 서버로 지정하며, 텔넷 서버로 이동하는 모든 트래픽에 대해 포트를 2323에서 23으로 변환하려면 소스 포트가 변환되도록 지정해야 합니다(실제 포트: 23, 매핑된 포트: 2323). 텔넷 서버 주소를 소스 주소로 지정했기 때문에 소스 포트를 지정하는 것입니다.

대상 주소는 선택 사항입니다. 대상 주소를 지정하는 경우 이를 대상 주소 자신에게 매핑할 수도 있고(ID NAT) 다른 주소에 매핑할 수도 있습니다. 대상 주소 매핑은 항상 고정 매핑입니다.

자동 NAT와 수동 NAT 비교

이 두 NAT 유형의 주요 차이점은 다음과 같습니다.

- 실제 주소를 정의하는 방법
  - 자동 NAT - NAT 규칙은 네트워크 개체의 파라미터가 됩니다. 네트워크 개체 IP 주소는 원래(실제) 주소 역할을 합니다.
  - 수동 NAT- 실제 주소와 매핑된 주소 모두에서 네트워크 개체 또는 네트워크 개체 그룹을 식별합니다. 이 경우 NAT는 네트워크 개체의 매개변수가 아닙니다. 네트워크 개체 또는 그룹은 NAT 컨피그레이션의 매개변수입니다. 실제 주소에 네트워크 개체 그룹을 사용할 수 있으므로 수동 NAT의 확장성이 더 뛰어납니다.
- 소스 및 대상 NAT의 구현 방법
  - 자동 NAT- 각 규칙을 패킷의 소스 또는 대상에 적용할 수 있습니다. 따라서 소스 IP 주소와 대상 IP 주소에 각각 하나씩 두 개의 규칙이 사용될 수 있습니다. 소스/대상조합에 특정 변환을 적용하기 위해 이러한 두 규칙을 결합할 수 없습니다.
  - 수동 NAT단일 규칙에서 소스와 대상을 모두 변환합니다. 패킷은 하나의 규칙에서만 일치하며, 더 이상 규칙이 점검되지 않습니다. 선택적 대상 주소를 컨피그레이션하지 않더라도 일치하는 패킷은 여전히 하나의 수동 NAT 규칙과만 일치합니다. 소스와 대상이 결합되어 있으므로, 소스/대상조합에 따라 서로 다른 변환을 적용할 수 있습니다. 예를 들어 소스A/대상A의 변환은 소스A/대상B의 변환과 다를 수 있습니다.
- NAT 규칙의 순서
  - 자동 NAT- NAT 테이블에서 자동으로 순서가 지정됩니다.
  - 수동 NAT - NAT 테이블에서 수동으로 순서가 지정됩니다(자동 NAT 규칙 앞이나 뒤).

NAT 규칙 순서

자동 NAT 및 수동 NAT 규칙은 세 개의 섹션으로 구분되는 단일 테이블에 저장됩니다. 섹션 1 규칙이 먼저 적용된 다음, 일치가 발견될 때까지 섹션 2, 마지막으로 섹션 3이 적용됩니다. 예를 들어 섹션 1에서 일치가 발견되면 섹션 2와 3은 평가되지 않습니다. 다음 표는 각 섹션 내의 규칙 순서를 보여줍니다.

참고 섹션 0에는 시스템이 자체적으로 사용하기 위해 생성하는 NAT 규칙이 포함되어 있습니다. 이러한 규칙은 다른 모든 규칙보다 우선순위가 높습니다. 시스템은 이러한 규칙을 자동으로 생성하고 필요에 따라 xlate를 지웁니다. 섹션 0에 있는 규칙을 추가, 편집 또는 수정할 수 없습니다.

표 ***11: NAT*** 규칙 테이블

테이블 섹션	규칙 유형	섹션 내 규칙의 순서
섹션 1	수동 NAT	첫 번째 일치부터 컨피그레이션에 나타나는 순서대로 적용됩니다. 첫 번째 일치가 적용되므로, 일반 규칙 앞에 특수 규칙이 오도록 해야 합니다. 그렇지 않으면 특수 규칙이 원하는 대로 적용되지 않을 수 있습니다. 기본적으로 수동 NAT 규칙은 섹션 1에 추가됩니다. "특정 규칙 우선"이라는 의미는 다음과 같습니다. • 정적 규칙이 동적 규칙 앞에 와야 합니다. • 대상 변환을 포함한 규칙은 소스 변환만을 포함한 규칙보다 앞에 와야 합니다. 소스 또는 대상 주소를 기반으로 둘 이상의 규칙이 적용될 수 있는 중복 규칙을 제거할 수 없는 경우에는 특히 주의하여 이러한 권장 사항을 따르십시오.
섹션 2	자동 NAT	섹션 1에서 일치하는 항목을 찾을 수 없으면 섹션 2 규칙이 다음 순서로 적용됩니다. **1.** 고정 규칙 **2.** 동적 규칙 각 규칙 유형 내에서는 다음의 순서 지침이 사용됩니다**.** **1.** 실제 IP 주소의 수량 - 가장 적은 것에서 가장 많은 것. 예를 들면 주소가 1개인 개체가 주소가 10개인 개체보다 먼저 평가됩니다. **2.** 수량이 동일한 경우 IP 주소 번호가 낮은 것에서 높은 것 순으로 사용됩니다. 예를 들면, 10.1.1.0이 11.1.1.0보다 먼저 평가됩니다. **3.** IP 주소가 동일한 경우 네트워크 개체의 이름이 알파벳순으로 사용됩니다. 예를 들면 abracadabra가 catwoman보다 먼저 평가됩니다.
섹션 3	수동 NAT	아직도 일치가 발견되지 않으면 섹션 3 규칙이 첫 번째부터 컨피그레이션에 나타나는 순서대로 적용됩니다. 이 섹션에는 가장 일반적인 규칙을 포함해야 합니다. 또한 이 섹션에서는 특정 규칙이 일반 규칙보다 먼저 적용되도록 해야 합니다.

예를 들어 섹션 2 규칙의 경우 네트워크 개체 내에서 다음 IP 주소를 정의합니다.

• 192.168.1.0/24(고정)

- 192.168.1.0/24(동적)
- 10.1.1.0/24(고정)
- 192.168.1.1/32(고정)
- 172.16.1.0/24(동적)(개체 def)
- 172.16.1.0/24(동적)(개체 abc)

결과 순서는 다음과 같습니다.

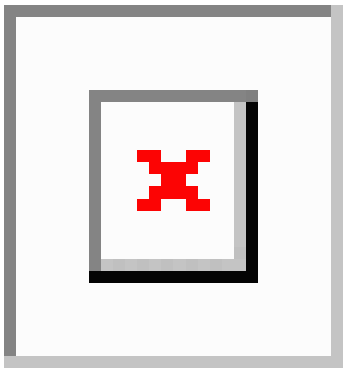
- 192.168.1.1/32(고정)
- 10.1.1.0/24(고정)
- 192.168.1.0/24(고정)
- 172.16.1.0/24(동적)(개체 abc)
- 172.16.1.0/24(동적)(개체 def)
- 192.168.1.0/24(동적)

NAT 인터페이스

브리지 그룹 멤버 인터페이스를 제외한 임의의 인터페이스(즉, 모든 인터페이스)에 적용할 NAT 규칙을 구성할 수도 있고, 특정 실제 및 매핑된 인터페이스를 지정할 수도 있습니다. 실제 주소에는 임의의 인터페이스를 지정하고, 매핑된 주소에는 특정 인터페이스를 지정하거나, 그 반대로 지정할 수도 있습니다.

예를 들어, 여러 인터페이스에서 동일한 사설 주소를 사용하며, 외부에 액세스할 때 이들을 모두 동일한 전역 풀로 변환하려는 경우 실제 주소에는 임의의 인터페이스를 지정하고, 매핑된 주소에는 외부 인터페이스를 지정할 수 있습니다.

그림 ***34:*** 임의의 인터페이스 지정



그러나 브리지 그룹 멤버 인터페이스에는 "any" 인터페이스라는 개념이 적용되지 않습니다. "any" 인터페이스를 지정하면 모든 브리지 그룹 멤버 인터페이스는 제외됩니다. 따라서 브리지 그룹 멤버에 NAT를 적용하려면 멤버 인터페이스를 지정해야 합니다. 이렇게 하면 유사한 여러 규칙에서 인터페

이스 하나만 다른 현상이 발생할 수 있습니다. BVI(브리지 가상 인터페이스) 자체에 대해서는 NAT를 구성할 수 없으며 멤버 인터페이스에 대해서만 NAT를 구성할 수 있습니다.

패시브 인터페이스에서는 NAT를 구성할 수 없습니다.

NAT 라우팅 구성

threat defense 디바이스는 변환(매핑)된 주소로 전송되는 모든 패킷의 대상이어야 합니다.

패킷을 전송할 때 디바이스는 대상 인터페이스를 지정한 경우 해당 인터페이스를 사용하고, 그렇지 않으면 라우팅 테이블 조회를 사용하여 이그레스 인터페이스를 결정합니다. ID NAT의 경우에는 대상 인터페이스를 지정하더라도 경로 조회를 사용하는 옵션이 있습니다.

필요한 라우팅 컨피그레이션의 유형은 다음 항목에서 설명하는 것처럼 매핑된 주소의 유형에 따라 다릅니다.

매핑된 인터페이스와 동일한 네트워크의 주소

대상(매핑된) 인터페이스와 동일한 네트워크의 주소를 사용하는 경우, 위협 방지 디바이스에서는 매핑된 주소에 대한 ARP 요청에 응답하기 위해 프록시 ARP를 사용하며, 이에 따라 매핑된 주소로 가야 하는 트래픽을 가로챕니다. 위협 방지 디바이스가 추가 네트워크에 대한 게이트웨이가 될 필요가 없으므로 이 솔루션은 라우팅을 간소화합니다. 이 솔루션은 외부 네트워크에 적절한 수의 여유 주소가 있는 경우 이상적이며, 동적 NAT 또는 고정 NAT 등 1:1 변환을 사용하는 경우 고려해볼 수 있습니다. 동적 PAT는 소수의 주소로 사용 가능한 변환의 수를 크게 확장합니다. 따라서 외부 네트워크에 사용 가능한 주소가 적어도 이 방법을 사용할 수 있습니다. PAT의 경우 매핑된 인터페이스의 IP 주소를 사용할 수도 있습니다.

고유한 네트워크의 주소

대상(매핑된) 인터페이스 네트워크에서 사용할 수 있는 것보다 더 많은 주소가 필요한 경우 별도의 서브넷에서 주소를 지정할 수 있습니다. 업스트림 라우터에는 위협 방지 디바이스를 가리키는, 매핑된 주소에 대한 고정 경로가 필요합니다.

실제 주소와 동일한 주소(ID NAT)

ID NAT의 기본 동작은 프록시 ARP를 활성화하고 기타 고정 NAT 규칙을 확인하는 것입니다. 원하는 경우 프록시 ARP를 사용 해제할 수 있습니다. 원하는 경우 정기적인 고정 NAT에 대해 프록시 ARP를 사용 해제할 수도 있습니다. 이 경우 업스트림 라우터에 적절한 경로가 있어야 합니다.

일반적으로 ID NAT에는 프록시 ARP가 필요하지 않으며, 프록시 ARP를 사용할 경우 연결 문제가 발생할 수도 있습니다. 예를 들어 "any" IP 주소에 대해 광범위한 ID NAT 규칙을 구성하고 프록시 ARP를 사용하는 상태로 두면 매핑된 인터페이스에 직접 연결된 네트워크에서 호스트 문제가 발생할 수 있습니다. 이 경우 매핑된 네트워크의 호스트가 동일한 네트워크의 다른 호스트와 통신하려면 ARP 요청의 주소가 NAT 규칙과 일치해야 합니다("any" 주소와 일치). 패킷이 실제로 위협 방지 디바이스로 이동하도록 지정되지 않아도 위협 방지 디바이스에서는 주소에 대해 프록시 ARP를 수행합니다. (이 문제는 수동 NAT 규칙이 있는 경우에도 발생합니다. NAT 규칙은 소스 주소 및 대상 주소와 모두 일치해야 하지만 프록시 ARP 결정은 "소스" 주소에 대해서만 내려집니다.) 실제 호스트 ARP 응답 전에 위협 방지 디바이스 ARP 응답을 수신하는 경우, 트래픽이 위협 방지 디바이스로 잘못 전송됩니다.

NAT용 지침

다음 주제에서는 NAT 구현에 대한 자세한 지침을 제공합니다.

인터페이스 지침

NAT는 표준 라우팅 물리적 또는 하위 인터페이스에 대해 지원됩니다.

그러나 브리지 그룹 멤버 인터페이스, 즉 BVI(브리지 가상 인터페이스)에 속하는 인터페이스에 대해 NAT를 구성할 때는 다음과 같은 제한이 있습니다.

- 브리지 그룹 멤버에 대해 NAT를 구성할 때는 멤버 인터페이스를 지정합니다. BVI(브리지 그룹 인터페이스) 자체에 대해서는 NAT를 구성할 수 없습니다.
- 브리지 그룹 멤버 인터페이스 간에 NAT를 수행할 때는 소스 및 대상 인터페이스를 지정해야 합니다. 인터페이스로 "any"를 지정할 수는 없습니다.
- 대상 인터페이스가 브리지 그룹 멤버 인터페이스일 때는 인터페이스 PAT를 구성할 수 없습니다. 인터페이스에 연결된 IP 주소가 없기 때문입니다.
- 소스 및 대상 인터페이스가 동일한 브리지 그룹의 멤버이면 IPv4 및 IPv6 네트워크(NAT64/46) 간을 변환할 수 없습니다. 지원되는 방법은 고정 NAT/PAT 44/66, 동적 NAT44/66 및 동적 PAT44 뿐이며 동적 PAT66은 지원되지 않습니다.

IPv6 NAT 지침

NAT는 다음 지침 및 제약 사항과 함께 IPv6를 지원합니다.

- 표준 라우팅 모드 인터페이스에서는 IPv4와 IPv6 간을 변환할 수도 있습니다.
- 동일한 브리지 그룹의 멤버인 인터페이스에 대해서는 IPv4 및 IPv6 간을 변환할 수 없습니다. 두 IPv6 또는 두 IPv4 네트워크 간에만 변환을 수행할 수 있습니다. 이 제한은 브리지 그룹 멤버와 표준 라우팅 인터페이스 간에는 적용되지 않습니다.
- 같은 브리지 그룹의 인터페이스 간 변환에는 IPv6에 대해 동적 PAT(NAT66)를 사용할 수 없습니다. 이 제한은 브리지 그룹 멤버와 표준 라우팅 인터페이스 간에는 적용되지 않습니다.
- 고정 NAT에서는 IPv6 서브넷을 최대 /64까지 지정할 수 있습니다. 더 큰 서브넷은 지원되지 않습니다.
- FTP with NAT46을 사용할 때, IPv4 FTP 클라이언트가 IPv6 FTP 서버에 연결될 때 클라이언트는 확장 패시브 모드(EPSV) 또는 확장 포트 모드(EPRT)를 사용해야 하며, PASV 및 PORT 명령은 IPv6에서 지원되지 않습니다.

IPv6 NAT 모범 사례

IPv6 네트워크 간 변환 및 IPv4와 IPv6 네트워크 간 변환(라우팅된 모드 전용)을 위해 NAT를 사용할 수 있습니다. 다음의 모범 사례를 권장합니다.

- NAT66(IPv6-IPv6) - 고정 NAT를 사용하는 것이 좋습니다. 동적 NAT 또는 PAT를 사용할 수 있고 IPv6 주소가 대량으로 공급되지만, 동적 NAT를 반드시 사용할 필요는 없습니다. 반환 트래픽을 허용하지 않으려면 정적 NAT 규칙을 단방향으로 설정할 수 있습니다(수동 NAT에만 해당함).
- NAT46(IPv4-IPv6) - 고정 NAT를 사용하는 것이 좋습니다. IPv6 주소 공간이 IPv4 주소 공간보다 훨씬 크기 때문에 고정 변환을 손쉽게 수용할 수 있습니다. 반환 트래픽을 허용하지 않으려면 정적 NAT 규칙을 단방향으로 설정할 수 있습니다(수동 NAT에만 해당함). IPv6 서브넷(/96 이하)으로 변환하면 결과로 나타나는 매핑된 주소는 기본적으로 IPv4가 포함된 IPv6 주소입니다. 이 경우 IPv6 접두사 뒤에 IPv4 주소의 32비트가 포함됩니다. 예를 들어 IPv6 접두사가 /96 접두사이면, 주소의 마지막 32비트에 IPv4 주소가 첨부됩니다. 예를 들어 192.168.1.0/24를 201b::0/96에 매핑하면 192.168.1.4는 201b::0.192.168.1.4(혼합된 표기로 표시됨)에 매핑됩니다. 접두사가 더 작으면(예: /64) IPv4 주소가 접두사 뒤에 첨부되고, 접미사 0이 IPv4 주소 뒤에 첨부됩니다.
- NAT64(IPv6-to-IPv4) - IPv6 주소의 수를 수용할 만큼 IPv4 주소가 충분하지 않을 수 있습니다. 대량의 IPv4 변환을 제공하려면 동적 PAT 풀을 사용하는 것이 좋습니다.

검사된 프로토콜에 대한 NAT 지원

보조 연결을 열거나 패킷에 IP 주소를 포함한 일부 애플리케이션 레이어 프로토콜을 검사하여 다음 서비스를 제공합니다.

- 핀홀 생성 - 일부 애플리케이션 프로토콜은 표준 포트 또는 협상된 포트에서 보조 TCP 또는 UDP 연결을 엽니다. 검사에서는 이러한 보조 포트를 허용하기 위한 액세스 제어 규칙을 생성할 필요가 없도록 해당 포트에 대해 핀홀을 엽니다.
- NAT 재작성 - FTP 등의 프로토콜은 프로토콜의 일부분으로 패킷 데이터에 보조 연결용 IP 주소 및 포트를 포함합니다. 엔드포인트 중 하나에서 NAT 변환이 수행되는 경우 검사 엔진은 포함된 주소와 포트의 NAT 변환을 반영하기 위해 패킷 데이터를 재작성합니다. NAT 재작성이 수행되지 않으면 보조 연결은 작동하지 않습니다.
- 프로토콜 적용 - 일부 검사에서는 검사된 프로토콜에 대해 특정 수준의 RFC 적합성을 적용합니다.

다음 표에는 NAT 재작성을 적용하는 검사된 프로토콜 및 이러한 프로토콜의 NAT 제한이 나와 있습니다. 이러한 프로토콜을 포함하는 NAT 규칙을 작성할 때는 이와 같은 제한에 주의해야 합니다. 여기에 나와 있지 않은 검사된 프로토콜은 NAT 재작성을 적용하지 않습니다. 이러한 검사에는 GTP, HTTP, IMAP, POP, SMTP, SSH 및 SSL이 포함됩니다.

참고 NAT 재작성은 여기에 나와 있는 포트에서만 지원됩니다. 비표준 포트에서 이러한 프로토콜을 사용하는 경우에는 연결에 NAT를 사용하지 마십시오.

표 ***12: NAT***가 지원되는 애플리케이션 검사

애플리케이션	검사된 프로토콜, 포트	**NAT** 제한	핀홀 생성 여부
DCERPC	TCP/135	NAT64 없음	예
DNS over UDP	UDP/53	WINS를 통한 이름 확인에 NAT 지원을 이용할 수 없음	아니요
ESMTP	TCP/25	NAT64 없음	아니요
FTP	TCP/21	제한 없음	예
H.323 H.225(호출 신호) H.323 RAS	TCP/1720 UDP/1718 RAS의 경우 UDP/1718-1719	NAT64 없음	예
ICMP ICMP Error	ICMP (디바이스 인터페이스로 전달된 ICMP 트래픽은 검사되지 않음)	제한 없음	아니요
IP Options	RSVP	NAT64 없음	아니요
NetBIOS Name Server over IP	UDP/137, 138(소스 포트)	NAT64 없음	아니요
RSH	TCP/514	PAT 없음 NAT64 없음	예
RTSP	TCP/554 (HTTP 클로킹을 처리하지 않음)	NAT64 없음	예
SIP	TCP/5060 UDP/5060	확장 PAT 없음 NAT64 또는 NAT46 없음	예
Skinny(SCCP)	TCP/2000	NAT64, NAT46 또는 NAT66 없음	예
SQL*Net (버전 1, 2)	TCP/1521	NAT64 없음	예
Sun RPC	TCP/111 UDP/111	NAT64 없음	예

애플리케이션	검사된 프로토콜, 포트	NAT 제한	핀홀 생성 여부
TFTP	UDP/69	NAT64 없음 페이로드 IP 주소는 변환되지 않습니다.	예
XDMCP	UDP/177	NAT64 없음	예

FQDN 대상 지침

IP 주소 대신 정규화된 도메인 이름(FQDN) 네트워크 개체를 사용하여 수동 NAT 규칙에서 변환된(매핑된) 대상을 지정할 수 있습니다. 예를 들어 www.example.com 웹 서버로 향하는 트래픽을 기반으로 규칙을 생성할 수 있습니다.

FQDN을 사용할 때 시스템은 DNS 확인을 가져오고 반환된 주소를 기반으로 NAT 규칙을 작성합니다. DNS 서버에서 둘 이상의 주소를 가져오는 경우 사용되는 주소는 다음을 기반으로 합니다.

- 지정된 인터페이스와 동일한 서브넷에 주소가 있으면 해당 주소가 사용됩니다. 동일한 서브넷에 없는 경우 반환된 첫 번째 주소가 사용됩니다.
- 변환된 소스 및 변환된 대상의 IP 유형이 일치해야 합니다. 예를 들어 변환된 소스 주소가 IPv6인 경우 FQDN 개체는 IPv6를 주소 유형으로 지정해야 합니다. 변환된 소스가 IPv4인 경우 FQDN 개체는 IPv4를 지정하거나 IPv4 및 IPv6을 모두 지정할 수 있습니다. 이 경우 IPv4 주소가 선택됩니다.

수동 NAT 대상에 사용되는 네트워크 그룹에는 FQDN 개체를 포함할 수 없습니다. NAT에서는 단일 대상 호스트만 이 유형의 NAT 규칙에 적합하므로 FQDN 개체만 사용해야 합니다.

FQDN을 IP 주소로 확인할 수 없는 경우에는 DNS 확인을 얻을 때까지 규칙이 작동하지 않습니다.

NAT 추가 지침

- 브리지 그룹 멤버인 인터페이스의 경우 멤버 인터페이스용 NAT 규칙을 작성합니다. BVI(브리지 가상 인터페이스) 자체에 대해서는 NAT 규칙을 작성할 수 없습니다.
- 사이트 대 사이트 VPN에서 사용되는 VTI(Virtual Tunnel Interface)에 대해서는 NAT 규칙을 작성할 수 없습니다. VTI의 소스 인터페이스에 대해 규칙을 작성하면 VPN 터널에 NAT가 적용되지 않습니다. VTI에서 터널링된 VPN 트래픽에 적용할 NAT 규칙을 작성하려면 "any"를 인터페이스로 사용해야 합니다. 인터페이스 이름을 명시적으로 지정할 수 없습니다.
- (자동 NAT에만 해당함.) 한 개체에는 단일 NAT 규칙만 정의할 수 있습니다. 한 개체에 대해 여러 NAT 규칙을 구성하려면 동일한 IP 주소를 지정하는 서로 다른 이름의 여러 개체를 생성해야 합니다.
- 인터페이스에 VPN이 정의되어 있으면 인터페이스의 인바운드 ESP 트래픽에는 NAT 규칙이 적용되지 않습니다. 시스템은 설정된 VPN 터널에 대해서만 ESP 트래픽을 허용하며 기존 터널과 연결되지 않은 트래픽은 삭제합니다. 이러한 제한은 ESP 및 UDP 포트 500과 4500에 적용됩니다.

- UDP 포트 500 및 4500이 실제로 사용되지 않도록 동적 PAT를 적용하는 디바이스 뒤에 있는 디바이스에서 사이트 대 사이트 VPN을 정의하는 경우에는 PAT 디바이스 뒤의 디바이스에서 연결을 시작해야 합니다. 응답자는 정확한 포트 번호를 모르므로 SA(보안 연결)를 시작할 수 없습니다.
- NAT 컨피그레이션을 변경할 때 새 NAT 컨피그레이션이 사용되기 전에 기존 변환이 시간 초과되기까지 기다리지 않으려면 디바이스 CLI에서 **clear xlate** 명령을 사용하여 변환 테이블을 지울 수 있습니다. 그러나 변환 테이블을 지우면 변환을 사용하는 현재의 모든 연결이 해제됩니다.

  기존 연결(예: VPN 터널)에 적용해야 하는 새 NAT 규칙을 생성하는 경우 **clear conn** 사용을 통해 연결을 종료해야 합니다. 그런 다음 연결 재설정 시도가 NAT 규칙에 도달해야 하며 연결이 NAT에 올바르게 연결되어야 합니다.

참고 동적 NAT 또는 PAT 규칙을 제거한 후 제거된 규칙의 주소와 중복되는 매핑된 주소가 포함된 새 규칙을 추가하는 경우, 새 규칙을 사용하려면 제거된 규칙과 관련된 모든 연결이 시간 초과되기까지 기다리거나 **clear xlate** 또는 **clear conn** 명령으로 해당 연결을 지워야 합니다. 이러한 안전 조치는 동일한 주소가 여러 호스트에 할당되는 것을 방지합니다.

- IPv4 및 IPv6 주소를 모두 포함하는 개체 그룹은 사용할 수 없습니다. 개체 그룹에는 한 가지 주소 유형만 포함해야 합니다.
- NAT에서 사용되는 네트워크 개체는 주소 범위 또는 서브넷에서 명시적으로 또는 묵시적으로 131,838개 이상의 IP 주소를 포함할 수 없습니다. 주소 공간을 더 작은 범위로 분할하고 더 작은 개체에 대해 별도의 규칙을 작성합니다.
- (수동 NAT에만 해당함.) NAT 규칙에서 **any**를 소스 주소로 사용하는 경우 "any" 트래픽의 정의(IPv4 대 IPv6)는 규칙에 따라 다릅니다. 위협 방지 디바이스가 패킷에 대해 NAT를 수행하기 전에 패킷은 IPv6-IPv6 또는 IPv4-IPv4여야 합니다. 이 전제 조건하에 위협 방지 디바이스는 NAT 규칙에서 **any**의 값을 결정할 수 있습니다. 예를 들어 **any**에서 IPv6 서버로 규칙을 구성하며 해당 서버가 IPv4 주소에서 매핑된 것이면 any는 "모든 IPv6 트래픽"을 의미합니다. “any” 에서 “any”로 규칙을 구성하며 소스를 인터페이스 IPv4 주소로 매핑하면 **any**는 “모든 IPv4 트래픽”을 의미합니다. 매핑된 인터페이스 주소는 대상 주소도 IPv4임을 암시하기 때문입니다.
- 여러 NAT 규칙에서 동일한 매핑된 개체 또는 그룹을 사용할 수 있습니다.
- 매핑된 IP 주소 풀에는 다음을 포함할 수 없습니다.
  - 매핑된 인터페이스 IP 주소. 규칙에 대해 "any" 인터페이스를 지정하면 모든 인터페이스 IP 주소가 허용되지 않습니다. 인터페이스 PAT(라우팅 모드만 해당함)의 경우 인터페이스 주소 대신 인터페이스 이름을 사용합니다.
  - 페일오버 인터페이스 IP 주소
  - (동적 NAT) VPN이 활성화된 경우의 스탠바이 인터페이스 IP 주소

- 고정 및 동적 NAT 정책에서는 겹치는 주소 사용을 피해야 합니다. 예를 들어, PPTP의 보조 연결이 동적 xlate 대신 고정 상태인 경우 겹치는 주소를 사용하면 PPTP 연결 설정에 실패할 수 있습니다.
- NAT 규칙의 소스 주소와 원격 액세스 VPN 주소 풀에서는 겹치는 주소를 사용할 수 없습니다.
- 규칙에서 대상 인터페이스를 지정하는 경우에는 라우팅 테이블에서 경로를 조회하지 않고 해당 인터페이스를 이그레스 인터페이스로 사용합니다. 그러나 ID NAT의 경우에는 경로 조회를 대신 사용할 수 있는 옵션이 제공됩니다.
- NAT는 통과 트래픽에만 적용됩니다. 시스템에서 생성된 트래픽에는 NAT가 적용되지 않습니다.
- 대문자 또는 소문자 조합을 사용하여 네트워크 개체 또는 그룹 pat-pool의 이름을 지정하지 마십시오.
- PIM(Protocol Independent Multicast) 레지스터의 내부 페이로드에는 NAT를 사용할 수 없습니다.
- (수동 NAT) 이중 ISP 인터페이스 설정(라우팅 구성에서 SLA를 사용하는 기본 및 백업 인터페이스)에 대한 NAT 규칙을 작성할 때 규칙에서 대상 기준을 지정하지 마십시오. 기본 인터페이스에 대한 규칙이 백업 인터페이스에 대한 규칙 앞에 와야 합니다. 이렇게 하면 기본 ISP를 사용할 수 없을 때 디바이스가 현재 라우팅 상태를 기반으로 올바른 NAT 대상 인터페이스를 선택할 수 있습니다. 대상 개체를 지정하면 NAT 규칙은 중복 규칙에 대해 항상 기본 인터페이스를 선택합니다.
- 인터페이스에 대해 정의된 NAT 규칙과 일치하지 않아야 하는 트래픽에 대해 ASP 삭제 이유 nat-no-xlate-to-pat-pool이 표시되는 경우, 트래픽이 변환되지 않은 상태로 통과할 수 있도록 영향을 받는 트래픽에 대한 ID NAT 규칙을 구성합니다.

NAT 구성

네트워크 주소 변환은 매우 복잡해질 수 있습니다. 따라서 변환 문제와 까다로운 트러블슈팅 상황을 방지하기 위해 규칙을 최대한 단순하게 유지하는 것이 좋습니다. 그리고 NAT를 구현하기 전에 면밀한 계획을 세워야 합니다. 다음 절차에서는 기본적인 구성 방식에 대해 설명합니다.

프로시저

단계 **1** **Policies(**정책**)** > **NAT**를 선택합니다.

단계 **2** 필요한 규칙의 종류를 결정합니다.

동적 NAT, 동적 PAT, 고정 NAT 및 ID NAT 규칙을 생성할 수 있습니다. 이와 관련된 개요는 NAT 유형, 587 페이지를 참조하십시오.

단계 **3** 수동 또는 자동 NAT로 구현할 규칙을 결정합니다.

이 두 가지 구현 옵션을 비교한 내용은 자동 NAT 및 수동 NAT, 588 페이지를 참조하십시오.

단계 **4** 다음 섹션에서 설명하는 대로 규칙을 생성합니다.

- 동적 NAT, 599 페이지
- 동적 PAT, 604 페이지
- 고정 NAT, 609 페이지
- ID NAT, 618 페이지

단계 **5** NAT 정책 및 규칙을 관리합니다.

다음을 수행하여 정책과 해당 규칙을 관리할 수 있습니다.

- 규칙을 수정하려면 해당 규칙의 수정 아이콘( )을 클릭합니다.
- 규칙을 삭제하려면 해당 규칙의 삭제 아이콘( )을 클릭합니다.

동적 NAT

다음 주제에서는 동적 NAT 및 동적 NAT를 구성하는 방법에 대해 설명합니다.

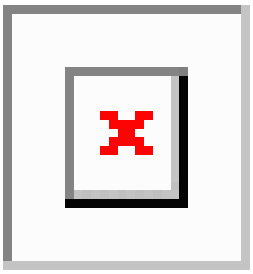
동적 NAT 정보

동적 NAT는 실제 주소의 그룹을 대상 네트워크에서 라우팅 가능한 매핑된 주소의 풀로 변환합니다. 매핑된 풀에는 일반적으로 실제 그룹보다 더 적은 수의 주소가 포함되어 있습니다. 변환하려는 호스트가 대상 네트워크에 액세스하면 NAT에서는 매핑된 풀의 IP 주소를 호스트에 할당합니다. 실제 호스트가 연결을 시작하는 경우에만 변환이 생성됩니다. 변환은 연결되어 있는 동안에만 이루어지며, 변환 시간이 초과된 후에는 사용자의 IP 주소가 동일하게 유지되지 않습니다. 따라서 액세스 규칙에서 연결을 허용하더라도, 대상 네트워크의 사용자는 동적 NAT를 사용하는 호스트에 대해 안정적인 연결을 시작할 수 없습니다.

참고 액세스 규칙에서 허용하는 경우, 변환 기간 동안 원격 호스트는 변환된 호스트로의 연결을 시작할 수 있습니다. 주소는 예측할 수 없으므로 호스트로의 연결이 실패할 수 있습니다. 그럼에도 불구하고 이 경우 사용자는 액세스 규칙의 보안에 의존할 수 있습니다.

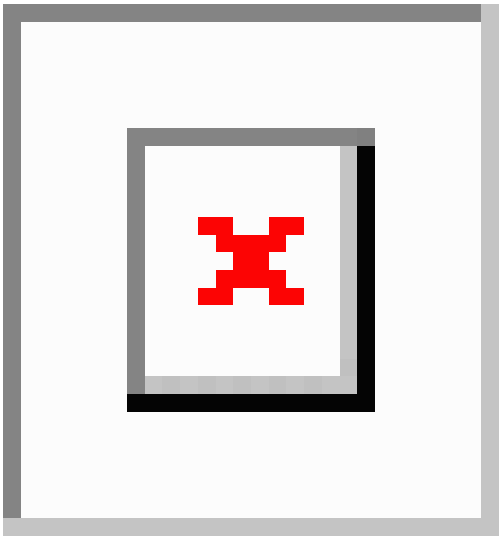
다음 그림은 일반적인 동적 NAT 시나리오를 보여줍니다. 실제 호스트만 NAT 세션을 생성할 수 있으며 응답 트래픽이 허용됩니다.

그림 35: 동적 NAT



다음 그림은 매핑된 주소로 연결을 시작하려고 시도하는 원격 호스트를 보여줍니다. 이 주소는 현재 변환 테이블에 있지 않으므로 패킷이 삭제됩니다.

그림 36: 매핑된 주소로 연결을 시작하려고 시도하는 원격 호스트



동적 NAT의 단점 및 장점

동적 NAT의 단점은 다음과 같습니다.

- 매핑된 풀의 주소 수가 실제 그룹의 주소 수보다 적은 경우, 트래픽의 양이 예상보다 많아지면 주소가 부족해질 수 있습니다.

  PAT는 단일 주소의 포트를 사용하여 64,000이 넘는 변환을 제공하므로, 이러한 상황이 발생하면 PAT 또는 PAT 대안을 사용하십시오.

- 매핑된 풀에서 대량의 라우팅 가능한 주소를 사용해야 하는데, 라우팅 가능한 주소는 대량으로 사용 가능하지 않을 수 있습니다.

동적 NAT의 장점은 일부 프로토콜이 PAT를 사용할 수 없다는 것입니다. PAT는 다음과 작동하지 않습니다.

- GRE 버전 0과 같이 오버로드할 포트가 없는 IP 프로토콜

- 한 포트에 데이터 스트림이 있고 다른 포트에 제어 경로가 있으며 개방형 표준이 아닌 일부 멀티미디어 애플리케이션

동적 자동 NAT 구성

동적 자동 NAT 규칙을 사용하여 주소를 대상 네트워크에서 라우팅할 수 있는 서로 다른 IP 주소로 변환합니다.

시작하기 전에

개체를 선택하여 규칙에 필요한 네트워크 개체 또는 그룹을 생성합니다. NAT 규칙을 정의하면서 개체를 생성할 수도 있습니다. 개체는 다음 요건을 충족해야 합니다.

- 원본 주소 — 이 주소는 그룹이 아닌 네트워크 개체여야 하며 호스트, 범위 또는 서브넷일 수 있습니다.
- 변환된 주소 — 이 주소는 네트워크 개체 또는 그룹일 수는 있지만 서브넷을 포함할 수는 없습니다. IPv4 주소와 IPv6 주소를 모두 포함할 수는 없으며 한 유형만 포함해야 합니다. 그룹에 범위와 호스트 IP 주소가 모두 포함되어 있으면 범위는 동적 NAT에 사용되고 호스트 IP 주소는 PAT 대안으로 사용됩니다.

프로시저

단계 **1** **Policies(**정책**)** > **NAT**를 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 새 규칙을 생성하려면 **+** 버튼을 클릭합니다.
- 기존 규칙을 수정하려면 해당 규칙의 수정 아이콘( )을 클릭합니다.

더 이상 필요하지 않은 규칙을 삭제하려면 해당 규칙의 휴지통 아이콘을 클릭합니다.

단계 **3** 기본 규칙 옵션을 구성합니다.

- **Title(**제목**)** — 규칙의 이름을 입력합니다.
- **Creat Rule For(**규칙 생성**)** — 자동 **NAT**를 선택합니다.
- **Type(**유형**)** — 동적을 선택합니다.

단계 **4** 다음 패킷 변환 옵션을 구성합니다.

- 소스 인터페이스, 대상 인터페이스 — (브리지 그룹 멤버 인터페이스의 경우 필수) 이 NAT 규칙을 적용할 인터페이스입니다. **Source(**소스**)**는 트래픽이 디바이스로 들어가는 데 사용되는 실제 인터페이스입니다. **Destination(**대상**)**은 트래픽이 디바이스에서 나오는 데 사용되는 매핑된 인터페이스입니다. 기본적으로 규칙은 브리지 그룹 멤버 인터페이스를 제외한 모든 인터페이스(**Any(**모두**)**)에 적용됩니다.
- 원본 주소 — 변환하는 주소가 포함된 네트워크 개체입니다.
- 변환된 주소 — 매핑된 주소를 포함하는 네트워크 개체 또는 그룹입니다.

단계 **5** (선택 사항). 고급 옵션 링크를 클릭하고 원하는 옵션을 선택합니다.

- 이 규칙과 일치하는 **DNS** 회신 변환 - DNS 응답의 IP 주소를 변환할지 여부를 선택합니다. 매핑된 인터페이스에서 실제 인터페이스로 이동하는 DNS 응답의 경우 주소(IPv4 A 또는 IPv6 AAAA) 레코드가 매핑된 값에서 실제 값으로 재작성됩니다. 반대로, 실제 인터페이스에서 매핑된 인터페이스로 이동하는 DNS 응답의 경우 실제 값에서 매핑된 값으로 레코드가 재작성됩니다. 이 옵션은 특정 상황에서 사용되며, 재작성 시 A 레코드와 AAAA 레코드 간의 변환도 수행되는 NAT64/46 변환에 필요한 경우도 있습니다. 자세한 내용은 NAT를 사용하여 DNS 쿼리 및 응답 재작성, 663 페이지를 참조하십시오.
- 인터페이스 **PAT(**대상 인터페이스**)**로 폴스루 - 다른 매핑된 주소가 이미 할당된 경우 대상 인터페이스의 IP 주소를 백업 방법으로 사용할지 여부를 선택합니다(인터페이스 PAT 대체). 이 옵션은 브리지 그룹의 멤버가 아닌 대상 인터페이스를 선택한 경우에만 사용할 수 있습니다.

단계 **6** **OK(**확인**)**를 클릭합니다.

동적 수동 NAT 구성

자동 NAT가 요구를 충족하지 않을 때는 동적 수동 NAT 규칙을 사용합니다. 대상에 따라 다른 변환을 수행하려는 경우를 예로 들 수 있습니다. 동적 NAT는 주소를 대상 네트워크에서 라우팅할 수 있는 서로 다른 IP 주소로 변환합니다.

시작하기 전에

개체를 선택하여 규칙에 필요한 네트워크 개체 또는 그룹을 생성합니다. 그룹은 IPv4 주소와 IPv6 주소를 모두 포함할 수는 없으며 한 유형만 포함해야 합니다. NAT 규칙을 정의하면서 개체를 생성할 수도 있습니다. 개체는 다음 요건도 충족해야 합니다.

- 원본 소스 주소 - 이 주소는 네트워크 개체 또는 그룹일 수 있으며 호스트, 범위 또는 서브넷을 포함할 수 있습니다. 모든 원본 소스 트래픽을 변환하려는 경우 이 단계를 건너뛰고 규칙에서 **Any(**모두**)**를 지정하면 됩니다.
- 변환된 소스 주소 - 이 주소는 네트워크 개체 또는 그룹일 수는 있지만 서브넷을 포함할 수는 없습니다. IPv4 주소와 IPv6 주소를 모두 포함할 수는 없으며 한 유형만 포함해야 합니다. 그룹에 범위와 호스트 IP 주소가 모두 포함되어 있으면 범위는 동적 NAT에 사용되고 호스트 IP 주소는 PAT 대안으로 사용됩니다.

규칙에서 원본 대상 주소 및 변환된 대상 주소에 대해 정적 변환을 구성하는 경우 이러한 주소에 대해 네트워크 개체를 생성할 수도 있습니다.

동적 NAT의 경우 대상에 대해 포트 변환을 수행할 수도 있습니다. 개체 관리자에서 원본 대상 포트 및 변환된 대상 포트에 사용할 수 있는 포트 개체가 있는지 확인합니다. 소스 포트를 지정하면 무시됩니다.

프로시저

단계 **1** **Policies(**정책**)** > **NAT**를 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 새 규칙을 생성하려면 **+** 버튼을 클릭합니다.
- 기존 규칙을 수정하려면 해당 규칙의 수정 아이콘( )을 클릭합니다.

더 이상 필요하지 않은 규칙을 삭제하려면 해당 규칙의 휴지통 아이콘을 클릭합니다.

단계 **3** 기본 규칙 옵션을 구성합니다.

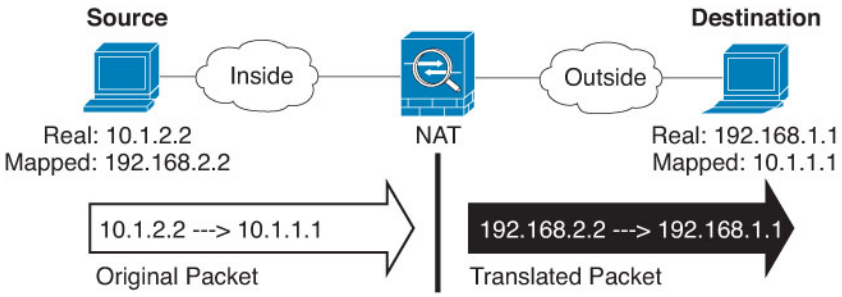
- **Title(**제목**)** — 규칙의 이름을 입력합니다.
- **Create Rule for(**규칙 생성**)** - 수동 **NAT**를 선택합니다.
- **Rule Placement(**규칙 배치**)** - 규칙을 추가할 위치를 선택합니다. 규칙은 카테고리에서 자동 NAT 규칙 앞이나 뒤에 삽입할 수도 있고, 선택한 규칙 위나 아래에 삽입할 수도 있습니다.
- **Type(**유형**)** - 동적을 선택합니다. 이 설정은 소스 주소에만 적용됩니다. 대상 주소에 대해 변환을 정의하는 경우 변환은 항상 고정입니다.

단계 **4** 다음 인터페이스 옵션을 구성합니다.

- 소스 인터페이스, 대상 인터페이스 — (브리지 그룹 멤버 인터페이스의 경우 필수) 이 NAT 규칙을 적용할 인터페이스입니다. **Source(**소스**)**는 트래픽이 디바이스로 들어가는 데 사용되는 실제 인터페이스입니다. **Destination(**대상**)**은 트래픽이 디바이스에서 나오는 데 사용되는 매핑된 인터페이스입니다. 기본적으로 규칙은 브리지 그룹 멤버 인터페이스를 제외한 모든 인터페이스(**Any(**모두**)**)에 적용됩니다.

단계 **5** 원본 패킷 주소(IPv4 또는 IPv6)를 식별합니다. 이 주소는 원본 패킷에 표시되는 패킷 주소입니다.

원래 패킷 대 변환된 패킷의 예는 다음 그림을 참조하십시오.



- **Original Source Address(**원본 소스 주소**)** - 변환 중인 주소가 포함된 네트워크 개체 또는 그룹입니다.
- **Original Destination Address(**원본 대상 주소**)** - (선택 사항) 대상의 주소를 포함하는 네트워크 개체입니다. 이 옵션을 비워 두면 대상에 관계없이 소스 주소 변환이 적용됩니다. 대상 주소를 지정하면 해당 주소에 대해 고정 변환을 구성할 수도 있고 단순히 ID NAT를 사용할 수도 있습니다.

  Interface(인터페이스**)**를 선택하여 소스 인터페이스(Any(모두)일 수 없음)를 기준으로 원본 대상을 지정할 수 있습니다. 이 옵션을 선택할 경우 변환된 대상 개체도 선택해야 합니다. 대상 주소에 대해 포트 변환 고정 인터페이스 NAT를 구현하려면 이 옵션을 선택하고 대상 포트에 대해 적절한 포트 개체도 선택합니다.

단계 **6** 변환된 패킷 주소(IPv4 또는 IPv6), 즉 대상 인터페이스 네트워크에 나타나는 패킷 주소를 확인합니다. 필요에 따라 IPv4 및 IPv6 간에 변환할 수 있습니다.

- 변환된 소스 주소 - 매핑된 주소를 포함하는 네트워크 개체 또는 그룹입니다.
- 변환된 대상 주소 - (선택 사항) 변환된 패킷에서 사용되는 대상 주소를 포함하는 네트워크 개체 또는 그룹입니다. 원본 대상 주소에 대해 개체를 선택한 경우 동일한 개체를 선택하여 ID NAT(변환 없음)를 설정할 수 있습니다.

단계 **7** (선택 사항). 서비스 변환용 대상 서비스 포트(**Original Destination Port(**원본 대상 포트**)**, **Translated Destination Port(**변환된 대상 포트**)**)를 식별합니다.

동적 NAT는 포트 변환을 지원하지 않으므로 **Original Destination Port(**원본 대상 포트**)** 및 **Translated Destination Port(**변환된 대상 포트**)** 필드를 비워 둡니다. 그러나 대상 변환은 항상 고정이므로 대상 포트의 포트 변환을 수행할 수 있습니다.

NAT는 TCP 또는 UDP만 지원합니다. 포트를 변환할 때는 실제 서비스 개체의 프로토콜과 매핑된 서비스 개체의 프로토콜이 동일해야 합니다(둘 다 TCP거나 둘 다 UDP). ID NAT의 경우 실제 포트와 매핑된 포트에 동일한 서비스 개체를 사용할 수 있습니다.

단계 **8** (선택 사항). 고급 옵션 링크를 클릭하고 원하는 옵션을 선택합니다.

- 이 규칙과 일치하는 **DNS** 회신 변환 - DNS 응답의 IP 주소를 변환할지 여부를 선택합니다. 매핑된 인터페이스에서 실제 인터페이스로 이동하는 DNS 응답의 경우 주소(IPv4 A 또는 IPv6 AAAA) 레코드가 매핑된 값에서 실제 값으로 재작성됩니다. 반대로, 실제 인터페이스에서 매핑된 인터페이스로 이동하는 DNS 응답의 경우 실제 값에서 매핑된 값으로 레코드가 재작성됩니다. 이 옵션은 특정 상황에서 사용되며, 재작성 시 A 레코드와 AAAA 레코드 간의 변환도 수행되는 NAT64/46 변환에 필요한 경우도 있습니다. 자세한 내용은 NAT를 사용하여 DNS 쿼리 및 응답 재작성, 663 페이지를 참조하십시오.
- 인터페이스 **PAT(**대상 인터페이스**)**로 폴스루 - 다른 매핑된 주소가 이미 할당된 경우 대상 인터페이스의 IP 주소를 백업 방법으로 사용할지 여부를 선택합니다(인터페이스 PAT 대체). 이 옵션은 브리지 그룹의 멤버가 아닌 대상 인터페이스를 선택한 경우에만 사용할 수 있습니다.

단계 **9** **OK(**확인**)**를 클릭합니다.

동적 PAT

다음 주제에서는 동적 PAT에 대해 설명합니다.

동적 PAT 정보

동적 PAT는 실제 주소 및 소스 포트를 매핑된 주소 및 고유한 포트로 변환함으로써 여러 실제 주소를 단일 매핑된 IP 주소로 변환합니다.

소스 포트는 각 연결에 대해 다르므로 연결마다 별도의 변환 세션이 필요합니다. 예를 들어 10.1.1.1:1025를 사용하려면 10.1.1.1:1026에서 별도로 변환해야 합니다.

다음 그림은 일반적인 동적 PAT 시나리오를 보여줍니다. 실제 호스트만 NAT 세션을 생성할 수 있으며 응답 트래픽이 허용됩니다. 매핑된 주소는 각 변환에 대해 동일하지만 포트는 동적으로 할당됩니다.

그림 *37:* 동적 ***PAT***

액세스 규칙에서 허용하는 경우, 변환 기간 동안 대상 네트워크의 원격 호스트는 변환된 호스트로의 연결을 시작할 수 있습니다. 포트 주소(실제 및 매핑된 주소 모두)는 예측할 수 없으므로 호스트에 대한 연결이 실패할 수 있습니다. 그럼에도 불구하고 이 경우 사용자는 액세스 규칙의 보안에 의존할 수 있습니다.

연결이 만료되면 포트 변환도 만료됩니다.

참고 각 인터페이스에 각기 다른 PAT 풀을 사용하는 것이 좋습니다. 여러 인터페이스에 동일한 풀을 사용하는 경우, 특히 "any" 인터페이스에 동일한 풀을 사용하는 경우에 풀이 빠르게 소진될 수 있어 새 변환에 포트를 사용할 수 없게 됩니다.

동적 PAT의 단점 및 장점

동적 PAT에서는 단일 매핑된 주소를 사용하여 라우팅 가능한 주소를 아낄 수 있습니다. 위협 방지 디바이스 인터페이스 IP 주소를 PAT 주소로서 사용할 수도 있습니다. 그러나 인터페이스의 IPv6 주소에 대해서는 인터페이스 PAT를 사용할 수 없습니다.

같은 브리지 그룹의 인터페이스 간 변환에는 IPv6에 대해 동적 PAT(NAT66)를 사용할 수 없습니다. 이 제한은 브리지 그룹 멤버와 표준 라우팅 인터페이스 간에는 적용되지 않습니다.

데이터 스트림이 제어 경로와 다른 일부 멀티미디어 애플리케이션에서는 동적 PAT가 작동하지 않습니다. 자세한 내용은 검사된 프로토콜에 대한 NAT 지원, 594 페이지를 참조하십시오.

동적 PAT는 단일 IP 주소에서 오는 것처럼 보이는 대량의 연결을 생성할 수 있으며, 서버는 이 트래픽을 DoS 공격으로 해석할 수 있습니다.

동적 자동 PAT 구성

동적 자동 PAT 규칙을 사용하여 주소를 여러 IP 주소만으로 변환하는 대신 고유한 IP 주소/포트 조합으로 변환합니다. 단일 주소(대상 인터페이스의 주소 또는 다른 주소)로 변환할 수 있습니다.

시작하기 전에

개체를 선택하여 규칙에 필요한 네트워크 개체 또는 그룹을 생성합니다. NAT 규칙을 정의하면서 개체를 생성할 수도 있습니다. 개체는 다음 요건을 충족해야 합니다.

- 원본 주소 — 이 주소는 그룹이 아닌 네트워크 개체여야 하며 호스트, 범위 또는 서브넷일 수 있습니다.
- 변환된 주소 - 다음 옵션을 사용하여 PAT 주소를 지정할 수 있습니다.
  - 대상 인터페이스 - 대상 인터페이스 IPv4 주소를 사용하려는 경우 네트워크 개체가 필요하지 않습니다. IPv6에는 인터페이스 PAT를 사용할 수 없습니다.
  - 단일 **PAT** 주소 - 단일 호스트를 포함하는 네트워크 개체를 생성합니다.

프로시저

단계 **1** **Policies(**정책**)** > **NAT**를 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 새 규칙을 생성하려면 **+** 버튼을 클릭합니다.
- 기존 규칙을 수정하려면 해당 규칙의 수정 아이콘()을 클릭합니다.

더 이상 필요하지 않은 규칙을 삭제하려면 해당 규칙의 휴지통 아이콘을 클릭합니다.

단계 **3** 기본 규칙 옵션을 구성합니다.

- **Title(**제목**)** — 규칙의 이름을 입력합니다.
- **Creat Rule For(**규칙 생성**)** — 자동 **NAT**를 선택합니다.
- **Type(**유형**)** — 동적을 선택합니다.

단계 **4** 다음 패킷 변환 옵션을 구성합니다.

- 소스 인터페이스, 대상 인터페이스 — (브리지 그룹 멤버 인터페이스의 경우 필수) 이 NAT 규칙을 적용할 인터페이스입니다. **Source(**소스**)**는 트래픽이 디바이스로 들어가는 데 사용되는 실제 인터페이스입니다. **Destination(**대상**)**은 트래픽이 디바이스에서 나오는 데 사용되는 매핑된 인터페이스입니다. 기본적으로 규칙은 브리지 그룹 멤버 인터페이스를 제외한 모든 인터페이스(**Any(**모두**)**)에 적용됩니다.
- 원본 주소 — 변환하는 주소가 포함된 네트워크 개체입니다.
- 변환된 주소 - 다음 중 하나입니다.
  - (인터페이스 PAT) 대상 인터페이스의 IPv4 주소를 사용하려면 인터페이스를 선택합니다. 특정 대상 인터페이스도 선택해야 합니다. 이 인터페이스는 브리지 그룹 멤버 인터페이스일 수 없습니다. IPv6에는 인터페이스 PAT를 사용할 수 없습니다.
  - 대상 인터페이스 주소가 아닌 단일 주소를 사용하려면 이러한 용도로 생성한 호스트 네트워크 개체를 선택합니다.

단계 **5** (선택 사항). 고급 옵션 링크를 클릭하고 원하는 옵션을 선택합니다.

- 인터페이스 **PAT(**대상 인터페이스**)**로 폴스루 - 다른 매핑된 주소가 이미 할당된 경우 대상 인터페이스의 IP 주소를 백업 방법으로 사용할지 여부를 선택합니다(인터페이스 PAT 대체). 이 옵션은 브리지 그룹의 멤버가 아닌 대상 인터페이스를 선택한 경우에만 사용할 수 있습니다. 인터페이스 PAT를 변환된 주소로 이미 컨피그레이션한 경우에는 이 옵션을 선택할 수 없습니다. 또한 IPv6 네트워크에서는 이 옵션을 사용할 수 없습니다.

단계 **6** **OK(**확인**)**를 클릭합니다.

동적 수동 **PAT** 구성

자동 PAT가 요구를 충족하지 않을 때는 동적 수동 PAT 규칙을 사용합니다. 대상에 따라 다른 변환을 수행하려는 경우를 예로 들 수 있습니다. 동적 PAT는 주소를 여러 IP 주소만으로 변환하는 대신 고유한 IP 주소/포트 조합으로 변환합니다. 단일 주소(대상 인터페이스의 주소 또는 다른 주소)로 변환할 수 있습니다.

시작하기 전에

개체를 선택하여 규칙에 필요한 네트워크 개체 또는 그룹을 생성합니다. 그룹은 IPv4 주소와 IPv6 주소를 모두 포함할 수는 없으며 한 유형만 포함해야 합니다. NAT 규칙을 정의하면서 개체를 생성할 수도 있습니다. 개체는 다음 요건도 충족해야 합니다.

- 원본 소스 주소 - 이 주소는 네트워크 개체 또는 그룹일 수 있으며 호스트, 범위 또는 서브넷을 포함할 수 있습니다. 모든 원본 소스 트래픽을 변환하려는 경우 이 단계를 건너뛰고 규칙에서 **Any(**모두**)**를 지정하면 됩니다.
- 변환된 소스 주소 - 다음 옵션을 사용하여 PAT 주소를 지정할 수 있습니다.
  - 대상 인터페이스 - 대상 인터페이스 IPv4 주소를 사용하려는 경우 네트워크 개체가 필요하지 않습니다. IPv6에는 인터페이스 PAT를 사용할 수 없습니다.
  - 단일 **PAT** 주소 - 단일 호스트를 포함하는 네트워크 개체를 생성합니다.

규칙에서 원본 대상 주소 및 변환된 대상 주소에 대해 정적 변환을 구성하는 경우 이러한 주소에 대해 네트워크 개체를 생성할 수도 있습니다.

동적 PAT의 경우 대상에 대해 포트 변환을 수행할 수도 있습니다. 개체 관리자에서 원본 대상 포트 및 변환된 대상 포트에 사용할 수 있는 포트 개체가 있는지 확인합니다. 소스 포트를 지정하면 무시됩니다.

프로시저

단계 **1** **Policies(**정책**)** > **NAT**를 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 새 규칙을 생성하려면 **+** 버튼을 클릭합니다.

- 기존 규칙을 수정하려면 해당 규칙의 수정 아이콘( )을 클릭합니다.

더 이상 필요하지 않은 규칙을 삭제하려면 해당 규칙의 휴지통 아이콘을 클릭합니다.

단계 **3** 기본 규칙 옵션을 구성합니다.

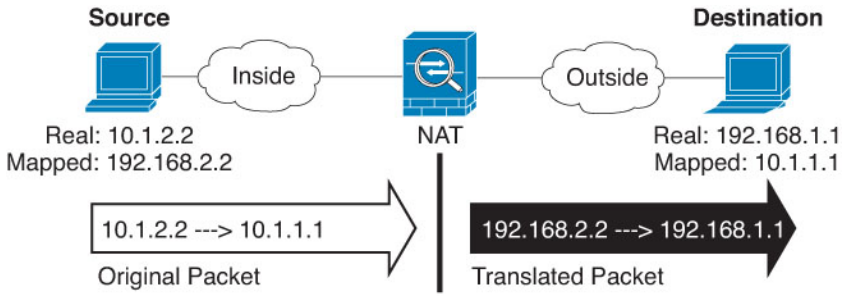
- **Title(**제목**)** — 규칙의 이름을 입력합니다.
- **Create Rule for(**규칙 생성**)** - 수동 **NAT**를 선택합니다.
- **Rule Placement(**규칙 배치**)** - 규칙을 추가할 위치를 선택합니다. 규칙은 카테고리에서 자동 NAT 규칙 앞이나 뒤에 삽입할 수도 있고, 선택한 규칙 위나 아래에 삽입할 수도 있습니다.
- **Type(**유형**)** - 동적을 선택합니다. 이 설정은 소스 주소에만 적용됩니다. 대상 주소에 대해 변환을 정의하는 경우 변환은 항상 고정입니다.

단계 **4** 다음 인터페이스 옵션을 구성합니다.

- 소스 인터페이스, 대상 인터페이스 — (브리지 그룹 멤버 인터페이스의 경우 필수) 이 NAT 규칙을 적용할 인터페이스입니다. **Source(**소스**)**는 트래픽이 디바이스로 들어가는 데 사용되는 실제 인터페이스입니다. **Destination(**대상**)**은 트래픽이 디바이스에서 나오는 데 사용되는 매핑된 인터페이스입니다. 기본적으로 규칙은 브리지 그룹 멤버 인터페이스를 제외한 모든 인터페이스(**Any(**모두**)**)에 적용됩니다.

단계 **5** 원본 패킷 주소(IPv4 또는 IPv6)를 식별합니다. 이 주소는 원본 패킷에 표시되는 패킷 주소입니다.

원래 패킷 대 변환된 패킷의 예는 다음 그림을 참조하십시오.



- **Original Source Address(**원본 소스 주소**)** - 변환 중인 주소가 포함된 네트워크 개체 또는 그룹입니다.

- **Original Destination Address(**원본 대상 주소**)** - (선택 사항) 대상의 주소를 포함하는 네트워크 개체입니다. 이 옵션을 비워 두면 대상에 관계없이 소스 주소 변환이 적용됩니다. 대상 주소를 지정하면 해당 주소에 대해 고정 변환을 구성할 수도 있고 단순히 ID NAT를 사용할 수도 있습니다.

  Interface(인터페이스**)**를 선택하여 소스 인터페이스(Any(모두)일 수 없음)를 기준으로 원본 대상을 지정할 수 있습니다. 이 옵션을 선택할 경우 변환된 대상 개체도 선택해야 합니다. 대상 주소에 대해 포트 변환 고정 인터페이스 NAT를 구현하려면 이 옵션을 선택하고 대상 포트에 대해 적절한 포트 개체도 선택합니다.

단계 **6** 변환된 패킷 주소(IPv4 또는 IPv6), 즉 대상 인터페이스 네트워크에 나타나는 패킷 주소를 확인합니다. 필요에 따라 IPv4 및 IPv6 간에 변환할 수 있습니다.

- 변환된 소스 주소 - 다음 중 하나입니다.
  - (인터페이스 PAT) 대상 인터페이스의 IPv4 주소를 사용하려면 인터페이스를 선택합니다. 특정 대상 인터페이스도 선택해야 합니다. 이 인터페이스는 브리지 그룹 멤버 인터페이스일 수 없습니다. IPv6에는 인터페이스 PAT를 사용할 수 없습니다.
  - 대상 인터페이스 주소가 아닌 단일 주소를 사용하려면 이러한 용도로 생성한 호스트 네트워크 개체를 선택합니다.
- 변환된 대상 주소 - (선택 사항) 변환된 패킷에서 사용되는 대상 주소를 포함하는 네트워크 개체 또는 그룹입니다. 원본 대상에 대해 개체를 선택한 경우 동일한 개체를 선택하여 ID NAT(변환 없음)를 설정할 수 있습니다.

단계 **7** (선택 사항). 서비스 변환용 대상 서비스 포트(**Original Destination Port(**원본 대상 포트**)**, **Translated Destination Port(**변환된 대상 포트**)**)를 식별합니다.

동적 NAT는 포트 변환을 지원하지 않으므로 **Original Destination Port(**원본 대상 포트**)** 및 **Translated Destination Port(**변환된 대상 포트**)** 필드를 비워 둡니다. 그러나 대상 변환은 항상 고정이므로 대상 포트의 포트 변환을 수행할 수 있습니다.

NAT는 TCP 또는 UDP만 지원합니다. 포트를 변환할 때는 실제 서비스 개체의 프로토콜과 매핑된 서비스 개체의 프로토콜이 동일해야 합니다(둘 다 TCP거나 둘 다 UDP). ID NAT의 경우 실제 포트와 매핑된 포트에 동일한 서비스 개체를 사용할 수 있습니다.

단계 **8** (선택 사항). 고급 옵션 링크를 클릭하고 원하는 옵션을 선택합니다.

- 인터페이스 **PAT(**대상 인터페이스**)**로 폴스루 - 다른 매핑된 주소가 이미 할당된 경우 대상 인터페이스의 IP 주소를 백업 방법으로 사용할지 여부를 선택합니다(인터페이스 PAT 대체). 이 옵션은 브리지 그룹의 멤버가 아닌 대상 인터페이스를 선택한 경우에만 사용할 수 있습니다. 인터페이스 PAT를 변환된 주소로 이미 컨피그레이션한 경우에는 이 옵션을 선택할 수 없습니다. 또한 IPv6 네트워크에서는 이 옵션을 사용할 수 없습니다.

단계 **9** **OK(**확인**)**를 클릭합니다.

고정 **NAT**

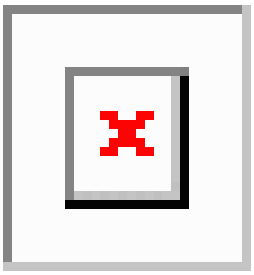
다음 주제에서는 고정 NAT 및 고정 NAT를 구현하는 방법에 대해 설명합니다.

고정 **NAT** 정보

고정 NAT는 실제 주소에서 매핑된 주소로의 고정된 변환을 생성합니다. 매핑된 주소는 각각의 연속 연결에 대해 동일하므로 NAT는 양방향 연결 시작을 허용합니다. 이를 허용하는 액세스 규칙이 있는 경우 호스트에서 나가기도 하고 호스트로 들어오기도 합니다. 반면 동적 NAT 및 PAT의 경우, 각 호스트는 각 후속 변환에 대해 서로 다른 주소 또는 포트를 사용하므로 양방향 시작이 지원되지 않습니다.

다음 그림은 일반적인 고정 NAT 시나리오를 보여줍니다. 변환이 항상 활성 상태이므로 실제 호스트와 원격 호스트 모두 연결을 시작할 수 있습니다.

그림 *38:* 고정 *NAT*



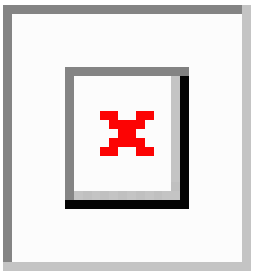
포트 변환 고정 NAT

포트 변환 고정 NAT를 사용하면 실제 및 매핑된 프로토콜과 포트를 지정할 수 있습니다.

고정 NAT로 포트를 지정하는 경우 포트 및/또는 IP 주소를 동일한 값으로 매핑할지 아니면 다른 값으로 매핑할지를 선택할 수 있습니다.

다음 그림은 자신에게 매핑되는 포트와 다른 값으로 매핑되는 포트 모두를 보여주는 포트 변환 시나리오의 일반적인 고정 NAT를 보여줍니다. 두 경우 모두 IP 주소는 다른 값으로 매핑됩니다. 변환이 항상 활성 상태이므로 변환된 호스트와 원격 호스트 모두 연결을 시작할 수 있습니다.

그림 *39:* 일반적인 포트 변환 고정 *NAT* 시나리오



포트 변환 고정 NAT 규칙은 지정된 포트에 대해서만 대상 IP 주소 액세스를 제한합니다. NAT 규칙이 적용되지 않는 다른 포트에서 대상 IP 주소에 액세스를 시도하면 연결은 차단됩니다. 또한 수동 NAT의 경우 NAT 규칙의 소스 IP 주소와 일치하지 않는 트래픽은 대상 포트와 관계없이 대상 IP 주소와 일치하는 경우 삭제됩니다. 그러므로 대상 IP 주소에 대해 허용되는 기타 모든 트래픽을 위한 규칙을 더 추가해야 합니다. 예를 들어 포트 사양 없이 IP 주소용 고정 NAT 규칙을 구성하여 포트 변환 규칙 뒤에 배치할 수 있습니다.

참고 보조 채널(예: FTP 및 VoIP)에 대해 애플리케이션 검사를 요구하는 애플리케이션의 경우 NAT에서는 자동으로 보조 포트를 변환합니다.

포트 변환 고정 NAT의 몇 가지 다른 사용 방식은 다음과 같습니다.

ID 포트 변환 고정 **NAT**

내부 리소스에 대한 외부 액세스를 간소화할 수 있습니다. 예를 들어, FTP, HTTP, SMTP 등 각기 다른 포트에서 서비스를 제공하는 개별 서버 3개가 있는 경우 외부 사용자에게 해당 서비스 액

세스를 위한 단일 IP 주소를 제공할 수 있습니다. 그런 후에 외부 사용자들이 액세스하려는 포트를 기준으로 하여 실제 서버의 올바른 IP 주소에 단일 외부 IP 주소를 매핑하도록 ID 포트 변환 고정 NAT를 구성할 수 있습니다. 이러한 서버는 표준 포트(각각 21, 80, 25)를 사용하므로 포트를 변경할 필요는 없습니다.

비표준 포트에 대한 포트 변환 고정 **NAT**

잘 알려진 포트를 비표준 포트로 또는 그 반대로 변환하려는 경우에도 포트 변환 고정 NAT를 사용할 수 있습니다. 예를 들어 내부 웹 서버가 포트 8080을 사용하는 경우 외부 사용자가 포트 80에 연결하도록 허용한 다음 원본 포트 8080으로의 변환을 취소할 수 있습니다. 마찬가지로, 보안을 강화하려면 웹 사용자에게 비표준 포트 6785로 연결하도록 안내한 다음 포트 80으로의 변환을 취소할 수 있습니다.

포트 변환 고정 인터페이스 **NAT**

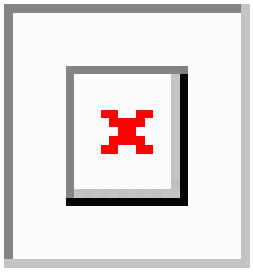
실제 주소를 인터페이스 주소/포트 조합으로 매핑하도록 고정 NAT를 구성할 수 있습니다. 예를 들어 디바이스의 외부 인터페이스에 대한 텔넷 액세스를 내부 호스트로 리디렉션하려는 경우 내부 호스트 IP 주소/포트 23을 외부 인터페이스 주소/포트 23에 매핑할 수 있습니다.

일대다 고정 **NAT**

일반적으로 NAT는 일대일 매핑으로 구성합니다. 그러나 경우에 따라 여러 매핑된 주소에 대해 단일 실제 주소를 구성해야 할 수도 있습니다(일대다). 일대다 고정 NAT를 구성할 경우, 실제 호스트가 트래픽을 시작하면 항상 첫 번째 매핑된 주소를 사용합니다. 그러나 호스트에 대해 시작된 트래픽의 경우, 매핑된 주소 중 하나에 대해 트래픽을 시작할 수 있습니다. 이러한 주소는 단일 실제 주소로 변환되지 않습니다.

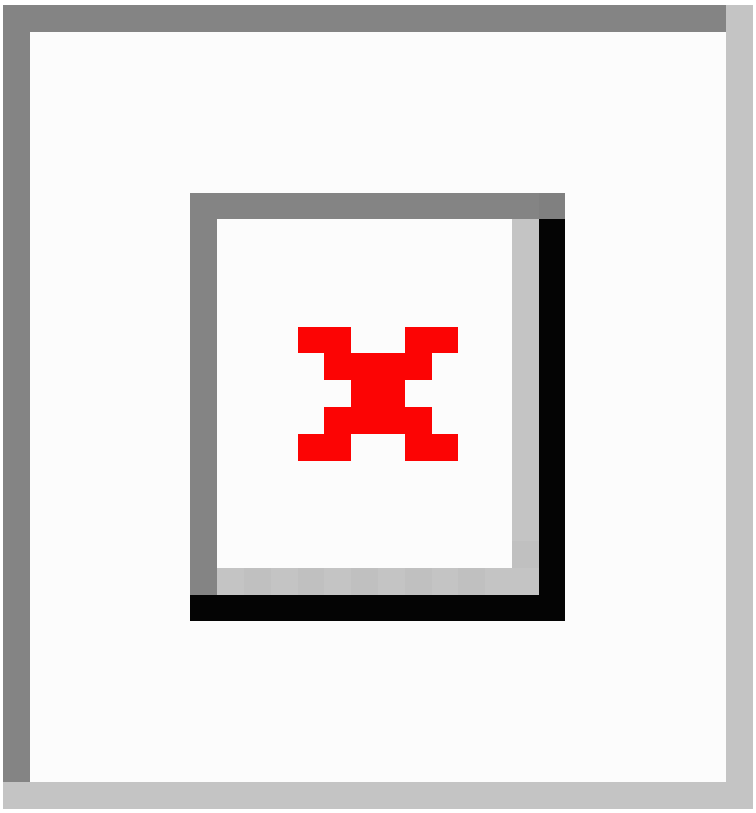
다음 그림은 일반적인 일대다 고정 NAT 시나리오를 보여줍니다. 실제 호스트에 의한 시작은 항상 첫 번째 매핑된 주소를 사용하므로, 실제 호스트 IP/첫 번째 매핑된 IP의 변환이 기술적으로 유일한 양방향 변환입니다.

그림 ***40:*** 일대다 고정 ***NAT***



예를 들어 10.1.2.27에 로드 밸런서가 있으면, 요청된 URL에 따라 트래픽이 올바른 웹 서버로 리디렉션됩니다.

그림 *41:* 일대다 고정 ***NAT*** 예



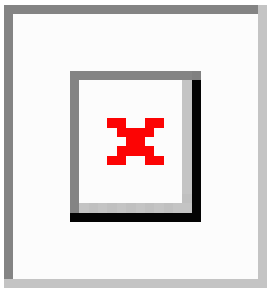
기타 매핑 시나리오(권장되지 않음)

NAT에서는 일대일, 일대다, 소수대다수, 다수대소수, 다대일 등 모든 종류의 고정 매핑 시나리오를 유연하게 허용합니다. 그러나 일대일 또는 일대다 매핑만 사용하는 것이 좋습니다. 다른 매핑 옵션을 사용할 경우 예기치 않은 결과가 발생할 수 있습니다.

소수대다수는 기능상 일대다와 같지만, 구성이 좀 더 복잡하고 실제 매핑이 한눈에 명확히 파악되지 않을 수 있으므로 필요한 경우 각 실제 주소에 대해 일대다 구성을 만드는 것이 좋습니다. 소수대다수 시나리오에서는 소수의 실제 주소가 다수의 매핑된 주소로 순서대로 매핑됩니다(A-1, B-2, C-3). 모든 실제 주소가 매핑되면 다음의 매핑된 주소는 첫 번째 실제 주소로 매핑되며, 모든 매핑된 주소가 매핑될 때까지 같은 방식이 반복됩니다(A-4, B-5, C-6). 그 결과 각 실제 주소에 다수의 매핑된 주소가 연결됩니다. 일대다 구성의 경우와 마찬가지로 첫 번째 매핑만 양방향이고 이후 매핑에서는 실제 호스트로만 트래픽이 시작되고, 실제 호스트로부터의 모든 트래픽은 소스에 대해 첫 번째 매핑된 주소만 사용합니다.

다음 그림은 일반적인 소수대다수 고정 NAT 시나리오를 보여줍니다.

그림 *42:* 소수대다수 고정 *NAT*

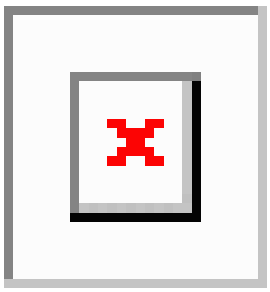


매핑된 주소보다 실제 주소가 더 많은 다수대소수 또는 다대일 컨피그레이션의 경우, 실제 주소가 소진되기 전에 매핑된 주소가 소진됩니다. 가장 낮은 실제 IP 주소와 매핑된 풀 간의 매핑만 양방향 시작이 가능합니다. 나머지 더 높은 실제 주소는 트래픽을 시작할 수 있지만 이러한 주소로 트래픽이 시작될 수는 없습니다. 연결에 대한 고유한 5튜플(소스/대상 IP 주소, 소스/대상 포트 및 프로토콜) 때문에 연결에 대한 반환 트래픽은 정확한 실제 주소로 전달됩니다.

참고 다수대소수 또는 다대일 NAT는 PAT가 아닙니다. 두 개의 실제 호스트가 동일한 소스 포트 번호를 사용하고 동일한 외부 서버 및 동일한 TCP 대상 포트로 이동하며 두 호스트가 동일한 IP 주소로 변환되면, 주소 충돌 때문에(5튜플이 고유하지 않음) 두 연결이 재설정됩니다.

다음 그림은 일반적인 다수대소수 고정 NAT 시나리오를 보여줍니다.

그림 *43:* 다수대소수 고정 *NAT*



고정 규칙을 이 방식으로 사용하는 대신, 양방향 시작이 필요한 트래픽에 대해 일대일 규칙을 만든 다음 나머지 주소에 대해 동적 규칙을 만드는 방식을 권장합니다.

고정 자동 **NAT** 구성

고정 자동 NAT 규칙을 사용하여 주소를 대상 네트워크에서 라우팅할 수 있는 서로 다른 IP 주소로 변환합니다. 또한 고정 NAT 규칙을 사용하여 포트 변환을 수행할 수도 있습니다.

시작하기 전에

개체를 선택하여 규칙에 필요한 네트워크 개체 또는 그룹을 생성합니다. NAT 규칙을 정의하면서 개체를 생성할 수도 있습니다. 개체는 다음 요건을 충족해야 합니다.

- 원본 주소 — 이 주소는 그룹이 아닌 네트워크 개체여야 하며 호스트, 범위 또는 서브넷일 수 있습니다.
- 변환된 주소 - 다음 옵션을 사용하여 변환된 주소를 지정할 수 있습니다.
  - 대상 인터페이스 - 대상 인터페이스 IPv4 주소를 사용하려는 경우 네트워크 개체가 필요하지 않습니다. 이 경우 포트 변환 고정 인터페이스 NAT가 구성됩니다. 소스 주소/포트는 인터페이스의 주소 및 동일한 포트 번호로 변환됩니다. IPv6에는 인터페이스 PAT를 사용할 수 없습니다.
  - 주소 - 호스트, 범위 또는 서브넷이 포함된 네트워크 개체 또는 그룹을 생성합니다. 그룹은 IPv4 주소와 IPv6 주소를 모두 포함할 수는 없으며 한 유형만 포함해야 합니다. 일반적으로 일대일 매핑의 경우 동일한 수의 매핑된 주소를 실제 주소로 구성합니다. 그러나 주소의 수가 일치하지 않아도 됩니다.

프로시저

단계 **1** **Policies(**정책**)** > **NAT**를 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 새 규칙을 생성하려면 **+** 버튼을 클릭합니다.
- 기존 규칙을 수정하려면 해당 규칙의 수정 아이콘()을 클릭합니다.

더 이상 필요하지 않은 규칙을 삭제하려면 해당 규칙의 휴지통 아이콘을 클릭합니다.

단계 **3** 기본 규칙 옵션을 구성합니다.

- **Title(**제목**)** — 규칙의 이름을 입력합니다.
- **Creat Rule For(**규칙 생성**)** — 자동 **NAT**를 선택합니다.
- **Type(**유형**)** - 고정을 선택합니다.

단계 **4** 다음 패킷 변환 옵션을 구성합니다.

- 소스 인터페이스, 대상 인터페이스 — (브리지 그룹 멤버 인터페이스의 경우 필수) 이 NAT 규칙을 적용할 인터페이스입니다. **Source(**소스**)**는 트래픽이 디바이스로 들어가는 데 사용되는 실제 인터페이스입니다. **Destination(**대상**)**은 트래픽이 디바이스에서 나오는 데 사용되는 매핑된 인터페이스입니다. 기본적으로 규칙은 브리지 그룹 멤버 인터페이스를 제외한 모든 인터페이스(**Any(**모두**)**)에 적용됩니다.
- 원본 주소 — 변환하는 주소가 포함된 네트워크 개체입니다.
- 변환된 주소 - 다음 중 하나입니다.
  - 설정된 주소 그룹을 사용하려면 매핑된 주소를 포함하는 네트워크 개체 또는 그룹을 선택합니다. 일반적으로 일대일 매핑의 경우 동일한 수의 매핑된 주소를 실제 주소로 구성합니다. 그러나 주소의 수가 일치하지 않아도 됩니다.
  - (포트 변환 기능이 있는 고정 인터페이스 NAT) 대상 인터페이스의 주소를 사용하려면 인터페이스를 선택합니다. 특정 대상 인터페이스도 선택해야 합니다. 이 인터페이스는 브리지 그룹 멤버 인터페이스일 수 없습니다. IPv6에는 인터페이스 PAT를 사용할 수 없습니다.이

경우 포트 변환 고정 인터페이스 NAT가 구성됩니다. 소스 주소/포트는 인터페이스의 주소 및 동일한 포트 번호로 변환됩니다.

- (선택 사항). 원 포트, 변환된 포트 - TCP 또는 UDP 포트를 변환해야 하는 경우 원 포트와 변환된 포트를 정의하는 포트 개체를 선택합니다. 이 경우 동일한 프로토콜의 개체를 선택해야 합니다. 개체가 아직 없으면 새 개체 생성 링크를 클릭합니다. 예를 들어, 필요에 따라 TCP/80을 TCP/8080으로 변환할 수 있습니다.

단계 **5** (선택 사항). 고급 옵션 링크를 클릭하고 원하는 옵션을 선택합니다.

- 이 규칙과 일치하는 **DNS** 회신 변환 -DNS 응답의 IP 주소를 변환할지 여부를 선택합니다. 매핑된 인터페이스에서 실제 인터페이스로 이동하는 DNS 응답의 경우 주소(IPv4 A 또는 IPv6 AAAA) 레코드가 매핑된 값에서 실제 값으로 재작성됩니다. 반대로, 실제 인터페이스에서 매핑된 인터페이스로 이동하는 DNS 응답의 경우 실제 값에서 매핑된 값으로 레코드가 재작성됩니다. 이 옵션은 특정 상황에서 사용되며, 재작성 시 A 레코드와 AAAA 레코드 간의 변환도 수행되는 NAT64/46 변환에 필요한 경우도 있습니다. 자세한 내용은 NAT를 사용하여 DNS 쿼리 및 응답 재작성, 663 페이지를 참조하십시오. 포트 변환을 수행하는 경우에는 이 옵션을 사용할 수 없습니다.
- 대상 인터페이스에서 **ARP** 프록시 설정 안 함 - 매핑된 IP 주소로 들어오는 패킷에 대해 프록시 ARP를 비활성화합니다. 매핑된 인터페이스와 동일한 네트워크의 주소를 사용하는 경우 시스템은 매핑된 주소에 대한 ARP 요청에 답하기 위해 프록시 ARP를 사용하며, 이에 따라 매핑된 주소로 가야 하는 트래픽을 가로챕니다. 디바이스가 추가 네트워크에 대한 게이트웨이가 될 필요가 없으므로 이 솔루션은 라우팅을 간소화합니다. 원하는 경우 프록시 ARP를 비활성화할 수 있습니다. 이 경우 업스트림 라우터에 적절한 경로가 있어야 합니다. 일반적으로 ID NAT에는 프록시 ARP가 필요하지 않으며, 프록시 ARP를 사용할 경우 연결 문제가 발생할 수도 있습니다.

단계 **6** **OK(**확인**)**를 클릭합니다.

고정 수동 **NAT** 구성

자동 NAT가 요구를 충족하지 않을 때는 고정 수동 NAT 규칙을 사용합니다. 대상에 따라 다른 변환을 수행하려는 경우를 예로 들 수 있습니다. 고정 NAT는 주소를 대상 네트워크에서 라우팅할 수 있는 서로 다른 IP 주소로 변환합니다. 또한 고정 NAT 규칙을 사용하여 포트 변환을 수행할 수도 있습니다.

시작하기 전에

개체를 선택하여 규칙에 필요한 네트워크 개체 또는 그룹을 생성합니다. 그룹은 IPv4 주소와 IPv6 주소를 모두 포함할 수는 없으며 한 유형만 포함해야 합니다. NAT 규칙을 정의하면서 개체를 생성할 수도 있습니다. 개체는 다음 요건도 충족해야 합니다.

- 원본 소스 주소 - 이 주소는 네트워크 개체 또는 그룹일 수 있으며 호스트, 범위 또는 서브넷을 포함할 수 있습니다. 모든 원본 소스 트래픽을 변환하려는 경우 이 단계를 건너뛰고 규칙에서 **Any(**모두**)**를 지정하면 됩니다.
- 변환된 소스 주소 - 다음 옵션을 사용하여 변환된 주소를 지정할 수 있습니다.

- 대상 인터페이스 - 대상 인터페이스 IPv4 주소를 사용하려는 경우 네트워크 개체가 필요하지 않습니다. 이 경우 포트 변환 고정 인터페이스 NAT가 구성됩니다. 소스 주소/포트는 인터페이스의 주소 및 동일한 포트 번호로 변환됩니다. IPv6에는 인터페이스 PAT를 사용할 수 없습니다.
- 주소 - 호스트, 범위 또는 서브넷이 포함된 네트워크 개체 또는 그룹을 생성합니다. 그룹은 IPv4 주소와 IPv6 주소를 모두 포함할 수는 없으며 한 유형만 포함해야 합니다. 일반적으로 일대일 매핑의 경우 동일한 수의 매핑된 주소를 실제 주소로 구성합니다. 그러나 주소의 수가 일치하지 않아도 됩니다.

규칙에서 원본 대상 주소 및 변환된 대상 주소에 대해 정적 변환을 구성하는 경우 이러한 주소에 대해 네트워크 개체를 생성할 수도 있습니다. 포트 변환 대상 고정 인터페이스 NAT만 구성하려면 대상 매핑된 주소에 대한 개체 추가를 건너뛰고 규칙에서 인터페이스를 지정할 수 있습니다.

소스나 대상 또는 둘 다에 대해 포트 변환을 수행할 수도 있습니다. 개체 관리자에서 원본 및 변환된 포트에 사용할 수 있는 포트 개체가 있는지 확인합니다.

프로시저

단계 **1** **Policies(**정책**)** > **NAT**를 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 새 규칙을 생성하려면 **+** 버튼을 클릭합니다.
- 기존 규칙을 수정하려면 해당 규칙의 수정 아이콘( )을 클릭합니다.

더 이상 필요하지 않은 규칙을 삭제하려면 해당 규칙의 휴지통 아이콘을 클릭합니다.

단계 **3** 기본 규칙 옵션을 구성합니다.

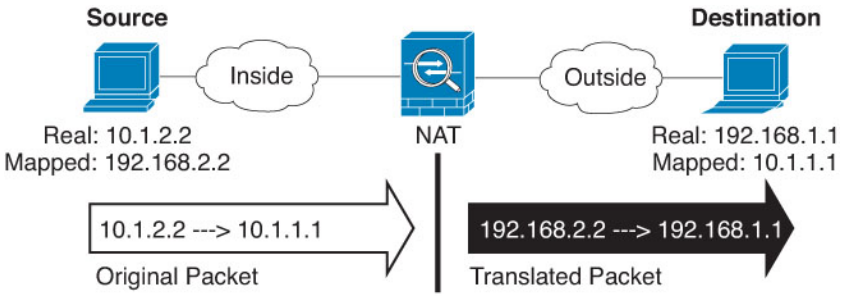
- **Title(**제목**)** — 규칙의 이름을 입력합니다.
- **Create Rule for(**규칙 생성**)** - 수동 **NAT**를 선택합니다.
- **Rule Placement(**규칙 배치**)** - 규칙을 추가할 위치를 선택합니다. 규칙은 카테고리에서 자동 NAT 규칙 앞이나 뒤에 삽입할 수도 있고, 선택한 규칙 위나 아래에 삽입할 수도 있습니다.
- **Type(**유형**)** - 고정을 선택합니다. 이 설정은 소스 주소에만 적용됩니다. 대상 주소에 대해 변환을 정의하는 경우 변환은 항상 고정입니다.

단계 **4** 다음 인터페이스 옵션을 구성합니다.

- 소스 인터페이스, 대상 인터페이스 — (브리지 그룹 멤버 인터페이스의 경우 필수) 이 NAT 규칙을 적용할 인터페이스입니다. **Source(**소스**)**는 트래픽이 디바이스로 들어가는 데 사용되는 실제 인터페이스입니다. **Destination(**대상**)**은 트래픽이 디바이스에서 나오는 데 사용되는 매핑된 인터페이스입니다. 기본적으로 규칙은 브리지 그룹 멤버 인터페이스를 제외한 모든 인터페이스(**Any(**모두**)**)에 적용됩니다.

단계 **5** 원본 패킷 주소(IPv4 또는 IPv6)를 식별합니다. 이 주소는 원본 패킷에 표시되는 패킷 주소입니다.

원래 패킷 대 변환된 패킷의 예는 다음 그림을 참조하십시오.



- **Original Source Address(**원본 소스 주소**)** - 변환 중인 주소가 포함된 네트워크 개체 또는 그룹입니다.
- **Original Destination Address(**원본 대상 주소**)** - (선택 사항) 대상의 주소를 포함하는 네트워크 개체입니다. 이 옵션을 비워 두면 대상에 관계없이 소스 주소 변환이 적용됩니다. 대상 주소를 지정하면 해당 주소에 대해 고정 변환을 구성할 수도 있고 단순히 ID NAT를 사용할 수도 있습니다.

  Interface(인터페이스**)**를 선택하여 소스 인터페이스(Any(모두)일 수 없음)를 기준으로 원본 대상을 지정할 수 있습니다. 이 옵션을 선택할 경우 변환된 대상 개체도 선택해야 합니다. 대상 주소에 대해 포트 변환 고정 인터페이스 NAT를 구현하려면 이 옵션을 선택하고 대상 포트에 대해 적절한 포트 개체도 선택합니다.

단계 **6** 변환된 패킷 주소(IPv4 또는 IPv6), 즉 대상 인터페이스 네트워크에 나타나는 패킷 주소를 확인합니다. 필요에 따라 IPv4 및 IPv6 간에 변환할 수 있습니다.

- 변환된 소스 주소 - 다음 중 하나입니다.
  - 설정된 주소 그룹을 사용하려면 매핑된 주소를 포함하는 네트워크 개체 또는 그룹을 선택합니다. 일반적으로 일대일 매핑의 경우 동일한 수의 매핑된 주소를 실제 주소로 구성합니다. 그러나 주소의 수가 일치하지 않아도 됩니다.
  - (포트 변환 기능이 있는 고정 인터페이스 NAT) 대상 인터페이스의 IPv4 주소를 사용하려면 인터페이스를 선택합니다. 특정 대상 인터페이스도 선택해야 합니다. 이 인터페이스는 브리지 그룹 멤버 인터페이스일 수 없습니다. 이 경우 포트 변환 고정 인터페이스 NAT가 구성됩니다. 소스 주소/포트는 인터페이스의 주소 및 동일한 포트 번호로 변환됩니다. IPv6에는 인터페이스 PAT를 사용할 수 없습니다.
- 변환된 대상 주소 - (선택 사항) 변환된 패킷에서 사용되는 대상 주소를 포함하는 네트워크 개체 또는 그룹입니다. 원본 대상에 대해 개체를 선택한 경우 동일한 개체를 선택하여 ID NAT(변환 없음)를 설정할 수 있습니다.

단계 **7** (선택 사항). 서비스 변환의 원본 또는 대상 서비스 포트를 식별합니다.

포트 변환 고정 NAT를 구성하는 경우 소스나 대상 또는 둘 다에 대해 포트를 변환할 수 있습니다. 예를 들어 TCP/80과 TCP/8080 간에 변환할 수 있습니다.

NAT는 TCP 또는 UDP만 지원합니다. 포트를 변환할 때는 실제 서비스 개체의 프로토콜과 매핑된 서비스 개체의 프로토콜이 동일해야 합니다(둘 다 TCP거나 둘 다 UDP). ID NAT의 경우 실제 포트와 매핑된 포트에 동일한 서비스 개체를 사용할 수 있습니다.

- 원본 소스 포트, 변환된 소스 포트 - 소스 주소에 대한 포트 변환을 정의합니다.
- 원본 대상 포트, 변환된 대상 포트 - 대상 주소에 대한 포트 변환을 정의합니다.

단계 **8** (선택 사항). 고급 옵션 링크를 클릭하고 원하는 옵션을 선택합니다.

- 이 규칙과 일치하는 **DNS** 회신 변환 -DNS 응답의 IP 주소를 변환할지 여부를 선택합니다. 매핑된 인터페이스에서 실제 인터페이스로 이동하는 DNS 응답의 경우 주소(IPv4 A 또는 IPv6 AAAA) 레코드가 매핑된 값에서 실제 값으로 재작성됩니다. 반대로, 실제 인터페이스에서 매핑된 인터페이스로 이동하는 DNS 응답의 경우 실제 값에서 매핑된 값으로 레코드가 재작성됩니다. 이 옵션은 특정 상황에서 사용되며, 재작성 시 A 레코드와 AAAA 레코드 간의 변환도 수행되는 NAT64/46 변환에 필요한 경우도 있습니다. 자세한 내용은 NAT를 사용하여 DNS 쿼리 및 응답 재작성, 663 페이지를 참조하십시오. 포트 변환을 수행하는 경우에는 이 옵션을 사용할 수 없습니다.
- 대상 인터페이스에서 **ARP** 프록시 설정 안 함 - 매핑된 IP 주소로 들어오는 패킷에 대해 프록시 ARP를 비활성화합니다. 매핑된 인터페이스와 동일한 네트워크의 주소를 사용하는 경우 시스템은 매핑된 주소에 대한 ARP 요청에 답하기 위해 프록시 ARP를 사용하며, 이에 따라 매핑된 주소로 가야 하는 트래픽을 가로챕니다. 디바이스가 추가 네트워크에 대한 게이트웨이가 될 필요가 없으므로 이 솔루션은 라우팅을 간소화합니다. 원하는 경우 프록시 ARP를 비활성화할 수 있습니다. 이 경우 업스트림 라우터에 적절한 경로가 있어야 합니다. 일반적으로 ID NAT에는 프록시 ARP가 필요하지 않으며, 프록시 ARP를 사용할 경우 연결 문제가 발생할 수도 있습니다.

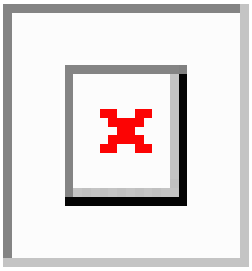
단계 **9** **OK(**확인**)**를 클릭합니다.

ID NAT

IP 주소를 자신으로 변환해야 하는 NAT 구성이 있을 수 있습니다. 예를 들어 NAT를 모든 네트워크에 적용하는 광범위한 규칙을 만들되 NAT에서 하나의 네트워크만 제외하고 싶은 경우, 주소를 자신으로 변환하는 고정 NAT 규칙을 만들 수 있습니다.

다음 그림은 일반적인 ID NAT 시나리오를 보여줍니다.

그림 ***44: ID NAT***



다음 주제에서는 ID NAT를 구성하는 방법을 설명합니다.

ID 자동 NAT 구성

주소 변환을 방지하려면 고정 ID 자동 NAT 규칙을 사용합니다. 이 경우 주소가 자체로 변환됩니다.

시작하기 전에

개체를 선택하여 규칙에 필요한 네트워크 개체 또는 그룹을 생성합니다. NAT 규칙을 정의하면서 개체를 생성할 수도 있습니다. 개체는 다음 요건을 충족해야 합니다.

- 원본 주소 — 이 주소는 그룹이 아닌 네트워크 개체여야 하며 호스트, 범위 또는 서브넷일 수 있습니다.
- 변환된 주소 - 원본 소스 개체와 내용이 정확히 동일한 네트워크 개체 또는 그룹입니다. 동일한 개체를 사용할 수 있습니다.

프로시저

단계 **1** **Policies(**정책**)** > **NAT**를 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 새 규칙을 생성하려면 **+** 버튼을 클릭합니다.
- 기존 규칙을 수정하려면 해당 규칙의 수정 아이콘( )을 클릭합니다.

더 이상 필요하지 않은 규칙을 삭제하려면 해당 규칙의 휴지통 아이콘을 클릭합니다.

단계 **3** 기본 규칙 옵션을 구성합니다.

- **Title(**제목**)** — 규칙의 이름을 입력합니다.
- **Creat Rule For(**규칙 생성**)** — 자동 **NAT**를 선택합니다.
- **Type(**유형**)** - 고정을 선택합니다.

단계 **4** 다음 패킷 변환 옵션을 구성합니다.

- 소스 인터페이스, 대상 인터페이스 — (브리지 그룹 멤버 인터페이스의 경우 필수) 이 NAT 규칙을 적용할 인터페이스입니다. **Source(**소스**)**는 트래픽이 디바이스로 들어가는 데 사용되는 실제 인터페이스입니다. **Destination(**대상**)**은 트래픽이 디바이스에서 나오는 데 사용되는 매핑된 인터페이스입니다. 기본적으로 규칙은 브리지 그룹 멤버 인터페이스를 제외한 모든 인터페이스(**Any(**모두**)**)에 적용됩니다.
- 원본 주소 — 변환하는 주소가 포함된 네트워크 개체입니다.
- 변환된 주소 - 원본 소스와 동일한 개체입니다. 원하는 경우 콘텐츠가 정확히 동일한 다른 개체를 선택할 수 있습니다.

ID NAT의 경우에는 원본 포트 및 변환된 포트 옵션을 구성하지 마십시오.

단계 **5** (선택 사항). 고급 옵션 링크를 클릭하고 원하는 옵션을 선택합니다.

- 이 규칙과 일치하는 **DNS** 응답 변환 - ID NAT의 경우에는 이 옵션을 구성하지 마십시오.
- 대상 인터페이스에서 **ARP** 프록시 설정 안 함 - 매핑된 IP 주소로 들어오는 패킷에 대해 프록시 ARP를 비활성화합니다. 매핑된 인터페이스와 동일한 네트워크의 주소를 사용하는 경우 시스템은 매핑된 주소에 대한 ARP 요청에 답하기 위해 프록시 ARP를 사용하며, 이에 따라 매핑된 주소로 가야 하는 트래픽을 가로챕니다. 디바이스가 추가 네트워크에 대한 게이트웨이가 될 필요가 없으므로 이 솔루션은 라우팅을 간소화합니다. 원하는 경우 프록시 ARP를 비활성화할 수 있습

니다. 이 경우 업스트림 라우터에 적절한 경로가 있어야 합니다. 일반적으로 ID NAT에는 프록시 ARP가 필요하지 않으며, 프록시 ARP를 사용할 경우 연결 문제가 발생할 수도 있습니다.

- 대상 인터페이스에 대해 경로 조회 수행 - 원본 및 변환된 소스 주소에 대해 동일한 개체를 선택할 때 소스 및 대상 인터페이스를 선택하는 경우 이 옵션을 선택하면 시스템이 NAT 규칙에 구성된 대상 인터페이스를 사용하는 대신 라우팅 테이블을 기준으로 하여 대상 인터페이스를 결정하도록 할 수 있습니다.

단계 **6** **OK(**확인**)**를 클릭합니다.

ID 수동 NAT 구성

자동 NAT가 요구를 충족하지 않을 때는 고정 ID 수동 NAT 규칙을 사용합니다. 대상에 따라 다른 변환을 수행하려는 경우를 예로 들 수 있습니다. 주소 변환을 방지하려면 고정 ID NAT 규칙을 사용합니다. 이 경우 주소가 자체로 변환됩니다.

시작하기 전에

개체를 선택하여 규칙에 필요한 네트워크 개체 또는 그룹을 생성합니다. 그룹은 IPv4 주소와 IPv6 주소를 모두 포함할 수는 없으며 한 유형만 포함해야 합니다. NAT 규칙을 정의하면서 개체를 생성할 수도 있습니다. 개체는 다음 요건도 충족해야 합니다.

- 원본 소스 주소 - 이 주소는 네트워크 개체 또는 그룹일 수 있으며 호스트, 범위 또는 서브넷을 포함할 수 있습니다. 모든 원본 소스 트래픽을 변환하려는 경우 이 단계를 건너뛰고 규칙에서 **Any(**모두**)**를 지정하면 됩니다.
- 변환된 소스 주소 - 원본 소스와 동일한 개체입니다. 원하는 경우 콘텐츠가 정확히 동일한 다른 개체를 선택할 수 있습니다.

규칙에서 원본 대상 주소 및 변환된 대상 주소에 대해 정적 변환을 구성하는 경우 이러한 주소에 대해 네트워크 개체를 생성할 수도 있습니다. 포트 변환 대상 고정 인터페이스 NAT만 구성하려면 대상 매핑된 주소에 대한 개체 추가를 건너뛰고 규칙에서 인터페이스를 지정할 수 있습니다.

소스나 대상 또는 둘 다에 대해 포트 변환을 수행할 수도 있습니다. 개체 관리자에서 원본 및 변환된 포트에 사용할 수 있는 포트 개체가 있는지 확인합니다. ID NAT에 대해 동일한 개체를 사용할 수 있습니다.

프로시저

단계 **1** **Policies(**정책**)** > **NAT**를 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 새 규칙을 생성하려면 **+** 버튼을 클릭합니다.
- 기존 규칙을 수정하려면 해당 규칙의 수정 아이콘()을 클릭합니다.

더 이상 필요하지 않은 규칙을 삭제하려면 해당 규칙의 휴지통 아이콘을 클릭합니다.

단계 **3** 기본 규칙 옵션을 구성합니다.

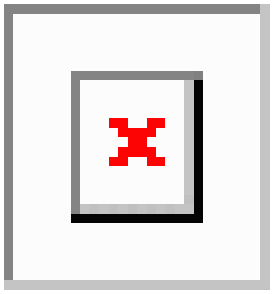
- **Title(**제목**)** — 규칙의 이름을 입력합니다.
- **Create Rule for(**규칙 생성**)** - 수동 **NAT**를 선택합니다.
- **Rule Placement(**규칙 배치**)** - 규칙을 추가할 위치를 선택합니다. 규칙은 카테고리에서 자동 NAT 규칙 앞이나 뒤에 삽입할 수도 있고, 선택한 규칙 위나 아래에 삽입할 수도 있습니다.
- **Type(**유형**)** - 고정을 선택합니다. 이 설정은 소스 주소에만 적용됩니다. 대상 주소에 대해 변환을 정의하는 경우 변환은 항상 고정입니다.

단계 **4** 다음 인터페이스 옵션을 구성합니다.

- 소스 인터페이스, 대상 인터페이스 — (브리지 그룹 멤버 인터페이스의 경우 필수) 이 NAT 규칙을 적용할 인터페이스입니다. **Source(**소스**)**는 트래픽이 디바이스로 들어가는 데 사용되는 실제 인터페이스입니다. **Destination(**대상**)**은 트래픽이 디바이스에서 나오는 데 사용되는 매핑된 인터페이스입니다. 기본적으로 규칙은 브리지 그룹 멤버 인터페이스를 제외한 모든 인터페이스(**Any(**모두**)**)에 적용됩니다.

단계 **5** 원본 패킷 주소(IPv4 또는 IPv6)를 식별합니다. 이 주소는 원본 패킷에 표시되는 패킷 주소입니다.

원래 패킷 대 변환된 패킷의 예는 다음 그림을 참조하십시오. 여기서 내부 호스트에 대해서는 ID NAT를 수행하지만 외부 호스트는 변환합니다.



- **Original Source Address(**원본 소스 주소**)** - 변환 중인 주소가 포함된 네트워크 개체 또는 그룹입니다.
- **Original Destination Address(**원본 대상 주소**)** - (선택 사항) 대상의 주소를 포함하는 네트워크 개체입니다. 이 옵션을 비워 두면 대상에 관계없이 소스 주소 변환이 적용됩니다. 대상 주소를 지정하면 해당 주소에 대해 고정 변환을 구성할 수도 있고 단순히 ID NAT를 사용할 수도 있습니다.

  인터페이스를 선택하여 소스 인터페이스(임의일 수 없음)를 기준으로 원본 대상을 지정할 수 있습니다. 이 옵션을 선택할 경우 변환된 대상 개체도 선택해야 합니다. 대상 주소에 대해 포트 변환 고정 인터페이스 NAT를 구현하려면 이 옵션을 선택하고 대상 포트에 대해 적절한 포트 개체도 선택합니다.

단계 **6** 변환된 패킷 주소(IPv4 또는 IPv6), 즉 대상 인터페이스 네트워크에 나타나는 패킷 주소를 확인합니다. 필요에 따라 IPv4 및 IPv6 간에 변환할 수 있습니다.

- 변환된 소스 주소 - 원본 소스와 동일한 개체입니다. 원하는 경우 콘텐츠가 정확히 동일한 다른 개체를 선택할 수 있습니다.

- 변환된 대상 주소 - (선택 사항) 변환된 패킷에서 사용되는 대상 주소를 포함하는 네트워크 개체 또는 그룹입니다. 원본 대상 주소에 대해 개체를 선택한 경우 동일한 개체를 선택하여 ID NAT(변환 없음)를 설정할 수 있습니다.

단계 **7** (선택 사항). 서비스 변환의 원본 또는 대상 서비스 포트를 식별합니다.

포트 변환 고정 NAT를 구성하는 경우 소스나 대상 또는 둘 다에 대해 포트를 변환할 수 있습니다. 예를 들어 TCP/80과 TCP/8080 간에 변환할 수 있습니다.

NAT는 TCP 또는 UDP만 지원합니다. 포트를 변환할 때는 실제 서비스 개체의 프로토콜과 매핑된 서비스 개체의 프로토콜이 동일해야 합니다(둘 다 TCP거나 둘 다 UDP). ID NAT의 경우 실제 포트와 매핑된 포트에 동일한 서비스 개체를 사용할 수 있습니다.

- 원본 소스 포트, 변환된 소스 포트 - 소스 주소에 대한 포트 변환을 정의합니다.
- 원본 대상 포트, 변환된 대상 포트 - 대상 주소에 대한 포트 변환을 정의합니다.

단계 **8** (선택 사항). 고급 옵션 링크를 클릭하고 원하는 옵션을 선택합니다.

- 이 규칙과 일치하는 **DNS** 응답 변환 - ID NAT의 경우에는 이 옵션을 구성하지 마십시오.
- 대상 인터페이스에서 **ARP** 프록시 설정 안 함 - 매핑된 IP 주소로 들어오는 패킷에 대해 프록시 ARP를 비활성화합니다. 매핑된 인터페이스와 동일한 네트워크의 주소를 사용하는 경우 시스템은 매핑된 주소에 대한 ARP 요청에 답하기 위해 프록시 ARP를 사용하며, 이에 따라 매핑된 주소로 가야 하는 트래픽을 가로챕니다. 디바이스가 추가 네트워크에 대한 게이트웨이가 될 필요가 없으므로 이 솔루션은 라우팅을 간소화합니다. 원하는 경우 프록시 ARP를 비활성화할 수 있습니다. 이 경우 업스트림 라우터에 적절한 경로가 있어야 합니다. 일반적으로 ID NAT에는 프록시 ARP가 필요하지 않으며, 프록시 ARP를 사용할 경우 연결 문제가 발생할 수도 있습니다.
- 대상 인터페이스에 대해 경로 조회 수행 - 원본 및 변환된 소스 주소에 대해 동일한 개체를 선택할 때 소스 및 대상 인터페이스를 선택하는 경우 이 옵션을 선택하면 시스템이 NAT 규칙에 구성된 대상 인터페이스를 사용하는 대신 라우팅 테이블을 기준으로 하여 대상 인터페이스를 결정하도록 할 수 있습니다.

단계 **9** **OK(**확인**)**를 클릭합니다.

Threat Defense NAT 규칙 속성

NAT(네트워크 주소 변환) 규칙을 사용하여 IP 주소를 다른 IP 주소로 변환합니다. 일반적으로는 NAT 규칙을 사용하여 전용 어드레스를 공개적으로 라우팅 가능한 주소로 변환합니다. 변환을 주소 간에 수행할 수도 있고, PAT(포트 주소 변환)를 사용해 여러 주소를 하나의 주소로 변환하고 포트 번호를 사용해 각 소스 주소를 구분할 수도 있습니다.

NAT 규칙은 다음 기본 속성을 포함합니다. 이러한 속성은 별도로 명시된 경우를 제외하면 자동 NAT 및 수동 NAT 규칙에 대해 동일합니다.

직책

규칙의 이름을 입력합니다. 이름은 공백을 포함할 수 없습니다.

규칙 생성

변환 규칙이 자동 **NAT**인지 아니면 수동 **NAT**인지를 나타냅니다. 자동 NAT는 수동 NAT보다 간단하지만, 수동 NAT를 수행하는 경우에는 대상 주소를 기준으로 하여 소스 주소에 대해 별도의 변환을 생성할 수 있습니다.

상태

규칙을 활성화할지 아니면 비활성화할지를 나타냅니다.

배치**(**수동 **NAT**에만 해당함**)**

규칙을 추가할 위치를 선택합니다. 규칙은 카테고리에서 자동 NAT 규칙 앞이나 뒤에 삽입할 수도 있고, 선택한 규칙 위나 아래에 삽입할 수도 있습니다.

유형

변환 규칙이 동적인지 아니면 정적인지를 나타냅니다. 동적 변환에서는 주소 풀에서 매핑된 주소를 자동으로 선택하며, PAT를 구현할 때는 주소/포트 조합을 선택합니다. 매핑된 주소/포트를 정확하게 정의하려면 정적 변환을 사용하십시오.

다음 주제에서는 나머지 NAT 규칙 속성에 대해 설명합니다.

자동 **NAT**의 패킷 변환 속성

패킷 변환 옵션을 사용하여 소스 주소와 매핑된 변환 주소를 정의합니다. 다음 속성은 자동 NAT에만 적용됩니다.

소스 인터페이스**,** 대상 인터페이스

(브리지 그룹 멤버 인터페이스의 경우 필수) 이 NAT 규칙을 적용할 인터페이스입니다. **Source(**소스**)**는 트래픽이 디바이스로 들어가는 데 사용되는 실제 인터페이스입니다. **Destination(**대상**)**은 트래픽이 디바이스에서 나오는 데 사용되는 매핑된 인터페이스입니다. 기본적으로 규칙은 브리지 그룹 멤버 인터페이스를 제외한 모든 인터페이스(**Any(**모두**)**)에 적용됩니다.

원본 주소**(**항상 필수**)**

변환 중인 소스 주소를 포함하는 네트워크 개체입니다. 그룹이 아닌 네트워크 개체여야 하며, 호스트, 범위 또는 서브넷일 수 있습니다.

변환된 주소**(**대개 필수**)**

원본 주소를 변환하는 매핑된 주소입니다. 여기서 선택하는 항목에 따라 정의하는 변환 규칙의 유형이 달라집니다.

- 동적 **NAT** - 매핑된 주소를 포함하는 네트워크 개체 또는 그룹입니다. 네트워크 개체 또는 그룹일 수 있지만 서브넷을 포함할 수는 없습니다. IPv4 주소와 IPv6 주소를 모두 포함할 수는 없으며 한 유형만 포함해야 합니다. 그룹에 범위와 호스트 IP 주소가 모두 포함되어 있으면 범위는 동적 NAT에 사용되고 호스트 IP 주소는 PAT 대안으로 사용됩니다.
- 동적 **PAT** - 다음 중 하나입니다.
  - (인터페이스 PAT) 대상 인터페이스의 IPv4 주소를 사용하려면 인터페이스를 선택합니다. 특정 대상 인터페이스도 선택해야 합니다. 이 인터페이스는 브리지 그룹 멤버 인터페이스일 수 없습니다. IPv6에는 인터페이스 PAT를 사용할 수 없습니다.

- 대상 인터페이스 주소가 아닌 단일 주소를 사용하려면 이러한 용도로 생성한 호스트 네트워크 개체를 선택합니다.

- 고정 **NAT** - 다음 중 하나입니다.
  - 설정된 주소 그룹을 사용하려면 매핑된 주소를 포함하는 네트워크 개체 또는 그룹을 선택합니다. 개체 또는 그룹은 호스트, 범위 또는 서브넷을 포함할 수 있습니다. 일반적으로 일대일 매핑의 경우 동일한 수의 매핑된 주소를 실제 주소로 구성합니다. 그러나 주소의 수가 일치하지 않아도 됩니다.
  - (포트 변환 기능이 있는 고정 인터페이스 NAT) 대상 인터페이스의 주소를 사용하려면 인터페이스를 선택합니다. 특정 대상 인터페이스도 선택해야 합니다. 이 인터페이스는 브리지 그룹 멤버 인터페이스일 수 없습니다. 이 경우 포트 변환 고정 인터페이스 NAT가 구성됩니다. 소스 주소/포트는 인터페이스의 주소 및 동일한 포트 번호로 변환됩니다. IPv6에는 인터페이스 PAT를 사용할 수 없습니다.

- **ID NAT** - 원본 소스와 동일한 개체입니다. 원하는 경우 콘텐츠가 정확히 동일한 다른 개체를 선택할 수 있습니다.

원본 포트**,** 변환된 포트**(**고정 **NAT**에만 해당됨**)**

TCP 또는 UDP 포트를 변환해야 하는 경우 원본 포트와 변환된 포트를 정의하는 포트 개체를 선택합니다. 이 경우 동일한 프로토콜의 개체를 선택해야 합니다. 예를 들어, 필요에 따라 TCP/80을 TCP/8080으로 변환할 수 있습니다.

수동 **NAT**의 패킷 변환 속성

패킷 변환 옵션을 사용하여 소스 주소와 매핑된 변환 주소를 정의합니다. 다음 속성은 수동 NAT에만 적용됩니다. 별도로 표시된 항목을 제외한 모든 항목은 선택 사항입니다.

소스 인터페이스**,** 대상 인터페이스

(브리지 그룹 멤버 인터페이스의 경우 필수) 이 NAT 규칙을 적용할 인터페이스입니다. **Source(**소스**)**는 트래픽이 디바이스로 들어가는 데 사용되는 실제 인터페이스입니다. **Destination(**대상**)**은 트래픽이 디바이스에서 나오는 데 사용되는 매핑된 인터페이스입니다. 기본적으로 규칙은 브리지 그룹 멤버 인터페이스를 제외한 모든 인터페이스(**Any(**모두**)**)에 적용됩니다.

원본 소스 주소**(**항상 필수**)**

변환 중인 주소를 포함하는 네트워크 개체 또는 그룹입니다. 네트워크 개체 또는 그룹일 수 있으며, 호스트, 범위 또는 서브넷을 포함할 수 있습니다. 모든 원본 소스 트래픽을 변환하려는 경우 규칙에서 임의를 지정하면 됩니다.

변환된 소스 주소**(**대개 필수**)**

원본 주소를 변환하는 매핑된 주소입니다. 여기서 선택하는 항목에 따라 정의하는 변환 규칙의 유형이 달라집니다.

- 동적 **NAT** - 매핑된 주소를 포함하는 네트워크 개체 또는 그룹입니다. 네트워크 개체 또는 그룹일 수 있지만 서브넷을 포함할 수는 없습니다. IPv4 주소와 IPv6 주소를 모두 포함할 수

는 없으며 한 유형만 포함해야 합니다. 그룹에 범위와 호스트 IP 주소가 모두 포함되어 있으면 범위는 동적 NAT에 사용되고 호스트 IP 주소는 PAT 대안으로 사용됩니다.

- 동적 **PAT** - 다음 중 하나입니다.
  - (인터페이스 PAT) 대상 인터페이스의 주소를 사용하려면 인터페이스를 선택합니다. 특정 대상 인터페이스도 선택해야 합니다. 이 인터페이스는 브리지 그룹 멤버 인터페이스일 수 없습니다. IPv6에는 인터페이스 PAT를 사용할 수 없습니다.
  - 대상 인터페이스 주소가 아닌 단일 주소를 사용하려면 이러한 용도로 생성한 호스트 네트워크 개체를 선택합니다.
- 고정 **NAT** - 다음 중 하나입니다.
  - 설정된 주소 그룹을 사용하려면 매핑된 주소를 포함하는 네트워크 개체 또는 그룹을 선택합니다. 개체 또는 그룹은 호스트, 범위 또는 서브넷을 포함할 수 있습니다. 일반적으로 일대일 매핑의 경우 동일한 수의 매핑된 주소를 실제 주소로 구성합니다. 그러나 주소의 수가 일치하지 않아도 됩니다.
  - (포트 변환 기능이 있는 고정 인터페이스 NAT) 대상 인터페이스의 주소를 사용하려면 인터페이스를 선택합니다. 특정 대상 인터페이스도 선택해야 합니다. 이 인터페이스는 브리지 그룹 멤버 인터페이스일 수 없습니다. 이 경우 포트 변환 고정 인터페이스 NAT가 구성됩니다. 소스 주소/포트는 인터페이스의 주소 및 동일한 포트 번호로 변환됩니다. IPv6에는 인터페이스 PAT를 사용할 수 없습니다.
- **ID NAT** - 원본 소스와 동일한 개체입니다. 원하는 경우 콘텐츠가 정확히 동일한 다른 개체를 선택할 수 있습니다.

원본 대상 주소

대상의 주소를 포함하는 네트워크 개체입니다. 이 옵션을 비워 두면 대상에 관계없이 소스 주소 변환이 적용됩니다. 대상 주소를 지정하면 해당 주소에 대해 고정 변환을 구성할 수도 있고 단순히 ID NAT를 사용할 수도 있습니다.

인터페이스를 선택하여 소스 인터페이스(임의일 수 없음)를 기준으로 원본 대상을 지정할 수 있습니다. 이 옵션을 선택할 경우 변환된 대상 개체도 선택해야 합니다. 대상 주소에 대해 포트 변환 고정 인터페이스 NAT를 구현하려면 이 옵션을 선택하고 대상 포트에 대해 적절한 포트 개체도 선택합니다.

변환된 대상 주소

변환된 패킷에서 사용되는 대상 주소를 포함하는 네트워크 개체 또는 그룹입니다. 원본 대상에 대해 개체를 선택한 경우 동일한 개체를 선택하여 ID NAT(변환 없음)를 설정할 수 있습니다.

정규화된 도메인 이름을 변환된 대상으로 지정하는 네트워크 개체를 사용할 수 있습니다. 자세한 내용은 FQDN 대상 지침, 596 페이지 항목을 참조하십시오.

원본 소스 포트, 변환된 소스 포트, 원본 대상 포트, 변환된 대상 포트

원본 및 변환된 패킷의 소스 및 대상 서비스를 정의하는 포트 개체입니다. 포트를 변환할 수도 있고, 동일한 개체를 선택하여 포트를 변환하지 않고 규칙이 서비스에 따라 달라지도록 설정할 수도 있습니다. 서비스를 구성할 때는 다음 규칙에 유의하십시오.

- (동적 NAT 또는 PAT) 원본 소스 포트 및 변환된 소스 포트에 대해서는 변환을 수행할 수 없습니다. 대상 포트에 대해서만 변환을 수행할 수 있습니다.
- NAT는 TCP 또는 UDP만 지원합니다. 포트를 변환할 때는 실제 서비스 개체의 프로토콜과 매핑된 서비스 개체의 프로토콜이 동일해야 합니다(둘 다 TCP거나 둘 다 UDP). ID NAT의 경우 실제 포트와 매핑된 포트에 동일한 개체를 사용할 수 있습니다.

고급 NAT 속성

NAT를 구성할 때는 고급 옵션에서 특수 서비스를 제공하는 속성을 구성할 수 있습니다. 이러한 모든 속성은 선택 사항이므로 서비스가 필요할 때만 구성하면 됩니다.

이 규칙과 일치하는 **DNS** 응답 변환

DNS 응답의 IP 주소를 변환할지 여부를 선택합니다. 매핑된 인터페이스에서 실제 인터페이스로 이동하는 DNS 응답의 경우 주소(IPv4 A 또는 IPv6 AAAA) 레코드가 매핑된 값에서 실제 값으로 재작성됩니다. 반대로, 실제 인터페이스에서 매핑된 인터페이스로 이동하는 DNS 응답의 경우 실제 값에서 매핑된 값으로 레코드가 재작성됩니다. 이 옵션은 특정 상황에서 사용되며, 재작성 시 A 레코드와 AAAA 레코드 간의 변환도 수행되는 NAT64/46 변환에 필요한 경우도 있습니다. 자세한 내용은 NAT를 사용하여 DNS 쿼리 및 응답 재작성, 663 페이지를 참조하십시오. 정적 NAT 규칙에서 포트 변환을 수행하는 경우에는 이 옵션을 사용할 수 없습니다.

인터페이스 **PAT(**대상 인터페이스**)**로 폴스루**(**동적 **NAT**만 해당됨**)**

다른 매핑된 주소가 이미 할당된 경우 대상 인터페이스의 IP 주소를 백업 방법으로 사용할지 여부를 선택합니다(인터페이스 PAT 대체). 이 옵션은 브리지 그룹의 멤버가 아닌 대상 인터페이스를 선택한 경우에만 사용할 수 있습니다. 인터페이스 PAT를 변환된 주소로 이미 컨피그레이션한 경우에는 이 옵션을 선택할 수 없습니다. IPv6 네트워크에서는 이 옵션을 사용할 수 없습니다.

대상 인터페이스에서 **ARP** 프록시 설정 안 함**(**고정 **NAT**만 해당됨**)**

매핑된 IP 주소로 들어오는 패킷에 대해 프록시 ARP를 비활성화합니다. 매핑된 인터페이스와 동일한 네트워크의 주소를 사용하는 경우 시스템은 매핑된 주소에 대한 ARP 요청에 답하기 위해 프록시 ARP를 사용하며, 이에 따라 매핑된 주소로 가야 하는 트래픽을 가로챕니다. 디바이스가 추가 네트워크에 대한 게이트웨이가 될 필요가 없으므로 이 솔루션은 라우팅을 간소화합니다. 원하는 경우 프록시 ARP를 비활성화할 수 있습니다. 이 경우 업스트림 라우터에 적절한 경로가 있어야 합니다. 일반적으로 ID NAT에는 프록시 ARP가 필요하지 않으며, 프록시 ARP를 사용할 경우 연결 문제가 발생할 수도 있습니다.

대상 인터페이스에 대해 경로 조회 수행**(**고정 **ID NAT** 및 라우팅 모드만 해당됨**)**

원본 및 변환된 소스 주소에 대해 동일한 개체를 선택할 때 소스 및 대상 인터페이스를 선택하는 경우 이 옵션을 선택하면 시스템이 NAT 규칙에 구성된 대상 인터페이스를 사용하는 대신 라우팅 테이블을 기준으로 하여 대상 인터페이스를 결정하도록 할 수 있습니다.

IPv6 네트워크 변환

IPv6 전용 및 IPv4 전용 네트워크 간에 트래픽을 전달해야 하는 경우에는 NAT를 사용해 주소 유형을 변환해야 합니다. 두 IPv6 네트워크 간에 트래픽을 전달할 때도 외부 네트워크에서 내부 네트워크를 숨기려는 경우가 있습니다.

IPv6 네트워크에서는 다음 변환 유형을 사용할 수 있습니다.

- NAT64, NAT46 - IPv6 패킷에서 IPv4 패킷으로, 또는 그 반대로 변환합니다. 이 경우 두 개의 정책(IPv6에서 IPv4로의 변환 정책과 IPv4에서 IPv6으로의 변환 정책)을 정의해야 합니다. 단일 수동 NAT 규칙을 사용하여 정책 2개를 정의할 수는 있지만, DNS 서버가 외부 네트워크에 있는 경우에는 DNS 응답을 재작성해야 할 수도 있습니다. 대상을 지정할 때는 수동 NAT 규칙에 대해 DNS 재작성을 활성화할 수 없으므로 자동 NAT 규칙 2개를 생성하는 것이 더 나은 해결책입니다.

참고 NAT46은 정적 매핑만 지원합니다.

- NAT66 - IPv6 패킷을 다른 IPv6 주소로 변환합니다. 고정 NAT를 사용하는 것이 좋습니다. 동적 NAT 또는 PAT를 사용할 수 있고 IPv6 주소가 대량으로 공급되지만, 동적 NAT를 반드시 사용할 필요는 없습니다.

참고 NAT64 및 NAT 46은 표준 라우팅 인터페이스에서만 사용할 수 있습니다. NAT66은 라우팅 인터페이스 및 브리지 그룹 멤버 인터페이스에서 모두 사용 가능합니다.

NAT64/46: IPv6 주소를 IPv4로 변환

트래픽이 IPv6 네트워크에서 IPv4 전용 네트워크로 이동하는 경우에는 IPv6 주소를 IPv4로 변환해야 하며, 반환 트래픽은 IPv4에서 IPv6으로 변환해야 합니다. 따라서 주소 풀 2개(IPv4 네트워크에서 IPv6 주소를 바인딩하기 위한 IPv4 주소 풀과 IPv6 네트워크에서 IPv4 주소를 바인딩하기 위한 IPv6 주소 풀)를 정의해야 합니다.

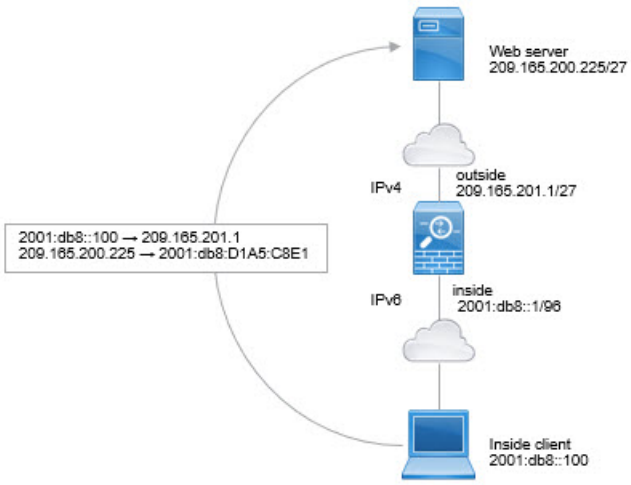
- NAT64 규칙용 IPv4 주소 풀은 일반적으로 크기가 작으므로 대개 IPv6 클라이언트 주소와 일대일로 매핑할 주소를 충분히 포함하지 않을 수 있습니다. 동적 PAT의 경우 동적 또는 고정 NAT에 비해 더 쉽게 많은 IPv6 클라이언트 주소를 포함할 수 있습니다.
- NAT46 규칙용 IPv6 주소 풀은 매핑할 IPv4 주소보다 많은 수의 주소를 포함할 수 있습니다. 따라서 각 IPv4 주소를 서로 다른 IPv6 주소에 매핑할 수 있습니다. NAT46은 고정 매핑만 지원하므로 동적 PAT는 사용할 수 없습니다.

소스 IPv6 네트워크와 대상 IPv4 네트워크 중에 하나씩 2개의 정책을 정의해야 합니다. 단일 수동 NAT 규칙을 사용하여 정책 2개를 정의할 수는 있지만, DNS 서버가 외부 네트워크에 있는 경우에는 DNS

응답을 재작성해야 할 수도 있습니다. 대상을 지정할 때는 수동 NAT 규칙에 대해 DNS 재작성을 활성화할 수 없으므로 자동 NAT 규칙 2개를 생성하는 것이 더 나은 해결책입니다.

NAT64/46 예: 내부 IPv6 네트워크 및 외부 IPv4 인터넷

다음은 내부 IPv6 전용 네트워크를 보유하고 있으며 인터넷으로 전송된 트래픽에 대해 IPv4로 변환하려는 경우의 간단한 예입니다. 이 예에서는 DNS 변환이 필요하지 않다고 가정하므로 단일 수동 NAT 규칙에서 NAT64 및 NAT46 변환을 모두 수행할 수 있습니다.



이 예에서는 외부 인터페이스의 IP 주소가 포함된 동적 인터페이스 PAT를 사용하여 내부 IPv6 네트워크를 IPv4로 변환합니다. 외부 IPv4 트래픽은 2001:db8::/96 네트워크의 주소로 정적 변환되어 내부 네트워크에서 전송을 허용합니다.

프로시저

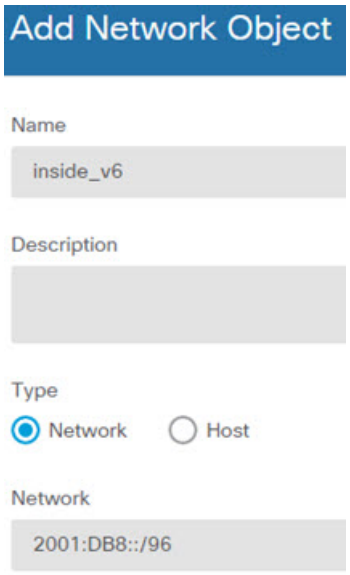
단계 **1** 내부 IPv6 네트워크용 네트워크 개체를 생성합니다.

a) **Objects(**개체**)**를 선택합니다.

b) 목차에서 **Network(**네트워크**)**를 선택하고 +를 클릭합니다.

c) 내부 IPv6 네트워크를 정의합니다.

네트워크 개체의 이름을 inside_v6과 같이 지정하고 **Network(**네트워크**)**를 선택한 후에 네트워크 주소 2001:db8::/96을 입력합니다.



d) **OK(**확인**)**를 클릭합니다.

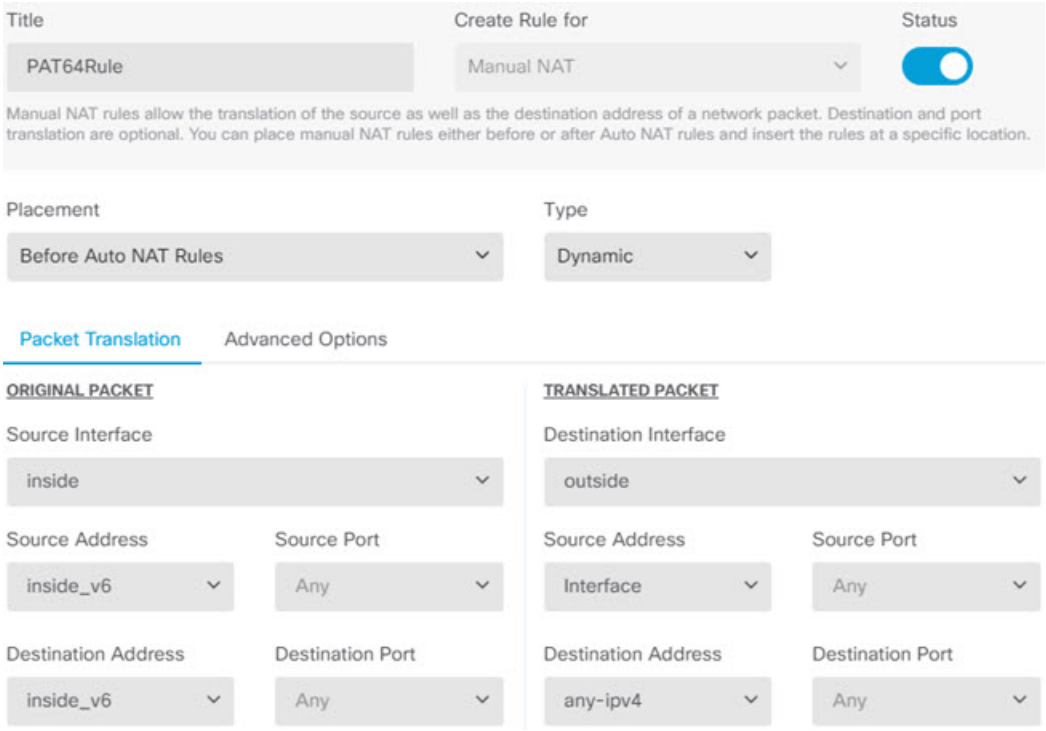
단계 **2** 수동 NAT 규칙을 생성하여 IPv6 네트워크를 IPv4로 변환한 후 다시 되돌립니다.

a) **Policies(**정책**)** > **NAT**를 선택합니다.

b) **+** 버튼을 클릭합니다.

c) 다음 속성을 구성합니다.

- **Title(**제목**)** = PAT64Rule 또는 원하는 다른 이름
- **Create Rule For(**규칙 생성 대상**)** = **Manual NAT(**수동 **NAT)**
- **Placement(**배치**)** = **Before Auto NAT Rules(**자동 **NAT** 규칙 앞**)**
- **Type(**유형**)** = **Dynamic(**동적**)**
- **Source Interface(**원본 인터페이스**)** = inside
- **Destination Interface(**대상 인터페이스**)** = outside
- **Original Packet Source Address(**원본 패킷 소스 주소**)** = inside_v6 네트워크 개체
- **Translated Packet Source Address(**변환된 패킷 소스 주소**)** = Interface(인터페이스) 이 옵션은 PAT 주소로 대상 인터페이스의 IPv4 주소를 사용합니다.
- **Original Packet Destination Address(**원본 패킷 대상 주소**)** = inside_v6 네트워크 개체
- **Translated Packet Destination Address(**변환된 패킷 대상 주소**)** = any-ipv4 네트워크 개체

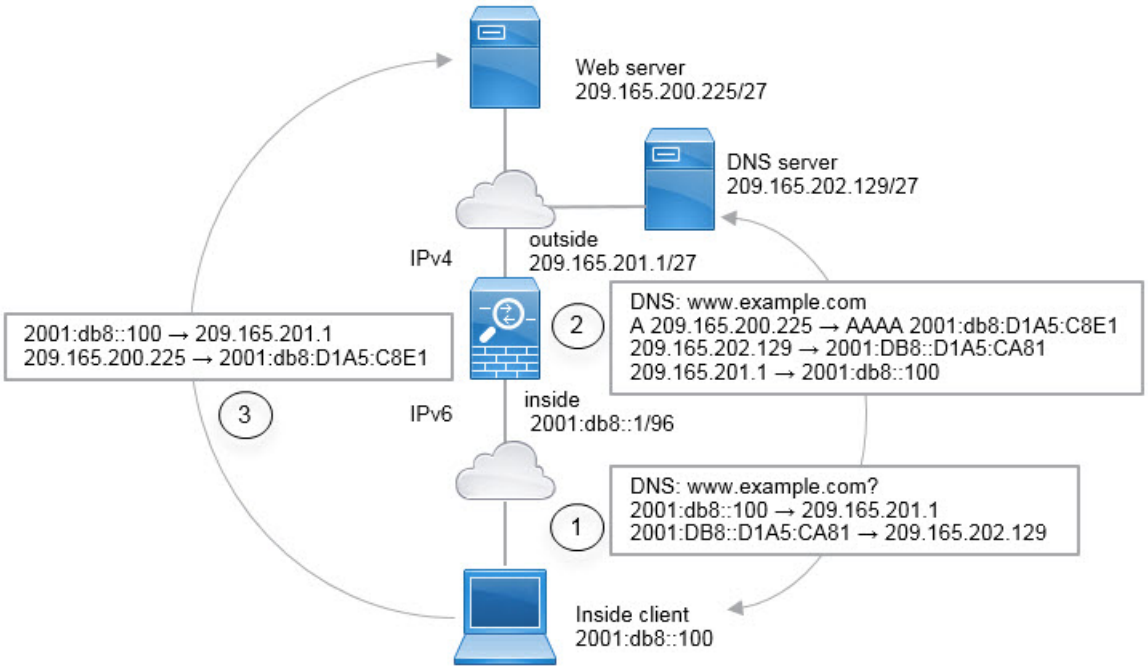


d) **OK(**확인**)**를 클릭합니다.

이 규칙을 사용하는 경우 내부 인터페이스의 2001:db8::/96 서브넷에서 외부 인터페이스로 이동하는 모든 트래픽은 외부 인터페이스의 IPv4 주소를 사용하여 NAT64 PAT로 변환됩니다. 반대로 외부 네트워크에서 내부 인터페이스로 들어오는 모든 IPv4 주소는 임베디드 IPv4 주소 메서드를 사용하여 2001:db8::/96 네트워크의 주소로 변환됩니다.

NAT64/46 예: 내부 IPv6 네트워크와 외부 IPv4 인터넷 및 DNS 변환

아래에는 내부 IPv6 전용 네트워크가 있는데 내부 사용자에게 필요한 일부 IPv4 전용 서비스는 외부 인터넷에 있는 일반적인 예가 나와 있습니다.



이 예에서는 외부 인터페이스의 IP 주소가 포함된 동적 인터페이스 PAT를 사용하여 내부 IPv6 네트워크를 IPv4로 변환합니다. 외부 IPv4 트래픽은 2001:db8::/96 네트워크의 주소로 정적 변환되어 내부 네트워크에서 전송을 허용합니다. 외부 DNS 서버의 회신을 A(IPv4) 레코드에서 AAAA(IPv6) 레코드로 변환하고 주소를 IPv4에서 IPv6으로 변환할 수 있도록 NAT46 규칙에 대해 DNS 재작성을 활성화합니다.

내부 IPv6 네트워크의 2001:DB8::100에 있는 클라이언트가 www.example.com을 열려고 하는 웹 요청의 일반적인 순서는 다음과 같습니다.

1. 클라이언트의 컴퓨터가 2001:DB8::D1A5:CA81에 있는 DNS 서버에 DNS 요청을 보냅니다. NAT 규칙이 DNS 요청에서 소스 및 대상을 다음과 같이 변환합니다.
   - 2001:DB8::100을 209.165.201.1의 고유 포트로 변환합니다(NAT64 인터페이스 PAT 규칙).
   - 2001:DB8::D1A5:CA81을 209.165.202.129로 변환합니다(NAT46 규칙. D1A5:CA81은 209.165.202.129에 해당하는 IPv6 주소입니다.).
2. DNS 서버가 www.example.com이 209.165.200.225에 있음을 나타내는 A 레코드로 응답합니다. DNS 재작성이 활성화된 NAT46 규칙이 A 레코드를 IPv6의 동일 AAAA 레코드로 변환하고 AAAA 레코드의 209.165.200.225를 2001:db8:D1A5:C8E1로 변환합니다. 또한 DNS 응답의 소스 및 대상 주소는 변환되지 않은 상태입니다.
   - 209.165.202.129 -> 2001:DB8::D1A5:CA81
   - 209.165.201.1 -> 2001:db8::100
3. 이제 IPv6 클라이언트는 웹 서버의 IP 주소를 포함하며 2001:db8:D1A5:C8E1의 www.example.com에 대한 HTTP 요청을 수행합니다. D1A5:C8E1은 209.165.200.225에 해당하는 IPv6 주소입니다. 그리고 HTTP 요청의 소스 및 대상이 변환됩니다.

- 2001:DB8::100을 209.156.101.54의 고유 포트로 변환합니다(NAT64 인터페이스 PAT 규칙).
- 2001:db8:D1A5:C8E1을 209.165.200.225로 변환합니다(NAT46 규칙).

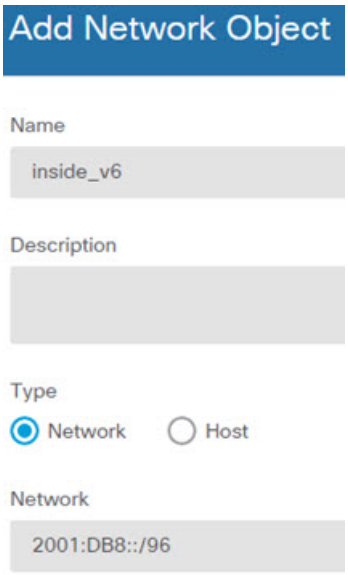
다음 절차에서는 이 예를 구성하는 방법을 설명합니다.

프로시저

단계 **1** 내부 IPv6 및 외부 IPv4 네트워크를 정의하는 네트워크 개체를 생성합니다.

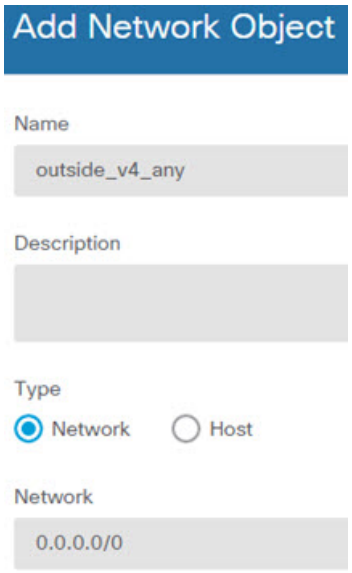
a) **Objects(**개체**)**를 선택합니다.
b) 목차에서 **Network(**네트워크**)**를 선택하고 +를 클릭합니다.
c) 내부 IPv6 네트워크를 정의합니다.

네트워크 개체의 이름을 inside_v6과 같이 지정하고 **Network(**네트워크**)**를 선택한 후에 네트워크 주소 2001:db8::/96을 입력합니다.



d) **OK(**확인**)**를 클릭합니다.
e) +를 클릭하여 외부 IPv4 네트워크를 정의합니다.

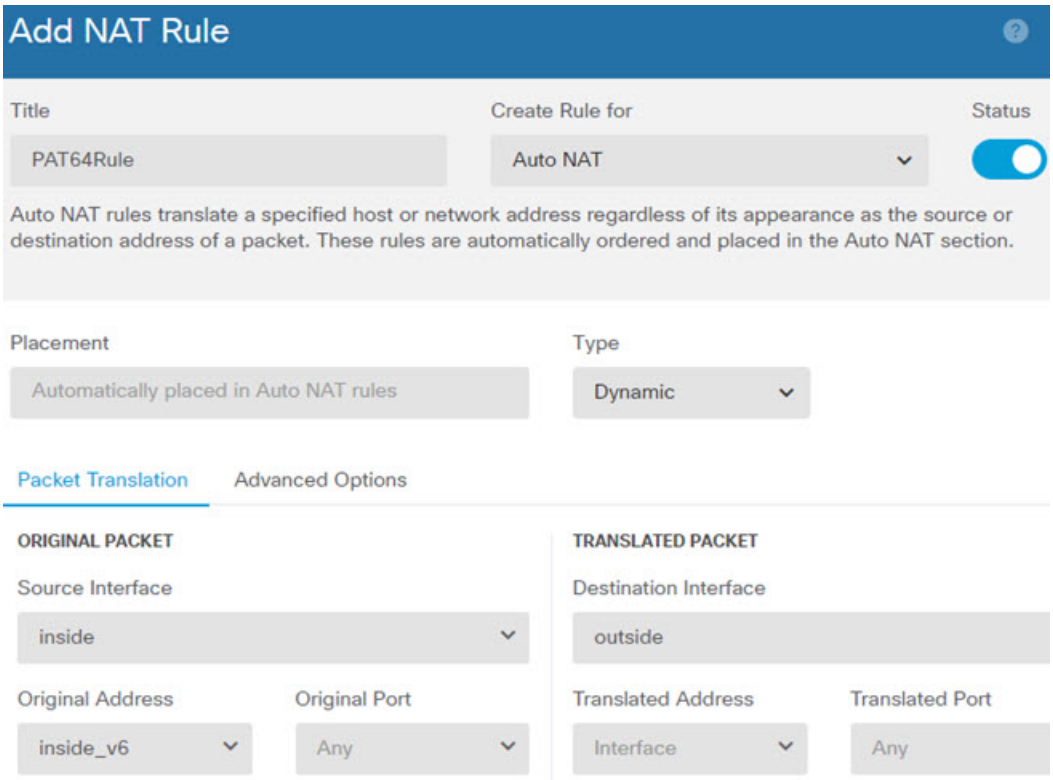
네트워크 개체의 이름을 outside_v4_any와 같이 지정하고 **Network(**네트워크**)**를 선택한 후에 네트워크 주소 0.0.0.0/0을 입력합니다.



단계 **2** 내부 IPv6 네트워크용 NAT64 동적 PAT 규칙을 구성합니다.

a) **Policies(**정책**)** > **NAT**를 선택합니다.
b) + 버튼을 클릭합니다.
c) 다음 속성을 구성합니다.

- **Title(**제목**)** = PAT64Rule 또는 원하는 다른 이름
- **Create Rule For(**규칙 생성**)** = 자동 NAT
- **Type(**유형**)** = 동적
- **Source Interface(**원본 인터페이스**)** = inside
- **Destination Interface(**대상 인터페이스**)** = outside
- **Original Address(**원본 주소**)** = inside_v6 네트워크 개체
- **Translated Address(**변환된 주소**)** = **Interface**. 이 옵션은 PAT 주소로 대상 인터페이스의 IPv4 주소를 사용합니다.



d) **OK(**확인**)**를 클릭합니다.

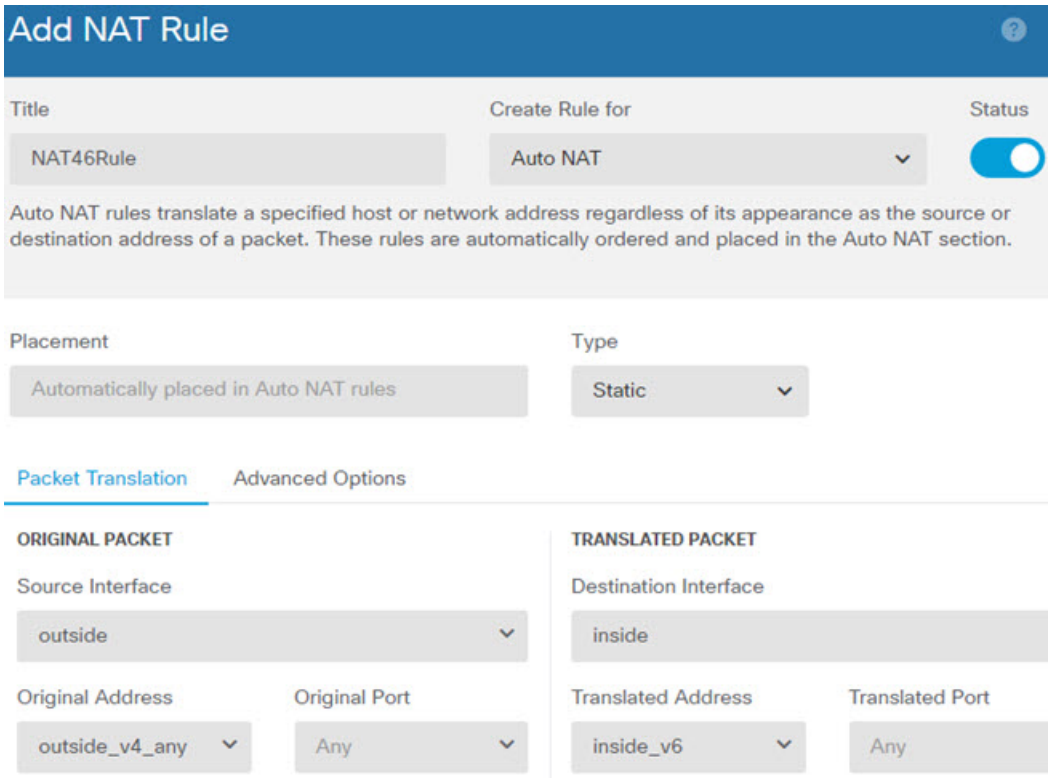
이 규칙을 사용하는 경우 내부 인터페이스의 2001:db8::/96 서브넷에서 외부 인터페이스로 이동하는 모든 트래픽은 외부 인터페이스의 IPv4 주소를 사용하여 NAT64 PAT로 변환됩니다.

단계 **3** 외부 IPv4 네트워크용 고정 NAT46 규칙을 구성합니다.

a) + 버튼을 클릭합니다.

b) 다음 속성을 구성합니다.

- **Title(**제목**)** = NAT46Rule 또는 원하는 다른 이름
- **Create Rule For(**규칙 생성**)** = 자동 NAT
- **Type(**유형**)** = 고정
- **Source Interface(**원본 인터페이스**)** = outside
- **Destination Interface(**대상 인터페이스**)** = inside
- **Original Address(**원본 주소**)** = outside_v4_any 네트워크 개체
- **Translated Address(**변환된 주소**)** = inside_v6 네트워크 개체
- **Advanced Options(**고급 옵션**)** 탭에서 **Translate DNS replies that match this rule(**이 규칙과 일치하는 **DNS** 응답 변환**)**을 선택합니다.



c) **OK(**확인**)**를 클릭합니다.

이 규칙을 사용하는 경우 외부 네트워크에서 내부 인터페이스로 들어오는 모든 IPv4 주소는 임베디드 IPv4 주소 방법을 사용하여 2001:db8::/96 네트워크의 주소로 변환됩니다. 또한 DNS 응답은 A(IPv4) 레코드에서 AAAA(IPv6) 레코드로 변환되며 주소는 IPv4에서 IPv6으로 변환됩니다.

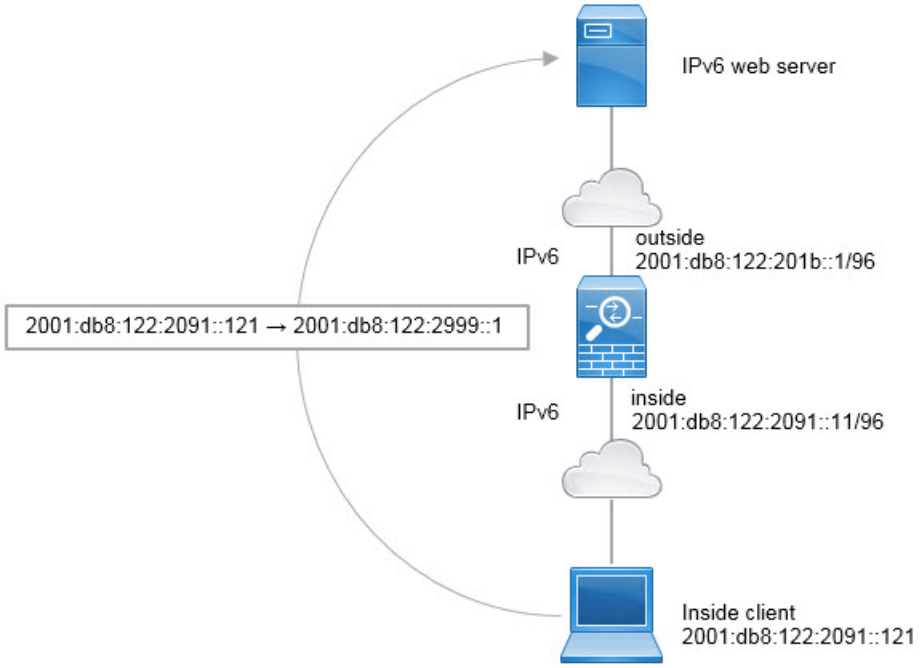
NAT66: IPv6 주소를 다른 IPv6 주소로 변환

IPv6 네트워크 간을 이동할 때는 주소를 외부 네트워크의 다른 IPv6 주소로 변환할 수 있습니다. 고정 NAT를 사용하는 것이 좋습니다. 동적 NAT 또는 PAT를 사용할 수 있고 IPv6 주소가 대량으로 공급되지만, 동적 NAT를 반드시 사용할 필요는 없습니다.

서로 다른 주소 유형 간을 변환하는 것이 아니므로 NAT66 변환을 위한 규칙 하나만 있으면 됩니다. 자동 NAT를 사용하면 이러한 규칙을 쉽게 모델링할 수 있습니다. 그러나 반환 트래픽을 허용하지 않으려면 수동 NAT만 사용해 정적 NAT 규칙을 단방향으로 설정할 수 있습니다.

NAT66 예, 네트워크 간의 고정 변환

자동 NAT를 사용하여 IPv6 주소 풀 간의 고정 변환을 컨피그레이션할 수 있습니다. 다음 예에서는 2001:db8:122:2091::/96 네트워크의 내부 주소를 2001:db8:122:2999::/96 네트워크의 외부 주소로 변환하는 방법을 설명합니다.



참고 이 예에서는 내부 인터페이스가 BVI(브리지 그룹 인터페이스)가 아닌 표준 라우팅 인터페이스라고 가정합니다. 내부 인터페이스가 BVI인 경우에는 각 멤버 인터페이스에 대한 규칙을 중복 생성해야 합니다.

프로시저

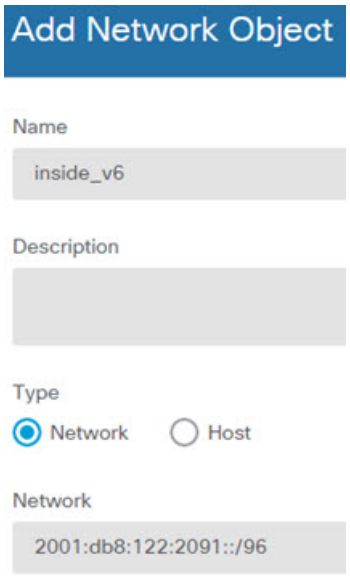
단계 **1** 내부 IPv6 및 외부 IPv6 NAT 네트워크를 정의하는 네트워크 개체를 생성합니다.

a) **Objects(**개체**)**를 선택합니다.

b) 목차에서 **Network(**네트워크**)**를 선택하고 +를 클릭합니다.

c) 내부 IPv6 네트워크를 정의합니다.

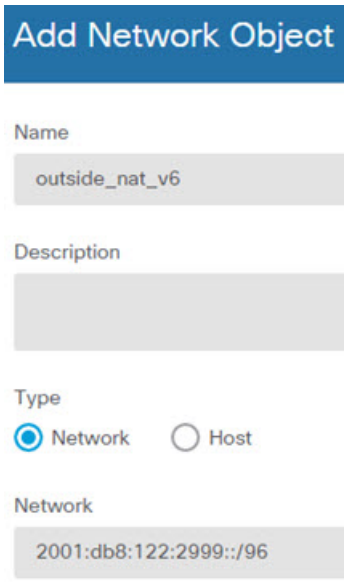
네트워크 개체의 이름을 inside_v6과 같이 지정하고 **Network(**네트워크**)**를 선택한 후에 네트워크 주소 2001:db8:122:2091::/96을 입력합니다.



d) **OK(**확인**)**를 클릭합니다.

e) +를 클릭하여 외부 IPv6 NAT 네트워크를 정의합니다.

네트워크 개체의 이름을 outside_nat_v6과 같이 지정하고 **Network(**네트워크**)**를 선택한 후에 네트워크 주소 2001:db8:122:2999::/96을 입력합니다.



단계 **2** 내부 IPv6 네트워크용 고정 NAT 규칙을 구성합니다.

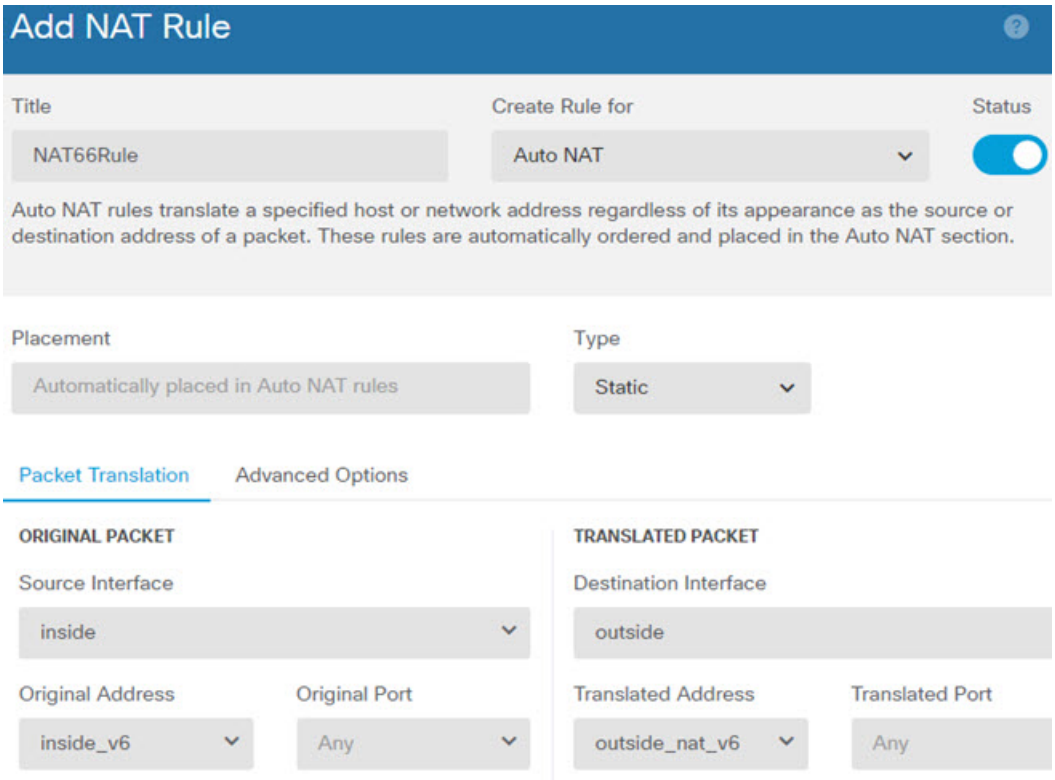
a) **Policies(**정책**)** > **NAT**를 선택합니다.

b) + 버튼을 클릭합니다.

c) 다음 속성을 구성합니다.

- **Title(**제목**)** = NAT66Rule 또는 원하는 다른 이름

- **Create Rule For(**규칙 생성**)** = 자동 NAT
- **Type(**유형**)** = 고정
- **Source Interface(**원본 인터페이스**)** = inside
- **Destination Interface(**대상 인터페이스**)** = outside
- **Original Address(**원본 주소**)** = inside_v6 네트워크 개체
- **Translated Address(**변환된 주소**)** = outside_nat_v6 네트워크 개체



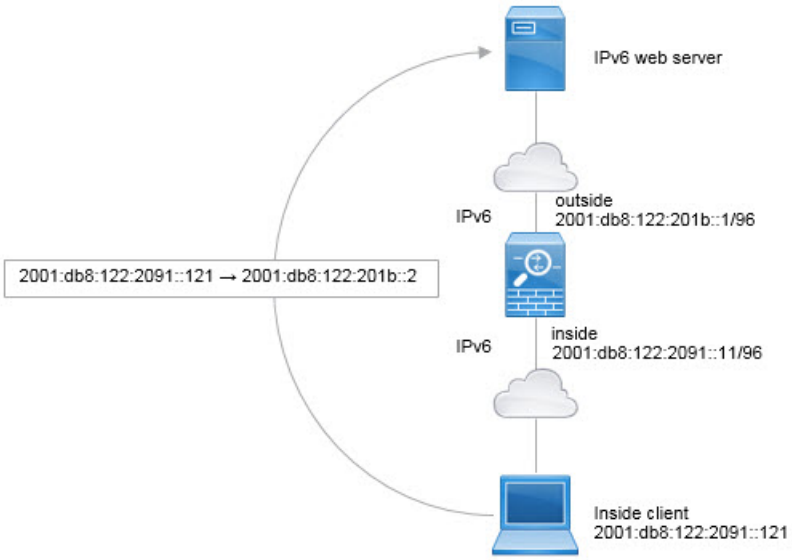
d) **OK(**확인**)**를 클릭합니다.

이 규칙을 사용하는 경우 내부 인터페이스의 2001:db8:122:2091::/96 서브넷에서 외부 인터페이스로 이동하는 모든 트래픽은 2001:db8:122:2999::/96 네트워크의 주소로 고정 NAT66 변환됩니다.

NAT66 예, 간단한 IPv6 인터페이스 PAT

NAT66을 구현하는 단순한 방식은 내부 주소를 외부 인터페이스 IPv6 주소의 각기 다른 포트에 동적으로 할당하는 것입니다.

그러나 device manager를 사용하는 인터페이스의 IPv6 주소를 사용하여 인터페이스 PAT를 구성할 수는 없습니다. 대신 동적 PAT 풀과 같은 네트워크에 있는 단일 사용 가능 주소를 사용합니다.



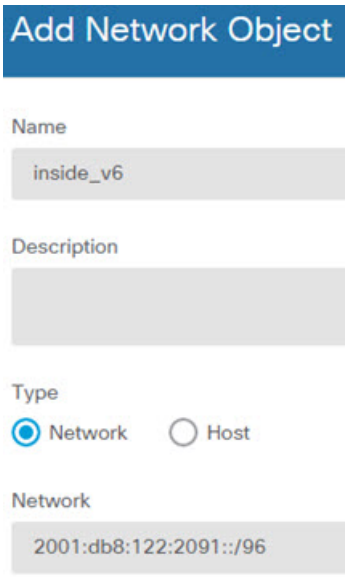
참고 이 예에서는 내부 인터페이스가 BVI(브리지 그룹 인터페이스)가 아닌 표준 라우팅 인터페이스라고 가정합니다. 내부 인터페이스가 BVI인 경우에는 각 멤버 인터페이스에 대한 규칙을 중복 생성해야 합니다.

프로시저

단계 **1** 내부 IPv6 네트워크 및 IPv6 PAT 주소를 정의하는 네트워크 개체를 생성합니다.

a) **Objects(**개체**)**를 선택합니다.
b) 목차에서 **Network(**네트워크**)**를 선택하고 +를 클릭합니다.
c) 내부 IPv6 네트워크를 정의합니다.

네트워크 개체의 이름을 inside_v6과 같이 지정하고 **Network(**네트워크**)**를 선택한 후에 네트워크 주소 2001:db8:122:2091::/96을 입력합니다.



d) **OK(**확인**)**를 클릭합니다.

e) +를 클릭하여 외부 IPv6 PAT 주소를 정의합니다.

네트워크 개체의 이름을 ipv6_pat와 같이 지정하고 **Host(**호스트**)**를 선택한 후에 호스트 주소 2001:db8:122:201b::2를 입력합니다.

단계 **2** 내부 IPv6 네트워크용 동적 PAT 규칙을 구성합니다.

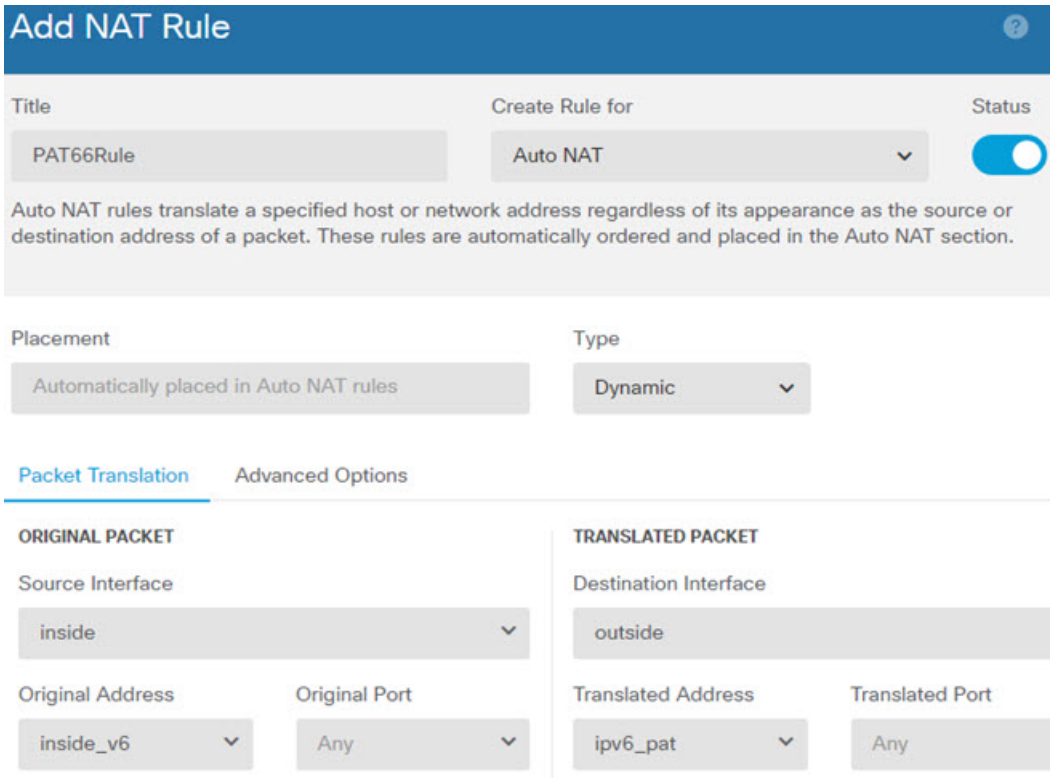
a) **Policies(**정책**)** > **NAT**를 선택합니다.

b) + 버튼을 클릭합니다.

c) 다음 속성을 구성합니다.

- 제목 = PAT66Rule 또는 원하는 다른 이름

- **Create Rule For(**규칙 생성**)** = 자동 NAT
- **Type(**유형**)** = 동적
- **Source Interface(**원본 인터페이스**)** = inside
- **Destination Interface(**대상 인터페이스**)** = outside
- **Original Address(**원본 주소**)** = inside_v6 네트워크 개체
- 변환된 주소 = ipv6_pat 네트워크 개체



d) **OK(**확인**)**를 클릭합니다.

이 규칙을 사용하는 경우 내부 인터페이스의 2001:db8:122:2091::/96 서브넷에서 외부 인터페이스로 이동하는 모든 트래픽은 2001:db8:122:201b::2의 포트로 동적 PAT66 변환됩니다.

NAT 모니터링

NAT 연결을 모니터링하고 트러블슈팅하려면 CLI 콘솔을 열거나 디바이스 CLI에 로그인하여 다음 명령을 사용합니다.

- **show nat** NAT 규칙 및 규칙별 적중 횟수를 표시합니다. NAT의 다른 측면을 표시하는 추가 키워드도 있습니다.
- **show xlate** 현재 활성 상태인 활성 NAT 변환을 표시합니다.
- **clear xlate** 활성 NAT 변환을 제거할 수 있습니다. NAT 규칙을 변경하는 경우에는 활성 변환을 제거해야 할 수 있습니다. 기존 연결은 종료될 때까지 이전 변환 슬롯을 계속 사용하기 때문입니다. 변환을 지우면 시스템에서 새 규칙을 기반으로 하여 클라이언트의 다음 연결 시도 시 클라이언트에 대한 새 변환을 작성할 수 있습니다. CLI 콘솔에서는 이 명령을 사용할 수 없습니다.

NAT의 예

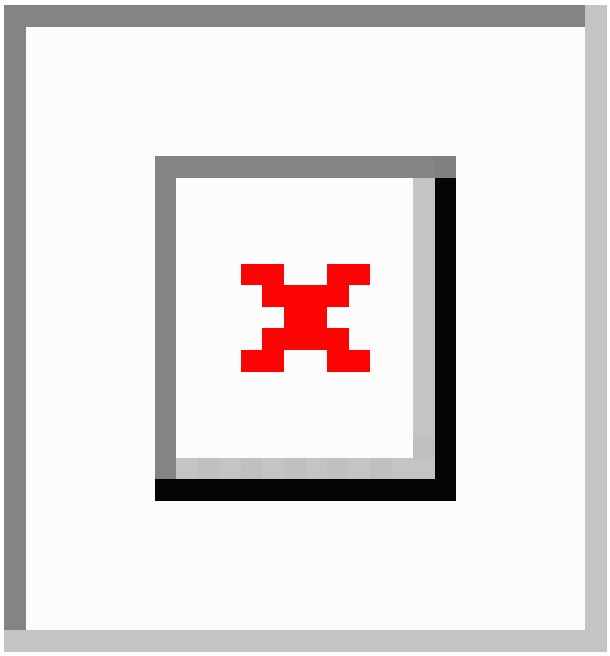
다음 항목에서는 Threat Defense 디바이스에서 NAT를 구성하는 예를 제공합니다.

내부 웹 서버에 대한 액세스 제공(고정 자동 NAT)

다음 예는 내부 웹 서버에 대해 고정 NAT를 수행합니다. 실제 주소는 사설 네트워크에 있으므로 공용 주소가 필요합니다. 호스트가 고정된 주소에서 웹 서버에 대한 트래픽을 시작할 수 있으려면 고정 NAT가 필요합니다.

참고 이 예에서는 내부 인터페이스가 BVI(브리지 그룹 인터페이스)가 아닌 표준 라우팅 인터페이스라고 가정합니다. 내부 인터페이스가 BVI인 경우 웹 서버가 연결된 특정 브리지 그룹 멤버 인터페이스(예: inside1_3)를 선택합니다.

그림 45: 내부 웹 서버에 대한 고정 NAT

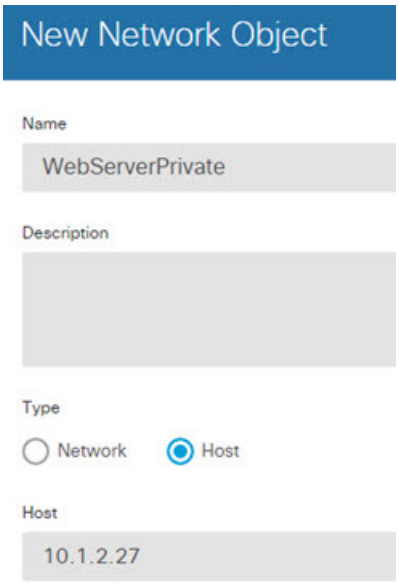


프로시저

단계 1 서버의 전용 및 공용 호스트 주소를 정의하는 네트워크 개체를 생성합니다.

a) **Objects(**개체**)**를 선택합니다.
b) 목차에서 **Network(**네트워크**)**를 선택하고 +를 클릭합니다.
c) 웹 서버의 전용 어드레스를 정의합니다.

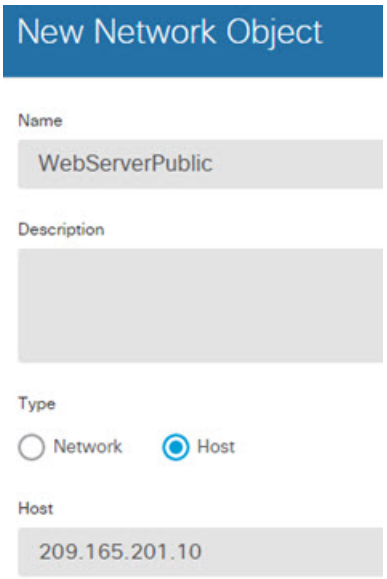
네트워크 개체의 이름을 WebServerPrivate과 같이 지정하고 **Host(**호스트**)**를 선택한 후에 실제 호스트 IP 주소 10.1.2.27을 입력합니다.



d) **OK(**확인**)**를 클릭합니다.

e) +를 클릭하여 공용 주소를 정의합니다.

네트워크 개체의 이름을 WebServerPublic과 같이 지정하고 **Host(**호스트**)**를 선택한 후에 호스트 주소 209.165.201.10을 입력합니다.



f) **OK(**확인**)**를 클릭합니다.

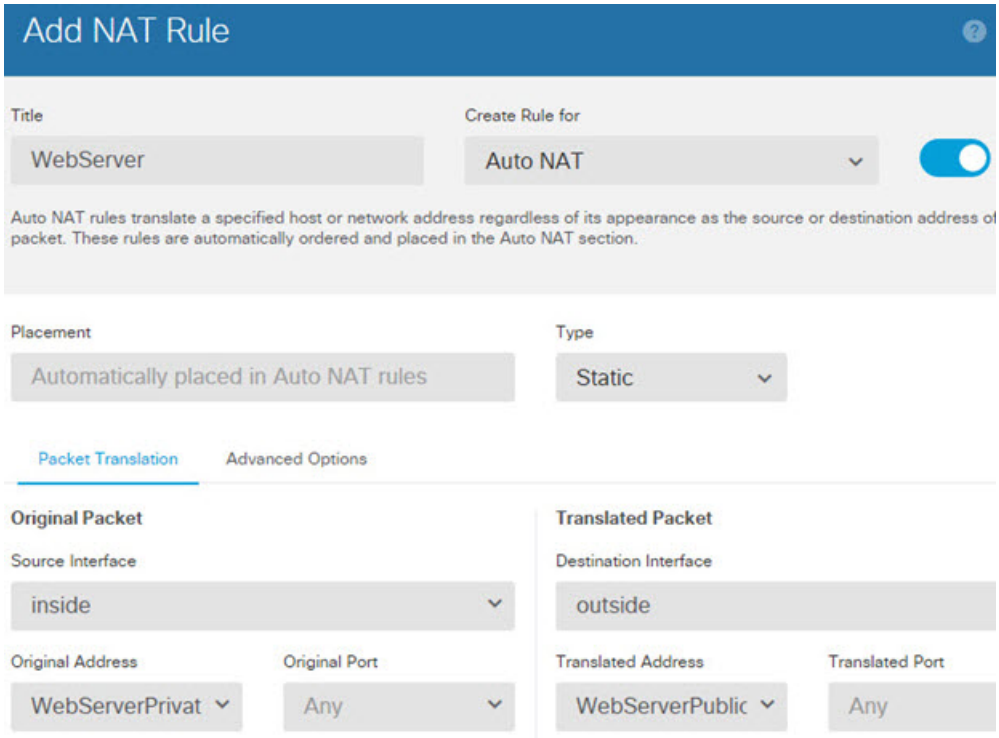
단계 **2** 개체용 고정 NAT를 구성합니다.

a) **Policies(**정책**)** > **NAT**를 선택합니다.

b) + 버튼을 클릭합니다.

c) 다음 속성을 구성합니다.

- **Title(**제목**)** = WebServer 또는 원하는 다른 이름
- **Create Rule For(**규칙 생성**)** = 자동 NAT
- **Type(**유형**)** = 고정
- **Source Interface(**원본 인터페이스**)** = inside
- **Destination Interface(**대상 인터페이스**)** = outside
- **Original Address(**원본 주소**)** = WebServerPrivate 네트워크 개체
- **Translated Address(**변환된 주소**)** = WebServerPublic 네트워크 개체



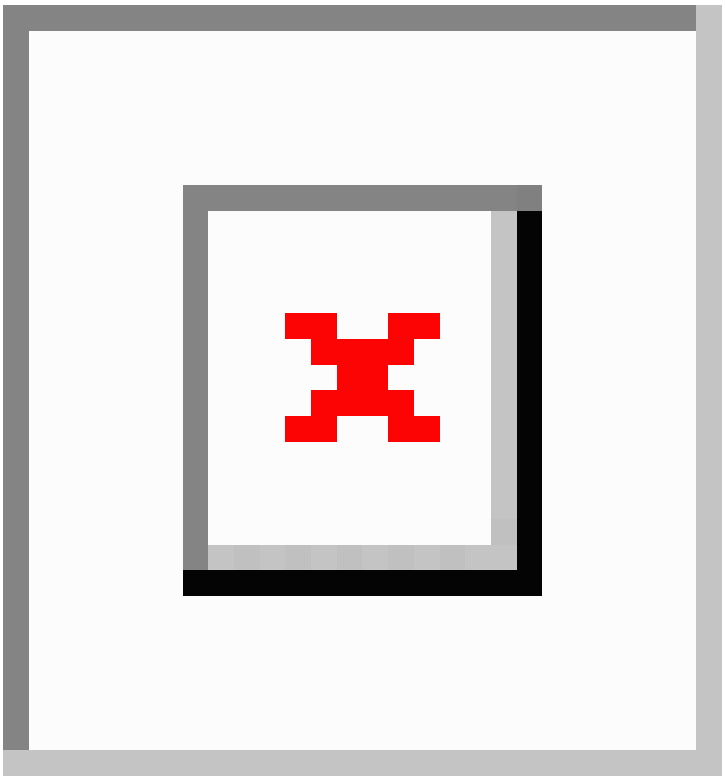
d) **OK(**확인**)**를 클릭합니다.

FTP, HTTP 및 SMTP용 단일 주소(포트 변환 고정 자동 NAT)

다음과 같은 포트 변환 고정 NAT의 예는 원격 사용자가 FTP, HTTP 및 SMTP에 액세스하기 위해 사용할 단일 주소를 제공합니다. 이러한 서버는 실제 네트워크에서 실제로 서로 다른 디바이스이지만, 각 서버에 대해 동일하게 매핑된 IP 주소를 사용하되 포트는 다른 포트 변환 고정 NAT 규칙을 지정할 수 있습니다.

참고 이 예에서는 내부 인터페이스가 스위치에 연결된 표준 라우팅 인터페이스이며 서버가 스위치에 연결되어 있다고 가정합니다. 내부 인터페이스가 BVI(브리지 그룹 인터페이스)이며 서버가 별도의 브리지 그룹 멤버 인터페이스에 연결되어 있으면 해당하는 규칙에 대해 각 서버가 연결된 특정 멤버 인터페이스를 선택합니다. 예를 들어 규칙이 소스 인터페이스에 대해 inside가 아닌 inside1_2, inside1_3 및 inside1_4를 포함할 수 있습니다.

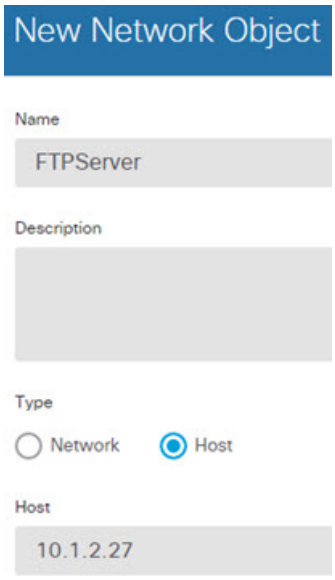
그림 *46:* 포트 변환 고정 *NAT*



프로시저

단계 **1** FTP 서버용 네트워크 개체를 만듭니다.

a) **Objects(**개체**)**를 선택합니다.
b) 목차에서 **Network(**네트워크**)**를 선택하고 +를 클릭합니다.
c) 네트워크 개체의 이름을 FTPserver와 같이 지정하고 **Host(**호스트**)**를 선택한 후에 FTP 서버의 실제 IP 주소 10.1.2.27을 입력합니다.

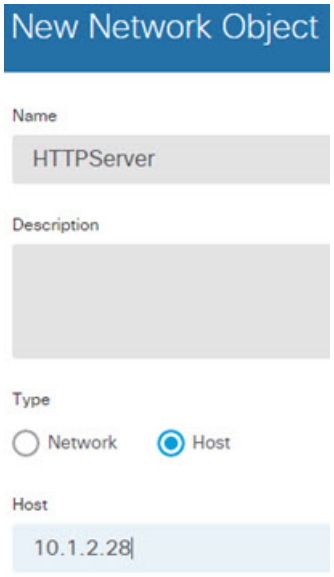


d) **OK(**확인**)**를 클릭합니다.

단계 **2** HTTP 서버용 네트워크 개체를 생성합니다.

a) +를 클릭합니다.

b) 네트워크 개체의 이름을 HTTPserver와 같이 지정하고 호스트를 선택한 후에 호스트 주소 10.1.2.28을 입력합니다.

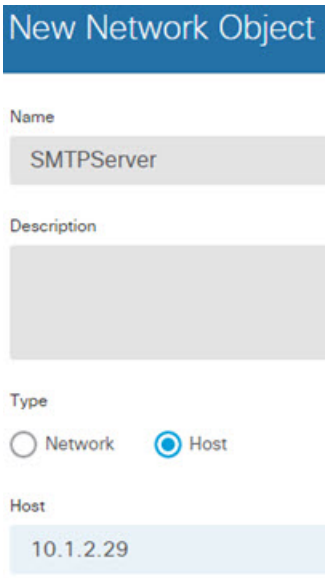


c) **OK(**확인**)**를 클릭합니다.

단계 **3** SMTP 서버용 네트워크 개체를 생성합니다.

a) +를 클릭합니다.

b) 네트워크 개체의 이름을 SMTPserver와 같이 지정하고 호스트를 선택한 후에 호스트 주소 10.1.2.29를 입력합니다.

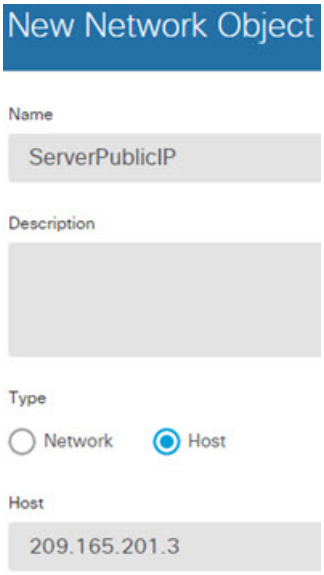


c) **OK(**확인**)**를 클릭합니다.

단계 **4** 서버 3대에 사용되는 공용 IP 주소용 네트워크 개체를 생성합니다.

a) +를 클릭합니다.

b) 네트워크 개체의 이름을 ServerPublicIP와 같이 지정하고 **Host(**호스트**)**를 선택한 후에 호스트 주소 209.165.201.3을 입력합니다.



c) **OK(**확인**)**를 클릭합니다.

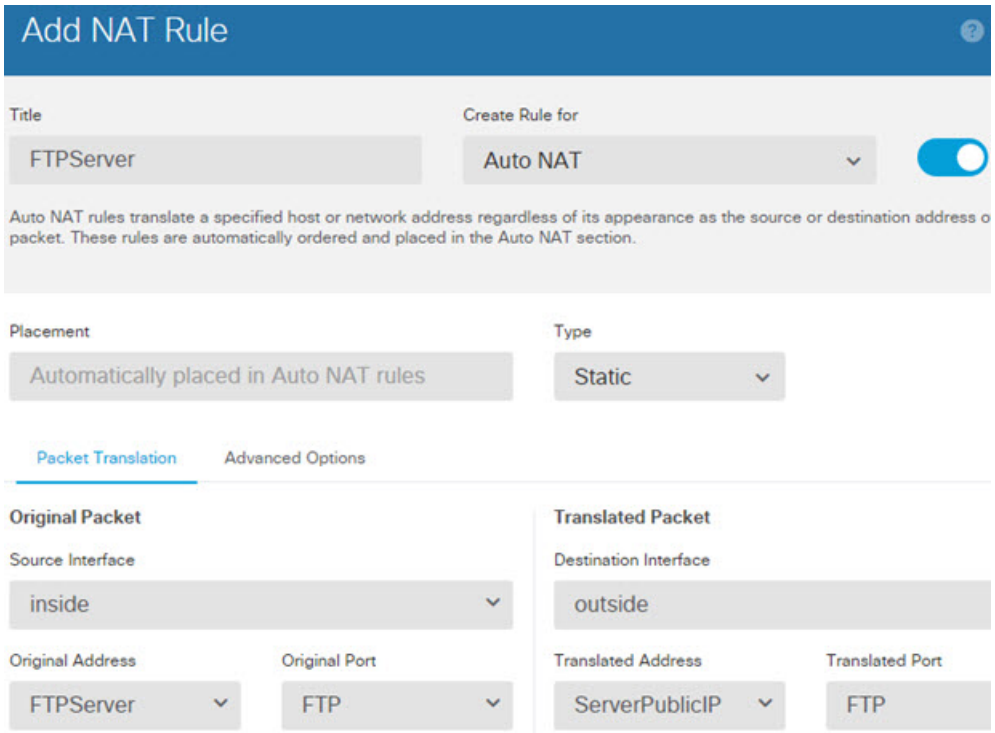
단계 **5** FTP 포트를 자기 자신에 매핑하는 FTP 서버용 포트 변환 고정 NAT를 구성합니다.

a) **Policies(**정책**)** > **NAT**를 선택합니다.

b) + 버튼을 클릭합니다.

c) 다음 속성을 구성합니다.

- **Title(**제목**)** = FTPServer 또는 원하는 다른 이름
- **Create Rule For(**규칙 생성**)** = 자동 NAT
- **Type(**유형**)** = 고정
- **Source Interface(**원본 인터페이스**)** = inside
- **Destination Interface(**대상 인터페이스**)** = outside
- **Original Address(**원본 주소**)** = FTPserver 네트워크 개체
- **Translated Address(**변환된 주소**)** = ServerPublicIP 네트워크 개체
- **Original Port(**원본 포트**)** = FTP 포트 개체
- **Translated Port(**변환된 포트**)** = FTP 포트 개체



d) **OK(**확인**)**를 클릭합니다.

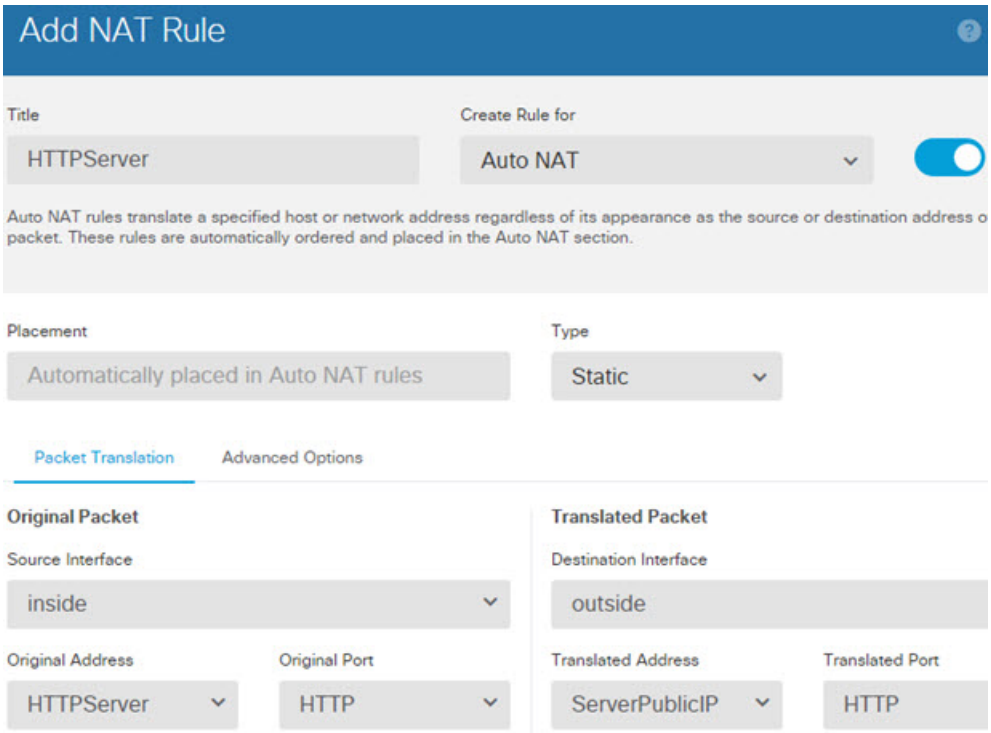
단계 **6** HTTP 포트를 자기 자신에 매핑하는 HTTP 서버용 포트 변환 고정 NAT를 구성합니다.

a) + 버튼을 클릭합니다.

b) 다음 속성을 구성합니다.

- **Title(**제목**)** = HTTPServer 또는 원하는 다른 이름
- **Create Rule For(**규칙 생성**)** = 자동 NAT
- **Type(**유형**)** = 고정

- **Source Interface(**원본 인터페이스**)** = inside
- **Destination Interface(**대상 인터페이스**)** = outside
- **Original Address(**원본 주소**)** = HTTPserver 네트워크 개체
- **Translated Address(**변환된 주소**)** = ServerPublicIP 네트워크 개체
- **Original Port(**원본 포트**)** = HTTP 포트 개체
- **Translated Port(**변환된 포트**)** = HTTP 포트 개체



c) **OK(**확인**)**를 클릭합니다.

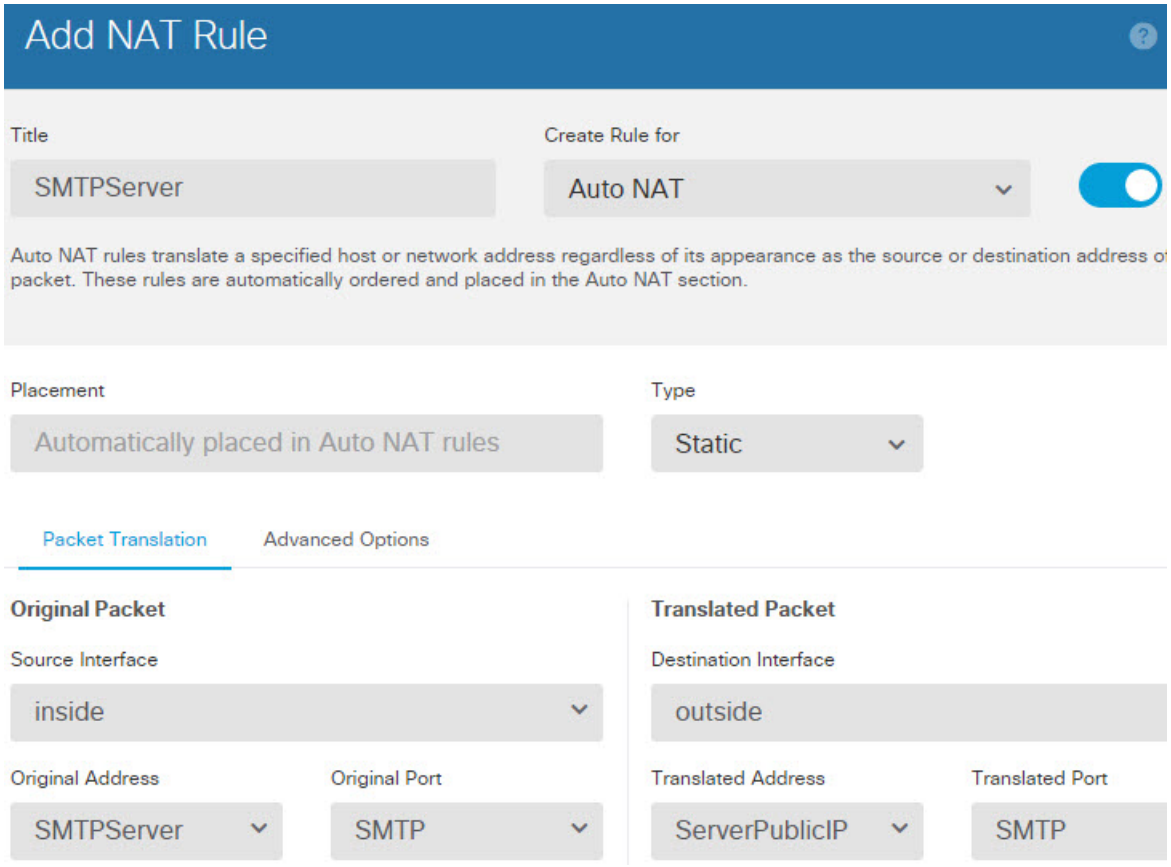
단계 **7** SMTP 포트를 자기 자신에 매핑하는 SMTP 서버용 포트 변환 고정 NAT를 구성합니다.

a) + 버튼을 클릭합니다.

b) 다음 속성을 구성합니다.

- **Title(**제목**)** = SMTPServer 또는 원하는 다른 이름
- **Create Rule For(**규칙 생성**)** = 자동 NAT
- **Type(**유형**)** = 고정
- **Source Interface(**원본 인터페이스**)** = inside
- **Destination Interface(**대상 인터페이스**)** = outside
- **Original Address(**원본 주소**)** = SMTPserver 네트워크 개체

- **Translated Address(**변환된 주소**)** = ServerPublicIP 네트워크 개체
- **Original Port(**원본 포트**)** = SMTP 포트 개체
- **Translated Port(**변환된 포트**)** = SMTP 포트 개체



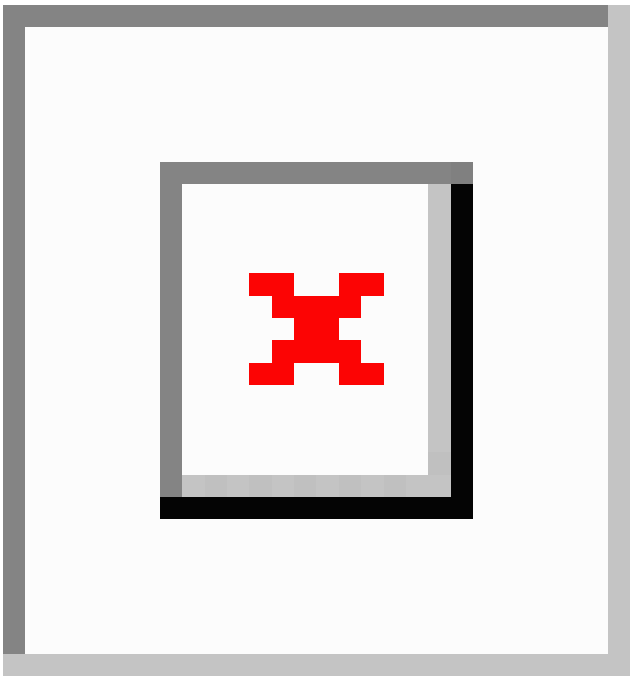
c) **OK(**확인**)**를 클릭합니다.

대상에 따라 다른 변환(동적 수동 **PAT)**

다음 그림은 두 개의 서로 다른 서버에 액세스하는 10.1.2.0/24 네트워크의 호스트를 보여줍니다. 호스트가 209.165.201.11의 서버에 액세스하면 실제 주소가 209.165.202.129:*port*로 변환됩니다. 호스트가 209.165.200.225의 서버에 액세스하면 실제 주소가 209.165.202.130:*port*로 변환됩니다.

참고 이 예에서는 내부 인터페이스가 스위치에 연결된 표준 라우팅 인터페이스이며 서버가 스위치에 연결되어 있다고 가정합니다. 내부 인터페이스가 BVI(브리지 그룹 인터페이스)이며 서버가 별도의 브리지 그룹 멤버 인터페이스에 연결되어 있으면 해당하는 규칙에 대해 각 서버가 연결된 특정 멤버 인터페이스를 선택합니다. 예를 들어 규칙이 소스 인터페이스에 대해 inside가 아닌 inside1_2 및 inside1_3을 포함할 수 있습니다.

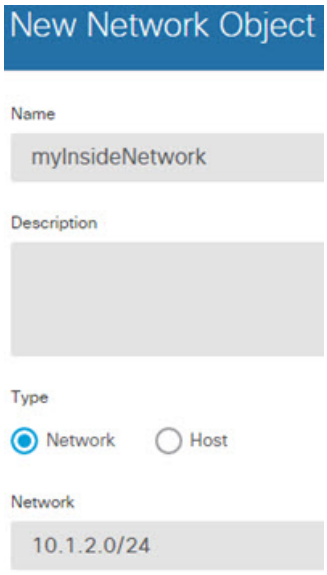
그림 ***47:*** 서로 다른 대상 주소를 사용하는 수동 ***NAT***



프로시저

단계 **1** 내부 네트워크용 네트워크 개체를 만듭니다.

a) **Objects(**개체**)**를 선택합니다.
b) 목차에서 **Network(**네트워크**)**를 선택하고 +를 클릭합니다.
c) 네트워크 개체의 이름을 myInsideNetwork와 같이 지정하고 **Network(**네트워크**)**를 선택한 후에 실제 네트워크 주소 10.1.2.0/24를 입력합니다.

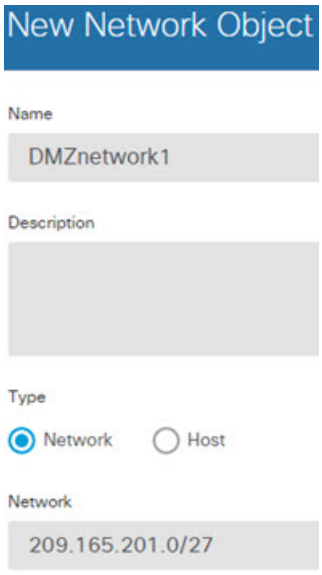


d) **OK(**확인**)**를 클릭합니다.

단계 **2** DMZ 네트워크 1용 네트워크 개체를 생성합니다.

a) +를 클릭합니다.

b) 네트워크 개체의 이름을 DMZnetwork1과 같이 지정하고 **Network(**네트워크**)**를 선택한 후에 네트워크 주소 209.165.201.0/27(서브넷 마스크 255.255.255.224)을 입력합니다.

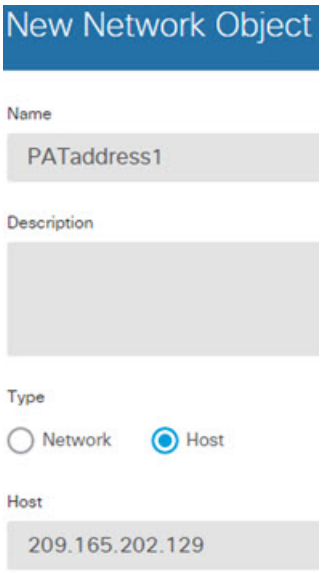


c) **OK(**확인**)**를 클릭합니다.

단계 **3** DMZ 네트워크 1용 PAT 주소의 네트워크 개체를 생성합니다.

a) +를 클릭합니다.

b) 네트워크 개체의 이름을 PATaddress1과 같이 지정하고 **Host(**호스트**)**를 선택한 후에 호스트 주소 209.165.202.129를 입력합니다.

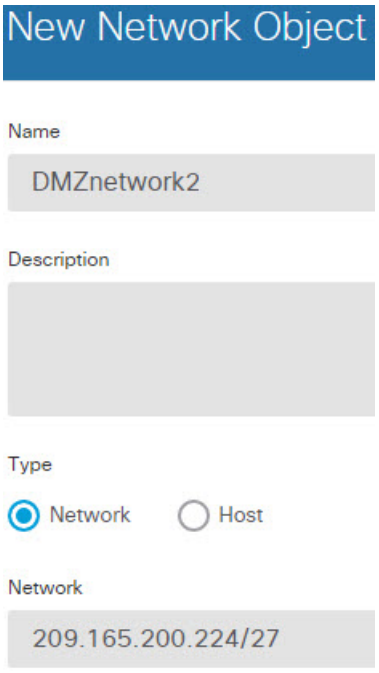


c) **OK(**확인**)**를 클릭합니다.

단계 **4** DMZ 네트워크 2용 네트워크 개체를 생성합니다.

a) +를 클릭합니다.

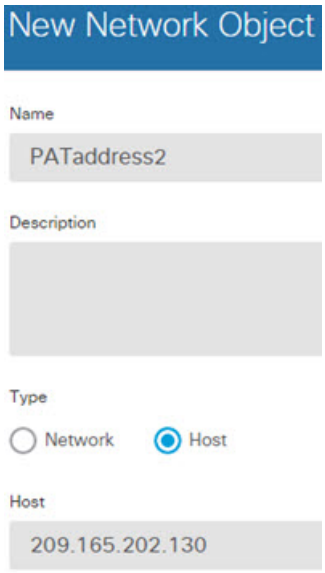
b) 네트워크 개체의 이름을 DMZnetwork2와 같이 지정하고 **Network(**네트워크**)**를 선택한 후에 네트워크 주소 209.165.200.224/27(서브넷 마스크 255.255.255.224)을 입력합니다.



c) **OK(**확인**)**를 클릭합니다.

단계 **5** DMZ 네트워크 2용 PAT 주소의 네트워크 개체를 생성합니다.

a) +를 클릭합니다.
b) 네트워크 개체의 이름을 PATaddress2와 같이 지정하고 **Host(**호스트**)**를 선택한 후에 호스트 주소 209.165.202.130을 입력합니다.



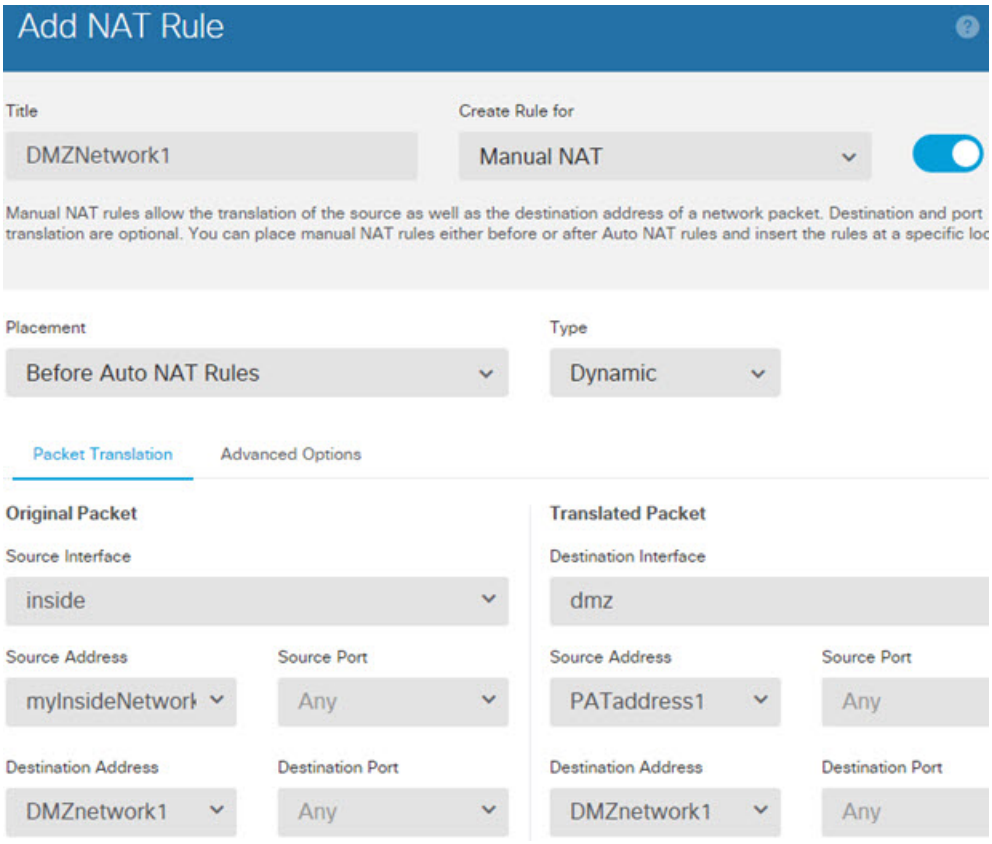
c) **OK(**확인**)**를 클릭합니다.

단계 **6** DMZ 네트워크 1용 동적 수동 PAT를 구성합니다.

a) **Policies(**정책**)** > **NAT**를 선택합니다.
b) + 버튼을 클릭합니다.
c) 다음 속성을 구성합니다.

- **Title(**제목**)** = DMZNetwork1 또는 원하는 다른 이름
- **Create Rule For(**규칙 생성**)** = 수동 NAT
- **Type(**유형**)** = 동적
- **Source Interface(**원본 인터페이스**)** = inside
- **Destination Interface(**대상 인터페이스**)** = dmz
- **Original Source Address(**원본 소스 주소**)** = myInsideNetwork 네트워크 개체
- **Translated Source Address(**변환된 소스 주소**)** = PATaddress1 네트워크 개체
- **Original Destination Address(**원본 대상 주소**)** = DMZnetwork1 네트워크 개체
- **Translated Destination Address(**변환된 대상 주소**)** = DMZnetwork1 네트워크 개체

참고 대상 주소를 변환하지 않을 것이기 때문에 원본 주소 및 변환된 대상 주소에 대해 동일한 주소를 지정하여 대상 주소에 대한 ID NAT를 구성해야 합니다. 포트 필드는 모두 비워 둡니다.



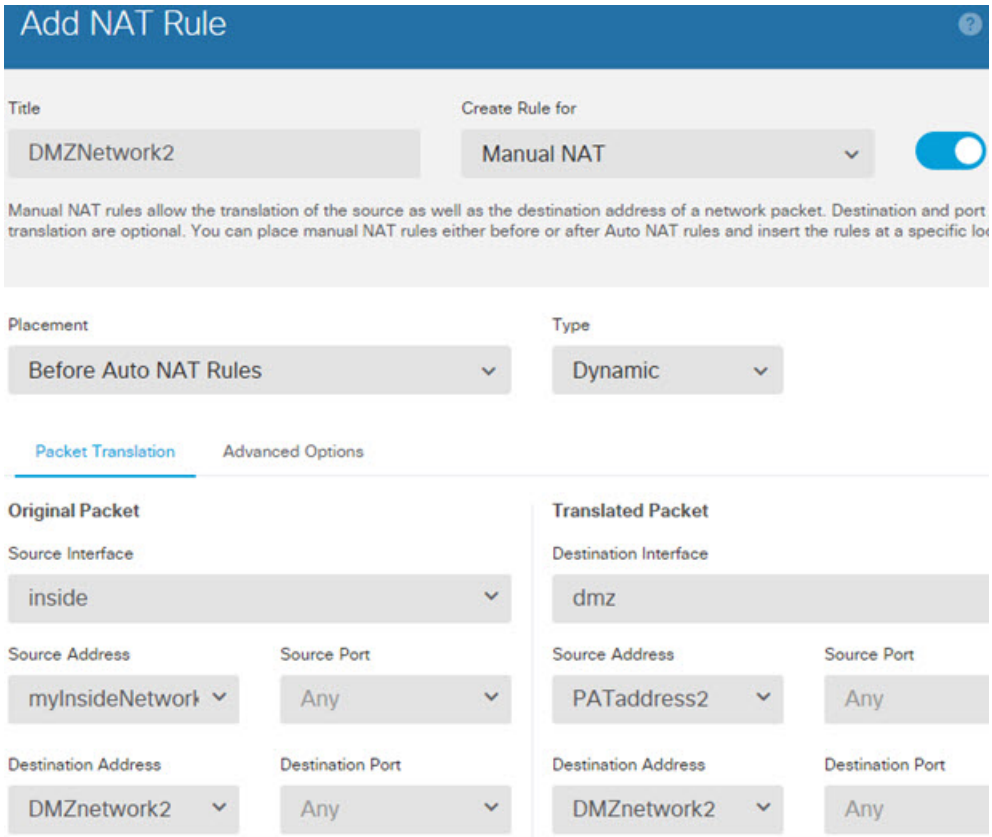
d) **OK**(확인)를 클릭합니다.

단계 **7** DMZ 네트워크 2용 동적 수동 PAT를 구성합니다.

a) + 버튼을 클릭합니다.

b) 다음 속성을 구성합니다.

- **Title**(제목) = DMZNetwork2 또는 원하는 다른 이름
- **Create Rule For**(규칙 생성) = 수동 NAT
- **Type**(유형) = 동적
- **Source Interface**(원본 인터페이스) = inside
- **Destination Interface**(대상 인터페이스) = dmz
- **Original Source Address**(원본 소스 주소) = myInsideNetwork 네트워크 개체
- **Translated Source Address**(변환된 소스 주소) = PATaddress2 네트워크 개체
- **Original Destination Address**(원본 대상 주소) = DMZnetwork2 네트워크 개체
- **Translated Destination Address**(변환된 대상 주소) = DMZnetwork2 네트워크 개체



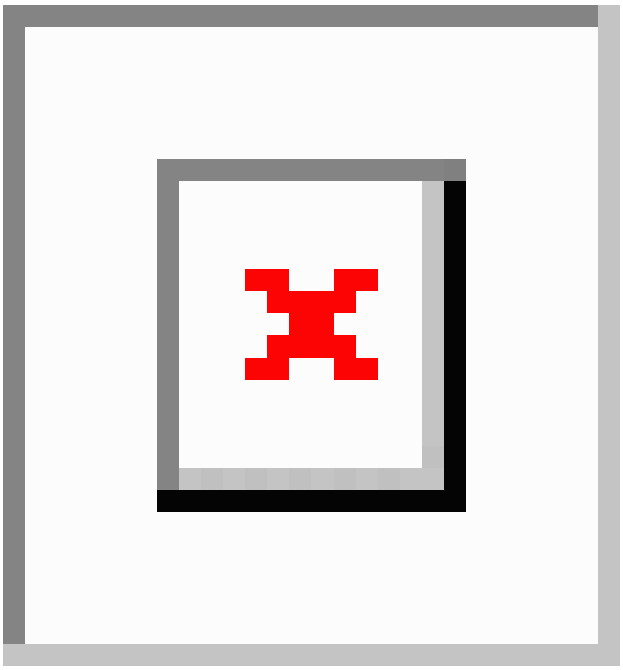
c) **OK(**확인**)**를 클릭합니다.

대상 주소 및 포트에 따라 다른 변환(동적 수동 **PAT)**

다음 그림은 소스 포트와 대상 포트의 사용법을 보여줍니다. 10.1.2.0/24 네트워크의 호스트가 웹 서비스와 텔넷 서비스를 모두 제공하는 단일 호스트에 액세스합니다. 호스트가 텔넷 서비스용 서버에 액세스하면 실제 주소가 209.165.202.129:*port*로 변환됩니다. 호스트가 동일한 웹 서비스용 서버에 액세스하면 실제 주소가 209.165.202.130:*port*로 변환됩니다.

참고 이 예에서는 내부 인터페이스가 스위치에 연결된 표준 라우팅 인터페이스이며 서버가 스위치에 연결되어 있다고 가정합니다. 내부 인터페이스가 BVI(브리지 그룹 인터페이스)이며 서버가 브리지 그룹 멤버 인터페이스에 연결되어 있으면 서버가 연결된 특정 멤버 인터페이스를 선택합니다. 예를 들어 규칙이 소스 인터페이스에 대해 inside가 아닌 inside1_2를 포함할 수 있습니다.

그림 ***48:*** 서로 다른 대상 포트를 사용하는 수동 ***NAT***



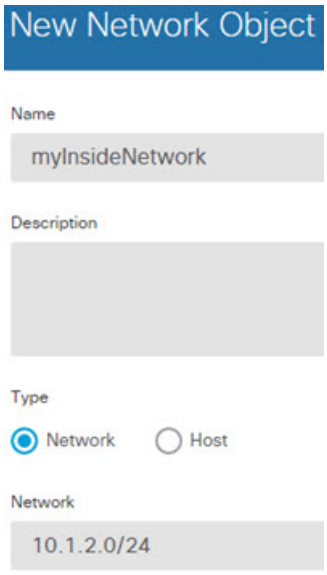
프로시저

단계 **1** 내부 네트워크용 네트워크 개체를 만듭니다.

a) **Objects(**개체**)**를 선택합니다.

b) 목차에서 **Network(**네트워크**)**를 선택하고 **+**를 클릭합니다.

c) 네트워크 개체의 이름을 myInsideNetwork와 같이 지정하고 **Network(**네트워크**)**를 선택한 후에 실제 네트워크 주소 10.1.2.0/24를 입력합니다.

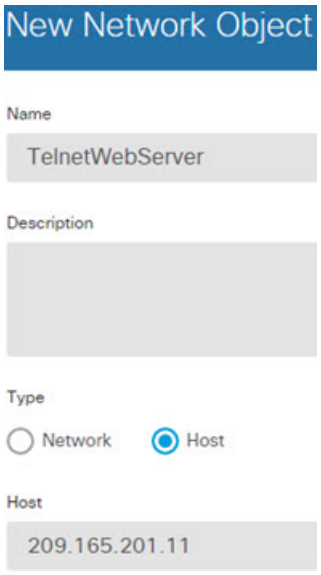


d) **OK(**확인**)**를 클릭합니다.

단계 **2** 텔넷/웹 서버용 네트워크 개체를 생성합니다.

a) +를 클릭합니다.

b) 네트워크 개체의 이름을 TelnetWebServer와 같이 지정하고 **Host(**호스트**)**를 선택한 후에 호스트 주소 209.165.201.11을 입력합니다.

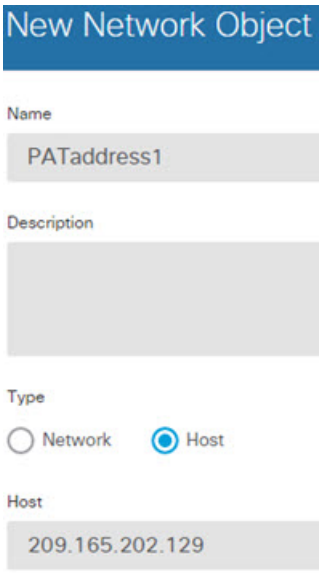


c) **OK(**확인**)**를 클릭합니다.

단계 **3** 텔넷 사용 시의 PAT 주소용 네트워크 개체를 생성합니다.

a) +를 클릭합니다.

b) 네트워크 개체의 이름을 PATaddress1과 같이 지정하고 **Host(**호스트**)**를 선택한 후에 호스트 주소 209.165.202.129를 입력합니다.

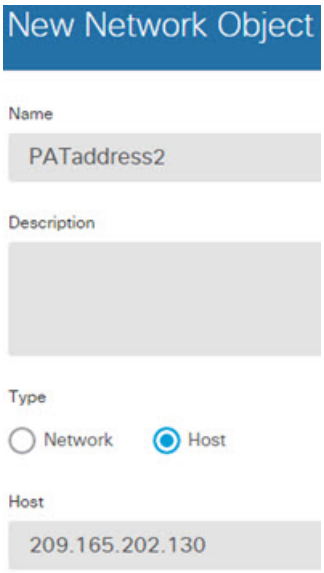


c) **OK(**확인**)**를 클릭합니다.

단계 **4** HTTP 사용 시의 PAT 주소용 네트워크 개체를 생성합니다.

a) **+**를 클릭합니다.

b) 네트워크 개체의 이름을 PATaddress2와 같이 지정하고 **Host(**호스트**)**를 선택한 후에 호스트 주소 209.165.202.130을 입력합니다.



c) **OK(**확인**)**를 클릭합니다.

단계 **5** 텔넷 액세스용 동적 수동 PAT를 구성합니다.

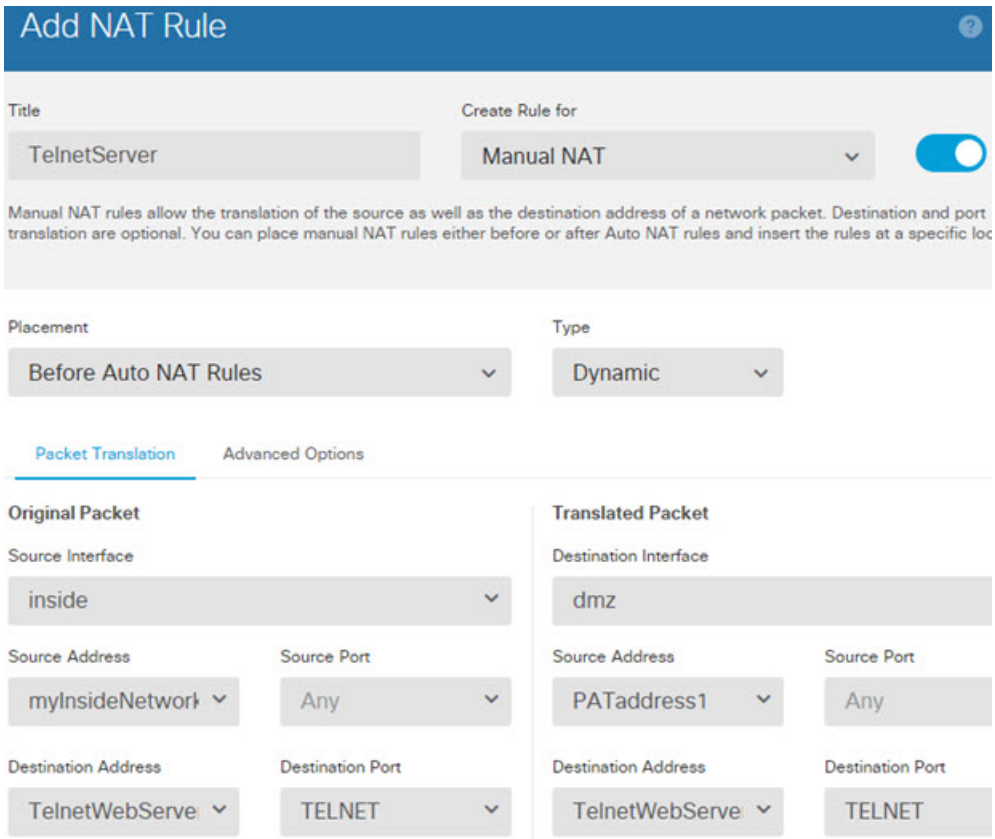
a) **Policies(**정책**)** > **NAT**를 선택합니다.

b) **+** 버튼을 클릭합니다.

c) 다음 속성을 구성합니다.

- **Title(**제목**)** = TelnetServer 또는 원하는 다른 이름
- **Create Rule For(**규칙 생성**)** = 수동 NAT
- **Type(**유형**)** = 동적
- **Source Interface(**원본 인터페이스**)** = inside
- **Destination Interface(**대상 인터페이스**)** = dmz
- **Original Source Address(**원본 소스 주소**)** = myInsideNetwork 네트워크 개체
- **Translated Source Address(**변환된 소스 주소**)** = PATaddress1 네트워크 개체
- **Original Destination Address(**원본 대상 주소**)** = TelnetWebServer 네트워크 개체
- **Translated Destination Address(**변환된 대상 주소**)** = TelnetWebServer 네트워크 개체
- **Original Destination Port(**원본 대상 포트**)** = TELNET 포트 개체
- **Translated Destination Port(**변환된 대상 포트**)** = TELNET 포트 개체

참고 대상 주소 또는 포트를 변환하지 않을 것이기 때문에 원본 및 변환된 대상 주소에 대해 동일한 주소를 지정하고 원본 및 변환된 포트에 대해 동일한 포트를 지정하여, 대상 주소 또는 포트에 대한 ID NAT를 구성해야 합니다.



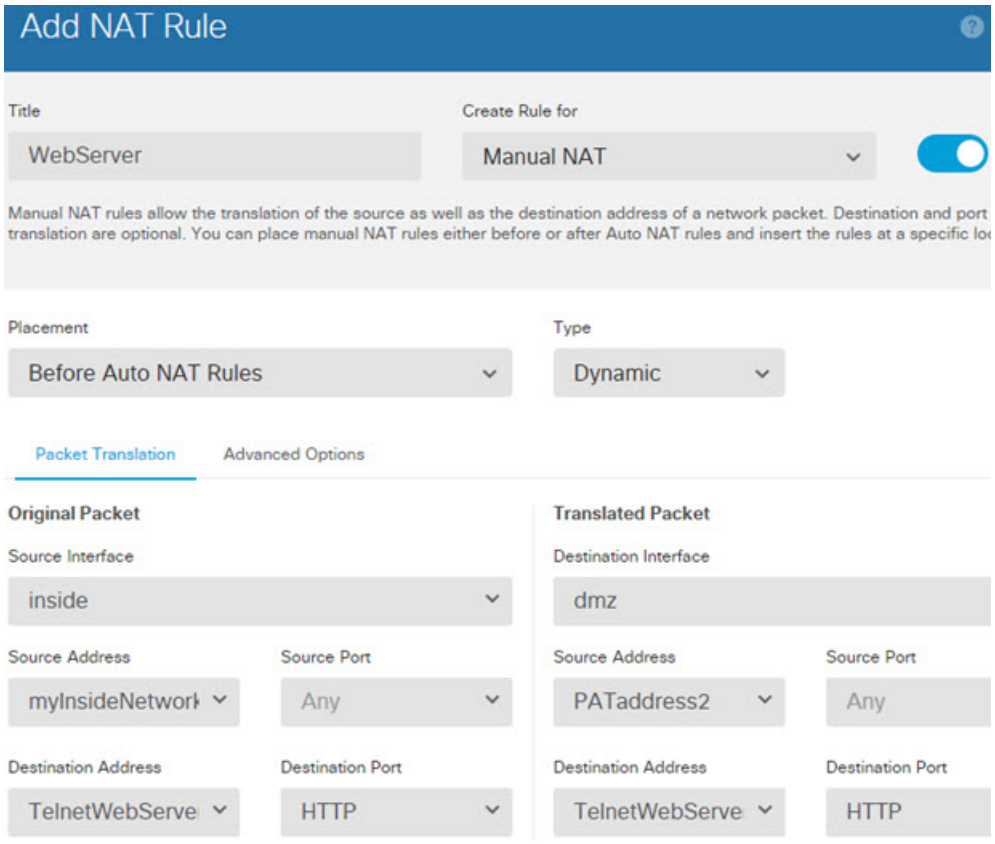
d) **OK(**확인**)**를 클릭합니다.

단계 **6** 웹 액세스용 동적 수동 PAT를 구성합니다.

a) **+** 버튼을 클릭합니다.

b) 다음 속성을 구성합니다.

- **Title(**제목**)** = WebServer 또는 원하는 다른 이름
- **Create Rule For(**규칙 생성**)** = 수동 NAT
- **Type(**유형**)** = 동적
- **Source Interface(**원본 인터페이스**)** = inside
- **Destination Interface(**대상 인터페이스**)** = dmz
- **Original Source Address(**원본 소스 주소**)** = myInsideNetwork 네트워크 개체
- **Translated Source Address(**변환된 소스 주소**)** = PATaddress2 네트워크 개체
- **Original Destination Address(**원본 대상 주소**)** = TelnetWebServer 네트워크 개체
- **Translated Destination Address(**변환된 대상 주소**)** = TelnetWebServer 네트워크 개체
- **Original Destination Port(**원본 대상 포트**)** = HTTP 포트 개체
- **Translated Destination Port(**변환된 대상 포트**)** = HTTP 포트 개체



c) **OK(**확인)를 클릭합니다.

NAT를 사용하여 DNS 쿼리 및 응답 재작성

회신의 주소를 NAT 구성과 일치하는 주소로 교체하여 DNS 회신을 수정하도록 위협 방지 디바이스를 구성해야 할 수 있습니다. 각 변환 규칙을 구성할 때 DNS 수정을 구성할 수 있습니다. DNS 수정은 DNS Doctoring이라고도 합니다.

이 기능은 NAT 규칙과 일치하는 DNS 쿼리 및 회신의 주소를 재작성합니다(예: IPv4의 A 레코드, IPv6의 AAAA 레코드 또는 역방향 DNS 쿼리의 PTR 레코드). 매핑된 인터페이스에서 다른 임의의 인터페이스로 이동하는 DNS 회신의 경우 매핑된 값에서 실제 값으로 레코드가 재작성됩니다. 반대로, 임의의 인터페이스에서 매핑된 인터페이스로 이동하는 DNS 회신의 경우 실제 값에서 매핑된 값으로 레코드가 재작성됩니다. 이 기능은 NAT44, NAT 66, NAT46 및 NAT64에서 작동합니다.

다음은 NAT 규칙에 DNS 재작성을 구성해야 하는 몇 가지 주요 상황입니다.

- 규칙이 NAT64 또는 NAT46이며 DNS 서버가 외부 네트워크에 있는 경우. DNS A 레코드(IPv4의 경우)를 AAAA 레코드(IPv6의 경우)로 변환하려면 DNS 재작성이 필요합니다.
- DNS 서버가 외부에 있고 클라이언트는 내부에 있으며 클라이언트가 사용하는 일부 FQDN(Fully Qualified Domain Name)이 다른 내부 호스트로 확인되는 경우.

- DNS 서버가 내부에 있고 프라이빗 IP 어드레스로 응답하며, 클라이언트는 외부에 있고 내부에서 호스팅되는 서버를 가리키는 FQDN(Fully Qualified Domain Name)에 액세스하는 경우.

DNS 재작성 제한

다음은 DNS 재작성의 몇 가지 제한 사항입니다.

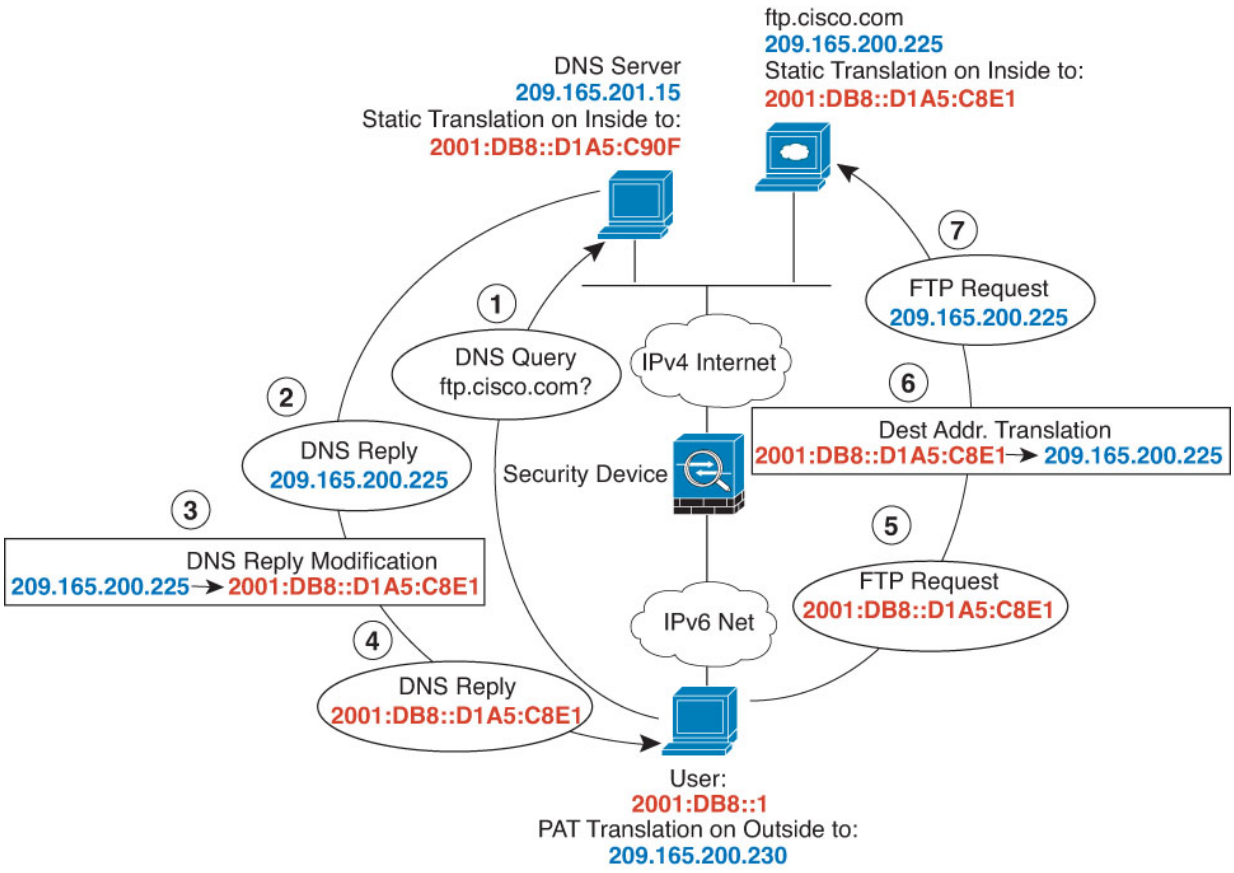
- 각 A 또는 AAAA 레코드에 여러 PAT 규칙을 적용할 수 있으며 사용할 PAT 규칙이 모호하므로 PAT에는 DNS 재작성이 적용되지 않습니다.
- 수동 NAT 규칙을 구성할 때 소스 주소와 대상 주소를 모두 지정하는 경우에는 DNS 수정을 구성할 수 없습니다. A와 B를 비교하여 전송하는 경우 이러한 종류의 규칙에는 잠재적으로 단일 주소에 다른 변환이 있을 수 있습니다. 따라서 이는 DNS 회신 내부의 IP 주소를 정확한 2회 NAT 규칙에 대해 올바르게 확인할 수 없습니다. DNS 회신에는 DNS 요청을 표시한 패킷에 어떤 source/destination 주소 조합이 있었는지에 대한 정보가 포함되어 있지 않습니다.
- DNS 재작성은 실제로 NAT 규칙이 아니라 xlate 항목에서 수행됩니다. 따라서 동적 규칙에 대한 xlate가 없으면 재작성을 정확히 수행할 수 없습니다. 고정 NAT에 대해서는 동일한 문제가 발생하지 않습니다.
- DNS 재작성에서는 DNS 동적 업데이트 메시지(opcode 5)를 재작성하지 않습니다.

다음 항목에서는 NAT 규칙의 DNS 재작성 예를 제공합니다.

DNS 64 회신 수정

다음 그림은 외부 IPv4 네트워크의 FTP 서버 및 DNS 서버를 보여줍니다. 시스템은 외부 서버에 대해 고정 변환을 수행합니다. 이 경우 내부 IPv6 사용자가 DNS 서버에서 ftp.cisco.com에 대한 주소를 요청하면 DNS 서버는 실제 주소인 209.165.200.225로 응답합니다.

내부 사용자가 ftp.cisco.com(2001:DB8::D1A5:C8E1, 여기서 D1A5:C8E1은 209.165.200.225에 해당하는 IPv6 주소)에 대한 매핑된 주소를 사용하도록 하려면 고정 변환에 대해 DNS 회신 수정을 구성해야 합니다. 이 예에는 DNS 서버용 고정 NAT 변환 및 내부 IPv6 호스트용 PAT 규칙도 포함되어 있습니다.



참고 이 예에서는 내부 인터페이스가 BVI(브리지 그룹 인터페이스)가 아닌 표준 라우팅 인터페이스라고 가정합니다. 내부 인터페이스가 BVI인 경우에는 각 멤버 인터페이스에 대한 규칙을 중복 생성해야 합니다.

프로시저

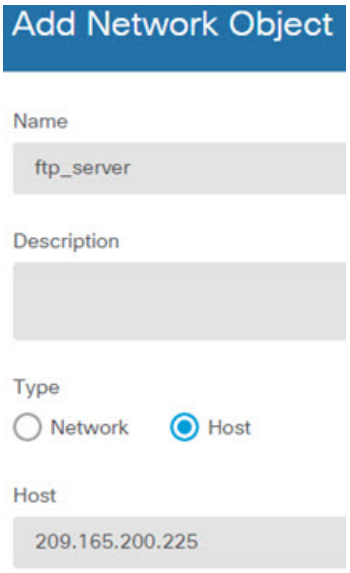
단계 **1** FTP 서버, DNS 서버, 내부 네트워크 및 PAT 풀용 네트워크 개체를 생성합니다.

a) **Objects(**개체**)**를 선택합니다.

b) 목차에서 **Network(**네트워크**)**를 선택하고 +를 클릭합니다.

c) 실제 FTP 서버 주소를 정의합니다.

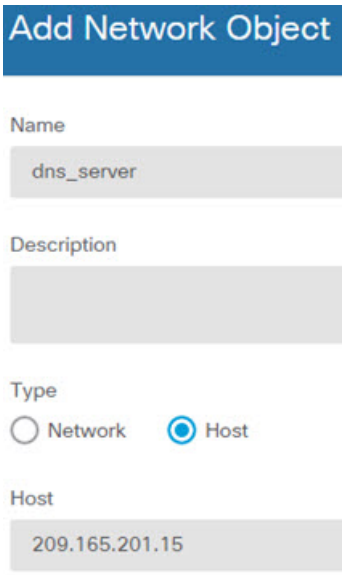
네트워크 개체의 이름을 ftp_server와 같이 지정하고 **Host(**호스트**)**를 선택한 후에 실제 호스트 IP 주소 209.165.200.225를 입력합니다.



d) **OK(**확인**)**를 클릭합니다.

e) +를 클릭하여 DNS 서버의 실제 주소를 정의합니다.

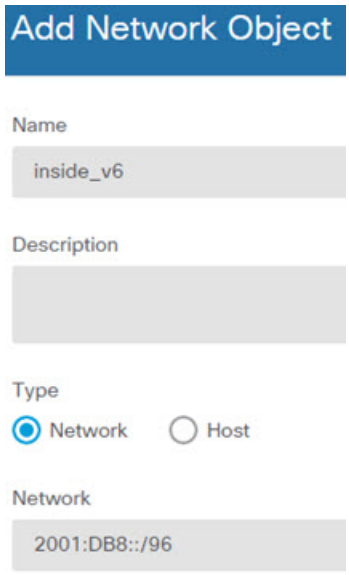
네트워크 개체의 이름을 dns_server와 같이 지정하고 **Host(**호스트**)**를 선택한 후에 호스트 주소 209.165.201.15를 입력합니다.



f) **OK(**확인**)**를 클릭합니다.

g) +를 클릭하여 내부 IPv6 네트워크를 정의합니다.

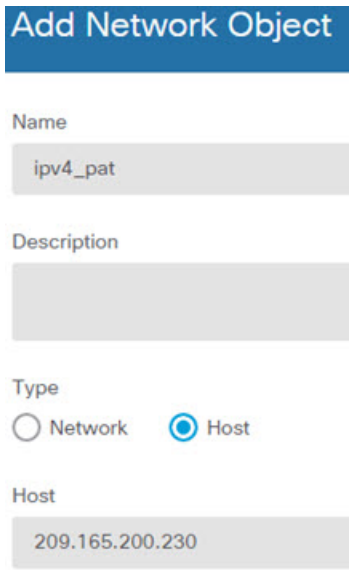
네트워크 개체의 이름을 inside_v6과 같이 지정하고 **Network(**네트워크**)**를 선택한 후에 네트워크 주소 2001:DB8::/96을 입력합니다.



h) **OK(**확인**)**를 클릭합니다.

i) +를 클릭하여 내부 IPv6 네트워크용 IPv4 PAT 주소를 정의합니다.

네트워크 개체의 이름을 ipv4_pat와 같이 지정하고 **Host(**호스트**)**를 선택한 후에 호스트 주소 209.165.200.230을 입력합니다.



j) **OK(**확인**)**를 클릭합니다.

단계 **2** FTP 서버에 대해 DNS를 수정하여 고정 NAT 규칙을 구성합니다.

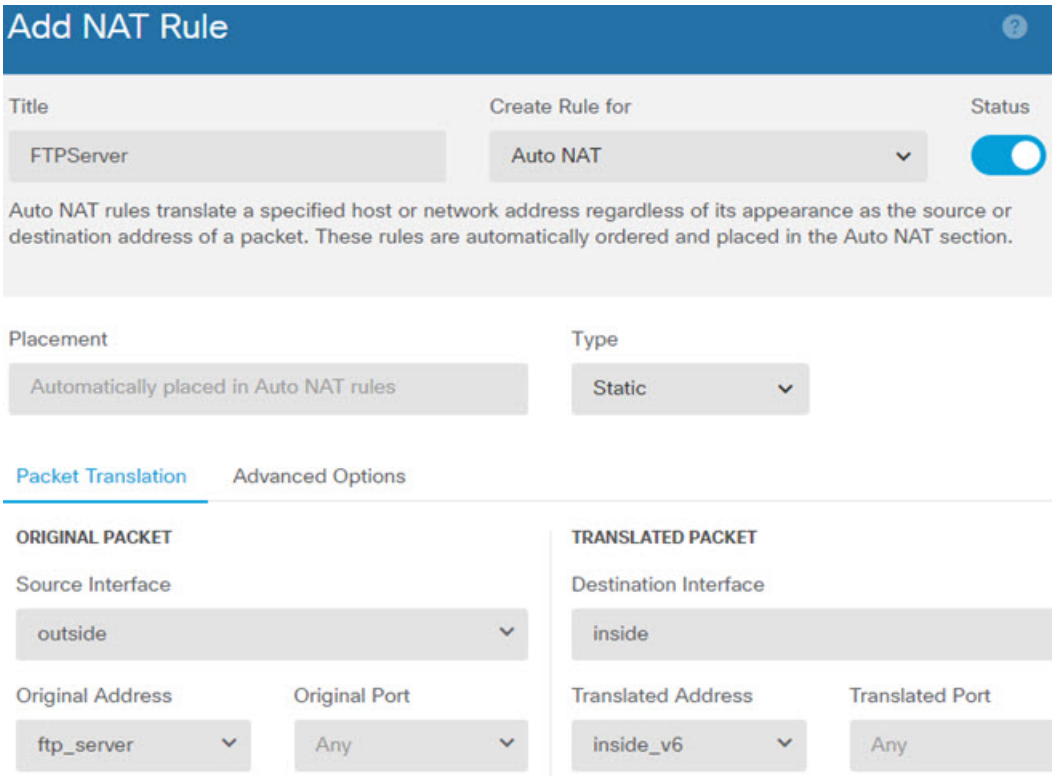
a) **Policies(**정책**)** > **NAT**를 선택합니다.

b) + 버튼을 클릭합니다.

c) 다음 속성을 구성합니다.

- **Title(**제목**)** = FTPServer 또는 원하는 다른 이름

- **Create Rule For(**규칙 생성**)** = 자동 NAT
- **Type(**유형**)** = 고정
- **Source Interface(**원본 인터페이스**)** = outside
- **Destination Interface(**대상 인터페이스**)** = inside
- **Original Address(**원본 주소**)** = ftp_server 네트워크 개체
- **Translated Address(**변환된 주소**)** = inside_v6 네트워크 개체 IPv4 주소를 IPv6 주소로 변환할 때는 IPv4 임베디드 주소 방법이 사용되므로 209.165.200.225는 동일한 IPv6 주소인 D1A5:C8E1로 변환되며, 네트워크 접두사가 추가되어 전체 주소는 2001:DB8::D1A5:C8E1이 됩니다.
- **Advanced Options(**고급 옵션**)** 탭에서 **Translate DNS replies that match this rule(**이 규칙과 일치하는 **DNS** 응답 변환**)**을 선택합니다.



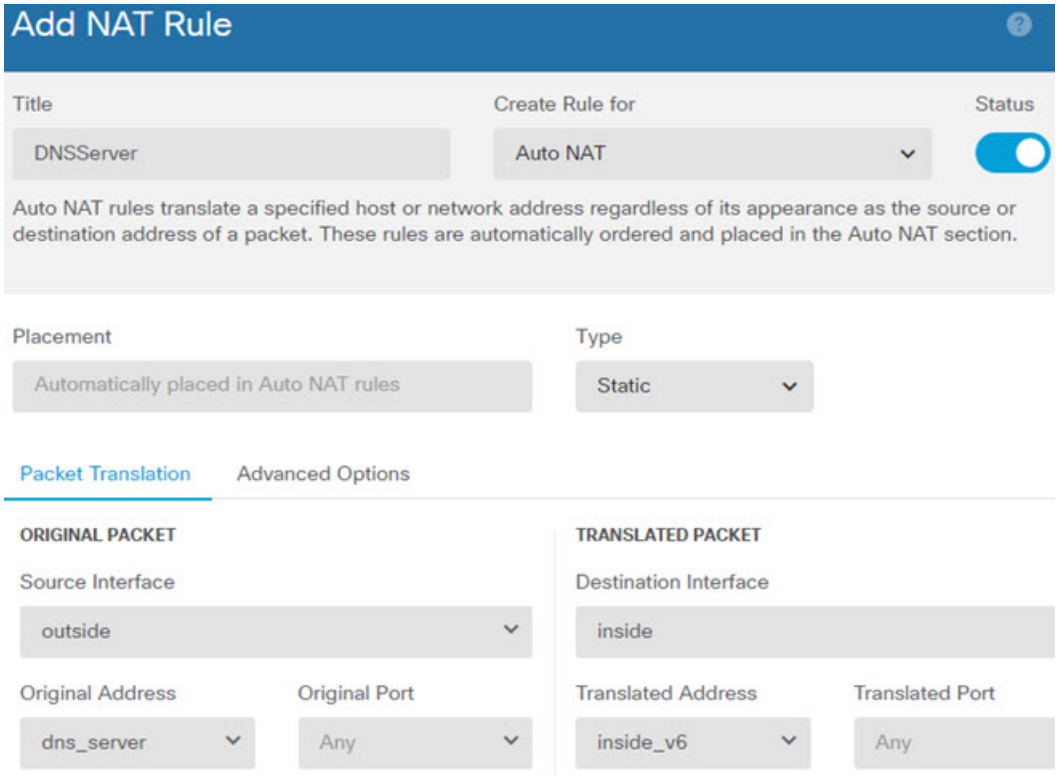
d) **OK(**확인**)**를 클릭합니다.

단계 **3** DNS 서버용 고정 NAT 규칙을 구성합니다.

a) **Policies(**정책**)** > **NAT**를 선택합니다.
b) + 버튼을 클릭합니다.
c) 다음 속성을 구성합니다.

- **Title(**제목**)** = DNSServer 또는 원하는 다른 이름
- **Create Rule For(**규칙 생성**)** = 자동 NAT

- **Type(**유형**)** = 고정
- **Source Interface(**원본 인터페이스**)** = outside
- **Destination Interface(**대상 인터페이스**)** = inside
- **Original Address(**원본 주소**)** = dns_server 네트워크 개체
- **Translated Address(**변환된 주소**)** = inside_v6 네트워크 개체 IPv4 주소를 IPv6 주소로 변환할 때는 IPv4 임베디드 주소 방법이 사용되므로 209.165.201.15는 동일한 IPv6 주소인 D1A5:C90F로 변환되며, 네트워크 접두사가 추가되어 전체 주소는 2001:DB8::D1A5:C90F가 됩니다.



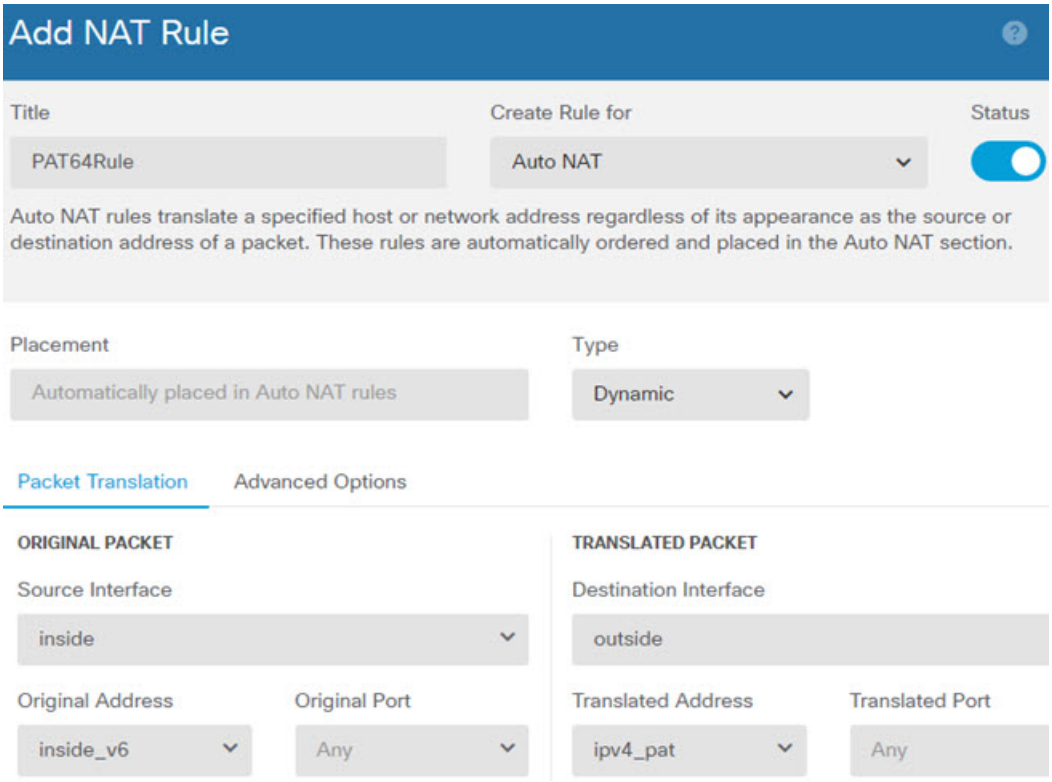
d) **OK(**확인**)**를 클릭합니다.

단계 **4** 내부 IPv6 네트워크용 동적 PAT 규칙을 구성합니다.

a) **Policies(**정책**)** > **NAT**를 선택합니다.
b) + 버튼을 클릭합니다.
c) 다음 속성을 구성합니다.

- **Title(**제목**)** = PAT64Rule 또는 원하는 다른 이름
- **Create Rule For(**규칙 생성**)** = 자동 NAT
- **Type(**유형**)** = 동적
- **Source Interface(**원본 인터페이스**)** = inside

- **Destination Interface(**대상 인터페이스**)** = outside
- **Original Address(**원본 주소**)** = inside_v6 네트워크 개체
- **Translated Address(**변환된 주소**)** = ipv4_pat 네트워크 개체



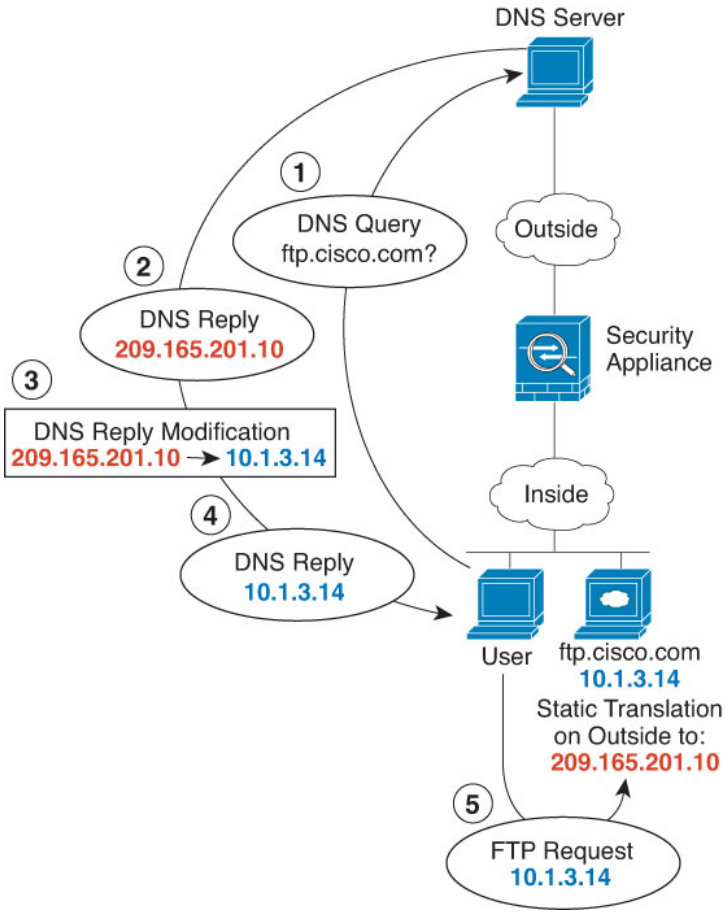
d) **OK(**확인**)**를 클릭합니다.

DNS 회신 수정, 외부의 DNS 서버

다음 그림은 인터페이스 외부에서 액세스할 수 있는 DNS 서버를 보여줍니다. ftp.cisco.com 서버는 내부 인터페이스에 있습니다. ftp.cisco.com 실제 주소(10.1.3.14)를 외부 네트워크에서 보이는 매핑된 주소(209.165.201.10)로 고정 변환하도록 NAT를 구성하십시오.

이 경우, 실제 주소를 사용하여 ftp.cisco.com에 액세스할 수 있는 내부 사용자가 DNS 서버에서 실제 주소(매핑된 주소가 아님)를 받을 수 있도록 고정 규칙에 대한 DNS 회신 수정을 사용할 수 있습니다.

내부 호스트가 ftp.cisco.com 주소에 DNS 요청을 전송하면, DNS 서버는 매핑된 주소(209.165.201.10)로 회신합니다. 시스템은 내부 서버에 대한 고정 규칙을 참조하여 DNS 회신에 있는 주소를 10.1.3.14로 변환합니다. DNS 회신 수정을 활성화하지 않으면 내부 호스트는 ftp.cisco.com에 직접 액세스하는 대신 트래픽을 209.165.201.10으로 전송하려고 시도하게 됩니다.



참고 이 예에서는 내부 인터페이스가 BVI(브리지 그룹 인터페이스)가 아닌 표준 라우팅 인터페이스라고 가정합니다. 내부 인터페이스가 BVI인 경우에는 각 멤버 인터페이스에 대한 규칙을 중복 생성해야 합니다.

프로시저

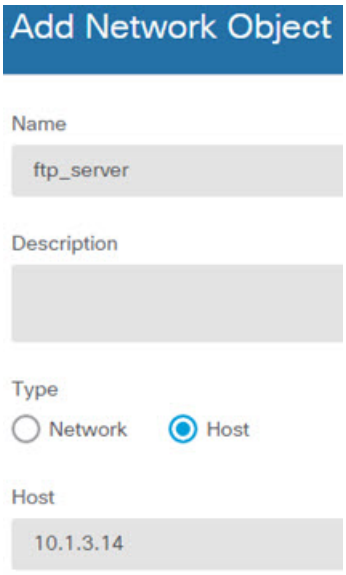
단계 **1** FTP 서버용 네트워크 개체를 생성합니다.

a) **Objects(**개체**)**를 선택합니다.

b) 목차에서 **Network(**네트워크**)**를 선택하고 +를 클릭합니다.

c) 실제 FTP 서버 주소를 정의합니다.

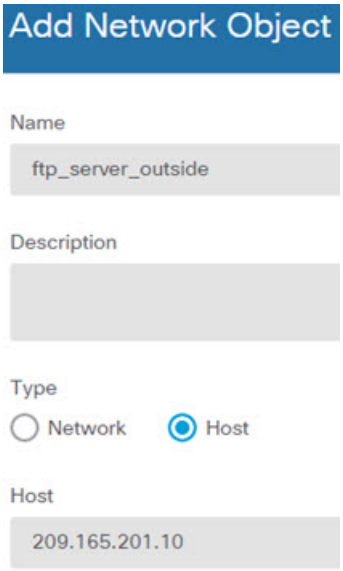
네트워크 개체의 이름을 ftp_server와 같이 지정하고 **Host(**호스트**)**를 선택한 후에 실제 호스트 IP 주소 10.1.3.14를 입력합니다.



d) **OK(**확인**)**를 클릭합니다.

e) **+**를 클릭하여 FTP 서버의 변환된 주소를 정의합니다.

네트워크 개체의 이름을 ftp_server_outside와 같이 지정하고 **Host(**호스트**)**를 선택한 후에 호스트 주소 209.165.201.10을 입력합니다.



단계 **2** FTP 서버에 대해 DNS를 수정하여 고정 NAT 규칙을 구성합니다.

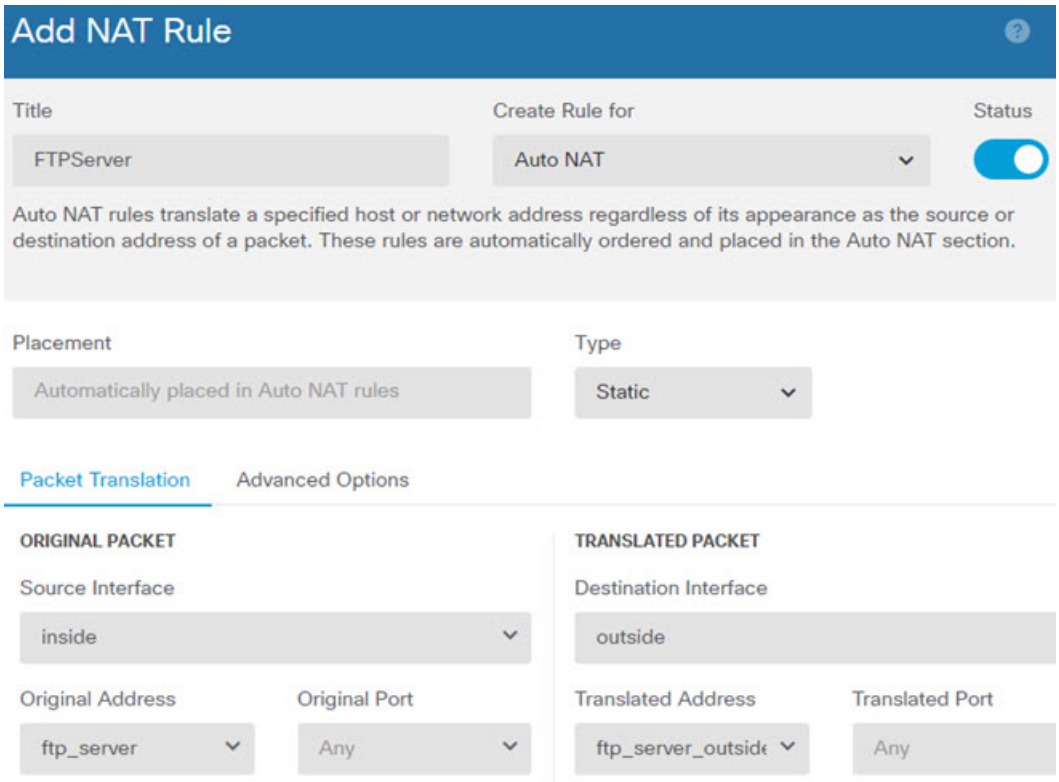
a) **Policies(**정책**)** > **NAT**를 선택합니다.

b) **+** 버튼을 클릭합니다.

c) 다음 속성을 구성합니다.

- **Title(**제목**)** = FTPServer 또는 원하는 다른 이름

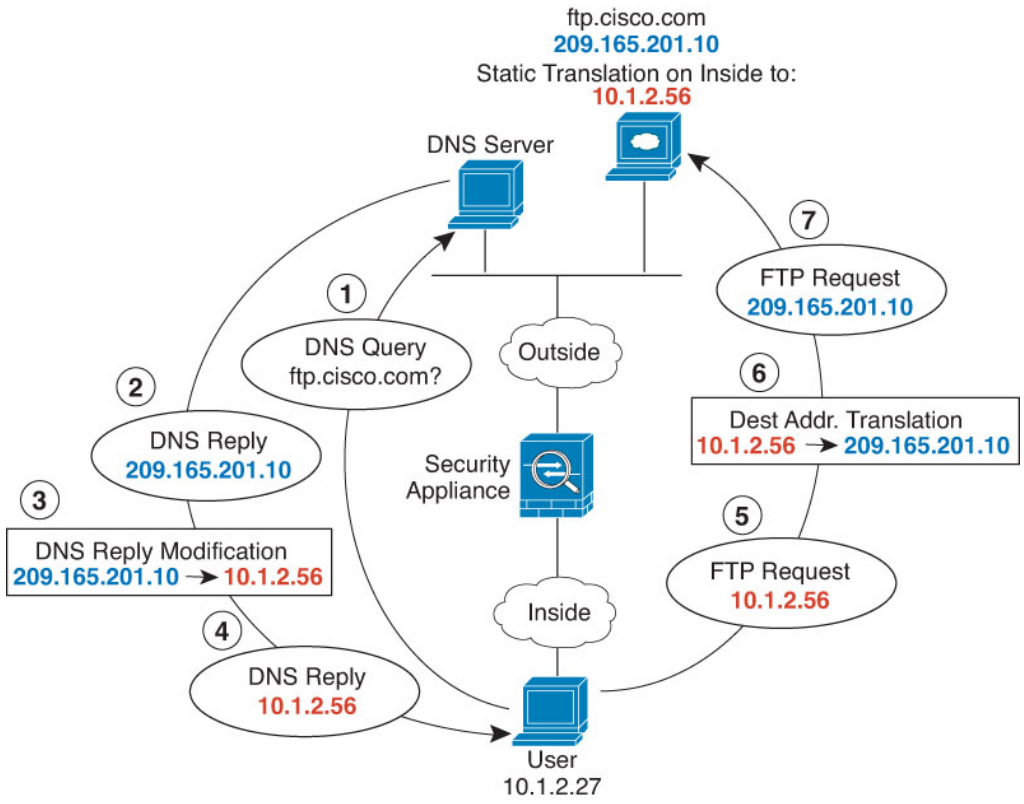
- **Create Rule For(**규칙 생성**)** = 자동 NAT
- **Type(**유형**)** = 고정
- **Source Interface(**원본 인터페이스**)** = inside
- **Destination Interface(**대상 인터페이스**)** = outside
- **Original Address(**원본 주소**)** = ftp_server 네트워크 개체
- **Translated Address(**변환된 주소**)** = ftp_server_outside 네트워크 개체
- **Advanced Options(**고급 옵션**)** 탭에서 **Translate DNS replies that match this rule(**이 규칙과 일치하는 **DNS** 응답 변환**)**을 선택합니다.



d) **OK(**확인**)**를 클릭합니다.

DNS 회신 수정, 호스트 네트워크의 **DNS** 서버

다음 그림은 외부의 FTP 서버 및 DNS 서버를 보여줍니다. 시스템은 외부 서버에 대해 고정 변환을 수행합니다. 이 경우 내부 사용자가 DNS 서버에서 ftp.cisco.com에 대한 주소를 요청하면 DNS 서버는 실제 주소인 209.165.20.10으로 응답합니다. 내부 사용자가 ftp.cisco.com(10.1.2.56)에 대한 매핑된 주소를 사용하도록 하려면 고정 변환에 대해 DNS 회신 수정을 구성해야 합니다.



참고 이 예에서는 내부 인터페이스가 BVI(브리지 그룹 인터페이스)가 아닌 표준 라우팅 인터페이스라고 가정합니다. 내부 인터페이스가 BVI인 경우에는 각 멤버 인터페이스에 대한 규칙을 중복 생성해야 합니다.

프로시저

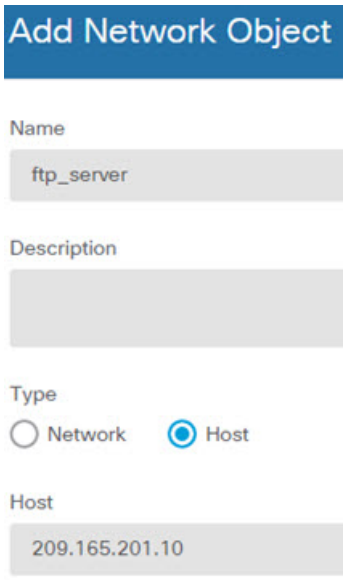
단계 **1** FTP 서버용 네트워크 개체를 생성합니다.

a) **Objects(**개체**)**를 선택합니다.

b) 목차에서 **Network(**네트워크**)**를 선택하고 +를 클릭합니다.

c) 실제 FTP 서버 주소를 정의합니다.

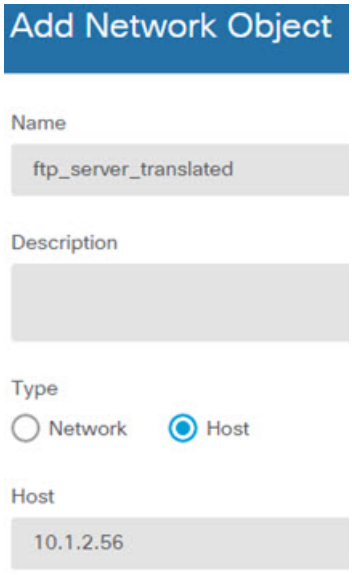
네트워크 개체의 이름을 ftp_server와 같이 지정하고 **Host(**호스트**)**를 선택한 후에 실제 호스트 IP 주소 209.165.201.10을 입력합니다.



d) **OK(**확인**)**를 클릭합니다.

e) +를 클릭하여 FTP 서버의 변환된 주소를 정의합니다.

네트워크 개체의 이름을 ftp_server_translated와 같이 지정하고 **Host(**호스트**)**를 선택한 후에 호스트 주소 10.1.2.56을 입력합니다.



단계 **2** FTP 서버에 대해 DNS를 수정하여 고정 NAT 규칙을 구성합니다.

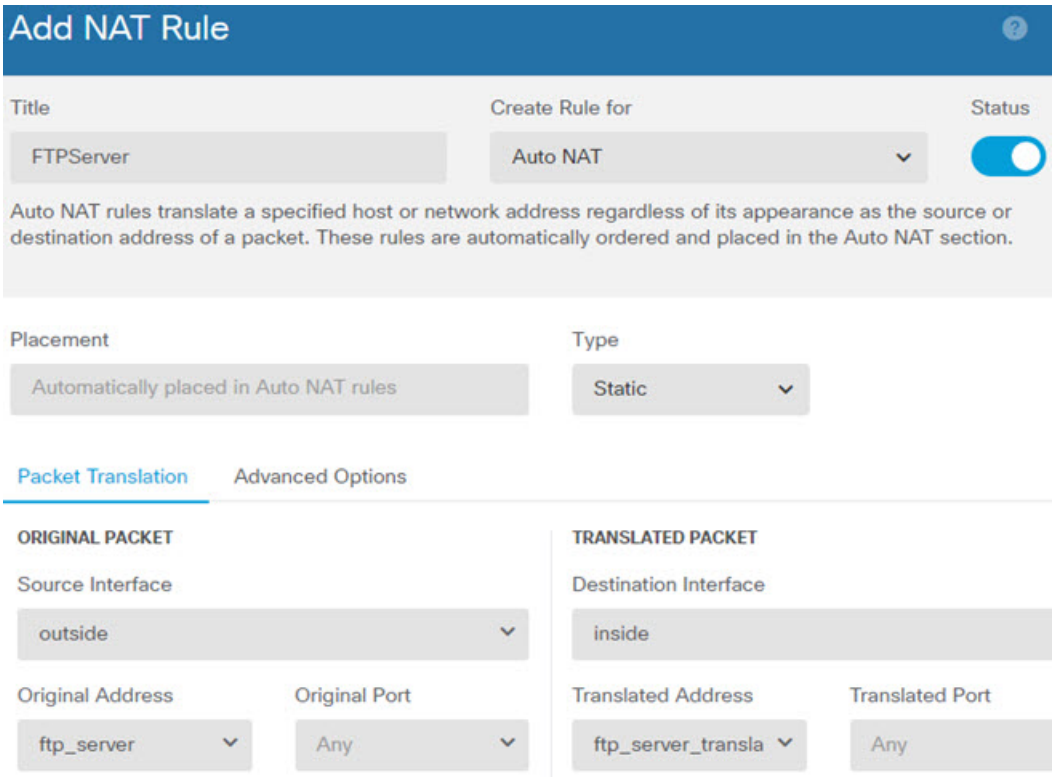
a) **Policies(**정책**)** > **NAT**를 선택합니다.

b) + 버튼을 클릭합니다.

c) 다음 속성을 구성합니다.

- **Title(**제목**)** = FTPServer 또는 원하는 다른 이름

- **Create Rule For(**규칙 생성**)** = 자동 NAT
- **Type(**유형**)** = 고정
- **Source Interface(**원본 인터페이스**)** = outside
- **Destination Interface(**대상 인터페이스**)** = inside
- **Original Address(**원본 주소**)** = ftp_server 네트워크 개체
- **Translated Address(**변환된 주소**)** = ftp_server_translated 네트워크 개체
- **Advanced Options(**고급 옵션**)** 탭에서 **Translate DNS replies that match this rule(**이 규칙과 일치하는 **DNS** 응답 변환**)**을 선택합니다.



d) **OK(**확인**)**를 클릭합니다.

VI 부

VPN(Virtual Private Network)

24 장

사이트 대 사이트 VPN

VPN(Virtual Private Network)은 인터넷과 같은 공개 소스나 기타 네트워크를 통해 원격 피어 간에 보안 터널을 설정하는 네트워크 연결입니다. VPN은 터널을 사용하여 IP 기반 네트워크를 통해 전달할 수 있도록 일반 IP 패킷 내의 데이터 패킷을 캡슐화합니다. VPN은 암호화를 사용해 개인 정보와 인증을 확인함으로써 데이터의 무결성을 보장합니다.

VPN 기본 사항

터널링을 통해 인터넷과 같은 공용 TCP/IP 네트워크를 사용하고 원격 사용자와 사설 기업 네트워크 간의 안전한 연결을 생성할 수 있습니다. 각 보안 연결을 터널이라고 부릅니다.

IPsec 기반 VPN 기술은 ISAKMP/IKE(Internet Security Association and Key Management Protocol) 및 IPsec 터널링 표준을 사용하여 터널을 작성하고 관리합니다. ISAKMP 및 IPsec는 다음 사항을 수행합니다.

- 터널 파라미터 협상
- 터널 설정
- 사용자 및 데이터 인증
- 보안 키 관리
- 데이터 암호화 및 암호 해독
- 터널을 통한 데이터 전송 관리
- 터널 엔드포인트 또는 라우터로 데이터 전송 인바운드 및 아웃바운드 관리

VPN의 디바이스는 양방향 터널 엔드포인트로 작동합니다. 사설 네트워크에서 일반 패킷을 수신하여 캡슐화하고 터널을 생성하며, 캡슐 해제하여 최종 대상에 전송하는 다른 쪽 터널의 끝으로 보낼

수 있습니다. 또한 공용 네트워크에서 캡슐화된 패킷을 수신하여 캡슐을 해제하여 사설 네트워크의 최종 대상에 보낼 수 있습니다.

사이트 대 사이트 VPN 연결이 설정되면 로컬 게이트웨이의 뒤에 있는 호스트는 보안 VPN 터널을 통해 원격 게이트의 뒤에 있는 호스트와 연결할 수 있습니다. 연결은 두 게이트웨이의 IP 주소와 호스트 이름, 그 뒤에 있는 서브넷, 두 게이트웨이가 상호 인증에 사용하는 방법으로 구성됩니다.

IKE(Internet Key Exchange)

IKE(Internet Key Exchange)는 IPsec 피어를 인증하고, IPsec 암호화 키를 협상 및 배포하고, IPsec SA(Security Association, 보안 연계)를 자동으로 설정하는 데 사용되는 키 관리 프로토콜입니다.

IKE 협상은 2단계로 구성됩니다. 1단계에서는 두 IKE 피어 간의 보안 연계를 협상합니다. 그러면 피어가 2단계에서 안전하게 통신할 수 있습니다. 2단계 협상 중에는 IKE가 IPsec 등의 기타 애플리케이션에 대해 SA를 설정합니다. 두 단계에서는 모두 연결을 협상할 때 제안을 사용합니다.

IKE 정책은 두 피어가 상호 간의 KIE 협상을 보호하는 데 사용하는 알고리즘 집합입니다. IKE 협상에서는 두 피어가 먼저 공통(공유) IKE 정책을 합의합니다. 이 정책은 후속 IKE 협상을 보호하는 보안 파라미터를 제시합니다. IKEv1(IKE 버전 1)의 경우 IKE 정책에는 단일 알고리즘 집합과 모듈러스 그룹이 포함됩니다. IKEv1과 달리 IKEv2 정책에서는 피어가 1단계 협상 중에 선택할 수 있는 여러 알고리즘 및 모듈러스 그룹을 선택할 수 있습니다. 단일 IKE 정책을 생성할 수도 있지만, 여러 정책을 생성해 가장 적절한 옵션에 더 높은 우선 순위를 지정할 수도 있습니다. 사이트 대 사이트 VPN의 경우에는 단일 IKE 정책을 생성할 수 있습니다.

IKE 정책을 정의하려면 다음 사항을 지정합니다.

- 고유한 우선 순위(1~65,543, 1이 우선 순위가 가장 높음)
- 데이터 및 개인정보를 보호하기 위한 IKE 협상의 암호화 방법
- 보낸 사람의 ID를 확인하고 메시지가 전송 중에 수정되지 않았는지 확인할 HMAC(Hashed Message Authentication Codes, 해시 메시지 인증 코드) 방법(IKEv2에서는 무결성 알고리즘이라고 함)
- IKEv2의 경우 IKEv2 터널 암호화에 필요한 키 요소 및 해싱 작업을 파생시키기 위한 알고리즘으로 사용되는 별도의 PRF(Pseudo Random Function, 의사 난수 함수). 옵션은 해시 알고리즘에 사용되는 것과 동일합니다.
- encryption-key-determination 알고리즘의 수준을 결정하는 Diffie-Hellman 그룹. 디바이스는 이 알고리즘을 사용하여 암호화 및 해시 키를 파생합니다.
- 피어의 ID를 확인할 인증 방법
- 디바이스가 교체 전 암호화 키를 사용하는 시간제한

IKE 협상이 시작되면 협상을 시작한 피어가 활성화된 모든 정책을 원격 피어로 보내고 원격 피어는 우선 순위대로 자신의 정책과 일치하는 정책을 검색합니다. 암호화, 해시(IKEv2의 경우 무결성 및 PRF), 인증 및 Diffie-Hellman 값이 동일하고 SA 수명이 전송된 정책의 수명보다 작거나 같으면 IKE 정책은 서로 일치하는 것으로 간주됩니다. 수명이 동일하지 않은 경우에는 원격 피어에서 가져온 더 짧은 수명이 적용됩니다. 기본적으로는 DES를 사용하는 단순 IKE 정책만 활성화됩니다. 우선 순위가 더 높은 다른 IKE 정책을 활성화하여 더욱 강력한 암호화 표준을 협상할 수도 있지만, DES 정책으로도 협상은 정상적으로 진행됩니다.

VPN 연결의 보안 수준 결정

VPN 터널은 일반적으로 공용 네트워크(대개 인터넷)를 통과하므로 연결을 암호화하여 트래픽을 보호해야 합니다. IKE 정책 및 IPsec 제안을 사용하여 적용할 암호화 및 기타 보안 기술을 정의합니다.

디바이스 라이선스에서 강력한 암호화 적용이 허용되는 경우에는 광범위한 암호화 및 해시 알고리즘과 Diffie-Hellman 그룹 중에서 선택할 수 있습니다. 그러나 일반적으로는 터널에 적용하는 암호화가 강력할수록 시스템 성능은 더 나빠집니다. 따라서 효율성을 저하하지 않으면서 충분한 보호 기능을 제공하는 보안과 성능 간의 적절한 균형 지점을 찾아야 합니다.

Cisco는 선택할 수 있는 옵션에 대한 구체적인 지침을 제공하지는 않습니다. 대규모 기업이나 기타 조직 내에서 보안을 담당하는 경우 충족해야 하는 표준이 이미 정의되어 있을 수 있습니다. 그렇지 않은 경우, 선택할 수 있는 옵션에 대해 조사해야 합니다.

다음 주제에서는 사용 가능한 옵션에 대해 설명합니다.

사용할 암호화 알고리즘 결정

IKE 정책 또는 IPsec 제안에 사용할 암호화 알고리즘을 결정할 때는 VPN의 디바이스가 지원하는 알고리즘으로 선택이 제한됩니다.

IKEv2의 경우 여러 암호화 알고리즘을 구성할 수 있습니다. 시스템은 가장 안전한 항목부터 가장 안전하지 않은 항목 순으로 설정 순서를 지정하고 해당 순서를 사용하여 피어와 협상합니다. IKEv1의 경우 단일 옵션만 선택할 수 있습니다.

IPsec 제안의 경우 알고리즘은 인증, 암호화 및 재생 방지 서비스를 제공하는 ESP(Encapsulating Security Protocol)에서 사용됩니다. ESP는 IP 프로토콜 유형 50입니다. IKEv1 IPsec 제안에서 알고리즘 이름에는 ESP- 접두사가 붙습니다.

디바이스 라이선스에 따라 강력한 암호화를 사용할 수 있는 경우 다음 암호화 알고리즘 중에서 선택할 수 있습니다. 강력한 암호화를 사용할 수 없으면 DES만 선택할 수 있습니다.

참고 강력한 암호화에 적합한 경우 평가판 라이선스에서 스마트 라이선스로 업그레이드하기 전에 VPN 구성이 제대로 작동하도록 암호화 알고리즘을 확인하고 업데이트하십시오. AES 기반 알고리즘을 선택합니다. 강력한 암호화를 지원하는 계정을 사용하여 등록한 경우 DES는 지원되지 않습니다. 등록 후에는 모든 DES 사용을 제거할 때까지 변경 사항을 구축할 수 없습니다.

- AES-GCM - (IKEv2에만 해당됨) 기밀 유지 및 데이터 원본 인증 기능을 제공하는 블록 암호화 작동 모드인 AES-GCM(Advanced Encryption Standard in Galois/Counter Mode)은 AES보다 보안성이 뛰어납니다. AES-GCM은 세 가지 키 강도(128비트, 192비트 및 256비트 키)를 제공합니다. 키 길이가 길수록 보안성은 더 높지만 성능은 낮습니다. GCM은 NSA Suite B를 지원하는 데 필요한 AES의 모드입니다. NSA Suite B는 암호화 강도에 대한 연방 기준을 충족시키기 위해 디바이스가 지원해야 하는 암호화 알고리즘 세트입니다. .
- AES - AES(Advanced Encryption Standard)는 DES보다 보안성이 뛰어나며 3DES보다 계산 효율성이 높은 대칭 암호화 알고리즘입니다. AES는 세 가지 키 강도(128비트, 192비트 및 256비트 키)를 제공합니다. 키 길이가 길수록 보안성은 더 높지만 성능은 낮습니다.

- DES - 56비트 키를 사용하여 암호화를 수행하는 DES(Data Encryption Standard)는 대칭 보안 키 블록 알고리즘입니다. 라이선스 어카운트가 내보내기 제어에 대한 요건을 충족하지 않는 경우에는 이 옵션이 유일한 옵션입니다.
- Null, ESP-Null-사용하지 않습니다. null 암호화 알고리즘은 암호화를 수행하지 않는 인증 기능을 제공합니다. 이는 대부분의 플랫폼에서 지원되지 않습니다.

사용할 해시 알고리즘 결정

IKE 정책에서 해시 알고리즘은 메시지 무결성을 보장하는 데 사용되는 메시지 다이제스트를 생성합니다. IKEv2에서 해시 알고리즘은 두 가지 옵션으로 구분됩니다. 그중 하나는 무결성 알고리즘 옵션이고 다른 하나는 PRF(Pseudo-Random Function: 의사 난수 함수) 옵션입니다.

IPsec 제안에서 해시 알고리즘은 인증을 위한 ESP(Encapsulating Security Protocol)에서 사용됩니다. IKEv2 IPsec 제안에서는 이러한 알고리즘을 무결성 해시라고 합니다. IKEv1 IPsec 제안에서는 알고리즘 이름에 ESP- 접두사가 붙으며 -HMAC(Hash Method Authentication Code) 접미사도 붙습니다.

IKEv2의 경우 여러 해시 알고리즘을 구성할 수 있습니다. 시스템은 가장 안전한 항목부터 가장 안전하지 않은 항목 순으로 설정 순서를 지정하고 해당 순서를 사용하여 피어와 협상합니다. IKEv1의 경우 단일 옵션만 선택할 수 있습니다.

다음 해시 알고리즘 중에서 선택할 수 있습니다.

- SHA(Secure Hash Algorithm) - 표준 SHA(SHA1)에서는 160비트 다이제스트를 생성합니다.

  IKEv2 컨피그레이션에는 다음과 같은 더욱 안전한 SHA-2 옵션을 사용할 수 있습니다. NSA Suite B 암호화 사양을 구현하려는 경우 이러한 옵션 중 하나를 선택합니다.

  - SHA256 - 256비트 다이제스트를 생성하는 Secure Hash Algorithm SHA 2를 지정합니다.
  - SHA384 - 384비트 다이제스트를 생성하는 Secure Hash Algorithm SHA 2를 지정합니다.
  - SHA512 - 512비트 다이제스트를 생성하는 Secure Hash Algorithm SHA 2를 지정합니다.

- null 또는 None(NULL, ESP-NONE) - (IPsec 제안에만 해당됨) null 해시 알고리즘으로, 대개 테스트용으로만 사용됩니다. 그러나 AES-GCM 옵션 중 하나를 암호화 알고리즘으로 선택하는 경우에는 null 무결성 알고리즘을 선택해야 합니다. null 이외의 옵션을 선택하더라도 이러한 암호화 표준에 대해서는 무결성 해시가 무시됩니다.

사용할 **Diffie-Hellman** 모듈러스 그룹 결정

다음 Diffie-Hellman 키 파생 알고리즘을 사용하여 IPsec 보안 연계(SA) 키를 생성할 수 있습니다. 각 그룹의 크기 모듈러스는 서로 다릅니다. 대형 모듈러스는 보안성은 더 높지만, 처리 시간이 더 오래 걸립니다. 두 피어에 일치하는 모듈러스 그룹이 있어야 합니다.

AES 암호화를 선택하는 경우 AES에 필요한 큰 키를 지원하려면 DH(Diffie-Hellman) 그룹 5 이상을 사용해야 합니다. IKEv1 정책에서는 아래에 나열된 그룹을 모두 지원하지는 않습니다.

NSA Suite B 암호화 사양을 구현하려면 IKEv2를 사용하고 ECDH(Elliptic Curve Diffie-Hellman) 옵션 19, 20, 21 중 하나를 선택합니다. 2048비트 모듈러스를 사용하는 엘립틱 커브 옵션과 그룹은 Logjam과 같은 공격에 노출될 가능성이 작습니다.

IKEv2의 경우에는 여러 그룹을 구성할 수 있습니다. 시스템은 가장 안전한 항목부터 가장 안전하지 않은 항목 순으로 설정 순서를 지정하고 해당 순서를 사용하여 피어와 협상합니다. IKEv1의 경우 단일 옵션만 선택할 수 있습니다.

- 14 - Diffie-Hellman 그룹 14: 2048비트 MODP(모듈식 지수) 그룹. 192비트 키에 적합한 보호를 제공합니다.
- 15 - Diffie-Hellman 그룹 15: 3072비트 MODP 그룹
- 16 - Diffie-Hellman 그룹 16: 4096비트 MODP 그룹
- 19 - Diffie-Hellman 그룹 19: NIST(국내 표준 및 기술) 256비트 ECP(elliptic curve modulo a prime) 그룹
- 20 - Diffie-Hellman 그룹 20: NIST 384비트 ECP 그룹
- 21 - Diffie-Hellman 그룹 21: NIST 521비트 ECP 그룹
- 31 - Diffie-Hellman 그룹 31: Curve25519 256비트 EC 그룹

사용할 인증 방법 결정

다음과 같은 방법을 사용하여 Site-to-Site VPN 연결에서 피어를 인증할 수 있습니다.

사전 공유 키

사전 공유 키는 연결에서 각 피어에 컨피그레이션된 암호 키 문자열입니다. 이 키는 인증 단계 중에 IKE에서 사용합니다. IKEv1의 경우, 각 피어에서 동일한 사전 공유 키를 컨피그레이션해야 합니다. IKEv2의 경우, 각 피어에 고유 키를 컨피그레이션할 수 있습니다.

사전 공유 키는 인증서에 비해 확장성이 떨어집니다. 다수의 Site-to-Site VPN 연결을 컨피그레이션해야 하는 경우, 사전 공유 키 방법 대신 인증서 방법을 사용하십시오.

인증서

디지털 인증서에서는 RSA 키 쌍을 사용하여 IKE 키 관리 메시지에 서명하고 이를 암호화합니다. Site-to-Site VPN 연결의 양쪽 엔드를 컨피그레이션하는 경우, 원격 피어에서 로컬 피어를 인증할 수 있도록 로컬 디바이스의 ID 인증서를 선택하십시오.

인증서 방법을 사용하려면 다음 작업을 수행해야 합니다.

1. CA(Certification Authority)로 로컬 피어를 등록하여 디바이스 ID 인증서를 가져옵니다. 이 인증서를 디바이스에 업로드합니다. 자세한 내용은 내부 및 내부 CA 인증서 업로드, 165 페이지를 참고하십시오.

   원격 피어에 대한 책임도 있는 경우, 원격 피어도 등록하십시오. 피어에 대해 동일한 CA를 사용하는 것이 편리하지만 필수 요건은 아닙니다.

   SSC(자가서명 인증서)를 사용해 VPN 연결을 설정할 수는 없습니다. Certificate Authority로 디바이스를 등록해야 합니다.

   Windows CA(Certificate Authority)를 사용하여 Site-to-Site VPN 엔드포인트용 인증서를 생성하는 경우, 애플리케이션 정책 확장을 위해 IP 보안 엔드 시스템을 지정하는 인증서를 사용해야 합니다. Windows CA 서버의 Extensions(확장) 탭에 있는 인증서의 Properties(속성) 대화

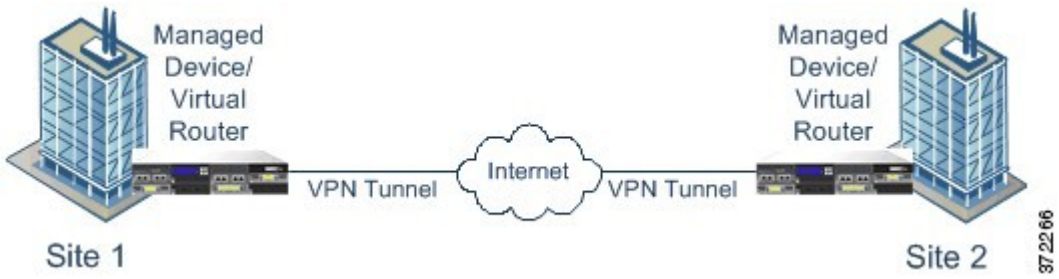
상자에서 이를 확인할 수 있습니다. 이 확장의 기본값은 device manager을 사용하여 구성된 Site-to-Site VPN에 대해 작동하지 않는 IP 보안 IKE 중개입니다.

2. 로컬 피어의 ID 인증서에 서명하는 데 사용된 신뢰할 수 있는 CA 인증서를 업로드합니다. 중간 CA를 사용한 경우, 루트 및 중간 인증서를 포함하여 전체 체인을 업로드합니다. 자세한 내용은 신뢰할 수 있는 CA 인증서 업로드, 169 페이지를 참고하십시오.
3. 원격 피어가 다른 CA로 등록된 경우, 원격 피어의 ID 인증서 서명에 사용된 신뢰할 수 있는 CA 인증서도 업로드하십시오. 원격 피어를 제어하는 조직에서 인증서를 가져옵니다. 중간 CA를 사용한 경우, 루트 및 중간 인증서를 포함하여 전체 체인을 업로드합니다.
4. 사이트 대 사이트 VPN 연결을 컨피그레이션하는 경우, 인증서 방법을 선택한 후 로컬 피어의 ID 인증서를 선택합니다. 연결의 양쪽 엔드에서는 연결의 로컬 엔드에 대해 인증서를 지정합니다. 원격 피어에 대해서는 인증서를 지정하지 마십시오.

VPN 토폴로지

device manager를 통해서는 포인트 투 포인트 VPN 연결만 구성할 수 있습니다. 모든 연결은 포인트 투 포인트 방식이지만, 디바이스가 참여하는 각 터널을 정의하여 보다 규모가 큰 허브 앤 스포크(hub and spoke) 또는 메시 VPN에 연결할 수 있습니다.

다음 다이어그램은 일반적인 포인트 투 포인트 VPN 토폴로지를 보여줍니다. 포인트 투 포인트 VPN 토폴로지에서는 2개의 엔드포인트가 서로 직접 통신합니다. 두 엔드포인트를 피어 디바이스로 구성하며, 두 디바이스 중 하나가 보안 연결을 시작할 수 있습니다.



동적 주소 지정 피어로 Site-to-Site VPN 연결 설정

피어의 IP 주소를 알지 못하는 경우에도 피어에 사이트 대 사이트 VPN 연결을 생성할 수 있습니다. 이러한 기능은 다음 상황에서 유용할 수 있습니다.

- 피어에서 DHCP를 사용하여 해당 주소를 가져오는 경우, 특정 정적 IP 주소가 있는 원격 엔드포인트에는 의존할 수 없습니다.
- hub-and-spoke 토폴로지에 허브 역할을 하는 디바이스와 연결을 설정하기 위해 확정되지 않은 수의 원격 피어를 허용하려는 경우

동적 주소 지정 피어 B에 보안 연결을 설정해야 하는 경우, 연결의 엔드인 A에 정적 IP 주소가 있는지 확인해야 합니다. 그런 다음, A에 연결을 생성할 때 피어의 주소가 동적 상태가 되도록 지정합니다.

그러나 피어 B에 연결을 컨피그레이션하는 경우, 반드시 A에 대한 IP 주소를 원격 피어 주소로 입력해야 합니다.

시스템에서 사이트 대 사이트 VPN 연결을 설정하는 경우, 피어에 동적 주소가 있는 모든 연결은 응답 전용입니다. 즉 원격 피어는 연결을 시작하는 것이어야 합니다. 원격 피어에서 연결 설정을 시도하면 장치에서는 사전 공유 키든 인증서든 연결에 정의한 방법을 사용하여 연결을 확인합니다.

원격 피어에서 연결을 시작한 후에만 VPN 연결이 설정되므로 VPN 터널에서 트래픽을 허용하는 액세스 제어 규칙과 일치하는 모든 아웃바운드 트래픽은 연결이 설정될 때까지 중단됩니다. 이를 통해 데이터가 적절한 암호화 및 VPN 보호 없이 네트워크를 벗어나지 않게 합니다.

Virtual Tunnel Interface 및 경로 기반 VPN

기존에는 VPN 터널을 통해 암호화할 특정 로컬 및 원격 네트워크를 정의하여 사이트 대 사이트 VPN 연결을 구성했습니다. 이는 VPN 연결 프로파일의 일부인 암호화 맵에서 정의됩니다. 이러한 유형의 사이트 대 사이트 VPN을 정책 기반이라고 합니다.

또는 경로 기반의 사이트 대 사이트 VPN을 구성할 수 있습니다. 이 경우 특정 물리적 인터페이스(일반적으로 외부 인터페이스)와 연결된 가상 인터페이스인 VTI(Virtual Tunnel Interface)를 생성합니다. 그 다음 정적 및 동적 경로와 함께 라우팅 테이블을 사용하여 원하는 트래픽을 VTI로 보냅니다. VTI(이그레스(egressing))를 통해 라우팅되는 모든 트래픽은 VTI에 대해 구성한 VPN 터널을 통해 암호화됩니다.

따라서 경로 기반 사이트 대 사이트 VPN을 통해 VPN 연결 프로파일을 전혀 변경하지 않고 간단히 라우팅 테이블을 변경하여 지정된 VPN 연결에서 보호된 네트워크를 관리할 수 있습니다. 이 변경 사항을 고려하여 원격 네트워크를 추적하고 VPN 연결 프로파일을 업데이트할 필요가 없습니다. 이는 클라우드 서비스 제공자 및 대기업에 대한 VPN 관리를 간소화합니다.

또한 터널에서 허용되는 트래픽 유형을 세부적으로 조정하기 위해 VTI에 대한 액세스 제어 규칙을 생성할 수 있습니다. 예를 들어 침입 검사, URL 및 애플리케이션 필터링을 적용할 수 있습니다.

경로 기반 VPN 구성을 위한 개요 프로세스

일반적으로 경로 기반 사이트 대 사이트 VPN을 설정하는 프로세스에는 다음 단계가 포함됩니다.

프로시저

단계 **1** 로컬 엔드포인트에 대한 IKEv1/2 정책 및 IPsec 제안을 생성합니다.

단계 **2** 원격 피어를 향하는 물리적 인터페이스와 연결된 VTI(Virtual Tunnel Interface)를 생성합니다.

단계 **3** VTI, IKE 정책 및 IPsec 제안을 사용하는 사이트 대 사이트 VPN 연결 프로파일을 생성합니다.

단계 **4** 원격 피어, 원격 VTI, 원격 피어 관점에서 이 로컬 VTI를 원격 엔드포인트로 지정하는 사이트 대 사이트 VPN 연결 프로파일에 동일한 IKE 및 IPsec 제안을 생성합니다.

단계 **5** 터널을 통해 적절한 트래픽을 전송하기 위해 두 피어에서 경로 및 액세스 제어 규칙을 생성합니다.

트래픽이 양방향으로 흐를 수 있도록 각 엔드포인트의 경로와 액세스 제어가 서로 미러링되는지 확인합니다.

정적 경로의 일반적인 특성은 다음과 같습니다.

- **Interface(**인터페이스**)** — VTI(Virtual Tunnel Interface) 이름입니다.
- **Networks(**네트워크**)** — 원격 엔드포인트로 보호되는 원격 네트워크를 정의하는 네트워크 개체입니다.
- **Gateway(**게이트웨이**)** — VPN 터널 원격 엔드포인트의 IP 주소를 정의하는 네트워크 개체입니다.

Virtual Tunnel Interface 및 경로 기반 VPN을 위한 지침

IPv6 지침

Virtual tunnel interface는 IPv4 주소만 지원합니다. VTI에서는 IPv6 주소를 구성할 수 없습니다.

추가 지침

- 최대 1,024개의 VTI를 생성할 수 있습니다.
- VTI 경로 기반 VPN에서는 정적이든 동적이든 RRI(reverse route injection) 설정을 구성할 수 없습니다. (threat defense API만 사용하여 RRI(reverse route injection) 설정을 구성할 수 있습니다.)
- VTI를 로컬 인터페이스로 선택할 경우 동적 피어 주소를 구성할 수 없습니다.
- VTI를 로컬 인터페이스로 선택할 경우 원격 백업 피어를 구성할 수 없습니다.
- 맞춤형 가상 라우터에 할당된 소스 인터페이스에는 VTI를 생성할 수 없습니다. 가상 라우터를 사용할 때 전역 가상 라우터의 인터페이스에서만 VTI를 설정할 수 있습니다.
- IKE 및 IPsec 보안 연계는 터널에서 데이터 트래픽에 관계없이 지속적으로 다시 입력됩니다. 이렇게 하면 VTI 터널은 항상 작동합니다.
- IKEv1 및 IKEv2는 모두 경로 기반 연결 프로파일에서 구성할 수 없습니다. 하나의 IKE 버전만 구성해야 합니다.
- VTI에 대한 암호화 맵 및 터널 대상에서 구성된 피어 주소가 서로 다르다면 동일한 물리적 스페이스에서 서로 다른 VTI 및 정책 기반(암호화 맵) 컨피그레이션을 구성할 수 있습니다.
- BTI 라우팅 프로토콜만 VTI를 통해 지원됩니다.
- 시스템에서 IOS IKEv2 VTI 클라이언트를 종료하는 경우 시스템이 IOS VTI 클라이언트에서 시작한 세션의 mode-CFG 특성을 검색할 수 없으므로 IOS에서 config-exchange 요청을 비활성화합니다.
- 경로 기반의 사이트 대 사이트 VPN은 양방향으로 구성됩니다. 즉, VPN 터널의 엔드포인트가 연결을 시작할 수 있습니다. 연결 프로파일을 생성한 후 이 엔드포인트를 유일한 이니시에이터(INITIATE_ONLY) 또는 전적으로 응답자(RESPOND_ONLY)로 변경할 수 있습니다. 보완 연결 유형을 사용하도록 원격 엔드포인트를 수정해야 합니다. 이 변경을 수행하려면 API Explorer로 이동하여 GET / devices/default/s2sconnectionprofiles를 사용하여 연결 프로파일을 찾아야 합니다.

그 다음 본문 콘텐츠를 PUT / devices/default/s2sconnectionprofiles/{objId} 메서드에 복사/붙여 넣기하고 **connectionType**을 업데이트하여 원하는 유형을 지정하고 메서드를 실행할 수 있습니다.

IPsec 플로우 오프로드

IPsec 플로우 오프로드를 사용하도록 지원 디바이스 모델을 구성할 수 있습니다. IPsec 사이트 간 VPN 또는 원격 액세스 VPN 보안 연계(SA)의 초기 설정 후 IPsec 연결은 디바이스의 FTPA(field-programmable gate Array)로 오프로드되므로 디바이스 성능이 향상됩니다.

오프로드된 작업은 특히 인그레스의 사전 암호 해독 및 암호 해독 처리 및 이그레스의 사전 암호화 및 암호화 처리와 관련이 있습니다. 시스템 소프트웨어는 보안 정책을 적용하기 위해 내부 플로우를 처리합니다.

IPsec 플로우 오프로드는 기본적으로 활성화되어 있으며 다음 디바이스 유형에 적용됩니다.

- Secure Firewall 3100

IPsec 플로우 오프로드에 대한 제한 사항

다음 IPsec 흐름은 오프로드되지 않습니다.

- IKEv1 터널. IKEv2 터널만 오프로드됩니다. IKEv2는 더 강력한 암호를 지원합니다.
- 볼륨 기반 키 재설정이 구성된 플로우.
- 압축이 구성된 플로우.
- 전송 모드 플로우. 터널 모드 플로우만 오프로드됩니다.
- AH 형식. ESP/NAT-T 형식만 지원됩니다.
- 사후 조각화가 구성된 플로우.
- 64비트 이외의 재생 방지 창 크기가 있는 플로우 및 재생 방지는 비활성화되지 않습니다.
- 방화벽 필터가 활성화된 플로우.

IPsec 플로우 오프로드 구성

IPsec 플로우 오프로드는 해당 기능을 지원하는 하드웨어 플랫폼에서 기본으로 활성화됩니다. 구성을 변경하려면 FlexConfig를 사용하여 **flow-offload-ipsec** 명령을 구현합니다. 명령에 대한 자세한 내용은 ASA 명령 참조를 확인하십시오.

사이트 대 사이트 VPN 관리

VPN(Virtual Private Network)은 인터넷과 같은 공개 소스나 기타 네트워크를 통해 원격 피어 간에 보안 터널을 설정하는 네트워크 연결입니다. VPN은 터널을 사용하여 IP 기반 네트워크를 통해 전달할 수 있도록 일반 IP 패킷 내의 데이터 패킷을 캡슐화합니다. VPN은 암호화를 사용해 개인 정보와 인증을 확인함으로써 데이터의 무결성을 보장합니다.

피어 디바이스에 대한 VPN 연결을 생성할 수 있습니다. 모든 연결은 포인트 투 포인트 방식이지만, 모든 관련 연결을 구성하여 규모가 더 큰 허브 앤 스포크(hub and spoke) 또는 메시 VPN에 디바이스를 연결할 수 있습니다.

시작하기 전에

다음 사실은 다시 생성할 수 있는 사이트 대 사이트 VPN 연결의 유형과 수를 제어합니다.

- VPN 연결은 암호화를 사용하여 네트워크 개인 정보를 보호합니다. 사용할 수 있는 암호화 알고리즘은 기본 라이선스가 강력한 암호화를 허용하는지에 따라 달라집니다. 강력한 암호화 허용 여부는 Cisco Smart License Manager에 등록할 때 디바이스에서 내보내기 제어 기능을 허용하는 옵션을 선택했는지에 따라 제어됩니다. 평가 라이선스를 사용 중이거나 내보내기 제어 기능을 활성화하지 않은 경우에는 강력한 암호화를 사용할 수 없습니다.
- 최대 20개의 고유한 IPsec 프로파일을 생성할 수 있습니다. 고유성은 IKEv1/v2 제안 및 인증서, 연결 유형, DH 그룹 및 SA 수명의 조합에 따라 결정됩니다. 기존 프로파일을 재사용할 수 있습니다. 따라서 모든 사이트 대 사이트 VPN 연결에 동일한 설정을 사용하는 경우 하나의 고유한 IPsec 프로파일을 갖습니다. 20개의 고유한 IPsec 프로파일 제한에 도달하면 기존 연결 프로파일에 사용한 것과 동일한 특성 조합을 사용하지 않는 한 새 사이트 대 사이트 VPN 연결을 생성할 수 없습니다.

프로시저

단계 **1** 디바이스를 클릭한 다음, 사이트 대 사이트 VPN 그룹에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

그러면 구성한 모든 연결이 나열되는 사이트 대 사이트 VPN 페이지가 열립니다.

단계 **2** 다음 중 하나를 수행합니다.

- 새 사이트 대 사이트 VPN 연결을 생성하려면 + 버튼을 클릭합니다. 사이트 대 사이트 VPN 연결 구성, 689 페이지의 내용을 참조하십시오.

  아직 연결이 없는 경우에는 **Create Site-to-Site Connection(**사이트 대 사이트 연결 생성**)** 버튼을 클릭할 수도 있습니다.

- 기존 연결을 수정하려면 해당 연결의 수정 아이콘()을 클릭합니다. 사이트 대 사이트 VPN 연결 구성, 689 페이지의 내용을 참조하십시오.

- 연결 컨피그레이션 요약을 클립보드에 복사하려면 해당 연결의 복사 아이콘()을 클릭합니다. 이 정보를 문서에 붙여넣은 다음 원격 디바이스 관리자에게 보내면 관리자가 해당 연결 쪽을 쉽게 구성할 수 있습니다.

- 더 이상 필요하지 않은 연결을 삭제하려면 해당 연결의 삭제 아이콘()을 클릭합니다.

사이트 대 사이트 VPN 연결 구성

원격 디바이스 소유자가 협조하며 권한을 제공한다고 가정할 때 디바이스를 서로 연결하기 위한 포인트 투 포인트 VPN 연결을 생성할 수 있습니다. 모든 연결은 포인트 투 포인트 방식이지만, 디바이스가 참여하는 각 터널을 정의하여 보다 규모가 큰 허브 앤 스포크(hub and spoke) 또는 메시 VPN에 연결할 수 있습니다.

시작하기 전에

로컬 네트워크/원격 네트워크 조합별로 단일 VPN 연결을 생성할 수 있습니다. 그러나 각 연결 프로파일에서 원격 네트워크가 고유한 경우에는 로컬 네트워크에 대해 여러 연결을 생성할 수 있습니다.

원격 네트워크가 중복되는 경우, 더욱 제한적인 연결 프로파일을 먼저 생성해야 합니다. 시스템에서는 표시되는 순서(단순히 영문자 순)가 아니라 연결 프로파일을 생성하는 순서대로 터널을 생성합니다.

예를 들어 192.16.0.0/16에서 10.91.0.0/16까지의 하나의 터널을 원격 엔드포인트 A로 이동하면서 터널 192.16.0.0/24를 원격 엔드포인트 B를 통해 나머지 10.0.0.0/8로 이동하게 하려면 B용 연결 프로파일을 생성하기 전에 A용 연결 프로파일을 생성해야 합니다.

프로시저

단계 **1** 디바이스를 클릭한 다음, 사이트 대 사이트 VPN 그룹에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 새 사이트 대 사이트 VPN 연결을 생성하려면 + 버튼을 클릭합니다.

  아직 연결이 없는 경우에는 **Create Site-to-Site Connection(**사이트 대 사이트 연결 생성**)** 버튼을 클릭할 수도 있습니다.

- 기존 연결을 수정하려면 해당 연결의 수정 아이콘()을 클릭합니다.

더 이상 필요하지 않은 연결을 삭제하려면 해당 연결의 삭제 아이콘()을 클릭합니다.

단계 **3** 포인트 투 포인트 VPN 연결의 엔드포인트를 정의합니다.

- **Connection Profile Name(**연결 프로파일 이름**)** - 이 연결의 이름을 공백 없이 64자까지 입력합니다. 예를 들면 MainOffice를 입력합니다. IP 주소는 이름으로 사용할 수 없습니다.
- 유형 — VPN 터널을 통해 어떤 트래픽을 전송해야 하는지 식별하는 방법입니다. 다음 중 하나를 선택합니다.
  - **Route Based (VTI)(**경로 기반**(VTI))** — 라우팅 테이블(주로 정적 경로)을 사용하여 터널에 참여해야 하는 로컬 및 원격 네트워크를 정의합니다. 이 옵션을 선택하는 경우 VTI(Virtual Tunnel Interface)를 로컬 VPN 액세스 인터페이스로 선택해야 합니다. 또한 터널의 원격 엔드에 대해 정적 IP 주소를 사용해야 합니다. VPN 연결 프로파일을 생성한 후 VTI에 대한 적절한 정적 경로 및 액세스 제어 규칙을 구성해야 합니다.

- **Policy Based(**정책 기반**)** — 사이트 대 사이트 VPN 연결 프로파일에서 로컬 및 원격 네트워크를 직접 지정합니다. 이는 VPN 터널로 보호해야 하는 트래픽을 정의하는 기존의 접근 방식입니다.

- 로컬 사이트 - 이러한 옵션은 로컬 엔드포인트를 정의합니다.
  - 로컬 **VPN** 액세스 인터페이스 - 원격 피어가 연결할 수 있는 인터페이스를 선택합니다. 이 인터페이스는 대개 외부 인터페이스이며, 브리지 그룹의 멤버일 수는 없습니다. 정책 기반 연결을 위해 백업 피어를 구성하는 경우, 피어가 연결할 수 있는 모든 인터페이스를 선택해야 합니다. 경로 기반 연결의 경우 하나의 인터페이스만 선택할 수 있습니다.
  - **Local Network(**로컬 네트워크**)** — (정책-기반 전용) +를 클릭하고 VPN 연결에 참여해야 하는 로컬 네트워크를 식별하는 네트워크 개체를 선택합니다. 이러한 네트워크의 사용자는 해당 연결을 통해 원격 네트워크에 접속할 수 있습니다.

    참고 이러한 네트워크에는 IPv4 또는 IPv6 주소를 사용할 수 있지만, 연결 양쪽의 주소 유형이 일치해야 합니다. 예를 들어 로컬 IPv4 네트워크에 대한 VPN 연결에는 원격 IPv4 네트워크가 하나 이상 있어야 합니다. 단일 연결의 양쪽에서 IPv4 및 IPv6를 함께 사용할 수 있습니다. 엔드포인트에 대한 보호된 네트워크는 겹칠 수 없습니다.

- 원격 사이트 - 이러한 옵션은 원격 엔드포인트를 정의합니다.
  - **Static(**정적**)**/**Dynamic(**동적**)** - 원격 피어의 IP 주소가 정적으로 정의되는지, 아니면 동적으로 정의되는지 여부(예: DHCP를 통한 정의). **Static(**정적**)**을 선택하는 경우, 원격 피어의 IP 주소도 입력합니다. **Dynamic(**동적**)**을 선택하는 경우, 원격 피어에서만 이 VPN 연결을 시작할 수 있습니다.

    경로-기반 VPN의 경우 **Static(**정적**)**만 선택할 수 있습니다.

  - **Remote IP Address(**원격 **IP** 주소**)**(정적 주소 지정에만 해당) - VPN 연결을 호스팅할 원격 VPN 피어 인터페이스의 IP 주소를 입력합니다.
  - **Remote Backup Peers(**원격 백업 피어**)** - (선택 사항, 정책 기반 연결에만 해당.) 원격 피어의 백업을 추가하려면 **Add Peer(**피어 추가**)**를 클릭합니다. 기본 엔드포인트를 사용할 수 없는 경우 시스템은 백업 피어 중 하나를 사용하여 VPN 연결 재설정을 시도합니다. 여러 백업을 추가할 수 있습니다.

    각 백업 피어를 구성할 때 해당 피어와 함께 사용할 사전 공유 키 및 인증서를 구성할 수 있습니다. 기본 원격 피어에 대해 구성한 것과 동일한 기술을 사용합니다. 연결 프로파일에 대해 설정된 동일한 값을 사용하려면 이 설정을 비워둡니다.

    첫 번째 백업 피어를 구성한 후에는 **Add Another Peer(**다른 피어 추가**)**를 클릭하여 피어를 추가 또는 삭제하거나 **Edit(**편집**)**를 클릭하여 피어의 설정을 변경할 수 있습니다.

    기본 피어가 아닌 다른 인터페이스를 통해 백업 피어에 연결할 수 있는 경우 **Local VPN Access Interface(**로컬 **VPN** 액세스 인터페이스**)**에서 필요한 인터페이스를 선택해야 합니다.

  - **Remote Network(**원격 네트워크**)** — (정책 기반 전용) +를 클릭하고 VPN 연결에 참여해야 하는 원격 네트워크를 식별하는 네트워크 개체를 선택합니다. 이러한 네트워크의 사용자는 해당 연결을 통해 로컬 네트워크에 접속할 수 있습니다.

단계 **4** **Next(**다음**)**를 클릭합니다.

단계 **5** VPN에 대한 프라이버시 컨피그레이션을 정의합니다.

참고 라이선스에 따라 선택 가능한 암호화 프로토콜이 결정됩니다. 가장 기본적인 옵션 외의 옵션을 선택하려면 강력한 암호화를 사용할 수 있어야 합니다(내보내기 제어를 충족해야 함).

- **IKE** 버전 **2**, **IKE** 버전 **1** - IKE(Internet Key Exchange) 협상 중에 사용할 IKE 버전을 선택합니다. 정책 기반 연결의 경우 둘 중 하나 또는 두 개 모두를 선택할 수 있습니다. 경로 기반의 경우 하나만 선택할 수 있습니다. 디바이스는 다른 피어와의 연결 협상을 시도할 때 사용자가 허용하며 다른 피어가 수락하는 버전을 사용합니다. 두 버전을 모두 허용하는 경우 디바이스는 처음 선택한 버전을 통한 협상이 실패하면 다른 버전으로 자동 대체합니다. IKEv2가 구성되어 있으면 IKEv2 사용을 항상 먼저 시도합니다. IKEv2를 협상에서 사용하려면 두 피어가 모두 IKEv2를 지원해야 합니다.

- **IKE** 정책 - IKE(Internet Key Exchange)는 IPsec 피어를 인증하고, IPsec 암호화 키를 협상 및 배포하고, IPsec SA(보안 연계)를 자동으로 설정하는 데 사용되는 키 관리 프로토콜입니다. IKE는 글로벌 정책이므로 활성화하는 개체가 모든 VPN에 적용됩니다. **Edit(**수정**)**을 클릭하여 IKE 버전별로 현재 전체적으로 활성화된 정책을 점검하고 새 정책을 활성화 및 생성합니다. 자세한 내용은 글로벌 IKE 정책 구성, 694 페이지의 내용을 참고하십시오.

- **IPsec** 제안 - IPsec 제안은 IPsec 터널에서 트래픽을 보호하는 보안 프로토콜 및 알고리즘 조합을 정의합니다. **Edit(**수정**)**을 클릭하고 각 IKE 버전에 대한 제안을 선택합니다. 허용하려는 모든 제안을 선택합니다. 시스템 기본값만 선택하려면 **Set Default(**기본값 설정**)**를 클릭합니다. 이러한 기본값은 내보내기 컴플라이언스에 따라 다릅니다. 시스템은 일치하는 항목이 합의될 때까지 가장 강력한 제안에서 가장 취약한 제안 순서대로 피어와 협상을 합니다. 자세한 내용은 IPsec 제안 구성, 699 페이지의 내용을 참고하십시오.

- 인증 유형 - VPN 연결에서 피어를 인증하고 싶은 방법으로 사전 공유 수동 키 또는 인증서를 선택합니다. 선택에 따라 다음 필드도 입력해야 합니다. IKEv1의 경우, 선택한 방법은 연결에 대해 컨피그레이션된 IKEv1 정책 개체에서 선택한 인증 방법과 일치해야 합니다. 이 옵션에 대한 세부 정보는 사용할 인증 방법 결정, 683 페이지의 내용을 참조하십시오.

  - (IKEv2) 로컬 사전 공유 키, 원격 피어 사전 공유 키 - VPN 연결을 위한 원격 디바이스와 이 디바이스에 정의된 키입니다. IKEv2에서는 이러한 키가 다를 수 있습니다. 키는 영숫자 1~127자가 될 수 있습니다.

  - (IKEv1) 사전 공유 키 - 로컬 디바이스와 원격 디바이스에 모두 정의된 키입니다. 키는 영숫자 1~127자가 될 수 있습니다.

  - 인증서 - 로컬 피어에 대한 디바이스 ID 인증서입니다. 이 인증서는 CA(Certification Authority)에서 가져온 것이어야 하며 SSC(자가서명 인증서)는 사용할 수 없습니다. 인증서를 업로드하지 않은 경우, **Create New Object(**새 개체 생성**)** 링크를 클릭합니다. ID 인증서 서명에 사용되는 신뢰할 수 있는 루트 및 중간 CA 인증서를 업로드해야 합니다. **IPsec** 클라이언트를 포함하도록 업로드된 인증서의 검증 사용을 설정해야 합니다. 인증서를 아직 업로드하지 않은 경우, 이 마법사를 완료한 후 업로드하면 됩니다.

- **IPsec Settings(IPsec** 설정**)** - 보안 연결의 수명입니다. 수명에 도달하면 시스템은 보안 연결을 다시 협상합니다. 시스템이 피어로부터 협상 요청을 받을 때, 피어에서 제안한 수명 값과 새 보안

연결의 수명으로 로컬에 설정된 수명 값 중 더 작은 값을 사용합니다. 수명에는 "timed" 수명과 "traffic-volume" 수명의 2가지가 있습니다. 이 수명 중 더 짧은 것에 도달하면 보안 연결이 만료됩니다.

- **Lifetime Duration(**수명 기간**)** - 보안 연결이 만료되기 전에 유지할 수 있는 시간(초)입니다. 범위는 120~214,783,647초입니다. 전역 기본값은 28,800초(8시간)입니다.
- **Lifetime Size(**수명 크기**)** - 보안 연결이 만료되기 전에 지정된 보안 연결을 사용하여 피어 간에 전달할 수 있는 트래픽 볼륨(KB)입니다. 범위는 10~2,147,483,647킬로바이트 또는 공백입니다. 전역 기본값은 4,608,000킬로바이트입니다. 크기 기반 제한을 제거하고 기간을 유일한 제한으로 사용하려면 필드를 비워 두십시오.

- **NAT Exempt(NAT** 제외**)** — (정책 기반 전용) 로컬 VPN 액세스 인터페이스의 NAT 정책에서 VPN 트래픽을 제외할지 여부를 선택합니다. NAT 규칙을 로컬 네트워크에 적용하지 않으려는 경우 로컬 네트워크를 호스팅하는 인터페이스를 선택합니다. 이 옵션은 로컬 네트워크가 단일 라우팅 인터페이스(브리지 그룹 멤버 아님) 뒤에 있는 경우에만 작동합니다. 로컬 네트워크가 둘 이상의 라우팅 인터페이스 또는 하나 이상의 브리지 그룹 멤버 뒤에 있는 경우에는 NAT 제외 규칙을 수동으로 생성해야 합니다. 필요한 규칙을 수동으로 생성하는 방법에 대한 자세한 내용은 NAT에서 사이트 대 사이트 VPN 트래픽 제외, 705 페이지를 참조하십시오.
- **PFS(Perfect Forward Secrecy)**에 대한 **Diffie-Helman** 그룹 - PFS(Perfect Forward Secrecy)를 사용하여 암호화된 각 교환에 대해 고유 세션 키를 생성하고 사용할지 여부를 선택합니다. 고유 세션 키는 전체 교환이 기록되었으며 공격자가 엔드포인트 디바이스에서 사용하는 사전 공유 키 또는 개인 키를 확보했더라도 후속 암호 해독에서 교환을 보호합니다. PFS(Perfect Forward Secrecy)를 활성화하려면 모듈러스 그룹 목록에서 PFS 세션 키를 생성할 때 사용할 Diffie-Hellman 키 파생 알고리즘을 선택합니다. IKEv1 및 IKEv2를 모두 활성화하면 IKEv1에서 지원하는 옵션만 선택할 수 있습니다. 옵션에 대한 설명은 사용할 Diffie-Hellman 모듈러스 그룹 결정, 682 페이지를 참조하십시오.

단계 **6** **Next(**다음**)**를 클릭합니다.

단계 **7** 요약을 검토하고 **Finish(**종료**)**를 클릭합니다.

요약 정보가 클립보드에 복사됩니다. 해당 정보를 문서에 붙여넣은 다음 원격 피어를 구성하는 데 사용하거나 피어 구성 담당자에게 보낼 수 있습니다.

사이트 대 사이트 VPN을 통한 트래픽 허용, 694 페이지의 설명대로 추가 단계를 수행하여 VPN 터널 내의 트래픽을 허용해야 합니다.

컨피그레이션을 구축한 후 디바이스 CLI에 로그인하고 **show ipsec sa** 명령을 사용하여 엔드포인트에서 보안 연결을 설정하는지 확인합니다. 사이트 대 사이트 VPN 연결 확인, 701 페이지의 내용을 참조하십시오.

Virtual Tunnel Interface 구성

경로 기반 사이트 대 사이트 VPN 연결 프로파일에서만 VTI(Virtual Tunnel Interface)를 사용할 수 있습니다. VTI는 물리적 인터페이스와 연결되며 이를 통해 원격 피어에 VPN 연결이 설정됩니다. 가상

인터페이스를 사용하면 연결 프로파일에서 VPN에 대한 로컬 및 원격 네트워크를 지정하는 대신 정적 및 동적 경로를 사용하여 사이트 대 사이트 VPN 연결을 간소화하고 트래픽을 제어할 수 있습니다.

프로시저

단계 **1** 디바이스를 클릭하고 인터페이스 요약의 링크를 클릭한 다음, **Virtual Tunnel Interfaces(Virtual Tunnel Interface)**를 클릭합니다.

단계 **2** 다음 중 하나를 수행합니다.

- **+** 또는 **Create Virtual Tunnel Interface(Virtual Tunnel Interface** 생성**)**를 클릭하여 새 인터페이스를 생성합니다.
- 기존 인터페이스에 대해 수정 아이콘( )을 클릭합니다.

인터페이스가 더 이상 필요하지 않은 경우 해당 인터페이스에 대해 삭제 아이콘( )을 클릭합니다. 먼저 인터페이스를 사용하는사이트 대 사이트 연결 프로파일을 삭제해야 이를 삭제할 수 있습니다.

단계 **3** 다음 옵션을 구성합니다.

- **Name(**이름**)** - 인터페이스의 이름(최대 48자)입니다. 기존 인터페이스의 이름을 변경하면 해당 인터페이스가 포함된 모든 정책 및 개체에서 자동으로 변경됩니다. 이름에 대문자를 사용할 수 없습니다.
- **Status(**상태**)** — Enabled(활성화됨) 위치로 슬라이더를 클릭합니다( ).
- **Description(**설명**)** — (선택 사항). 설명은 줄 바꿈 없이 1줄, 최대 200자로 작성할 수 있습니다.
- **Tunnel ID(**터널 **ID)** — 0~10413 사이의 숫자. 이 번호는 Tunnel이라는 단어에 추가되어 인터페이스의 하드웨어 이름을 구성합니다. 다른 VTI에는 아직 사용하지 않은 번호를 선택해야 합니다. 예를 들어, 인터페이스 Tunnel1을 생성하려면 1을 입력합니다.
- **Tunnel Source(**터널 소스**)** — 이 VTI와 연결된 인터페이스를 선택합니다. 터널 소스는 가상 터널 인터페이스에 정의된 사이트 대 사이트 VPN이 원격 엔드포인트에 연결하는 데 사용하는 인터페이스입니다. 외부 인터페이스와 같이 원격 엔드포인트에 연결할 수 있는 인터페이스를 선택합니다. 소스 인터페이스는 물리적 인터페이스, 하위 인터페이스 또는 Etherchannel일 수 있으며, 이름이 있어야 합니다. BVI(Bridge Virtual Interface)의 멤버일 수는 없습니다.
- **IP Address and Subnet Mask(IP** 주소 및 서브넷 마스크**)** — IPv4 주소 및 관련 서브넷 마스크입니다. 예를 들어 192.168.1.1/24 또는 /255.255.255.0입니다. 이 주소는 터널 소스 인터페이스의 주소와 동일한 서브넷에 있을 필요는 없습니다. 하지만 소스 인터페이스에서 RA(원격 액세스) VPN을 설정하는 경우 VTI IP 주소는 RA VPN에 대해 설정된 주소 풀 내에 있을 수 없습니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

사이트 대 사이트 VPN을 통한 트래픽 허용

다음 기법 중 하나를 사용해 Site-to-Site VPN 터널의 트래픽 흐름을 활성화할 수 있습니다.

- **sysopt connection permit-vpn** 명령을 컨피그레이션합니다. 이 명령에서는 VPN 연결과 일치하는 트래픽을 액세스 제어 정책에서 제외합니다. 이 명령의 기본값은 **no sysopt connection permit-vpn** 입니다. 이는 액세스 제어 정책에서도 VPN 트래픽을 허용해야 한다는 의미입니다.

  이 방법은 외부 사용자가 보호되는 원격 네트워크에서 IP 주소를 스푸핑할 수 없기 때문에 VPN에서 트래픽을 더 안전하게 허용할 수 있습니다. 하지만 VPN 트래픽이 검사되지 않는다는 단점이 있습니다. 즉, 침입 및 파일 보호, URL 필터링 또는 기타 고급 기능이 트래픽에 적용되지 않습니다. 즉 트래픽에 대해 연결 이벤트가 생성되지 않고, 따라서 통계 대시보드에 VPN 연결이 반영되지 않는다는 의미이기도 합니다.

  이 명령을 컨피그레이션하는 더 나은 방법은 원격 액세스 VPN 연결 프로파일을 만들어 여기에서 **Bypass Access Control policy for decrypted traffic(**암호 해독된 트래픽에 대해 액세스 제어 정책 우회**)** 옵션을 선택하는 것입니다. RA VPN을 컨피그레이션하고 싶지 않거나 RA VPN을 컨피그레이션할 수 없는 경우, FlexConfig를 사용해 명령을 컨피그레이션할 수 있습니다.

참고 이 방법은 VTI(Virtual Tunnel Interface)에 구성된 경로 기반 VPN 연결에는 적용되지 않습니다. 항상 경로 기반 VPN에 대한 액세스 제어 규칙을 구성해야 합니다.

- 원격 네트워크에서 연결을 허용하는 액세스 제어 규칙을 생성합니다. 이 방법을 사용하는 경우 VPN 트래픽이 검사되며, 연결에 고급 서비스를 적용할 수 있습니다. 하지만 외부 사용자가 IP 주소를 스푸핑하여 내부 네트워크에 액세스할 가능성이 있다는 단점이 있습니다.

글로벌 IKE 정책 구성

IKE(Internet Key Exchange)는 IPsec 피어를 인증하고, IPsec 암호화 키를 협상 및 배포하고, IPsec SA(보안 연계)를 자동으로 설정하는 데 사용되는 키 관리 프로토콜입니다.

IKE 협상은 2단계로 구성됩니다. 1단계에서는 두 IKE 피어 간의 보안 연계를 협상합니다. 그러면 피어가 2단계에서 안전하게 통신할 수 있습니다. 2단계 협상 중에는 IKE가 IPsec 등의 기타 애플리케이션에 대해 SA를 설정합니다. 두 단계에서는 모두 연결을 협상할 때 제안을 사용합니다. IKE 제안은 두 피어가 상호 간의 IKE 협상을 보호하는 데 사용하는 알고리즘 집합입니다. IKE 협상에서는 두 피어가 먼저 공통(공유) IKE 정책을 합의합니다. 이 정책은 후속 IKE 협상을 보호하는 데 사용되는 보안 파라미터를 제시합니다.

IKE 정책 개체는 이러한 협상을 위한 IKE 제안을 정의합니다. 활성화하는 개체는 피어가 VPN 연결을 협상할 때 사용됩니다. 연결당 서로 다른 IKE 정책을 지정할 수는 없습니다. 각 개체의 상대 우선순위에 따라 이러한 정책 중 먼저 사용을 시도할 정책이 결정되며, 숫자가 작을수록 우선 순위는 높습니다. 협상에서 장애가 발생하여 두 피어가 모두 지원할 수 있는 정책을 찾지 못하면 연결이 설정되지 않습니다.

글로벌 IKE 정책을 정의하려면 각 IKE 버전에 대해 활성화할 개체를 선택합니다. 사전 정의된 개체가 요건을 충족하지 않는 경우 새 정책을 생성하여 보안 정책을 적용합니다.

다음 절차에서는 개체 페이지를 통해 글로벌 정책을 구성하는 방법을 설명합니다. IKE 정책 설정에서 **Edit(**수정**)**을 클릭하여 VPN 연결을 수정할 때 정책을 활성화, 비활성화 및 생성할 수도 있습니다.

참고 최대 20개의 IKE 정책을 활성화할 수 있습니다.

프로시저

단계 **1** 목차에서 **Objects(**개체**)**와 **IKE Policies(IKE** 정책**)**를 차례로 선택합니다.

IKEv1과 IKEv2에 대한 정책이 개별 목록에 표시됩니다.

단계 **2** 각 IKE 버전에 대해 허용할 IKE 정책을 활성화합니다.

a) 개체 테이블 위의 **IKEv1** 또는 **IKEv2**를 선택하여 해당 버전의 정책을 표시합니다.

b) **State(**상태**)** 토글을 클릭하여 적절한 개체를 활성화하고 요건을 충족하지 않는 개체를 비활성화합니다.

보안 요건 중 일부가 기존 개체에 반영되어 있지 않은 경우에는 새 개체를 정의하여 요건을 구현합니다. 자세한 내용은 다음 항목을 참조하십시오.

• IKEv1 정책 구성, 695 페이지
• IKEv2 정책 구성, 697 페이지

c) 상대 우선 순위가 요건과 일치하는지 확인합니다.

정책 우선 순위를 변경해야 하는 경우 정책을 수정합니다. 사전 정의된 시스템 정책의 경우에는 정책의 고유 버전을 생성하여 우선 순위를 변경해야 합니다.

우선 순위는 절대값이 아닌 상대값입니다. 예를 들어 우선 순위 80이 160보다 높습니다. 최고 우선 순위 개체로 80을 활성화하면 해당 정책이 첫 번째로 선택됩니다. 그런 후에 우선 순위가 25인 정책을 활성화하면 해당 정책이 최우선으로 선택됩니다.

d) 두 IKE 버전을 모두 사용하는 경우에는 다른 버전에 대해 프로세스를 반복합니다.

IKEv1 정책 구성

IKE(Internet Key Exchange) 버전 1 정책 개체에는 VPN 연결을 정의할 때 IKEv1 정책에 필요한 파라미터가 포함되어 있습니다. IKE는 IPsec 기반 통신을 쉽게 관리할 수 있도록 하는 키 관리 프로토콜이며 IPsec 피어를 인증하고, IPsec 암호화 키를 협상 및 배포하고, IPsec SA(보안 연계)를 자동으로 설정하는 데 사용됩니다.

여러 가지 사전 정의된 IKEv1 정책이 있습니다. 필요에 맞는 정책이 있으면 **State(**상태**)** 토글을 클릭하여 활성화하면 됩니다. 새 정책을 생성하여 다른 보안 설정 조합을 구현할 수도 있습니다. 시스템 정의 개체는 수정하거나 삭제할 수 없습니다.

다음 절차에서는 개체 페이지를 통해 개체를 직접 생성하고 수정할 수 있는 방법을 설명합니다. 개체 목록에 표시되는 **Create New IKE Policy(**새 **IKE** 정책 생성**)** 링크를 클릭하여 VPN 연결에서 IKEv1 설정을 수정하면서 IKEv1 정책 개체를 생성할 수도 있습니다.

프로시저

단계 **1** 목차에서 **Objects(**개체**)**와 **IKE Policies(IKE** 정책**)**를 차례로 선택합니다.

단계 **2** 개체 테이블 위의 **IKEv1**을 선택하여 IKEv1 정책을 표시합니다.

단계 **3** 요구사항에 맞는 시스템 정의 정책이 있으면 **State(**상태**)** 토글을 클릭하여 활성화합니다.

원치 않는 정책을 비활성화할 때도 **State(**상태**)** 토글을 사용합니다. 상대 우선 순위에 따라 이러한 정책 중 먼저 사용을 시도할 정책이 결정되며, 숫자가 작을수록 우선 순위가 높습니다.

단계 **4** 다음 중 하나를 수행합니다.

- 개체를 생성하려면 + 버튼을 클릭합니다.
- 개체를 수정하려면 개체의 수정 아이콘( )을 클릭하십시오.

참조되지 않는 개체를 삭제하려면 해당 개체의 휴지통 아이콘( )을 클릭합니다.

단계 **5** IKEv1 속성을 구성합니다.

- **Priority(**우선순위**)** - IKE 정책의 상대 우선 순위는 1~65,535입니다. 우선 순위에 따라 일반 SA(보안 연계) 찾기를 시도할 때 두 협상 피어가 비교하는 IKE 정책의 순서가 결정됩니다. 원격 IPsec 피어는 최고 우선 순위 정책에서 선택한 파라미터를 지원하지 않는 경우 그 다음 우선 순위에 정의된 파라미터 사용을 시도합니다. 번호가 낮을수록 우선 순위가 높습니다.
- **Name(**이름**)** - 개체의 이름(최대 128자)입니다.
- **State(**상태**)** - IKE 정책이 활성화되어 있는지 여부입니다. 토글을 클릭하여 상태를 변경합니다. IKE 협상 중에는 활성화된 정책만 사용됩니다.
- **Authentication(**인증**)** - 두 피어 간에 사용할 인증 방법입니다. 자세한 내용은 사용할 인증 방법 결정, 683 페이지의 내용을 참조하십시오.
  - **Preshared Key(**사전 공유 키**)** - 각 디바이스에 정의된 사전 공유 키를 사용합니다. 이 키를 사용하면 보안 키를 두 피어 간에 공유할 수 있으며 인증 단계 수행 시 IKE에서 보안 키를 사용할 수 있습니다. 동일한 사전 공유 키를 사용하여 피어를 구성하지 않으면 IKE SA를 설정할 수 없습니다.
  - **Certificate(**인증서**)** - 서로 식별할 피어에 대해 디바이스 ID 인증서를 사용합니다. Certificate Authority에서 각 피어를 등록하여 이 인증서를 가져와야 합니다. 또한 각 피어에서 ID 인증서 서명에 사용되는 신뢰할 수 있는 CA 루트 및 중간 CA 인증서를 업로드해야 합니다. 피어

는 동일한 또는 다른 CA에 등록할 수 있습니다. 어느 피어든 간에 SSC(자가서명 인증서)를 사용할 수 없습니다.

- **Encryption(**암호화**)** - 2단계 협상 보호를 위한 1단계 SA(보안 연계)를 설정하는 데 사용되는 암호화 알고리즘입니다. 옵션에 대한 설명은 사용할 암호화 알고리즘 결정, 681 페이지를 참조하십시오.
- **Diffie-Hellman Group(Diffie-Hellman** 그룹**)** - 공유 암호를 각 IPsec 피어에 전송하지 않고 두 IPsec 피어 간에 파생하는 데 사용할 Diffie Hellman 그룹입니다. 대형 모듈러스는 보안성은 더 높지만, 처리 시간이 더 오래 걸립니다. 두 피어의 모듈러스 그룹이 일치해야 합니다. 옵션에 대한 설명은 사용할 Diffie-Hellman 모듈러스 그룹 결정, 682 페이지를 참조하십시오.
- **Hash(**해시**)** - 메시지 무결성을 보장하는 데 사용되는 메시지 다이제스트를 생성하기 위한 해시 알고리즘입니다. 옵션에 대한 설명은 사용할 해시 알고리즘 결정, 682 페이지를 참조하십시오.
- **Lifetime(**수명 주기**)** - SA(보안 연결)의 라이프타임(초)으로, 120~2147483647의 값이거나 비어 있습니다. 라이프타임이 초과되면 SA는 만료되며 두 피어 간에 SA를 재협상해야 합니다. 일반적으로 특정 지점까지는 라이프타임이 짧을수록 IKE 협상이 보다 안전합니다. 그러나 라이프타임이 길면 라이프타임이 짧은 경우에 비해 이후 IPsec 보안 연계를 더 빠르게 설정할 수 있습니다. 기본값은 86400입니다. 무제한 라이프타임을 지정하려면 아무 값도 입력하지 않고 필드를 비워 둡니다.

단계 **6** **OK(**확인**)**를 클릭하여 변경 사항을 저장합니다.

IKEv2 정책 구성

IKE(Internet Key Exchange) 버전 2 정책 개체에는 VPN 연결을 정의할 때 IKEv2 정책에 필요한 파라미터가 포함되어 있습니다. IKE는 IPsec 기반 통신을 쉽게 관리할 수 있도록 하는 키 관리 프로토콜이며 IPsec 피어를 인증하고, IPsec 암호화 키를 협상 및 배포하고, IPsec SA(보안 연계)를 자동으로 설정하는 데 사용됩니다.

여러 가지 사전 정의된 IKEv2 정책이 있습니다. 필요에 맞는 정책이 있으면 **State(**상태**)** 토글을 클릭하여 활성화하면 됩니다. 새 정책을 생성하여 다른 보안 설정 조합을 구현할 수도 있습니다. 시스템 정의 개체는 수정하거나 삭제할 수 없습니다.

다음 절차에서는 개체 페이지를 통해 개체를 직접 생성하고 수정할 수 있는 방법을 설명합니다. 개체 목록에 표시되는 **Create New IKE Policy(**새 **IKE** 정책 생성**)** 링크를 클릭하여 VPN 연결에서 IKEv2 설정을 수정하면서 IKEv2 정책 개체를 생성할 수도 있습니다.

프로시저

단계 **1** 목차에서 **Objects(**개체**)**와 **IKE Policies(IKE** 정책**)**를 차례로 선택합니다.

단계 **2** 개체 테이블 위의 **IKEv2**를 선택하여 IKEv2 정책을 표시합니다.

단계 **3** 요구사항에 맞는 시스템 정의 정책이 있으면 **State(**상태**)** 토글을 클릭하여 활성화합니다.

원치 않는 정책을 비활성화할 때도 **State(**상태**)** 토글을 사용합니다. 상대 우선 순위에 따라 이러한 정책 중 먼저 사용을 시도할 정책이 결정되며, 숫자가 작을수록 우선 순위가 높습니다.

단계 **4** 다음 중 하나를 수행합니다.

- 개체를 생성하려면 **+** 버튼을 클릭합니다.
- 개체를 수정하려면 개체의 수정 아이콘()을 클릭하십시오.

참조되지 않는 개체를 삭제하려면 해당 개체의 휴지통 아이콘()을 클릭합니다.

단계 **5** IKEv2 속성을 구성합니다.

- **Priority(**우선순위**)** - IKE 정책의 상대 우선 순위는 1~65,535입니다. 우선 순위에 따라 일반 SA(보안 연계) 찾기를 시도할 때 두 협상 피어가 비교하는 IKE 정책의 순서가 결정됩니다. 원격 IPsec 피어는 최고 우선 순위 정책에서 선택한 파라미터를 지원하지 않는 경우 그 다음 우선 순위에 정의된 파라미터 사용을 시도합니다. 번호가 낮을수록 우선 순위가 높습니다.
- **Name(**이름**)** - 개체의 이름(최대 128자)입니다.
- **State(**상태**)** - IKE 정책이 활성화되어 있는지 여부입니다. 토글을 클릭하여 상태를 변경합니다. IKE 협상 중에는 활성화된 정책만 사용됩니다.
- **Encryption(**암호화**)** - 2단계 협상 보호를 위한 1단계 SA(보안 연계)를 설정하는 데 사용되는 암호화 알고리즘입니다. 허용하려는 모든 알고리즘을 선택합니다. 단, 같은 정책에 혼합 모드(AES-GCM) 및 일반 모드 옵션을 둘 다 포함할 수는 없습니다. 일반 모드에서는 무결성 해시를 선택해야 하는 반면 혼합 모드에서는 개별 무결성 해시 선택이 금지됩니다. 시스템은 일치하는 항목이 합의될 때까지 가장 강력한 알고리즘에서 가장 취약한 알고리즘 순서대로 피어와 협상을 합니다. 옵션에 대한 설명은 사용할 암호화 알고리즘 결정, 681 페이지를 참조하십시오.
- **Diffie-Hellman Group(Diffie-Hellman** 그룹**)** - 공유 암호를 각 IPsec 피어에 전송하지 않고 두 IPsec 피어 간에 파생하는 데 사용할 Diffie Hellman 그룹입니다. 대형 모듈러스는 보안성은 더 높지만, 처리 시간이 더 오래 걸립니다. 두 피어의 모듈러스 그룹이 일치해야 합니다. 허용하려는 모든 알고리즘을 선택합니다. 시스템은 일치하는 항목이 합의될 때까지 가장 강력한 그룹에서 가장 취약한 그룹 순서대로 피어와 협상을 합니다. 옵션에 대한 설명은 사용할 Diffie-Hellman 모듈러스 그룹 결정, 682 페이지를 참조하십시오.
- **Integrity Hash(**무결성 해시**)** - 메시지 무결성을 보장하는 데 사용되는 메시지 다이제스트를 생성하기 위한 해시 알고리즘의 무결성 부분입니다. 허용하려는 모든 알고리즘을 선택합니다. 시스템은 일치하는 항목이 합의될 때까지 가장 강력한 알고리즘에서 가장 취약한 알고리즘 순서대로 피어와 협상을 합니다. AES-GCM 암호화 옵션에서는 무결성 해시가 사용되지 않습니다. 옵션에 대한 설명은 사용할 해시 알고리즘 결정, 682 페이지를 참조하십시오.
- **PRF(Pseudo Random Function)** 해시 - 해시 알고리즘의 PRF(Pseudo Random Function) 부분으로, IKEv2 터널 암호화에 필요한 키 요소 및 해싱 작업을 파생시키기 위해 알고리즘으로 사용됩니다. IKEv1에서는 무결성 및 PRF 알고리즘이 구분되지 않지만 IKEv2에서는 이러한 요소에 대해 서로 다른 알고리즘을 지정할 수 있습니다. 허용하려는 모든 알고리즘을 선택합니다. 시스템은 일치하는 항목이 합의될 때까지 가장 강력한 알고리즘에서 가장 취약한 알고리즘 순서대로 피어와 협상을 합니다. 옵션에 대한 설명은 사용할 해시 알고리즘 결정, 682 페이지를 참조하십시오.

- **Lifetime(**수명 주기**)** - SA(보안 연결)의 라이프타임(초)으로, 120~2147483647의 값이거나 비어 있습니다. 라이프타임이 초과되면 SA는 만료되며 두 피어 간에 SA를 재협상해야 합니다. 일반적으로 특정 지점까지는 라이프타임이 짧을수록 IKE 협상이 보다 안전합니다. 그러나 라이프타임이 길면 라이프타임이 짧은 경우에 비해 이후 IPsec 보안 연계를 더 빠르게 설정할 수 있습니다. 기본값은 86400입니다. 무제한 라이프타임을 지정하려면 아무 값도 입력하지 않고 필드를 비워 둡니다.

단계 **6** **OK(**확인**)**를 클릭하여 변경 사항을 저장합니다.

IPsec 제안 구성

IPsec는 가장 안전하게 VPN 설정을 하는 방법 중 하나입니다. IPsec는 IP 패킷 레벨에서 데이터 암호화 기능을 제공하는 강력한 표준 기반 솔루션입니다. IPsec를 사용하는 경우 데이터는 터널을 통해 공용 네트워크를 사용하여 전송됩니다. 터널은 두 피어 간의 안전한 논리적 통신 경로입니다. IPsec 터널로 진입하는 트래픽은 보안 프로토콜 및 알고리즘이 조합된 변환 집합에 의해 보호됩니다. IPsec 보안 연계(SA) 협상 중에 피어는 두 피어에서 동일한 변환 집합을 검색합니다.

IKE 버전(IKEv1 또는 IKEv2)에 따라 각기 다른 IPsec 제안 개체가 있습니다.

- IKEv1 IPsec 제안을 생성할 때는 IPsec가 동작하는 모드를 선택하고 필요한 암호화 및 인증 유형을 정의합니다. 알고리즘에 대해서는 단일 옵션을 선택할 수 있습니다. VPN에서 여러 조합을 지원하려면 여러 IKEv1 IPsec 제안 개체를 생성하여 선택합니다.
- IKEv2 IPsec 제안을 생성할 때는 VPN에서 허용되는 모든 암호화 및 해시 알고리즘을 선택할 수 있습니다. 시스템은 가장 안전한 항목부터 가장 안전하지 않은 항목 순으로 설정 순서를 지정하고 일치하는 항목을 찾을 때까지 피어와 협상합니다. 이를 통해 IKEv1과 마찬가지로 허용된 각 조합을 개별적으로 전송하는 대신 모든 허용된 조합을 전달하는 단일 제안서를 보낼 수 있습니다.

IKEv1 및 IKEv2 IPsec 제안에는 모두 ESP(Encapsulating Security Protocol)가 사용됩니다. ESP는 인증, 암호화 및 재생 방지 서비스를 제공합니다. ESP는 IP 프로토콜 유형 50입니다.

참고 IPsec 터널에서는 암호화 및 인증을 모두 사용하는 것이 좋습니다.

다음 항목에서는 각 IKE 버전에 대해 IPsec 제안을 구성하는 방법을 설명합니다.

IKEv1용 IPsec 제안 구성

IKEv1 IPsec 제안 개체를 사용하여 IKE 2단계 협상 시 사용되는 IPsec 제안을 구성합니다. IPsec 제안은 IPsec 터널에서 트래픽을 보호하는 보안 프로토콜 및 알고리즘 조합을 정의합니다.

여러 가지 사전 정의된 IKEv1 IPsec 제안이 있습니다. 새 제안을 생성하여 다른 보안 설정 조합을 구현할 수도 있습니다. 시스템 정의 개체는 수정하거나 삭제할 수 없습니다.

다음 절차에서는 개체 페이지를 통해 개체를 직접 생성하고 수정할 수 있는 방법을 설명합니다. 개체 목록에 표시되는 **Create New IPsec Proposal(**새 **IPsec** 제안 생성**)** 링크를 클릭하여 VPN 연결에서 IKEv1 IPsec 설정을 수정하면서 IKEv1 IPsec 제안 개체를 생성할 수도 있습니다.

프로시저

단계 **1** 목차에서 **Objects(**개체**)**와 **IPsec Proposals(IPsec** 제안**)**를 차례로 선택합니다.

단계 **2** 개체 테이블 위의 **IKEv1**을 선택하여 IKEv1 IPsec 제안을 표시합니다.

단계 **3** 다음 중 하나를 수행합니다.

- 개체를 생성하려면 **+** 버튼을 클릭합니다.
- 개체를 수정하려면 개체의 수정 아이콘()을 클릭하십시오.

참조되지 않는 개체를 삭제하려면 해당 개체의 휴지통 아이콘()을 클릭합니다.

단계 **4** IKEv1 IPsec 제안 속성을 구성합니다.

- **Name(**이름**)** - 개체의 이름(최대 128자)입니다.
- **Mode(**모드**)** - IPSec 터널이 작동하는 모드입니다.
  - 터널 모드에서는 전체 IP 패킷이 캡슐화됩니다. IPSec 헤더는 원본 IP 헤더와 새 IP 헤더 사이에 추가됩니다. 이는 기본값입니다. 방화벽 뒤에 배치되어 있는 호스트와 주고받는 트래픽을 방화벽이 보호하는 경우 터널 모드를 사용합니다. 터널 모드는 인터넷 등의 신뢰할 수 없는 네트워크를 통해 연결하는 두 방화벽 또는 기타 보안 게이트웨이 간에 일반 IPsec가 구현되는 통상적인 방식입니다.
  - 전송 모드에서는 IP 패킷의 상위 레이어 프로토콜만 캡슐화됩니다. IPSec 헤더는 TCP 등의 상위 계층 프로토콜 헤더와 IP 헤더 사이에 삽입됩니다. 전송 모드에서는 소스 호스트와 대상 호스트가 모두 IPsec를 지원해야 합니다. 터널의 대상 피어가 IP 패킷의 최종 대상인 경우에만 전송 모드를 사용할 수 있습니다. 전송 모드는 대개 GRE, L2TP, DLSW 등의 레이어 2 또는 레이어 3 터널링 프로토콜을 보호할 때만 사용됩니다.
- **ESP Encryption(ESP** 암호화**)** - 이 제안에 대한 ESP(Encapsulating Security Protocol) 암호화 알고리즘입니다. 옵션에 대한 설명은 사용할 암호화 알고리즘 결정, 681 페이지를 참조하십시오.
- **ESP Hash(ESP** 해시**)** - 인증에 사용할 해시 또는 무결성 알고리즘입니다. 옵션에 대한 설명은 사용할 해시 알고리즘 결정, 682 페이지를 참조하십시오.

단계 **5** **OK(**확인**)**를 클릭하여 변경 사항을 저장합니다.

IKEv2용 IPsec 제안 구성

IKEv2 IPsec 제안 개체를 사용하여 IKE 2단계 협상 시 사용되는 IPsec 제안을 구성합니다. IPsec 제안은 IPsec 터널에서 트래픽을 보호하는 보안 프로토콜 및 알고리즘 조합을 정의합니다.

여러 가지 사전 정의된 IKEv2 IPsec 제안이 있습니다. 새 제안을 생성하여 다른 보안 설정 조합을 구현할 수도 있습니다. 시스템 정의 개체는 수정하거나 삭제할 수 없습니다.

다음 절차에서는 개체 페이지를 통해 개체를 직접 생성하고 수정할 수 있는 방법을 설명합니다. 개체 목록에 표시되는 **Create New IPsec Proposal(**새 **IPsec** 제안 생성**)** 링크를 클릭하여 VPN 연결에서 IKEv2 IPsec 설정을 수정하면서 IKEv2 IPsec 제안 개체를 생성할 수도 있습니다.

프로시저

단계 **1** 목차에서 **Objects(**개체**)**와 **IPsec Proposals(IPsec** 제안**)**를 차례로 선택합니다.

단계 **2** 개체 테이블 위의 **IKEv2**를 선택하여 IKEv2 IPsec 제안을 표시합니다.

단계 **3** 다음 중 하나를 수행합니다.

- 개체를 생성하려면 **+** 버튼을 클릭합니다.
- 개체를 수정하려면 개체의 수정 아이콘( )을 클릭하십시오.

참조되지 않는 개체를 삭제하려면 해당 개체의 휴지통 아이콘( )을 클릭합니다.

단계 **4** IKEv2 IPsec 제안 속성을 구성합니다.

- **Name(**이름**)** - 개체의 이름(최대 128자)입니다.
- **Encryption(**암호화**)** - 이 제안에 대한 ESP(Encapsulating Security Protocol) 암호화 알고리즘입니다. 허용하려는 모든 알고리즘을 선택합니다. 시스템은 일치하는 항목이 합의될 때까지 가장 강력한 알고리즘에서 가장 취약한 알고리즘 순서대로 피어와 협상을 합니다. 옵션에 대한 설명은 사용할 암호화 알고리즘 결정, 681 페이지를 참조하십시오.
- **Integrity Hash(**무결성 해시**)** - 인증에 사용할 해시 또는 무결성 알고리즘입니다. 허용하려는 모든 알고리즘을 선택합니다. 시스템은 일치하는 항목이 합의될 때까지 가장 강력한 알고리즘에서 가장 취약한 알고리즘 순서대로 피어와 협상을 합니다. 옵션에 대한 설명은 사용할 해시 알고리즘 결정, 682 페이지를 참조하십시오.

  참고 암호화 알고리즘으로 AES-GCM/GMAC 옵션 중 하나를 선택하는 경우에는 null 무결성 알고리즘을 선택해야 합니다. null이 아닌 옵션을 선택하더라도 이러한 암호화 표준은 무결성 해시를 사용하지 않습니다.

단계 **5** **OK(**확인**)**를 클릭하여 변경 사항을 저장합니다.

사이트 대 사이트 VPN 연결 확인

사이트 대 사이트 VPN 연결을 구성하고 디바이스에 컨피그레이션을 구축한 후에는 시스템이 원격 디바이스와 보안 연결을 설정했는지 확인합니다.

연결을 설정할 수 없는 경우, 디바이스 CLI에서 **ping interface***interface_name remote_ip_address* 명령을 사용하여 VPN 인터페이스를 경유해 원격 디바이스에 이르는 경로가 있는지 확인합니다. 컨피그

레이션된 인터페이스를 경유하는 연결이 없는 경우, **interface** *interface_name* 키워드를 중단하고 연결이 다른 인터페이스를 경유하는지 확인합니다. 연결에 잘못된 인터페이스를 연결했을 가능성이 있습니다. 보호되는 네트워크를 향한 네트워크가 아닌, 원격 디바이스를 향하는 인터페이스를 선택해야 합니다.

네트워크 경로가 있을 경우, 두 엔드포인트에서 지원하는 IKE 버전 및 키를 확인하고 필요한 경우 VPN 연결을 조정합니다. 액세스 제어 또는 NAT 규칙이 연결을 차단하고 있지 않은지 확인합니다.

프로시저

단계 **1** CLI(Command Line Interface) 로그인, 6 페이지에 설명된 대로 디바이스 CLI에 로그인합니다.

단계 **2** **show ipsec sa** 명령을 사용해 IPsec 보안 연결이 설정되어 있는지 확인합니다.

디바이스(**local addr**)와 원격 피어(**current_peer**) 사이에 VPN 연결이 설정되었는지 확인해야 합니다. 연결을 통해 트래픽을 전송할 때 패킷(pkts) 수가 증가해야 합니다. 액세스 목록에는 연결의 로컬 및 원격 네트워크가 표시되어야 합니다.

예를 들어 다음 출력은 IKEv2 연결을 표시합니다.

```
> show ipsec sa
interface: site-a-outside
    Crypto map tag: s2sCryptoMap, seq num: 1, local addr: 192.168.2.15

      access-list |s2sAcl|0730e31c-1e5f-11e7-899f-27f6e1030344
extended permit ip 192.168.1.0 255.255.255.0 192.168.3.0 255.255.255.0
      local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
      current_peer: 192.168.4.6


      #pkts encaps: 69, #pkts encrypt: 69, #pkts digest: 69
      #pkts decaps: 69, #pkts decrypt: 69, #pkts verify: 69
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 69, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 192.168.2.15/500, remote crypto endpt.: 192.168.4.6/500
      path mtu 1500, ipsec overhead 55(36), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: CD22739C
      current inbound spi : 52D2F1E4

    inbound esp sas:
      spi: 0x52D2F1E4 (1389556196)
         SA State: active
         transform: esp-aes-gcm-256 esp-null-hmac no compression
         in use settings ={L2L, Tunnel, PFS Group 19, IKEv2, }
         slot: 0, conn_id: 62738432, crypto-map: s2sCryptoMap
         sa timing: remaining key lifetime (kB/sec): (4285434/28730)
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
```

```
        0xFFFFFFFF 0xFFFFFFFF
    outbound esp sas:
      spi: 0xCD22739C (3441587100)
         SA State: active
         transform: esp-aes-gcm-256 esp-null-hmac no compression
         in use settings ={L2L, Tunnel, PFS Group 19, IKEv2, }
         slot: 0, conn_id: 62738432, crypto-map: s2sCryptoMap
         sa timing: remaining key lifetime (kB/sec): (4055034/28730)
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```

다음 출력은 IKEv1 연결을 표시합니다.

```
> show ipsec sa
interface: site-a-outside
    Crypto map tag: s2sCryptoMap, seq num: 1, local addr: 192.168.2.15

      access-list |s2sAcl|0730e31c-1e5f-11e7-899f-27f6e1030344
extended permit ip 192.168.1.0 255.255.255.0 192.168.3.0 255.255.255.0
      local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
      current_peer: 192.168.4.6


      #pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
      #pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 10, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 192.168.2.15/0, remote crypto endpt.: 192.168.4.6/0
      path mtu 1500, ipsec overhead 74(44), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: 077D72C9
      current inbound spi : AC146DEC

    inbound esp sas:
      spi: 0xAC146DEC (2887020012)
         SA State: active
         transform: esp-aes-256 esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, PFS Group 5, IKEv1, }
         slot: 0, conn_id: 143065088, crypto-map: s2sCryptoMap
         sa timing: remaining key lifetime (kB/sec): (3914999/28567)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x000007FF
    outbound esp sas:
      spi: 0x077D72C9 (125661897)
         SA State: active
         transform: esp-aes-256 esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, PFS Group 5, IKEv1, }
         slot: 0, conn_id: 143065088, crypto-map: s2sCryptoMap
         sa timing: remaining key lifetime (kB/sec): (3914999/28567)
         IV size: 16 bytes
         replay detection support: Y
```

```
        Anti replay bitmap:
         0x00000000 0x00000001
```

단계 **3** **show isakmp sa** 명령을 사용해 IKE 보안 연결을 확인합니다.

sa 키워드 없이 명령을 사용하거나 **stats** 키워드를 대신 사용하여 IKE 통계를 볼 수 있습니다.

예를 들어 다음 출력은 IKEv2 보안 연결을 표시합니다.

```
> show isakmp sa

There are no IKEv1 SAs

IKEv2 SAs:

Session-id:15317, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local             Remote            Status   Role
592216161 192.168.2.15/500  192.168.4.6/500   READY    INITIATOR
      Encr: AES-GCM, keysize: 256, Hash: N/A, DH Grp:21, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/12 sec
Child sa: local selector  192.168.1.0/0 - 192.168.1.255/65535
          remote selector 192.168.3.0/0 - 192.168.3.255/65535
          ESP spi in/out: 0x52d2f1e4/0xcd22739c
```

다음 출력은 IKEv1 보안 연결을 표시합니다.

```
> show isakmp sa

IKEv1 SAs:

   Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 192.168.4.6
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_ACTIVE

There are no IKEv2 SAs
```

사이트 대 사이트 VPN 모니터링

사이트 대 사이트 VPN 연결을 모니터링하고 트러블슈팅하려면 CLI 콘솔을 열거나 디바이스 CLI에 로그인하여 다음 명령을 사용합니다.

- **show ipsec sa** VPN 세션(보안 연결)을 표시합니다. **clear ipsec sa counters** 명령을 사용하여 이 통계를 재설정할 수 있습니다.
- **show ipsec** *keyword* IPsec 운영 데이터 및 통계가 표시됩니다. 사용 가능한 키워드를 보려면 **show ipsec ?**를 입력합니다.

- **show isakmp** ISAKMP 운영 데이터 및 통계를 표시합니다.

사이트 대 사이트 VPN의 예시

다음에는 사이트 대 사이트 VPN을 구성하는 예시가 나와 있습니다.

NAT에서 사이트 대 사이트 VPN 트래픽 제외

인터페이스에 사이트 대 사이트 VPN 연결이 정의되어 있고 해당 인터페이스에 대한 NAT 규칙도 있는 경우 NAT 규칙에서 VPN의 트래픽을 선택적으로 제외할 수 있습니다. VPN 연결의 원격 쪽에서 내부 주소를 처리할 수 있는 경우 이러한 VPN 트래픽을 제외할 수 있습니다.

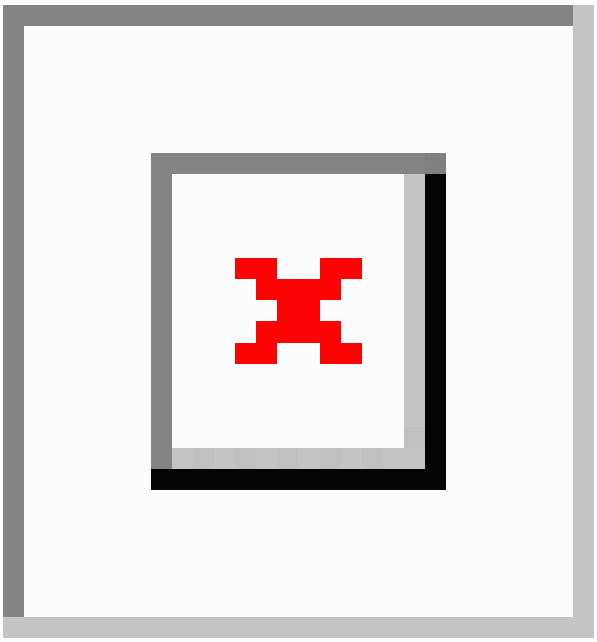
VPN 연결을 생성할 때 **NAT Exempt(NAT** 제외**)** 옵션을 선택하여 규칙을 자동으로 생성할 수 있습니다. 그러나 브리지 그룹 멤버가 아닌 단일 라우팅 인터페이스를 통해 보호된 로컬 네트워크에 연결하는 경우에만 이 방법을 사용할 수 있습니다. 그렇지 않고 연결의 로컬 네트워크가 둘 이상의 라우팅 인터페이스 또는 하나 이상의 브리지 그룹 멤버에 있는 경우에는 NAT 제외 규칙을 수동으로 구성해야 합니다.

NAT 규칙에서 VPN 트래픽을 제외하려면 대상이 원격 네트워크일 때 로컬 트래픽에 대한 ID 수동 NAT 규칙을 생성합니다. 그런 다음 대상이 인터넷 등의 다른 항목일 때 트래픽에 NAT를 적용합니다. 로컬 네트워크의 인터페이스가 여러 개인 경우 각 인터페이스에 대해 규칙을 생성합니다. 또한 다음과 같은 제안 사항을 고려합니다.

- 연결에 로컬 네트워크가 여러 개 있으면 네트워크를 정의하는 개체를 포함할 네트워크 개체 그룹을 생성합니다.
- VPN에 IPv4 및 IPv6 네트워크를 둘 다 포함하는 경우 각 네트워크에 대해 별도의 ID NAT 규칙을 생성합니다.

볼더 사무실과 산호세 사무실을 연결하는 사이트 대 사이트 터널을 보여주는 다음 예를 살펴보십시오. 인터넷으로 이동할 트래픽(예: 볼더의 10.1.1.6에서 www.example.com으로)의 경우 인터넷 액세스를 위해 NAT에서 제공하는 공용 IP 주소가 필요합니다. 아래의 예에서는 인터페이스 PAT 규칙을 사용합니다. 그러나 VPN 터널을 지나갈 트래픽(예: 볼더의 10.1.1.6에서 산호세의 10.2.2.78로)에 대해서는 NAT를 수행하지 않으려고 합니다. 그렇게 하려면 ID NAT 규칙을 만들어 해당 트래픽을 제외해야 합니다. ID NAT는 단순히 주소를 동일한 주소로 변환합니다.

그림 49: 사이트 대 사이트 VPN을 위한 인터페이스 PAT 및 ID NAT



다음 예에서는 방화벽1(볼더)의 컨피그레이션에 대해 설명합니다. 이 예에서는 내부 인터페이스가 브리지 그룹이라고 가정하므로 각 멤버 인터페이스에 대해 규칙을 작성해야 합니다. 라우팅 내부 인터페이스가 하나이든 여러 개이든 프로세스는 동일합니다.

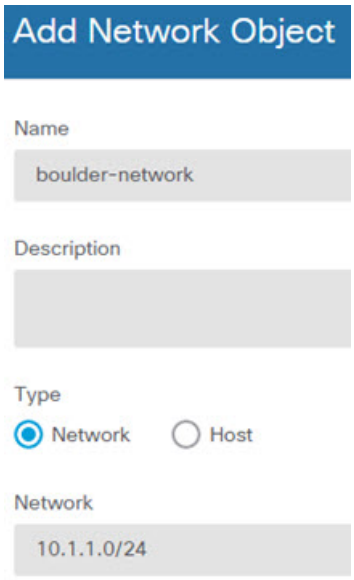
참고 이 예에서는 IPv4만 사용한다고 가정합니다. VPN에 IPv6 네트워크도 포함되어 있으면 IPv6용 병렬 규칙을 생성합니다. IPv6 인터페이스 PAT를 구현할 수는 없으므로 PAT에 사용할 고유 IPv6 주소가 포함된 호스트 개체를 생성해야 합니다.

프로시저

단계 1 여러 네트워크를 정의하기 위한 개체를 생성합니다.

a) **Objects(**개체**)**를 선택합니다.
b) 목차에서 **Network(**네트워크**)**를 선택하고 +를 클릭합니다.
c) 볼더 내부 네트워크를 확인합니다.

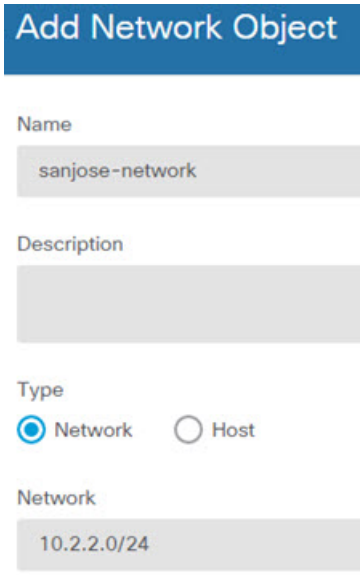
네트워크 개체의 이름을 boulder-network와 같이 지정하고 **Network(**네트워크**)**를 선택한 후에 네트워크 주소 10.1.1.0/24를 입력합니다.



d) **OK(**확인**)**를 클릭합니다.

e) +를 클릭하여 내부 산호세 네트워크를 정의합니다.

네트워크 개체의 이름을 sanjose-network와 같이 지정하고 **Network(**네트워크**)**를 선택한 후에 네트워크 주소 10.2.2.0/24를 입력합니다.



f) **OK(**확인**)**를 클릭합니다.

단계 **2** 방화벽1(볼더)에서 VPN을 통해 산호세로 이동할 때 볼더 네트워크용 수동 ID NAT를 구성합니다.

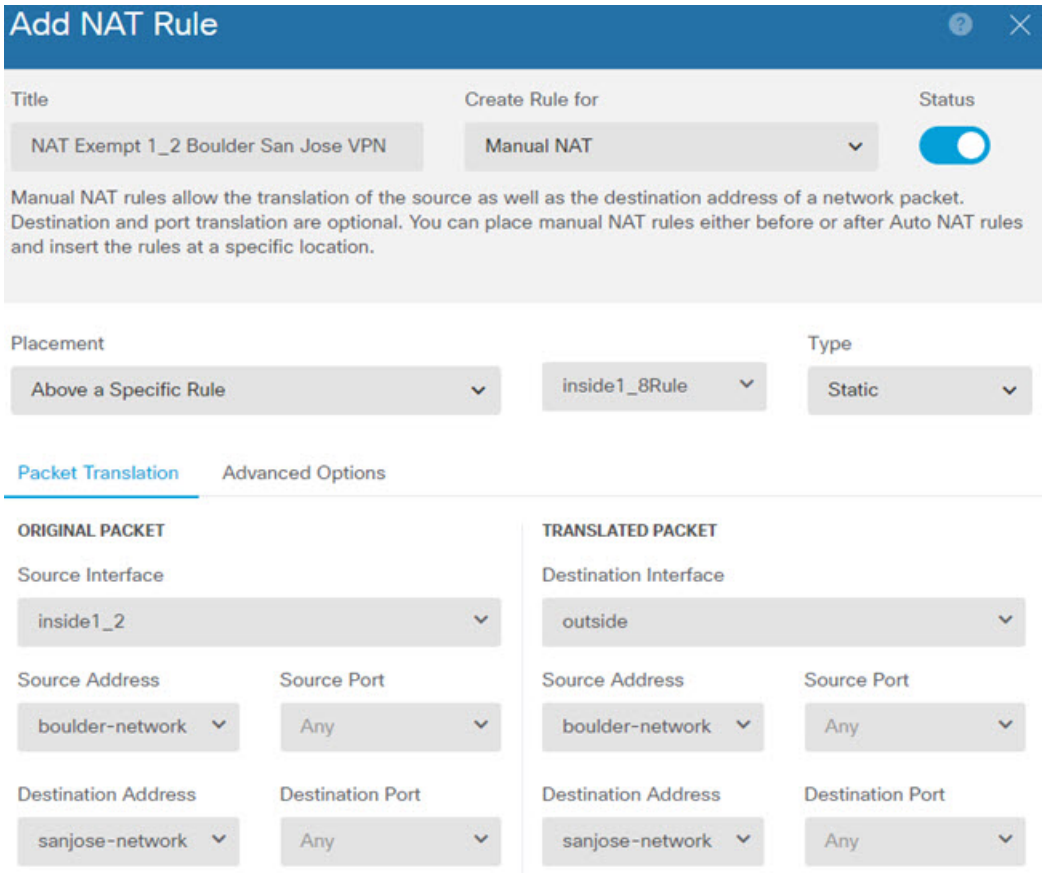
a) **Policies(**정책**)** > **NAT**를 선택합니다.

b) + 버튼을 클릭합니다.

c) 다음 속성을 구성합니다.

- **Title(**제목**)** = NAT Exempt 1_2 Boulder San Jose VPN 또는 원하는 다른 이름
- **Create Rule For(**규칙 생성**)** = 수동 NAT
- **Placement(**배치**)** = 특정 규칙 위를 선택하고 자동 NAT 앞의 수동 NAT 섹션에서 첫 번째 규칙을 선택합니다. 대상 인터페이스의 모든 일반 인터페이스 PAT 규칙 앞에 이 규칙을 배치해야 합니다. 그렇지 않으면 규칙이 적절한 트래픽에 적용되지 않을 수 있습니다.
- **Type(**유형**)** = 고정
- **Source Interface(**소스 인터페이스**)** = inside1_2
- **Destination Interface(**대상 인터페이스**)** = outside
- **Original Source Address(**원본 소스 주소**)** = boulder-network 네트워크 개체
- **Translated Source Address(**변환된 소스 주소**)** = boulder-network 네트워크 개체
- **Original Destination Address(**원본 대상 주소**)** = sanjose-network 네트워크 개체
- **Translated Destination Address(**변환된 대상 주소**)** = sanjose-network 네트워크 개체

  참고 대상 주소를 변환하지 않을 것이기 때문에 원본 주소 및 변환된 대상 주소에 대해 동일한 주소를 지정하여 대상 주소에 대한 ID NAT를 구성해야 합니다. 포트 필드는 모두 비워 둡니다. 이 규칙은 소스 및 대상 둘 다에 대해 ID NAT를 구성합니다.



d) **Advanced(**고급**)** 탭에서 **Do not proxy ARP on Destination interface(**대상 인터페이스에서 **ARP** 프록시 설정 안 함**)**를 선택합니다.

e) **OK(**확인**)**를 클릭합니다.

f) 이 프로세스를 반복하여 각각의 기타 내부 인터페이스에 대해 동일 규칙을 생성합니다.

단계 **3** 방화벽1(볼더)에서 내부 볼더 네트워크에 대해 인터넷으로 이동할 때 수동 동적 인터페이스 PAT를 구성합니다.

참고 모든 IPv4 트래픽에 적용되는 내부 인터페이스용 동적 인터페이스 PAT 규칙은 이미 있을 수 있습니다. 이러한 규칙은 초기 컨피그레이션 중에 기본적으로 생성되기 때문입니다. 그러나 여기서는 완전한 설명을 위해 컨피그레이션을 제공합니다. 이러한 단계를 완료하기 전에 내부 인터페이스와 네트워크에 적용되는 규칙이 이미 있는지 확인하고 해당 규칙이 있으면 이 단계를 건너뜁니다.

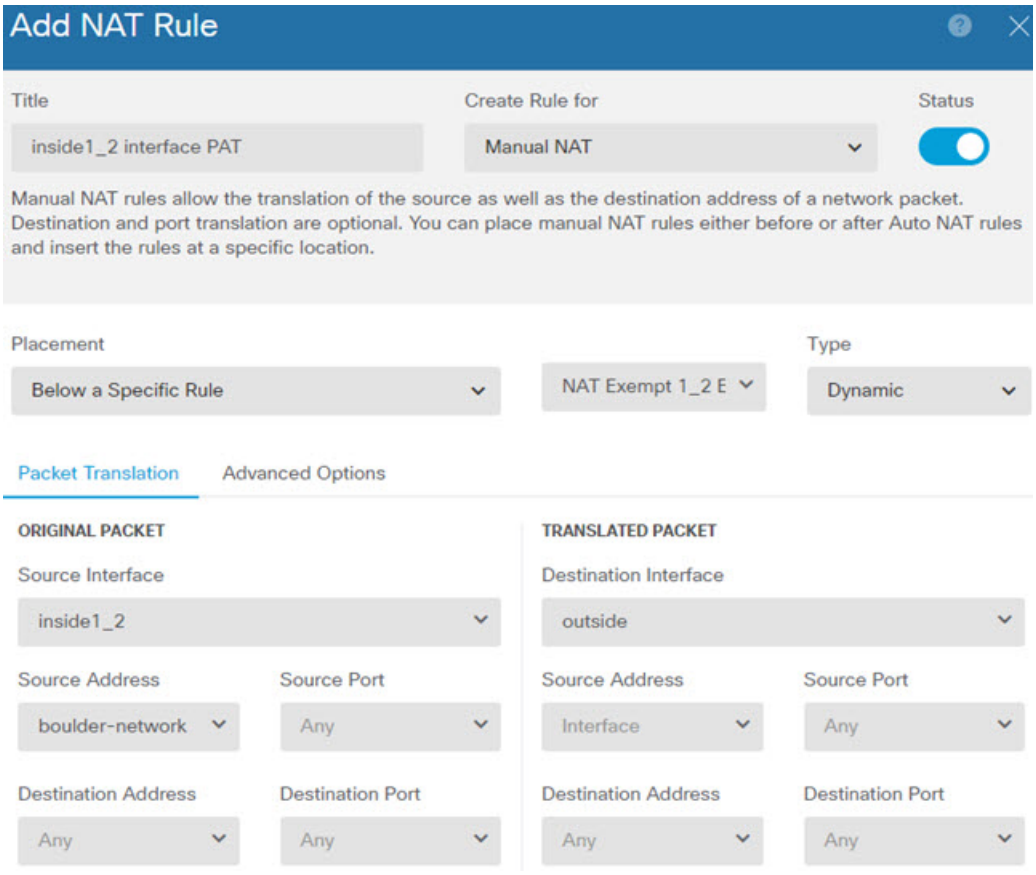
a) + 버튼을 클릭합니다.

b) 다음 속성을 구성합니다.

- **Title(**제목**)** = inside1_2 interface PAT 또는 원하는 다른 이름
- **Create Rule For(**규칙 생성**)** = 수동 NAT
- **Placement(**배치**)** = 특정 규칙 아래를 선택하고 자동 NAT 앞의 수동 NAT 섹션에서 이 인터페이스용으로 생성한 규칙을 선택합니다. 이 규칙은 모든 대상 주소에 적용되므로 sanjose-network

를 대상으로 사용하는 규칙이 이 규칙 앞에 와야 합니다. 그렇지 않으면 sanjose-network 규칙은 어떤 주소와도 일치하지 않게 됩니다. 기본적으로는 "자동 NAT 앞의 NAT 규칙" 섹션 끝에 새 수동 NAT 규칙을 배치합니다. 이 기본 배치를 사용해도 충분합니다.

- **Type(**유형**)** = 동적
- **Source Interface(**소스 인터페이스**)** = inside1_2
- **Destination Interface(**대상 인터페이스**)** = outside
- **Original Source Address(**원본 소스 주소**)** = boulder-network 네트워크 개체
- **Translated Source Address(**변환된 소스 주소**)** = **Interface** 이 옵션은 대상 인터페이스를 사용하여 인터페이스 PAT를 구성합니다.
- **Original Destination Address(**원본 대상 주소**)** = 임의
- **Translated Destination Address(**변환된 대상 주소**)** = 임의



c) **OK(**확인**)**를 클릭합니다.

d) 이 프로세스를 반복하여 각각의 기타 내부 인터페이스에 대해 동일 규칙을 생성합니다.

단계 **4** 변경 사항을 커밋합니다.

a) 웹 페이지의 오른쪽 상단에 있는 **Deploy Changes(**변경 사항 구축**)** 아이콘을 클릭합니다.

b) **Deploy Now(**지금 구축**)** 버튼을 클릭합니다.

구축이 완료될 때까지 기다리거나 **OK(**확인**)**를 클릭하고 나중에 작업 목록 또는 구축 기록을 확인할 수 있습니다.

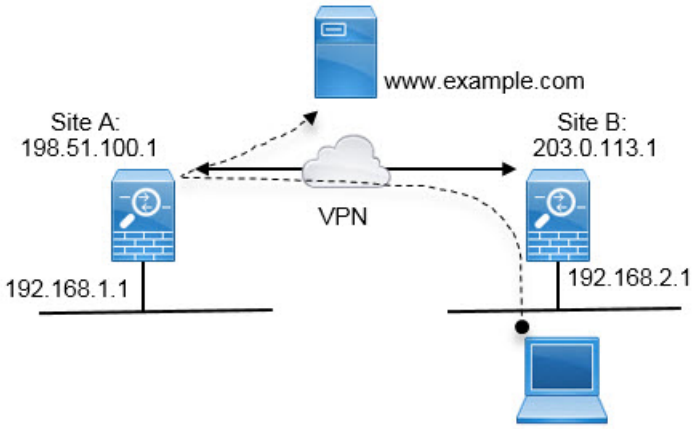
단계 **5** 방화벽2(산호세)도 관리하는 경우 해당 디바이스에 대해 비슷한 규칙을 구성할 수 있습니다.

- 대상이 boulder-network일 때는 sanjose-network용 수동 ID NAT 규칙을 구성합니다. 방화벽2 내부 및 외부 네트워크용으로 새 인터페이스 개체를 생성합니다.
- 대상이 "임의"일 때는 sanjose-network용 수동 동적 인터페이스 PAT 규칙을 생성합니다.

외부 사이트 대 사이트 VPN 사용자에게 외부 인터페이스를 통해 인터넷 액세스를 제공하는 방법(헤어피닝)

사이트 대 사이트 VPN에서는 원격 네트워크의 사용자가 디바이스를 통해 인터넷에 액세스하도록 할 수 있습니다. 그러나 원격 사용자는 인터넷에 연결되는 것과 동일한 인터페이스(외부 인터페이스)를 통해 디바이스에 진입하므로 인터넷 트래픽이 외부 인터페이스로 다시 나가도록 바운스해야 합니다. 이 기술을 헤어피닝이라고도 합니다.

다음 그림에 예시가 나와 있습니다. 기본 사이트인 사이트 A의 198.51.100.1과 원격 사이트인 사이트 B의 203.0.113.1 사이에 사이트 대 사이트 VPN 터널이 구성되어 있습니다. 원격 사이트 내부 네트워크인 192.168.2.0/24의 모든 사용자 트래픽은 VPN을 통과합니다. 따라서 해당 네트워크의 사용자가 www.example.com 등의 인터넷 서버로 이동하려는 경우 해당 연결은 먼저 VPN을 통과한 다음 198.51.100.1 인터페이스에서 인터넷으로 다시 라우팅됩니다.



다음 절차에서는 이 서비스를 구성하는 방법을 설명합니다. VPN 터널의 두 엔드포인트를 모두 구성해야 합니다.

시작하기 전에

이 절차에서는 VPN 트래픽을 허용하기 위해 기본 설정을 사용 중이며 이를 통해 VPN 트래픽을 액세스 제어 정책에 종속시킨다고 가정합니다. 이것은 실행 중인 컨피그레이션에서 **no sysopt connection permit-vpn** 명령으로 표시됩니다. 대신에 **sysopt connection permit-vpn** FlexConfig를 통해 또는 RA VPN 연결 프로파일에서 **Bypass Access Control policy for decrypted traffic(**암호 해독된 트래픽에 대해 액세스 제어 정책 우회**)** 옵션을 선택하여 활성화한 경우, 액세스 제어 규칙을 컨피그레이션하는 단계는 필요하지 않습니다.

프로시저

단계 **1** (사이트 A, 기본 사이트.) 원격 사이트 B로의 사이트 대 사이트 VPN 연결을 구성합니다.

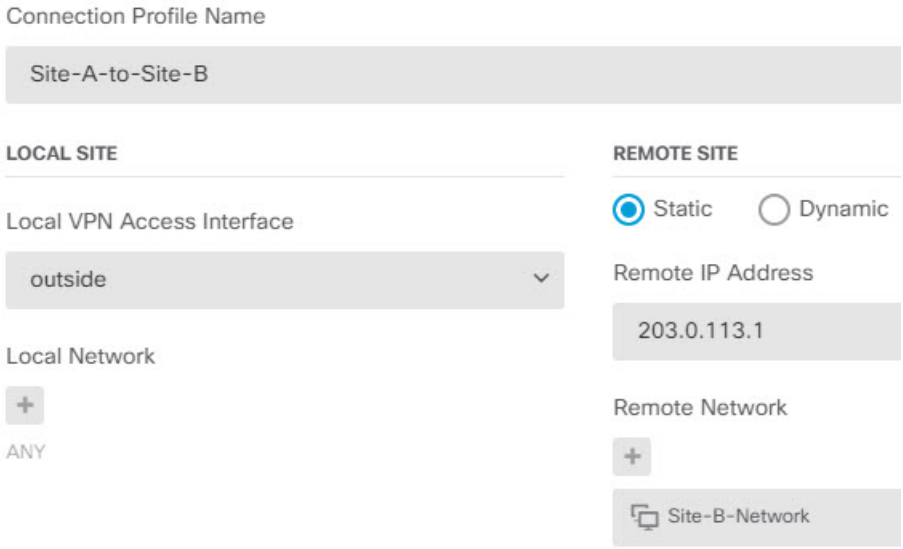
a) 디바이스를 클릭한 다음 사이트 대 사이트 VPN 그룹에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

b) **+**를 클릭하여 새 연결을 추가합니다.

c) 다음과 같이 엔드포인트를 정의하고 **Next(**다음**)**를 클릭합니다.

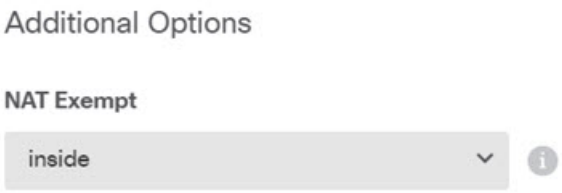
- **Connection Profile Name(**연결 프로파일 이름**)** - Site-A-to-Site-B와 같이 의미 있는 이름을 연결에 지정합니다.
- **Local VPN Access Interface(**로컬 **VPN** 액세스 인터페이스**)** - 외부 인터페이스를 선택합니다.
- **Local Network(**로컬 네트워크**)** - 기본값인 Any(모두)를 유지합니다.
- **Remote IP Address(**원격 **IP** 주소**)** - 원격 피어 외부 인터페이스의 IP 주소를 입력합니다. 이 예시에서는 203.0.113.1입니다.
- **Remote Network(**원격 네트워크**)** - **+**를 클릭하고 원격 피어의 보호된 네트워크를 정의하는 네트워크 개체를 선택합니다. 이 예시에서는 192.168.2.0/24입니다. **Create New Network(**새 네트워크 생성**)**를 클릭하면 바로 개체를 생성할 수 있습니다.

다음 그림은 어떻게 첫 단계가 표시되는지를 보여줍니다.



d) 프라이버시 컨피그레이션을 정의하고 **Next(**다음**)**를 클릭합니다.

- **IKE Policy(IKE** 정책**)** - IKE 설정은 헤어피닝에 영향을 주지 않습니다. 보안 요구 사항에 맞는 IKE 버전, 정책 및 제안만 선택하면 됩니다. 입력하는 로컬 및 원격 사전 공유 키를 적어 두십시오. 원격 피어를 구성할 때 해당 키가 필요합니다.
- **NAT Exempt(NAT** 면제**)** - 내부 인터페이스를 선택합니다.



- **Diffie Helman Group for Perfect Forward Secrecy(PFS(Perfect Forward Secrecy)**를 위한 **Diffie Hellman** 그룹**)** - 이 설정은 헤어피닝에 영향을 주지 않습니다. 따라서 적합하게 구성하면 됩니다.

e) **Finish(**마침**)**를 클릭합니다.

연결 요약이 클립보드에 복사됩니다. 해당 요약을 텍스트 파일 또는 다른 문서에 붙여넣어 원격 피어를 구성하는 데 사용할 수 있습니다.

단계 **2** (사이트 A, 기본 사이트.) 외부 인터페이스에서 외부 IP 주소의 포트로 나가는 모든 연결을 변환하는 NAT 규칙(인터페이스 PAT)을 구성합니다.

초기 디바이스 컨피그레이션을 완료하면 InsideOutsideNatRule이라는 NAT 규칙이 생성됩니다. 이 규칙은 외부 인터페이스를 통해 디바이스에서 나가는 모든 인터페이스의 IPv4 트래픽에 인터페이스 PAT를 적용합니다. 외부 인터페이스는 "Any" 소스 인터페이스에 포함되므로 필요한 규칙을 수정하거나 삭제한 경우가 아니면 규칙이 이미 존재합니다.

다음 절차에서는 필요한 규칙을 생성하는 방법을 설명합니다.

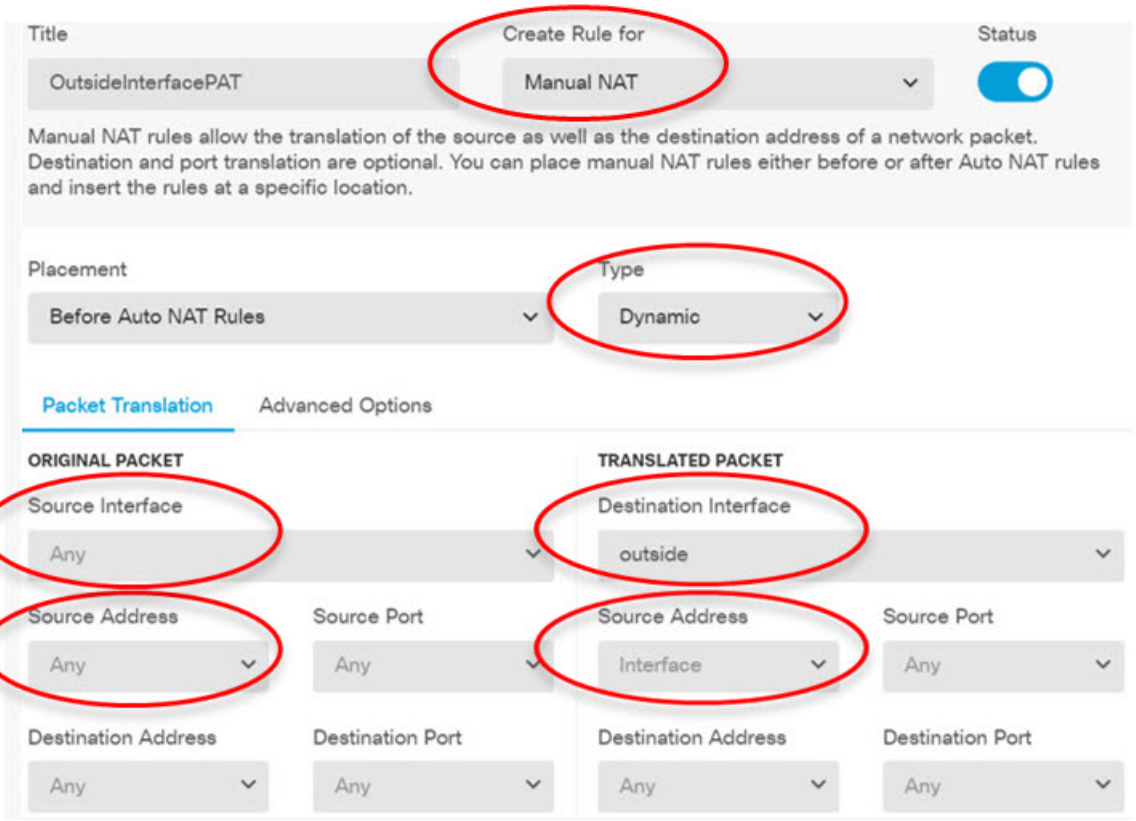
a) **Policies(**정책**)** > **NAT**를 클릭합니다.
b) 다음 중 하나를 수행합니다.

- InsideOutsideNatRule을 수정하려면 **Action(**작업**)** 열 위에 마우스를 놓고 수정 아이콘( )을 클릭합니다.
- 새 규칙을 생성하려면 **+**를 클릭합니다.

c) 다음 속성을 사용하여 규칙을 구성합니다.

- **Title(**제목**)** - 새 규칙의 경우 의미 있는 이름을 공백 없이 입력합니다. 예를 들어 OutsideInterfacePAT를 입력합니다.
- **Create Rule For(**규칙 생성 대상**)** - **Manual NAT(**수동 **NAT)**.
- **Placement(**배치**)** - **Before Auto NAT Rules(**자동 **NAT** 규칙 앞**)**(기본값).
- **Type(**유형**)** - **Dynamic(**동적**)**.
- **Original Packet(**원본 패킷**)** - **Source Address(**소스 주소**)**의 경우 Any(모두) 또는 any-ipv4를 선택합니다. **Source Interface(**소스 인터페이스**)**의 경우 기본값인 Any(모두)를 선택해야 합니다. 기타 모든 Original Packet(원본 패킷) 옵션의 경우 기본값인 Any(모두)를 유지합니다.
- **Translated Packet(**변환된 패킷**)** - **Destination Interface(**대상 인터페이스**)**의 경우 outside(외부)를 선택합니다. **Translated Address(**변환된 주소**)**의 경우 **Interface(**인터페이스**)**를 선택합니다. 기타 모든 Translated Packet(변환된 패킷) 옵션의 경우 기본값인 Any(모두)를 유지합니다.

다음 그림에는 소스 주소로 Any(모두)를 선택하는 간단한 사례가 나와 있습니다.



d) **OK(**확인**)**를 클릭합니다.

단계 **3** (사이트 A, 기본 사이트.) 사이트 B에서 보호된 네트워크에 대한 액세스를 허용하는 액세스 제어 규칙을 구성합니다.

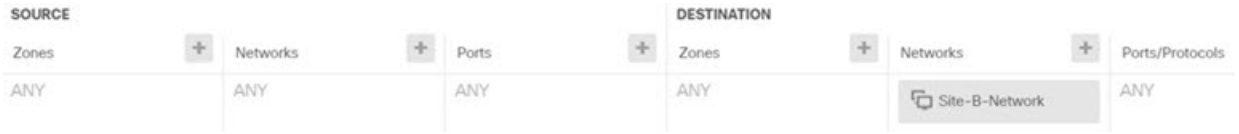
단순히 VPN 연결을 생성한다고 해서 VPN에서 트래픽을 자동으로 허용하지 않습니다. 액세스 제어 정책이 원격 네트워크로의 트래픽을 허용하는지를 확인해야 합니다.

다음 절차는 원격 네트워크에 대해 구체적으로 규칙을 추가하는 방법을 보여줍니다. 추가 규칙이 필요한지 여부는 기존 규칙에 따라 달라집니다.

a) **Policies(**정책**)** > **Access Control(**액세스 제어**)**을 클릭합니다.
b) +를 클릭하여 새 규칙을 생성합니다.
c) 다음 속성을 사용하여 규칙을 구성합니다.

- **Order(**순서**)** - 연결을 찾아 차단하는 다른 규칙 앞에 해당 규칙을 넣도록 정책 내의 위치를 선택합니다. 기본적으로는 규칙이 정책의 끝에 추가됩니다. 나중에 규칙을 재배치해야 하는 경우 이 옵션을 수정하거나, 규칙을 끌어서 표의 원하는 슬롯에 놓을 수 있습니다.
- **Title(**제목**)** - 의미 있는 이름을 공백 없이 입력합니다. 예를 들어 Site-B-Network를 입력합니다.
- **Action(**작업**)** - **Allow(**허용**)**. 이 트래픽의 프로토콜 위반 또는 침입을 검사하지 않으려는 경우 Trust(신뢰)를 선택할 수 있습니다.

- **Source/Destination(**소스/대상**)** 탭 - **Destination(**대상**)** > **Network(**네트워크**)**의 경우 원격 네트워크의 VPN 연결 프로파일에서 사용한 것과 같은 개체를 선택합니다. 기타 모든 Source(소스) 및 Destination(대상) 옵션의 경우 기본값인 Any(모두)를 유지합니다.



- **Application(**애플리케이션**)**, **URL** 및 **Users(**사용자**)** 탭 - 이러한 탭에서는 기본 설정, 즉 아무 설정도 선택하지 않은 상태를 유지합니다.
- **Intrusion(**침입**)**, **File(**파일**)** 탭 - 선택적으로 위협이나 악성코드를 검사하기 위한 침입 또는 파일 정책을 선택할 수 있습니다.
- **Logging(**로깅**)** 탭 - 선택적으로 연결 로깅을 활성화할 수 있습니다.

d) **OK(**확인**)**를 클릭합니다.

단계 **4** (사이트 A, 기본 사이트.) 변경 사항을 커밋합니다.

a) 웹 페이지의 오른쪽 상단에 있는 **Deploy Changes(**변경 사항 구축**)** 아이콘을 클릭합니다.

b) **Deploy Now(**지금 구축**)** 버튼을 클릭합니다.

구축이 완료될 때까지 기다리거나 **OK(**확인**)**를 클릭하고 나중에 작업 목록 또는 구축 기록을 확인할 수 있습니다. 창을 활성화한 상태로 유지하면 구축에 성공한 후에 보류 중인 변경 사항이 없다는 메시지가 표시됩니다.

단계 **5** (사이트 B, 원격 사이트.) 원격 사이트의 디바이스에 로그인하여 사이트 A로의 사이트 대 사이트 VPN 연결을 구성합니다.

사이트 A 디바이스 컨피그레이션에서 가져온 연결 요약을 사용하여 연결의 사이트 B 측을 구성할 수 있습니다.

a) 디바이스를 클릭한 다음 사이트 대 사이트 VPN 그룹에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

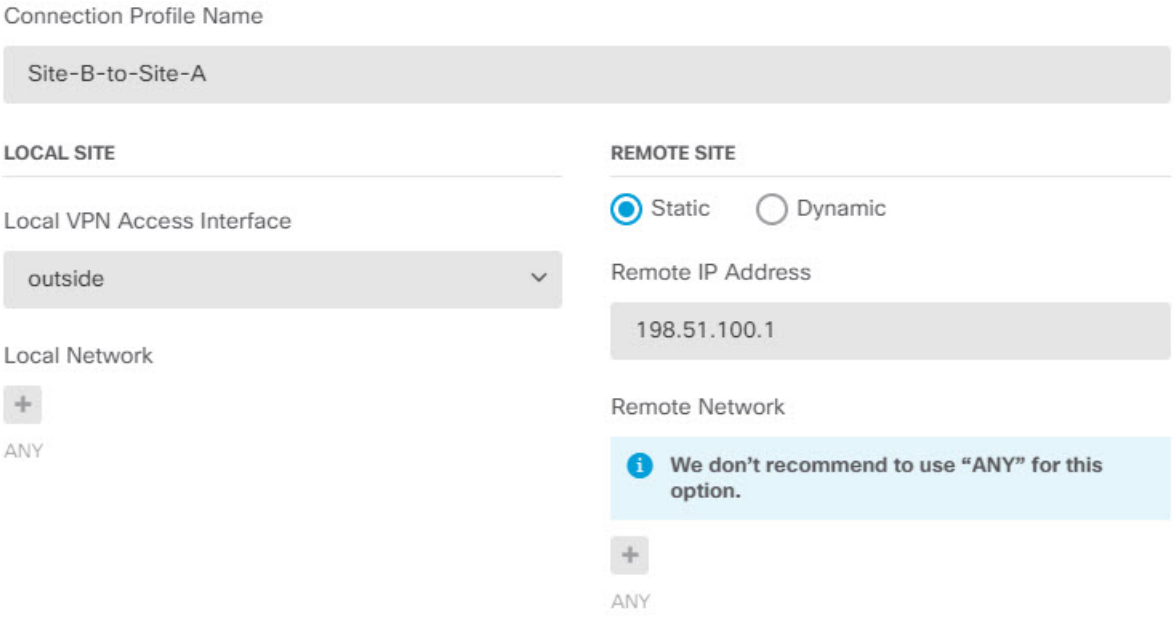
b) +를 클릭하여 새 연결을 추가합니다.

c) 다음과 같이 엔드포인트를 정의하고 **Next(**다음**)**를 클릭합니다.

- **Connection Profile Name(**연결 프로파일 이름**)** - Site-B-to-Site-A와 같이 의미 있는 이름을 연결에 지정합니다.
- **Local VPN Access Interface(**로컬 **VPN** 액세스 인터페이스**)** - 외부 인터페이스를 선택합니다.
- **Local Network(**로컬 네트워크**)** - +를 클릭하고 보호된 로컬 네트워크를 정의하는 네트워크 개체를 선택합니다. 이 예시에서는 192.168.2.0/24입니다. **Create New Network(**새 네트워크 생성**)**를 클릭하면 바로 개체를 생성할 수 있습니다.

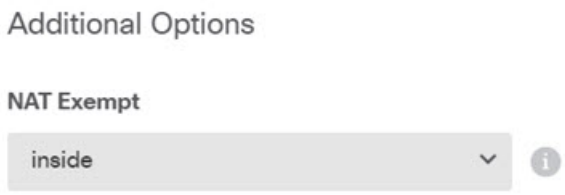
- **Remote IP Address(**원격 **IP** 주소**)** - 기본 사이트 외부 인터페이스의 IP 주소를 입력합니다. 이 예시에서는 198.51.100.1입니다.
- **Remote Network(**원격 네트워크**)** - 기본값인 Any(모두)를 유지합니다. 경고는 이 사용 사례와 관련이 없으므로 무시하십시오.

다음 그림은 어떻게 첫 단계가 표시되는지를 보여줍니다.



d) 프라이버시 컨피그레이션을 정의하고 **Next(**다음**)**를 클릭합니다.

- **IKE Policy(IKE** 정책**)** - IKE 설정은 헤어피닝에 영향을 주지 않습니다. 사이트 A의 VPN 연결 끝과 같거나 호환되는 옵션을 구성합니다. 사전 공유 키를 올바르게 구성해야 합니다. 사이트 A 디바이스에 구성된 로컬 및 원격 키(IKEv2용)를 전환합니다. IKEv1의 경우에는 키가 하나뿐이며 두 피어에서 동일해야 합니다.
- **NAT Exempt(NAT** 면제**)** - 내부 인터페이스를 선택합니다.



- **Diffie Helman Group for Perfect Forward Secrecy(PFS(Perfect Forward Secrecy)**를 위한 **Diffie Hellman** 그룹**)** - 이 설정은 헤어피닝에 영향을 주지 않습니다. 사이트 A의 VPN 연결 끝에서 사용한 설정과 일치시킵니다.

e) **Finish(**마침**)**를 클릭합니다.

단계 **6** (사이트 B, 원격 사이트.) 사이트에서 나가는 모든 트래픽이 VPN 터널을 통과하도록 보호된 네트워크의 모든 NAT 규칙을 삭제합니다.

사이트 A 디바이스가 주소 변환을 수행하므로 이 디바이스에서는 NAT를 수행할 필요가 없습니다. 하지만 구체적인 상황을 점검해야 합니다. 내부 네트워크가 여러 개인데 그중 일부가 이 VPN 연결에 포함되지 않는 경우 해당 네트워크에 필요한 NAT 규칙은 삭제하지 마십시오.

a) **Policies(**정책**)** > **NAT**를 클릭합니다.
b) 다음 중 하나를 수행합니다.

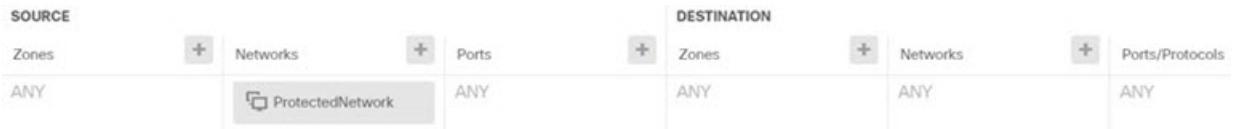
- 규칙을 삭제하려면 Action(작업) 열 위에 마우스를 놓고 삭제 아이콘( )을 클릭합니다.
- 보호된 네트워크에 더 이상 적용되지 않도록 규칙을 수정하려면 Action(작업) 열 위에 마우스를 놓고 수정 아이콘( )을 클릭합니다.

단계 **7** (사이트 B, 원격 사이트.) 보호된 네트워크에서 인터넷에 대한 액세스를 허용하는 액세스 제어 규칙을 구성합니다.

다음 예시에서는 보호된 네트워크에서 특정 대상으로의 트래픽을 허용합니다. 구체적인 요구 사항에 맞게 이 예시를 조정할 수 있습니다. 또한 이 규칙 앞에 원치 않는 트래픽을 필터링하여 제거하는 차단 규칙을 배치할 수도 있습니다. 사이트 A 디바이스에서 차단 규칙을 구성하는 옵션도 있습니다.

a) **Policies(**정책**)** > **Access Control(**액세스 제어**)**을 클릭합니다.
b) +를 클릭하여 새 규칙을 생성합니다.
c) 다음 속성을 사용하여 규칙을 구성합니다.

- **Order(**순서**)** - 연결을 찾아 차단하는 다른 규칙 앞에 해당 규칙을 넣도록 정책 내의 위치를 선택합니다. 기본적으로는 규칙이 정책의 끝에 추가됩니다. 나중에 규칙을 재배치해야 하는 경우 이 옵션을 수정하거나, 규칙을 끌어서 표의 원하는 슬롯에 놓을 수 있습니다.
- **Title(**제목**)** - 의미 있는 이름을 공백 없이 입력합니다. 예를 들어 Protected-Network-to-Any를 입력합니다.
- **Action(**작업**)** - **Allow(**허용**)**. 이 트래픽의 프로토콜 위반 또는 침입을 검사하지 않으려는 경우 Trust(신뢰)를 선택할 수 있습니다.
- **Source/Destination(**소스/대상**)** 탭 - **Source(**소스**)** > **Network(**네트워크**)**의 경우 로컬 네트워크의 VPN 연결 프로파일에서 사용한 것과 같은 개체를 선택합니다. 기타 모든 Source(소스) 및 Destination(대상) 옵션의 경우 기본값인 Any(모두)를 유지합니다.



- **Application(**애플리케이션**)**, **URL** 및 **Users(**사용자**)** 탭 - 이러한 탭에서는 기본 설정, 즉 아무 설정도 선택하지 않은 상태를 유지합니다.
- **Intrusion(**침입**)**, **File(**파일**)** 탭 - 선택적으로 위협이나 악성코드를 검사하기 위한 침입 또는 파일 정책을 선택할 수 있습니다.

• **Logging(**로깅**)** 탭 - 선택적으로 연결 로깅을 활성화할 수 있습니다.

d) **OK(**확인**)**를 클릭합니다.

단계 **8** (사이트 B, 원격 사이트.) 변경 사항을 커밋합니다.

a) 웹 페이지의 오른쪽 상단에 있는 **Deploy Changes(**변경 사항 구축**)** 아이콘을 클릭합니다.

b) **Deploy Now(**지금 구축**)** 버튼을 클릭하고 구축이 완료될 때까지 기다립니다.

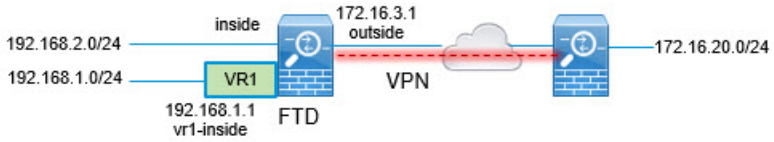
구축이 완료될 때까지 기다리거나 **OK(**확인**)**를 클릭하고 나중에 작업 목록 또는 구축 기록을 확인할 수 있습니다. 창을 활성화한 상태로 유지하면 구축에 성공한 후에 보류 중인 변경 사항이 없다는 메시지가 표시됩니다.

사이트 간 VPN을 통해 여러 가상 라우터의 네트워크에서 트래픽을 보호하는 방법

디바이스에서 여러 가상 라우터를 구성하는 경우에는 전역 가상 라우터에서 사이트 간 VPN을 구성해야 합니다. 사용자 지정 가상 라우터에 할당된 인터페이스에는 사이트 간 VPN을 구성할 수 없습니다.

가상 라우터의 라우팅 테이블은 별도이기 때문에, 사이트 간 VPN을 통해 맞춤형 가상 라우터에서 호스팅되는 네트워크에서 연결을 보호해야 하는 경우 정적 경로를 생성해야 합니다. 또한 이러한 추가 네트워크를 포함하도록 사이트 간 VPN 연결을 업데이트해야 합니다.

다음과 같은 사례를 가정해보십시오. 이 경우 사이트 간 VPN은 172.16.3.1의 외부 인터페이스에 정의됩니다. 내부 인터페이스는 전역 가상 라우터의 일부이므로 이 VPN에는 추가 구성없이 내부 네트워크 192.168.2.0/24를 포함할 수 있습니다. 그러나 VR1 가상 라우터의 일부인 192.168.1.0/24 네트워크에 사이트 간 VPN 서비스를 제공해야 하는 경우에는 정적 경로를 두 가지 방식으로 모두 구성하고 사이트 간 VPN 구성에 네트워크를 추가해야 합니다.



시작하기 전에

이 예에서는 192.168.2.0/24 로컬 네트워크와 172.16.20.0/24 외부 네트워트 간의 사이트 간 VPN을 이미 구성하고 가상 라우터를 정의했으며 적절한 가상 라우터에 인터페이스를 구성 및 할당한 것으로 가정합니다.

프로시저

단계 **1** 전역 가상 라우터에서 VR1으로의 경로 유출을 구성합니다.

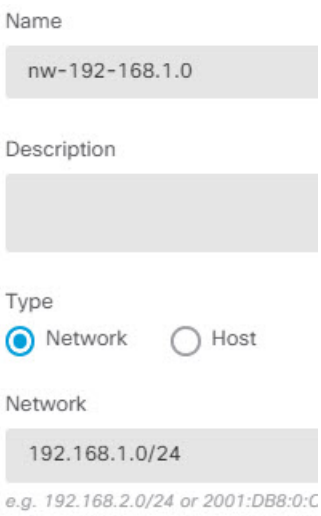
이 경로는 사이트 간 VPN의 외부(원격) 끝에서 보호하는 엔드포인트를 VR1 가상 라우터의 192.168.1.0/24 네트워크에 액세스하는 데 사용할 수 있습니다.

a) **Device(**디바이스**)** > **Routing(**라우팅**)** > **View Configuration(**구성 보기**)**을 선택합니다.

b) 전역 가상 라우터의 View Icon(아이콘 보기)을 클릭합니다.

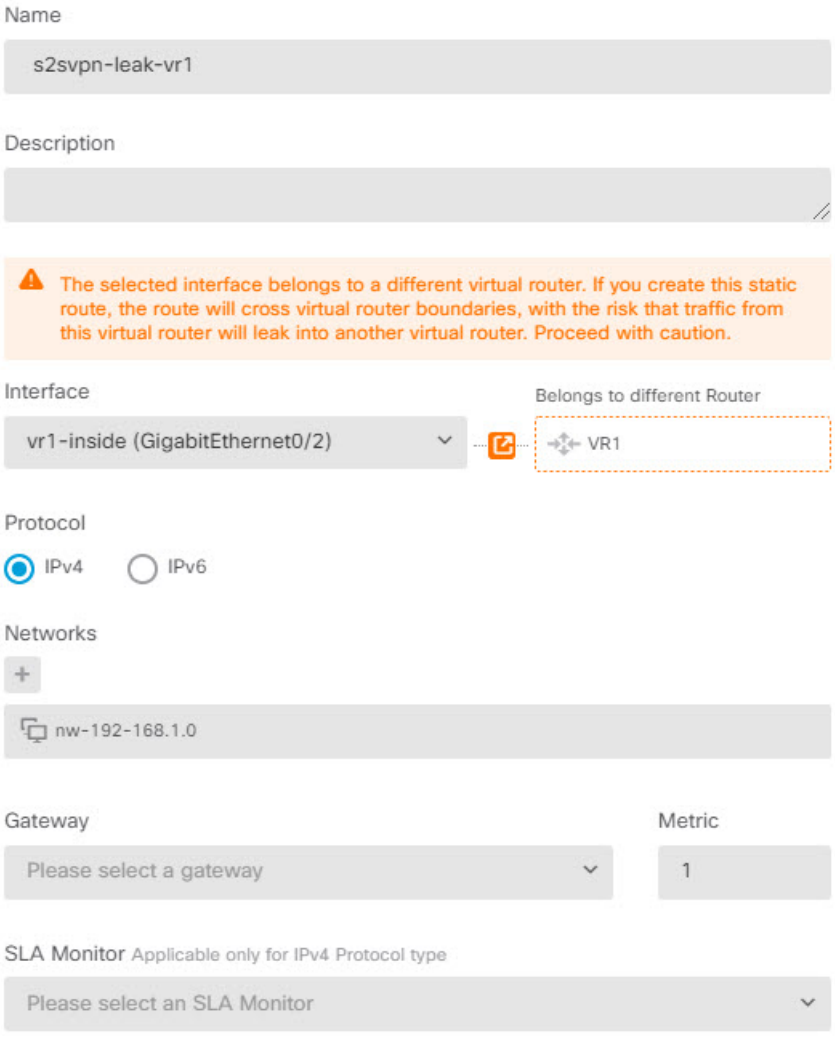
c) 전역 라우터에 대한 **Static Routing(**정적 라우팅**)** 탭에서 **+**를 클릭하고 다음과 같이 경로를 구성합니다.

- **Name(**이름**)**—모든 이름(예: **s2svpn-leak-vr1**)이 수행됩니다.
- **Interface(**인터페이스**)** — **vr1-inside**를 선택합니다.
- **Protocol(**프로토콜**)** — **IPv4**를 선택합니다.
- **Network(**네트워크**)**—192.168.1.0/24 네트워크를 정의하는 개체를 선택합니다. 필요한 경우 **Create New Network(**새 네트워크 생성**)**를 클릭하면 바로 개체를 생성할 수 있습니다.



- **Gateway(**게이트웨이**)** — 이 항목은 비워둡니다. 다른 가상 라우터로 경로를 유출할 경우에는 게이트웨이 주소를 선택하지 않습니다.

대화 상자가 다음과 비슷하게 표시됩니다.



d) **OK(**확인**)**를 클릭합니다.

단계 **2** VR1에서 전역 가상 라우터로의 경로 유출을 구성합니다.

이 경로를 사용하면 192.168.1.0/24 네트워크의 엔드포인트에서 사이트 간 VPN 터널을 통과하는 연결을 시작할 수 있습니다. 이 예에서는 원격 엔드포인트에서 172.16.20.0/24 네트워크를 보호하고 있습니다.

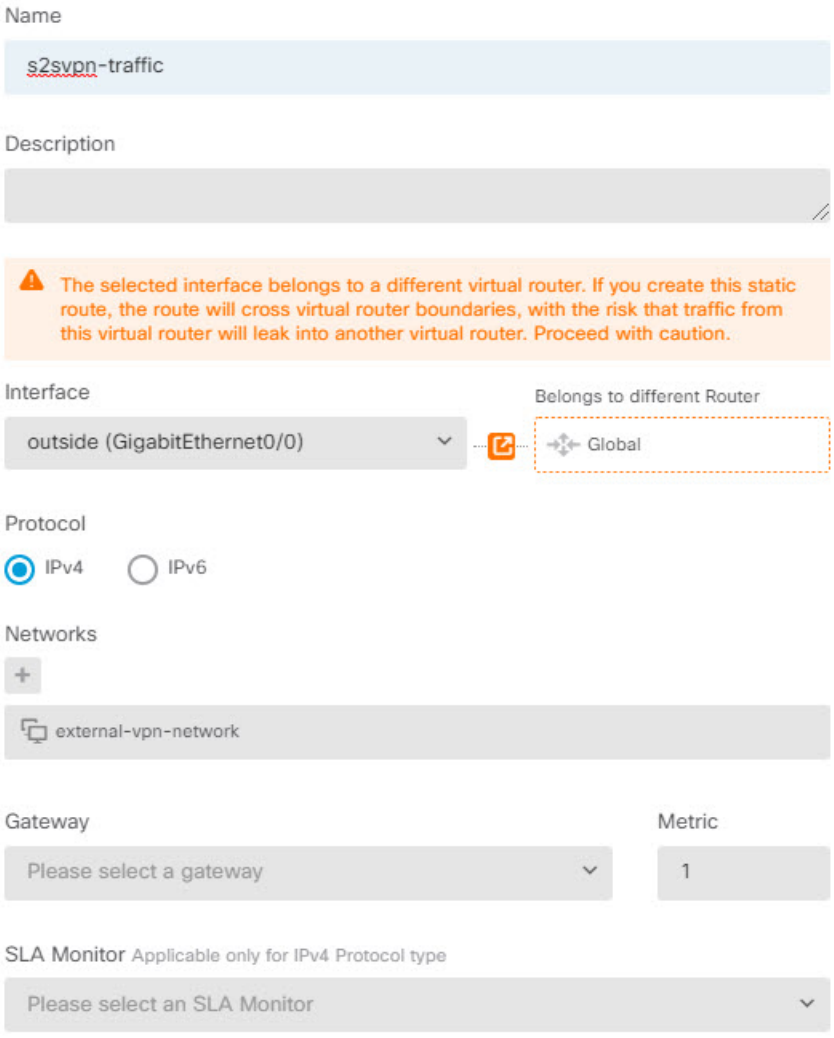
a) 가상 라우터 드롭다운 목록에서 **VR1**을 선택하여 VR1 구성으로 전환합니다.

b) VR1 가상 라우터에 대한 **Static Routing(**정적 라우팅**)** 탭에서 +를 클릭하고 다음과 같이 경로를 구성합니다.

- **Name(**이름**)** — 모든 이름(예: **s2svpn-traffic**)이 수행됩니다.
- **Interface(**인터페이스**)** — **outside**를 선택합니다.
- **Protocol(**프로토콜**)** — **IPv4**를 선택합니다.

- **Network(**네트워크**)** —원격 엔드포인트의 보호된 네트워크(예: 외부 **VPN** 네트워크)에 대해 생성한 개체를 선택합니다.
- **Gateway(**게이트웨이**)** — 이 항목은 비워둡니다. 다른 가상 라우터로 경로를 유출할 경우에는 게이트웨이 주소를 선택하지 않습니다.

대화 상자가 다음과 비슷하게 표시됩니다.



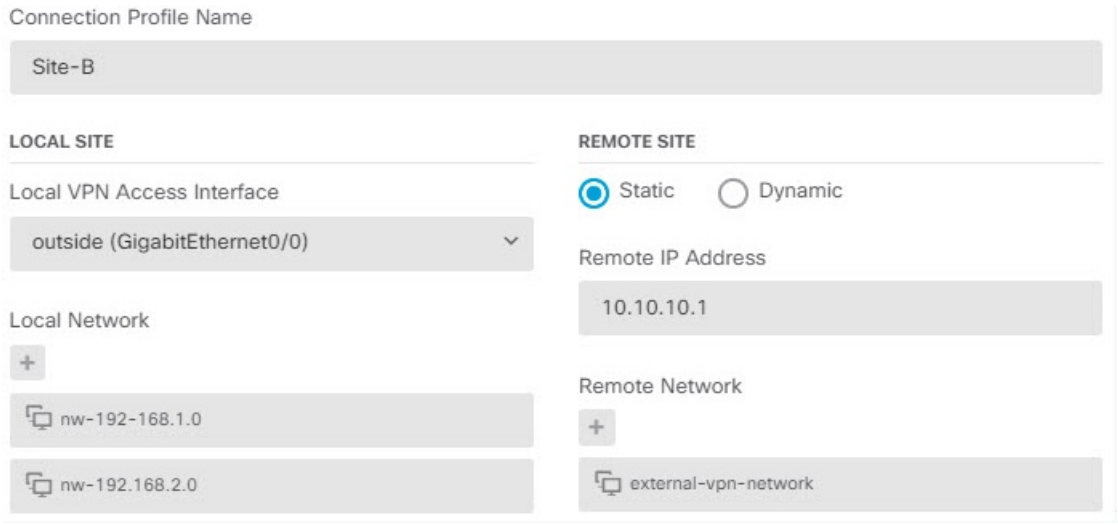
c) **OK(**확인**)**를 클릭합니다.

단계 **3** 사이트 간 VPN 연결 프로파일에 192.168.1.0/24 네트워크를 추가합니다.

a) **Device(**디바이스**)** > **Site-to-Site VPN(**사이트 간 **VPN)** > **View Configuration(**구성 보기**)**을 선택합니다.

b) 연결 프로파일에 대한 edit icon(수정 아이콘)()을(를) 클릭합니다.

c) 마법사의 첫 번째 페이지에서 로컬 네트워크 아래의 +을(를) 클릭하고 192.168.1.0/24 네트워크에 대한 개체를 추가합니다.


Connection Profile Name
Site-B
LOCAL SITE
Local VPN Access Interface
outside (GigabitEthernet0/0)
Local Network
nw-192-168.1.0
nw-192.168.2.0
REMOTE SITE
Static
Dynamic
Remote IP Address
10.10.10.1
Remote Network
external-vpn-network

d) 마법사를 완료합니다.

25 장

원격 액세스 VPN

원격 액세스 VPN(Virtual Private Network)을 사용하면 개별 사용자가 인터넷에 연결된 컴퓨터 또는 기타 지원되는 iOS 또는 Android 디바이스를 사용하여 원격 위치에서 네트워크에 연결할 수 있습니다. 따라서 모바일 근무자가 홈 네트워크 또는 공개 Wi-Fi 네트워크 등에서 연결할 수 있습니다.

다음 주제에서는 네트워크용으로 원격 액세스 VPN을 구성하는 방법을 설명합니다.

원격 액세스 VPN 개요

device manager를 사용하여 Secure Client 소프트웨어를 통한 원격 액세스 VPN over SSL을 구성할 수 있습니다.

Secure Client는 threat defense 디바이스와 SSL VPN 연결을 협상할 때 TLS(Transport Layer Security: 전송 계층 보안) 또는 DTLS(Datagram Transport Layer Security: 데이터그램 전송 계층 보안)를 사용하여 연결합니다. DTLS는 일부 SSL 연결에서 발생하는 레이턴시 및 대역폭 문제를 방지하고 패킷 지연에 민감한 실시간 애플리케이션의 성능을 높입니다. 클라이언트 및 threat defense 디바이스에서는 사용할 TLS/DTLS 버전을 협상합니다. 클라이언트가 지원하는 경우 DTLS가 사용됩니다.

디바이스 모델별 최대 동시 VPN 세션

디바이스 모델에 따라 디바이스에서 허용되는 동시 원격 액세스 VPN 세션 수에는 최대 제한이 적용됩니다. 이러한 제한은 시스템 성능이 부적절한 레벨로 저하되지 않도록 설계된 것입니다. 용량 계획 시에 이러한 제한을 사용하십시오.

디바이스 모델	최대 동시 원격 액세스 **VPN** 세션
Firepower 1010	75
Firepower 1120	150
Firepower 1140	400
Firepower 2110	1500
Firepower 2120	3500
Firepower 2130	7500
Firepower 2140	10,000
Secure Firewall 3110	1500
Secure Firewall 3120	3500
Secure Firewall 3130	7500
Secure Firewall 3140	10,000
Firepower 4100 Series, 모든 모델	10,000
Firepower 9300 Appliance, 모든 모델	20,000
Threat Defense Virtual: FTDv5	50
Threat Defense Virtual: FTDv10, FTDv20, FTDv30	250
Threat Defense Virtual: FTDv50	750
Threat Defense Virtual: FTDv100	10,000
ISA 3000	25

Secure Client 소프트웨어 다운로드

원격 액세스 VPN를 구성하려면 먼저 워크스테이션에 Secure Client 소프트웨어를 다운로드해야 합니다. VPN를 정의할 때 이러한 패키지를 업로드해야 합니다.

최신 기능, 버그 수정 및 보안 패치를 적용하려면 최신 Secure Client 버전을 다운로드해야 합니다. threat defense 디바이스에서 패키지를 정기적으로 업데이트합니다.

참고 운영 체제(Windows, Mac, Linux)별로 Secure Client 패키지를 하나씩 업로드할 수 있습니다. 지정된 OS 유형의 여러 버전을 업로드할 수는 없습니다.

Secure Client 소프트웨어 패키지는 software.cisco.com에서 다운로드합니다. 클라이언트의 "전체 설치 패키지" 버전을 다운로드해야 합니다.

사용자가 Secure Client 소프트웨어를 설치할 수 있는 방법

VPN 연결을 완료하려면 사용자가 Secure Client 소프트웨어를 설치해야 합니다. 기존 소프트웨어 배포 방법을 사용하여 소프트웨어를 직접 설치할 수 있습니다. 또는 사용자가 threat defense 디바이스에서 Secure Client를 직접 설치하게 할 수도 있습니다.

소프트웨어를 설치하려면 사용자에게 워크스테이션에 대한 관리자 권한이 있어야 합니다.

Secure Client를 설치하고 나면 시스템에 새 Secure Client 버전을 업로드하는 경우 사용자가 다음 번에 VPN에 연결할 때 Secure Client가 새 버전을 탐지합니다. 그러면 시스템에서 업데이트된 클라이언트 소프트웨어를 다운로드하여 설치하라는 메시지를 사용자에게 자동으로 표시합니다. 이러한 자동화로 인해 개발자와 고객을 위한 소프트웨어 배포를 간소화할 수 있습니다.

사용자가 threat defense 디바이스에서 소프트웨어를 처음 설치하도록 하려면 사용자에게 다음 단계를 수행하도록 하십시오.

참고 안드로이드 및 iOS 사용자는 해당 앱 스토어에서 Secure Client를 다운로드해야 합니다.

프로시저

단계 **1** 웹 브라우저를 사용하여 **https://***ravpn-address*를 엽니다. 여기서 *ravpn-address*는 VPN 연결을 허용할 외부 인터페이스의 IP 주소 또는 호스트 이름입니다.

원격 액세스 VPN을 구성할 때 이 인터페이스를 식별합니다. 시스템에서 사용자에게 로그인하라는 메시지를 표시합니다.

원격 액세스 VPN 연결용 포트를 변경한 경우 URL에 맞춤형 포트를 포함해야 합니다. 예를 들어 포트를 4443으로 변경한 경우 https://ravpn.example.com:4443과 같습니다.

단계 **2** 사이트에 로그인합니다.

사용자는 원격 액세스 VPN용으로 구성된 디렉터리 서버를 사용하여 인증을 합니다. 로그인이 성공해야 설치를 계속할 수 있습니다.

로그인이 성공하면 시스템은 사용자에게 필요한 Secure Client 버전이 이미 있는지를 확인합니다. 사용자 컴퓨터에 Secure Client가 없거나 클라이언트가 하위 레벨인 경우에는 시스템에서 Secure Client 소프트웨어 설치를 자동으로 시작합니다.

설치가 완료되면, Secure Client에서 원격 액세스 VPN 연결을 완료합니다.

RADIUS 및 그룹 정책을 이용한 사용자 권한 및 속성 제어

외부 RADIUS 서버 또는 threat defense 디바이스에 정의된 그룹 정책에서 RA VPN 연결에 사용자 인증 속성(사용자 자격 또는 권한이라고도 함)을 적용할 수 있습니다. threat defense 디바이스에서 그룹 정책에 컨피그레이션된 속성과 충돌하는 속성을 AAA 서버로부터 수신하는 경우, AAA 서버에서 오는 속성이 항상 우선 적용됩니다.

threat defense 디바이스에서는 다음 순서로 속성을 적용합니다.

1. 외부 AAA 서버에 정의된 사용자 속성 - 인증 및/또는 권한 부여가 성공적으로 수행되면 서버에서 이 속성을 반환합니다.
2. threat defense 디바이스에 컨피그레이션된 그룹 정책 - RADIUS 서버에서 사용자에 대해 RADIUS CLASS 속성 IETF-Class-25(OU=group-policy) 값을 반환하면 threat defense 디바이스에서는 해당 사용자를 이름이 같은 그룹 정책에 배치하고 서버에서 반환하지 않은 그룹 정책의 모든 속성을 적용합니다.
3. 연결 프로파일에서 할당한 그룹 정책 - 연결 프로파일에는 연결을 위한 예비 설정이 있으며 인증 전에 사용자에게 적용되는 기본 그룹 정책을 포함합니다. threat defense 디바이스에 처음 접속하는 모든 사용자는 이 그룹에 속하며, 이를 통해 AAA 서버에서 반환한 사용자 속성 또는 사용자에게 할당된 그룹 정책에 없는 모든 속성을 제공합니다.

Threat Defense 디바이스에서는 벤더 ID가 3076인 RADIUS 속성을 지원합니다. 사용하는 RADIUS 서버에 이러한 속성이 정의되지 않은 경우, 수동으로 정의해야 합니다. 특성을 정의하려면 특성 이름 또는 번호, 유형, 값 및 공급업체 코드(3076)를 사용합니다.

다음 주제에서는 값이 RADIUS 서버에 정의되어 있는지 또는 값이 시스템에서 RADIUS 서버로 전송하는 값인지 여부에 따라 지원되는 속성을 설명합니다.

RADIUS 서버로 전송되는 속성

RADIUS 속성 146 및 150은 인증 및 권한 부여 요청을 위해 threat defense 디바이스에서 RADIUS 서버로 전송됩니다. 다음 속성 모두 계정 관리 시작, 중간 업데이트, 중단 요청을 위해 threat defense 디바이스에서 RADIUS 서버로 전송됩니다.

표 *13: Threat Defense*에서 *RADIUS*로 전송하는 속성

특성	속성 번호	구문, 유형	단일 또는 다중 값 지정	설명 또는 값
클라이언트 유형	150	정수	단일	VPN에 접속 중인 클라이언트의 유형: 2 = Secure Client SSL VPN
세션 유형	151	정수	단일	연결 유형: 1 = Secure Client SSL VPN
터널 그룹 이름	146	문자열	단일	threat defense 디바이스에 정의된 대로 세션을 설정하는 데 사용된 연결 프로파일의 이름입니다. 이름은 1~253자일 수 있습니다.

RADIUS 서버에서 수신한 속성

다음 사용자 권한 부여 속성은 RADIUS 서버에서 threat defense 디바이스로 전송됩니다.

표 ***14: RADIUS*** 속성이 전송되는 대상***: Threat Defense***

특성	속성 번호	구문, 유형	단일 또는 다중 값 지정	설명 또는 값
Access-List-Inbound	86	문자열	단일	액세스 목록(Acess-List) 속성 둘 다 threat defense 디바이스에 컨피그레이션된 ACL의 이름을 따릅니다. 스마트 CLI 확장 액세스 목록 개체 유형을 사용해 이 ACL을 생성합니다(**Device(**장치**)** > **Advanced Configuration(**고급 컨피그레이션**)** > **Smart CLI(**스마트 **CLI)** > **Objects(**개체**)** 선택). 이 ACL에서는 인바운드(threat defense 디바이스로 들어가는 트래픽) 또는 아웃바운드(threat defense 디바이스에서 나가는 트래픽) 방향으로 트래픽 흐름을 제어합니다.
Access-List-Outbound	87	문자열	단일	
Address-Pools	217	문자열	단일	RA VPN에 접속하는 클라이언트에 대한 주소 풀로 사용될 서브넷을 식별하는 threat defense 디바이스에 정의된 네트워크 개체의 이름입니다. **Objects(**개체**)** 페이지에서 네트워크 개체를 정의합니다.
Banner1	15	문자열	단일	사용자가 로그인하면 표시할 배너입니다.
Banner2	36	문자열	단일	사용자가 로그인하면 표시할 배너의 두 번째 부분입니다. 배너2는 배너1에 추가됩니다.
Group-Policy	25	문자열	단일	연결에 사용할 그룹 정책입니다. RA VPN **Group Policy(**그룹 정책**)** 페이지에서 그룹 정책을 생성해야 합니다. 다음 형식 중 하나를 사용할 수 있습니다. • *group policy name* • OU=*group policy name* • OU=*group policy name*;
Simultaneous-Logins	2	정수	단일	사용자가 설정하도록 허용되는 별도의 동시 연결 개수입니다(0~2147483647).
VLAN	140	정수	단일	사용자의 연결을 제한할 VLAN입니다(0~4094). 또한 threat defense 디바이스의 하위 인터페이스에 이 VLAN을 컨피그레이션해야 합니다.

이중 인증

RA VPN에 대한 이중 인증을 컨피그레이션할 수 있습니다. 이중 인증의 경우, 사용자는 사용자 이름 및 정적 암호뿐 아니라 RSA 토큰 또는 듀오 암호와 같은 추가 항목도 제공해야 합니다. 이중 인증이 두 번째 인증 소스를 사용하는 것과 다른 점은 두 가지 인증 요소가 기본 인증 소스와 연결된 RSA/듀오 서버와의 관계에 따라 단일 인증 소스에서 컨피그레이션된다는 것입니다. 보조 인증 소스로 Duo LDAP 서버를 구성하는 Duo LDAP은 예외입니다.

시스템은 이중 인증 프로세스에서 첫 번째 요소인 RADIUS 또는 AD 서버와 함께 두 번째 요소에 대해 모바일로 푸시된 RSA 토큰 및 듀오 암호에 대한 테스트를 마쳤습니다.

RSA 이중 인증

다음 접근 방식 중 하나를 사용하여 RSA를 컨피그레이션할 수 있습니다. RSA 측 컨피그레이션에 대한 내용은 RSA 문서를 참조하십시오.

- device manager에서 RADIUS 서버를 RSA 서버로 직접 정의하고 RA VPN에서 서버를 기본 인증 소스로 사용합니다.

  이 접근 방식을 사용하는 경우, 사용자는 RSA RADIUS 서버에 컨피그레이션된 사용자 이름을 사용하여 인증하고 암호와 토큰을 쉼표로 구분하여(암호,토큰) 암호를 일회용 임시 RSA 토큰과 연결해야 합니다.

  이 컨피그레이션에서는 별도의 RADIUS 서버(예: Cisco ISE에서 제공되는 것)를 사용하여 권한 부여 서비스를 제공하는 것이 일반적입니다. 두 번째 RADIUS 서버를 권한 부여 서버 및 과금 서버(선택 사항)로 컨피그레이션합니다.

- 직접 통합을 지원하는 RADIUS 또는 AD 서버와 RSA 서버를 통합하고 비 RSA RADIUS 또는 AD 서버를 기본 인증 소스로 사용하도록 RA VPN을 컨피그레이션합니다. 이 경우, RADIUS/AD 서버에서는 RSA SDI를 사용하여 클라이언트와 RSA 서버 간의 이중 인증을 위임하고 오케스트레이션합니다.

  이 접근 방식을 사용하는 경우, 사용자는 비 RSA RADIUS 또는 AD 서버에 컨피그레이션된 사용자 이름을 사용하여 인증하고 암호와 토큰을 쉼표로 구분하여(암호,토큰) 암호를 일회용 임시 RSA 토큰과 연결해야 합니다.

  이 컨피그레이션에서는 비 RSA RADIUS 서버도 권한 부여 서버 및 과금 서버(선택 사항)로 사용합니다.

RADIUS를 사용하는 Duo 이중 인증

듀오 RADIUS 서버를 기본 인증 소스로 컨피그레이션할 수 있습니다. 이 접근 방식에서는 듀오 RADIUS 인증 프록시를 사용합니다.

듀오를 컨피그레이션하는 세부 절차는 https://duo.com/docs/cisco-firepower의 내용을 참조하십시오.

그런 다음, 프록시 서버로 가는 인증 요청을 전달하여 다른 RADIUS 서버 또는 AD 서버를 첫 번째 인증 요소로 사용하고 듀오 클라우드 서비스는 두 번째 요소로 사용하도록 컨피그레이션합니다.

이 접근 방식을 사용하는 경우, 사용자는 듀오 인증 프록시 및 연결된 RADIUS/AD 서버 둘 다에 컨피그레이션된 사용자 이름과 RADIUS/AD 서버에 컨피그레이션된 사용자 이름의 암호(다음 듀오 코드 중 하나가 바로 뒤에 나옴)를 사용해 인증해야 합니다.

- *Dou-passcode*. 예: *my-password*,**12345**.
- **push**. 예: *my-password*,**push**. **push(**푸시**)**를 사용하여 듀오에게 듀오 모바일 앱으로 푸시 인증을 전송하도록 지시합니다. 사용자는 이미 이 앱을 설치하여 등록했어야 합니다.
- **SMS**. 예: *my-password*,**SMS**. **SMS**를 사용하여 듀오에게 사용자의 모바일 디바이스로 새로운 암호 배치가 포함된 SMS 메시지를 전송하도록 지시합니다. **SMS**를 사용하는 경우, 사용자의 인증 시도가 실패합니다. 그러면 사용자는 다시 인증하고 두 번째 요인으로 새 암호를 입력해야 합니다.
- **phone(**전화**)**. 예: *my-password*,**phone**. 전화를 사용해 듀오에게 전화 콜백 인증을 수행하도록 지시합니다.

사용자 이름 및 암호가 인증되면 듀오 인증 프록시에서는 듀오 클라우드 서비스에 접속합니다. 이를 통해 요청이 유효한 컨피그레이션 프록시 디바이스에서 발신되었는지 확인한 다음, 지시받은 대로 사용자의 모바일 디바이스에 임시 암호를 푸시합니다. 사용자가 이 암호를 수락하면 듀오에서 세션을 인증된 것으로 표시하고 RA VPN이 설정됩니다.

LDAP를 사용하는 Duo 이중 인증

기본 소스로 Microsoft AD(Microsoft Active Directory) 또는 RADIUS 서버를 함께 사용하여 Duo LDAP 서버를 보조 인증 소스로 사용할 수 있습니다. Duo LDAP를 사용하는 경우 보조 인증에서는 Duo 암호, 푸시 알림 또는 전화 통화를 사용하여 기본 인증을 검증합니다.

threat defense 디바이스에서는 TCP/636 포트를 통해 LDAPS를 사용하여 Duo LDAP과 통신합니다.

Duo LDAP 서버에서는 인증 서비스만 제공하며, ID 서비스는 제공하지 않습니다. 따라서, Duo LDAP를 기본 인증 소스로 사용하는 경우, 어떠한 대시보드에도 RA VPN 연결과 관련된 사용자 이름이 표시되지 않으며 이러한 사용자에 대한 액세스 제어 규칙을 작성할 수 없게 됩니다.

이 접근 방식을 사용하는 경우 사용자는 RADIUS/AD 서버 및 Duo LDAP 서버에 구성된 사용자 이름을 사용하여 인증해야 합니다. Secure Client에서 로그인하라는 프롬프트가 표시되면 사용자는 기본 **Password(**비밀번호**)** 필드에 RADIUS/AD 비밀번호를 입력하고 **Secondary Password(**보조 비밀번호**)**에는 Duo를 사용하여 인증하기 위해 다음 중 하나를 입력합니다. 자세한 내용은 https://guide.duo.com/anyconnect를 참조하십시오.

- *Duo passcode(Duo* 암호*)* - Duo Mobile을 통해 생성되었거나 SMS를 통해 전송되었거나 하드웨어 토큰에 의해 생성되었거나 관리자가 제공한 암호를 사용하여 인증합니다. 1234567을 예로 들 수 있습니다.
- **push(**푸시**)** - Duo Mobile 앱을 설치하고 활성화한 경우 전화기에 로그인 요청을 푸시합니다. 요청을 검토하고 **Approve(**승인**)**를 눌러 로그인합니다.
- **phone(**전화기**)** - 전화기 콜백을 사용하여 인증합니다.
- **sms** - 텍스트 메시지로 Duo 암호를 요청합니다. 로그인 시도가 실패합니다. 새 암호를 사용하여 다시 로그인합니다.

Duo LDAP 사용에 대한 자세한 설명과 예는 Duo LDAP를 사용하여 이중 인증을 구성하는 방법, 768 페이지의 내용을 참조하십시오.

원격 액세스 VPN에 대한 라이선싱 요구 사항

기본 디바이스 라이선스가 내보내기 요구 사항을 충족해야 원격 액세스 VPN을 구성할 수 있습니다. 디바이스를 등록할 때는 내보내기 제어 기능에 대해 활성화된 Smart Software Manager 어카운트를 사용하여 등록을 수행해야 합니다. 또한, 평가 라이선스로는 기능을 구성할 수 없습니다.

그뿐만 아니라 AnyConnect Plus, AnyConnect Apex 또는 AnyConnect VPN Only 원격 액세스 VPN 라이선스도 구매하고 활성화해야 합니다. 이러한 라이선스는 threat defense 디바이스에 대해 동일하게 처리되지만, ASA 소프트웨어 기반 헤드엔드와 함께 사용할 때는 각기 다른 기능 집합을 허용하도록 설계되었습니다.

라이선스를 활성화하려면 디바이스 > 스마트 라이선스 > 컨피그레이션 보기를 선택한 다음 RA VPN 라이선스 그룹에서 적절한 라이선스를 선택합니다. Smart Software Manager 어카운트에 사용 가능한 라이선스가 있어야 합니다. 라이선스를 활성화하는 방법에 대한 자세한 내용은 선택 가능한 라이선스 활성화 또는 비활성화, 98 페이지를 참조하십시오.

자세한 내용은 *Cisco AnyConnect* 주문 가이드, http://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-og.pdf를 참조하십시오. http://www.cisco.com/c/en/us/products/security/anyconnect-secure-mobility-client/datasheet-listing.html에서는 다른 데이터 시트도 제공합니다.

원격 액세스 VPN에 대한 지침 및 제한 사항

RA VPN을 구성하는 경우 다음 지침과 제한 사항에 유의하십시오.

- 동일한 TCP 포트에 대한 동일한 인터페이스에서 device manager 액세스(관리 액세스 목록의 HTTPS 액세스)와 원격 액세스 SSL VPN을 모두 구성할 수는 없습니다. 예를 들어, 외부 인터페이스에서 원격 액세스 SSL VPN을 구성하는 경우, 포트 443에서 HTTPS 연결에 대한 외부 인터페이스도 열 수 없습니다. 동일한 인터페이스에서 두 기능을 모두 구성하는 경우 충돌을 방지하기 위해 이러한 서비스 중 하나 이상에 대해 HTTPS 포트를 변경해야 합니다.
- RA VPN 외부 인터페이스는 전역 설정입니다. 서로 다른 인터페이스에서 별도의 연결 프로파일을 구성할 수 없습니다.
- NAT 규칙의 소스 주소와 원격 액세스 VPN 주소 풀에서는 겹치는 주소를 사용할 수 없습니다.
- RADIUS 및 RSA 토큰을 사용하여 이중 인증을 구성하는 경우, 기본 인증 시간 제한 값인 12초는 너무 짧아 대부분의 경우 성공적인 인증을 허용하기 어렵습니다. 클라이언트 프로파일 구성 및 업로드, 734 페이지의 설명에 따라 맞춤형 Secure Client 프로파일을 생성한 다음 RA VPN 연결 프로파일에 적용하여 인증 시간 제한 값을 늘릴 수 있습니다. 사용자가 인증을 한 다음 RSA 토큰을 붙여넣고 토큰의 라운드트립을 확인할 수 있는 시간이 충분하도록 인증 시간 제한을 60초 이상으로 설정하는 것이 좋습니다.

원격 액세스 VPN 구성

클라이언트에 대한 원격 액세스 VPN을 활성화하려면 여러 개의 개별 항목을 구성해야 합니다. 다음 절차에서는 엔드 투 엔드 프로세스에 대해 설명합니다.

프로시저

단계 1 라이선스를 구성합니다.

두 개의 라이선스를 활성화해야 합니다.

- 디바이스를 등록할 때는 내보내기 제어 기능에 대해 활성화된 Smart Software Manager 어카운트를 사용하여 등록을 수행해야 합니다. 기본 라이선스가 내보내기 제어 요구사항을 충족해야 원격 액세스 VPN을 구성할 수 있습니다. 또한, 평가 라이선스로는 기능을 구성할 수 없습니다. 디바이스를 등록하는 절차는 디바이스 등록, 96 페이지를 참조하십시오.
- 원격 액세스 VPN 라이선스. 자세한 내용은 원격 액세스 VPN에 대한 라이선싱 요구 사항, 732 페이지를 참조해 주십시오. 라이선스를 활성화하려면 선택 가능한 라이선스 활성화 또는 비활성화, 98 페이지를 참조하십시오.

단계 2 인증서를 구성합니다.

클라이언트와 디바이스 간의 SSL 연결을 인증하려면 인증서가 필요합니다. VPN용으로 사전 정의된 DefaultInternalCertificate를 사용할 수도 있고 인증서를 직접 생성할 수도 있습니다.

인증에 사용되는 디렉터리 영역에 대해 암호화된 연결을 사용하는 경우에는 신뢰할 수 있는 CA 인증서를 업로드해야 합니다.

인증서 및 인증서를 업로드하는 방법에 관한 자세한 내용은 인증서 구성, 164 페이지를 참조하십시오.

단계 3 (선택 사항). TLS/SSL 설정 지정.

기본적으로 시스템은 원격 사용자가 지원하는 모든 TLS 버전 및 암호화 암호를 사용하여 원격 액세스 VPN에 연결할 수 있도록 허용합니다. 하지만 허용된 TLS/DTLS 버전, 암호 및 Diffie-Hellman 그룹을 제한하여 더 안전한 연결을 적용할 수 있습니다. TLS / SSL 암호 설정 설정, 851 페이지의 내용을 참조하십시오.

단계 4 (선택 사항). 클라이언트 프로파일 구성 및 업로드, 734 페이지에 전달하는 고성능 고속 어플라이언스입니다.

단계 5 원격 사용자 인증에 사용되는 ID 소스를 구성합니다.

원격 액세스 VPN 로그인이 허용되는 사용자 어카운트에 대해 다음 소스를 사용할 수 있습니다. 아니면 인증을 위해 클라이언트 인증서를 단독으로 또는 ID 소스와 함께 사용할 수 있습니다.

- AD(Active Directory) ID 영역 - 기본 인증 소스로 사용됩니다. AD(Active Directory) 서버에서 사용자 어카운트가 정의됩니다. AD ID 영역 구성, 177 페이지를 참조하십시오.
- RADIUS 서버 그룹 - 기본 또는 보조 인증 소스로서, 권한 부여 및 계정 관리를 위한 것입니다. RADIUS 서버 그룹 구성, 184 페이지를 참조하십시오.

- LocalIdentitySource - 기본 또는 대체 소스로 사용됩니다. 외부 서버를 사용하지 않고 디바이스에서 직접 사용자를 정의할 수 있습니다. 로컬 데이터베이스를 대체 소스로 사용하는 경우 외부 서버에 정의한 것과 같은 사용자 이름/비밀번호를 정의해야 합니다. 로컬 사용자 구성, 192 페이지를 참조하십시오.
- Duo LDAP 서버 - 기본 또는 보조 인증 소스로 사용됩니다. Duo LDAP 서버를 기본 소스로 사용할 수는 있지만 이는 일반적인 구성이 아닙니다. 일반적으로 이를 보조 소스로 사용하여 기본 Active Directory 또는 RADIUS 서버와 함께 이중 인증을 제공합니다. 자세한 내용은 Duo LDAP를 사용하여 이중 인증을 구성하는 방법, 768 페이지를 참조해 주십시오.

단계 **6** (선택 사항). RA VPN에 대한 그룹 정책 컨피그레이션, 749 페이지

그룹 정책에서는 사용자와 관련된 속성을 정의합니다. 그룹 멤버십에 근거하여 리소스에 차등 액세스를 제공하도록 그룹 정책을 컨피그레이션할 수 있습니다. 또는 모든 연결에 기본 정책을 사용할 수 있습니다.

단계 **7** RA VPN 연결 프로파일 컨피그레이션, 740 페이지.

단계 **8** 원격 액세스 VPN을 통한 트래픽 허용, 737 페이지.

단계 **9** 원격 액세스 VPN 컨피그레이션 확인, 737 페이지.

연결을 완료할 때 문제가 발생한 경우 원격 액세스 VPN 트러블슈팅, 756 페이지의 내용을 참조하십시오.

단계 **10** (선택 사항). ID 정책을 활성화하고 패시브 인증에 사용할 규칙을 생성합니다.

패시브 사용자 인증을 활성화하는 경우 원격 액세스 VPN을 통해 로그인한 사용자는 대시보드에 표시되며 정책에서 트래픽 일치 기준으로도 사용할 수 있게 됩니다. 패시브 인증을 활성화하지 않는 경우 RA VPN 사용자는 활성 인증 정책과 일치하는 경우에만 사용 가능합니다. 대시보드에서 또는 트래픽 일치용으로 사용자 이름 정보를 가져오려면 ID 정책을 활성화해야 합니다.

클라이언트 프로파일 구성 및 업로드

Secure Client 프로파일은 Secure Client 소프트웨어와 함께 클라이언트에 다운로드됩니다. 이러한 프로파일은 시작 시의 자동 연결 및 자동 다시 연결, 그리고 엔드 유저가 Secure Client 환경 설정 및 고급 설정에서 옵션을 변경할 수 있는지 여부와 같은 여러 클라이언트 관련 옵션을 정의합니다.

원격 액세스 VPN 연결을 구성할 때 외부 인터페이스의 FQDN(모든 자격을 갖춘 호스트 이름)을 구성하는 경우 시스템에서 클라이언트 프로파일을 생성합니다. 이 프로파일은 기본 설정을 활성화합니다. 기본 동작이 아닌 동작을 수행하려는 경우에만 클라이언트 프로파일을 생성하여 업로드하면 됩니다. 클라이언트 프로파일은 선택 사항이므로 업로드하지 않으면 Secure Client는 프로파일을 통해 제어되는 모든 옵션에 대해 기본 설정을 사용합니다.

참고 첫 번째 연결에서 Secure Client가 모든 사용자 제어 가능 설정을 표시하도록 하려면 VPN 프로파일의 서버 목록에 threat defense 디바이스의 외부 인터페이스를 포함해야 합니다. 프로파일에 있는 호스트 항목으로 FQDN 또는 주소를 추가하지 않은 경우, 필터가 세션에 적용되지 않습니다. 예를 들어 인증서 일치를 생성하고 인증서가 기준과 제대로 일치하지만 해당 프로파일에 있는 호스트 항목으로 디바이스를 추가하지 않는 경우, 인증서 일치가 무시됩니다.

AMP Enabler와 같이 Secure Client에서 선택적으로 사용할 수 있는 다양한 모듈 및 Secure Client에 대한 프로파일을 생성할 수 있습니다. 이러한 모듈에 대한 프로파일을 업로드할 수 있긴 하지만 device manager에서는 Secure Client 프로파일만 생성할 수 있습니다. 그러나 device manager을 통해 모든 종류의 프로파일을 업로드한 다음 API Explorer에서 threat defense API를 사용하여 개체의 프로파일 유형을 변경할 수 있습니다. 프로파일 페이지에는 모든 유형의 모든 프로파일이 표시되지만 목록에는 프로파일 유형이 표시되지 않습니다. 절차에서는 이를 수행하는 방법을 설명합니다.

다음 절차에서는 개체 페이지를 통해 개체를 직접 생성하고 수정할 수 있는 방법을 설명합니다. 개체 목록에 표시되는 새 보안 클라이언트 프로파일 생성 링크를 클릭하여 프로파일 속성을 수정하면서 Secure Client 프로파일 개체를 생성할 수도 있습니다.

시작하기 전에

클라이언트 프로파일을 업로드하려면 다음을 수행해야 합니다.

- 독립형 Secure Client "프로파일 편집기 - Windows/독립형 설치 관리자(MSI)"를 다운로드하여 설치합니다. 설치 파일은 Windows 전용이며 파일 이름은 anyconnect-profileeditor-win-<version>-k9.msi입니다. 여기서 <version>은 Secure Client 버전입니다(이에 따라 파일 이름 변경). 예를 들면 anyconnect-profileeditor-win-4.3.04027-k9.msi와 같습니다. 또한 프로파일 편집기를 설치하기 전에 Java JRE 1.6 이상도 설치해야 합니다. software.cisco.com에서 Secure Client 프로파일 편집기를 다운로드합니다. 이 패키지에는 VPN 클라이언트용 프로파일 편집기뿐만 아니라 모든 프로파일 편집기가 포함되어 있습니다.
- 프로파일 편집기를 사용하여 필요한 프로파일을 생성합니다. 프로파일에서 외부 인터페이스의 호스트 이름 또는 IP 주소를 지정해야 합니다. 자세한 내용은 편집기의 온라인 도움말을 참조하십시오.

프로시저

단계 **1** 목차에서 **Objects(**개체**)**와 **Secure Client Profile(**보안 클라이언트 프로파일**)**을 차례로 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 개체를 생성하려면 + 버튼을 클릭합니다.
- 개체를 수정하려면 개체의 수정 아이콘()을 클릭하십시오.
- 개체와 연결된 프로파일을 다운로드하려면 해당 개체의 다운로드 아이콘()을 클릭합니다.

참조되지 않는 개체를 삭제하려면 해당 개체의 휴지통 아이콘()을 클릭합니다.

단계 **3** 개체의 이름과 설명(선택 사항)을 입력합니다.

모듈 프로파일을 업로드하는 경우 Secure Client 프로파일과 쉽게 구분할 수 있도록 개체 이름을 사용하여 모듈 유형을 나타냅니다.

단계 **4** **Upload(**업로드**)**를 클릭하고 프로파일 편집기를 사용하여 생성한 파일을 선택합니다.

단계 **5** **Open(**열기**)**을 클릭하여 프로파일을 업로드합니다.

단계 **6** **OK(**확인**)**를 클릭하여 개체를 추가합니다.

단계 **7** 생성한 프로파일이 사실상 Secure Client 프로파일과 다른 유형인 경우 다음 단계를 완료하여 개체의 프로파일 유형을 변경하십시오.

a) More options(추가 옵션) 버튼(⋮)을 클릭하고 **API Explorer**를 선택합니다.

브라우저 설정에 따라 별도의 탭 또는 창에 API Explorer가 열립니다.

b) AnyConnectClientProfile 리소스를 엽니다.

c) GET /object /anyconnectclientprofiles 메소드를 선택하고 **Try It Out!(**시도**)** 버튼을 클릭합니다.

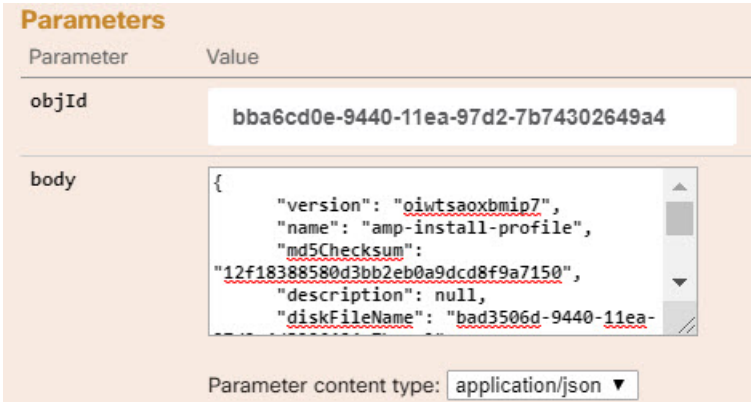
각 프로파일 개체는 다음과 같이 표시됩니다. 강조 표시된 특성이 변경해야 할 속성입니다.

```
{
      "version": "oiwtsaoxbmip7",
      "name": "amp-install-profile",
      "md5Checksum": "12f18388580d3bb2eb0a9dcd8f9a7150",
      "description": null,
      "diskFileName": "bad3506d-9440-11ea-97d2-4d3296494e7b.xml",
      "anyConnectModuleType": "ANY_CONNECT_CLIENT_PROFILE",
      "id": "bba6cd0e-9440-11ea-97d2-7b74302649a4",
      "type": "anyconnectclientprofile",
      "links": {
        "self": "https://10.89.5.38/api/fdm/v6/object/
anyconnectclientprofiles/bba6cd0e-9440-11ea-97d2-7b74302649a4"
      }
```

d) 출력에서 개체를 찾은 다음 코드를 선택하고 Ctrl + 클릭을 사용하여 이를 클립 보드에 복사합니다.

e) PUT / object/anyconnectclientprofiles/{objId} 메소드를 선택하고 **body** 필드에 내용을 붙여 넣습니다.

f) **ID** 값을 복사하여 본문 위의 **objId** 수정 상자에 붙여 넣습니다. "self" URL의 끝에서도 개체 ID를 찾을 수 있습니다.



g) 개체 본문에서 **anyConnectModuleType** 필드를 찾아 값을 프로파일 유형에 해당하는 값으로 바꿉니다. DART, FEEDBACK, WEB_SECURITY, ANY_CONNECT_CLIENT_PROFILE, AMP_ENABLER, NETWORK_ACCESS_MANAGER, NETWORK_VISIBILITY, START_BEFORE_LOGIN, ISE_POSTURE, UMBRELLA 중에서 선택합니다.

h) **body**에서 다시 **type** 값 뒤의 쉼표를 포함하여 **links** 특성을 삭제합니다.

개체 본문은 다음과 비슷해야 합니다.

```
{
      "version": "oiwtsaoxbmip7",
      "name": "amp-install-profile",
      "md5Checksum": "12f18388580d3bb2eb0a9dcd8f9a7150",
      "description": null,
      "diskFileName": "bad3506d-9440-11ea-97d2-4d3296494e7b.xml",
      "anyConnectModuleType": "AMP_ENABLER",
      "id": "bba6cd0e-9440-11ea-97d2-7b74302649a4",
      "type": "anyconnectclientprofile"
      }
```

i) **Try It Out!(**시도**)**을 클릭합니다. 응답을 검사하여 개체가 올바르게 수정되었는지 확인합니다. 응답 코드 200 및 변경 사항을 반영하는 응답 본문을 가져와야 합니다. GET 방법을 사용하여 결과를 추가로 확인할 수 있습니다.

원격 액세스 VPN을 통한 트래픽 허용

다음 기법 중 하나를 사용해 원격 액세스 VPN 터널에서 트래픽 흐름을 활성화할 수 있습니다.

- **sysopt connection permit-vpn** 명령을 컨피그레이션합니다. 이 명령에서는 VPN 연결과 일치하는 트래픽을 액세스 제어 정책에서 제외합니다. 이 명령의 기본값은 **no sysopt connection permit-vpn** 입니다. 이는 액세스 제어 정책에서도 VPN 트래픽을 허용해야 한다는 의미입니다.

  이 방법은 외부 사용자가 원격 액세스 VPN 주소 풀에서 IP 주소를 스푸핑할 수 없기 때문에 VPN에서 트래픽을 더 안전하게 허용할 수 있습니다. 하지만 VPN 트래픽이 검사되지 않는다는 단점이 있습니다. 즉, 침입 및 파일 보호, URL 필터링 또는 기타 고급 기능이 트래픽에 적용되지 않습니다. 즉 트래픽에 대해 연결 이벤트가 생성되지 않고, 따라서 통계 대시보드에 VPN 연결이 반영되지 않는다는 의미이기도 합니다.

  이 명령을 컨피그레이션하려면 RA VPN 연결 프로파일에서 **Bypass Access Control policy for decrypted traffic(**암호 해독된 트래픽에 대해 액세스 제어 정책 우회**)** 옵션을 선택하십시오.

- 원격 액세스 VPN 주소 풀에서 연결을 허용하는 액세스 제어 규칙을 생성합니다. 이 방법을 사용하는 경우 VPN 트래픽이 검사되며, 연결에 고급 서비스를 적용할 수 있습니다. 하지만 외부 사용자가 IP 주소를 스푸핑하여 내부 네트워크에 액세스할 가능성이 있다는 단점이 있습니다.

원격 액세스 VPN 컨피그레이션 확인

원격 액세스 VPN을 구성하고 디바이스에 컨피그레이션을 구축한 후에는 원격 연결을 수행할 수 있는지 확인합니다.

문제가 발생할 경우, 트러블슈팅 항목을 충분히 읽은 후 문제를 구분하고 해결합니다. 원격 액세스 VPN 트러블슈팅, 756 페이지를 참조하십시오.

프로시저

단계 **1** 외부 네트워크에서 Secure Client를 사용하여 VPN 연결을 설정합니다.

웹 브라우저를 사용하여 **https://***ravpn-address*를 엽니다. 여기서 *ravpn-address*는 VPN 연결을 허용할 외부 인터페이스의 IP 주소 또는 호스트 이름입니다. 필요한 경우, 클라이언트 소프트웨어를 설치하여 연결을 완료합니다. 사용자가 Secure Client 소프트웨어를 설치할 수 있는 방법, 727 페이지를 참조하십시오.

원격 액세스 VPN 연결용 포트를 변경한 경우 URL에 맞춤형 포트를 포함해야 합니다. 예를 들어 포트를 4443으로 변경한 경우 https://ravpn.example.com:4443과 같습니다.

그룹 URL을 컨피그레이션한 경우, 그룹 URL도 시도해 보십시오.

단계 **2** CLI(Command Line Interface) 로그인, 6 페이지에 설명된 대로 디바이스 CLI에 로그인합니다. 또는 CLI 콘솔을 여십시오.

단계 **3** **show vpn-sessiondb** 명령을 사용하여 현재 VPN 세션에 대한 요약 정보를 확인합니다.

통계에는 활성 Secure Client 세션, 누적 세션에 대한 정보, 최대 동시 세션 수, 비활성 세션이 표시되어야 합니다. 다음은 명령의 샘플 출력입니다.

```
> show vpn-sessiondb
--------------------------------------------------------------------------------
VPN Session Summary
--------------------------------------------------------------------------------
                            Active : Cumulative : Peak Concur : Inactive
                           ------------------------------------------------
AnyConnect Client          :      1 :         49 :           3 :        0
  SSL/TLS/DTLS             :      1 :         49 :           3 :        0
Clientless VPN             :      0 :          1 :           1
  Browser                  :      0 :          1 :           1
--------------------------------------------------------------------------------
Total Active and Inactive  :      1             Total Cumulative :     50
Device Total VPN Capacity  :  10000
Device Load                :     0%
--------------------------------------------------------------------------------

--------------------------------------------------------------------------------
Tunnels Summary
--------------------------------------------------------------------------------
                            Active : Cumulative : Peak Concurrent
                           ------------------------------------------------
Clientless                 :      0 :          1 :               1
AnyConnect-Parent          :      1 :         49 :               3
SSL-Tunnel                 :      1 :         46 :               3
DTLS-Tunnel                :      1 :         46 :               3
--------------------------------------------------------------------------------
Totals                     :      3 :        142
--------------------------------------------------------------------------------

--------------------------------------------------------------------------------
IPv6 Usage Summary
--------------------------------------------------------------------------------
```

```
                                Active : Cumulative : Peak Concurrent
                               ----------------------------------------
AnyConnect SSL/TLS/DTLS       :        :            :
  Tunneled IPv6               :      1 :         20 :           2
-------------------------------------------------------------------------
```

단계 **4** **show vpn-sessiondb anyconnect** 명령을 사용하여 현재 VPN 세션에 대한 세부 정보를 확인합니다.

세부 정보에는 사용된 암호화, 전송 및 수신한 바이트 수, 기타 통계 정보가 포함됩니다. VPN 연결을 사용하면 이 명령을 다시 호출할 경우 전송/수신한 바이트 수 변경 사항이 표시되어야 합니다.

```
> show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : priya                  Index        : 4820
Assigned IP  : 172.18.0.1             Public IP    : 192.168.2.20
Assigned IPv6: 2009::1
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256  DTLS-Tunnel: (1)AES256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 27731                  Bytes Rx     : 14427
Group Policy : MyRaVpn|Policy         Tunnel Group : MyRaVpn
Login Time   : 21:58:10 UTC Mon Apr 10 2017
Duration     : 0h:51m:13s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : c0a800fd012d400058ebfff2
Security Grp : none                   Tunnel Zone  : 0
```

원격 액세스 VPN 컨피그레이션 관리

원격 액세스 VPN 연결 프로파일에서는 외부 사용자가 Secure Client를 사용하여 시스템에 VPN 연결을 할 수 있게 허용하는 특성을 정의합니다. 각 프로파일에서 정의하는 것은 사용자를 인증하는 데 사용되는 AAA 서버 및 인증서, 사용자에게 IP 주소를 할당하기 위한 주소 풀, 다양한 사용자 중심 속성을 정의하는 그룹 정책입니다.

여러 사용자 그룹에 가변적인 서비스를 제공해야 하는 경우 또는 인증 소스가 여러 개인 경우, 프로파일을 여러 개 만듭니다. 예를 들어 조직이 다른 인증 서버를 사용하는 다른 조직과 병합하는 경우, 해당 인증 서버를 사용하는 새 그룹에 대해 프로파일을 만들 수 있습니다.

프로시저

단계 **1** **Device(**디바이스**)** > **Remote Access VPN(**원격 액세스 **VPN)** 그룹에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

현재 얼마나 많은 연결 프로파일 및 그룹 정책이 컨피그레이션되어 있는지 나타내는 요약 정보를 그룹에서 표시합니다.

단계 **2** 목차에서 **Connection Profiles(**연결 프로파일**)**을 아직 선택하지 않은 경우 클릭합니다.

단계 **3** 다음 중 하나를 수행합니다.

- + 버튼을 클릭하여 새 연결 프로파일을 생성합니다. 자세한 내용은 RA VPN 연결 프로파일 컨피그레이션, 740 페이지를 참고하십시오.
- 보기 버튼()을 클릭하여 연결 프로파일 및 연결 지침에 관한 요약 정보를 엽니다. 요약 정보 내에서 **Edit(**수정**)**을 클릭하여 변경할 수 있습니다.
- 삭제 버튼()을 클릭하여 더 이상 필요하지 않은 연결 프로파일을 삭제합니다.
- 목차에서 **Group Policies(**그룹 정책**)**를 선택하여 연결 프로파일에 대해 사용자 중심 속성을 정의합니다. RA VPN에 대한 그룹 정책 컨피그레이션, 749 페이지의 내용을 참조하십시오.

RA VPN 연결 프로파일 컨피그레이션

홈 네트워크 등의 외부 네트워크에 있는 사용자가 내부 네트워크에 연결할 수 있도록 원격 액세스 VPN 연결 프로파일을 생성할 수 있습니다. 다른 인증 방법을 수용하기 위해 별도 프로파일을 생성합니다.

시작하기 전에

RA(원격 액세스) VPN 연결을 구성하기 전에 다음 작업을 수행합니다.

- software.cisco.com에서 필요한 Secure Client 소프트웨어 패키지를 워크스테이션에 다운로드합니다.
- 원격 액세스 VPN 연결을 종료하는 외부 인터페이스가 동일한 포트에서 HTTPS 연결을 허용하는 관리 액세스 목록도 포함할 수는 없습니다. 관리 액세스를 위해 다른 포트를 구성하거나(데이터 인터페이스에서 관리 액세스에 대한 HTTPS 포트 구성, 812 페이지 참조) 연결 프로파일에 대해 다른 포트를 구성합니다. 두 서비스 모두 기본적으로 포트 443을 사용하므로 하나를 변경해야 합니다.

프로시저

단계 **1** **Device(**디바이스**)** > **Remote Access VPN(**원격 액세스 **VPN)** 그룹에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

현재 얼마나 많은 연결 프로파일 및 그룹 정책이 컨피그레이션되어 있는지 나타내는 요약 정보를 그룹에서 표시합니다.

단계 **2** 목차에서 **Connection Profiles(**연결 프로파일**)**을 아직 선택하지 않은 경우 클릭합니다.

단계 **3** 다음 중 하나를 수행합니다.

- + 버튼을 클릭하여 새 연결 프로파일을 생성합니다.

- 보기 버튼( )을 클릭하여 연결 프로파일 및 연결 지침에 관한 요약 정보를 엽니다. 요약 정보 내에서 **Edit(**수정**)**을 클릭하여 변경할 수 있습니다.

단계 **4** 기본 연결 속성을 컨피그레이션합니다.

- **Connection Profile Name(**연결 프로파일 이름**)** — 이 연결의 이름을 공백 없이 50자까지 입력합니다. 예를 들면 MainOffice를 입력합니다. IP 주소는 이름으로 사용할 수 없습니다.

  참고 여기서 입력하는 이름이 Secure Client 클라이언트에서 사용자에게 표시되는 연결 목록에 나타납니다. 따라서 사용자가 쉽게 이해할 수 있는 이름을 선택해야 합니다.

- **Group Alias(**그룹 별칭**)**, **Group URL(**그룹 **URL)** — 별칭에는 특정 연결 프로파일에 대한 대체 이름 또는 URL이 포함되어 있습니다. threat defense 디바이스에 연결하는 경우, VPN 사용자는 연결 목록의 Secure Client 클라이언트에서 별칭 이름을 선택할 수 있습니다. 연결 프로파일 이름이 그룹 별칭으로 자동 추가됩니다. 별칭은 최대 31자입니다.

  또한 원격 액세스 VPN 연결을 시작하는 동안 엔드포인트에서 선택할 수 있는 그룹 URL의 목록을 컨피그레이션할 수 있습니다. 사용자가 그룹 URL을 사용하여 연결하는 경우, 시스템에서는 URL과 일치하는 연결 프로파일을 자동으로 사용합니다. 이 URL은 설치된 Secure Client 클라이언트가 아직 없는 클라이언트에서 사용됩니다.

  그룹 별칭 및 URL을 필요한 만큼 추가하십시오. 이러한 별칭 및 URL은 디바이스에 정의된 모든 연결 프로파일 전반에 걸쳐 고유한 것이어야 합니다. 그룹 URL은 **https://**로 시작해야 합니다.

  예를 들어 별칭 계약자 및 그룹 URL https://ravpn.example.com/contractor가 있을 수 있습니다. Secure Client 클라이언트가 설치된 후 사용자는 연결의 Secure Client VPN 드롭다운 목록에서 그룹 별칭을 선택하기만 하면 됩니다.

단계 **5** 기본 ID 소스를 컨피그레이션하고, 선택적으로 보조 ID 소스를 컨피그레이션합니다.

이 옵션을 통해 원격 사용자가 원격 액세스 VPN 연결을 활성화하기 위해 디바이스에 인증하는 방식을 결정합니다. 가장 간단한 방식은 AAA만 사용하여 AD 영역을 선택하거나 LocalIdentitySource를 사용하는 것입니다. **Authentication Type(**인증 유형**)**에는 다음과 같은 방식을 사용할 수 있습니다.

- **AAA Only(AAA**만**)** — 사용자 이름 및 암호에 근거하여 사용자를 인증하고 사용자에게 권한을 부여합니다. 자세한 내용은 연결 프로파일에 대해 AAA 컨피그레이션, 744 페이지 섹션을 참조해 주십시오.
- **Client Certificate Only(**클라이언트 인증서만**)** — 클라이언트 디바이스 ID 인증서에 근거하여 사용자를 인증합니다. 자세한 내용은 연결 프로파일에 대한 인증서 인증 컨피그레이션, 747 페이지 섹션을 참조해 주십시오.
- **AAA and ClientCertificate(AAA** 및 **ClientCertificate)** — 사용자 이름/암호와 클라이언트 디바이스 ID 인증서를 모두 사용합니다.
- **SAML** — 기본 인증에서 SAML 서버를 사용합니다. SAML을 사용할 때는 대체 또는 보조 인증 소스를 구성할 수 없습니다. 자세한 내용은 연결 프로파일에 대해 AAA 컨피그레이션, 744 페이지를 참조해 주십시오.

단계 **6** 클라이언트에 대해 주소 풀을 컨피그레이션합니다.

주소 풀에서는 원격 클라이언트가 VPN 연결을 설정할 때 시스템에서 원격 클라이언트에 할당할 수 있는 IP 주소를 정의합니다. 자세한 내용은 RA VPN에 대한 클라이언트 주소 지정 컨피그레이션, 748 페이지를 참고하십시오.

단계 **7** **Next(**다음**)**를 클릭합니다.

단계 **8** 이 프로파일에 사용할 **Group Policy(**그룹 정책**)**를 선택합니다.

그룹 정책에서는 터널이 설정된 후에 사용자 연결에 대한 조건을 설정합니다. 시스템에는 DfltGrpPolicy라는 이름의 기본 그룹 정책이 포함되어 있습니다. 필요한 서비스를 제공하는 추가 그룹 정책을 만들 수 있습니다.

그룹 정책을 선택하는 경우, 그룹 특성에 관한 요약 정보가 표시됩니다. 변경하려면 요약 정보에서 **Edit(**수정**)**을 클릭합니다.

필요한 그룹 정책이 아직 없는 경우, 드롭다운 목록에서 **Create New Group Policy(**새 그룹 정책 생성**)**를 클릭합니다.

그룹 정책에 대한 세부 정보는 RA VPN에 대한 그룹 정책 컨피그레이션, 749 페이지의 내용을 참조하십시오.

단계 **9** **Next(**다음**)**를 클릭합니다.

단계 **10** 전역 설정을 구성합니다.

이 옵션은 모든 연결 프로파일에 적용됩니다. 첫 번째 연결 프로파일을 만들고 나면 각 후속 프로파일에 대해 이 옵션이 사전 컨피그레이션됩니다. 변경하는 경우, 컨피그레이션된 모든 연결 프로파일이 변경됩니다.

- **Certificate of Device Identity(**디바이스 **ID**의 인증서**)** — 디바이스의 ID를 설정하는 데 사용되는 내부 인증서를 선택합니다. 보안 VPN 연결을 완료하려면 클라이언트가 이 인증서를 허용해야 합니다. 인증서가 아직 없는 경우 드롭다운 목록에서 **Create New Internal Certificate(**새 내부 인증서 생성**)**를 클릭합니다. 인증서를 구성해야 합니다.

- **Outside Interface(**외부 인터페이스**)** - 사용자가 원격 액세스 VPN 연결을 설정할 때 연결하는 인터페이스입니다. 이 인터페이스는 대개 외부(인터넷 연결) 인터페이스이지만, 지원하려는 디바이스와 엔드 유저 간의 인터페이스를 선택하면 됩니다.

- 외부 인터페이스의 **FQDN(Fully-Qualified Domain Name)** - ravpn.example.com과 같은 인터페이스의 이름입니다. 이름을 지정하는 경우 시스템이 클라이언트 프로파일을 자동으로 생성할 수 있습니다.

  참고 VPN과 클라이언트에 사용되는 DNS 서버가 외부 인터페이스 IP 주소에 대해 이 이름을 확인할 수 있도록 해야 합니다. 관련 DNS 서버에 FQDN을 추가합니다.

- **Port(**포트**)** — RA VPN 연결에 사용할 TCP 포트입니다. 기본값은 443입니다. RA VPN에 사용된 것과 동일한 인터페이스에서 device manager에 연결해야 하는 경우 연결 프로파일 또는 device manager의 포트 번호를 변경해야 합니다. 두 서비스 모두 기본적으로 443을 사용합니다. 원격 액세스 VPN 연결용 포트를 변경하는 경우 사용자가 URL에 포트 번호를 포함해야 합니다.

- **Bypass Access Control policy for decrypted traffic(**암호 해독된 트래픽에 대해 액세스 제어 정책 우회**)(sysopt permit-vpn)** - VPN 트래픽을 액세스 제어 정책에 종속시킬지 여부. 암호 해독된 VPN 트래픽에는 기본적으로 액세스 제어 정책 검사가 적용됩니다. **Bypass Access Control policy for**

decrypted traffic(암호 해독된 트래픽에 대해 액세스 제어 정책 우회**)** 옵션을 활성화하면 액세스 제어 정책을 우회하지만, 원격 액세스 VPN의 경우에는 VPN 필터 ACL과 AAA 서버에서 다운로드한 인증 ACL이 VPN 트래픽에 계속 적용됩니다.

이 옵션을 선택하는 경우, 시스템에서는 전역 설정인 **sysopt connection permit-vpn** 명령을 컨피그레이션한다는 점에 유의하십시오. 이로 인해 Site-to-Site VPN 연결의 동작도 영향을 받습니다. 또한 연결 프로파일 전반에서 이 옵션에 대해 서로 다른 항목을 선택할 수 없습니다. 즉 모든 프로파일에 대해 기능을 켜거나 꺼야 합니다.

이 옵션을 선택하지 않는 경우, 외부 사용자가 원격 액세스 VPN 주소 풀의 IP 주소를 스푸핑할 수 있고, 따라서 네트워크에 액세스할 수 있습니다. 이것이 가능한 이유는 주소 풀에서 내부 리소스에 액세스할 수 있게 허용하는 액세스 제어 규칙을 생성해야 하기 때문입니다. 액세스 제어 규칙을 사용하는 경우, 소스 IP 주소만 사용하기보다 사용자 사양을 이용해 액세스를 제어하는 것이 좋습니다.

이 옵션을 선택할 경우의 단점은 VPN 트래픽이 검사되지 않는다는 것입니다. 즉 침입 및 파일 보호, URL 필터링 또는 기타 고급 기능이 트래픽에 적용되지 않습니다. 즉 트래픽에 대해 연결 이벤트가 생성되지 않고, 따라서 통계 대시보드에 VPN 연결이 반영되지 않는다는 의미이기도 합니다.

- **NAT Exempt(NAT** 제외**)** - NAT 변환에서 원격 액세스 VPN 엔드포인트와 주고받는 트래픽을 제외하려면 NAT 제외를 활성화합니다. NAT에서 VPN 트래픽을 제외하지 않는 경우 내부 인터페이스와 외부 인터페이스에 대한 기존 NAT 규칙이 주소의 RA VPN 풀에 적용되지 않는지 확인합니다. NAT 제외 규칙은 지정된 소스/대상 인터페이스 및 네트워크 조합에 대한 수동 고정 ID NAT 규칙이며 NAT 정책에서는 반영되지 않고 숨겨집니다. NAT 제외를 활성화하는 경우에는 다음 항목도 구성해야 합니다.

  이것은 전역 옵션이므로 모든 연결 프로파일에 적용된다는 점에 유의하십시오. 따라서 인터페이스와 내부 네트워크를 추가하기만 하고 교체하지 마십시오. 그러지 않으면 이미 정의한 다른 모든 연결 프로파일에 대한 NAT 제외 설정이 변경됩니다.

  - 내부 인터페이스 - 원격 사용자가 액세스할 내부 네트워크의 인터페이스를 선택합니다. NAT 규칙은 이러한 인터페이스에 대해 생성됩니다.
  - 내부 네트워크 - 원격 사용자가 액세스할 내부 네트워크를 나타내는 네트워크 개체를 선택합니다. 네트워크 목록에는 지원할 주소 풀과 동일한 IP 유형이 포함되어 있어야 합니다.

- **Secure Client Package(**보안 클라이언트 패키지**)** - RA VPN 연결에서 지원할 Secure Client 전체 설치 소프트웨어 이미지입니다. 각 패키지의 파일 이름(확장자 포함)은 60자 이하여야 합니다. Windows, Mac 및 Linux 엔드포인트에 대해 별도의 패키지를 업로드할 수 있습니다. 그러나 여러 연결 프로파일에 대해 여러 패키지를 컨피그레이션할 수는 없습니다. 다른 프로파일에 대해 패키지를 이미 컨피그레이션한 경우, 패키지가 미리 선택되어 있습니다. 패키지를 변경하면 모든 프로파일에 대해 변경이 이루어집니다.

  패키지는 software.cisco.com에서 다운로드합니다. 엔드포인트에 적합한 패키지가 아직 설치되어 있지 않으면 사용자에게 사용자 인증 후 패키지를 다운로드하여 설치하라는 메시지가 표시됩니다.

단계 **11** **Next(**다음**)**를 클릭합니다.

단계 **12** 요약을 검토합니다.

먼저 요약이 정확한지 확인합니다.

그런 다음 지침을 클릭하여 Secure Client 소프트웨어를 처음으로 설치하고 VPN 연결을 완료할 수 있는지를 테스트하기 위해 엔드 유저가 수행해야 하는 작업을 파악합니다. 복사를 클릭하여 이러한 지침을 클립보드에 복사한 다음 사용자에게 배포합니다.

단계 **13** **Finish(**마침**)**를 클릭합니다.

다음에 수행할 작업

원격 액세스 VPN을 통한 트래픽 허용, 737 페이지의 설명대로 VPN 터널에서 트래픽이 허용되는지 확인합니다.

연결 프로파일에 대해 **AAA** 컨피그레이션

인증, 권한 부여, 계정 관리 (AAA) 서버에서는 사용자 이름과 암호를 사용하여 사용자에게 원격 액세스 VPN에 대한 액세스가 허용되어 있는지 확인합니다. RADIUS 서버를 사용하는 경우, 인증된 사용자들 사이에서 권한 부여 수준을 구별하여 보호받는 리소스에 대한 차등 액세스를 제공할 수 있습니다. 또한 RADIUS 계정 관리 서비스를 사용하여 사용량을 추적할 수 있습니다.

AAA를 컨피그레이션하는 경우, 기본 ID 소스를 컨피그레이션해야 합니다. 보조 및 대체 소스는 선택 사항입니다. 이중 인증을 구현하려면 RSA 토큰 또는 듀오와 같은 보조 소스를 사용하십시오.

기본 **ID** 소스 옵션

- **Primary Identity Source for User Authentication(**사용자 인증을 위한 기본 **ID** 소스**)** - 원격 사용자 인증에 사용되는 기본 ID 소스입니다. VPN 연결을 완료하려면 이 소스 또는 대체 소스(선택 사항)에서 최종 사용자를 정의해야 합니다. 다음 중 하나를 선택합니다.
  - AD(Active Directory) ID 영역. 필요한 영역이 아직 없는 경우, **Create New Identity Realm(**새 **ID** 영역 생성**)**을 클릭합니다.
  - Radius 서버 그룹.
  - LocalIdentitySource(로컬 사용자 데이터베이스) - 외부 서버를 사용하지 않고 디바이스에서 직접 사용자를 정의할 수 있습니다.
  - Duo LDAP 서버. 그러나 이 서버는 Duo LDAP를 사용하여 이중 인증을 구성하는 방법, 768 페이지에 설명된 대로 이중 인증을 제공하기 위한 보조 인증 소스로 사용되는 것이 가장 바람직합니다. 이 서버를 기본 소스로 사용하는 경우 사용자 ID 정보를 가져올 수 없고, 대시보드에 사용자 정보가 표시되지 않으며, 사용자 기반 액세스 제어 규칙을 작성할 수도 없습니다.
  - SAML 서버 SAML 서버를 사용하는 경우 대체 또는 보조 인증 소스를 구성할 수 없습니다. RADIUS를 권한 부여 서버로 사용할 수 있지만 인증이 필요하지 않도록 RADIUS 서버를 구성해야 합니다. 즉, RADIUS 서버는 SAML에서 연결을 인증한 후 권한 부여 정보를 제공합니다.

- **SAML Login Experience(SAML** 로그인 환경**)** - SAML을 기본 인증 소스로 선택한 경우 웹 인증을 완료하는 데 사용할 클라이언트 브라우저를 선택해야 합니다.
  - **VPN Client embedded browser(VPN** 클라이언트 임베디드 브라우저**)** - VPN 클라이언트는 웹 인증을 위해 임베디드 브라우저를 사용하므로 인증은 VPN 연결에만 적용됩니다. 이는 기본값이며 추가로 구성할 필요가 없습니다.
  - **Default OS Browser(**기본 **OS** 브라우저**)** - VPN 클라이언트는 웹 인증을 위해 시스템의 기본 브라우저를 사용합니다. 이 옵션은 VPN 인증과 기타 기업 로그인 간에 SSO(Single Sign-On)를 활성화합니다. 생체 인증과 같이 임베디드 브라우저에서 수행할 수 없는 웹 인증 방법을 지원하고자 하는 경우 이 옵션을 선택합니다.

    브라우저에서 웹 인증을 활성화하는 패키지를 업로드해야 합니다. 패키지는 software.cisco.com에서 다운로드합니다. 업로드하는 패키지는 SAML을 기본 OS 브라우저와 함께 사용하는 모든 연결 프로파일에서 사용됩니다. 패키지는 전역이며, 연결 프로파일에 한정되지 않습니다.

- **Fallback Local Identity Source(**대체 로컬 **ID** 소스**)** - 기본 소스가 외부 서버인데 기본 서버를 사용할 수 없는 경우, 대체 소스로 LocalIdentitySource를 선택할 수 있습니다. 로컬 데이터베이스를 대체 소스로 사용하는 경우 외부 서버에 정의한 것과 같은 로컬 사용자 이름/비밀번호를 정의해야 합니다.

Advanced options(고급 옵션**)** - **Advanced(**고급**)** 링크를 클릭하고 다음 옵션을 구성합니다.

- **Strip options(**제거 옵션**)** - 영역은 관리 도메인입니다. 다음 옵션을 활성화하면 사용자 이름에만 근거하여 인증할 수 있습니다. 이러한 옵션의 조합을 활성화할 수 있습니다. 그러나 서버에서 구분 기호를 구문 분석할 수 없는 경우, 두 확인란을 모두 선택해야 합니다.
  - **Strip Identity Source Server from Username(**사용자 이름에서 **ID** 소스 서버 제거**)** - AAA 서버로 사용자 이름을 전달하기 전에 사용자 이름에서 ID 소스 이름을 제거할지 여부. 예를 들어 이 옵션을 선택하고 사용자가 도메인\사용자 이름을 사용자 이름으로 입력하는 경우, 도메인은 사용자 이름에서 제거되고 인증을 위해 AAA 서버로 전송됩니다. 기본적으로 이 옵션은 선택되어 있지 않습니다.
  - **Strip Group from Username(**사용자 이름에서 그룹 제거**)** - AAA 서버로 사용자 이름을 전달하기 전에 사용자 이름에서 그룹 이름을 제거할지 여부. 이 옵션은 username@domain 형식에서 지정된 이름에 적용되며, 도메인 및 @ 기호를 제거합니다. 기본적으로 이 옵션은 선택되어 있지 않습니다.

- **Enable Password Management(**비밀번호 관리 활성화**)** - 비밀번호가 만료될 때 사용자가 비밀번호를 변경할 수 있는지 여부를 설정합니다. 이 옵션을 선택하지 않으면 사용자의 비밀번호가 만료될 때 Secure Client는 연결을 거부하며 사용자는 AAA 서버에서 비밀번호를 변경해야 합니다. 이 옵션을 선택하면 비밀번호가 만료될 때 Secure Client에서 사용자에게 비밀번호를 변경하라는 메시지가 표시되므로 사용자에게 훨씬 더 편리합니다. 다음 옵션 중 하나를 선택합니다. 또한 AAA 서버에서 MSCHAPv2를 활성화해야 합니다.
  - **Notify user x days before password expiration(**비밀번호 만료 **x**일 전에 사용자에게 알림**)**(LDAP만 해당) - 지정한 일 수부터 시작하여 사용자에게 비밀번호 만료를 경고합니다. 1일에서 180일 사이로 설정할 수 있으며, 기본값은 14일입니다.

- **Notify user on the day of password expiration(**비밀번호 만료일에 사용자에게 알림**)** - 사용자에게 경고가 표시되지 않지만 비밀번호가 만료되면 비밀번호를 변경하라는 메시지가 계속 표시됩니다. 경고 기간을 설정하더라도 RADIUS 사용자는 항상 이 동작을 수행합니다.

보조 **ID** 소스

- **Secondary Identity Source for User Authorization(**사용자 권한 부여를 위한 보조 **ID** 소스**)** - 두 번째 ID 소스로서 선택 사항입니다. 사용자가 기본 소스로 인증에 성공하는 경우, 사용자에게 보조 소스를 사용해 인증하라는 메시지가 표시됩니다. AD 영역, RADIUS 서버 그룹, Duo LDAP 서버 또는 로컬 ID 소스를 선택할 수 있습니다.
- **Advanced options(**고급 옵션**)** - **Advanced(**고급**)** 링크를 클릭하고 다음 옵션을 컨피그레이션합니다.
  - **Fallback Local Identity Source for Secondary(**보조용 대체 시스템 로컬 **ID** 소스**)** - 보조 소스가 외부 서버인데 보조 서버를 사용할 수 없는 경우, LocalIdentitySource를 대체 소스로 선택할 수 있습니다. 로컬 데이터베이스를 대체 소스로 사용하는 경우, 보조 외부 서버에 정의한 것과 같은 로컬 사용자 이름/암호를 정의해야 합니다.
  - **Use Primary Username for Secondary Login(**보조 로그인에 기본 사용자 이름 사용**)** - 보조 ID 소스를 사용하는 경우, 시스템에서는 기본적으로 보조 소스에 대한 사용자 이름 및 암호를 모두 입력하라는 메시지를 표시합니다. 이 옵션을 선택하는 경우, 시스템에서는 보조 암호만 입력하라는 메시지를 표시하고 기본 ID 소스에 대해 인증된 보조 소스에 동일한 사용자 이름을 사용합니다. 기본 및 보조 ID 소스 모두에서 동일한 사용자 이름을 컨피그레이션하는 경우, 이 옵션을 선택합니다.
  - **Username for Session Server(**세션 서버의 사용자 이름**)** - 인증에 성공하면 사용자 이름이 이벤트 및 통계 대시보드에 표시되고, 이 이름은 사용자 또는 그룹 기반 SSL 암호 해독 및 액세스 제어 규칙에 대한 일치 여부를 확인하고 계정을 관리하는 데 사용됩니다. 두 가지 인증 소스를 사용하고 있기 때문에 기본 또는 보조 사용자 이름을 사용자 ID로 사용할지 여부를 시스템에 알려주어야 합니다. 기본적으로 기본 이름을 사용합니다.
  - **Password Type(**암호 유형**)** - 보조 서버의 암호를 가져오는 방법. 이 필드는 인증 유형으로 **AAA and Client Certificate(AAA** 및 클라이언트 인증서**)**를 선택한 경우에만 적용되며, 인증서 옵션의 경우 **Prefill username from certificate on user login window(**인증서의 사용자 이름을 사용자 로그인 창에 미리 채우기**)** 및 **Hide username in login window(**로그인 창에서 사용자 이름 숨기기**)**를 모두 선택합니다. 기본값은 **Prompt(**프롬프트**)**입니다. 이는 사용자에게 암호를 입력하라는 메시지가 표시됨을 뜻합니다.

    사용자가 기본 서버에 인증할 때 입력한 암호를 자동으로 사용하려면 **Primary Identity Source Password(**기본 **ID** 소스 암호**)**를 선택합니다.

    모든 사용자에 대해 동일한 암호를 사용하려면 **Common Password(**공통 암호**)**를 선택한 다음, **Common Password(**공통 암호**)** 필드에 해당 암호를 입력합니다.

추가 옵션

- **Authorization Server(**권한 부여 서버**)** - 원격 액세스 VPN 사용자를 인증하도록 컨피그레이션된 RADIUS 서버 그룹.

  인증이 완료되면 권한 부여 기능에서 인증된 각 사용자에게 사용할 수 있는 서비스 및 명령을 제어합니다. 권한 부여 기능은 사용자가 수행할 수 있도록 인가를 받은 것이 무엇인지, 즉 사용자의 실제 능력 및 제한 사항을 설명하는 일련의 속성을 결합함으로써 작동합니다. 권한 부여 기능을 사용하지 않는 경우, 인증 기능에서만 인증된 모든 사용자에게 동일한 액세스 권한을 제공합니다. 권한 부여를 위한 RADIUS 컨피그레이션에 대한 정보는 RADIUS 및 그룹 정책을 이용한 사용자 권한 및 속성 제어, 728 페이지의 내용을 참조하십시오.

  시스템이 그룹 정책에 정의된 것과 중복되는 권한 부여 속성을 RADIUS 서버에서 가져오는 경우, RADIUS 속성은 그룹 정책 속성을 재정의한다는 점에 유의하십시오.

- **Accounting Server(**과금 서버**)** - (선택 사항) 원격 액세스 VPN 세션에 대한 계정 관리에 사용할 RADIUS 서버 그룹입니다.

  계정 관리 기능에서는 사용자가 액세스 중인 서비스뿐 아니라 사용 중인 네트워크 리소스의 양까지도 추적합니다. threat defense 디바이스에서는 RADIUS 서버에 사용자 활동을 보고합니다. 계정 관리 정보에는 세션 시작 및 중지 시각, 사용자 이름, 각 세션의 디바이스를 통과한 바이트 수, 사용한 서비스, 각 세션의 지속시간이 포함됩니다. 네트워크 관리, 클라이언트 요금 청구 또는 감사에 대한 데이터를 분석할 수 있습니다. 관리 계정 기능을 단독으로 사용하거나 인증 및 권한 부여 기능과 함께 사용할 수 있습니다.

연결 프로파일에 대한 인증서 인증 컨피그레이션

클라이언트 디바이스에 설치된 인증서를 사용해 원격 액세스 VPN 연결을 인증할 수 있습니다. 인증서 인증을 사용하는 경우 원격 액세스 사용자 연결을 검증하는 데 사용되는 신뢰할 수 있는 CA 인증서에 **Validation Usage(**검증 사용**)**에 대한 **SSL Client(SSL** 클라이언트**)** 옵션이 포함되어 있는지 확인합니다.

클라이언트 인증서를 사용하는 경우에도 보조 ID 소스, 대체 소스, 권한 부여 및 과금 서버를 컨피그레이션할 수 있습니다. 이 옵션은 AAA 옵션입니다. 자세한 내용은 연결 프로파일에 대해 AAA 컨피그레이션, 744 페이지의 내용을 참조하십시오.

다음은 인증서별 속성입니다. 기본 및 보조 ID 소스에 대해 개별적으로 이러한 속성을 컨피그레이션할 수 있습니다. 보조 소스 컨피그레이션은 선택 사항입니다.

- **Username from Certificate(**인증서의 사용자 이름**)** - 다음 중 하나를 선택하십시오.

  - **Map Specific Field(**특정 필드 매핑**)** - **Primary Field(**기본 필드**)** 및 **Secondary Field(**보조 필드**)**의 순서대로 인증서 요소를 사용합니다. 기본값은 CN(Common Name) 및 OU(Organizational Unit)입니다. 조직에 대해 작동하는 옵션을 선택합니다. 필드는 서로 결합하여 사용자 이름을 제공하고, 이 이름은 이벤트, 대시보드에서 사용되며 SSL 암호 해독 및 액세스 제어 규칙에서 일치 목적으로 사용됩니다.

  - **Use entire DN (distinguished name) as username(**전체 **DN(**고유 이름**)**을 사용자 이름으로 사용**)** - 시스템은 DN 필드에서 사용자 이름을 자동으로 파생합니다.

- **Advanced options(**고급 옵션**)** - **Advanced(**고급**)** 링크를 클릭하고 다음 옵션을 컨피그레이션합니다.
  - **Prefill username from certificate on user login window(**인증서의 사용자 이름을 사용자 로그인 창에 미리 채우기**)** - 사용자에게 인증하라는 메시지를 표시할 때 사용자 이름 필드에 검색된 사용자 이름을 입력할지 여부.
  - **Hide username in login window(**로그인 창에서 사용자 이름 숨기기**)** - **Prefill(**미리 채우기**)** 옵션을 선택하면 사용자 이름을 숨길 수 있습니다. 따라서 사용자는 암호 프롬프트에서 사용자 이름을 수정할 수 없습니다.

RA VPN에 대한 클라이언트 주소 지정 컨피그레이션

원격 액세스 VPN에 연결하는 엔드포인트에 대한 IP 주소를 시스템에서 제공할 방법이 있어야 합니다. 이 주소는 AAA 서버, DHCP 서버, 그룹 정책에 컨피그레이션된 IP 주소 풀 또는 연결 프로파일에 컨피그레이션된 IP 주소 풀에서 제공할 수 있습니다. 시스템은 순서대로 이 리소스를 시도하고 사용 가능한 주소를 가져올 때 중지했다가 이 주소를 클라이언트에 할당합니다. 따라서 동시 연결 수가 비정상적인 경우에 페일세이프를 생성할 수 있는 여러 가지 옵션을 컨피그레이션할 수 있습니다.

연결 프로파일에 대한 주소 풀을 컨피그레이션하려면 다음 방법 중 한 가지 이상을 사용하십시오.

- **AAA** 서버 - 먼저 주소 풀에 대한 서브넷을 지정하는 threat defense 디바이스에서 네트워크 개체를 컨피그레이션합니다. 그런 다음, RADIUS 서버에서 개체 이름으로 사용자에 대한 Address-Pools(217) 속성을 컨피그레이션합니다. 또한 연결 프로파일에서 인증용 RADIUS 서버를 지정합니다.
- **DHCP** - 먼저 RA VPN에 대한 IPv4 주소 범위를 하나 이상 사용하여 DHCP 서버를 컨피그레이션합니다(DHCP를 사용하여 IPv6 풀을 컨피그레이션할 수는 없음). 그런 다음, DHCP 서버의 IP 주소로 호스트 네트워크 개체를 생성합니다. 그러면 연결 프로파일의 **DHCP Servers(DHCP** 서버**)** 속성에서 이 개체를 선택할 수 있습니다. 최대 10개의 DHCP 서버를 설정할 수 있습니다.

  DHCP 서버에 주소 풀이 여러 개인 경우, 연결 프로파일에 연결하는 그룹 정책에서 **DHCP Scope(DHCP** 범위**)** 속성을 사용해 어떤 풀을 사용할지 선택할 수 있습니다. 풀의 네트워크 주소로 호스트 네트워크 개체를 생성합니다. 예를 들어 DHCP 풀에 192.168.15.0/24 및 192.168.16.0/24가 포함된 경우, DHCP 범위를 192.168.16.0으로 설정하면 192.168.16.0/24 서브넷에서 주소가 선택됩니다.
- 로컬 **IP** 주소 풀 - 먼저 서브넷을 지정하는 네트워크 개체를 최대 6개 생성합니다. IPv4 및 IPv6에 대해 별도 풀을 컨피그레이션할 수 있습니다. 그런 다음, 그룹 정책 또는 연결 프로파일의 **IPv4 Address Pool(IPv4** 주소 풀**)** 및 **IPv6 Address Pool(IPv6** 주소 풀**)** 옵션에서 이러한 개체를 선택합니다. IPv4 및 IPv6 모두 컨피그레이션할 필요는 없고 지원하려는 주소 체계만 컨피그레이션하면 됩니다.

  또한 그룹 정책 및 연결 프로파일 모두에서 풀을 컨피그레이션할 필요는 없습니다. 그룹 정책에서는 연결 프로파일 설정을 재정의하므로 그룹 정책에서 풀을 컨피그레이션하는 경우, 연결 프로파일에서 옵션을 비워두십시오.

  풀은 나열한 순서대로 사용된다는 점에 유의하십시오.

RA VPN에 대한 그룹 정책 컨피그레이션

그룹 정책은 원격 액세스 VPN 연결에 대한 일련의 사용자 중심 속성/값 쌍입니다. 연결 프로파일에서는 터널이 설정된 후 사용자 연결에 대해 조건을 설정하는 그룹 정책을 사용합니다. 그룹 정책을 사용하면 각 사용자에 대해 개별적으로 각 특성을 지정할 필요 없이 사용자 또는 사용자 그룹에 전체 특성 집합을 적용할 수 있습니다.

시스템에는 DfltGrpPolicy라는 이름의 기본 그룹 정책이 포함되어 있습니다. 필요한 서비스를 제공하는 추가 그룹 정책을 만들 수 있습니다.

프로시저

단계 **1** **Device(**디바이스**)** > **Remote Access VPN(**원격 액세스 **VPN)** 그룹에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

현재 얼마나 많은 연결 프로파일 및 그룹 정책이 컨피그레이션되어 있는지 나타내는 요약 정보를 그룹에서 표시합니다.

단계 **2** 목차에서 **Group Policies(**그룹 정책**)**를 클릭합니다.

단계 **3** 다음 중 하나를 수행합니다.

- + 버튼을 클릭하여 새 그룹을 생성합니다. 그룹 정책 페이지에서 속성에 대한 설명은 다음 주제를 참조하십시오.
  - 일반 속성, 749 페이지
  - 세션 설정 속성, 750 페이지
  - 주소 할당 속성, 751 페이지
  - 스플릿 터널링 속성, 751 페이지
  - Secure Client 속성, 752 페이지
  - 트래픽 필터 속성, 754 페이지
  - Windows 브라우저 프록시 속성, 755 페이지
- 기존 그룹 정책을 수정하려면 수정 버튼()을 클릭합니다.
- 더 이상 필요하지 않은 그룹을 삭제하려면 삭제 버튼()을 클릭합니다. 이 그룹은 현재 연결 프로파일에서 사용할 수 없습니다.

일반 속성

그룹 정책의 일반 속성에서는 그룹의 이름 및 기타 기본 설정을 정의합니다. Name(이름) 속성만 필수 속성입니다.

- **Name(**이름**)** - 그룹 정책의 이름입니다. 이름은 최대 64자까지 입력할 수 있고 공백이 허용됩니다.
- **Description(**설명**)** - 그룹 정책에 대한 설명입니다. 설명은 최대 1,024자까지 입력할 수 있습니다.
- **DNS Server(DNS** 서버**)** - VPN에 연결할 때 클라이언트가 도메인 이름 확인에 사용해야 하는 DNS 서버를 정의하는 DNS 서버 그룹을 선택합니다. 필요한 그룹이 아직 정의되지 않은 경우, **Create DNS Group(DNS** 그룹 생성**)**을 클릭하여 바로 생성합니다.
- 배너 - 로그인 시 사용자에게 표시할 배너 텍스트 또는 환영 메시지입니다. 기본값은 배너 없음입니다. 길이는 최대 496자까지 가능합니다. Secure Client 섹션 부분 HTML을 지원합니다. 원격 사용자에게 배너가 적절히 표시되게 하려면
 태그를 사용하여 줄 바꿈을 나타냅니다.
- **Default Domain(**기본 도메인**)** - RA VPN의 사용자에 대한 기본 도메인 이름입니다. example.com 등을 예로 들 수 있습니다. 이 도메인은 정규화되지 않은 호스트 이름(예: serverA.example.com이 아닌 serverA)에 추가됩니다.
- **Secure Client** 프로파일 - **+**를 클릭하고 이 그룹에 사용할 Secure Client 프로파일을 선택합니다. 연결 프로파일에서 외부 인터페이스에 대해 FQDN(fully-qualified domain name)을 컨피그레이션하는 경우, 기본 프로파일이 생성됩니다. 원하는 클라이언트 프로파일을 직접 업로드할 수도 있습니다. software.cisco.com에서 다운로드하여 설치할 수 있는 독립형 Secure Client 프로파일 편집기를 사용하여 이러한 프로파일을 생성합니다. 클라이언트 프로파일을 선택하지 않으면 Secure Client는 모든 옵션에 대해 기본값을 사용합니다. 이 목록의 항목은 프로파일 자체가 아니라 Secure Client 프로파일 개체입니다. 드롭다운 목록에서 **Create New Secure Client Profile(**새 보안 클라이언트 프로파일 생성**)**을 클릭하면 새 프로파일을 생성하고 업로드할 수 있습니다.

  Secure Client 프로파일 외에 AMP Enabler와 같은 Secure Client 모듈 프로파일을 선택할 수 있습니다. 모듈 유형당 하나의 프로파일을 선택할 수 있습니다.

세션 설정 속성

그룹 정책의 세션 설정에서는 사용자가 VPN을 통해 연결할 수 있는 시간과 설정할 수 있는 별도 연결의 개수를 제어합니다.

- **Maximum Connection Time(**최대 연결 시간**)** - 사용자가 로그아웃했다가 다시 연결하지 않고 VPN에 연결된 상태를 유지할 수 있는 최대 시간을 1~4473924(분)로 입력하거나 비워 둡니다. 기본값은 무제한(비워 둠)이지만 유휴 시간 제한은 계속 적용됩니다.
- **Connection Time Alert Interval(**연결 시간 알림 간격**)** - 최대 연결 시간을 지정하는 경우, 알림 간격에서는 사용자에게 앞으로 다가올 자동 연결 해제에 관해 경고를 표시하기까지 지나야 할 최대 시간을 정의합니다. 사용자는 연결 종료를 선택하고 다시 접속해 타이머를 다시 시작할 수 있습니다. 기본값은 1분입니다. 1분에서 30분까지 지정할 수 있습니다.
- **Idle Time(**유휴 시간**)** - VPN 연결이 자동으로 종료될 때까지 유휴 상태일 수 있는 시간을 1~35791394(분) 범위 내로 입력합니다. 이 연속되는 분 단위 시간 동안 연결에서 통신 활동이 없는 경우, 시스템에서는 연결을 중지합니다. 기본값은 30분입니다.
- **Idle Time Alert Interval(**유휴 시간 알림 간격**)** - 유휴 세션으로 인해 사용자에게 앞으로 다가올 자동 연결 해제에 관해 경고를 표시하기까지 지나야 할 유휴 시간입니다. 어떤 활동에서도 타이머를 재설정할 수 있습니다. 기본값은 1분입니다. 1분에서 30분까지 지정할 수 있습니다.

- **Simultaneous Login Per User(**사용자당 동시 로그인 수**)** - 한 사용자에게 허용되는 동시 연결의 최대 개수입니다. 기본값은 3입니다. 1~2147483647개의 연결을 지정할 수 있습니다. 다수의 동시 연결을 허용하면 보안이 취약해지고 성능이 저하될 수 있습니다.

주소 할당 속성

그룹 정책의 주소 할당 속성에서는 그룹에 대해 IP 주소 풀을 정의합니다. 여기에 정의된 풀은 이 그룹을 사용하는 모든 연결 프로파일에 정의된 풀을 재정의합니다. 연결 프로파일에 정의된 풀을 사용하려면 이러한 설정을 비워둡니다.

- **IPv4 Address Pool(IPv4** 주소 풀**)**, **IPv6 Address Pool(IPv6** 주소 풀**)** - 이 옵션에서는 원격 엔드포인트의 주소 풀을 정의합니다. 클라이언트가 VPN 연결을 설정하는 데 사용하는 IP 버전에 따라 이러한 풀의 주소가 클라이언트에 할당됩니다. 지원하려는 각 IP 유형에 대한 서브넷을 정의하는 네트워크 개체를 선택합니다. 해당 IP 버전을 지원하고 싶지 않은 경우, 목록을 비워두십시오. 예를 들어 IPv4 풀을 10.100.10.0/24로 정의할 수 있습니다. 주소 풀은 외부 인터페이스의 IP 주소와 동일한 서브넷에 있을 수 없습니다.

  로컬 주소 할당에 사용할 최대 6개의 주소 풀로 구성된 목록을 지정할 수 있습니다. 풀을 지정하는 순서는 중요합니다. 시스템에서는 풀이 표시되는 순서에 따라 이 풀에서 주소를 할당합니다.

- **DHCP Scope(DHCP** 범위**)** - 연결 프로파일에서 주소 풀에 대한 DHCP 서버를 컨피그레이션하는 경우, DHCP 범위에서는 이 그룹에 대한 풀에 사용할 서브넷을 식별합니다. 또한 DHCP 서버 주소에는 해당 범위에서 식별하는 동일한 서브넷에 주소가 있어야 합니다. 이 범위를 통해 사용자는 DHCP 서버에 정의된 주소 풀의 하위 집합을 선택하여 이 특정 그룹에 사용할 수 있습니다.

  네트워크 범위를 정의하지 않으면 DHCP 서버에서 구성된 주소 풀 순으로 IP 주소를 할당합니다. 할당되지 않은 주소를 식별할 때까지 풀을 검색합니다.

  범위를 지정하려면 원하는 풀과 동일한 서브넷에서 풀에 라우팅 가능한 주소를 포함하는 네트워크 개체를 선택하거나 생성합니다. DHCP 서버는 이 IP 주소가 속한 서브넷을 확인하고 해당 풀에서 IP 주소를 할당합니다.

  라우팅을 위해 가능한 경우 항상 인터페이스의 IP 주소를 사용하는 것이 좋습니다. 예를 들어 풀이 10.100.10.2-10.100.10.254이고 인터페이스 주소가 10.100.10.1/24이면 DHCP 범위로 10.100.10.1을 사용합니다. 네트워크 번호를 사용하지 마십시오. 개체가 아직 없는 경우, **Create New Network(**새 네트워크 생성**)**를 클릭합니다. IPv4 주소 지정에만 DHCP를 사용할 수 있습니다. 선택한 주소가 인터페이스 주소가 아닌 경우 범위 주소에 대한 고정 경로를 생성해야 할 수 있습니다.

스플릿 터널링 속성

그룹 정책의 스플릿 터널링 속성에서는 내부 네트워크로 가는 트래픽과 외부로 가는 트래픽을 시스템에서 각각 분별하여 처리하는 방식을 정의합니다. 스플릿 터널링은 일부 네트워크 트래픽이 VPN 터널(암호화됨)을 통과하도록 유도하고 나머지 네트워크 트래픽은 VPN 터널 외부(암호화되지 않음 또는 일반 텍스트 형식)로 보냅니다.

- **IPv4 Split Tunneling(IPv4** 스플릿 터널링**)**, **IPv6 Split Tunneling(IPv6** 스플릿 터널링**)** - 트래픽에서 IPv4와 IPv6 중 어떤 주소 지정을 사용하는지에 따라 다른 옵션을 지정할 수 있지만, 각각의

경우 옵션은 동일합니다. 스플릿 터널링을 활성화하려는 경우, 네트워크 개체를 선택해야 하는 옵션 중 하나를 지정합니다.

- **Allow all traffic over tunnel(**터널을 지나는 모든 트래픽 허용**)** - 스플릿 터널링은 실행하지 마십시오. 사용자가 RA VPN 연결을 하면 사용자의 모든 트래픽은 보호된 터널을 통과합니다. 이는 기본값입니다. 또한 이 기본값은 가장 안전한 옵션으로 간주됩니다.
- **Allow specified traffic over tunnel(**터널을 지나는 지정된 트래픽 허용**)** - 대상 네트워크 및 호스트 주소를 정의하는 네트워크 개체를 선택합니다. 이러한 대상으로 가는 모든 트래픽은 보호된 터널을 통과합니다. 기타 대상으로 가는 트래픽은 클라이언트에서 터널 외부 연결(예: 로컬 Wi-Fi 또는 네트워크 연결)로 라우팅합니다.
- **Exclude networks specified below(**아래에 지정된 네트워크 제외**)** - 대상 네트워크 또는 호스트 주소를 정의하는 네트워크 개체를 선택합니다. 이러한 대상으로 가는 모든 트래픽은 클라이언트에서 터널 외부 연결로 라우팅합니다. 기타 대상으로 가는 트래픽은 터널을 통과합니다.

- **Split DNS(**스플릿 **DNS)** - 보안 연결을 통해 일부 DNS 요청을 전송하도록 시스템을 컨피그레이션함과 동시에 클라이언트가 클라이언트에 컨피그레이션된 DNS 서버로 다른 DNS 요청을 전송하도록 허용할 수 있습니다. 다음 DNS 동작을 컨피그레이션할 수 있습니다.
  - **Send DNS Request as per split tunnel policy(**스플릿 터널 정책에 따라 **DNS** 요청 전송**)** - 이 옵션을 사용하면 스플릿 터널 옵션을 정의하는 것과 동일한 방식으로 DNS 요청이 처리됩니다. 스플릿 터널링을 활성화하는 경우, DNS 요청은 대상 주소에 근거하여 전송됩니다. 스플릿 터널링을 활성화하지 않는 경우, 모든 DNS 요청은 보호된 연결을 경유해 전송됩니다.
  - **Always send DNS requests over tunnel(**항상 터널을 통해 **DNS** 요청 전송**)** - 스플릿 터널링을 활성화하되 모든 DNS 요청을 보호된 연결을 경유해 그룹에 정의된 DNS 서버로 전송하려는 경우, 이 옵션을 선택합니다.
  - **Send only specified domains over tunnel(**지정된 도메인만 터널을 통해 전송**)** - 보호된 DNS 서버에서 특정 도메인에 대해서만 주소를 확인하게 하고 싶은 경우, 이 옵션을 선택합니다. 그런 다음, 도메인 이름을 쉼표로 구분하여 해당 도메인을 지정합니다. example.com, example1.com을 예로 들 수 있습니다. 내부 DNS 서버에서는 내부 도메인의 이름을 확인하고 외부 DNS 서버에서는 다른 모든 인터넷 트래픽을 처리하게 하려는 경우, 이 옵션을 사용합니다.

Secure Client 속성

그룹 정책의 Secure Client 속성에서는 원격 액세스 VPN 연결에 대해 Secure Client에서 사용하는 일부 SSL 및 연결 설정을 정의합니다.

SSL 설정

- **Enable Datagram Transport Layer Security (DTLS)(DTLS(Datagram Transport Layer Security)** 활성화**)** — Secure Client에서 2개의 터널(SSL 터널 및 DTLS 터널)을 동시에 사용하도록 허용할지 여부를 선택합니다. DTLS를 사용하면 일부 SSL 연결에서 발생하는 레이턴시 및 대역폭 문제를 방지하고 패킷 지연에 민감한 실시간 애플리케이션의 성능을 개선할 수 있습니다. DTLS를

활성화하지 않은 경우에는 SSL VPN 연결을 설정하는 Secure Client 사용자가 SSL 터널만 사용하여 연결합니다.

- **DTLS Compression(DTLS 압축)** — LZS를 사용하여 이 그룹에 대한 DTLS(Datagram Transport Layer Security) 연결을 압축할지 여부를 선택합니다. DTLS 압축은 기본적으로 비활성화되어 있습니다.
- **SSL Compression(SSL 압축)** — 데이터 압축을 활성화할지 여부, 활성화하는 경우 사용할 데이터 압축 방법(**Deflate(**압축 해제**)** 또는 **LZS**)을 선택합니다. SSL 압축은 기본적으로 **Disabled(**비활성화**)** 상태입니다. 데이터를 압축하면 전송 속도가 빨라지지만 각 사용자 세션에 대한 메모리 요건 및 CPU 사용량이 증가합니다. 따라서 SSL 압축으로 인해 디바이스의 전체 처리량은 줄어듭니다.
- **SSL Rekey Method(SSL 키 재입력 방법)**, **SSL Rekey Interval(SSL 키 재입력 간격)** — 클라이언트는 VPN 연결에 키를 재입력하여 암호화 키 및 초기화 벡터를 재협상할 수 있어 연결 보안이 강화됩니다. **None(**없음**)**을 선택하여 키 재입력을 비활성화합니다. 키 재입력을 활성화하려면 **New Tunnel(**새 터널**)**을 선택하여 매번 새 터널을 생성합니다. (**Existing Tunnel(**기존 터널**)** 옵션을 선택하면 **New Tunnle(**새 터널**)**과 동일한 조치가 수행됩니다.) 키 재입력을 활성화하는 경우, 키 재입력 간격도 설정하십시오. 기본값은 4분입니다. 4~10080분(일주일) 범위 내에서 간격을 설정할 수 있습니다.

연결 설정

- **Ignore the DF (Don't Fragment) bit(DF(Don't Fragment)** 비트 무시**)** — 단편화해야 하는 패킷에서 DF(Don't Fragment) 비트를 무시할지 여부를 선택합니다. 이 옵션을 선택하면 DF 비트가 설정된 패킷의 강제 단편화가 허용되므로 이 패킷이 터널을 통과할 수 있습니다.
- **Client Bypass Protocol(**클라이언트 우회 프로토콜**)** — 이 옵션을 선택하면 보안 게이트웨이에서 IPv6 트래픽만 예상할 때 IPv4 트래픽을 관리하는 방법 또는 IPv4 트래픽만 예상할 때 IPv6 트래픽을 관리하는 방법을 컨피그레이션할 수 있습니다.

  Secure Client에서 헤드엔드와의 VPN 연결을 수행할 때 헤드엔드에서는 IPv4 주소나 IPv6 주소 또는 IPv4 및 IPv6 주소 모두를 지정합니다. 헤드엔드에서 Secure Client 연결에 IPv4 주소만 또는 IPv6 주소만 지정할 경우, 헤드엔드에서 IP 주소를 지정하지 않은 네트워크 트래픽을 삭제하거나 이 트래픽이 헤드엔드를 우회하여 암호화되지 않은 또는 "일반 텍스트" 형태(활성화 및 확인된 상태)로 클라이언트에서 전송되는 것을 허용하도록 Client Bypass Protocol(클라이언트 우회 프로토콜)을 컨피그레이션할 수 있습니다.

  예를 들어 보안 게이트웨이에서 Secure Client 연결에 IPv4 주소만 지정하고 엔드포인트는 이중 스택이라고 가정합시다. 엔드포인트가 IPv6 주소에 연결하려고 시도할 때 클라이언트 우회 프로토콜이 비활성화된 경우 IPv6 트래픽이 끊기지만 클라이언트 우회 프로토콜이 활성화된 경우, IPv6 트래픽은 클라이언트에서 암호화되지 않은 상태로 전송됩니다.
- **MTU** — Secure Client에서 설정한 SSL VPN 연결의 MTU(Maximum Transmission Unit)입니다. 기본값은 1406바이트입니다. 범위는 576~1462바이트입니다.
- **Keepalive Messages Between Secure Client and VPN Gateway(**보안 클라이언트와 **VPN** 게이트웨이 간의 연결 유지 메시지**)** - 피어 간에 연결 유지 메시지를 교환하여 터널에서 데이터를 송수신

하는 데 사용할 수 있다는 것을 시연할지 여부를 선택합니다. 연결 유지 메시지는 설정된 간격에 따라 전송됩니다. 기본 간격은 20초, 유효 범위는 15~600초입니다.

- **DPD on Gateway Side Interval(**게이트웨이 측 간격의 **DPD)**, **DPD on Client Side Interval(**클라이언트 측 간격의 **DPD)** — DPD(Dead Peer Detection)를 활성화하면 피어가 더 이상 응답하지 않을 경우 VPN 게이트웨이 또는 VPN 클라이언트를 신속하게 탐지할 수 있습니다. 게이트웨이 또는 클라이언트 DPD를 별도로 활성화할 수 있습니다. DPD 메시지 전송의 기본 간격은 30초입니다. 간격은 5-3600초 사이일 수 있습니다.

트래픽 필터 속성

그룹 정책의 트래픽 필터 속성에서는 그룹에 할당된 사용자에게 부과하고 싶은 제한 사항을 정의합니다. 액세스 제어 정책 규칙을 생성하는 대신 이 속성을 사용해 RA VPN 사용자를 호스트 또는 서브넷 주소 및 프로토콜, VLAN에 따라 특정 리소스로 제한할 수 있습니다.

기본적으로 그룹 정책에 따라 RA VPN 사용자는 보호된 네트워크의 어떤 대상에 액세스하는 것도 제한되지 않습니다.

- **Access List Filter(**액세스 목록 필터**)** - 확장된 ACL(액세스 제어 목록)을 사용하여 액세스를 제한합니다. 스마트 CLI 확장 ACL 개체를 선택하거나 **Create Extended Access List(**확장 액세스 목록 생성**)**를 클릭하여 바로 생성합니다.

  확장 ACL을 통해 소스 주소, 대상 주소 및 프로토콜(예: IP 또는 TCP)을 기준으로 필터링할 수 있습니다. ACL은 하향식, 최초 일치 방식에 따라 평가되므로 특정 규칙이 다수의 일반 규칙보다 먼저 배치되도록 보장합니다. ACL의 끝에는 암묵적 "deny any(모두 거부)"가 있으므로 서브넷 몇 개에 대한 액세스만 거부하고 다른 모든 액세스는 허용하려면 ACL의 끝에 "permit any(모두 허용)" 규칙을 포함하십시오. VPN 필터는 초기 연결에만 적용됩니다. 애플리케이션 검사 작업으로 인해 열리는 SIP 미디어 연결과 같은 보조 연결에는 적용되지 않습니다.

  확장 ACL 스마트 CLI 개체를 수정하는 중에는 네트워크 개체를 생성할 수 없으므로 그룹 정책을 수정하기 전에 ACL을 생성해야 합니다. 그러지 않는 경우, 개체만 생성할 수 있습니다. 그런 다음 다시 돌아가 네트워크 개체를 생성한 후 필요한 모든 액세스 제어 항목을 생성하면 됩니다. ACL을 생성하려면 **Device(**디바이스**)** > **Advanced Configuration(**고급 구성**)** > **Smart CLI(**스마트 **CLI)** > **Objects(**개체**)**로 이동하여 개체를 생성하고 **Extended Access List(**확장 액세스 목록**)**를 개체 유형으로 선택합니다. 예시는 그룹별로 RA VPN 액세스를 제어하는 방법, 795 페이지의 내용을 참조하십시오.

- **Restrict VPN to VLAN(VPN**을 **VLAN**으로 제한**)** - “VLAN 매핑”이라고도 하는 이 속성에서는 이 그룹 정책이 적용되는 세션에 이그레스(egress) VLAN 인터페이스를 지정합니다. 시스템에서는 이 그룹에서 나오는 모든 트래픽을 선택한 VLAN으로 전달합니다.

  이 특성을 사용하여 그룹 정책에 VLAN을 할당하면 액세스 제어를 간소화할 수 있습니다. ACL을 사용하여 세션의 트래픽을 필터링하는 방법 대신 이 속성에 값을 할당하는 방법도 가능합니다. 디바이스에서 하위 인터페이스에 정의된 VLAN 번호를 반드시 지정하십시오. 값의 범위는 1에서 4094까지입니다.

Windows 브라우저 프록시 속성

그룹 정책의 Windows 브라우저 프록시 속성에서는 사용자의 브라우저에 정의된 프록시의 작동 방식과 작동 여부를 결정합니다.

Browser Proxy During VPN Session(VPN 세션 중 브라우저 프록시**)**에 대해 다음 값 중 하나를 선택할 수 있습니다.

- **No change in endpoint settings(**엔드포인트 설정에 변경 사항 없음**)** - 이 옵션을 통해 사용자는 HTTP에 대해 브라우저 프록시를 컨피그레이션하거나 컨피그레이션하지 않을 수 있으며 컨피그레이션되어 있는 경우 프록시를 사용할 수 있습니다.
- **Disable browser proxy(**브라우저 프록시 비활성화**)** - 브라우저에 대해 정의된 프록시(있는 경우)를 사용하지 않습니다. 이 경우 프록시를 통해 브라우저 연결이 설정되지 않습니다.
- **Auto detect settings(**설정 자동 탐지**)** - 클라이언트 디바이스에 대해 브라우저에서 자동 프록시 서버 감지를 사용하도록 활성화합니다.
- **Use custom settings(**사용자 정의 설정 사용**)** - HTTP 트래픽에 대해 모든 클라이언트 디바이스에서 사용해야 하는 프록시를 정의합니다. 다음 설정을 구성합니다.
  - **Proxy Server IP or Hostname(**프록시 서버 **IP** 또는 호스트네임**)**, **Port(**포트**)** - 프록시 서버의 IP 주소 또는 호스트네임, 프록시 서버에서 프록시 연결에 사용하는 포트입니다. 호스트와 포트를 합해 100자를 초과할 수 없습니다.
  - **Browser Exemption List(**브라우저 면제 목록**)** - 면제 목록의 호스트/포트에 대한 연결은 프록시를 통과하지 않습니다. 프록시를 사용해서는 안 되는 대상에 대해 모든 호스트/포트 값을 추가합니다. www.example.com port 80을 예로 들 수 있습니다. **Add(**추가**)** 링크를 클릭하여 목록에 항목을 추가합니다. 항목을 삭제하려면 휴지통 아이콘을 클릭합니다. 모든 주소와 포트를 합한 전체 프록시 예외 목록은 255자를 초과할 수 없습니다.

원격 액세스 VPN 모니터링

원격 액세스 VPN 연결을 모니터링하고 트러블슈팅하려면 CLI 콘솔을 열거나 디바이스 CLI에 로그인하여 다음 명령을 사용합니다.

- **show vpn-sessiondb** VPN 세션에 대한 정보를 표시합니다. **clear vpn-sessiondb** 명령을 사용하여 이 통계를 재설정할 수 있습니다.
- **show webvpn** *keyword* 통계 및 설치된 AnyConnect 이미지를 비롯하여 원격 액세스 VPN 컨피그레이션에 대한 정보를 표시합니다. 사용 가능한 키워드를 보려면 **show webvpn ?**를 입력합니다.
- **show aaa-server** 원격 액세스 VPN에 사용되는 디렉터리 서버에 대한 통계를 표시합니다.

원격 액세스 VPN 트러블슈팅

원격 액세스 VPN 연결 문제는 클라이언트 또는 threat defense 디바이스 컨피그레이션에서 발생할 수 있습니다. 다음 항목에서는 발생할 수 있는 주요 트러블슈팅 문제에 관해 설명합니다.

SSL 연결 문제 트러블슈팅

사용자가 Secure Client를 다운로드하기 위해 외부 IP 주소에 대한 초기 비Secure Client SSL 연결을 설정할 수 없는 경우 다음 작업을 수행합니다.

1. 원격 액세스 VPN 연결 프로파일에 기본 포트가 아닌 포트를 구성한 경우 사용자가 URL에 포트 번호를 포함하고 있는지 확인합니다(예: https://ravpn.example.com:4443).
2. 클라이언트 워크스테이션에서 외부 인터페이스의 IP 주소에 대해 Ping을 수행할 수 있는지 확인합니다. ping을 수행할 수 없는 경우 사용자 워크스테이션에서 해당 주소로의 경로가 없는 이유를 확인합니다.
3. 클라이언트 워크스테이션에서 RA(원격 액세스) VPN 연결 프로파일에 정의되어 있는 외부 인터페이스의 FQDN(Fully Qualified Domain name)에 대해 ping을 수행할 수 있는지 확인합니다. IP 주소의 ping은 가능한데 FQDN의 ping은 불가능한 경우에는 클라이언트 및 RA VPN 연결 프로파일에서 사용하는 DNS 서버를 업데이트하여 FQDN에서 IP 주소로의 매핑을 추가해야 합니다.
4. 사용자가 외부 인터페이스에서 제공하는 인증서를 수락하는지 확인합니다. 사용자는 해당 인증서를 영구적으로 수락해야 합니다.
5. RA VPN 연결 컨피그레이션을 검사하여 올바른 외부 인터페이스를 선택했는지 확인합니다. RA VPN 사용자를 대상으로 하는 외부 인터페이스가 아닌 내부 네트워크를 대상으로 하는 내부 인터페이스를 실수로 선택하는 경우가 많습니다.
6. SSL 암호화가 정상적으로 구성되어 있으면 외부 스니퍼를 사용하여 TCP 3방향 핸드셰이크에 성공하는지 확인합니다.

Secure Client 다운로드 및 설치 문제 해결

사용자가 외부 인터페이스로의 SSL 연결을 설정할 수 있는데 Secure Client 패키지를 다운로드하여 설치할 수는 없는 경우 다음 사항을 고려하십시오.

- 클라이언트 운영 체제용 Secure Client 패키지를 업로드했는지 확인합니다. 예를 들어 사용자 워크스테이션에서 Linux를 실행하는데 Linux Secure Client 이미지를 업로드하지 않은 경우에는 설치할 수 있는 패키지가 없습니다.
- Windows 클라이언트의 경우 사용자에게는 소프트웨어를 설치할 수 있는 관리자 권한이 있어야 합니다.
- Windows 클라이언트의 경우 워크스테이션에서 ActiveX를 활성화하거나 Java JRE 1.5 이상(JRE 7 권장)을 설치해야 합니다.

- Safari 브라우저의 경우에는 Java를 활성화해야 합니다.
- 다른 브라우저를 사용해 보면 특정 브라우저에서만 다운로드와 설치에 실패할 수도 있습니다.

Secure Client 연결 문제 해결

사용자가 외부 인터페이스에 연결하여 Secure Client를 다운로드하고 설치할 수 있었는데 그 후에 Secure Client를 사용한 연결을 완료할 수는 없는 경우 다음 사항을 고려하십시오.

- 인증에 실패하는 경우, 사용자가 올바른 사용자 이름과 암호를 입력했는지, 사용자 이름이 인증 서버에 올바르게 정의되어 있는지 확인합니다. 인증 서버는 데이터 인터페이스 중 하나를 통해서도 사용할 수 있어야 합니다.

참고 인증 서버가 외부 네트워크에 있는 경우, 외부 네트워크에 대한 사이트 대 사이트 VPN 연결을 컨피그레이션하고 VPN 내에 원격 액세스 VPN 인터페이스 주소를 포함해야 합니다. 자세한 내용은 원격 액세스 VPN을 통해 외부 네트워크에서 디렉터리 서버를 사용하는 방법, 780 페이지를 참조해 주십시오.

- RA(원격 액세스) VPN 연결 프로필에서 외부 인터페이스에 대한 FQDN(Fully Qualified Domain Name)을 구성한 경우 클라이언트 디바이스에서 FQDN에 대해 ping을 수행할 수 있는지 확인합니다. IP 주소의 ping은 가능한데 FQDN의 ping은 불가능한 경우에는 클라이언트 및 RA VPN 연결 프로파일에서 사용하는 DNS 서버를 업데이트하여 FQDN에서 IP 주소로의 매핑을 추가해야 합니다. 외부 인터페이스의 FQDN을 지정할 때 생성된 기본 Secure Client 프로파일을 사용하는 경우, 사용자는 DNS가 업데이트될 때까지 IP 주소를 사용하도록 서버 주소를 수정해야 합니다.
- 사용자가 외부 인터페이스에서 제공하는 인증서를 수락하는지 확인합니다. 사용자는 해당 인증서를 영구적으로 수락해야 합니다.
- 사용자의 Secure Client에 여러 연결 프로파일이 포함되어 있으면 사용자가 올바른 프로파일을 선택하는지 확인합니다.
- 클라이언트 쪽의 모든 설정이 올바른 것으로 확인되면 threat defense 디바이스에 대한 SSH 연결을 설정하고 **debug webvpn** 명령을 입력합니다. 그런 후에 연결 시도 중에 발급된 메시지를 검사합니다.

RA VPN 트래픽 흐름 문제 트러블슈팅

사용자가 보안 RA(원격 액세스) VPN 연결을 설정할 수는 있는데 트래픽을 보내고 받을 수는 없으면 다음 작업을 수행합니다.

1. 클라이언트의 연결을 끊었다가 다시 연결합니다. 이렇게 하면 문제가 해결될 수도 있습니다.
2. Secure Client에서 트래픽 통계를 점검하여 전송 카운터와 수신 카운터의 값이 모두 증가하는지를 확인합니다. 수신된 패킷 수가 0으로 유지되는 경우, threat defense 디바이스에서 트래픽을 전혀

반환하지 않고 있는 것입니다. threat defense 컨피그레이션에 문제가 있을 가능성이 있습니다. 흔히 발생하는 문제는 다음과 같습니다.

- 액세스 규칙이 트래픽을 차단하고 있습니다. 액세스 제어 정책에서 내부 네트워크와 RA VPN 주소 풀 간의 트래픽을 차단하는 규칙을 확인하십시오. 기본 작업이 트래픽 차단인 경우에는 명시적 허용 규칙을 생성해야 할 수 있습니다.
- VPN 필터에서 트래픽을 차단하고 있습니다. 연결 프로파일에 대한 그룹 정책에 컨피그레이션된 ACL 트래픽 필터 또는 VLAN 필터를 확인합니다. 또한 파일 정책을 액세스 제어 규칙의 트래픽에 적용하는 경우, 파일 액세스나 악성코드 또는 둘 다를 제어하려면 파일 이벤트 메시지를 외부 syslog 서버로 전송하도록 시스템을 컨피그레이션할 수 있습니다.
- RA VPN 트래픽에 대해 NAT 규칙이 우회되고 있지 않습니다. 모든 내부 인터페이스의 RA VPN 연결에 대해 NAT 제외가 구성되어 있는지 확인하십시오. 또는 NAT 규칙이 내부 네트워크 및 인터페이스와 RA VPN 주소 풀 및 외부 인터페이스 간의 통신을 차단하지 않는지 확인하십시오.
- 경로가 잘못 구성되어 있습니다. 정의된 모든 경로가 유효하며 올바르게 동작하고 있는지 확인하십시오. 예를 들어, 외부 인터페이스에 고정 IP 주소가 정의되어 있는 경우 0.0.0.0/0 및 ::/0에 대한 기본 경로가 라우팅 테이블에 포함되어 있는지 확인하십시오.
- RA VPN에 구성된 DNS 서버 및 도메인 이름이 올바르며 클라이언트 시스템이 올바른 DNS 서버와 도메인 이름을 사용하고 있는지 확인하십시오. DNS 서버에 연결할 수 있는지 확인합니다.
- RA VPN의 스플릿 터널링을 활성화하는 경우, 지정된 내부 네트워크로 전송되는 트래픽은 터널을 통과하고 기타 모든 트래픽은 터널을 우회하는지(threat defense 디바이스에서 해당 트래픽을 확인할 수 없음) 확인합니다.

3. threat defense 디바이스에 SSH 연결을 설정하여 원격 액세스 VPN에 대해 트래픽이 전송 및 수신되고 있는지 확인합니다. 이렇게 하려면 다음 명령을 사용합니다.
   - **show webvpn anyconnect**
   - **show vpn-sessiondb**

원격 액세스 VPN의 예시

다음에는 원격 액세스 VPN을 구성하는 예시가 나와 있습니다.

RADIUS CoA(Change of Authorization) 구현 방법

동적 인증이라고도 하는 RADIUS CoA(Change of Authorization)에서는 threat defense 원격 액세스 VPN에 대한 엔드포인트 보안을 제공합니다. RA VPN의 주요 당면 과제는 감염된 엔드포인트로부터 내부 네트워크를 보호하는 것입니다. 또한 엔드포인트에 대한 공격을 해결하여 바이러스 또는 악성코드의 침해를 받을 때 엔드포인트 자체를 보호하는 것입니다. RA VPN 세션 전, 중, 후 모든 단계에서 엔

드포인트와 내부 네트워크를 보호해야 합니다. RADIUS CoA 기능을 통해 이 목표를 달성할 수 있습니다.

Cisco Identity Services Engine(ISE) RADIUS 서버를 사용하는 경우, CoA(Change of Authorization) 정책 시행을 컨피그레이션할 수 있습니다.

ISE CoA(Change of Authorization) 기능에서는 설정 후 AAA(인증, 권한 부여 및 계정 관리) 세션의 속성을 변경할 수 있는 메커니즘을 제공합니다. 정책에서 AAA의 사용자 또는 사용자 그룹을 변경하는 경우, ISE에서는 threat defense 디바이스로 CoA 메시지를 전송하여 인증을 다시 시작하고 새 정책을 적용합니다. IPEP(Inline Posture Enforcement Point: 인라인 보안 상태 시행 지점)에는 threat defense 디바이스로 설정된 각 VPN 세션에 대한 ACL(Access Control List: 액세스 제어 목록)이 필요하지 않습니다.

다음 주제에서는 CoA의 작동 방식 및 컨피그레이션 방법에 대해 설명합니다.

CoA(Change of Authorization)를 위한 시스템 흐름

Cisco ISE에는 프로세스, 파일, 레지스트리 항목, 안티바이러스 보호, 안티스파이웨어 보호, 호스트에 설치된 방화벽 소프트웨어 등의 기준에 대한 엔드포인트의 규정 준수를 평가하는 클라이언트 보안 상태 에이전트가 있습니다. 관리자는 엔드포인트에서 규정을 준수할 때까지 네트워크 액세스를 제한하거나 로컬 사용자 권한을 격상하여 보안정책 교정 사례를 설정할 수 있습니다. ISE Posture는 클라이언트 측 평가를 실시합니다. 클라이언트는 ISE에서 보안 상태 요건 정책을 수신하고 보안 상태 데이터 수집을 수행하며 결과를 정책과 비교하여 평가 결과를 ISE로 반송합니다.

다음은 CoA(Change of Authorization)를 위한 threat defense 디바이스, ISE, RA VPN 클라이언트 간 시스템 흐름을 설명한 것입니다.

1. 원격 사용자는 threat defense 디바이스에서 Secure Client를 사용하여 RA VPN 세션을 시작합니다.
2. threat defense 디바이스에서는 ISE 서버로 해당 사용자에 대한 RADIUS Access-Request 메시지를 전송합니다.
3. 이 시점에는 클라이언트 보안 상태를 알 수 없기 때문에 ISE에서는 알 수 없는 보안 상태에 대해 컨피그레이션된 권한 부여 정책에 사용자를 매칭합니다. 이 정책에서는 ISE가 RADIUS Access-Accept 응답에서 threat defense로 전송하는 다음 cisco-av-pair 옵션을 정의합니다.
   - **url-redirect-acl=***acl_name*, 여기서 *acl_name*은 threat defense 디바이스에 컨피그레이션된 확장 ACL의 이름입니다. 이 ACL에서는 ISE 서버로 리디렉션되어야 할 사용자 트래픽, 즉 HTTP 트래픽을 정의합니다. 예를 들면 다음과 같습니다.

     ```
     url-redirect-acl=redirect
     ```

   - **url-redirect=***url*, 여기서 URL은 트래픽이 리디렉션되어야 할 대상 URL입니다. 예를 들면 다음과 같습니다.

     ```
     url-redirect=https://ise2.example.com:8443/guestportal/gateway?sessionId=xx&action=cpp
     ```

   호스트네임을 확인할 수 있도록 데이터 인터페이스에 대해 DNS를 컨피그레이션해야 합니다. 또한 연결 프로파일에 대한 그룹 정책에서 트래픽 필터링을 컨피그레이션하는 경우, 클라이언트 풀에서 포트(예시의 TCP/8443)를 통해 ISE 서버에 연결할 수 있는지 확인합니다.

4. threat defense 디바이스에서는 RADIUS Accounting-Request 시작 패킷을 전송하고 ISE에서 오는 응답을 수신합니다. 계정 관리 요청에는 세션 ID, VPN 클라이언트의 외부 IP 주소, threat defense 디바이스의 IP 주소를 포함한 세션의 모든 상세정보가 포함되어 있습니다. ISE에서는 세션 ID를 사용해 해당 세션을 식별합니다. threat defense 디바이스에서도 주기적인 임시 계정 정보를 전송할 수 있습니다. 여기서 가장 중요한 속성은 threat defense 디바이스에서 클라이언트에 할당하는 IP 주소가 있는 Framed-IP-Address입니다.
5. 알 수 없는 보안 상태 중에 threat defense 디바이스에서는 리디렉션 ACL과 일치하는 클라이언트에서 오는 트래픽을 리디렉션 URL로 리디렉션합니다. ISE에서는 클라이언트에 필수 보안 상태 규정 준수 모듈이 있는지 확인하고, 필요한 경우 이 모듈을 설치하라는 메시지를 사용자에게 표시합니다.
6. 클라이언트 디바이스에 에이전트를 설치하고 나면 ISE 보안 상태 정책에 구성된 확인 작업이 자동으로 수행됩니다. 클라이언트는 ISE와 직접 통신합니다. 클라이언트는 ISE에 보안 상태 보고서를 전송하는데, 여기에는 SWISS 프로토콜 및 포트 TCP/UDP 8905를 사용하는 여러 교환이 포함될 수 있습니다.
7. ISE는 에이전트에서 보안 상태 보고서를 받으면 권한 부여 규칙을 다시 한번 처리합니다. 이때 보안 상태 결과를 알 수 있고 이제 다른 규칙에서는 클라이언트와 일치합니다. ISE에서는 규정 준수 또는 미준수 엔드포인트에 대한 다운로드 가능 ACL(DACL)을 포함하는 RADIUS CoA 패킷을 전송합니다. 예를 들어 준수 DACL에서는 모든 액세스를 허용할 수 있지만, 미준수 DACL에서는 모든 액세스를 거부합니다. DACL의 콘텐츠는 ISE 관리자의 책임입니다.
8. threat defense 디바이스에서는 리디렉션을 제거합니다. 이 디바이스에서 DACL을 캐싱하지 않는 경우, ISE에서 다운로드할 수 있도록 Access-Request를 전송해야 합니다. 특정 DACL은 VPN 세션에 연결되어 있으므로 디바이스 컨피그레이션의 일부가 되지 않습니다.
9. 다음번에 RA VPN 사용자가 웹 페이지에 액세스하려 할 때 사용자는 해당 세션에 대해 threat defense 디바이스에 설치된 DACL에서 허용하는 리소스에 액세스할 수 있습니다.

참고 엔드포인트에서 모든 필수 요건을 충족하지 못하고 수동 교정이 필요한 경우, Secure Client에서 교정 창이 열려 작업이 필요한 항목이 표시됩니다. 보안정책 교정 창은 네트워크 활동의 업데이트가 팝업으로 표시되어 방해하거나 중단하지 않도록 배경에서 실행됩니다. 사용자는 Secure Client의 ISE 보안 상태 바둑판식 배열 부분에 있는 **Details(**상세정보**)**를 클릭하여 탐지된 항목과 네트워크에 연결하기 위해 필요한 업데이트를 확인할 수 있습니다.

Threat Defense 디바이스에서 COA(Change of Authorization) 컨피그레이션

CoA(Change of Authorization) 정책의 대부분은 ISE 서버에서 컨피그레이션됩니다. 그러나 ISE에 올바르게 연결하려면 threat defense 디바이스를 컨피그레이션해야 합니다. 다음 절차에서는 컨피그레이션 중에서 threat defense 측을 컨피그레이션하는 방법에 대해 설명합니다.

시작하기 전에

모든 개체에서 호스트네임을 사용하는 경우, 데이터 인터페이스에 사용할 DNS 서버를 데이터 및 관리 트래픽용 DNS 설정, 827 페이지에 설명된 대로 컨피그레이션하십시오. 일반적으로 시스템이 온전히 작동하도록 어떤 식으로든 DNS를 컨피그레이션해야 합니다.

프로시저

단계 **1** 초기 연결을 ISE로 리디렉션하기 위한 확장 ACL(Access Control List)을 컨피그레이션합니다.

리디렉션 ACL의 목적은 초기 트래픽을 ISE로 전송하여 ISE에서 클라이언트 보안 상태를 평가할 수 있게 하는 것입니다. ACL에서는 ISE에 HTTPS 트래픽을 전송해야 하지만, 이미 ISE가 대상으로 지정된 트래픽 또는 이름 확인을 위해 DNS 서버로 전송되는 트래픽은 전송해서는 안 됩니다. 샘플 리디렉션 ACL은 다음과 같이 표시될 수 있습니다.

```
access-list redirect extended deny ip any host <ISE server IP>
access-list redirect extended deny ip any host <DNS server IP>
access-list redirect extended deny icmp any any
access-list redirect extended permit tcp any any eq www
```

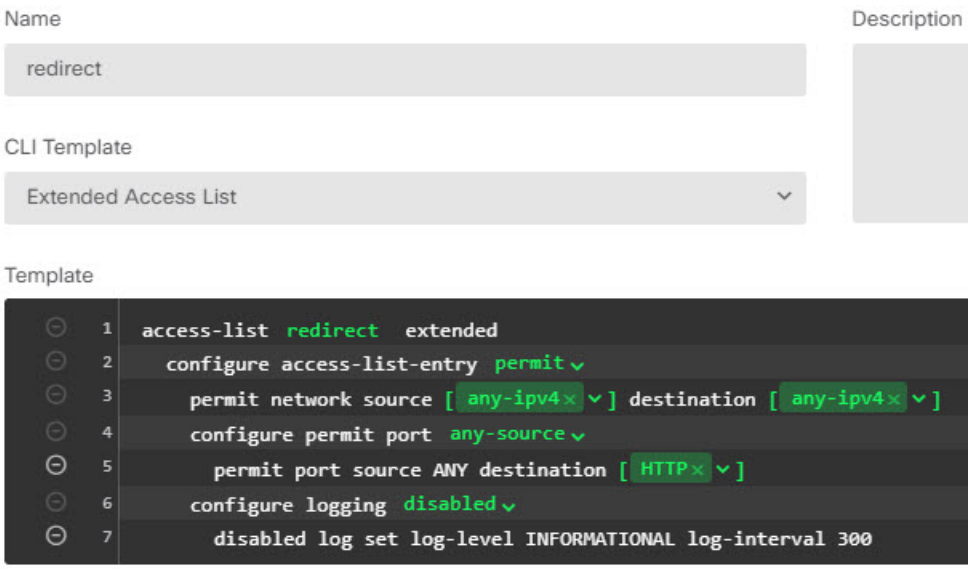
하지만 ACL에는 마지막 ACE(액세스 제어 항목)인 암시적 “deny any any”가 있다는 점에 유의하십시오. 이 예에서는 TCP 포트 www(즉 포트 80)와 일치하는 마지막 ACE가 첫 ACE 3개와 일치하는 모든 트래픽과 일치하지 않습니다. 따라서 이 ACE 3개는 이중화됩니다. 마지막 ACE로 ACL을 생성하기만 해도 동일한 결과를 얻을 수 있습니다.

리디렉션 ACL의 허용 및 거부 작업에서는 일치하는 것은 허용하고 일치하지 않는 것은 거부하여 ACL과 일치하는 트래픽을 확인할 뿐이라는 점에 유의하십시오. 트래픽이 실제로 차단되는 경우는 없으며, 거부된 트래픽은 ISE로 리디렉션되지 않을 뿐입니다.

리디렉션 ACL을 생성하려면 스마트 CLI 개체를 컨피그레이션해야 합니다.

a) **Device(**디바이스**)** > **Advanced Configuration(**고급 컨피그레이션**)** > **Smart CLI(**스마트 **CLI)** > **Objects(**개체**)**를 선택합니다.
b) +를 클릭하여 새 개체를 생성합니다.
c) ACL의 이름을 입력합니다. 예: **redirect(**리디렉션**)**.
d) **CLI Template(CLI** 템플릿**)**에서 **Extended Access List(**확장 액세스 목록**)**를 선택합니다.
e) **Template(**템플릿**)** 본문에서 다음과 같이 컨피그레이션합니다.
   - configure access-list-entry action = permit
   - source-network = any-ipv4
   - destination-network = any-ipv4
   - configure permit port = any-source
   - destination-port = HTTP
   - configure logging = disabled

ACE는 다음과 같이 표시되어야 합니다.



f) **OK(**확인**)**를 클릭합니다.

이 ACL은 다음번에 변경 사항을 구축할 때 컨피그레이션됩니다. 다른 정책에서 개체를 사용하여 구축을 강제 적용할 필요가 없습니다.

참고 이 ACL은 IPv4에만 적용됩니다. IPv6도 지원하려면 속성이 모두 동일한 두 번째 ACE를 추가하기만 하면 됩니다. 단, 소스 및 대상 네트워크용으로 선택된 any-ipv6은 제외합니다. 트래픽이 ISE 또는 DNS 서버로 리디렉션되지 않도록 다른 ACE를 추가할 수도 있습니다. 먼저 해당 서버의 IP 주소를 보류할 호스트 네트워크 개체를 생성해야 합니다.

단계 **2** 동적 권한 부여를 위해 RADIUS 서버 그룹을 컨피그레이션합니다.

동적 권한 부여라고도 하는 CoA(Change of Authorization)를 활성화하기 위해 RADIUS 서버 및 서버 그룹 개체에서 올바르게 선택해야 할 중요한 옵션이 몇 가지 있습니다. 다음 절차에서는 이러한 속성에 중점을 둡니다. 이러한 개체에 대한 자세한 내용은 RADIUS 서버 및 그룹, 182 페이지의 내용을 참조하십시오.

a) **Objects(**개체**)** > **Identity Sources(ID** 소스**)**를 선택합니다.

b) **+** > **RADIUS Server(RADIUS** 서버**)**를 클릭합니다.

c) 서버 이름, ISE RADIUS 서버의 호스트네임/IP 주소, 인증 포트, 서버에 컨피그레이션된 암호 키를 입력합니다. 원하는 경우, 시간 초과를 조정합니다. 이러한 옵션은 동적 권한 부여와 직접적인 관련이 없습니다.

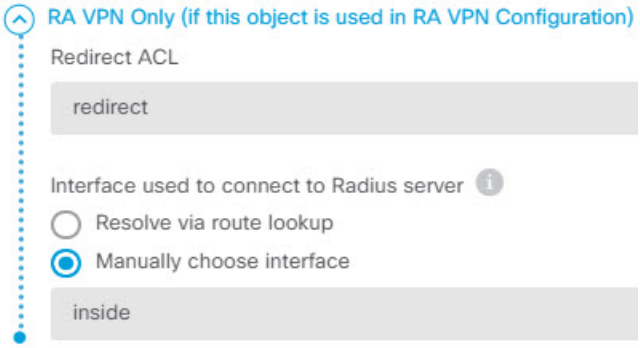
d) RA VPN Only(RA VPN 전용) 링크를 클릭하고 다음 옵션을 컨피그레이션합니다.

- **Redirect ACL(**리디렉션 **ACL)** - 리디렉션을 위해 생성한 확장 ACL을 선택합니다. 이 예에서는 ACL의 이름이 redirect입니다.
- **Interface used to connect to Radius server(RADIUS** 서버에 연결하는 데 사용할 인터페이스**) - Manually Choose Interface(**수동으로 인터페이스 선택**)**를 선택하고, 서버에 연결하기 위해 사용할 인터페이스를 선택합니다. 시스템에서 인터페이스에 CoA 리스너를 올바르게 활성화할 수 있도록 특정 인터페이스를 선택해야 합니다.

서버가 관리 주소와 동일한 네트워크에 있는 경우(진단 인터페이스 선택을 의미함), 진단 인터페이스의 IP 주소도 컨피그레이션해야 합니다. 관리 IP 주소로는 충분하지 않습니다. **Device(**디바이스**)** > **Interfaces(**인터페이스**)**로 이동하여 관리 IP 주소와 동일한 서브넷에 있는 진단 인터페이스에서 IP 주소를 설정합니다.

또한 device manager 관리 액세스를 위해 이 서버를 사용하는 경우, 이 인터페이스는 무시됩니다. 관리 액세스 시도는 항상 관리 IP 주소를 통해 인증됩니다.

다음 예는 내부 인터페이스에 대해 컨피그레이션되는 옵션을 나타낸 것입니다.



e) **OK(**확인**)**를 클릭하여 서버 개체를 저장합니다.

여러 개의 중복 ISE RADIUS 서버에 이중화 설정이 되어 있는 경우에는 이들 각 서버에 대해 서버 개체를 생성합니다.

f) **+** > **RADIUS Server Group(RADIUS** 서버 그룹**)**을 클릭합니다.

g) 서버 그룹의 이름을 입력하고, 원하는 경우 비활성 시간 및 최대 시도 횟수를 조정합니다.

h) **Dynamic Authorization(**동적 권한 부여**)** 옵션을 선택하고, ISE 서버에서 다른 포트를 사용하도록 컨피그레이션된 경우에는 포트 번호를 변경합니다. 포트 1700은 CoA 패킷에 대한 수신에 사용되는 기본 포트입니다.

i) 사용자 인증을 위해 AD 서버를 사용하도록 RADIUS 서버를 컨피그레이션하는 경우, 이 RADIUS 서버와 함께 사용되는 AD 서버를 지정하는 **Realm that Supports the RADIUS Server(RADIUS** 서버를 지원하는 영역**)**를 선택합니다. 영역이 아직 없는 경우, 목록 아래에 있는 **Create New Identity Realm(**새 **ID** 영역 생성**)**을 클릭하여 영역을 바로 컨피그레이션합니다.

j) **RADIUS Server(RADIUS** 서버**)**에서 **+** 버튼을 클릭하고 RA VPN에 대해 생성한 서버 개체를 선택합니다.

k) **OK(**확인**)**를 클릭하여 서버 그룹 개체를 저장합니다.

단계 **3** **Device(**디바이스**)** > **RA VPN** > **Connection Profiles(**연결 프로파일**)**를 선택하고, 이 RADIUS 서버 그룹을 사용하는 연결 프로파일을 생성합니다.

AAA Authentication(AAA 인증**)**을 사용하고(이것만 사용하거나 인증서와 함께 사용), **Primary Identity Source for User Authentication(**사용자 인증을 위한 기본 **ID** 소스**)**, **Authorization(**권한 부여**)** 및 **Accounting(**계정 관리**)** 옵션에서 서버 그룹을 선택합니다.

조직의 필요에 따라 다른 옵션을 모두 컨피그레이션합니다.

참고 VPN 네트워크를 통해 DNS 서버에 접속할 경우, 스플릿 터널링 속성 페이지에서 연결 프로파일에 사용되는 그룹 정책을 수정하여 **Split DNS(**스플릿 **DNS)** 옵션을 컨피그레이션합니다.

ISE에서 COA(Change of Authorization) 컨피그레이션

CoA(Change of Authorization) 컨피그레이션의 대부분은 ISE 서버에서 수행됩니다. ISE에는 엔드포인트 디바이스에서 실행되는 보안 상태 평가 에이전트가 있고, ISE에서는 디바이스와 직접 통신하여 보안 상태를 확인합니다. threat defense 디바이스에서는 기본적으로 특정 최종 사용자를 처리하는 방법에 대한 ISE의 지침을 기다립니다.

보안 상태 평가 정책 컨피그레이션에 대한 전체적인 논의는 이 문서의 범위를 벗어납니다. 그러나 다음 절차에서는 몇 가지 기본 사항에 관해 설명합니다. ISE를 컨피그레이션하기 위한 시작점으로 이것을 사용하십시오. 정확한 명령 경로, 페이지 이름 및 속성 이름은 릴리스에 따라 달라질 수 있다는 점에 유의하십시오. 사용 중인 ISE 버전에서는 다른 용어 또는 조직을 사용할 수 있습니다.

지원되는 최소 ISE 릴리스는 2.2 패치 1입니다.

시작하기 전에

이 절차에서는 ISE RADIUS 서버에서 사용자를 이미 컨피그레이션한 것으로 가정합니다.

프로시저

단계 **1** 관리 > 네트워크 리소스 > 네트워크 디바이스 > 네트워크 디바이스를 선택하고 threat defense 디바이스를 ISE 네트워크 디바이스 인벤토리에 추가한 뒤 RADIUS 설정을 구성합니다.

RADIUS 인증 설정을 선택하고 threat defense RADIUS 서버 개체에 구성된 동일한 공유 암호를 구성합니다. 원하는 경우 **CoA** 포트 번호를 변경하고 threat defense RADIUS 그룹 개체의 동일한 포트를 구성하도록 합니다.

단계 **2** **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Authorization(**권한 부여**)** > **Downloadable ACLs(**다운로드 가능한 **ACL)**를 선택합니다.

규정 준수 엔드포인트에서 사용할 것 1개와 규정 미준수 엔드포인트에서 사용할 것 1개, 즉 2개의 DACL(다운로드 가능 ACL)을 생성합니다.

예를 들어 규정 준수 엔드포인트에 대한 모든 액세스를 허용(permit ip any any)하는 반면, 규정 미준수 엔드포인트에 대한 모든 액세스를 거부(deny ip any any)할 수 있습니다. 필요에 따라 이 DACL의 복잡도를 조절하여 사용자의 규정 준수 상태에 따라 사용자가 가져야 할 정확한 액세스 권한을 제공할 수 있습니다. 권한 부여 프로파일에서 이 DACL을 사용합니다.

단계 **3** **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Authorization(**권한 부여**)** > **Authorization Profile(**권한 부여 프로파일**)**을 선택하고 필요한 프로파일을 컨피그레이션합니다.

다음 상태에 대한 프로파일이 필요합니다. 각각에 대한 최소 속성이 나열됩니다.

- **Unknown(**알 수 없음**)** - 알 수 없는 보안 상태 프로파일이 기본 보안 상태 프로파일입니다. 모든 엔드포인트는 RA VPN 연결을 처음 설정하는 경우 이 정책에 매칭됩니다. 이 규칙의 요점은 리디렉션 ACL 및 URL을 적용하고, 엔드포인트에 보안 상태 에이전트가 아직 없는 경우 다운로드하는 것입니다. 에이전트가 설치되어 있지 않은 경우 또는 설치에 실패한 경우, 엔드포인트는 이 프로파일에 연결된 상태를 유지할 수 있습니다. 그러지 않으면 엔드포인트는 보안 상태를 평가한 후 규정 준수 또는 미준수 프로파일로 이동합니다.

  최소 속성은 다음과 같습니다.

  - **Name(**이름**)** - 예: PRE_POSTURE
  - **Access Type(**액세스 유형**) - ACCESS_ACCEPT**를 선택합니다.
  - 일반 작업 - 웹 리디렉션**(CWA, MDM, NSP, CPP)**을 선택하고 클라이언트 프로비저닝**(**상태**)**를 선택한 후 threat defense 디바이스에 구성한 리디렉션 ACL의 이름을 입력합니다. 아직 선택하지 않은 경우 **Value(**값**)**에서 **Client Provisioning Portal(**클라이언트 프로비저닝 포털**)**을 선택합니다.
  - **Attribute Details(**속성 상세정보**)**에서는 url-redirect-acl 및 url-redirect에 대한 2개의 cisco-av-pair 값을 표시해야 합니다. ISE에서 이 데이터를 threat defense 디바이스로 전송하고, 이 디바이스에서는 기준을 RA VPN 사용자 세션에 적용합니다.

- **Compliant(**규정 준수**)** - 보안 상태 평가 완료 후 엔드포인트에 대해 컨피그레이션된 모든 요구사항을 엔드포인트가 충족하는 경우, 클라이언트는 규정을 준수하는 것으로 간주되며 이 프로파일을 가져옵니다. 일반적으로 이 클라이언트에 전체 액세스 권한을 부여합니다.

  최소 속성은 다음과 같습니다.

  - **Name(**이름**)** - 예: FULL_ACCESS
  - **Access Type(**액세스 유형**) - ACCESS_ACCEPT**를 선택합니다.
  - **Common Tasks(**일반 작업**) - DACL Name(DACL** 이름**)**을 선택하고, 규정 준수 사용자에 대해 다운로드 가능 ACL을 선택합니다(예: PERMIT_ALL_TRAFFIC). ISE에서 ACL을 threat defense 디바이스로 전송하고, 이 디바이스에서는 이 ACL을 사용자 세션에 적용합니다. 이 DACL은 사용자 세션에 대한 초기 리디렉션 ACL을 대체합니다.

- **Non-compliant(**규정 미준수**)** - 보안 상태 평가를 통해 엔드포인트가 모든 요건을 충족하지 못한다는 것이 확인되는 경우, 카운트다운이 실행되는데 이 시간 동안 클라이언트에서는 필요한 업데이트를 설치하는 것과 같은 방법으로 엔드포인트를 규정 준수 상태로 가져올 수 있습니다. Secure Client이 컴플라이언스 문제가 있는 사용자를 안내합니다. 카운트다운을 하는 동안 엔드포인트는 알 수 없는 규정 준수 상태를 유지합니다. 카운트다운이 만료된 후에도 엔드포인트가 여전히 규정 미준수 상태를 유지하는 경우, 세션은 규정 미준수로 표시되며 규정 미준수 프로파일을 가져옵니다. 일반적으로 이 엔드포인트에 대한 모든 액세스를 금지하거나 최소한 몇 가지 방법으로 액세스를 제한합니다.

  최소 속성은 다음과 같습니다.

  - **Name(**이름**)** - 예: Non_Compliant
  - **Access Type(**액세스 유형**) - ACCESS_ACCEPT**를 선택합니다.

- **Common Tasks(**일반 작업**) - DACL Name(DACL** 이름**)**을 선택하고, 규정 미준수 사용자에 대해 다운로드 가능 ACL을 선택합니다(예: DENY_ALL_TRAFFIC). ISE에서 ACL을 threat defense 디바이스로 전송하고, 이 디바이스에서는 이 ACL을 사용자 세션에 적용합니다. 이 DACL은 사용자 세션에 대한 초기 리디렉션 ACL을 대체합니다.

단계 **4** **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Client Provisioning(**클라이언트 프로비저닝**)** > **Resources(**리소스**)**를 선택하고 다음 리소스를 컨피그레이션합니다.

- **AnyConnect package(AnyConnect** 패키지**)** - 헤드 엔드 패키지 파일로서, software.cisco.com에서 다운로드합니다. 지원하는 클라이언트 플랫폼에 대한 별도 패키지가 필요하므로 AnyConnectDesktopWindows와 같은 여러 가지 유형을 구성해야 할 수도 있습니다.
- **ISE Posture Configuration File(Type: AnyConnectProfile)(ISE** 보안 상태 구성 파일**(**유형**: AnyConnectProfile))** - 이 구성 파일에서는 규정 준수 모듈에서 엔드 유저의 디바이스를 평가하는 데 사용하는 설정을 정의합니다. 이 파일에서는 사용자가 규정 미준수 디바이스를 규정 준수 상태로 가져올 수 있는 시간의 길이도 정의합니다.
- 컴플라이언스 모듈 패키지**(**유형**: ComplianceModule)** - Secure Client 컴플라이언스 모듈 파일은 설치된 AnyConnect 패키지에 공급되어 엔드포인트 컴플라이언스를 확인하는 파일입니다. **Add Resource from Cisco Site(Cisco** 사이트에서 리소스 추가**)** 명령을 사용하여 이 파일을 다운로드합니다. 구성한 Secure Client 패키지에 따라 올바른 모듈을 다운로드했는지 확인합니다. 그렇지 않은 경우 사용자는 다운로드를 실패합니다. ISEComplianceModule 폴더의 Secure Client 목록에 있는 software.cisco.com에서도 파일을 확인할 수 있습니다.
- **Anyconnect** 구성 파일**(**유형**: AnyConnectConfig)** - 이 Secure Client 릴리스별 설정은 적용할 **AnyConnect** 패키지, 컴플라이언스 모듈, **ISE** 상태를 정의합니다. 패키지는 OS별로 되어 있기 때문에 지원할 각 클라이언트 OS(예: Windows, MAC, Linux)에 대해 별도 컨피그레이션 파일을 생성합니다.

단계 **5** **Policy(**정책**)** > **Client Provisioning(**클라이언트 프로비저닝**)**을 선택하고 클라이언트 프로비저닝 정책을 컨피그레이션합니다.

예를 들어 CoA를 구현해야 하는 각 운영 체제에 대해 CoA_ClientProvisionWin과 같은 이름의 새 규칙을 생성합니다. 규칙에 대해 적절한 운영 체제를 선택하고 결과에서 해당 OS에 대해 생성한 Secure Client 구성 파일을 에이전트로 선택합니다.

교체하려는 기본 OS별 규칙을 비활성화합니다.

단계 **6** 보안 상태 정책을 컨피그레이션합니다.

이 단계에서는 조직에 의미가 있는 보안 상태 요건을 개발합니다.

- **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Conditions(**조건**)** > **Posture(**보안 상태**)**를 선택하고 충족해야 하는 단순 보안 상태 조건을 정의합니다. 예를 들어 사용자에게 특정 애플리케이션을 설치하도록 요구할 수 있습니다.
- **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Posture(**보안 상태**)** > **Requirements(**요건**)**를 선택하고, 엔드포인트에 대해 규정 준수 모듈 요건을 정의합니다.

- **Policy(**정책**)** > **Posture(**보안 상태**)** > **Posture Policy(**보안 상태 정책**)**를 선택하고 지원되는 운영 체제에 대한 정책을 컨피그레이션합니다.

단계 **7** **Policy(**정책**)** > **Policy Sets(**정책 집합**)** > **Default(**기본값**)** > **Authorization Policy(**권한 부여 정책**)**를 선택하고 정책을 생성합니다.

각 규정 준수 조건에 대해 규칙을 추가합니다. 이 샘플 값은 이전 단계의 예시에 따른 것입니다.

- 알 수 없음: 사전 보안 상태 및 보안 상태 다운로드의 경우
  - Name(이름) - 예: PRE_POSTURE
  - Condition(조건) - ”Session-PostureStatus EQUALS Unknown” 및 “Radius-NAS-Port-Type EQUALS Virtual”
  - Profiles(프로파일) - 예: PRE_POSTURE
- 규정 준수: 보안 상태 요건을 충족하는 클라이언트의 경우
  - Name(이름) - 예: FULL_ACCESS
  - Condition(조건) - ”Session-PostureStatus EQUALS Compliant” 및 “Radius-NAS-Port-Type EQUALS Virtual”
  - Profiles(프로파일) - 예: FULL_ACCESS
- 규정 미준수: 보안 상태 요건 충족에 실패하는 클라이언트의 경우
  - Name(이름) - 예: NON-COMPLIANT
  - Condition(조건) - ”Session-PostureStatus EQUALS NonCompliant” 및 “Radius-NAS-Port-Type EQUALS Virtual”
  - Profiles(프로파일) - 예: Non_Compliant

단계 **8** (선택 사항). **Administration(**관리**)** > **Settings(**설정**)** > **Posture(**보안 상태**)** > **Reassessments(**재평가**)**를 선택하고 보안 상태 재평가를 활성화합니다.

기본적으로 보안 상태는 연결 시에만 평가됩니다. 보안 상태 재평가를 활성화하여 연결된 엔드포인트의 보안 상태를 주기적으로 확인할 수 있습니다. 재평가 간격을 설정하여 재평가가 실행되는 빈도를 결정할 수 있습니다.

시스템에서 재평가에 실패하는 경우, 시스템에서 어떻게 응답해야 하는지 정의할 수 있습니다. 사용자가 계속 진행하도록 허용하거나(연결 유지) 사용자를 로그오프하거나 시스템을 교정하도록 사용자에게 요청할 수 있습니다.

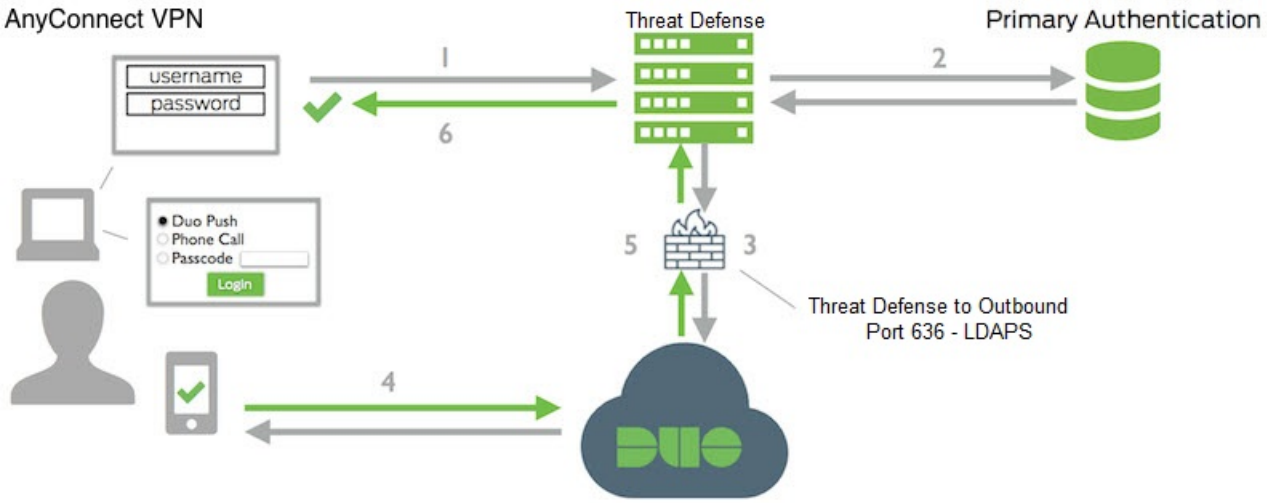
Duo LDAP를 사용하여 이중 인증을 구성하는 방법

기본 소스로 Microsoft AD(Microsoft Active Directory) 또는 RADIUS 서버를 함께 사용하여 Duo LDAP 서버를 보조 인증 소스로 사용할 수 있습니다. Duo LDAP를 사용하는 경우 보조 인증에서는 Duo 암호, 푸시 알림 또는 전화 통화를 사용하여 기본 인증을 검증합니다.

다음 주제에서는 구성에 대해 자세히 설명합니다.

Duo LDAP 보조 인증을 위한 시스템 플로우

다음 그래픽에는 LDAP를 사용하여 이중 인증을 제공하기 위해 threat defense 및 Duo가 함께 작동하는 방법이 나와 있습니다.



다음은 시스템 플로우에 대한 설명입니다.

1. 사용자는 threat defense 디바이스에 대한 원격 액세스 VPN 연결을 설정하고 사용자 이름과 비밀번호를 입력합니다.
2. Threat Defense에서는 기본 인증 서버(Active Directory 또는 RADIUS일 수 있음)를 사용하여 이 기본 인증 시도를 인증합니다.
3. 기본 인증이 작동하는 경우 threat defense에서는 보조 인증에 대한 요청을 Duo LDAP 서버로 전송합니다.
4. 그런 다음, Duo에서 푸시 알림, 암호를 사용한 문자 메시지 또는 전화 통화를 통해 사용자를 개별적으로 인증합니다. 사용자는 이 인증을 성공적으로 완료해야 합니다.
5. Duo에서는 사용자가 성공적으로 인증되었는지 여부를 나타내기 위해 threat defense 디바이스에 응답합니다.
6. 보조 인증에 성공하면 threat defense 디바이스에서 사용자의Secure Client와 원격 액세스 VPN 연결을 설정합니다.

Duo LDAP 보조 인증 구성

다음 절차에서는 Duo LDAP를 보조 인증 소스로 사용하여 원격 액세스 VPN에 이중 인증을 구성하는 엔드 투 엔드 프로세스에 대해 설명합니다. 이 구성을 완료하려면 Duo를 사용하는 어카운트가 있어야 하며 Duo에서 일부 정보를 얻어야 합니다.

프로시저

단계 **1** Duo 어카운트를 생성하고 통합 키, 비밀 키 및 API 호스트 이름을 가져옵니다.

프로세스는 간단히 다음과 같습니다. 자세한 내용은 Duo 웹 사이트인 https://duo.com을 참조하십시오.

a) Duo 어카운트에 등록합니다.
b) Duo 관리 패널에 로그인하여 **Applications(**애플리케이션**)**로 이동합니다.
c) 애플리케이션 목록에서 **Protect an Application(**애플리케이션 보호**)**을 클릭하고 Cisco SSL VPN을 찾습니다. **Protect this Application(**이 애플리케이션 보호**)**을 클릭하여 통합 키, 비밀 키 및 API 호스트 이름을 가져옵니다. 도움이 필요한 경우 Duo *Getting Started* 가이드(https://duo.com/docs/getting-started)를 참조하십시오.

단계 **2** Duo LDAP 서버의 Duo LDAP ID 소스를 생성합니다.

threat defense API를 사용하여 Duo LDAP 개체를 생성해야 합니다. device manager을 사용하여 생성할 수는 없습니다. API Explorer를 사용하거나 고유한 클라이언트 애플리케이션을 작성하여 개체를 생성할 수 있습니다. 다음 절차에서는 API Explorer를 사용하여 개체를 생성하는 방법을 설명합니다.

a) device manager에 로그인하고 추가 옵션 버튼(⋮)을 클릭한 후 **API Explorer**를 선택합니다.

브라우저 설정에 따라 별도의 탭 또는 창에 API Explorer가 열립니다.

b) (선택 사항). 시스템에서 Duo LDAP 서버에 연결할 때 사용해야 하는 인터페이스를 식별하는 데 필요한 값을 가져옵니다.

인터페이스를 지정하지 않으면 시스템에서 라우팅 테이블을 사용합니다. 필요한 경우 Duo LDAP 서버에 대한 정적 경로를 생성할 수 있습니다. 또는 Duo LDAP 개체에서 사용할 인터페이스를 지정할 수 있습니다. 인터페이스를 지정하려는 경우 인터페이스 그룹의 다양한 GET 메서드를 사용하여 필요한 값을 가져옵니다. 물리적 인터페이스, 하위 인터페이스, EtherChannel 또는 VLAN 인터페이스를 사용할 수 있습니다. 예를 들어, 물리적 인터페이스의 값을 가져오려면 GET /devices/default/interfaces 메서드를 사용하여 사용해야 하는 인터페이스의 개체를 찾습니다. 인터페이스 개체에서는 다음과 같은 값이 필요합니다.

- id
- type
- version
- name

c) **DuoLDAPIdentitySource** 머리글을 클릭하여 그룹을 엽니다.

d) **POST /object/duoldapidentitysources** 메서드를 클릭합니다.

e) **Parameters(**파라미터**)** 머리글 아래의 **body(**본문**)** 요소에서 오른쪽의 **Data Type(**데이터 유형**)** 열에 있는 **Example Value(**예시 값**)** 표시 상자를 클릭합니다. 이 작업을 수행하면 본문 값 수정 상자에 예시가 로드됩니다.

f) **body value(**본문 값**)** 수정 상자에서 다음 작업을 수행합니다.

- 특성 줄인 **version**, **id**를 삭제합니다. 이러한 특성은 PUT 호출에 필요하지만 POST에는 필요하지 않습니다.
- **name**에는 개체의 이름(예: Duo-LDAP-server)을 입력합니다.
- **description**에는 참조 목적으로 개체에 대한 의미 있는 설명을 입력하거나 특성 줄을 삭제합니다.
- **apiHostname**에는 Duo 어카운트에서 가져온 API 호스트 이름을 입력합니다. 호스트 이름은 X가 고유한 값으로 교체되면 API-XXXXXXXX.DUOSECURITY.COM과 유사하게 표시되어야 합니다. 대문자는 필요하지 않습니다.
- **port**에는 LDAPS에 사용할 TCP 포트를 입력합니다. 포트는 다른 포트를 사용하도록 Duo에서 지시한 경우를 제외하고는 636이어야 합니다. 액세스 제어 목록에서 이 포트를 통해 Duo LDAP 서버에 대한 트래픽을 허용하는지 확인해야 합니다.
- **timeout**에는 Duo 서버에 연결할 시간 제한(초)을 입력합니다. 이 값은 1~300초일 수 있습니다. 기본값은 120입니다. 기본값을 사용하려면 120을 입력하거나 특성 줄을 삭제합니다.
- **integrationKey**에는 Duo 어카운트에서 가져온 통합 키를 입력합니다.
- **secretKey**에는 Duo 어카운트에서 가져온 비밀 키를 입력합니다. 이 키는 이후에 마스킹됩니다.
- **interface**에는 Duo LDAP 서버에 연결하는 데 사용할 인터페이스의 ID, 유형, 버전 및 이름 값을 입력하거나 후행 닫는 중괄호를 포함하여 인터페이스 특성을 정의하는 데 사용되는 6개의 줄을 삭제합니다.
- **type**의 값은 duoldapidentitysource로 남겨 둡니다.

예를 들어, 개체 본문은 다음과 유사하게 표시될 수 있습니다. 여기에서 apiHostname 및 integrationKey는 난독 처리되지만, 의도적으로 위조한 비밀 키가 표시됩니다.

```
{
  "name": "Duo-LDAP-server",
  "description": "Duo LDAP server for RA VPN",
  "apiHostname": "API-XXXXXXXX.DUOSECURITY.COM",
  "port": 636,
  "timeout": 120,
  "integrationKey": "XXXXXXXXXXXXXXXXXXXX",
  "secretKey": "123456789",
  "type": "duoldapidentitysource"
}
```

g) **Try It Out!(**시도**)** 버튼을 클릭합니다.

시스템에서 디바이스 구성에 개체를 게시하기 위해 **curl** 명령을 실행합니다. 여기에는 curl 명령, 응답 본문 및 응답 코드가 표시됩니다. 유효한 본문을 생성한 경우 **Response Code(**응답 코드**)** 필드에 **200**이 표시되어야 합니다.

오류가 발생한 경우 응답 본문에서 오류 메시지를 확인합니다. 본문 값을 수정하고 다시 시도할 수 있습니다.

h) 상단 메뉴에서 **Device(**디바이스**)**를 클릭하여 device manager으로 돌아갑니다.

i) 목차에서 **Objects(**개체**)**와 **Identity Sources(ID** 소스**)**를 차례로 클릭합니다.

Duo LDAP 개체가 목록에 표시되어야 합니다. 표시되지 않는 경우, API Explorer로 돌아가 개체를 다시 생성해 보십시오. GET 메서드를 사용하여 실제로 생성되었는지 여부를 확인할 수 있습니다.

device manager을 사용하여 개체를 삭제할 수는 있지만 개체를 수정하거나 내용을 볼 수는 없습니다. 이러한 작업을 수행할 때는 API를 사용해야 합니다. 관련된 메서드가 **DuoLDAPIdentitySource** 그룹에 표시됩니다.

단계 **3** Duo 웹 사이트의 신뢰할 수 있는 CA 인증서를 device manager에 업로드합니다.

threat defense 시스템에는 Duo LDAP 서버에 대한 연결을 검증하는 데 필요한 인증서가 있어야 합니다. 이 절차를 사용하여 인증서를 가져오고 업로드할 수 있으며 이 절차는 Google Chrome 브라우저를 통해 수행되었습니다. 브라우저마다 정확한 단계는 다를 수 있습니다. 또는 https://www.digicert.com/digicert-root-certificates.htm으로 직접 이동하여 인증서를 다운로드할 수 있지만, 다음과 같은 절차가 일반적이며 이를 사용하여 모든 사이트에 대해 신뢰할 수 있는 루트 CA 인증서를 가져올 수 있습니다.

a) 브라우저에서 https://duo.com을 엽니다.

b) 브라우저의 URL 필드에서 사이트 정보 링크를 클릭한 다음, **Certificate(**인증서**)** 링크를 클릭합니다. 이 작업을 수행하면 인증서 정보 대화 상자가 열립니다.

c) **Certificate Path(**인증서 경로**)** 탭을 클릭하고 경로의 루트(상위) 레벨을 선택합니다. 이 경우에는 DigiCert입니다.

d) DigiCert를 선택하고 **View Certificate(**인증서 보기**)**를 클릭합니다. 이 작업을 수행하면 새 Certificate(인증서) 대화 상자가 열리고 General(일반) 탭에 인증서가 DigiCert High Assurance EV Root CA로 발급되었음이 표시되어야 합니다. 이 인증서는 device manager에 업로드해야 하는 루트 CA 인증서입니다.

e) **Details(**세부 사항**)** 탭을 클릭한 다음, **Copy To File(**파일에 복사**)** 버튼을 클릭하여 인증서 다운로드 마법사를 시작합니다.

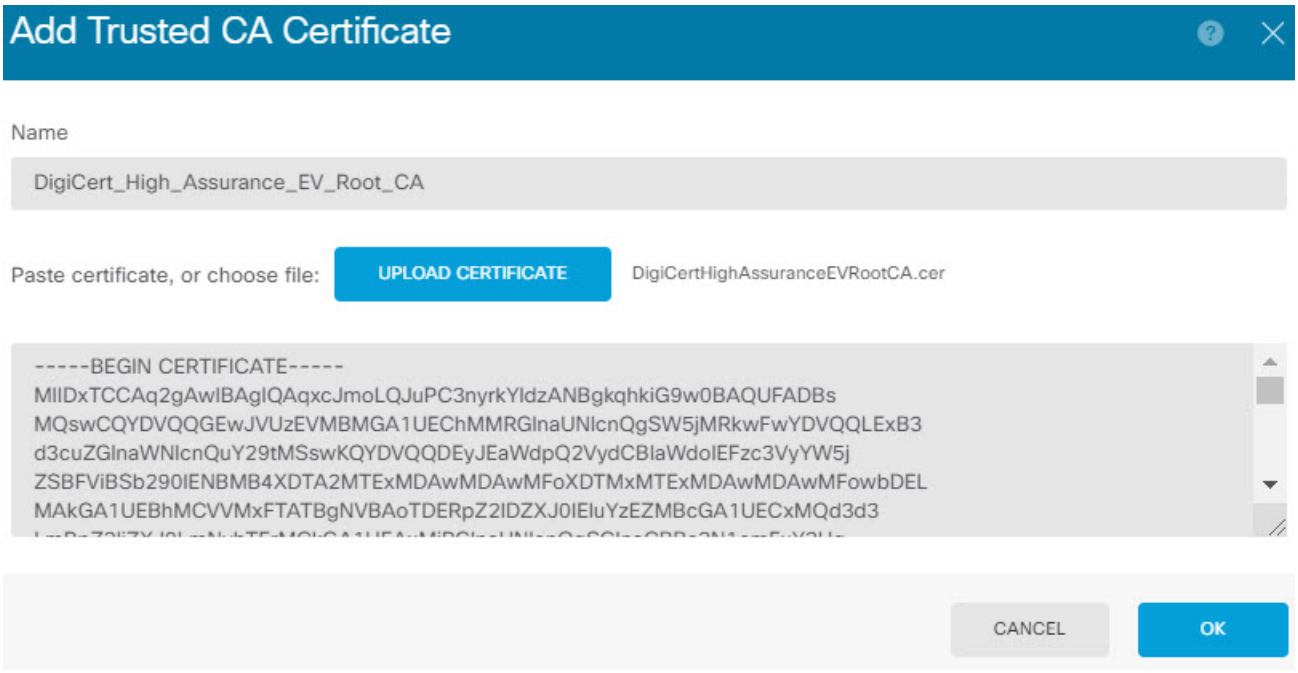
f) 이 마법사를 사용하여 워크스테이션에 인증서를 다운로드합니다. 기본 DER 형식을 사용하여 다운로드합니다.

g) device manager에서 **Objects(**개체**)** > **Certificates(**인증서**)**를 선택합니다.

h) **+** > **Add Trusted CA Certificate(**신뢰받는 **CA** 인증서 추가**)**를 클릭합니다.

i) 인증서의 이름(예: DigiCert_High_Assurance_EV_Root_CA)을 입력합니다. 공백은 허용되지 않습니다.

j) **Upload Certificate(**인증서 업로드**)**를 클릭하고 다운로드한 파일을 선택합니다.



k) **OK(**확인**)**를 클릭합니다.

단계 **4** 인증 시간 제한에 60초 이상을 지정하는 프로필을 생성하려면 Secure Client 프로필 편집기를 사용합니다.

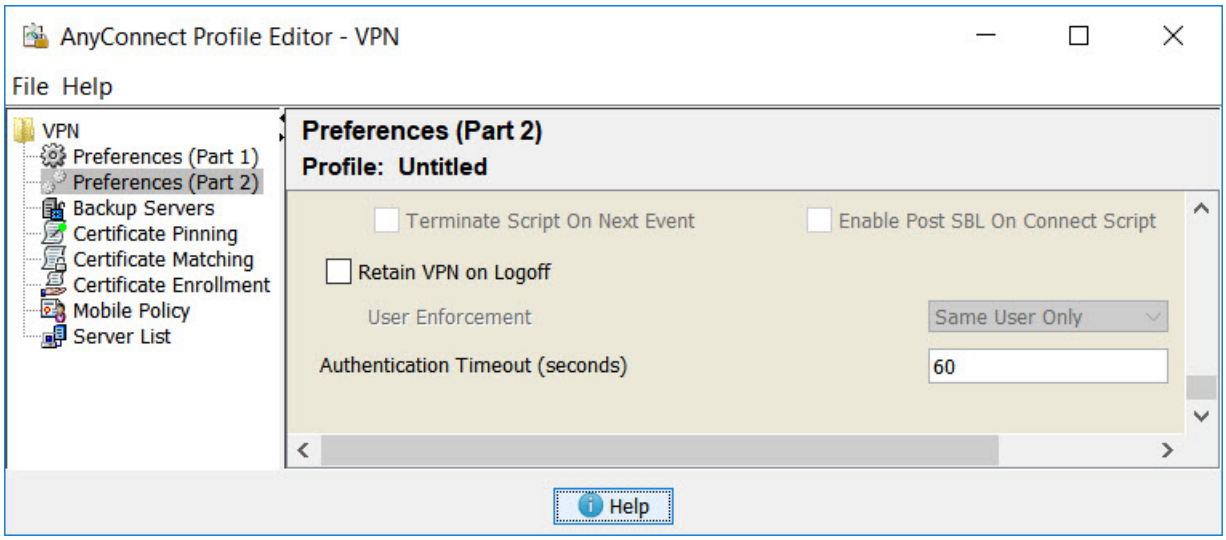
사용자에게 Duo 암호를 얻고 보조 인증을 완료할 추가 시간을 제공해야 합니다. 60초 이상 제공하는 것이 좋습니다.

Secure Client 프로필을 생성하고 업로드하는 방법에 대한 자세한 내용은 클라이언트 프로파일 구성 및 업로드, 734 페이지를 참조하십시오. 다음 절차에서는 인증 시간 제한만 구성한 후 프로필을 threat defense에 업로드하는 방법에 대해 설명합니다. 다른 설정을 변경하려는 경우 지금 하면 됩니다.

a) 아직 작업을 수행하지 않은 경우, Secure Client 프로필 편집기 패키지를 다운로드하여 설치합니다. 이는 Cisco Software Center(software.cisco.com)(Secure Client 버전용 폴더)에서 찾을 수 있습니다.

b) Secure Client **VPN Profile Editor(VPN** 프로필 편집기**)**를 엽니다.

c) 목차에서 **Preferences(Part 2)(**기본 설정**(**파트 **2))**를 선택하고 페이지 끝으로 스크롤한 다음, **Authentication Timeout(**인증 시간 제한**)**을 60 이상으로 변경합니다. 다음 이미지는 AnyConnect 4.7 VPN 프로필 편집기의 이미지입니다(이전 버전 또는 후속 버전의 경우 다를 수 있음).



d) **File(**파일**)** > **Save(**저장**)**를 선택하고 프로필 XML 파일을 적절한 이름(예: duo-ldap-profile.xml)의 워크스테이션에 저장합니다.

이제 VPN 프로필 편집기 애플리케이션을 닫으면 됩니다.

e) device manager에서 **Objects(**개체**)** > **Secure Client Profiles(**보안 클라이언트 프로파일**)**를 선택합니다.

f) +를 클릭하여 새 프로필 개체를 생성합니다.

g) 개체의 **Name(**이름**)**을 입력합니다. 예를 들어, Duo-LDAP-profile입니다.

h) **Upload(**업로드**)**를 클릭하고 생성한 XML 파일을 선택합니다.

i) **OK(**확인**)**를 클릭합니다.

단계 **5** 그룹 정책을 생성하고 정책에서 Secure Client 프로필을 선택합니다.

사용자에게 할당하는 그룹 정책으로 인해 연결의 여러 측면이 제어됩니다. 다음 절차에서는 프로필 XML 파일을 그룹에 할당하는 방법에 대해 설명합니다. 그룹 정책으로 수행할 수 있는 작업에 대한 자세한 내용은 RA VPN에 대한 그룹 정책 컨피그레이션, 749 페이지를 참조하십시오.

a) **Device(**디바이스**)** > **Remote Access VPN(**원격 액세스 **VPN)**에서 **View Configuration(**구성 보기**)**을 클릭합니다.

b) 목차에서 **Group Policies(**그룹 정책**)**를 선택합니다.

c) DfltGrpPolicy를 수정하거나 +를 클릭하고 새 그룹 정책을 생성합니다. 예를 들어 모든 사용자를 대상으로 단일 원격 액세스 VPN 연결 프로필이 필요한 경우, 기본 그룹 정책을 수정하는 것이 바람직합니다.

d) General(일반) 페이지에서 다음 속성을 구성합니다.

- **Name(**이름**)** - 새 프로필의 경우 이름을 입력합니다. 예를 들어, Duo-LDAP-group과 같이 입력합니다.
- **Secure Client Profile(**보안 클라이언트 프로파일**)** - +를 클릭하고 생성한 Secure Client 클라이언트 프로필 개체를 선택합니다.

e) 그룹 프로필을 저장하려면 **OK(**확인**)**를 클릭합니다.

단계 **6** Duo-LDAP 보조 인증에 사용할 원격 액세스 VPN 연결 프로필을 생성하거나 수정합니다.

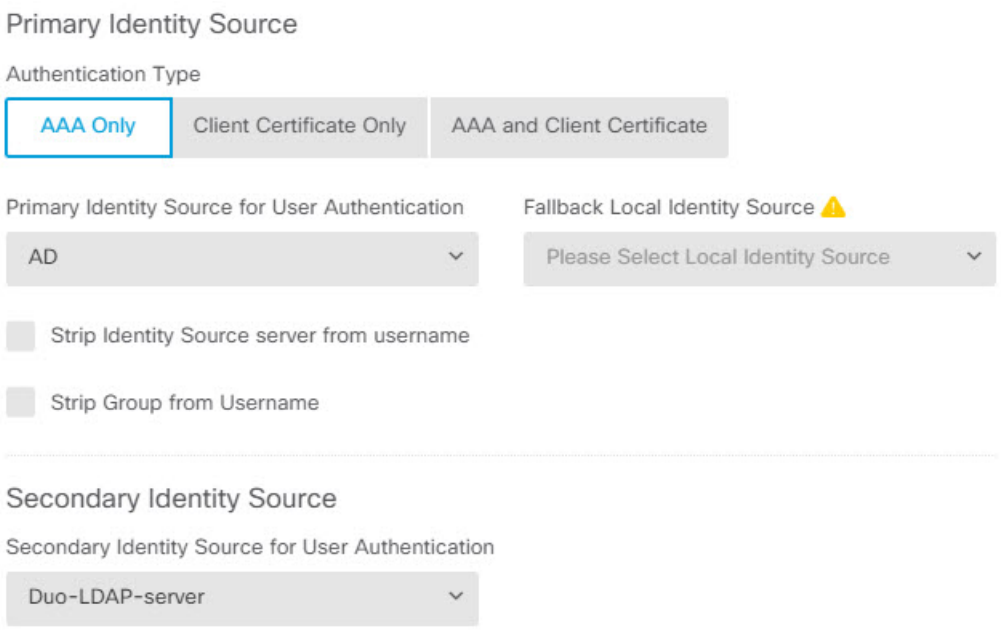
연결 프로필을 구성하는 단계는 여러 가지가 있으며 RA VPN 연결 프로파일 컨피그레이션, 740 페이지에 설명되어 있습니다. 다음 절차에서는 Duo-LDAP를 보조 인증 소스로 활성화하고 Secure Client 프로파일을 적용하기 위한 주요 변경 사항에 대해서만 설명합니다. 새 연결 프로필의 경우 나머지 필수 필드를 구성해야 합니다. 이 절차에서는 기존 연결 프로필을 수정하는 중이며 이러한 두 가지 설정만 변경하면 된다고 가정합니다.

a) RA VPN 페이지의 목차에서 **Connection Profiles(**연결 프로필**)**를 선택합니다.

b) 기존 연결 프로필을 수정하거나 새 프로필을 생성합니다.

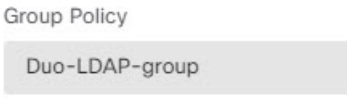
c) Primary Identity Source(기본 ID 소스) 아래에서 다음을 구성합니다.

- **Authentication Type(**인증 유형**) - AAA Only(AAA** 전용**)** 또는 **AAA and Client Certificate(AAA** 및 클라이언트 인증서**)** 중 하나를 선택합니다. AAA를 사용하지 않는 한, 이중 인증을 구성할 수 없습니다.
- **Primary Identity Source for User Authentication(**사용자 인증을 위한 기본 **ID** 소스**)** - 기본 Active Directory 또는 RADIUS 서버를 선택합니다. Duo-LDAP ID 소스를 기본 소스로 선택할 수 있습니다. 그러나 Duo-LDAP에서는 인증 서비스만 제공하며 ID 서비스는 제공하지 않습니다. 따라서 이를 기본 인증 소스로 사용하는 경우, 어떠한 대시보드에도 RA VPN 연결과 관련된 사용자 이름이 표시되지 않으며, 이러한 사용자에 대한 액세스 제어 규칙을 작성할 수 없게 됩니다. 원하는 경우 로컬 ID 소스로의 대체 기능을 구성할 수 있습니다.
- **Secondary Identity Source(**보조 **ID** 소스**)** - Duo-LDAP ID 소스를 선택합니다.



d) **Next(**다음**)**를 클릭합니다.

e) Remote User Experience (원격 사용자 환경) 페이지에서 생성했거나 수정한 **Group Policy(**그룹 정책**)**를 선택합니다.



f) 이 페이지 및 다음 페이지인 Global Settings(글로벌 설정)에서 **Next(**다음**)**를 클릭합니다.

g) **Finish(**마침**)**를 클릭하여 연결 프로필에 변경 사항을 저장합니다.

단계 **7** 변경 사항을 커밋합니다.

a) 웹 페이지의 오른쪽 상단에 있는 **Deploy Changes(**변경 사항 구축**)** 아이콘을 클릭합니다.

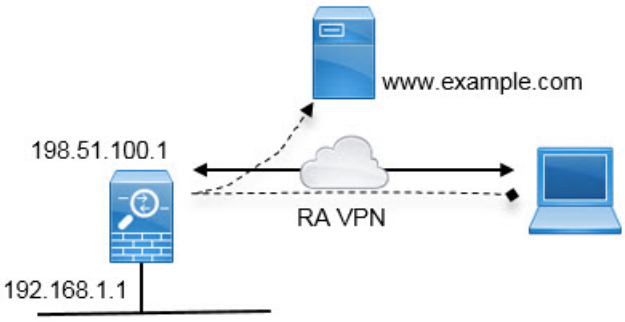
b) **Deploy Now(**지금 구축**)** 버튼을 클릭합니다.

구축이 완료될 때까지 기다리거나 **OK(**확인**)**를 클릭하고 나중에 작업 목록 또는 구축 기록을 확인할 수 있습니다.

원격 액세스 VPN 사용자에게 외부 인터페이스를 통해 인터넷 액세스를 제공하는 방법(헤어피닝)

원격 액세스 VPN에서는 원격 네트워크의 사용자가 디바이스를 통해 인터넷에 액세스하도록 할 수 있습니다. 그러나 원격 사용자는 인터넷에 연결되는 것과 동일한 인터페이스(외부 인터페이스)를 통해 디바이스에 진입하므로 인터넷 트래픽이 외부 인터페이스로 다시 나가도록 바운스해야 합니다. 이 기술을 헤어피닝이라고도 합니다.

다음 그림에 예시가 나와 있습니다. 외부 인터페이스 198.51.100.1에 원격 액세스 VPN이 구성되어 있습니다. 여기서 내부 네트워크로의 트래픽은 디바이스를 계속 통과하게 하면서 인터넷 바인딩 트래픽은 외부 인터페이스로 다시 나가도록 원격 사용자의 VPN 터널을 분할할 수 있습니다. 따라서 원격 사용자가 www.example.com 등의 인터넷 서버로 이동하려는 경우 해당 연결은 먼저 VPN을 통과한 다음 198.51.100.1 인터페이스에서 인터넷으로 다시 라우팅됩니다.



다음 절차에서는 이 서비스를 구성하는 방법을 설명합니다.

시작하기 전에

이 예시에서는 이미 디바이스를 등록했고 원격 액세스 VPN 라이선스를 적용했으며 Secure Client 이미지를 업로드했다고 가정합니다. 또한 ID 정책에서도 사용되는 ID 영역을 구성했다고 가정합니다.

프로시저

단계 1 원격 액세스 VPN 연결을 컨피그레이션합니다.

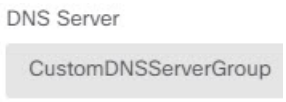
컨피그레이션하려면 연결 프로파일 외에도 맞춤형 그룹 정책이 필요합니다. 헤어피닝은 일반적인 컨피그레이션이며, 그룹 정책의 필수 설정이 일반적으로 적용됩니다. 이 예시에서는 새 그룹 정책을 생성하는 대신 기본 그룹 정책을 수정할 것입니다. 둘 중 한 가지 접근 방식을 선택할 수 있습니다.

a) **Device(**디바이스**)** > **Remote Access VPN(**원격 액세스 **VPN)** 그룹에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

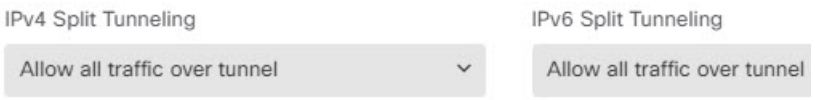
b) 목차에서 **Group Policies(**그룹 정책**)**을 클릭한 후 DfltGrpPolicy 개체에 대해 수정 아이콘( )을 클릭합니다.

c) 기본 그룹 정책을 다음과 같이 변경합니다.

- **General(**일반**)** 페이지의 **DNS Server(DNS** 서버**)**에서 도메인 이름을 확인하기 위해 VPN 엔드포인트에서 사용해야 하는 서버를 정의하는 DNS 서버 그룹을 선택합니다.



- **Split Tunneling(**스플릿 터널링**)** 페이지에서 **IPv4** 및 **IPv6 Split Tunneling(IPv6** 스플릿 터널링**)**에 대해 **Allow all traffic over tunnel option(**터널 옵션을 통해 모든 트래픽 허용**)**을 선택합니다. 이것이 기본 설정이므로 이미 올바르게 컨피그레이션되어 있을 수 있습니다.



참고 이것은 헤어피닝 활성화에 중요한 설정입니다**.** 여기서 모든 트래픽을 VPN 게이트웨이로 이동하게 할 수 있습니다. 스플릿 터널링은 원격 클라이언트가 VPN 외부의 로컬 또는 인터넷 사이트에 직접 액세스하도록 허용하는 방식입니다.

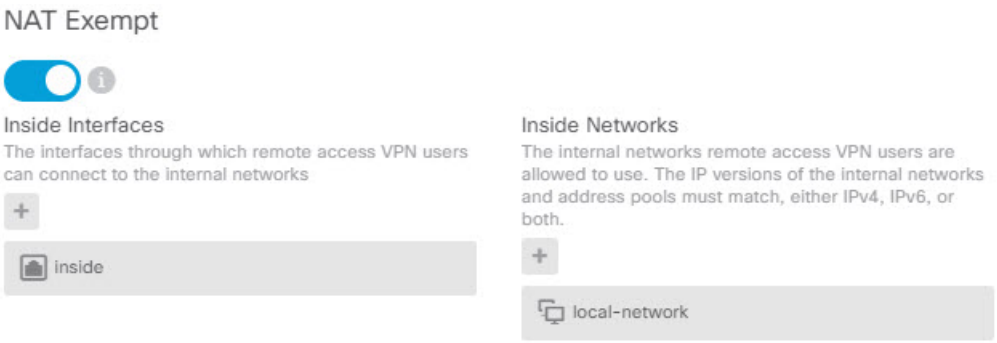
d) 기본 그룹 정책에 대한 변경 사항을 저장하려면 **OK(**확인**)**를 클릭합니다.

e) **Connection Profiles(**연결 프로파일**)**를 클릭하고 기존 프로파일을 수정하거나 새 프로파일을 생성합니다.

f) 연결 프로파일에서 마법사를 두루 탐색하여 기타 RA VPN 컨피그레이션에 대해 원하는 모든 옵션을 컨피그레이션합니다. 그러나 헤어피닝을 활성화하려면 다음 옵션을 올바르게 컨피그레이션해야 합니다.

- 2단계의 **Group Policy(**그룹 정책**)**입니다. 헤어피닝에 대해 맞춤형 그룹 정책을 선택합니다.

- 3단계의 **NAT Exempt(NAT** 제외**)**. 이 기능을 활성화합니다. 내부 인터페이스를 선택한 다음, 내부 네트워크를 정의하는 네트워크 개체를 선택합니다. 이 예시에서는 개체에 192.168.1.0/24를 지정해야 합니다. 내부 네트워크로 이동하는 RA VPN 트래픽의 경우 주소 변환이 수행되지 않습니다. 하지만 헤어피닝된 트래픽은 외부 인터페이스에서 나가므로 NAT가 수행됩니다. NAT 면제는 내부 인터페이스에만 적용되기 때문입니다. 다른 연결 프로파일을 정의한 경우, 컨피그레이션이 모든 연결 프로파일에 적용되므로 기존 설정에 추가해야 한다는 점에 유의하십시오.



참고 **NAT Exempt(NAT** 제외**)** 옵션은 헤어핀 컨피그레이션에 대한 기타 중요 설정입니다.

g) (선택 사항). **Global Settings(**전역 설정**)** 단계에서 **Bypass Access Control policy for decrypted traffic(**암호 해독된 트래픽에 대해 액세스 제어 정책 우회**) (sysopt permit-vpn)** 옵션을 선택합니다.

이 옵션을 선택하면 RA VPN 풀 주소에서 발신되는 트래픽을 허용하도록 액세스 제어 규칙을 컨피그레이션할 필요가 없어집니다. 이 옵션에서는 향상된 보안을 제공합니다(외부 사용자가 풀에서 주소를 스푸핑할 수 없음). 그러나 이것은 RA VPN 트래픽에 대해서는 URL 필터링 및 침입 방지를 포함한 검사가 면제됨을 뜻합니다. 장점과 단점을 고려한 후 이 옵션을 선택할지 결정하십시오.

h) RA VPN 컨피그레이션을 검토한 다음, **Finish(**마침**)**를 클릭합니다.

단계 **2** 외부 인터페이스에서 외부 IP 주소의 포트로 나가는 모든 연결을 변환하는 NAT 규칙(인터페이스 PAT)을 구성합니다.

초기 디바이스 컨피그레이션을 완료하면 InsideOutsideNatRule이라는 NAT 규칙이 생성됩니다. 이 규칙은 외부 인터페이스를 통해 디바이스에서 나가는 모든 인터페이스의 IPv4 트래픽에 인터페이스 PAT를 적용합니다. 외부 인터페이스는 "Any" 소스 인터페이스에 포함되므로 필요한 규칙을 수정하거나 삭제한 경우가 아니면 규칙이 이미 존재합니다.

다음 절차에서는 필요한 규칙을 생성하는 방법을 설명합니다.

a) **Policies(**정책**)** > **NAT**를 클릭합니다.

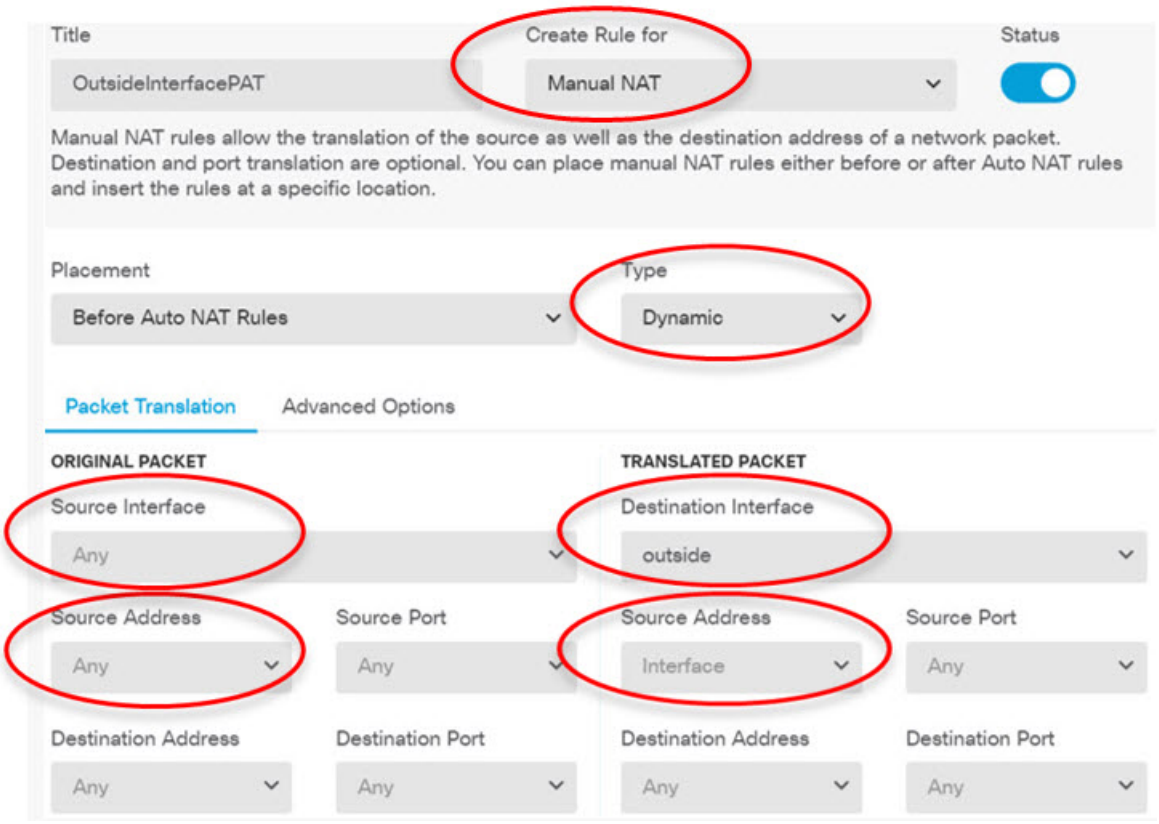
b) 다음 중 하나를 수행합니다.

- InsideOutsideNatRule을 수정하려면 **Action(**작업**)** 열 위에 마우스를 놓고 수정 아이콘( )을 클릭합니다.
- 새 규칙을 생성하려면 **+**를 클릭합니다.

c) 다음 속성을 사용하여 규칙을 구성합니다.

- **Title(**제목**)** - 새 규칙의 경우 의미 있는 이름을 공백 없이 입력합니다. 예를 들어 OutsideInterfacePAT를 입력합니다.
- **Create Rule For(**규칙 생성 대상**)** - **Manual NAT(**수동 **NAT)**.
- **Placement(**배치**)** - **Before Auto NAT Rules(**자동 **NAT** 규칙 앞**)**(기본값).
- **Type(**유형**)** - **Dynamic(**동적**)**.
- **Original Packet(**원본 패킷**)** - **Source Address(**소스 주소**)**의 경우 Any(모두) 또는 any-ipv4를 선택합니다. **Source Interface(**소스 인터페이스**)**의 경우 기본값인 Any(모두)를 선택해야 합니다. 기타 모든 Original Packet(원본 패킷) 옵션의 경우 기본값인 Any(모두)를 유지합니다.
- **Translated Packet(**변환된 패킷**)** - **Destination Interface(**대상 인터페이스**)**의 경우 outside(외부)를 선택합니다. **Translated Address(**변환된 주소**)**의 경우 **Interface(**인터페이스**)**를 선택합니다. 기타 모든 Translated Packet(변환된 패킷) 옵션의 경우 기본값인 Any(모두)를 유지합니다.

다음 그림에는 소스 주소로 Any(모두)를 선택하는 간단한 사례가 나와 있습니다.



d) **OK(**확인**)**를 클릭합니다.

단계 **3** (연결 프로파일에서 **Bypass Access Control policy for decrypted traffic(**암호 해독된 트래픽에 대해 액세스 제어 정책 우회**) (sysopt permit-vpn)**을 컨피그레이션하지 않는 경우.) 원격 액세스 VPN 주소 풀에서 액세스를 허용하는 액세스 제어 규칙을 구성합니다.

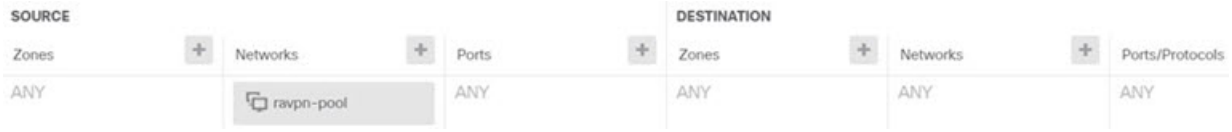
연결 프로파일에서 **Bypass Access Control policy for decrypted traffic(**암호 해독된 트래픽에 대해 액세스 제어 정책 우회**) (sysopt permit-vpn)**을 선택하는 경우, RA VPN 풀 주소에서 발신되는 트래픽은 액세스 제어 정책을 우회합니다. 트래픽에 적용할 액세스 제어 규칙을 작성할 수 없습니다. 옵션을 비활성화하는 경우에만 규칙을 작성해야 합니다.

다음 예시에서는 주소 풀에서 특정 대상으로의 트래픽을 허용합니다. 구체적인 요구 사항에 맞게 이 예시를 조정할 수 있습니다. 또한 이 규칙 앞에 원치 않는 트래픽을 필터링하여 제거하는 차단 규칙을 배치할 수도 있습니다.

a) **Policies(**정책**)** > **Access Control(**액세스 제어**)**을 클릭합니다.
b) +를 클릭하여 새 규칙을 생성합니다.
c) 다음 속성을 사용하여 규칙을 구성합니다.

- **Order(**순서**)** - 연결을 찾아 차단하는 다른 규칙 앞에 해당 규칙을 넣도록 정책 내의 위치를 선택합니다. 기본적으로는 규칙이 정책의 끝에 추가됩니다. 나중에 규칙을 재배치해야 하는 경우 이 옵션을 수정하거나, 규칙을 끌어서 표의 원하는 슬롯에 놓을 수 있습니다.
- **Title(**제목**)** - 의미 있는 이름을 공백 없이 입력합니다. 예를 들어 RAVPN-address-pool을 입력합니다.

- **Action(**작업**) - Allow(**허용**)**. 이 트래픽의 프로토콜 위반 또는 침입을 검사하지 않으려는 경우 Trust(신뢰)를 선택할 수 있습니다.
- **Source/Destination(**소스/대상**)** 탭 - **Source(**소스**)** > **Network(**네트워크**)**의 경우 주소 풀의 RA VPN 연결 프로파일에서 사용한 것과 같은 개체를 선택합니다. 기타 모든 Source(소스) 및 Destination(대상) 옵션의 경우 기본값인 Any(모두)를 유지합니다.



- **Application(**애플리케이션**)**, **URL** 및 **Users(**사용자**)** 탭 - 이러한 탭에서는 기본 설정, 즉 아무 설정도 선택하지 않은 상태를 유지합니다.
- **Intrusion(**침입**)**, **File(**파일**)** 탭 - 선택적으로 위협이나 악성코드를 검사하기 위한 침입 또는 파일 정책을 선택할 수 있습니다.
- **Logging(**로깅**)** 탭 - 선택적으로 연결 로깅을 활성화할 수 있습니다.

d) **OK(**확인**)**를 클릭합니다.

단계 **4** 변경 사항을 커밋합니다.

a) 웹 페이지의 오른쪽 상단에 있는 **Deploy Changes(**변경 사항 구축**)** 아이콘을 클릭합니다.

b) **Deploy Now(**지금 구축**)** 버튼을 클릭합니다.

구축이 완료될 때까지 기다리거나 **OK(**확인**)**를 클릭하고 나중에 작업 목록 또는 구축 기록을 확인할 수 있습니다.

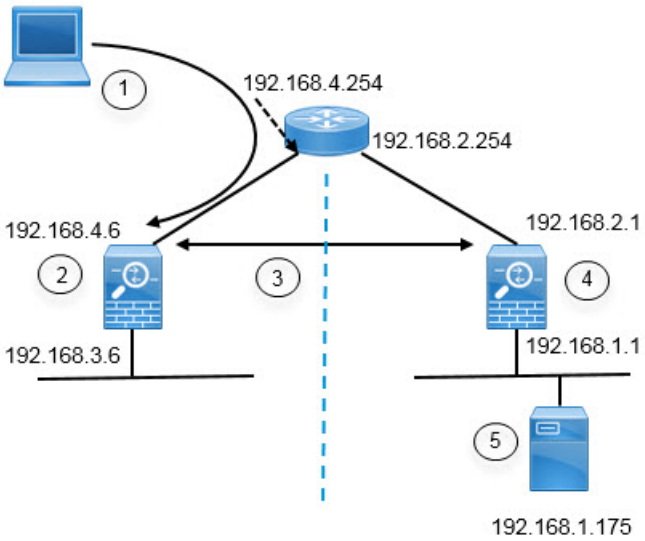
원격 액세스 VPN을 통해 외부 네트워크에서 디렉터리 서버를 사용하는 방법

모바일 작업자와 재택 근무자가 내부 네트워크에 안전하게 연결할 수 있도록 원격 액세스 VPN을 구성할 수 있습니다. 연결의 보안은 권한이 있는 사용자만 진입할 수 있도록 사용자 연결을 인증하는 디렉터리 서버에 따라 달라집니다.

디렉터리 서버가 내부 네트워크가 아닌 외부 네트워크에 있는 경우에는 외부 인터페이스에서 디렉터리 서버를 포함하는 네트워크로의 사이트 대 사이트 VPN 연결을 구성해야 합니다. 사이트 대 사이트 **VPN** 컨피그레이션을 수행할 때 기억해야 할 한 가지 사항은, 디렉터리 서버가 있는 디바이스의 원격 네트워크와 사이트 대 사이트 VPN 연결의 "내부" 네트워크 내에 원격 액세스 VPN 디바이스의 외부 인터페이스 주소를 포함해야 한다는 것입니다. 다음 절차에서 이에 대해 자세히 설명하겠습니다.

참고 가상 관리 인터페이스의 게이트웨이로 데이터 인터페이스를 사용하는 경우 이 컨피그레이션은 ID 정책용 디렉터리 사용도 활성화합니다. 데이터 인터페이스를 관리 게이트웨이로 사용하지 않는 경우에는 관리 네트워크에서 사이트 대 사이트 VPN 연결에 참여하는 내부 네트워크로의 경로가 있는지 확인하십시오.

이 활용 사례에서는 다음 네트워크 시나리오를 구현합니다.



그림의 설명선	**Description**
1	192.168.4.6에 대한 VPN 연결을 설정하는 원격 액세스 호스트. 클라이언트는 172.18.1.0/24 주소 풀의 주소를 가져옵니다.
2	원격 액세스 VPN을 호스팅하는 사이트 A
3	사이트 A 및 사이트 B threat defense 디바이스의 외부 인터페이스 간 사이트 대 사이트 VPN 터널.
4	디렉터리 서버를 호스팅하는 사이트 B
5	사이트 B의 내부 네트워크에 있는 디렉터리 서버

시작하기 전에

이 활용 사례에서는 디바이스 설정 마법사의 단계에 따라 일반 베이스라인 컨피그레이션을 설정했다고 가정합니다. 구체적으로 다음과 같습니다.

- inside_zone에서 outside_zone으로 이동하는 트래픽을 허용(신뢰)하는 Inside_Outside_Rule 액세스 제어 규칙이 있습니다.
- inside_zone 및 outside_zone 보안 영역은 각각 내부 및 외부 인터페이스를 포함합니다.

- 내부 인터페이스에서 외부 인터페이스로 이동하는 모든 트래픽에 대해 인터페이스 PAT를 수행하는 InsideOutsideNATRule이 있습니다. 기본적으로 내부 브리지 그룹을 사용하는 디바이스에는 인터페이스 PAT에 대한 여러 규칙이 있을 수 있습니다.
- 외부 인터페이스를 가리키는 0.0.0.0/0에 대한 고정 IPv4 경로가 있습니다. 이 예시에서는 외부 인터페이스에 대해 고정 IP 주소를 사용한다고 가정하지만, DHCP를 사용하여 정적 경로를 동적으로 가져올 수도 있습니다. 이 예시에서는 다음 정적 경로를 사용한다고 가정합니다.
  - 사이트 A: 외부 인터페이스, 게이트웨이: 192.168.4.254
  - 사이트 B: 외부 인터페이스, 게이트웨이: 192.168.2.254

프로시저

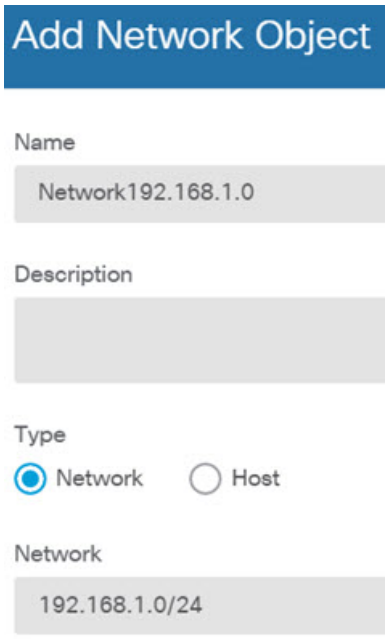
단계 **1** 디렉터리 서버를 호스팅하는 사이트 **B**에서 사이트 대 사이트 VPN 연결을 구성합니다.

a) **Device(**디바이스**)**를 클릭한 다음 사이트 대 사이트 VPN 그룹에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

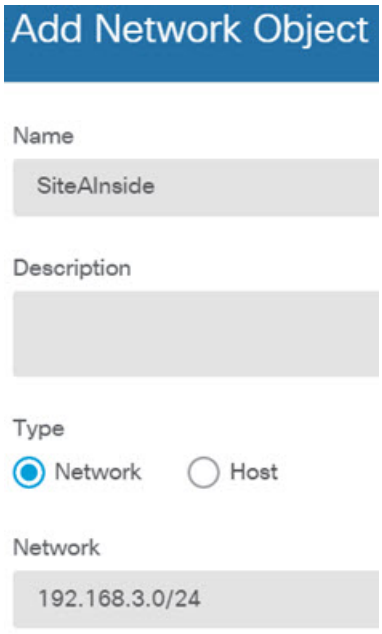
b) **+** 버튼을 클릭합니다.

c) 엔드포인트 설정에 대해 다음 옵션을 구성합니다.

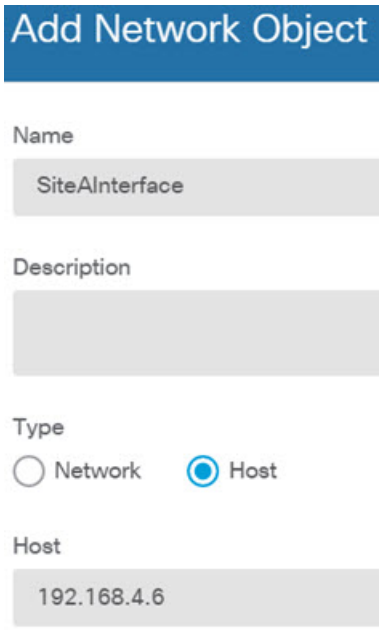
- **Connection Profile Name(**연결 프로파일 이름**)** — 사이트 A에 대한 연결임을 나타내는 SiteA와 같은 이름을 입력합니다.
- 로컬 사이트 - 이러한 옵션은 로컬 엔드포인트를 정의합니다.
  - **Local VPN Access Interface(**로컬 **VPN** 액세스 인터페이스**)** — 외부 인터페이스(다이어그램에서 주소가 192.168.2.1인 인터페이스)를 선택합니다.
  - **Local Network(**로컬 네트워크**) -** +를 클릭하고 VPN 연결에 참여해야 하는 로컬 네트워크를 식별하는 네트워크 개체를 선택합니다. 디렉터리 서버는 이 네트워크에 있으므로 사이트 대 사이트 VPN에 참여할 수 있습니다. 개체가 아직 없다고 가정하고, **Create New Network(**새 네트워크 생성**)**를 클릭하여 192.168.1.0/24 네트워크에 대한 개체를 구성합니다. 개체를 저장한 후 드롭다운 목록에서 해당 개체를 선택하고 **OK(**확인**)**를 클릭합니다.



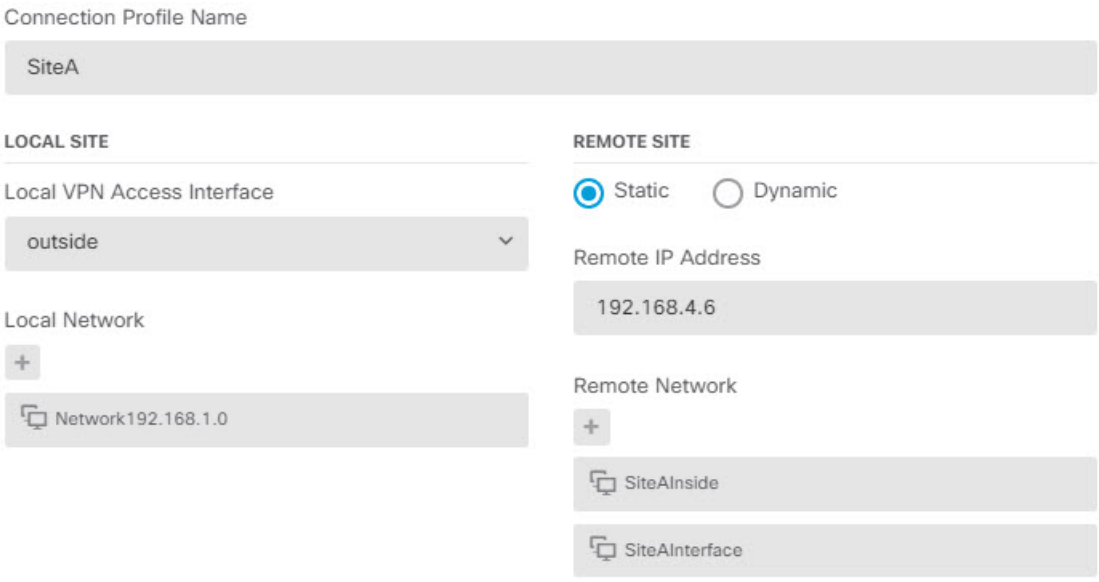
- 원격 사이트 - 이러한 옵션은 원격 엔드포인트를 정의합니다.
  - **Remote IP Address(**원격 **IP** 주소**)** — VPN 연결을 호스팅할 원격 VPN 피어 인터페이스의 IP 주소인 192.168.4.6을 입력합니다.
  - **Remote Network(**원격 네트워크**)** — **+**를 클릭하고 VPN 연결에 참여해야 하는 원격 네트워크를 식별하는 네트워크 개체를 선택합니다. **Create New Network(**새 네트워크 생성**)**를 클릭하고 다음 개체를 구성한 후에 목록에서 해당 개체를 선택합니다.
    1. SiteAInside, 네트워크, 192.168.3.0/24



2. SiteAInterface, 호스트, 192.168.4.6. 이 개체를 구성할 때 주의해야 할 점은, 해당 인터페이스에서 호스팅되는 **RA VPN**이 디렉터리 서버를 사용할 수 있도록 사이트 대 사이트 **VPN** 연결용 원격 네트워크의 일부분으로 원격 액세스 **VPN** 연결 지점 주소를 포함해야 한다는 것입니다.



개체 구성을 완료하고 나면 엔드포인트 설정이 다음과 같이 표시됩니다.



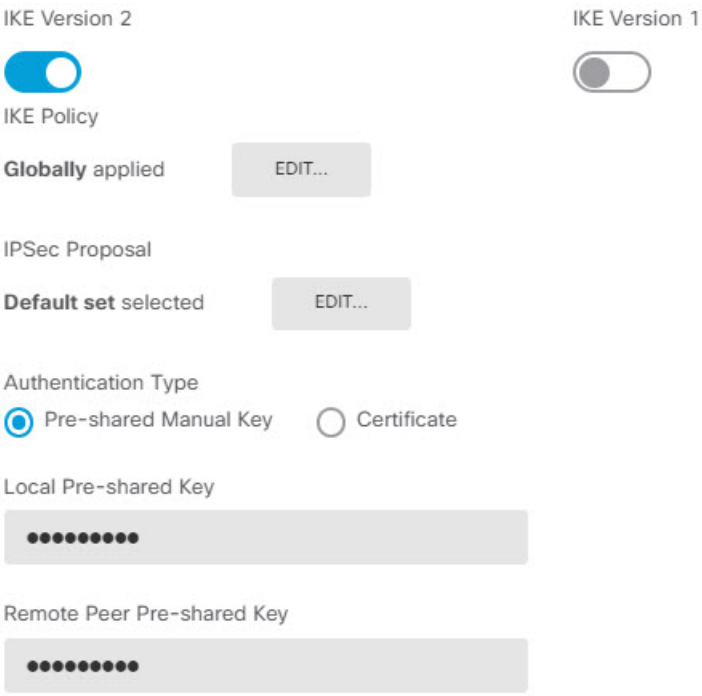
d) **Next(**다음**)**를 클릭합니다.

e) VPN에 대한 프라이버시 컨피그레이션을 정의합니다.

이 활용 사례에서는 강력한 암호화 사용을 허용하는 내보내기 제어 기능을 사용할 수 있다고 가정합니다. 라이선스 컴플라이언스와 요구사항을 충족하도록 이러한 예시 설정을 조정하십시오.

- **IKE** 버전 **2**, **IKE** 버전 **1** - **IKE** 버전 **2**는 활성화되고 **IKE** 버전 **1**은 비활성화된 기본값을 유지합니다.
- **IKE** 정책 - 수정을 클릭하여 **AES-GCM-NULL-SHA** 및 **AES-SHA-SHA**를 활성화하고 **DES-SHA-SHA**를 비활성화합니다.
- **IPsec** 제안 - 수정을 클릭하고 IPSec 제안 선택 대화 상자에서 +를 클릭한 다음 기본값 설정을 클릭하여 기본 AES-GCM 제안을 선택합니다.
- 로컬 사전 공유 키, 원격 피어 사전 공유 키 - VPN 연결을 위한 원격 디바이스와 이 디바이스에 정의된 키를 입력합니다. IKEv2에서는 이러한 키가 다를 수 있습니다. 키는 영숫자 1~127자가 될 수 있습니다. 사이트 **A** 디바이스에서 사이트 대 사이트 **VPN** 연결을 생성할 때 동일한 문자열을 구성해야 하므로 이러한 키를 기억해 두어야 합니다**.**

IKE 정책은 다음과 같이 표시됩니다.



f) 추가 옵션을 구성합니다.

- **NAT Exempt(NAT** 제외**)** — 내부 네트워크를 호스팅하는 인터페이스(이 예시에서는 내부 인터페이스)를 선택합니다. 일반적으로는 사이트 대 사이트 VPN 터널 내 트래픽의 IP 주소를 변환하지 않습니다. 이 옵션은 로컬 네트워크가 단일 라우팅 인터페이스(브리지 그룹 멤버 아님) 뒤에 있는 경우에만 작동합니다. 로컬 네트워크가 둘 이상의 라우팅 인터페이스 또는 하나 이상의 브리지 그룹 멤버 뒤에 있는 경우에는 NAT 제외 규칙을 수동으로 생

성해야 합니다. 필요한 규칙을 수동으로 생성하는 방법에 대한 자세한 내용은 NAT에서 사이트 대 사이트 VPN 트래픽 제외, 705 페이지를 참조하십시오.

- **Diffie-Helman Group for Perfect Forward Secrecy(PFS(Perfect Forward Secrecy)**를 위한 **Diffie-Hellman)** 그룹 — 그룹 **19**를 선택합니다. 이 옵션은 PFS(Perfect Forward Secrecy)를 사용하여 암호화된 각 교환에 대해 고유 세션 키를 생성하고 사용할지를 결정합니다. 고유 세션 키는 전체 교환이 기록되었으며 공격자가 엔드포인트 디바이스에서 사용하는 사전 공유 키 또는 개인 키를 확보했더라도 후속 암호 해독에서 교환을 보호합니다. 옵션에 대한 설명은 사용할 Diffie-Hellman 모듈러스 그룹 결정, 682 페이지를 참조하십시오.

옵션은 다음과 같이 표시됩니다.

g) **Next(**다음**)**를 클릭합니다.

h) 요약을 검토하고 **Finish(**종료**)**를 클릭합니다.

요약 정보가 클립보드에 복사됩니다. 해당 정보를 문서에 붙여넣은 다음 원격 피어를 구성하는 데 사용하거나 피어 구성 담당자에게 보낼 수 있습니다.

i) 웹 페이지의 오른쪽 상단에 있는 **Deploy Changes(**변경 사항 구축**)** 아이콘을 클릭합니다.

j) **Deploy Now(**지금 구축**)** 버튼을 클릭하고 구축이 정상적으로 완료될 때까지 기다립니다.

이제 사이트 B 디바이스는 사이트 대 사이트 VPN 연결의 한쪽을 호스팅할 준비가 되었습니다.

단계 **2** 사이트 **B** 디바이스에서 로그아웃하고 사이트 **A** 디바이스에 로그인합니다.

단계 **3** 원격 액세스 VPN을 호스팅할 사이트 **A**에서 사이트 대 사이트 VPN 연결을 구성합니다.

a) **Device(**디바이스**)**를 클릭한 다음 사이트 대 사이트 VPN 그룹에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

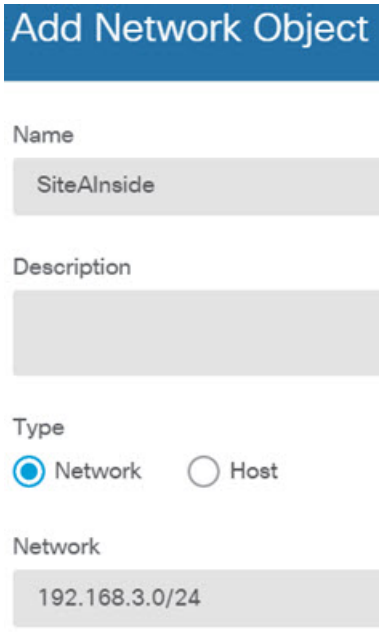
b) **+** 버튼을 클릭합니다.

c) 엔드포인트 설정에 대해 다음 옵션을 구성합니다.

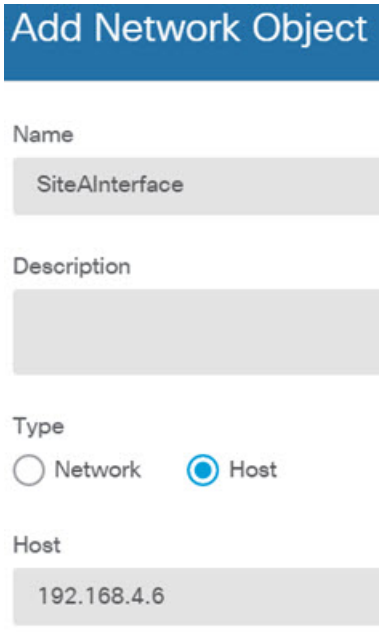
- **Connection Profile Name(**연결 프로파일 이름**)** — 사이트 B에 대한 연결임을 나타내는 SiteB와 같은 이름을 입력합니다.
- 로컬 사이트 - 이러한 옵션은 로컬 엔드포인트를 정의합니다.
  - **Local VPN Access Interface(**로컬 **VPN** 액세스 인터페이스**)** — 외부 인터페이스(다이어그램에서 주소가 192.168.4.6인 인터페이스)를 선택합니다.
  - **Local Network(**로컬 네트워크**)** — **+**를 클릭하고 VPN 연결에 참여해야 하는 로컬 네트워크를 식별하는 네트워크 개체를 선택합니다. **Create New Network(**새 네트워크 생

성)를 클릭하고 다음 개체를 구성한 후에 목록에서 해당 개체를 선택합니다. 사이트 B 디바이스에서 같은 개체를 생성했어도 사이트 A 디바이스에서 해당 개체를 다시 생성해야 합니다.

1. SiteAInside, 네트워크, 192.168.3.0/24

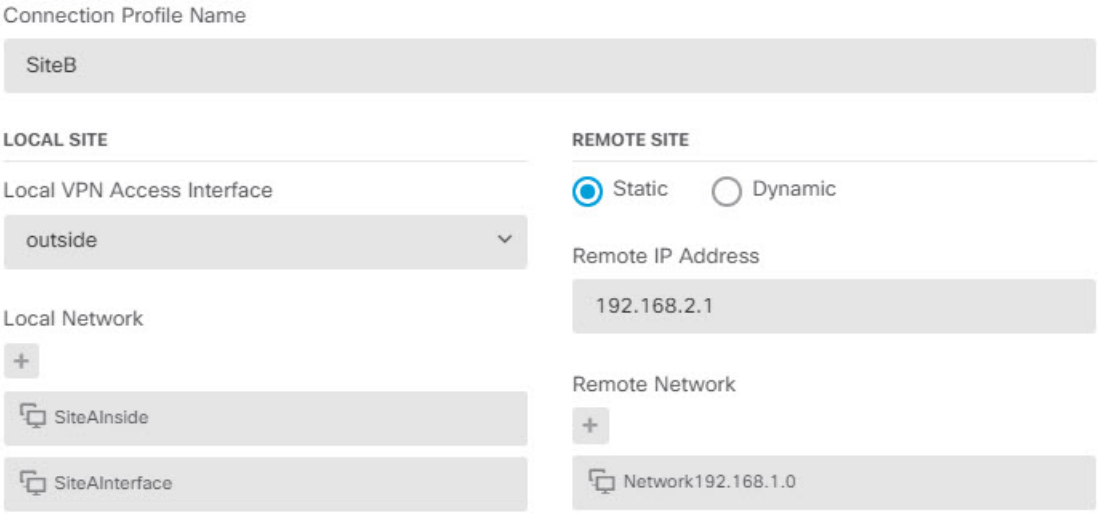


2. SiteAInterface, 호스트, 192.168.4.6. 이 개체를 구성할 때 주의해야 할 점은, 해당 인터페이스에서 호스팅되는 RA VPN이 원격 네트워크의 디렉터리 서버를 사용할 수 있도록 사이트 대 사이트 VPN 연결용 내부 네트워크의 일부분으로 원격 액세스 VPN 연결 지점 주소를 포함해야 한다는 것입니다.



- 원격 사이트 - 이러한 옵션은 원격 엔드포인트를 정의합니다.
  - **Remote IP Address(**원격 **IP** 주소**)** — VPN 연결을 호스팅할 원격 VPN 피어 인터페이스의 IP 주소인 192.168.2.1을 입력합니다.
  - **Remote Network(**원격 네트워크**)** — **+**를 클릭하고 VPN 연결에 참여해야 하는 원격 네트워크를 식별하는 네트워크 개체(디렉터리 서버를 포함하는 개체)를 선택합니다. 새 네트워크 생성을 클릭하여 192.168.1.0/24 네트워크에 대한 개체를 구성합니다. 개체를 저장한 후 드롭다운 목록에서 해당 개체를 선택하고 **OK(**확인**)**를 클릭합니다. 사이트 **B** 디바이스에서 같은 개체를 생성했어도 사이트 **A** 디바이스에서 해당 개체를 다시 생성해야 합니다**.**

개체 구성을 마치면 엔드포인트 설정이 다음과 같이 표시됩니다. 로컬/원격 네트워크는 사이트 B 설정과 반대입니다. 포인트 투 포인트 연결의 양쪽은 항상 이렇게 표시되어야 합니다.

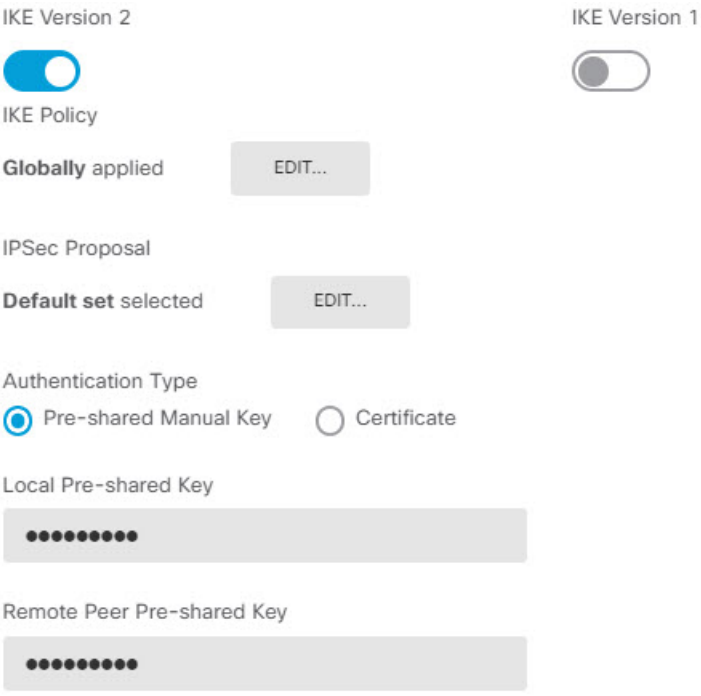


d) **Next(**다음**)**를 클릭합니다.

e) VPN에 대한 프라이버시 컨피그레이션을 정의합니다.

사이트 B에서와 동일한 IKE 버전, 정책, IPsec 제안 및 사전 공유 키를 구성하되 로컬 사전 공유 키와 원격 사전 공유 키를 반대로 구성해야 합니다.

IKE 정책은 다음과 같이 표시됩니다.



f) 추가 옵션을 구성합니다.

- **NAT Exempt(NAT** 제외**)** — 내부 네트워크를 호스팅하는 인터페이스(이 예시에서는 내부 인터페이스)를 선택합니다. 일반적으로는 사이트 대 사이트 VPN 터널 내 트래픽의 IP 주소

를 변환하지 않습니다. 이 옵션은 로컬 네트워크가 단일 라우팅 인터페이스(브리지 그룹 멤버 아님) 뒤에 있는 경우에만 작동합니다. 로컬 네트워크가 둘 이상의 라우팅 인터페이스 또는 하나 이상의 브리지 그룹 멤버 뒤에 있는 경우에는 NAT 제외 규칙을 수동으로 생성해야 합니다. 필요한 규칙을 수동으로 생성하는 방법에 대한 자세한 내용은 NAT에서 사이트 대 사이트 VPN 트래픽 제외, 705 페이지를 참조하십시오.

- **Diffie-Helman Group for Perfect Forward Secrecy(PFS(Perfect Forward Secrecy)**를 위한 **Diffie-Hellman)** 그룹 — 그룹 **19**를 선택합니다.

옵션은 다음과 같이 표시됩니다.

g) **Next(**다음**)**를 클릭합니다.
h) 요약을 검토하고 **Finish(**종료**)**를 클릭합니다.
i) 웹 페이지의 오른쪽 상단에 있는 **Deploy Changes(**변경 사항 구축**)** 아이콘을 클릭합니다.

j) **Deploy Now(**지금 구축**)** 버튼을 클릭하고 구축이 정상적으로 완료될 때까지 기다립니다.

이제 사이트 A 디바이스는 사이트 대 사이트 VPN 연결의 반대쪽을 호스팅할 준비가 되었습니다. 사이트 B가 호환 설정으로 이미 구성되어 있으므로 두 디바이스는 VPN 연결을 협상합니다.

디바이스 CLI에 로그인한 다음 디렉터리 서버 ping을 수행하여 연결을 확인할 수 있습니다. **show ipsec sa** 명령을 사용하여 세션 정보를 확인할 수도 있습니다.

단계 **4** 사이트 **A**에서 디렉터리 서버를 구성합니다. 테스트를 클릭하여 연결이 있는지 확인합니다.

a) 목차에서 **Objects(**개체**)**와 **Identity Sources(ID** 소스**)**를 차례로 선택합니다.
b) **+** > **AD**를 클릭합니다.
c) 기본 영역 속성을 구성합니다.

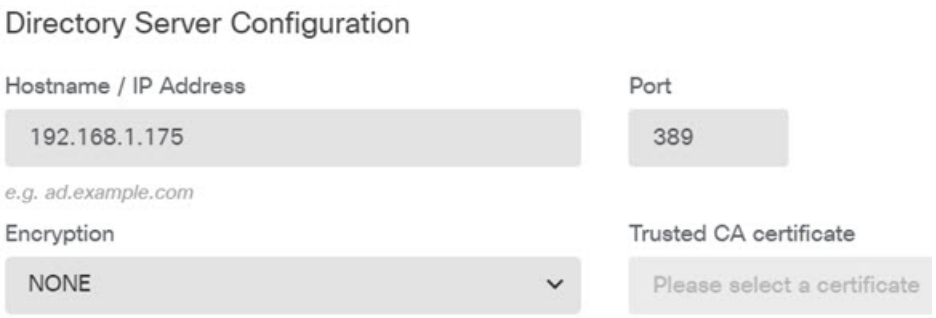
- **Name(**이름**)** — 디렉토리 영역의 이름입니다. AD와 같은 이름이 지정되어 있을 수 있습니다.
- **Type(**유형**)** - 디렉터리 서버의 유형입니다. 지원되는 유형은 Active Directory뿐이며 이 필드의 내용은 변경할 수 없습니다.
- **Directory Username(**디렉터리 사용자 이름**)**, **Directory Password(**디렉터리 비밀번호**)** - 검색하려는 사용자 정보에 대한 적절한 권한이 있는 사용자의 고유 사용자 이름 및 비밀번호입니다. Active Directory의 경우에는 사용자에게 상승된 권한이 필요하지 않습니다. 도메인에 어떤 사용자라도 지정할 수 있습니다. 사용자 이름은 모든 자격 요건에 부합해야 합니다(예: 단지 Administrator가 아닌 Administrator@example.com).

참고 시스템은 이 정보에서 ldap-login-dn 및 ldap-login-password를 생성합니다. 예를 들어 Administrator@example.com은 cn=administrator,cn=users,dc=example,dc=com으로 변환됩니다. cn=users는 항상 이 변환에 포함되므로 일반 이름 "users" 폴더 아래에 여기서 지정하는 사용자를 구성해야 합니다.

- **Base DN(**기본 **DN)** - 사용자 및 그룹 정보를 검색하거나 쿼리하기 위한 디렉터리 트리, 즉 사용자와 그룹의 공통 상위 항목입니다. cn=users,dc=example,dc=com을 예로 들 수 있습니다. 기본 DN을 찾는 방법에 대한 자세한 내용은 디렉터리 기본 DN 결정, 176 페이지를 참조하십시오.
- **AD Primary Domain(AD** 기본 도메인**)** - 디바이스가 조인해야 하는 정규화된 Active Directory 도메인 이름입니다. example.com 등을 예로 들 수 있습니다.

d) 디렉터리 서버 속성을 구성합니다.

- **Hostname/IP Address(**호스트 이름**/IP** 주소**)** - 디렉터리 서버의 호스트 이름 또는 IP 주소입니다. 서버에 대한 암호화된 연결을 사용하는 경우에는 IP 주소가 아닌 FQDN(Fully-Qualified Domain Name)을 입력해야 합니다. 이 예시에서는 192.168.1.175를 입력합니다.
- **Port(**포트**)** - 서버와의 통신에 사용되는 포트 번호입니다. 기본값은 389입니다. 암호화 방법으로 LDAPS를 선택하는 경우에는 포트 636을 사용합니다. 이 예시에서는 389를 유지합니다.
- **Encryption(**암호화**)** - 사용자 및 그룹 정보를 다운로드하기 위해 암호화된 연결을 사용할지를 선택합니다. 기본값은 **None(**없음**)**입니다. 이 옵션은 사용자 및 그룹 정보를 일반 텍스트로 다운로드함을 의미합니다. RA VPN의 경우 **LDAPS**(LDAP over SSL)를 사용할 수 있습니다. 이 옵션을 선택하는 경우 포트 636을 사용합니다. RA VPN은 STARTTLS를 지원하지 않습니다. 이 예시에서는 없음을 선택합니다.
- **Trusted CA Certificate(**신뢰할 수 있는 **CA** 인증서**)** - 암호화 방법을 선택하는 경우 CA(인증 증명) 인증서를 업로드하여 시스템과 디렉터리 서버 간에 신뢰할 수 있는 연결을 설정합니다. 인증서를 사용하여 인증하는 경우에는 인증서의 서버 이름이 서버 호스트 이름/IP 주소와 일치해야 합니다. 예를 들어 IP 주소로 192.168.1.175를 사용하는데 인증서의 주소는 ad.example.com이면 연결은 실패합니다.



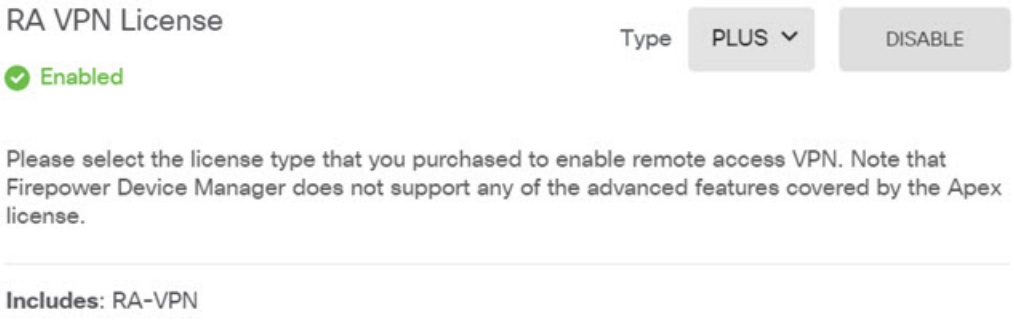
e) **Test(**테스트**)** 버튼을 클릭하여 시스템이 서버에 연결할 수 있는지 확인합니다.

시스템은 별도의 프로세스를 사용하여 서버에 액세스하므로, 연결이 특정 사용 유형에는 작동하지만 다른 유형에는 작동하지 않음을 나타내는 오류가 발생합니다. 연결을 ID 정책에는 사용할 수 있지만, 원격 액세스 VPN에는 사용할 수 없는 경우를 예로 들 수 있습니다. 서버에 연결할 수 없는 경우에는 IP 주소와 호스트 이름이 올바른지와 DNS 서버에 호스트 이름의 항목이 있는지 등을 확인합니다. 또한, 사이트 대 사이트 VPN 연결이 작동하고, 사이트 A의 외부 인터페이스 주소를 VPN에 포함했으며, NAT가 디렉터리 서버에 대한 트래픽을 변환하지 않는지 확인합니다. 서버에 대한 정적 경로도 구성해야 할 수 있습니다.

f) **OK(**확인**)**를 클릭합니다.

단계 **5** **Device(**디바이스**)** > **Smart License(**스마트 라이선스**)** > **View Configuration(**컨피그레이션 보기**)**을 클릭하고 RA VPN 라이선스를 활성화합니다.

RA VPN 라이선스를 활성화하는 경우 구매한 라이선스의 유형을 선택합니다. Plus나 Apex 중 하나 또는 둘 다를 선택하거나 VPN Only를 선택할 수 있습니다. 자세한 내용은 원격 액세스 VPN에 대한 라이선싱 요구 사항, 732 페이지를 참고하십시오.

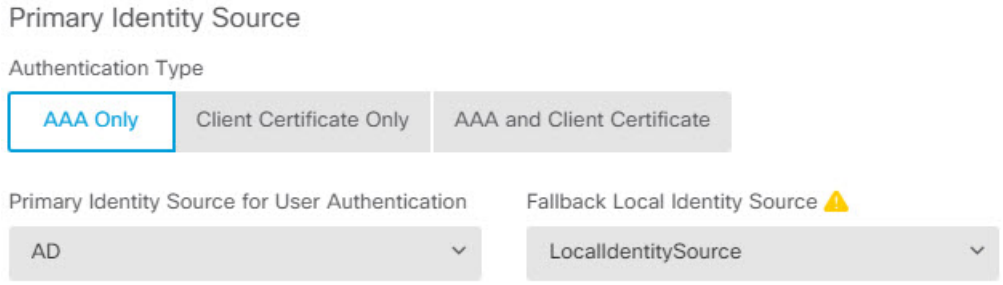


단계 **6** 사이트 A에서 원격 액세스 VPN을 구성합니다.

a) **Device(**디바이스**)** > **Remote Access VPN(**원격 액세스 **VPN)** 그룹에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다. **Connection Profiles(**연결 프로파일**)** 페이지 있어야 합니다.

b) 연결 프로파일을 생성하거나 수정합니다.

c) 마법사의 첫 번째 단계에서는 프로파일 이름을 컨피그레이션하고 AD 영역을 기본 인증 소스로 선택합니다. 선택적으로 로컬 데이터베이스를 대체 ID 소스로 선택할 수 있습니다.



d) 주소 풀을 컨피그레이션합니다.

이 예시에서는 +를 클릭한 후 IPv4 주소 풀에서 **Create New Network(**새 네트워크 생성**)**를 선택하고 172.18.1.0/24 네트워크용 개체를 생성한 후 이 개체를 선택합니다. 그러면 클라이언트에 이 풀의 주소가 할당됩니다. IPv6 풀은 비워 둡니다. 주소 풀은 외부 인터페이스의 IP 주소와 동일한 서브넷에 있을 수 없습니다.

개체는 다음과 같이 표시됩니다.

풀 사양은 다음과 같이 표시됩니다.

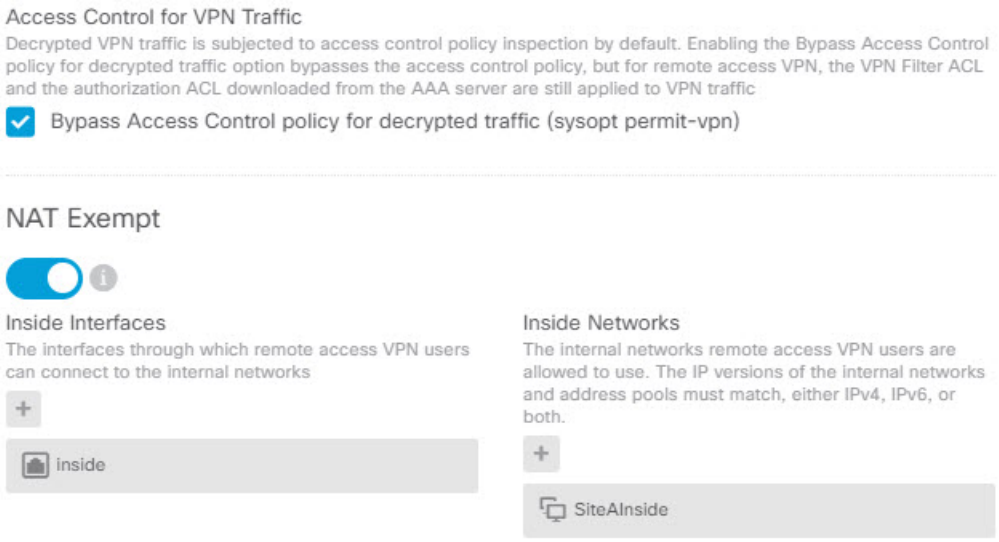
e) **Next(**다음**)**를 클릭한 다음, 적절한 그룹 정책을 선택합니다.

선택한 정책에 대한 요약 정보를 확인합니다. DNS 서버가 컨피그레이션되어 있는지 확인합니다. 그렇지 않은 경우, 지금 바로 정책을 수정하고 DNS를 컨피그레이션합니다.

f) **Next(**다음**)**를 클릭하고, 전역 설정에서 **Bypass Access Control policy for decrypted traffic(**암호 해독된 트래픽에 대해 액세스 제어 정책 우회**) (sysopt permit-vpn)** 옵션을 선택하고 **NAT Exempt(NAT** 제외**)** 옵션을 컨피그레이션합니다.

NAT Exempt(NAT 제외**)**에 대해서는 다음 옵션을 컨피그레이션해야 합니다. 다른 연결 프로파일을 정의한 경우, 컨피그레이션이 모든 연결 프로파일에 적용되므로 기존 설정에 추가해야 한다는 점에 유의하십시오.

- **Inside Interfaces(**내부 인터페이스**)** — 내부 인터페이스를 선택합니다. 이러한 인터페이스는 원격 사용자가 액세스할 내부 네트워크용 인터페이스입니다. NAT 규칙은 이러한 인터페이스에 대해 생성됩니다.
- **Inside Networks(**내부 네트워크**)** — SiteAInside 네트워크 개체를 선택합니다. 이러한 개체는 원격 사용자가 액세스할 내부 네트워크를 나타내는 네트워크 개체입니다.



g) 지원하는 플랫폼에 대한 Secure Client 패키지를 업로드합니다.

h) **Next(**다음**)**를 클릭하고 설정을 확인합니다.

먼저 요약이 정확한지 확인합니다.

그런 다음 지침을 클릭하여 Secure Client 소프트웨어를 처음으로 설치하고 VPN 연결을 완료할 수 있는지를 테스트하기 위해 엔드 유저가 수행해야 하는 작업을 파악합니다. 복사를 클릭하여 이러한 지침을 클립보드에 복사한 다음 텍스트 파일이나 이메일에 붙여넣습니다.

i) **Finish(**종료**)**를 클릭합니다.

단계 **7** 웹 페이지의 오른쪽 상단에 있는 **Deploy Changes(**변경 사항 구축**)** 아이콘을 클릭합니다.

단계 **8** **Deploy Now(**지금 구축**)** 버튼을 클릭하고 구축이 정상적으로 완료될 때까지 기다립니다.

이제 사이트 A 디바이스는 RA VPN 연결을 수락할 준비가 되었습니다. 외부 사용자에게 Secure Client 클라이언트를 설치하고 VPN 연결을 완료하도록 합니다.

디바이스 CLI에 로그인한 다음 **show vpn-sessiondb anyconnect** 명령을 사용해 세션 정보를 확인하면 연결을 확인할 수 있습니다.

그룹별로 RA VPN 액세스를 제어하는 방법

그룹 정책에 따라 내부 리소스에 대한 차등 액세스를 제공하도록 원격 액세스 VPN 연결 프로파일을 컨피그레이션할 수 있습니다. 예를 들어 직원에게는 무제한 액세스를 제공하되 계약업체에는 단일 내부 네트워크 외에는 액세스를 제공하지 않는 경우, 그룹 정책을 사용해 서로 다른 ACL을 정의하여 액세스를 적절히 제한할 수 있습니다.

다음 예에서는 192.168.2.0/24 내부 서브넷에만 액세스해야 하는 계약업체에 대해 RA VPN 연결을 설정하는 방법을 보여줍니다. 정규 직원의 경우, VPN에 대해 정의된 트래픽 필터가 없는 기본 그룹 정책을 사용할 수 있습니다. 이러한 사용자에게 제한을 적용하려면 기본 그룹 정책을 수정하고, 아래에 설명된 대로 구성된 ACL을 적용할 수 있습니다.

시작하기 전에

이 절차에서는 계약업체에 사용할 ID 소스를 이미 생성했다고 가정합니다. 이 소스는 정규 직원에게 사용하는 것과 다를 수 있습니다. 이 ID 소스는 액세스 제한과 딱히 관련이 없으므로 이 예시에서는 생략했습니다.

또한 이 예시에서는 "inside2" 인터페이스가 192.168.2.0/24 서브넷을 호스팅하도록 컨피그레이션되어 있고 IP 주소는 192.168.2.1(서브넷에 있는 다른 주소도 허용됨)이라고 가정합니다.

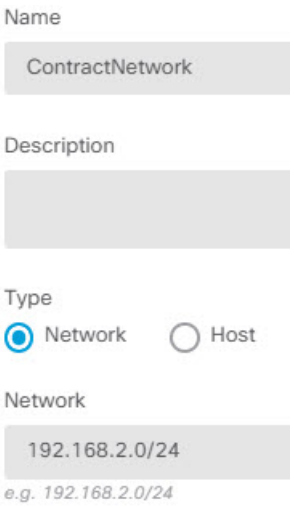
프로시저

단계 **1** RA VPN 트래픽을 제한하기 위한 확장 ACL(액세스 제어 목록)을 컨피그레이션합니다.

타겟인 192.168.2.0/24를 정의하는 네트워크 개체를 먼저 컨피그레이션한 다음, 액세스 목록을 정의하는 스마트 CLI 개체를 생성해야 합니다. ACL은 종단에 암시적 거부가 있기 때문에 서브넷에 대한 액세스만 허용해야 하고, 서브넷 외부의 모든 IP 주소로 전송되는 트래픽은 거부됩니다. 이 예시는 IPv4에만 적용되므로 특정 서브넷에 대한 IPv6 액세스를 제한하기 위해 개체를 구성할 수도 있습니다. 네트워크 개체를 생성하고 동일한 ACL에 IPv6 기반 ACE를 추가하기만 하면 됩니다.

a) **Objects(**개체**)** > **Networks(**네트워크**)**를 선택하고 필요한 개체를 생성합니다.

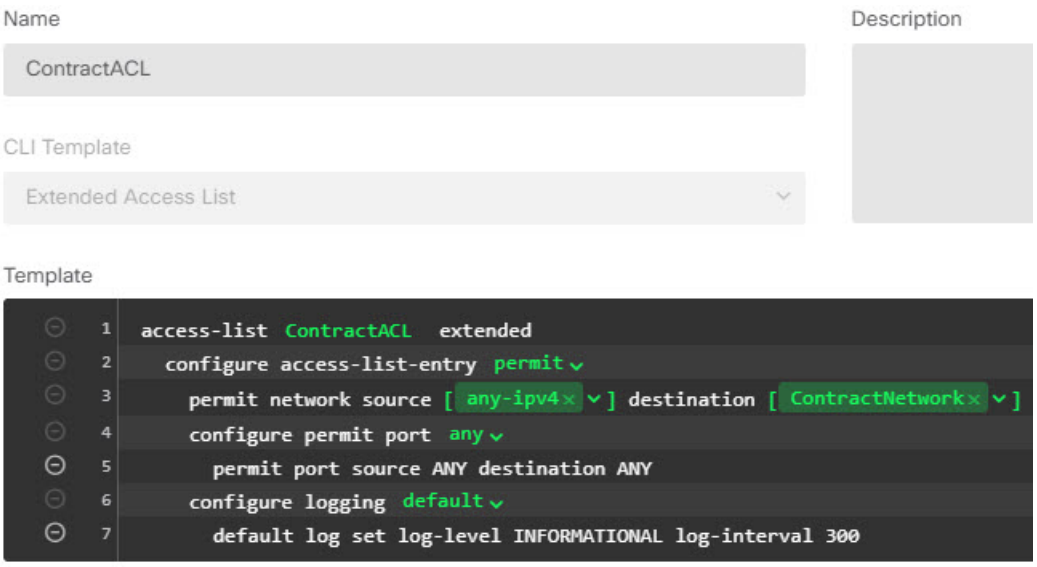
예를 들어 개체에 ContractNetwork라는 이름을 지정합니다. 개체는 다음과 비슷해야 합니다.



b) **Device(**디바이스**)** > **Advanced Configuration(**고급 컨피그레이션**)** > **Smart CLI(**스마트 **CLI)** > **Objects(**개체**)**를 선택합니다.
c) **+**를 클릭하여 새 개체를 생성합니다.
d) ACL의 이름을 입력합니다. 예: **ContractACL**.
e) **CLI Template(CLI** 템플릿**)**에서 **Extended Access List(**확장 액세스 목록**)**를 선택합니다.
f) **Template(**템플릿**)** 본문에서 다음과 같이 컨피그레이션합니다.

- configure access-list-entry action = permit
- source-network = any-ipv4
- destination-network = ContractNetwork object
- configure permit port = any
- configure logging = default

ACE는 다음과 같이 표시되어야 합니다.



g) **OK(**확인**)**를 클릭합니다.

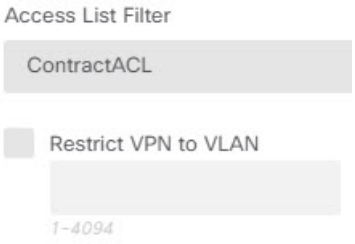
이 ACL은 다음번에 변경 사항을 구축할 때 컨피그레이션됩니다. 다른 정책에서 개체를 사용하여 구축을 강제 적용할 필요가 없습니다.

단계 **2** ACL을 사용하는 그룹 정책을 생성합니다.

최소한 그룹 정책에 대한 DNS 서버도 컨피그레이션해야 합니다. 필요에 따라 다른 옵션을 컨피그레이션할 수 있습니다. 다음 절차에서는 이 활용 사례와 관련이 있는 한 가지 설정에 중점을 둡니다.

a) **Device(**장치**)** > **RA VPN** > **Group Policies(**그룹 정책**)**를 선택합니다.
b) 새 그룹 정책을 생성하려면 **+**를 클릭합니다.
c) **General(**일반**)** 페이지에서 **ContractGroup**과 같이 정책의 이름을 입력합니다.
d) 목차에서 **Traffic Filters(**트래픽 필터**)**를 클릭합니다.
e) **Access List Filter(**액세스 목록 필터**)**에서 ContractACL 개체를 선택합니다.

이 예에서는 VLAN 옵션을 비워 둡니다. 필터링 목적으로 VLAN을 설정하고 VLAN에 대해 하위 인터페이스를 컨피그레이션하는 방법도 있습니다.



f) 그룹 정책을 저장하려면 **OK(**확인**)**를 클릭합니다.

단계 **3** 계약업체를 위한 연결 프로파일을 컨피그레이션합니다.

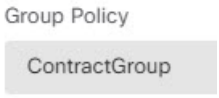
a) RA VPN 페이지의 목차에서 **Connection Profiles(**연결 프로파일**)**를 클릭합니다.
b) **+** 버튼을 클릭하여 새 연결 프로파일을 생성합니다.

c) 마법사의 1단계를 완료하고 **Next(**다음**)**를 클릭합니다.

예를 들어 Contractors와 같이 프로파일에 대한 이름을 입력합니다.

평상시와 같이 나머지 옵션을 컨피그레이션합니다. 여기에는 계약업체를 위한 적절한 인증 소스를 선택하고 주소 풀을 정의하는 작업이 포함됩니다.

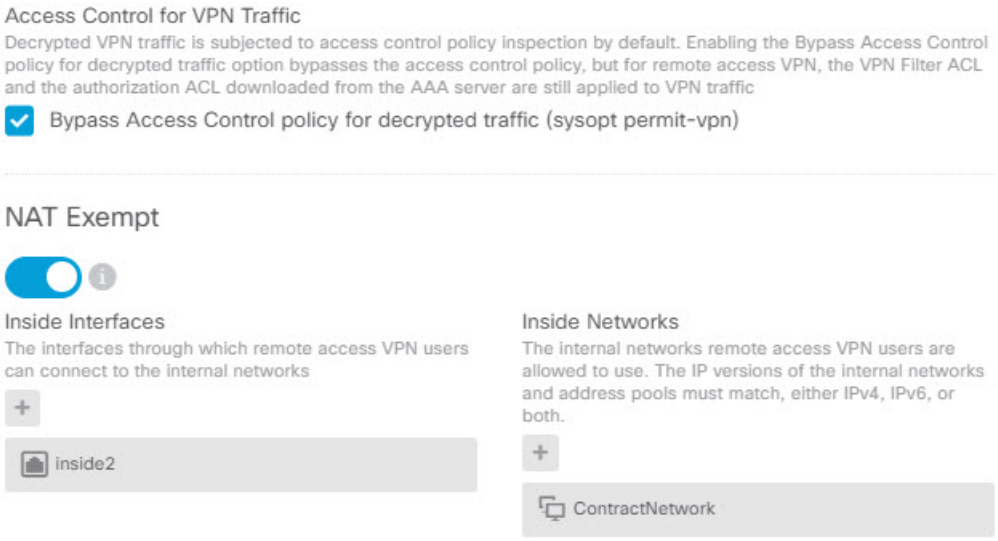
d) 계약업체에 대해 컨피그레이션한 그룹 정책을 선택하고 **Next(**다음**)**를 클릭합니다.



e) 전역 설정에서 **Bypass Access Control policy for decrypted traffic(**암호 해독된 트래픽에 대해 액세스 제어 정책 우회**) (sysopt permit-vpn)** 옵션을 선택하고 **NAT Exempt(NAT** 제외**)** 옵션을 컨피그레이션합니다.

NAT Exempt(NAT 제외**)**에 대해서는 다음 옵션을 컨피그레이션해야 합니다. 다른 연결 프로파일을 정의한 경우, 컨피그레이션이 모든 연결 프로파일에 적용되므로 기존 설정에 추가해야 한다는 점에 유의하십시오.

- **Inside Interfaces(**내부 인터페이스**) - inside2** 인터페이스를 선택합니다. 이러한 인터페이스는 원격 사용자가 액세스할 내부 네트워크용 인터페이스입니다. NAT 규칙은 이러한 인터페이스에 대해 생성됩니다.
- **Inside Networks(**내부 네트워크**)** - ContractNetwork 네트워크 개체를 선택합니다. 이러한 개체는 원격 사용자가 액세스할 내부 네트워크를 나타내는 네트워크 개체입니다.



f) 지원하는 플랫폼에 대한 Secure Client 패키지를 업로드합니다.

g) **Next(**다음**)**를 클릭하고 설정을 확인합니다.

먼저 요약이 정확한지 확인합니다.

그런 다음 지침을 클릭하여 Secure Client 소프트웨어를 처음으로 설치하고 VPN 연결을 완료할 수 있는지를 테스트하기 위해 엔드 유저가 수행해야 하는 작업을 파악합니다. 복사를 클릭하여 이러한 지침을 클립보드에 복사한 다음 텍스트 파일이나 이메일에 붙여넣습니다.

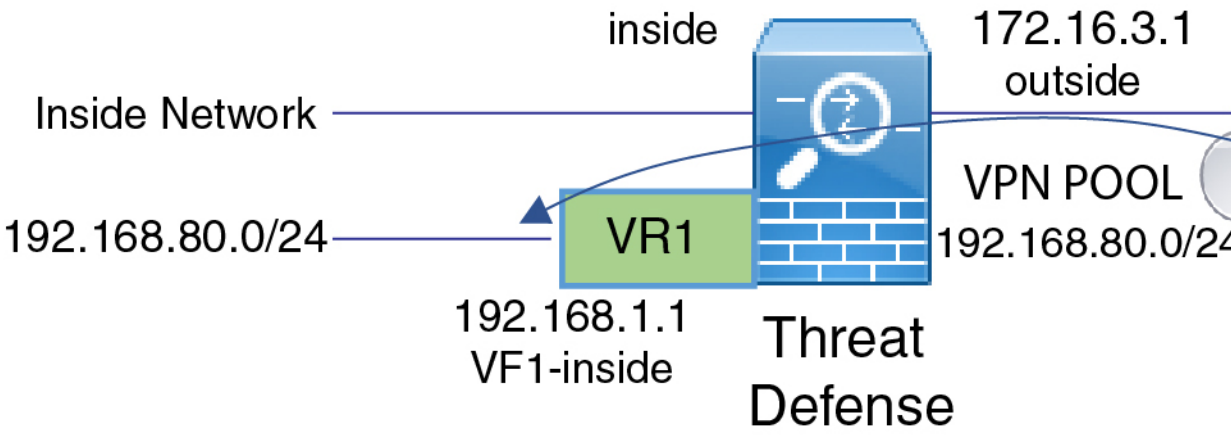
h) **Finish(**종료**)**를 클릭합니다.

RA VPN 액세스를 다른 가상 라우터의 내부 네트워크에 허용하는 방법

디바이스에서 여러 가상 라우터를 구성하는 경우에는 전역 가상 라우터에서 RA VPN을 구성해야 합니다. 사용자 지정 가상 라우터에 할당된 인터페이스에는 RA VPN을 구성할 수 없습니다.

가상 라우터의 라우팅 테이블은 별도이므로 RA VPN 사용자가 다른 가상 라우터에 속한 네트워크에 액세스해야 하는 경우 정적 경로를 생성해야 합니다.

다음과 같은 사례를 가정해보십시오. 이 경우 RA VPN 사용자는 172.16.3.1의 외부 인터페이스에 연결되며 192.168.80.0/24 풀 내에 IP 주소가 지정됩니다. 이 사용자는 이제 전역 가상 라우터에 연결된 내부 네트워크에 액세스할 수 있습니다. 그러나 사용자는 가상 라우터 VR1의 일부인 192.168.1.0/24 네트워크에 연결할 수 없습니다. VR1 네트워크와 RA VPN 사용자 간의 트래픽 흐름을 허용하려면 정적 경로를 두 가지 방식으로 모두 구성해야 합니다.



시작하기 전에

이 예에서는 RA VPN을 이미 구성하고 가상 라우터를 정의했으며 적절한 가상 라우터에 인터페이스를 구성 및 할당한 것으로 가정합니다.

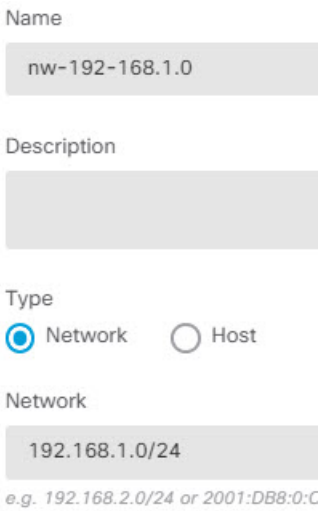
프로시저

단계 **1** 전역 가상 라우터에서 VR1으로의 경로 유출을 구성합니다.

이 경로를 사용하면 VPN 풀에서 Secure Client 할당 IP 주소로 VR1 가상 라우터에서 192.168.1.0/24 네트워크에 액세스할 수 있습니다.

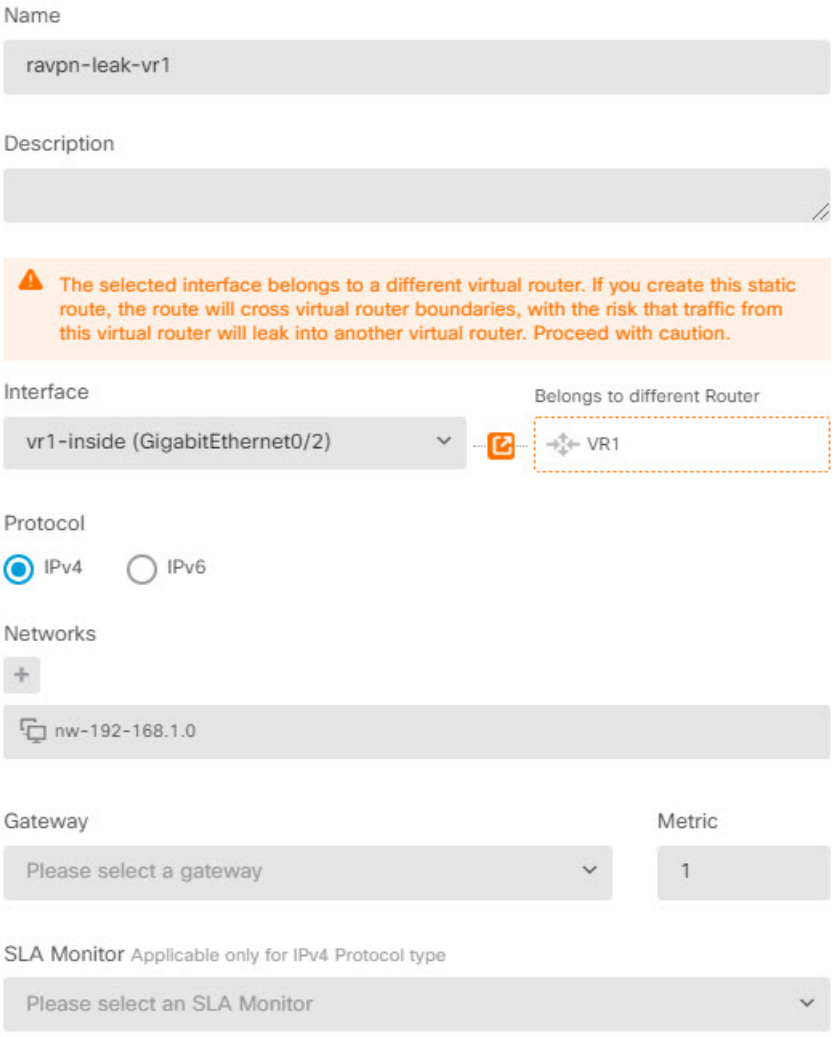
a) **Device(**디바이스**)** > **Routing(**라우팅**)** > **View Configuration(**구성 보기**)**을 선택합니다.
b) 전역 가상 라우터의 View Icon(아이콘 보기)을 클릭합니다.
c) 전역 라우터에 대한 **Static Routing(**정적 라우팅**)** 탭에서 **+**를 클릭하고 다음과 같이 경로를 구성합니다.

- **Name(**이름**)**-모든 이름(예: **ravpn-leak-vr1**)이 수행됩니다.
- **Interface(**인터페이스**)** — **vr1-inside**를 선택합니다.
- **Protocol(**프로토콜**)** — **IPv4**를 선택합니다.
- **Network(**네트워크**)**—192.168.1.0/24 네트워크를 정의하는 개체를 선택합니다. 필요한 경우 **Create New Network(**새 네트워크 생성**)**를 클릭하면 바로 개체를 생성할 수 있습니다.



- **Gateway(**게이트웨이**)** — 이 항목은 비워둡니다. 다른 가상 라우터로 경로를 유출할 경우에는 게이트웨이 주소를 선택하지 않습니다.

대화 상자가 다음과 비슷하게 표시됩니다.



d) **OK(**확인**)**를 클릭합니다.

단계 **2** VR1에서 전역 가상 라우터로의 경로 유출을 구성합니다.

이 경로를 사용하면 192.168.1.0/24 네트워크의 엔드포인트가 VPN 풀에서 Secure Client 할당 IP 주소에 대한 연결을 시작할 수 있습니다.

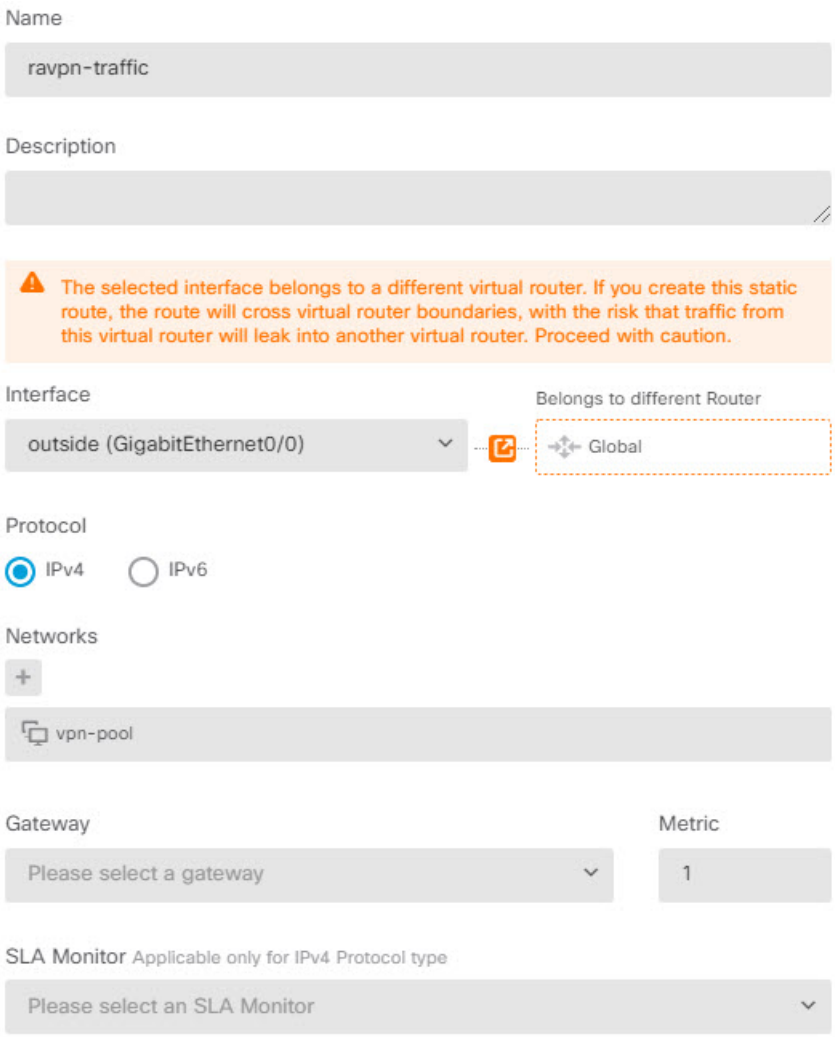
a) 가상 라우터 드롭다운 목록에서 **VR1**을 선택하여 VR1 구성으로 전환합니다.

b) VR1 가상 라우터에 대한 **Static Routing(**정적 라우팅**)** 탭에서 +를 클릭하고 다음과 같이 경로를 구성합니다.

- **Name(**이름**)** - 모든 이름(예: **ravpn-traffic**)이 수행됩니다.
- **Interface(**인터페이스**)** — **outside**를 선택합니다.
- **Protocol(**프로토콜**)** — **IPv4**를 선택합니다.
- **Natwork(**네트워크**)** - VPN 풀에 대해 생성한 개체(예: **vpn-pool**)를 선택합니다.

- **Gateway(**게이트웨이**)** — 이 항목은 비워둡니다. 다른 가상 라우터로 경로를 유출할 경우에는 게이트웨이 주소를 선택하지 않습니다.

대화 상자가 다음과 비슷하게 표시됩니다.



c) **OK(**확인**)**를 클릭합니다.

다음에 수행할 작업

RA VPN 주소 풀과 사용자 지정 가상 라우터의 IP 주소 간에 중복 항목이 있는 경우 IP 주소에서 고정 NAT 규칙을 또한 사용하여 적절한 라우팅을 활성화해야 합니다. 그러나 중복되지 않도록 간단히 RA VPN 주소 풀을 변경하는 것이 훨씬 쉽습니다.

Secure Client 아이콘 및 로고를 맞춤화하는 방법

Windows 및 Linux 클라이언트 시스템에서 Secure Client 앱의 아이콘과 로고를 맞춤화할 수 있습니다. 아이콘의 이름은 미리 정의되어 있으며 업로드하는 이미지의 파일 유형 및 크기에 대한 특정 제한이 있습니다.

GUI를 맞춤화하기 위해 고유한 실행 파일을 구축할 경우 어떠한 파일명도 사용할 수 있지만, 이 예에서는 맞춤화된 프레임워크를 구축하지 않고 단순히 아이콘과 로고를 교체한다고 가정합니다.

대체할 수 있는 여러 이미지가 있으며 파일 이름은 플랫폼에 따라 다릅니다. 맞춤화 옵션, 파일 이름, 유형 및 크기에 대한 자세한 내용은 *Cisco Secure Client* 관리자 가이드에서 Secure Client 및 설치 프로그램의 맞춤화 및 현지화에 대한 챕터를 참조하십시오. 예를 들어 4.8 클라이언트 챕터는 다음에서 사용할 수 있습니다.

https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect48/administration/guide/b_AnyConnect_Administrator_Guide_4-8/customize-localize-anyconnect.html

시작하기 전에

이 예의 목적을 위해 Windows 클라이언트의 다음 이미지를 교체합니다. 이미지가 최대 크기와 다른 경우 시스템에서는 자동으로 이를 최대 크기로 조정하고 필요한 경우 이미지를 늘립니다.

- app_logo.png

  이 애플리케이션 로고 이미지는 애플리케이션 아이콘이며 최대 크기는 128 x 128 픽셀입니다.

- company_logo.png

  이 기업 로고 이미지는 트레이 플라이아웃 및 Advanced(고급) 대화 상자의 왼쪽 위 모서리에 표시됩니다. 최대 크기는 97 x 58 픽셀입니다.

- company_logo_alt.png

  다른 기업 로고 이미지는 About(정보) 대화 상자의 오른쪽 아래 모서리에 표시됩니다. 최대 크기는 97 x 58 픽셀입니다.

이러한 파일을 업로드하려면 threat defense 디바이스가 액세스할 수있는 서버에 파일을 배치해야 합니다. TFTP, FTP, HTTP, HTTPS 또는 SCP 서버를 사용할 수 있습니다. 이러한 파일에서 이미지를 가져오는 URL에는 서버 설정에 필요한대로 경로 및 사용자 이름/비밀번호가 포함될 수 있습니다. 이 예에서는 TFTP를 사용합니다.

프로시저

단계 **1** 맞춤화된 아이콘 및 로고를 사용해야 하는 RA VPN 헤드엔드 역할을 하는 각 threat defense 디바이스에 이미지 파일을 업로드합니다.

a) SSH 클라이언트를 사용하여 디바이스 CLI에 로그인합니다.

b) CLI에서 **system support diagnostic-cli** 명령을 입력하여 진단 CLI 모드를 시작합니다.

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
```

```
Type help or '?' for a list of available commands.

ftdv1>
```

참고 메시지를 읽어보십시오! **Ctrl+a**를 누른 다음 **d**를 눌러 진단 CLI에서 나와 일반 threat defense CLI 모드로 돌아와야 합니다.

c) 명령 프롬프트를 참고합니다. 일반 CLI에서는 > 만 사용하는 반면, 진단 CLI의 사용자 EXEC 모드에서는 호스트 이름 + >를 사용합니다. 이 예에서는 ftdv1>입니다. #를 종료 문자로 사용하는 특별 권한 EXEC 모드를 시작해야 합니다(예 : ftdv1 #). 프롬프트에 이미 #이 있는 경우 이 단계를 건너 뜁니다. 그렇지 않으면 enable 명령을 입력하고 비밀번호를 입력하지 않고 비밀번호 프롬프트에서 Enter를 누릅니다.

```
ftdv1> enable
Password:
ftdv1#
```

d) **copy** 명령을 사용하여 각 파일을 호스팅 서버에서 threat defense 디바이스의 disk0으로 복사합니다. disk0:/anyconnect-images/와 같은 하위 디렉토리에 이들을 배치할 수 있습니다. **mkdir** 명령을 사용하여 새 폴더를 생성할 수 있습니다.

예를 들어 TFTP 서버의 IP 주소가 10.7.0.80이고 새 디렉토리를 생성하려는 경우 명령은 다음과 유사합니다. 첫 번째 예 이후에는 **copy** 명령에 대한 응답이 생략됩니다.

```
ftdv1# mkdir disk0:anyconnect-images

Create directory filename [anyconnect-images]? yes

Created dir disk0:/anyconnect-images

ftdv1# copy /noconfirm tftp://10.7.0.80/app_logo.png
disk0:/anyconnect-images/app_logo.png

Accessing tftp://10.7.0.80/app_logo.png...!!!!!!
Writing file disk0:/anyconnect-images/app_logo.png...
!!!!!!
12288 bytes copied in 1.000 secs (12288 bytes/sec)

ftdv1# copy /noconfirm tftp://10.7.0.80/company_logo.png
disk0:/anyconnect-images/company_logo.png
ftdv1# copy /noconfirm tftp://10.7.0.80/company_logo_alt.png
disk0:/anyconnect-images/company_logo_alt.png
```

단계 **2** 클라이언트 시스템에 설치할 때 진단 CLI의 **import webvpn** 명령을 사용하여 Secure Client에 이러한 이미지를 다운로드하도록 지시합니다.

import webvpn AnyConnect-customization type resource platform win name *filename* **disk0:**/*directoryname/filename*

이 명령은 Windows용입니다. Linux의 경우 **win** 키워드를 클라이언트에 따라 **linux** 또는 **linux-64**으로 대체합니다.

예를 들어 이전 단계에서 업로드한 파일을 가져오고 진단 CLI에 아직 있다고 가정합니다.

```
ftdv1# import webvpn AnyConnect-customization type resource platform win
name app_logo.png disk0:/anyconnect-images/app_logo.png
```

```
ftdv1# import webvpn AnyConnect-customization type resource platform win
name company_logo.png disk0:/anyconnect-images/company_logo.png

ftdv1# import webvpn AnyConnect-customization type resource platform win
name company_logo_alt.png disk0:/anyconnect-images/company_logo_alt.png
```

단계 **3** 컨피그레이션을 확인합니다.

- 가져온 파일을 확인하려면 진단 CLI의 특별 권한 EXEC 모드에서 **show import webvpn AnyConnect-customization** 명령을 사용하십시오.
- 이미지가 클라이언트에 다운로드되었는지 확인하려면 사용자가 클라이언트를 실행할 때 이미지가 표시되어야 합니다. Windows 클라이언트에서 다음 폴더를 확인할 수도 있습니다. 여기서 %PROGRAMFILES%는 일반적으로 c:\Program Files로 확인됩니다.

  %PROGRAMFILES%\Cisco\Cisco AnyConnect Secure Mobility Client\res\

다음에 수행할 작업

기본 이미지로 돌아가려면 맞춤화한 각 이미지에 대해(진단 CLI 특별 권한 EXEC 모드에서) **revert webvpn** 명령을 사용합니다. 명령은 다음과 같습니다.

revert webvpn AnyConnect-customization type resource platform win name *filename*

import webvpn에서와 마찬가지로 해당 클라이언트 플랫폼을 맞춤화한 경우, **win**을 **linux** 또는 **linux-64**로 대체하고 가져온 각 이미지 파일 이름에 대해 명령을 개별적으로 실행합니다. 예를 들면 다음과 같습니다.

```
ftdv1# revert webvpn AnyConnect-customization type resource platform win
name app_logo.png

ftdv1# revert webvpn AnyConnect-customization type resource platform win
name company_logo.png

ftdv1# revert webvpn AnyConnect-customization type resource platform win
name company_logo_alt.png
```

VII 부

시스템 관리

26 장

시스템 설정

다음 주제에서는 시스템 설정 페이지에서 함께 그룹화되어 있는 여러 시스템 설정을 구성하는 방법을 설명합니다. 이러한 설정에는 전반적인 시스템 기능이 포함됩니다.

관리 액세스 구성

관리 액세스는 컨피그레이션 및 모니터링을 위해 threat defense 디바이스에 로그인하는 기능을 의미합니다. 다음과 같은 항목을 구성할 수 있습니다.

- 사용자 액세스 인증에 사용할 ID 소스를 식별할 AAA. 로컬 사용자 데이터베이스 또는 외부 AAA 서버를 사용할 수 있습니다. 관리자 권한 사용자를 관리하는 방법에 대한 자세한 내용은 Device Manager 및 Threat Defense 사용자 액세스 관리, 878 페이지의 내용을 참조하십시오.
- 관리 인터페이스 및 데이터 인터페이스에 대한 액세스 제어. 이러한 인터페이스에는 별도의 액세스 목록이 있습니다. HTTPS(device manager에 사용됨) 및 SSH(CLI에 사용됨)에 어떤 IP 주소를 허용할지 결정할 수 있습니다. 관리 액세스 목록 구성, 810 페이지를 참조하십시오.

- 사용자가 Fdevice manager에 연결하기 위해 승인해야 하는 Management Web Server 인증서. 현재 사용 중인 웹 브라우저에서 기존에 인증한 인증서를 업로드하면, 알 수 없는 인증서를 승인하라는 요청이 사용자에게 표시되지 않습니다. Threat Defense 웹 서버 인증서 구성, 813 페이지의 내용을 참조하십시오.

관리 액세스 목록 구성

기본적으로는 모든 IP 주소에서 관리 주소의 디바이스의 device manager 웹 또는 CLI 인터페이스에 연결할 수 있습니다. 시스템 액세스는 사용자/비밀번호를 통해서만 보호됩니다. 그러나 특정 IP 주소 또는 서브넷으로부터의 연결만 허용하도록 액세스 목록을 구성하여 보호 레벨을 추가로 제공할 수 있습니다.

데이터 인터페이스를 열어 device manager 또는 SSH의 CLI 연결을 허용할 수도 있습니다. 그러면 관리 주소를 사용하지 않고도 디바이스를 관리할 수 있습니다. 예를 들어 디바이스를 원격으로 구성하기 위해 외부 인터페이스에 대한 관리 액세스를 허용할 수 있습니다. 사용자 이름/비밀번호를 통해 원치 않는 연결로부터 디바이스를 보호할 수 있습니다. 기본적으로 데이터 인터페이스에 대한 HTTPS 관리 액세스는 내부 인터페이스에서는 활성화되지만 외부 인터페이스에서는 비활성화됩니다. device managerFirepower 1010에서 "내부" 브리지 그룹이 있는 의 경우 브리지 그룹 내에 있는 모든 데이터 인터페이스를 통해 브리지 그룹 IP 주소(기본값: 192.168.95.1)에 대한 Firepower Device Manager 연결을 설정할 수 있습니다. 디바이스에 진입하는 데 사용하는 인터페이스에서만 관리 연결을 열 수 있습니다.

⚠

주의 특정 주소에 대한 액세스를 제한하면 시스템이 잠겨 사용이 차단되기 쉽습니다. 현재 사용 중인 IP 주소에 대한 액세스 권한을 삭제하여 "모든" 주소에 대한 항목이 없으면 정책 배포 시 시스템에 액세스할 수 없게 됩니다. 따라서 액세스 목록을 구성하려는 경우 각별히 주의해야 합니다.

시작하기 전에

동일한 TCP 포트에 대한 동일한 인터페이스에서 device manager 액세스(HTTPS 액세스)와 원격 액세스 SSL VPN을 모두 구성할 수는 없습니다. 예를 들어, 외부 인터페이스에서 원격 액세스 SSL VPN을 구성하는 경우, 포트 443에서 HTTPS 연결에 대한 외부 인터페이스도 열 수 없습니다. 동일한 인터페이스에서 두 기능을 모두 구성하는 경우 충돌을 방지하기 위해 이러한 서비스 중 하나 이상에 대해 HTTPS 포트를 변경해야 합니다.

프로시저

단계 **1** 디바이스을(를) 클릭한 다음, **System Settings(**시스템 설정**)** > **Management Access(**관리 액세스**)** 링크를 클릭합니다.

System Settings(시스템 설정) 페이지가 이미 열려 있는 경우 목차에서 **Management Access(**관리 액세스**)**를 클릭하면 됩니다.

이 페이지에서 AAA를 구성하여 외부 AAA 서버에 정의된 사용자에 대해 관리 액세스를 허용할 수도 있습니다. 자세한 내용은 Device Manager 및 Threat Defense 사용자 액세스 관리, 878 페이지를 참조해 주십시오.

단계 **2** 관리 주소에 대한 규칙을 생성하려면 다음을 수행합니다.

a) **Management Interface(**관리 인터페이스**)** 탭을 선택합니다.

규칙 목록에 따라 지정된 포트 액세스가 허용되는 주소가 정의됩니다. 이 포트는 device manager의 경우 443(HTTPS 웹 인터페이스)이고 SSH CLI의 경우 22입니다.

규칙은 순서가 지정된 목록이 아닙니다. IP 주소가 요청된 포트에 대한 어떤 규칙에든 일치하는 경우 사용자의 디바이스 로그인 시도는 허용됩니다.

참고 규칙을 삭제하려면 해당 규칙의 휴지통 아이콘()을 클릭합니다. 프로토콜에 대한 모든 규칙을 삭제하는 경우, 아무도 그 프로토콜을 사용하여 해당 인터페이스에 있는 디바이스에 액세스할 수 없습니다.

b) +를 클릭하고 다음 옵션에 내용을 입력합니다.

- 프로토콜 - 규칙이 HTTPS(포트 443)용인지 아니면 SSH(포트 22)용인지를 선택합니다.
- **IP** 주소 - 시스템에 액세스할 수 있어야 하는 IPv4 또는 IPv6 네트워크나 호스트를 정의하는 네트워크 개체를 선택합니다. "임의" 주소를 지정하려면 **any-ipv4**(0.0.0.0/0) 및 **any-ipv6**(::/0)를 선택합니다.

c) **OK(**확인**)**를 클릭합니다.

단계 **3** 데이터 인터페이스에 대한 규칙을 생성하려면 다음을 수행합니다.

a) **Data Interfaces(**데이터 인터페이스**)** 탭을 선택합니다.

규칙 목록에 따라 인터페이스에서 지정된 포트 액세스가 허용되는 주소가 정의됩니다. 이 포트는 device manager의 경우 443(HTTPS 웹 인터페이스)이고 SSH CLI의 경우 22입니다.

규칙은 순서가 지정된 목록이 아닙니다. IP 주소가 요청된 포트에 대한 어떤 규칙에든 일치하는 경우 사용자의 디바이스 로그인 시도는 허용됩니다.

참고 규칙을 삭제하려면 해당 규칙의 휴지통 아이콘()을 클릭합니다. 프로토콜에 대한 모든 규칙을 삭제하는 경우, 아무도 그 프로토콜을 사용하여 해당 인터페이스에 있는 디바이스에 액세스할 수 없습니다.

b) +를 클릭하고 다음 옵션에 내용을 입력합니다.

- 인터페이스 - 관리 액세스를 허용할 인터페이스를 선택합니다.
- 프로토콜 - 규칙이 HTTPS(포트 443)용인지, SSH(포트 22)용인지 아니면 둘 다에 사용할 수 있는지를 선택합니다. 원격 액세스 VPN 연결 프로파일에 사용되는 외부 인터페이스에 대해서는 HTTPS 규칙을 구성할 수 없습니다.
- 허용된 네트워크 - 시스템에 액세스할 수 있어야 하는 IPv4 또는 IPv6 네트워크나 호스트를 정의하는 네트워크 개체를 선택합니다. "임의" 주소를 지정하려면 **any-ipv4**(0.0.0.0/0) 및 **any-ipv6**(::/0)를 선택합니다.

c) (선택 사항). HTTPS 데이터 포트 번호를 변경하려면 해당 번호를 클릭하고 새 포트를 입력합니다. 데이터 인터페이스에서 관리 액세스에 대한 HTTPS 포트 구성, 812 페이지의 내용을 참조하십시오.

d) **OK(**확인**)**를 클릭합니다.

데이터 인터페이스에서 관리 액세스에 대한 HTTPS 포트 구성

기본적으로 device manager 또는 threat defense API 관리를 위해 디바이스에 액세스하면 포트 TCP/443을 통과합니다. 데이터 인터페이스에 대한 관리 액세스 포트를 변경할 수 있습니다.

포트를 변경하는 경우 사용자는 시스템에 액세스하려면 URL에 맞춤형 포트를 포함해야 합니다. 예를 들어 데이터 인터페이스가 ftd.example.com이고 포트를 4443으로 변경하는 경우 사용자는 URL을 https://ftd.example.com:4443으로 수정해야 합니다.

모든 데이터 인터페이스는 동일한 포트를 사용합니다. 인터페이스마다 다른 포트를 구성할 수 없습니다.

참고 관리 인터페이스의 관리 액세스 포트는 변경할 수 없습니다. 관리 인터페이스는 항상 포트 443을 사용합니다.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 후 **System Settings(**시스템 설정**)** > **Management Access(**관리 액세스**)** 링크를 클릭합니다.

System Settings(시스템 설정) 페이지가 이미 열려 있는 경우 목차에서 **Management Access(**관리 액세스**)**를 클릭하면 됩니다.

단계 **2** **Data Interfaces(**데이터 인터페이스**)** 탭을 클릭합니다.

단계 **3** **HTTPS Data Port(HTTPS** 데이터 포트**)** 번호를 클릭합니다.

단계 **4** Data Interfaces Setting(데이터 인터페이스 설정) 대화 상자에서 **HTTPS Data Port(HTTPS** 데이터 포트**)**를 사용하려는 포트로 변경합니다.

다음 번호는 지정할 수 없습니다.

- 22. SSH 연결에 사용됩니다.
- 원격 액세스 VPN에 사용되는 포트(관리 액세스도 허용하는 인터페이스에 대해 구성한 경우). 원격 액세스 VPN은 기본적으로 포트 443을 사용하지만 맞춤형 포트를 구성할 수 있습니다.
- ID 정책에서 활성 인증에 사용되는 포트입니다(기본값은 885).

단계 **5** **OK(**확인**)**를 클릭합니다.

Threat Defense 웹 서버 인증서 구성

웹 인터페이스에 로그인할 경우, 시스템은 디지털 인증서를 사용하여 HTTPS를 사용하는 통신을 보호합니다. 기본 인증서는 브라우저에서 신뢰하지 않으므로, Untrusted Authority(신뢰할 수 없는 증명) 경고가 표시되며 해당 인증서를 신뢰할 것인지 묻는 메시지가 표시됩니다. 사용자는 신뢰할 수 있는 루트 인증서 저장소에 인증서를 저장할 수 있지만, 그 대신에 브라우저에서 신뢰하도록 이미 컨피그레이션되었다는 새 인증서를 업로드할 수 있습니다.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 후 **System Settings(**시스템 설정**)** > **Management Access(**관리 액세스**)** 링크를 클릭합니다.

System Settings(시스템 설정) 페이지가 이미 열려 있는 경우 목차에서 **Management Access(**관리 액세스**)**를 클릭하면 됩니다.

단계 **2** **Management Web Server(**관리 웹 서버**)** 탭을 클릭합니다.

단계 **3** **Web Server Certificate(**웹 서버 인증서**)**에서 device manager에 대한 HTTPS 연결을 보호하는 데 사용할 내부 인증서를 선택합니다.

인증서를 업로드하거나 생성하지 않은 경우, 목록 하단의 **Create New Internal Certificate(**새 내부 인증서 생성**)** 링크를 클릭하여 지금 인증서를 생성합니다.

기본값은 사전 정의된 DefaultWebserverCertificate 개체입니다.

단계 **4** 인증서가 자체 서명되지 않은 경우 완전 신뢰 체인의 모든 중간 및 루트 인증서를 **Trusted Chain(**신뢰할 수 있는 체인**)** 목록에 추가합니다.

체인에서 인증서를 10개까지 추가할 수 있습니다. +를 클릭하여 각 중간 인증서를 추가하고 마지막으로 루트 인증서를 추가합니다. **Save(**저장**)**를 클릭한 다음, 웹 서버가 재시작되는 것을 경고하는 대화 상자에서 **Proceed(**계속 진행**)**를 클릭하는 경우, 인증서가 누락되면 누락된 체인에서 다음 인증서의 공통 이름이 포함된 오류 메시지가 표시됩니다. 체인에 없는 인증서를 추가하는 경우에도 오류가 표시됩니다. 이러한 메시지를 신중하게 검사하여 추가하거나 제거해야 하는 인증서를 식별합니다.

+를 클릭한 후에 **Create New Trusted CA Certificate(**신뢰할 수 있는 새 **CA** 인증서 생성**)**을 클릭하여 여기에서 인증서를 업로드할 수 있습니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

변경 사항이 즉시 적용되고, 시스템에서는 웹 서버를 다시 시작합니다. 컨피그레이션을 구축할 필요가 없습니다.

재시작이 완료될 때까지 몇 분간 기다렸다가 브라우저를 새로고침합니다.

시스템 기록 설정 컨피그레이션

threat defense 디바이스에 대한 시스템 로그를 활성화할 수 있습니다. 기록 정보는 네트워크 또는 디바이스 구성 관련 문제를 식별하고 격리하는 데 도움이 됩니다. 액세스 제어, 침입 방지, 파일 및 악성코드 기록을 포함한 진단 기록 및 연결 관련 기록에 대해 syslog를 활성화할 수 있습니다.

진단 기록에서는 디바이스 및 시스템 상태, 네트워크 컨피그레이션 관련 이벤트에 대한 syslog 메시지를 제공합니다. 이러한 이벤트는 연결과 관련이 없습니다. 개별 액세스 제어 규칙 내에서 연결 로깅을 구성합니다.

진단 기록에서는 데이터 플레인에서 실행되는 기능, 즉 **show running-config** 명령으로 볼 수 있는 CLI 컨피그레이션에 정의된 기능에 대해 메시지를 생성합니다. 여기에는 라우팅, VPN, 데이터 인터페이스, DHCP 서버, NAT 등과 같은 기능이 포함됩니다.

이 메시지에 대한 정보는 https://www.cisco.com/c/en/us/td/docs/security/firepower/Syslogs/b_fptd_syslog_guide.html의 *Cisco Threat Defense* 시스템 로그 메시지를 참조하십시오.

다음 주제에서는 다양한 출력 위치에 대한 진단 및 파일/악성코드 메시지에 관한 기록을 컨피그레이션하는 방법에 대해 설명합니다.

심각도 레벨

다음 표는 syslog 메시지 심각도 수준을 나열합니다.

표 ***15: Syslog*** 메시지 심각도 레벨

레벨 번호	심각도 레벨	설명
0	**emergencies**(비상)	시스템을 사용할 수 없습니다.
1	**Alert**(긴급 경고)	즉각적인 행동이 필요합니다.
2	**critical**(심각)	심각한 상태입니다.
3	**error**(오류)	오류 상태입니다.
4	**warning**(경고)	경고 상태입니다.
5	**notification**(알림)	일반적이지만 중요한 상태입니다.
6	**informational**(정보)	정보 메시지만 해당됩니다.
7	**debugging**(디버깅)	디버깅 메시지만 해당됩니다. 문제를 디버깅할 때 이 레벨에서 일시적으로만 기록합니다. 이 로그 레벨은 시스템 성능에 영향을 미칠 수 있는 메시지를 너무 많이 생성할 수 있습니다.

참고 ASA 및 Threat Defense은 심각도 레벨 0(응급)으로 시스템 로그 메시지를 생성하지 않습니다.

원격 **Syslog** 서버에 대한 기록 컨피그레이션

외부 syslog 서버로 syslog 메시지를 전송하도록 시스템을 컨피그레이션할 수 있습니다. 이것은 시스템 기록을 위한 최상의 옵션입니다. 외부 서버를 사용하여 메시지를 보관할 수 있는 공간을 더 많이 제공하고 서버의 기능을 사용하여 메시지를 보고, 분석 및 보관할 수 있습니다.

또한 파일 정책을 액세스 제어 규칙의 트래픽에 적용하는 경우, 파일 액세스나 악성코드 또는 둘 다를 제어하려면 파일 이벤트 메시지를 외부 syslog 서버로 전송하도록 시스템을 컨피그레이션할 수 있습니다. 시스템 로그 서버를 컨피그레이션하지 않는 경우, 이벤트는 device manager 이벤트 뷰어에서만 제공됩니다.

다음 절차에서는 진단 (데이터) 기록 및 파일/악성코드 기록을 위해 syslog를 활성화하는 방법에 대해 설명합니다. 다음 항목에 대해 외부 기록을 컨피그레이션할 수도 있습니다.

- 연결 이벤트: 개별 액세스 제어 규칙, SSL 암호 해독 규칙 또는 보안 인텔리전스 정책 설정에서 syslog 서버 선택
- 침입 이벤트: 침입 정책 설정에서 syslog 서버 선택

시작하기 전에

파일/악성코드 이벤트에 대한 시스템 로그 설정은 IPS 및 악성코드 방어 라이선스 가 필요한 파일 또는 악성코드 정책을 적용하는 경우에만 해당됩니다.

또한 정책을 적용하는 액세스 제어 규칙에서 **File Events(**파일 이벤트**)** > **Log Files(**로그 파일**)** 옵션을 선택해야 합니다. 그러지 않으면 syslog 또는 이벤트 뷰어 이벤트에 대해 이벤트가 전혀 생성되지 않습니다.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음, **System Settings(**시스템 설정**)** > **Logging Settings(**기록 설정**)** 링크를 클릭합니다.

시스템 설정 페이지가 이미 열려 있는 경우 목차에서 로깅 설정을 클릭하면 됩니다.

단계 **2** **Remote Server(**원격 서버**)**에서 **Data Logging(**데이터 기록**)** 슬라이더를 **On(**켜짐**)**으로 밀어 외부 syslog 서버에 대한 진단 데이터 플레인 생성 메시지의 기록을 활성화합니다. 이어서 다음 옵션을 컨피그레이션합니다.

- **Syslog Server(Syslog** 서버**)** - **+**(을)를 클릭하고 하나 이상의 syslog 서버 개체를 선택한 후 **OK(**확인**)**를 클릭합니다. 개체가 없는 경우, **Add Syslog Server(Syslog** 서버 추가**)** 링크를 클릭하고 지금 바로 개체를 생성합니다. 자세한 내용은 syslog 서버 구성, 157 페이지를 참고하십시오.

- **Severity Level for Filtering FXOS Chassis Syslogs(FXOS** 섀시 **syslog** 필터링을 위한 심각도 레벨**)** - FXOS를 사용하는 특정 디바이스 모델의 경우, 기본 FXOS 플랫폼에서 생성한 syslog 메시지의 심각도 레벨. 이 옵션은 디바이스와 관련이 있는 경우에만 표시됩니다. 심각도 레벨을 선택합니다. 이 레벨 이상의 메시지가 syslog 서버로 전송됩니다.
- **Message Filtering(**메시지 필터링**)** - threat defense 운영 체제에 대해 생성된 메시지를 제어하려면 다음 옵션 중 하나를 선택합니다.
  - **Severity Level for Filtering All Events(**모든 이벤트 필터링을 위한 심각도 레벨**)** - 심각도 레벨을 선택합니다. 이 레벨 이상의 메시지가 syslog 서버로 전송됩니다.
  - **Custom Logging Filter(**맞춤형 기록 필터**)** - 관심 있는 메시지만 가져올 수 있도록 추가 메시지 필터링을 수행하려는 경우, 생성하려는 메시지를 정의하는 이벤트 목록 필터를 선택합니다. 필터가 아직 없는 경우, **Create New Event List Filter(**새 이벤트 목록 필터 생성**)**를 클릭하여 지금 바로 생성합니다. 자세한 내용은 이벤트 목록 필터 구성, 817 페이지를 참고하십시오.

단계 **3** **File/Malware(**파일/악성코드**)** 슬라이더를 **On(**켜짐**)**으로 밀어 파일 및 악성코드 이벤트용 외부 syslog 서버에 기록을 활성화합니다. 그런 다음, 파일/악성코드 기록에 대해 다음 옵션을 컨피그레이션합니다.

- **Syslog Server(Syslog** 서버**)** - syslog 서버 개체를 선택합니다. 개체가 없는 경우, **Add Syslog Server(Syslog** 서버 추가**)** 링크를 클릭하고 지금 바로 개체를 생성합니다.
- **Log at Severity Level(**심각도 레벨의 로그**)** - 파일/악성코드 이벤트에 할당해야 하는 심각도 레벨을 선택합니다. 모든 파일/악성코드 이벤트는 동일한 심각도에서 생성되므로 필터링이 수행되지 않습니다. 따라서 선택하는 레벨에 관계없이 모든 이벤트가 표시됩니다. 이것은 메시지의 심각도 필드에 표시되는 레벨입니다(즉 FTD-x-<message_ID>의 x). 파일 이벤트는 메시지 ID 430004, 악성코드 이벤트는 430005입니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

내부 버퍼에 대한 기록 컨피그레이션

Syslog 메시지를 내부 기록 버퍼에 저장하도록 시스템을 컨피그레이션할 수 있습니다. 버퍼의 내용을 보려면 CLI 또는 CLI 콘솔에서 **show logging** 명령을 사용하십시오.

새 메시지는 버퍼의 끝에 추가됩니다. 버퍼가 가득 차면 시스템에서는 버퍼를 지운 다음, 메시지를 계속 추가합니다. 로그 버퍼가 가득 차면 시스템에서는 가장 오래된 메시지를 삭제하여 새 메시지를 위한 버퍼 공간을 확보합니다.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음, **System Settings(**시스템 설정**)** > **Logging Settings(**기록 설정**)** 링크를 클릭합니다.

시스템 설정 페이지가 이미 열려 있는 경우 목차에서 로깅 설정을 클릭하면 됩니다.

단계 **2** **Internal Buffer(**내부 버퍼**)** 슬라이더를 **On(**켜짐**)**으로 밀어 버퍼를 기록 대상으로 활성화합니다.

단계 **3** 내부 버퍼 기록에 대한 옵션을 다음과 같이 컨피그레이션합니다.

- **Severity Level for Filtering All Events(**모든 이벤트 필터링을 위한 심각도 레벨**)** - 심각도 레벨을 선택합니다. 이 레벨 이상의 메시지가 내부 버퍼로 전송됩니다.
- **Custom Logging Filter(**맞춤형 기록 필터**)** - (선택 사항) 관심 있는 메시지만 가져올 수 있도록 추가 메시지 필터링을 수행하려는 경우, 생성하려는 메시지를 정의하는 이벤트 목록 필터를 선택합니다. 필터가 아직 없는 경우, **Create New Event List Filter(**새 이벤트 목록 필터 생성**)**를 클릭하여 지금 바로 생성합니다. 자세한 내용은 이벤트 목록 필터 구성, 817 페이지를 참고하십시오.
- **Buffer Size(**버퍼 크기**)** - syslog 메시지가 저장되는 내부 버퍼의 크기. 버퍼는 가득 차면 덮어쓰기 됩니다. 기본값은 4096바이트입니다. 범위는 4096~52428800입니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

콘솔에 기록 컨피그레이션

콘솔에 메시지를 전송하도록 시스템을 컨피그레이션할 수 있습니다. 콘솔 포트에서 CLI에 로그인하면 이러한 메시지가 표시됩니다. **show console-output** 명령을 사용하면 다른 인터페이스에 대한 SSH 세션에서도 이러한 로그를 확인할 수 있습니다(관리 주소 포함). 또한 진단 CLI에서 실시간으로 이러한 메시지를 확인할 수 있습니다. 기본 CLI에서 **system support diagnostic-cli**(을)를 입력하십시오.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음, **System Settings(**시스템 설정**)** > **Logging Settings(**기록 설정**)** 링크를 클릭합니다.

시스템 설정 페이지가 이미 열려 있는 경우 목차에서 로깅 설정을 클릭하면 됩니다.

단계 **2** **Console Filter(**콘솔 필터**)** 슬라이더를 **On(**켜짐**)**으로 밀어 콘솔을 기록 대상으로 활성화합니다.

단계 **3** 심각도 레벨을 선택합니다. 이 레벨 이상의 메시지가 콘솔로 전송됩니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

이벤트 목록 필터 구성

이벤트 목록 필터는 어떤 메시지를 대상으로 전송할지 제어하기 위해 기록 대상에 적용할 수 있는 맞춤형 필터입니다. 일반적으로 심각도만을 기준으로 대상에 대한 메시지를 필터링하지만, 이벤트 클래스, 심각도 및 메시지 ID(식별자)의 조합을 기준으로 전송할 메시지를 세부 조정할 수 있습니다.

심각도 레벨에 따라서만 메시지를 제한하는 것으로는 목적을 달성하지 못하는 경우에만 필터를 사용합니다.

다음 절차에서는 **Objects(**개체**)** 페이지에서 필터를 생성하는 방법을 설명합니다. 필터를 사용할 수 있는 기록 대상을 컨피그레이션하는 중에 필터를 생성할 수도 있습니다.

프로시저

단계 **1** 목차에서 **Objects(**개체**)**를 선택한 다음, **Event List Filters(**이벤트 목록 필터**)**를 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 개체를 생성하려면 **+** 버튼을 클릭합니다.
- 개체를 수정하려면 개체의 수정 아이콘()을 클릭하십시오.

참조되지 않는 개체를 삭제하려면 해당 개체의 휴지통 아이콘()을 클릭합니다.

단계 **3** 필터 속성을 다음과 같이 구성합니다.

- **Name(**이름**)** - 필터 개체의 이름입니다.
- **Description(**설명**)** - 개체의 설명(선택 사항)입니다.
- **Severity and Log Class(**심각도 및 로그 클래스**)** - 메시지 클래스를 기준으로 필터링하려는 경우, **+**를 클릭하고 클래스 필터에 대한 심각도 레벨을 선택한 다음, **OK(**확인**)**를 클릭합니다. 그런 다음, 심각도 레벨 내에서 드롭다운 화살표를 클릭하고 해당 심각도 레벨에서 필터링할 클래스를 하나 이상 선택한 후 **OK(**확인**)**를 클릭합니다.

  시스템에서는 지정된 클래스의 메시지가 해당 심각도 레벨 이상인 경우에만 이 메시지에 대해 syslog 메시지를 전송합니다. 각 심각도 레벨에 대해 최대 한 개의 행을 추가할 수 있습니다.

  특정 심각도 레벨에서 모든 클래스를 필터링하려는 경우, 심각도 목록을 빈 상태로 두고 대신에 기록 대상을 활성화할 때 기록 대상에 대한 전역 심각도 레벨을 선택합니다.
- **Syslog Range/Message ID(Syslog** 범위/메시지 **ID)** - syslog 메시지 ID를 기준으로 필터링하려는 경우, 단일 메시지 ID를 입력하거나 메시지를 생성하려는 ID 번호의 범위를 입력합니다. 범위의 시작 및 종료 번호를 하이픈으로 구분합니다(예: 100000-200000). ID는 6자리 숫자입니다. 특정 메시지 ID 및 관련 메시지에 관해서는 https://www.cisco.com/c/en/us/td/docs/security/firepower/Syslogs/b_fptd_syslog_guide.html의 *Cisco Threat Defense* 시스템 로그 메시지를 참조하십시오.

단계 **4** **Save(**저장**)**를 클릭합니다.

이제 이 개체를 허용하는 기록 대상에 대한 맞춤형 필터링 옵션에서 이 개체를 선택할 수 있습니다. **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Logging Settings(**기록 설정**)**로 이동합니다.

DHCP 구성

DHCP 서버는 IP 주소와 같은 네트워크 구성 매개변수를 DHCP 클라이언트에 제공합니다. 연결된 네트워크의 DHCP 클라이언트에 구성 매개변수를 제공하도록 인터페이스에서 DHCP 서버를 구성하거나 인터페이스의 DHCP 릴레이를 활성화하여 네트워크의 다른 디바이스에서 작동 중인 외부 DHCP 서버에 요청을 전달할 수 있습니다.

이러한 기능은 상호 배타적이므로, 둘 중 하나만 구성할 수 있고 두 가지 모두 구성할 수는 없습니다.

DHCP 서버 설정

DHCP 서버는 IP 주소와 같은 네트워크 컨피그레이션 파라미터를 DHCP 클라이언트에 제공합니다. 연결된 네트워크의 DHCP 클라이언트에 컨피그레이션 파라미터를 제공하기 위해 인터페이스에서 DHCP 서버를 구성할 수 있습니다.

IPv4 DHCP 클라이언트는 서버와 연결하는 데 멀티캐스트 주소가 아닌 브로드캐스트를 사용합니다. DHCP 클라이언트는 UDP 포트 68에서 메시지를 수신합니다. DHCP 서버는 UDP 포트 67에서 메시지를 수신합니다. DHCP 서버는 BOOTP 요청을 지원하지 않습니다.

참고 이미 DHCP 서버가 작동 중인 네트워크에서는 DHCP 서버를 구성하지 마십시오. 이렇게 하면 두 서버가 충돌하여 예측할 수 없는 결과가 발생합니다.

시작하기 전에

DHCP 클라이언트는 서버가 활성화된 인터페이스와 같은 네트워크에 있어야 합니다. 즉, 서버와 클라이언트 사이에 스위치는 있을 수 있지만 개입하는 라우터가 있어서는 안 됩니다.

여러 네트워크를 지원해야 하고 각 인터페이스에서 DHCP 서버를 구성하지 않으려는 경우, 대신 DHCP 요청을 한 네트워크에서 다른 네트워크에 있는 DHCP 서버로 전달하도록 구성할 수 있습니다. 이 경우 DHCP 서버는 네트워크의 다른 디바이스에 있어야 합니다. 한 디바이스에서 DHCP 서버를 구성하고 동일한 디바이스의 다른 인터페이스에서 DHCP 릴레이를 구성할 수는 없습니다. DHCP 릴레이를 사용하는 경우 DHCP 서버가 관리할 각 네트워크 주소 공간에 대해 주소 풀을 사용하여 DHCP 서버를 설정해야 합니다.

DHCP 릴레이를 구성하려면 DHCP 릴레이 구성, 821 페이지 항목을 참조하십시오.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음 **System Settings(**시스템 설정**)** > **DHCP Server / Relay(DHCP** 서버/릴레이**)** 링크를 클릭합니다.

시스템 설정 페이지가 이미 열려 있는 경우 목차에서 **DHCP** > **DHCP Server(DHCP** 서버**)**를 클릭하면 됩니다.

이 페이지에는 2개의 탭이 있습니다. 먼저 **Configuration(**컨피그레이션**)** 탭에는 글로벌 파라미터가 표시됩니다.

DHCP Servers(DHCP 서버**)** 탭에는 DHCP 서버를 구성한 인터페이스, 서버 활성화 여부 및 서버의 주소 풀이 표시됩니다.

단계 **2** **Configuration(**컨피그레이션**)** 탭에서 자동 컨피그레이션 및 글로벌 설정을 구성합니다.

DHCP 자동 컨피그레이션은 DHCP 서버가 지정된 인터페이스에서 실행 중인 어떤 DHCP 클라이언트로부터 얻은 DNS 서버, 도메인 이름, WINS 서버 정보를 DHCP 클라이언트에 제공할 수 있게 합니다. 일반적으로는 외부 인터페이스의 DHCP를 사용하여 주소를 가져오는 경우 자동 컨피그레이션을 사용하지만, DHCP를 통해 주소를 가져오는 모든 인터페이스를 선택할 수 있습니다. 자동 컨피그레이션을 사용할 수 없는 경우에는 필요한 옵션을 수동으로 정의할 수 있습니다.

a) 자동 컨피그레이션을 사용하려면 **Enable Auto Configuration(**자동 컨피그레이션 활성화**)** > **On(**켜기**)**을 클릭(슬라이더가 오른쪽에 있어야 함)한 다음 인터페이스에서에서 DHCP를 통해 주소를 가져오는 인터페이스를 선택합니다.

가상 라우터를 구성하는 경우 전역 가상 라우터의 인터페이스에서만 DHCP 서버 자동 컨피그레이션을 사용할 수 있습니다. 자동 컨피그레이션은 사용자 정의 가상 라우터에 할당된 인터페이스에 대해 지원되지 않습니다.

b) 자동 컨피그레이션을 활성화하지 않거나 자동으로 구성된 설정을 재정의하려는 경우 다음의 글로벌 옵션을 구성합니다. 이러한 설정은 DHCP 서버를 호스팅하는 모든 인터페이스의 DHCP 클라이언트에 전송됩니다.

- **1**차 **WINS IP** 주소, **2**차 **WINS IP** 주소 - 클라이언트가 NetBIOS 이름 확인에 사용해야 하는 WINS(Windows 인터넷 이름 서비스) 서버의 주소입니다.
- **Primary DNS IP Address(**기본 **DNS IP** 주소**)**, **Secondary DNS IP Address(**보조 **DNS IP** 주소**)** - 클라이언트가 도메인 이름 확인에 사용해야 하는 DNS(Domain Name System) 서버의 주소입니다. OpenDNS 공개 DNS 서버를 구성하려면 **Use OpenDNS(OpenDNS** 사용**)**를 클릭합니다. 버튼을 클릭하면 필드에 적절한 IP 주소가 로드됩니다.

c) **Save(**저장**)**를 클릭합니다.

단계 **3** **DHCP Servers(DHCP** 서버**)** 탭을 클릭하고 서버를 구성합니다.

a) 다음 중 하나를 수행합니다.

- 이미 나열되어 있지 않은 인터페이스에 대해 DHCP 서버를 구성하려면 **+**를 클릭합니다.
- 기존 DHCP 서버를 수정하려면 해당 서버의 수정 아이콘( )을 클릭합니다.

서버를 삭제하려면 해당 서버의 휴지통 아이콘( )을 클릭합니다.

b) 서버 속성을 구성합니다.

- **DHCP** 서버 활성화 - 서버를 활성화할지를 선택합니다. 서버를 구성하되 사용할 준비가 될 때까지 비활성화해 둘 수 있습니다.
- 인터페이스 - 클라이언트에 DHCP 주소를 제공할 인터페이스를 선택합니다. 이 인터페이스에는 고정 IP 주소가 있어야 합니다. 인터페이스에서 DHCP 서버를 실행하려는 경우 DHCP

를 사용하여 인터페이스 주소를 가져올 수는 없습니다. 브리지 그룹의 경우 멤버 인터페이스가 아닌 BVI(브리지 가상 인터페이스)에서 DHCP 서버를 구성합니다. 그러면 서버가 모든 멤버 인터페이스에서 작동합니다.

진단 인터페이스에서는 DHCP 서버를 설정할 수 없습니다. 대신 **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Management Interface(**관리 인터페이스**)** 페이지를 통해 관리 인터페이스에서 DHCP 서버를 설정합니다.

- 주소 풀 - 서버가 주소를 요청하는 클라이언트에 제공할 수 있는 IP 주소의 범위(최저 범위에서 최고 범위 순서)입니다. 풀의 시작 주소와 끝 주소를 하이픈으로 구분하여 지정합니다. 예를 들면 10.100.10.12-10.100.10.250과 같이 지정합니다.

  이 IP 주소 범위는 선택된 인터페이스와 동일한 서브넷에 있어야 하며, 인터페이스 자체의 IP 주소, 브로드캐스트 주소 또는 서브넷 네트워크 주소는 포함할 수 없습니다.

  주소 풀의 크기는 threat defense 디바이스에 있는 풀당 최대 256개 주소로 제한됩니다. 주소 풀의 범위가 253개 주소보다 클 경우, threat defense 인터페이스의 넷마스크는 클래스 C 주소(예: 255.255.255.0)가 될 수 없으며 그보다 더 커야 합니다(예: 255.255.254.0).

c) **OK(**확인**)**를 클릭합니다.

DHCP 릴레이 구성

인터페이스에서 수신한 DHCP 요청을 하나 이상의 DHCP 서버에 전달하도록 DHCP 릴레이 에이전트를 구성할 수 있습니다.

DHCP 클라이언트는 최초 DHCPDISCOVER 메시지를 보내는 데 UDP 브로드캐스트를 사용합니다. 연결된 네트워크에 대한 정보가 없기 때문입니다. 클라이언트가 연결된 세그먼트에 서버가 없을 경우, threat defense 디바이스는 (브로드캐스트 트래픽을 전달하지 않으므로) 대개는 UDP 브로드캐스트를 전달하지 않습니다. DHCP 릴레이 에이전트를 사용하면 DHCP 요청을 다른 인터페이스를 통해 DHCP 서버로 전송하는 브로드캐스트를 수신하는 threat defense 디바이스의 인터페이스를 구성할 수 있습니다.

따라서 DHCP 서버를 호스팅하지 않는 서브넷의 클라이언트는 다른 서브넷에 있는 DHCP 서버에서 IP 주소 리스를 계속 가져올 수 있습니다.

시작하기 전에

- 추가할 각 서브넷에 대해 주소 풀을 사용하여 DHCP 서버를 구성합니다. 예를 들어, 192.168.1.1/24 주소의 인터페이스에서 DHCP 릴레이 클라이언트를 활성화한 경우, 192.168.1.0/24 네트워크의 클라이언트를 지원하려면 DHCP 서버가 192.168.1.0/24 서브넷의 IP 주소를 제공할 수 있어야 합니다(예: 192.168.1.2-192.168.1.254).
- 각 DHCP 서버에 대한 호스트 네트워크 개체를 생성하고, 서버의 IP 주소를 지정합니다.
- **DHCP** > **DHCP Servers(DHCP** 서버**)** 페이지에서 모든 서버를 제거 또는 비활성화해야 합니다. 인터페이스에서 DHCP 릴레이가 활성화된 상태에서는 서로 다른 인터페이스인 경우에도 DHCP 서버를 호스팅할 수 없습니다.

- 인터페이스 제한 - 인터페이스에는 서버 또는 에이전트에 사용할 이름이 있어야 합니다. 그 외에도,
  - 인터페이스는 라우팅 ECMP 트래픽 영역의 멤버일 수 없습니다.
  - 인터페이스는 DHCP를 사용하여 주소를 가져올 수 없습니다.
  - 물리적 인터페이스, 하위 인터페이스, VLAN 인터페이스 및 EtherChannel(멤버 제외)에서 DHCP 서버와 DHCP 릴레이를 모두 구성할 수 있습니다.
  - VTI(Virtual Tunnel Interface)에서 DHCP 릴레이 서버를 구성할 수도 있습니다.
  - 어떤 서비스도 관리 인터페이스 또는 브리지 그룹과 멤버를 지원하지 않습니다.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음 **System Settings(**시스템 설정**)** > **DHCP Server / Relay(DHCP** 서버/릴레이**)** 링크를 클릭하고, 목차에서 **DHCP** > **DHCP Relay(DHCP** 릴레이**)**를 클릭합니다.

System Settings(시스템 설정) 페이지가 이미 열려 있는 경우 목차에서 **DHCP** > **DHCP Relay(DHCP** 릴레이**)**를 클릭하면 됩니다.

단계 **2** (선택 사항). 필요에 따라 **IPv4 Relay Timeout(IPv4** 릴레이 시간 초과**)** 및 **IPv6 Relay Timeout(IPv6** 릴레이 시간 초과**)** 설정을 조정합니다.

이러한 시간 제한은 지정된 IP 버전에 대한 DHCP 릴레이 주소 협상에 허용되는 시간(초)을 설정합니다. 기본값은 60초(1분)이지만 1~3600초에서 시간 제한을 설정할 수 있습니다. 서브넷과 DHCP 서버 간에 상당한 지연이 있는 경우 더 긴 시간 초과가 적절할 수 있습니다.

단계 **3** **DHCP** 릴레이 서버를 구성합니다.

DHCP 릴레이 서버는 DHCP 릴레이 요청을 처리해야 하는 네트워크의 DHCP 서버입니다. 이러한 DHCP 서버는 네트워크에서 구성 중인 디바이스와 다른 디바이스에 있습니다.

a) +를 클릭하고 DHCP 서버의 IP 주소가 있는 호스트 네트워크 개체를 선택한 다음 **OK(**확인**)**를 클릭합니다.

개체가 아직 없는 경우 **Create New Network(**새 네트워크 생성**)**를 클릭하여 바로 생성합니다. 추가한 DHCP 서버를 더 이상 사용하지 않으려면 서버 항목의 오른쪽에 있는 **X**를 클릭하여 삭제합니다.

b) 추가한 DHCP 서버 항목을 클릭하고, DHCP 서버에 연결할 수 있는 인터페이스를 선택합니다.

단계 **4** DHCP 릴레이 에이전트를 구성합니다.

DHCP 릴레이 에이전트는 인터페이스에서 실행됩니다. 네트워크 세그먼트의 클라이언트에서 DHCP 서버로 DHCP 요청을 전달한 다음 응답을 클라이언트로 반환합니다.

a) +를 클릭하고 DHCP 릴레이 에이전트를 실행해야 하는 인터페이스를 선택한 다음 **OK(**확인**)**를 클릭합니다.

더 이상 인터페이스에서 DHCP 릴레이 에이전트를 실행하지 않으려면 서버 항목의 오른쪽에 있는 **X**를 클릭하여 삭제합니다. 선택적으로 테이블에서 인터페이스를 제거하지 않고 모든 DHCP 릴레이 서비스를 비활성화할 수 있습니다.

b) 추가한 인터페이스 항목을 클릭하고 에이전트에서 제공할 DHCP 서비스를 선택한 다음 **OK(**확인**)**를 클릭합니다.

- **Enable IPv4(IPv4** 활성화**)** - DHCP 서버에 대한 IPv4 주소 요청을 전달합니다. 이 옵션을 선택하지 않으면 모든 IPv4 주소 요청이 무시되고 클라이언트가 IPv4 주소를 가져올 수 없습니다.
- **Set Route(**경로 설정**)**(IPv4만 해당) - DHCP 서버에서 전송된 패킷의 첫 번째 기본 라우터 주소를 DHCP 릴레이 에이전트를 실행 중인 threat defense 디바이스 인터페이스의 주소로 변경합니다. 이 작업을 수행하면 클라이언트는 DHCP 서버가 다른 라우터를 지정하더라도 threat defense 디바이스를 가리키는 기본 경로를 설정할 수 있습니다. 패킷에 기본 라우터 옵션이 없는 경우 DHCP 릴레이 에이전트는 인터페이스 주소를 포함하는 옵션을 추가합니다.
- **Enable IPv6(IPv6** 활성화**)** - DHCP 서버에 대한 IPv6 주소 요청을 전달합니다. 이 옵션을 선택하지 않으면 모든 IPv6 주소 요청이 무시되고 클라이언트가 IPv6 주소를 가져올 수 없습니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

동적 **DNS** 구성

DDNS(Dynamic Domain Name System) 변경 사항을 동적 DNS 서비스에 전송하기 위해 웹 업데이트 방법을 사용하도록 시스템을 설정할 수 있습니다. 이러한 서비스는 FQDN(Fully Qualified Domain Name)과 연결된 새 IP 주소를 사용하도록 DNS 서버를 업데이트합니다. 따라서 사용자가 호스트 이름을 사용하여 시스템에 액세스하려고 하면 DNS가 올바른 IP 주소로 이름을 확인합니다.

DDNS를 사용하면 시스템의 인터페이스에 대해 정의된 FQDN이 항상 올바른 IP 주소로 확인되도록 할 수 있습니다. 이는 DHCP를 사용하여 주소를 가져오도록 인터페이스를 설정하는 경우 특히 중요합니다. 하지만 DNS 서버가 올바른 주소를 갖도록 하고 정적 주소를 변경하는 경우 쉽게 업데이트될 수 있도록 할 수 있다는 점에서 정적 IP 주소에 사용하는 것이 좋습니다.

선택한 DDNS 서비스 제공자 그룹을 사용하도록 DDNS를 설정하거나, 맞춤형 옵션을 사용하여 웹 업데이트를 지원하는 다른 DDNS 제공자로 업데이트를 전달할 수 있습니다. 인터페이스에 대해 지정하는 FQDN은 이러한 서비스 제공자에 등록되어야 합니다.

참고 device manager을 사용하여 웹 업데이트 DDNS만 설정할 수 있습니다. IETF RFC 2136에 정의된 방법에 대해 DDNS를 설정할 수 없습니다.

시작하기 전에

시스템에 제공자의 인증서를 검증할 신뢰할 수 있는 CA 인증서가 있어야 합니다. 그러지 않으면 DDNS 연결에 실패합니다. 서비스 제공자 사이트에서 인증서를 다운로드할 수 있습니다. 적절한 인

증서가 업로드 및 구축되었는지 확인하십시오. 또한 **SSL** 서버를 포함하도록 업로드된 인증서의 검증 사용을 설정해야 합니다. 신뢰할 수 있는 CA 인증서 업로드, 169 페이지의 내용을 참조하십시오.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음 **System Settings(**시스템 설정**)** > **DDNS Service(DDNS** 서비스**)** 링크를 클릭합니다.

시스템 설정 페이지가 이미 열려 있는 경우 목차에서 **DDNS Service(DDNS** 서비스**)**를 클릭하면 됩니다.

이 페이지에는 서비스 제공자, 인터페이스, 인터페이스의 FQDN(Fully Qualified Domain Name)을 비롯한 DDNS 업데이트 방법 목록과 FQDN의 IP 주소 변경을 위해 DNS 서버가 업데이트되는 빈도가 표시됩니다. 항목의 **Show Status(**상태 표시**)** 링크를 클릭하여 항목이 올바르게 작동하는지 확인할 수 있습니다.

단계 **2** 다음 중 하나를 수행합니다.

- 새로운 동적 DNS 업데이트 방법을 생성하려면 **+** 또는 **Create DDNS Service(DDNS** 서비스 생성**)** 버튼을 클릭합니다.
- 기존 동적 DNS 업데이트 방법을 편집하려면 해당 방법의 편집 아이콘( )을 클릭합니다.

방법을 삭제하려면 해당 방법의 휴지통 아이콘( )을 클릭합니다.

단계 **3** 동적 DNS 서비스 속성 설정:

- **Name(**이름**)** - 서비스의 이름입니다.
- **Web Type Update(**웹 유형 업데이트**)** - DDNS 서비스 제공자가 지원하는 주소를 기반으로 하여 업데이트할 주소 유형을 선택합니다. 기본값은 IPv4와 IPv6, **All Addresses(**모든 주소**)** 업데이트입니다. **IPv4 Address(IPv4** 주소**)**, **IPv4 and One IPv6 Address(IPv4**와 **1**개의 **IPv6** 주소**)**, **One IPv6 Address(1**개의 **IPv6** 주소**)**, **All IPv6 Addresses(**모든 **IPv6** 주소**)** 업데이트 옵션을 선택할 수 있습니다.

  IPv6 주소의 경우 다음에 유의하십시오.

  - 전역 주소만 업데이트됩니다. 링크 로컬 주소는 업데이트되지 않습니다.
  - device manager에서는 인터페이스당 단일 IPv6 주소를 설정할 수 있으므로 실제로는 1개의 IPv6 주소만 업데이트됩니다.

- **Service Provider(**서비스 제공자**)** - 동적 DNS 업데이트를 수신 및 처리하는 서비스 제공자를 선택합니다. 다음 서비스 제공자를 사용할 수 있습니다.
  - **No-IP** - No-IP DDNS 서비스 제공자(https://www.noip.com/).
  - **Dynamic DNS** - Oracle Dynamic DNS 서비스 제공자(https://account.dyn.com/).
  - **Google** - Google Domains 서비스 제공자(https://domains.google.com).

- **Custom URL(맞춤형 URL)** - 다른 모든 DDNS 서비스 제공자. 사용자 이름 및 암호를 포함하여 선택한 제공자가 요구하는 URL을 **Web URL(웹 URL)** 필드에 입력해야 합니다. DDNS 서비스는 https://help.dyn.com/remote-access-api/에서 설명하는 표준을 준수해야 합니다.

- **Username(사용자 이름)**, **Password(암호)**(맞춤형이 아닌 URL 방법) - 동적 DNS 업데이트를 전송할 때 서비스 제공자의 플랫폼에서 정의한 사용자 이름 및 암호를 사용합니다.

  참고:

  - 사용자 이름에는 공백이나 @ 및 : 기호가 포함될 수 없습니다. 구분 기호 역할을 하기 때문입니다.
  - 암호에는 공백이나 @ 문자가 포함될 수 없습니다. 구분 기호 역할을 하기 때문입니다. 첫 번째 : 기호 뒤와 @ 앞에 사용되는 모든 : 기호는 암호의 일부로 간주됩니다.

- **Web URL(웹 URL)**(맞춤형 URL 방법) - 서비스 제공자로 맞춤형 URL을 선택한 경우 동적 DNS 서비스에 대한 URL을 입력해야 합니다. URL은 511자로 제한되는 다음 형식이어야 합니다.

  http(s)://username:password@provider-domain/xyz?hostname=<h>&myip=<a>

  https://username:password@domain-provider/xyz?hostname=%3Ch%3E&myip=%3Ca%3E

- **Interfaces and Fully-Qualified Domain Name(인터페이스 및 FQDN)** - 이 서비스 제공자에 업데이트하고자 하는 DNS 레코드의 인터페이스를 선택한 다음 각 인터페이스에 대한 FQDN(Fully Qualified Domain Name)을 입력합니다. interface.example.com을 예로 들 수 있습니다. 인터페이스는 다음과 같이 제한됩니다.

  - 이름이 지정된 물리적 인터페이스와 하위 인터페이스만 선택할 수 있습니다.
  - 관리, BVI/EtherChannel 또는 해당 구성원, VLAN, VTI(Virtual Tunnel Interface) 유형의 인터페이스는 선택할 수 없습니다.
  - 지정된 인터페이스는 하나의 DDNS 업데이트 방법으로만 선택할 수 있습니다. 동일한 DDNS 업데이트 개체에서 서비스 제공자를 사용해야 하는 모든 인터페이스를 선택할 수 있습니다.

- **Update Interval(업데이트 간격)** - 동적 DNS 업데이트를 보내는 빈도입니다. 기본값은 **On Change(변경 시)**로, 인터페이스의 IP 주소가 변경될 때마다 업데이트를 보냅니다. 또는 **Hourly(매시간)**, **Daily(매일)** 또는 **Monthly(매월)**를 선택할 수 있습니다. 매일 또는 매월의 경우 업데이트를 보낼 시간을 설정하고, 매월의 경우 업데이트를 보낼 날짜를 설정합니다.

단계 **4** **OK(확인)**를 클릭합니다.

DNS 구성

DNS(Domain Name System) 서버는 호스트 이름을 IP 주소로 확인하는 데 사용됩니다. 초기 시스템 설정 중에 DNS 서버를 구성하면 이러한 서버가 데이터 및 관리 인터페이스에 적용됩니다. 설정 후에

이러한 서버를 변경할 수 있으며 데이터 및 관리 인터페이스에 별도의 서버 집합을 사용할 수 있습니다.

최소한 관리 인터페이스용 DNS를 구성해야 합니다. FQDN 기반 액세스 제어 규칙을 사용하려는 경우 또는 **ping** 등의 CLI 명령에서 호스트네임을 사용하려는 경우에는 데이터 인터페이스용 DNS도 컨피그레이션해야 합니다.

DNS 구성은 2단계 프로세스입니다. 즉, DNS 그룹을 구성한 다음 이러한 인터페이스용 DNS를 구성합니다.

다음 주제에서는 이 프로세스에 대해 자세히 설명합니다.

DNS 그룹 구성

DNS 그룹은 DNS 서버 및 일부 관련 특성의 목록을 정의합니다. 관리 및 데이터 인터페이스에서 DNS를 각기 별도로 구성할 수 있습니다. www.example.com과 같은 FQDN(Fully Qualified Domain Name)을 IP 주소로 확인하려면 DNS 서버가 필요합니다.

디바이스 설정 마법사를 완료하고 나면 다음의 시스템 정의 DNS 그룹 중 하나 또는 두 그룹이 모두 생성됩니다.

- CiscoUmbrellaDNSServerGroup - 이 그룹에는 Cisco Umbrella에서 사용할 수 있는 DNS 서버의 IP 주소가 포함되어 있습니다. 초기 설정 중에 이러한 서버를 선택한 경우 시스템 정의 그룹은 이 그룹뿐입니다. 이 그룹의 이름 또는 서버 목록을 변경할 수는 없지만 기타 속성을 수정할 수는 있습니다.
- CustomDNSServerGroup - 디바이스 설정 중에 Umbrella 서버를 선택하지 않는 경우 시스템에서 서버 목록이 포함된 이 그룹을 생성합니다. 이 그룹의 모든 속성을 수정할 수 있습니다.

프로시저

단계 **1** 목차에서 **Objects(**개체**)**와 **DNS Groups(DNS** 그룹**)**를 차례로 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 그룹을 생성하려면 **Add Group(**그룹 추가**)**( ) 버튼을 클릭합니다.
- 그룹을 수정하려면 해당 그룹의 수정 아이콘( )을 클릭합니다.

참조되지 않는 개체를 삭제하려면 해당 개체의 휴지통 아이콘( )을 클릭합니다.

단계 **3** 다음 속성을 구성합니다.

- **Name(**이름**)** - DNS 서버 그룹의 이름입니다. DefaultDNS는 예약된 이름이므로 사용할 수 없습니다.
- **DNS IP Addresses(DNS IP** 주소**)** — DNS 서버의 IP 주소를 입력합니다. 두 개 이상의 서버를 구성하려면 **Add Another DNS IP Address(**다른 **DNS IP** 주소 추가**)**를 클릭합니다. 서버 주소를 제거하려는 경우 해당 주소의 삭제 아이콘( )을 클릭합니다.

목록은 우선순위에 따라 나열됩니다. 목록의 첫 번째 서버가 항상 사용되며, 그다음 서버는 위에 있는 서버에서 응답이 수신되지 않는 경우에만 사용됩니다. 서버는 6개까지 구성할 수 있습니다. 그러나 6개의 서버는 데이터 인터페이스에서만 지원됩니다. 관리 인터페이스에서는 처음 3개 서버만 사용됩니다.

- **Domail Search Name(**도메인 검색 이름**)** - example.com과 같은 네트워크의 도메인 이름을 입력합니다. 이 도메인은 정규화되지 않은 호스트 이름(예: serverA.example.com이 아닌 serverA)에 추가됩니다. 그룹을 데이터 인터페이스에 사용하려면 이름이 63자 미만이어야 합니다.
- **Retries(**재시도 횟수**)** — 시스템이 응답을 받지 못한 경우 DNS 서버 목록을 재시도할 횟수(0~10회)입니다. 기본값은 2입니다. 이 설정은 데이터 인터페이스에서 사용되는 DNS 그룹에만 적용됩니다.
- **Timeout(**시간 초과**)** — 다음 DNS 서버를 시도하기 전에 기다리는 시간(1~30초)입니다. 기본값은 2초입니다. 시스템이 서버 목록을 재시도할 때마다 이 시간 초과 값이 두 배로 늘어납니다. 이 설정은 데이터 인터페이스에서 사용되는 DNS 그룹에만 적용됩니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

데이터 및 관리 트래픽용 DNS 설정

DNS(Domain Name System) 서버는 호스트 이름을 IP 주소로 확인하는 데 사용됩니다. 서로 다른 트래픽 유형에 적용되는 두 가지 DNS 서버 설정(데이터 및 특수 관리 트래픽)이 있습니다. 데이터 트래픽에는 액세스 제어 규칙 및 원격 액세스 VPN과 같이 DNS 조회가 필요한 FQDN을 사용하는 모든 서비스가 포함됩니다. 특수 관리 트래픽에는 스마트 라이선싱 및 데이터베이스 업데이트와 같은 관리 인터페이스에서 발생하는 트래픽이 포함됩니다.

CLI 설정 마법사를 사용하는 경우 초기 시스템 컨피그레이션 중에 관리 DNS 서버를 구성합니다. device manager 설정 마법사에서 데이터 및 관리 DNS 서버를 설정할 수도 있습니다. 다음 절차를 사용하여 DNS 서버 기본값을 변경할 수 있습니다.

configure network dns servers 및 **configure network dns searchdomains** 명령을 사용하여 CLI에서 관리 DNS 컨피그레이션을 변경할 수도 있습니다. 데이터 및 관리 인터페이스가 같은 DNS 그룹을 사용 중이라면 해당 그룹이 업데이트되며 다음 구축 시 데이터 인터페이스에도 변경 사항이 적용됩니다.

DNS 서버 통신에 대한 올바른 인터페이스를 결정하기 위해 threat defense는 라우팅 조회를 사용하지만, 사용되는 라우팅 테이블은 DNS를 활성화하는 인터페이스에 따라 다릅니다. 자세한 내용은 아래 인터페이스 설정을 참조하십시오.

DNS 확인에 문제가 있는 경우 다음 주제를 참조하십시오.

- 일반 DNS 문제 문제 해결, 829 페이지
- 관리 인터페이스용 DNS 문제 해결, 893 페이지

시작하기 전에

- DNS 서버 그룹을 만들었는지 확인합니다. 자세한 내용은 DNS 그룹 구성, 826 페이지 섹션을 참조해 주십시오.
- threat defense 디바이스에 DNS 서버에 액세스하기 위한 적절한 정적 또는 동적 경로가 있는지 확인합니다.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음 **System Settings(**시스템 설정**)** > **DNS Server(DNS** 서버**)** 링크를 클릭합니다.

System Settings(시스템 설정**)** 페이지가 이미 열려 있는 경우 목차에서 **DNS Server(DNS** 서버**)**를 클릭합니다.

단계 **2** 데이터 인터페이스용 DNS를 설정합니다.

a) 모든 인터페이스 또는 특정 인터페이스에서 DNS 조회를 활성화합니다. 이러한 선택은 사용되는 라우팅 테이블에도 영향을 미칩니다.

인터페이스에서 DNS 조회를 활성화하는 것은 조회를 위해 소스 인터페이스를 지정하는 것과 다릅니다. 디바이스는 항상 경로 조회를 사용하여 소스 인터페이스를 결정합니다.

- **ANY**(인터페이스를 선택하지 않음) - 관리 및 관리 전용 인터페이스를 포함하여 모든 인터페이스에서 DNS 조회를 활성화합니다. 디바이스는 데이터 라우팅 확인하며, 경로가 없으면 관리 전용 라우팅 테이블로 폴백됩니다.
- 인터페이스 미선택, 진단 인터페이스 또는 관리 전용 인터페이스 - 지정된 인터페이스에 DNS 조회를 활성화합니다. 디바이스는 데이터 라우팅 테이블만 확인합니다.
- 인터페이스 선택, 진단 인터페이스 또는 관리 전용 인터페이스 - 지정된 인터페이스에 DNS 조회를 활성화합니다. 디바이스는 데이터 라우팅 테이블을 확인하며, 경로가 없으면 관리 전용 라우팅 테이블로 폴백됩니다.
- 진단 인터페이스 또는 관리 전용 인터페이스만 선택 - 진단 또는 관리 전용 인터페이스에서 DNS 조회를 활성화합니다. 디바이스는 관리 전용 라우팅 테이블만 확인합니다.

b) 데이터 인터페이스에서 사용할 서버를 정의하는 **DNS Group(DNS** 그룹**)**을 선택합니다. 그룹이 아직 없으면 **Create New DNS Group(**새 **DNS** 그룹 생성**)**을 클릭하여 바로 생성합니다. 데이터 인터페이스에서 조회를 금지하려는 경우 **None(**없음**)**을 선택합니다.

c) (선택 사항). 액세스 제어 규칙에서 FQDN 네트워크 개체를 사용하려면 **FQDN DNS Settings(FQDN DNS** 설정**)**를 구성합니다.

이러한 옵션은 FQDN 개체를 확인할 때만 사용되며 기타 모든 유형의 DNS 확인에서는 무시됩니다.

- **Poll Time(**폴링 시간**)** - FQDN 네트워크 개체를 IP 주소로 확인하는 데 사용되는 폴링 주기의 시간(분)입니다. FQDN 개체는 액세스 제어 정책에서 사용되는 경우에만 확인됩니다. 타이머는 최대 확인 주기를 결정합니다. IP 주소 확인을 업데이트할 시기를 결정할 때는 DNS 항

목의 TTL(Time to Live) 값도 사용되므로, 개별 FQDN은 폴링 주기보다 더 자주 확인될 수 있습니다. 기본값은 240분(4시간)입니다. 범위는 1~65535분입니다.

- **Expiry(**만료**)** - DNS 항목이 만료(즉, DNS 서버에서 가져온 TTL이 경과함)될 때까지의 시간(분)입니다. 이 시간이 지나면 DNS 조회 테이블에서 항목이 제거됩니다. 항목 제거 시 테이블을 다시 컴파일해야 하므로 자주 제거하면 디바이스의 처리 부하가 증가할 수 있습니다. 일부 DNS 항목은 매우 짧은 TTL(3초 정도)을 가질 수 있으므로 이 설정을 사용하여 TTL을 가상으로 늘릴 수 있습니다. 기본값은 1분입니다(즉, TTL이 경과한지 1분 이후에 항목이 제거됨). 범위는 1~65535분입니다.

d) **Save(**저장**)**를 클릭합니다. 또한 컨피그레이션을 구축하여 디바이스에 변경 사항을 적용해야 합니다.

단계 **3** 관리 인터페이스용 DNS를 설정합니다.

a) 관리 인터페이스에서 사용할 서버를 정의하는 **DNS Group(DNS** 그룹**)**을 선택합니다. 그룹이 아직 없으면 **Create New DNS Group(**새 **DNS** 그룹 생성**)**을 클릭하여 바로 생성합니다.

b) **Save(**저장**)**를 클릭합니다. 관리 DNS 서버를 업데이트하려면 변경 사항을 구축해야 합니다.

일반 **DNS** 문제 문제 해결

DNS 서버는 관리 인터페이스 및 데이터 인터페이스에 대해 각기 별도로 설정해야 합니다. 일부 기능은 이 중 하나의 유형을 통해 이름 확인을 수행하지만 두 유형을 모두 사용하지는 않습니다. 그리고 사용 방식에 따라 특정 기능이 다른 확인 방법을 사용하는 경우도 있습니다.

예를 들어 **ping** *hostname* 및 **ping interface** *interface_name hostname* 명령에서는 데이터 인터페이스 DNS 서버를 사용하여 이름을 확인하는 반면, **ping system** *hostname* 명령에서는 관리 인터페이스 DNS 서버를 사용합니다. 따라서 특정 인터페이스 및 라우팅 테이블을 통해 연결을 테스트할 수 있습니다.

호스트 이름 조회 문제를 트러블슈팅할 때는 이 점에 유념하십시오.

관리 인터페이스용 DNS 문제 해결의 경우 관리 인터페이스용 DNS 문제 해결, 893 페이지의 내용도 참조하십시오.

이름 확인이 수행되지 않는 경우

이름 확인이 전혀 수행되지 않는 경우의 몇 가지 트러블슈팅 팁은 다음과 같습니다.

- 관리 인터페이스 및 데이터 인터페이스 모두에 대해 DNS 서버를 구성했는지 확인합니다. 데이터 인터페이스의 경우 인터페이스로 Any(모두)를 사용합니다. 일부 인터페이스에서 DNS를 허용하지 않으려는 경우에만 인터페이스를 명시적으로 지정하십시오.
- 데이터 인터페이스에서 조회를 위해 진단 인터페이스를 사용하고 있는 경우, 인터페이스에 IP 주소를 컨피그레이션했는지 확인합니다. 조회하려면 인터페이스에 IP 주소가 있어야 합니다.
- 진단 인터페이스를 통해 또는 관리 전용 인터페이스를 통해 DNS 서버에 연결할 수 없는데, 경로 조회 시 데이터 라우팅 테이블에서 일치를 찾으므로 관리 전용 라우팅 테이블에 대한 폴백이 없기 때문입니다. 진단 인터페이스를 사용하려면 해당 인터페이스만 선택해야 합니다.

- 각 DNS 서버의 IP 주소에 대해 ping을 실행하여 해당 주소에 연결할 수 있는지 확인합니다. 특정 인터페이스를 테스트하려면 **system** 및 **interface** 키워드를 사용합니다. ping에 실패하면 정적 경로와 게이트웨이를 확인합니다. 서버에 정적 경로를 추가해야 할 수 있습니다.
- ping에 성공했으나 이름 확인에 실패하는 경우 액세스 제어 규칙을 확인합니다. 서버 연결에 사용하는 인터페이스에 대해 DNS 트래픽(UDP/53)을 허용하고 있는지 확인합니다. 시스템과 DNS 서버 사이에 있는 디바이스에 의해 이 트래픽이 차단될 수도 있으므로 다른 DNS 서버를 사용해야 할 수 있습니다.
- ping이 정상적으로 실행되고 적절한 경로가 있으며 액세스 제어 규칙에 문제가 없다면 DNS 서버에 FQDN에 대한 매핑이 없을 가능성을 고려하십시오. 이러한 경우에는 다른 서버를 사용해야 할 수 있습니다.

잘못된 이름이 확인되는 경우

이름이 확인되기는 하지만 이름의 IP 주소가 최신 정보가 아닌 경우 캐싱 문제가 있을 수 있습니다. 이 문제는 액세스 제어 규칙에 사용되는 FQDN 네트워크 개체 등의 데이터 인터페이스 기반 기능에만 영향을 줍니다.

시스템에는 이전 조회에서 가져온 DNS 정보의 로컬 캐시가 있습니다. 새 조회를 수행해야 하는 경우 시스템은 먼저 로컬 캐시를 확인합니다. 로컬 캐시에 해당 정보가 있으면 그 결과 IP 주소를 반환합니다. 로컬 캐시에서 요청을 해결하지 못하면 DNS 서버로 DNS 쿼리가 전송됩니다. 외부 DNS 서버에서 요청을 해결한 경우 그 결과 IP 주소는 해당 호스트 이름과 함께 로컬 캐시에 저장됩니다.

각 조회에는 DNS 서버에 의해 정의되며 캐시에서 자동으로 만료되는 TTL(Time to Live) 값이 있습니다. 또한 시스템은 액세스 제어 규칙에 사용되는 FQDN의 값을 주기적으로 새로 고칩니다. 이러한 새로 고침은 최소한 폴링 시간 간격(기본적으로 4시간마다)으로 수행되지만 항목의 TTL(Time to Live) 값에 따라 더 자주 수행될 수도 있습니다.

로컬 캐시를 확인하려면 **show dns-hosts** 및 **show dns** 명령을 사용합니다. FQDN의 IP 주소가 잘못된 경우, **dns update** [**host** *hostname*] 명령을 사용하여 시스템에서 정보를 새로 고치도록 강제할 수 있습니다. 호스트를 지정하지 않고 명령을 사용하면 모든 호스트 이름이 새로 고쳐집니다.

clear dns [**host** *fqdn*] 및 **clear dns-hosts cache** 명령을 사용하면 캐시된 정보를 제거할 수 있습니다.

관리 인터페이스 구성

관리 인터페이스는 물리적 관리 포트에 연결된 가상 인터페이스입니다. 물리적 인터페이스에는 진단 가상 인터페이스도 포함됩니다. 이 인터페이스는 다른 물리적 인터페이스를 사용하여 **Interfaces(**인터페이스**)** 페이지에서 구성할 수 있습니다. 진단 인터페이스에 대한 자세한 내용은 관리/진단 인터페이스, 257 페이지를 참조하십시오.

관리 인터페이스는 다음과 같은 두 가지 용도로 사용됩니다.

- IP 주소에 대한 웹 및 SSH 연결을 열고 인터페이스를 통해 디바이스를 구성할 수 있습니다.
- 시스템은 이 IP 주소를 통해 스마트 라이선싱 및 데이터베이스 업데이트를 가져옵니다.

CLI 설정 마법사를 사용하는 경우 초기 시스템 컨피그레이션 중에 디바이스의 관리 주소 및 게이트웨이를 구성합니다. device manager 설정 마법사를 사용하는 경우에는 관리 주소와 게이트웨이가 기본값으로 유지됩니다.

필요한 경우 device manager를 통해 이러한 주소를 변경할 수 있습니다. **configure network ipv4 manual** 및 **configure network ipv6 manual** 명령을 사용하여 CLI에서 관리 주소 및 게이트웨이를 변경할 수도 있습니다. 기본 관리 인터페이스 설정을 복원하려면 **configure network** {**ipv4** | **ipv6**} **dhcp-dp-route** 명령을 사용하십시오.

고정 주소를 정의할 수도 있고, 관리 네트워크의 다른 디바이스가 DHCP 서버로 작동하는 경우에는 DHCP를 통해 주소를 가져올 수 있습니다. 대부분의 플랫폼에서 관리 인터페이스는 기본적으로 DHCP에서 IP 주소를 가져옵니다.

주의 현재 연결된 주소를 변경할 경우 변경 사항을 저장하면 즉시 적용되므로 device manager 또는 CLI에 액세스할 수 없게 됩니다. 디바이스와 다시 연결해야 합니다. 관리 네트워크에서 새 주소가 유효하며 사용 가능한지 확인합니다.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 후 **System Settings(**시스템 설정**)** > **Management Interface(**관리 인터페이스**)** 링크를 클릭합니다.

System Settings(시스템 설정**)** 페이지가 이미 열려 있는 경우 목차에서 **Management Interface(**관리 인터페이스**)**를 클릭하면 됩니다.

단계 **2** 관리 게이트웨이를 정의할 방법을 선택합니다.

게이트웨이는 시스템에서 스마트 라이선스 및 데이터베이스 업데이트(VDB, 규칙, 지리위치, URL 등)를 받고 관리 DNS 및 NTP 서버에 접속하기 위해 인터넷에 연결할 수 있는 방법을 결정합니다. 다음 옵션 중에서 선택합니다.

정적 **IP** 옵션**:**

- 데이터 인터페이스를 게이트웨이로 사용 - 별도의 관리 네트워크를 관리 인터페이스에 연결하지 않은 경우 이 옵션을 선택합니다. 라우팅 테이블에 따라 트래픽이 인터넷에 라우팅되며, 대개 외부 인터페이스를 거칩니다. 이 옵션은 threat defense virtual 디바이스에서는 지원되지 않습니다.
- 관리 인터페이스에 고유 게이트웨이 사용 - 별도의 관리 네트워크를 관리 인터페이스에 연결한 경우 IPv4 및 IPv6를 위한 고유 게이트웨이(아래)를 지정합니다.

DHCP IP 옵션**:**

- 데이터 인터페이스에 대체 시스템을 가진 관리 인터페이스에 고유한 게이트웨이 사용-DHCP 서버가 게이트웨이를 제공하는 경우 시스템은 관리 인터페이스를 통해 게이트웨이를 통과하는 관리 트래픽을 라우팅합니다. DHCP 서버가 게이트웨이를 제공하지 않는 경우, 시스템은 데이터

인터페이스 라우팅 테이블에 따라 관리 트래픽을 라우팅합니다. 일반적으로 외부 인터페이스를 통해 트래픽을 전송합니다. 이 옵션은 threat defense virtual 디바이스에서는 지원되지 않습니다.

- 관리 인터페이스에 고유한 게이트웨이 사용**(**대체 시스템 없음**)**— 시스템은 관리 인터페이스를 통해 DHCP 서버에서 제공하는 게이트웨이로 관리 트래픽을 라우팅합니다. DHCP 서버가 게이트웨이를 제공하지 않는 경우 시스템은 관리 인터페이스의 로컬 호스트에만 연결할 수 있습니다. 데이터 인터페이스를 통해 라우팅하려면 Fallback(대체 시스템) 옵션을 선택합니다.

단계 **3** IPv4, IPv6 중 하나 또는 둘 다의 관리 주소, 서브넷 마스크 또는 IPv6 접두사 및 게이트웨이(필요한 경우)를 구성합니다.

속성 집합을 하나 이상 구성해야 합니다. 특정 집합의 주소 지정 방법을 비활성화하려면 해당 집합을 비워 둡니다.

Type(유형**)** > **DHCP**를 선택하여 DHCP 또는 IPv6 자동 컨피그레이션을 통해 주소와 게이트웨이를 가져옵니다.

단계 **4** (선택 사항). 정적 IPv4 주소를 구성하는 경우 인터페이스에서 DHCP 서버를 구성합니다.

관리 인터페이스에서 DHCP 서버를 구성하는 경우, 관리 네트워크의 클라이언트가 DHCP 풀에서 주소를 가져올 수 있습니다. 이 옵션은 threat defense virtual 디바이스에서는 지원되지 않습니다.

a) **Enable DHCP Server(DHCP** 서버 활성화**)** > **On(**켜기**)**을 클릭합니다.
b) 서버의 주소 풀을 입력합니다.

주소 풀은 서버가 주소를 요청하는 클라이언트에 제공할 수 있는 IP 주소의 범위(최저 범위에서 최고 범위 순서)입니다. 이 IP 주소 범위는 관리 주소와 동일한 서브넷에 있어야 하며, 인터페이스 자체의 IP 주소, 브로드캐스트 주소 또는 서브넷 네트워크 주소는 포함할 수 없습니다. 풀의 시작 주소와 끝 주소를 하이픈으로 구분하여 지정합니다. 예를 들면 192.168.45.46-192.168.45.254와 같이 지정합니다.

단계 **5** **Save(**저장**)**를 클릭하고 경고를 확인한 후에 **OK(**확인**)**를 클릭합니다.

디바이스 호스트 이름 구성

디바이스 호스트 이름을 변경할 수 있습니다.

configure network hostname 명령을 사용하여 CLI에서 호스트네임을 변경할 수도 있습니다.

⚠

주의 호스트 이름을 사용하여 시스템에 연결할 때 호스트 이름을 변경하는 경우 변경 사항을 저장하면 즉시 적용되므로 device manager에 액세스할 수 없게 됩니다. 디바이스와 다시 연결해야 합니다.

프로시저

단계 **1** 디바이스를 클릭한 다음, **System Settings(**시스템 설정**)** > **Hostname(**호스트네임**)** 링크를 클릭합니다.

시스템 설정 페이지가 이미 열려 있는 경우 목차에서 호스트 이름을 클릭하면 됩니다.

단계 **2** 새 호스트 이름을 입력합니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

일부 시스템 프로세스의 경우에는 호스트 이름 변경 사항이 즉시 적용됩니다. 그러나 모든 시스템 프로세스에서 같은 이름이 사용되도록 하려면 변경 사항을 구축하여 업데이트를 완료해야 합니다.

시간 서비스(NTP, PTP) 구성

시스템은 NTP(Network Time Protocol)를 사용하여 시스템 시간을 설정합니다. NTP를 구성해야 합니다.

디바이스가 Cisco ISA 3000 어플라이언스인 경우, 네트워크에서 PTP를 사용하는 경우에도 PTP(Precision Time Protocol)를 구성할 수 있습니다.

NTP(Network Time Protocol) 구성

시스템에서 시간을 정의하려면 NTP(Network Time Protocol) 서버를 구성해야 합니다. NTP 서버는 초기 시스템 설정 시 구성하지만, 다음 절차를 통해 변경할 수 있습니다. NTP 연결에 문제가 있는 경우, NTP 트러블슈팅, 892 페이지를 참조하십시오.

threat defense 디바이스는 NTPv4를 지원합니다.

참고 Firepower 4100/9300의 경우, device manager을 통해 NTP를 설정하지 않습니다. FXOS에서 NTP를 컨피그레이션하십시오.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음 **System Settings(**시스템 설정**)** > **Time Services(**시간 서비스**)** 링크를 클릭합니다.

System Settings(시스템 설정) 페이지가 이미 열려 있는 경우 목차에서 **Time Services(**시간 서비스**)**를 클릭하면 됩니다.

단계 **2** **NTP Time Server(NTP** 시간 서버**)**에서 자체 시간 서버를 사용할지 아니면 Cisco 시간 서버를 사용할지를 선택합니다.

- **Default NTP Servers(**기본 **NTP** 서버**) -** 이 옵션을 선택하는 경우 서버 목록에는 NTP에 사용되는 서버 이름이 표시됩니다.
- **User-Defined NTP Servers(**사용자 정의 **NTP** 서버**) -** 이 옵션을 선택하는 경우 사용하려는 NTP 서버의 IPv4 또는 IPv6 주소 또는 FQDN(Fully Qualified Domain Name)을 입력합니다. 예를 들어 ntp1.example.com 또는 10.100.10.10을 입력합니다. NTP 서버를 3개까지 추가할 수 있습니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

PTP(Precision Time Protocol) 구성(ISA 3000)

PTP(Precision Time Protocol)는 패킷 기반 네트워크에서 다양한 디바이스의 클록을 동기화하기 위해 개발된 시간 동기화 프로토콜입니다. 이러한 디바이스 클록은 일반적으로 정밀도와 안정성이 다양합니다. 이 프로토콜은 산업, 네트워크에 연결된 측정 및 제어 시스템을 위해 특별히 설계되었으며 최소한의 대역폭 및 적은 처리 오버헤드를 필요로 하기 때문에 분산 시스템에서 사용하기에 가장 적합합니다.

PTP 시스템은 PTP 및 비 PTP 디바이스의 조합으로 구성된 분산형, 네트워크에 연결된 시스템입니다. PTP 디바이스에는 일반 클록, 경계 클록 및 투명 클록이 있습니다. 비 PTP 디바이스에는 네트워크 스위치, 라우터 및 기타 인프라 디바이스가 있습니다.

threat defense 디바이스를 투명 클록이 되도록 구성할 수 있습니다. threat defense 디바이스에서는 클록을 PTP 클록과 동기화하지 않습니다. threat defense 디바이스에서는 PTP 클록에 정의된 대로 PTP 기본 프로필을 사용합니다.

PTP 디바이스를 구성할 때 함께 작동할 디바이스의 도메인 번호를 정의합니다. 따라서 여러 PTP 도메인을 구성한 다음, 하나의 특정 도메인에 대해 PTP 클록을 사용하도록 비 PTP 디바이스를 각각 구성할 수 있습니다.

시작하기 전에

디바이스에서 사용해야 하는 PTP 클록에 구성된 도메인 번호를 결정합니다. 또한 시스템에서 도메인의 PTP 클록에 연결하기 위해 통과하는 인터페이스를 결정합니다.

다음은 PTP 구성에 대한 지침입니다.

- 이 기능은 Cisco ISA 3000 어플라이언스에서만 사용할 수 있습니다.
- Cisco PTP는 멀티캐스트 PTP 메시지만 지원합니다.
- PTP는 IPv4 네트워크용으로만 사용할 수 있으며 IPv6 네트워크용으로는 사용할 수 없습니다.
- PTP 구성은 라우팅 또는 브리지 그룹 멤버에 관계없이 물리적 이더넷 데이터 인터페이스에서 지원됩니다. 이는 관리 인터페이스, 하위 인터페이스, EtherChannel, BVI(Bridge Virtual Interfaces) 또는 기타 가상 인터페이스에서 지원되지 않습니다.
- VLAN 하위 인터페이스에서 이동하는 PTP가 지원되며 이때 적절한 PTP 구성이 현재 상위 인터페이스에 있다고 가정합니다.

- PTP 패킷이 디바이스를 통해 이동할 수 있는지 확인해야 합니다. PTP 트래픽은 UDP 대상 포트 319 및 320과 대상 IP 주소 224.0.1.129로 식별되므로 이 트래픽을 허용하는 액세스 제어 규칙이 작동해야 합니다.
- 라우팅 인터페이스 간에 PTP 패킷이 이동할 경우, 멀티캐스트 라우팅을 활성화해야 하며 각 인터페이스는 224.0.1.129 IGMP 멀티캐스트 그룹에 조인해야 합니다. 동일한 브리지 그룹에 있는 인터페이스 간에 PTP 패킷이 이동할 경우에는 멀티캐스트 라우팅을 활성화하고 IGMP 그룹을 구성하지 않아도 됩니다.

프로시저

단계 **1** PTP 클록 연결 인터페이스의 구성을 확인합니다.

기본 구성에서는 모든 인터페이스를 동일한 브리지 그룹에 배치하지만, 브리지 그룹에서 인터페이스를 제거할 수 있습니다. 멀티캐스트 IGMP 그룹과 관련하여 다르게 구성해야 하므로 인터페이스가 라우팅되었는지 아니면 브리지 그룹 멤버인지 여부를 확인하는 것이 중요합니다.

다음 절차에서는 브리지 그룹에 포함된 인터페이스를 확인하는 방법에 대해 설명합니다. PTP용으로 구성하는 인터페이스가 브리지 그룹 멤버인지 확인합니다.

a) **Device(**디바이스**)** > **Interfaces(**인터페이스**)**에서 **View All Interfaces(**모든 인터페이스 보기**)**를 클릭합니다.
b) 목록에서 인터페이스를 찾고 Mode(모드) 열을 선택합니다. BridgeGroupMember는 브리지 그룹의 일부임을 의미하며, 그 외의 경우에는 라우팅되어야 합니다.

단계 **2** **Device(**디바이스**)**를 클릭한 다음 **System Settings(**시스템 설정**)** > **Time Services(**시간 서비스**)** 링크를 클릭합니다.

System Settings(시스템 설정**)** 페이지가 이미 열려 있는 경우 목차에서 **Time Services(**시간 서비스**)**를 클릭하면 됩니다.

단계 **3** PTP 설정을 구성합니다.

- **Domain Number(**도메인 번호**)** — 네트워크의 PTP 디바이스에 구성된 도메인 번호(0~255)입니다. 다른 도메인에서 수신한 패킷은 일반 멀티캐스트 패킷으로 처리되며 PTP 처리를 거치지 않습니다.
- **Clock Mode(**클록 모드**)** — **EndToEndTransparent**를 선택합니다. 이 디바이스는 PTP 투명 클록으로만 작동할 수 있습니다.

  또는 **Forward(**포워드**)**를 선택할 수 있지만, 이는 PTP를 구성하지 않는 것과 같습니다. 도메인 번호가 무시됩니다. PTP 패킷은 멀티캐스트 트래픽에 대한 라우팅 테이블을 기준으로 디바이스를 통과합니다. 이는 기본 PTP 컨피그레이션입니다.
- **Interfaces(**인터페이스**)** — 시스템이 네트워크의 PTP 클록에 연결할 때 통과하는 모든 인터페이스를 선택합니다. PTP는 이러한 인터페이스에서만 활성화됩니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

단계 **5** 선택한 인터페이스 중에서 라우팅된 인터페이스, 즉 브리지 그룹 구성원이 아닌 인터페이스의 경우에는 FlexConfig를 사용하여 멀티캐스트 라우팅을 활성화하고 라우팅된 인터페이스를 올바른 IGMP 그룹에 조인해야 합니다.

선택한 모든 인터페이스가 브리지 그룹 구성원인 경우 이 단계를 완료하지 마십시오. 브리지 그룹 구성원에서 IGMP를 구성하려고 하면 구축 오류가 발생합니다.

a) **Device(**디바이스**)** > **Advanced Configuration(**고급 컨피그레이션**)**에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

b) Advanced Configuration(고급 컨피그레이션) 목차에서 **FlexConfig** > **FlexConfig Objects(FlexConfig** 개체**)**를 클릭합니다.

c) 멀티캐스트 라우팅을 활성화하고 라우팅된 인터페이스에 대한 IGMP 조인을 구성하는 데 필요한 개체를 생성합니다.

다음은 개체에 대한 기본 템플릿이 될 수 있습니다. 이 예시에서 GigabitEthernet1/2는 PTP를 활성화하는 하나의 라우팅된 인터페이스입니다. 인터페이스 하드웨어 이름을 적절하게 변경하고, 라우팅된 인터페이스가 두 개 이상 있을 경우 각각의 추가 인터페이스에 **interface** 및 **igmp** 명령을 반복합니다.

igmp 명령은 224.0.1.129 IGMP 그룹에 조인합니다. 이 주소는 네트워크 주소와 관계없이 모든 인터페이스에 대한 올바른 IP 주소입니다.

```
multicast-routing
interface GigabitEthernet1/2
 igmp join-group 224.0.1.129
```

무효화 템플릿은 다음과 같이 표시됩니다.

```
no multicast-routing
interface GigabitEthernet1/2
 no igmp join-group 224.0.1.129
```

d) 목차에서 **FlexConfig Policy(FlexConfig** 정책**)**를 클릭하고, 이 개체를 FlexConfig 정책에 추가한 후 **Save(**저장**)**를 클릭합니다.

미리보기에 개체의 정상적인 명령이 표시되는지 확인합니다.

다음에 수행할 작업

변경 사항을 구축한 후에 PTP 설정을 확인할 수 있습니다. device manager CLI 콘솔에서 또는 SSH나 콘솔 세션에서 다양한 **show ptp** 명령을 실행합니다. 예를 들어 GigabitEthernet1/2에만 도메인 10에 대한 PTP를 구성한 경우, 출력은 다음과 같이 표시될 수 있습니다.

```
> show ptp clock
 PTP CLOCK INFO
  PTP Device Type: End to End Transparent Clock
  Operation mode: One Step
  Clock Identity: 34:62:88:FF:FE:1:73:81
  Clock Domain: 10
  Number of PTP ports: 4
> show ptp port
```

```
PTP PORT DATASET: GigabitEthernet1/1
 Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
 Port identity: Port Number: 1
 PTP version: 2
 Port state: Disabled

PTP PORT DATASET: GigabitEthernet1/2
 Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
 Port identity: Port Number: 2
 PTP version: 2
 Port state: Enabled

PTP PORT DATASET: GigabitEthernet1/3
 Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
 Port identity: Port Number: 3
 PTP version: 2
 Port state: Disabled

PTP PORT DATASET: GigabitEthernet1/4
 Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
 Port identity: Port Number: 4
 PTP version: 2
 Port state: Disabled
```

관리 연결용 HTTP 프록시 구성

시스템과 인터넷 사이에 직접 연결이 없는 경우 관리 인터페이스에 대한 HTTP 프록시를 설정할 수 있습니다. 그러면 시스템에서 데이터베이스 업데이트를 다운로드하기 위해 device manager에 대한 연결 및 시스템에서 Cisco로의 연결을 비롯한 모든 관리 연결에 프록시를 사용합니다.

configure network http-proxy 명령을 사용하여 threat defense CLI에서 HTTP 프록시를 구성할 수도 있습니다.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음, **System Settings(**시스템 설정**)** > **HTTP Proxy(HTTP** 프록시**)** 링크를 클릭합니다.

System Settings(시스템 설정**)** 페이지가 이미 열려 있는 경우 목차에서 **HTTP Proxy(HTTP** 프록시**)**를 클릭하면 됩니다.

단계 **2** 토글을 클릭하여 프록시를 활성화한 다음, 프록시 설정을 구성합니다.

- **HTTP Proxy(HTTP** 프록시**)** — 프록시 서버의 IP 주소입니다.
- **Port(**포트**)** — 프록시 서버가 HTTP 연결을 수신 대기하도록 구성된 포트 번호입니다.
- **Use Proxy authentication(**프록시 인증 사용**)** — 서버가 프록시 연결에 대한 인증을 요구하도록 구성된 경우 이 옵션을 선택합니다. 이 옵션을 선택하는 경우에는 프록시 서버에 로그인할 수 있는 어카운트의 **Username(**사용자 이름**)** 및 **Password(**비밀번호**)**도 입력합니다.

단계 **3** **Save(**저장**)**를 클릭한 다음, 변경할 사항을 확인합니다.

변경 사항은 즉시 적용됩니다. 구축 작업은 필요하지 않습니다.

시스템에서 관리 연결을 완료하는 방법을 변경하고 있으므로 device manager에 대한 연결이 끊어집니다. 변경을 완료하려면 몇 분 정도 기다린 다음, 브라우저 창을 새로 고침하시고 다시 로그인하십시오.

클라우드 서비스 구성

Cisco Defense Orchestrator, Cisco Threat Response 및 CDO와 같은 다양한 클라우드 기반 애플리케이션을 사용할 수 있도록 클라우드 서비스에 등록할 수 있습니다.

클라우드에 등록되면 페이지에 등록 상태와 테넌시 유형 및 디바이스가 등록된 어카운트 이름이 표시됩니다.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음 **System Settings(**시스템 설정**)** > **Cloud Services(**클라우드 서비스**)** 링크를 클릭합니다.

System Settings(시스템 설정**)** 페이지가 이미 열려 있는 경우 목차에서 **Cloud Services(**클라우드 서비스**)**를 클릭하면 됩니다.

디바이스가 등록되지 않은 경우 이 페이지에는 Cisco 클라우드에 등록하기 위한 등록 방법이 표시됩니다. 클라우드에 등록한 후에는 개별 클라우드 서비스를 활성화 또는 비활성화할 수 있습니다.

단계 **2** Cisco 클라우드에 등록하려면(평가 모드에서 또는 클라우드 서비스에서 등록을 취소한 후) 다음 옵션 중 하나를 선택합니다.

- **Security/CDO Account(**보안/**CDO** 계정**)** — 다음 방법 중 하나를 사용할 수 있습니다.

  참고 CDO는 클라우드 제공 관리 센터를 사용해 threat defense 디바이스를 관리할 수 있습니다. CDO의 간소화된 디바이스 관리자 기능은 이미 이 모드에서 threat defense를 관리하고 있는 기존 사용자만 사용할 수 있습니다.

  - **Auto-enroll with Tenancy from Cisco Defense Orchestrator(Cisco Defense Orchestrator**에서 테넌시로 자동 등록**)**(Firepower 1000, 2100, Secure Firewall 3100만 해당). 등록 키를 얻는 대신 자동 등록을 사용할 수 있습니다. 먼저, CDO로 이동하여 디바이스의 일련 번호를 사용하여 디바이스를 추가합니다. 그 다음 device manager에서 이 체크 박스를 선택하고 등록을 시작합니다. 디바이스 섀시 또는 포장 전표에서 일련 번호를 확인합니다. FXOS의 경우 FXOS CLI로 이동하고 **show chassis detail** 명령을 사용하여 일련 번호(SN)로 레이블이 표시된 올바른 일련 번호를 검색할 수 있습니다. threat defense 명령 **show serial-number**은 CDO 등록에 권장되지 않는 다른 일련 번호를 제공합니다. 이 방법은 CDO의 클라우드 제공 관리 센터 및 CDO의 레거시 디바이스 관리자 모드에서 작동합니다.
  - CDO 또는 보안 계정에 로그인하여 등록 키를 생성합니다. 그런 다음 이 페이지로 돌아와서 **Cloud Services Region(**클라우드 서비스 영역**)**을 선택하고 **Registration Key(**등록 키**)**에 붙여

넣습니다. 이 방법은 CDO의 레거시 디바이스 관리자 모드에서만 작동합니다. CDO의 클라우드 제공 관리 센터는 Device Manager에서 Management Center 또는 CDO로 전환, 844 페이지를 참조하십시오.

이때 **Cisco Defense Orchestrator** 및 **Cisco Success Network**를 활성화할 수도 있습니다. 이는 기본적으로 활성화됩니다.

- 스마트 라이선스—(CDO 미사용 시에만 해당) 링크를 클릭하여 Smart Licensing(스마트 라이선싱) 페이지로 이동하고 CSSM에 등록합니다. 등록 프로세스 중에 Cisco Success Network를 활성화하는 경우

  참고 클라우드 서비스에서 등록을 취소했거나 등록을 위한 스마트 라이선스 접근 방식에 몇 가지 추가 단계가 있습니다. 이 경우 **Cloud Services Region(**클라우드 서비스 지역**)**을 선택한 다음, **Register (**등록**)**를 클릭합니다. 공개된 내용을 읽고 **Accept(**수락**)**를 클릭합니다.

단계 **3** 클라우드 서비스에 등록한 후에는 필요에 따라 기능을 활성화하거나 비활성화할 수 있습니다. 다음 주제를 참고하십시오.

- 활성화 또는 비활성화 CDO (레거시 디바이스 관리자 모드), 839 페이지
- Cisco Success Network에 연결, 840 페이지
- Cisco Cloud로 이벤트 전송, 841 페이지
- 클라우드 서비스에서 등록 취소, 842 페이지

활성화 또는 비활성화 CDO (레거시 디바이스 관리자 모드)

참고 이 섹션은 CDO의 레거시 디바이스 관리자 모드에만 적용되며 클라우드 제공 관리 센터에는 적용되지 않습니다.

클라우드 서비스 구성, 838 페이지에서 권장하는 대로 CDO의 등록 키를 사용하여 클라우드 서비스에 등록한 경우, 디바이스가 이미 CDO에 등록되어 있습니다. 나중에 필요에 따라 연결을 비활성화하거나 다시 활성화할 수 있습니다.

디바이스가 스마트 라이선싱을 사용하여 클라우드 서비스에 등록된 경우 CDO를 활성화하면 문제가 발생합니다. 디바이스가 CDO 인벤토리에 표시되지 않습니다. 먼저 클라우드 서비스에서 디바이스 등록을 해제하는 것이 좋습니다. 기어(⚙) 드롭다운 목록에서 **Unregister Cloud Services(**클라우드 서비스 등록 해제**)**를 선택합니다. 등록을 취소한 후에는 CDO에서 등록 토큰을 가져오고 클라우드 서비스 구성, 838 페이지에서 설명하는 것과 같이 토큰과 보안 어카운트를 사용하여 다시 등록합니다.

클라우드 관리 방식에 대한 자세한 내용을 확인하려면 CDO 포털(http://www.cisco.com/go/cdo)을 참조하거나 서비스를 받고 있는 리셀러 또는 파트너에게 문의하십시오.

시작하기 전에

고가용성을 구성하려는 경우 고가용성 그룹에서 사용할 두 디바이스를 모두 등록해야 합니다.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음 **System Settings(**시스템 설정**)** > **Cloud Services(**클라우드 서비스**)** 링크를 클릭합니다.

System Settings(시스템 설정) 페이지가 이미 열려 있는 경우 목차에서 **Cloud Services(**클라우드 서비스**)**를 클릭하면 됩니다.

단계 **2** 설정을 적절하게 변경하려면 CDO 기능의 **Enable(**활성화**)/Disable(**비활성화**)** 버튼을 클릭합니다.

Cisco Success Network에 연결

디바이스를 등록할 때 Cisco Success Network에 대한 연결을 활성화할지를 결정합니다. 디바이스 등록, 96 페이지의 내용을 참조하십시오.

Cisco Success Network를 활성화하면 Cisco가 기술 지원을 제공하는 데 필수적인 사용자 정보 및 통계를 Cisco에 제공하게 됩니다. 또한, 이 정보를 통해 Cisco는 제품을 개선할 수 있으며 사용 가능하지만 사용되지 않은 기능을 알려 네트워크의 제품 가치를 최대화하도록 할 수 있습니다.

연결을 활성화하는 경우, 디바이스에서는 기술 지원 서비스, 클라우드 관리 및 모니터링 서비스와 같은 Cisco의 추가 제공 서비스에 참여할 수 있도록 Cisco Cloud에 대한 보안 연결을 설정합니다. 디바이스는 이 안전한 연결을 설정하고 항상 유지합니다. 클라우드에서 연결을 완전히 해제하는 방법에 대한 내용은 클라우드 서비스에서 등록 취소, 842 페이지를 참조하십시오.

디바이스를 등록하고 나면 Cisco Success Network 설정을 변경할 수 있습니다.

참고 시스템에서 Cisco에 데이터를 전송할 때 작업 목록에는 텔레메트리 작업이 표시됩니다.

시작하기 전에

Cisco Success Network를 활성화하려면 디바이스를 클라우드에 등록해야 합니다. 디바이스를 등록하려면 디바이스를 Cisco Smart Software Manager(Smart Licensing(스마트 라이선싱) 페이지)에 등록(등록 중 Cisco Success Network 옵션 선택)하거나, 등록 키를 입력(CDO 전용 레거시 디바이스 관리자 모드)하여 CDO에 등록하십시오.

참고 고가용성 그룹의 액티브 유닛에서 Cisco Success Network를 활성화하면 스탠바이 유닛에서도 연결이 활성화됩니다.

프로시저

단계 1 **Device(**디바이스**)**를 클릭한 다음 **System Settings(**시스템 설정**)** > **Cloud Services(**클라우드 서비스**)** 링크를 클릭합니다.

System Settings(시스템 설정) 페이지가 이미 열려 있는 경우 목차에서 **Cloud Services(**클라우드 서비스**)**를 클릭하면 됩니다.

단계 2 설정을 적절하게 변경하려면 Cisco Success Network 기능의 **Enable**/**Disable(**활성화/비활성화**)** 제어를 클릭합니다.

sample data(샘플 데이터**)** 링크를 클릭하면 Cisco에 전송된 정보 유형을 확인할 수 있습니다.

연결을 활성화하는 경우 공개되는 내용을 읽고 **Accept(**수락**)**를 클릭합니다.

Cisco Cloud로 이벤트 전송

Cisco Cloud 서버에 이벤트를 전송할 수 있습니다. 여기서는 다양한 Cisco Cloud 서비스에서 이벤트에 액세스할 수 있습니다. 그러면 이러한 클라우드 애플리케이션(예: SecureX threat response)을 사용하여 이벤트를 분석하고 디바이스에 발생했을 가능성이 있는 위협을 평가할 수 있습니다.

클라우드 툴은 전송하는 이벤트의 사용 여부를 결정합니다. 사용하지 않는 이벤트를 클라우드로 보내지 않으면서 대역폭 및 스토리지 공간을 모두 낭비하지 않도록 툴의 설명서를 참조하거나 이벤트 데이터를 검토하십시오. 툴은 동일한 소스에서 이벤트를 가져오므로 선택 시 가장 제한적인 툴이 아니라 사용하는 모든 툴을 반영해야 합니다. 대표적인 예는 다음과 같습니다.

- CDO의 보안 애널리틱스 및 로깅 툴은 모든 연결 이벤트를 사용할 수 있습니다.
- SecureX threat response 및 SecureX는 우선순위가 높은 연결 이벤트만 사용하므로 이러한 툴만 사용하는 경우에는 모든 연결 이벤트를 클라우드로 전송할 필요가 없습니다. 또한 이러한 툴은 보안 인텔리전스 우선순위가 높은 이벤트만 사용합니다.

시작하기 전에

디바이스를 클라우드 서비스에 등록해야 이 서비스를 활성화할 수 있습니다.

미국 지역의 경우 https://visibility.amp.cisco.com/에서, EU 지역의 https://visibility.eu.amp.cisco.com경우에는 에서, APJC 지역의 경우 https://visibility.apjc.amp.cisco.com에서 SecureX threat response에 연결할 수 있습니다. http://cs.co/CTRvideos에서 YouTube를 통해 애플리케이션의 용도와 이점에 대한 비디오를 볼 수 있습니다. SecureX threat response와 함께 threat defense를 사용하는 방법에 대한 자세한 내용은 *Cisco Secure Firewall Threat Defense* 및 *SecureX threat* 통합 가이드(https://www.cisco.com/c/en/us/support/security/defense-center/products-installation-and-configuration-guides-list.html에서 확인 가능)를 참조하십시오.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음 **System Settings(**시스템 설정**)** > **Cloud Services(**클라우드 서비스**)** 링크를 클릭합니다.

System Settings(시스템 설정) 페이지가 이미 열려 있는 경우 목차에서 **Cloud Services(**클라우드 서비스**)**를 클릭하면 됩니다.

단계 **2** 설정을 적절하게 변경하려면 **Send Events to the Cisco Cloud(Cisco Cloud**에 이벤트 전송**)** 옵션의 **Enable**/**Disable(**활성화/비활성화**)** 제어를 클릭합니다.

단계 **3** 서비스를 활성화하는 경우 클라우드에 전송할 이벤트를 선택하라는 메시지가 표시됩니다. 나중에 선택한 이벤트 목록 옆에 있는 **Edit(**수정**)**를 클릭하여 이러한 선택 사항을 변경할 수 있습니다. 전송할 이벤트 유형을 선택하고 **OK(**확인**)**를 클릭합니다.

- **File/Malware(**파일/악성코드**)** - 액세스 제어 규칙에 적용한 모든 파일 정책에 해당합니다.
- **Intrusion(**침입**)** - 액세스 제어 규칙에 적용한 모든 침입 정책에 해당합니다.
- **Connection(**연결**)** - 기록을 활성화한 액세스 제어 규칙에 해당합니다. 이 옵션을 선택하는 경우 모든 연결 이벤트를 전송하거나 높은 우선순위 연결 이벤트만 전송하도록 선택할 수도 있습니다. 높은 우선순위 연결 이벤트는 침입, 파일 또는 악성코드 이벤트를 트리거하는 연결이나 보안 인텔리전스 차단 정책과 일치하는 연결과 관련된 이벤트입니다.

클라우드 서비스에서 등록 취소

더 이상 클라우드 서비스를 사용하지 않으려는 경우 클라우드에서 디바이스 등록을 취소할 수 있습니다. 디바이스를 서비스에서 제거하거나 달리 삭제하는 경우 등록을 취소할 수 있습니다. 클라우드 서비스 지역을 변경해야 하는 경우 등록을 취소한 후 다시 등록할 때 새 지역을 선택합니다.

이 절차를 사용하여 클라우드에서 등록을 취소해도 스마트 라이선싱 등록에는 영향을 주지 않습니다.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음 **System Settings(**시스템 설정**)** > **Cloud Services(**클라우드 서비스**)** 링크를 클릭합니다.

System Settings(시스템 설정) 페이지가 이미 열려 있는 경우 목차에서 **Cloud Services(**클라우드 서비스**)**를 클릭하면 됩니다.

단계 **2** 기어(⚙) 드롭다운 목록에서 **Unregister Cloud Services(**클라우드 서비스 등록 취소**)**를 선택합니다.

단계 **3** 경고를 읽고 **Unregister(**등록 취소**)**를 클릭합니다.

활성화한 클라우드 서비스는 자동으로 비활성화되며 해당 서비스를 다시 활성화할 수 있는 기능은 제거됩니다. 그러나 이제 클라우드에 등록하기 위한 컨트롤이 표시되고 다시 등록할 수 있습니다.

웹 분석 활성화 또는 비활성화

웹 분석을 활성화하면 페이지 조회 수를 기반으로 하는 익명 제품 사용 정보가 Cisco에 제공됩니다. 이 정보에는 확인한 페이지, 특정 페이지를 사용한 시간, 브라우저 버전, 제품 버전, 디바이스 호스트 이름 등이 포함됩니다. Cisco는 이 정보를 활용해 기능 사용 패턴을 확인하고 제품을 개선할 수 있습니다. 모든 사용량 데이터는 익명으로 전송되며 민감한 데이터는 전송되지 않습니다.

웹 분석은 기본적으로 활성화됩니다.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음, **System Settings(**시스템 설정**)** > **Web Analytics(**웹 분석**)** 링크를 클릭합니다.

System Settings(시스템 설정) 페이지가 이미 열려 있는 경우 목차에서 **Web Analytics(**웹 분석**)**를 클릭하면 됩니다.

단계 **2** 설정을 적절하게 변경하려면 **Web Analytics(**웹 분석**)** 기능의 **Enable**/**Disable(**활성화/비활성화**)** 제어를 클릭합니다.

URL Filtering(URL 필터링) 기본 설정 컨피그레이션

시스템에서는 CSI(Cisco 종합적 보안 인텔리전스)(Cisco Talos Intelligence Group(Talos))에서 URL 카테고리 및 평판 데이터베이스를 가져옵니다. 이러한 환경 설정은 데이터베이스 업데이트 및 시스템이 카테고리나 평판을 알 수 없는 URL을 처리하는 방법을 제어합니다. 이러한 환경 설정을 지정하려면 URL 필터링 라이선스를 활성화해야 합니다.

프로시저

단계 **1** 디바이스를 클릭한 다음, **System Settings(**시스템 설정**)** > **URL Filtering Preferences(URL** 필터링 환경 설정**)** 링크를 클릭합니다.

시스템 설정 페이지가 이미 열려 있는 경우 목차에서 **URL** 필터링 기본 설정을 클릭하면 됩니다.

단계 **2** 다음 옵션을 구성합니다.

- **Enable Automatic Updates(**자동 업데이트 활성화**)** - 업데이트된 URL 데이터를 시스템에서 자동으로 확인하고 다운로드할 수 있도록 합니다. 이 데이터에는 카테고리 및 평판 정보가 포함됩니다. 시스템은 30분마다 업데이트를 확인하지만, 데이터는 대개 매일 한 번씩 업데이트됩니다. 기

본적으로는 업데이트가 활성화됩니다. 이 옵션을 선택 취소하는 경우 범주 및 평판 필터링을 사용 중이라면 자동 업데이트를 주기적으로 활성화하여 새 URL 데이터를 가져옵니다.

- **Query Cisco CSI for Unknown URLs(Cisco CSI**에서 알 수 없는 **URL** 쿼리**)** - 로컬 URL 필터링 데이터베이스에 범주 및 평판 데이터가 없는 URL에 대해 Cisco CSI에 업데이트된 정보를 확인할지를 선택합니다. 조회에서 적절한 시간제한 이내에 이 정보가 반환되면 URL 조건을 기준으로 액세스 규칙을 선택할 때 해당 정보가 사용됩니다. 그렇지 않으면 URL은 미분류 범주와 일치합니다. 메모리 제한으로 인해 더 작은 URL 데이터베이스를 설치하는 저가형 시스템에서는 이 옵션을 반드시 선택해야 합니다.

- **URL Time to Live(Query Cisco CSI for Unknown URLs(**알 수 없는 **URL**의 경우 **Cisco CSI**에 쿼리**)**를 선택하면 사용 가능함) - 지정된 URL에 대해 카테고리 및 평판 조회 값을 캐시할 기간입니다. TTL(Time to Live)이 만료되면 다음 번에 URL 액세스를 시도할 때 카테고리/평판을 새로 조회합니다. 이 시간이 짧을수록 URL 필터링 정확도가 높아지고, 시간이 길수록 알 수 없는 URL에 대한 필터링 성능이 향상됩니다. TTL은 2, 4, 8, 12, 24, 48시간, 1주 또는 Never(안 함, 기본값)로 설정할 수 있습니다.

단계 **3** 필요에 따라 **Check the Category for a URL(URL**의 카테고리 확인**)**이 가능합니다.

특정 URL의 카테고리 및 평판을 확인할 수 있습니다. **URL to Check(**확인할 **URL)** 상자에서 URL을 입력하고 **Go(**이동**)**를 클릭하십시오. 결과를 볼 수 있는 외부 웹 사이트로 연결됩니다. 분류에 동의하지 않는 경우 **Submit a URL Category Dispute(URL** 카테고리 이의 제출**)** 링크를 클릭하고 저희에게 알려주십시오.

단계 **4** **Save(**저장**)**를 클릭합니다.

Device Manager에서 Management Center 또는 CDO로 전환

device manager에서 전환하고자 하는 경우 관리를 위해 threat defense 디바이스가 management center 또는 CDO에 연결되도록 구성할 수 있습니다.

참고 CDO는 클라우드 제공 관리 센터를 사용해 threat defense 디바이스를 관리할 수 있습니다. CDO의 간소화된 디바이스 관리자 기능은 이미 이 모드에서 threat defense를 관리하고 있는 기존 사용자만 사용할 수 있습니다. 이 절차는 클라우드 제공 관리 센터에만 적용됩니다.

device manager을 사용하여 management center/CDO 설정을 수행할 때 관리를 위해 management center/CDO로 전환하면 관리 인터페이스 및 관리자 액세스 설정과 더불어 device manager에서 완료된 모든 인터페이스 구성이 유지됩니다. 액세스 제어 정책 또는 보안 영역과 같은 기타 기본 구성 설정은 유지되지 않습니다. threat defense CLI를 사용하는 경우 관리 및 management center/CDO 액세스 설정만 유지됩니다(예: 기본 내부 인터페이스 구성은 유지되지 않음).

management center/CDO/로 전환한 후에는 더 이상 device manager를 사용하여 threat defense 디바이스를 관리할 수 없습니다.

시작하기 전에

방화벽이 고가용성으로 구성된 경우에는 먼저 device manager(사용 가능한 경우) 또는 **configure high-availability disable** 명령을 사용하여 고가용성 구성을 해제해야 합니다. 액티브 유닛에서 고가용성을 해제하는 것이 가장 좋습니다.

프로시저

단계 **1** Cisco Smart Software Manager에 방화벽을 등록한 경우 관리자를 전환하기 전에 등록을 취소해야 합니다. 디바이스 등록 취소, 99 페이지을 참조하십시오.

방화벽 등록을 취소하면 기본 라이선스와 모든 기능 라이선스가 해제됩니다. 방화벽을 등록 취소하지 않으면 해당 라이선스는 Cisco Smart Software Manager에서 방화벽에 할당된 상태로 유지됩니다.

단계 **2** (필요할 수 있음) 관리 인터페이스를 구성합니다. 관리 인터페이스 구성, 830 페이지 섹션을 참조하십시오.

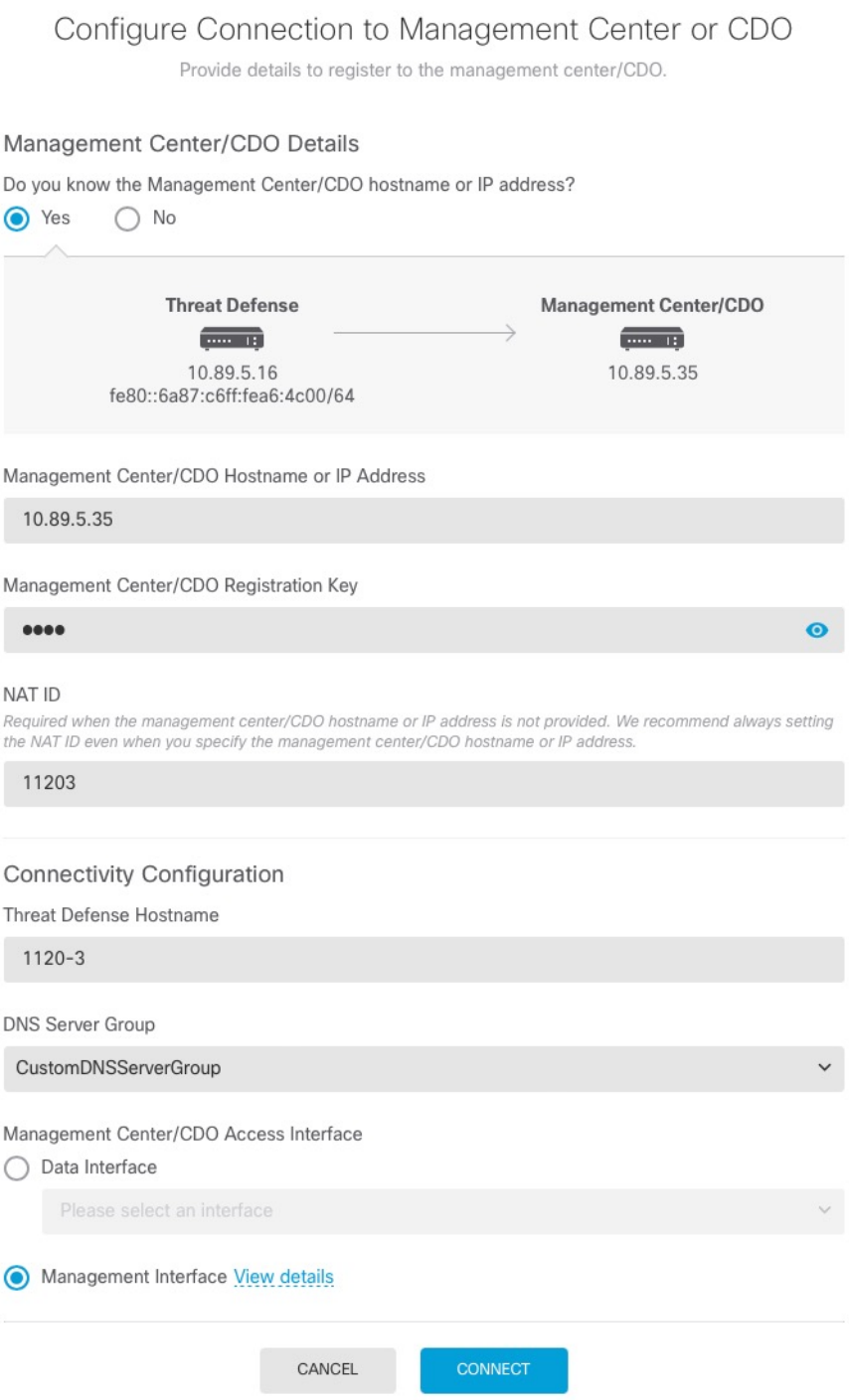
관리자 액세스에 데이터 인터페이스를 사용하려는 경우에도 관리 인터페이스 구성을 변경해야 할 수 있습니다. device manager 연결을 위해 관리 인터페이스를 사용하는 경우 device manager에 다시 연결해야 합니다.

- 관리자 액세스용 데이터 인터페이스 - 관리 인터페이스에 데이터 인터페이스로 설정된 게이트웨이가 있어야 합니다. 기본적으로 관리 인터페이스는 DHCP에서 IP 주소 및 게이트웨이를 수신합니다. DHCP에서 게이트웨이를 수신하지 못한 경우(예: 이 인터페이스를 네트워크에 연결하지 않은 경우) 게이트웨이는 기본적으로 데이터 인터페이스로 설정되며, 아무것도 구성할 필요가 없습니다. DHCP에서 게이트웨이를 수신한 경우 대신 고정 IP 주소로 이 인터페이스를 구성하고 게이트웨이를 데이터 인터페이스로 설정해야 합니다.
- 관리자 액세스용 관리 인터페이스 - 고정 IP 주소를 구성하려면 기본 게이트웨이도 데이터 인터페이스 대신 고유한 게이트웨이로 설정해야 합니다. DHCP를 사용하는 경우 DHCP에서 게이트웨이를 성공적으로 가져오면 어떤 것도 구성할 필요가 없습니다.

단계 **3** **Device**(디바이스) > **System Settings**(시스템 설정) > **Central Management**(중앙 관리)를 선택하고 **Proceed**(계속)을 눌러 management center/CDO 관리를 설정합니다.

단계 **4** **Management Center/CDO Details**(관리 센터/**CDO** 세부 정보)를 구성합니다.

그림 *50: Management Center/CDO* 세부 정보



a) **Do you know the Management Center/CDO hostname or IP address(**관리 센터**/CDO** 호스트 이름 또는 **IP** 주소를 알고 있습니까**)**에 대해 IP 주소 또는 호스트 이름을 사용하여 management center/CDO에 도달할 수 있으면 **Yes(**예**)**를, management center/CDO에 퍼블릭 IP 주소 또는 호스트 이름이 없거나 NAT 뒤에 있는 경우 **No(**아니요**)**를 클릭합니다.

하나 이상의 디바이스(management center/CDO 또는 threat defense)에는 두 디바이스 간 양방향 SSL 암호화 통신 채널을 설정하기 위한 연결 가능한 IP 주소가 있어야 합니다.

b) **Yes(**예**)**를 선택한 경우 **Management Center/CDO Hostname/IP Address(**관리 센터**/CDO** 호스트 이름**/IP** 주소**)**를 입력합니다.

c) **Management Center/CDO Registration Key(**관리 센터**/CDO** 등록 키**)**를 지정합니다.

threat defense 디바이스 등록 시에 management center/CDO에서 지정할 일회용 등록 키입니다. 이 등록 키는 37자를 초과해서는 안 됩니다. 영숫자(A~Z, a~z, 0~9)와 하이픈(-)을 사용할 수 있습니다. 이 ID는 management center/CDO에 등록하는 여러 디바이스에 사용할 수 있습니다.

d) **NAT ID**를 지정합니다.

이 ID는 management center/CDO에서 지정할 고유한 일회성 문자열을 지정합니다. 이 필드는 디바이스 중 하나의 IP 주소만 지정하는 경우 입력해야 합니다. 두 디바이스의 IP 주소를 모두 알고 있는 경우에도 NAT ID를 지정하는 것이 좋습니다. NAT ID는 37자를 초과할 수 없습니다. 영숫자(A~Z, a~z, 0~9)와 하이픈(-)을 사용할 수 있습니다. 이 ID는 management center/CDO에 등록하는 다른 디바이스에 사용할 수 없습니다. NAT ID는 연결이 올바른 디바이스에서 오는지 확인하기 위해 IP 주소와 함께 사용됩니다. IP 주소/NAT ID 인증 후에만 등록 키가 확인됩니다.

단계 **5** 연결성 설정을 구성합니다.

a) **FTD** 호스트 이름을 지정합니다.

Management Center/CDO Access Interface 액세스를 위해 데이터 인터페이스를 사용하는 경우 이 FQDN이 이 인터페이스에 사용됩니다.

b) **DNS** 서버 그룹을 지정합니다.

기존 그룹을 선택하거나 새로 생성합니다. 기본 DNS 그룹은 **CiscoUmbrellaDNSServerGroup**이며, 여기에는 OpenDNS 서버가 포함됩니다.

관리 센터**/CDO** 액세스 인터페이스에 대한 데이터 인터페이스를 선택하려는 경우 이 설정은 데이터 인터페이스 DNS 서버를 설정합니다. 설정 마법사를 사용하여 설정하는 관리 DNS 서버는 관리 트래픽에 사용됩니다. 데이터 DNS 서버는 DDNS(설정된 경우) 또는 이 인터페이스에 적용된 보안 정책에 사용됩니다. 관리 및 데이터 트래픽이 모두 외부 인터페이스를 통해 DNS 서버에 연결되므로 관리에 사용한 것과 동일한 DNS 서버 그룹을 선택할 수 있습니다.

management center/CDO에서 이 threat defense 디바이스에 할당하는 플랫폼 설정 정책에서 데이터 인터페이스 DNS 서버가 설정됩니다. management center/CDO에 threat defense 디바이스를 추가하면 로컬 설정이 유지되고 DNS 서버가 플랫폼 설정 정책에 추가되지 않습니다. 그러나 나중에 DNS 컨피그레이션을 포함하는 threat defense 디바이스에 플랫폼 설정 정책을 할당하면 해당 컨피그레이션이 로컬 설정을 덮어씁니다. management center/CDO와 threat defense 디바이스를 동기화하려면 이 설정과 일치하도록 DNS 플랫폼 설정을 적극적으로 구성하는 것이 좋습니다.

또한 로컬 DNS 서버는 초기 등록시 DNS 서버가 검색된 경우에만 management center/CDO에 의해 유지됩니다.

관리 센터**/CDO** 액세스 인터페이스관리 인터페이스를 선택하려는 경우 이 설정은 관리 DNS 서버를 구성합니다.

c) **Management Center/CDO Access Interface(**관리 센터**/CDO** 액세스 인터페이스**)**의 경우 구성된 인터페이스를 선택합니다.

threat defense 디바이스를 management center/CDO에 등록한 후 관리자 인터페이스를 관리 인터페이스 또는 다른 데이터 인터페이스로 변경할 수 있습니다.

단계 **6** (선택 사항) 데이터 인터페이스를 선택했는데 외부 인터페이스가 아닌 경우 기본 경로를 추가합니다.

인터페이스를 통과하는 기본 경로가 있는지 확인하라는 메시지가 표시됩니다. 외부를 선택한 경우 설정 마법사의 일부로 이 경로를 이미 구성한 것입니다. 다른 인터페이스를 선택한 경우 management center/CDO에 연결하기 전에 기본 경로를 수동으로 구성해야 합니다.정적 경로 구성에 대한 자세한 내용은 고정 경로 구성, 339 페이지 항목을 참조하십시오.

관리 인터페이스를 선택한 경우 이 화면에서 계속 진행하기 전에 게이트웨이를 고유한 게이트웨이로 구성해야 합니다. 관리 인터페이스 구성, 830 페이지 섹션을 참조하십시오.

단계 **7** (선택 사항) 데이터 인터페이스를 선택한 경우 **Add a Dynamic DNS (DDNS) method(**동적 **DNS(DDNS)** 메서드 추가**)**를 클릭합니다.

DDNS는 management center/CDO 의 IP 주소가 변경될 경우 threat defense 디바이스가 FQDN(Fully-Qualified Domain Name)에서 에 연결할 수 있도록 합니다. **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **DDNS Service(DDNS** 서비스**)**를 참조하여 DDNS를 구성합니다.

management center/CDO에 threat defense 디바이스를 추가하기 전에 DDNS를 구성할 경우 threat defense 디바이스가 HTTPS 연결을 위해 DDNS 서버 인증서를 검증할 수 있도록 Cisco Trusted Root CA 번들에서 threat defense 디바이스가 모든 주요 CA에 대한 인증서를 자동으로 추가합니다. Threat Defense는 DynDNS 원격 API 사양(https://help.dyn.com/remote-access-api/)을 사용하는 모든 DDNS 서버를 지원합니다.

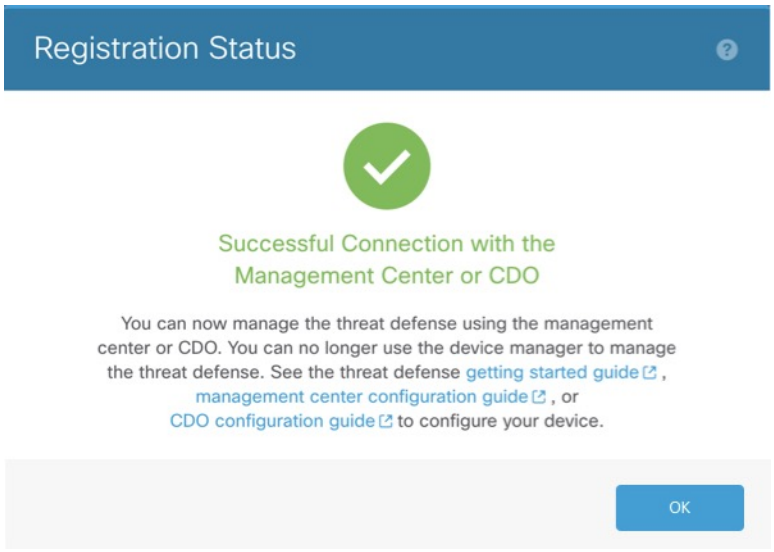
관리자 액세스용 관리 인터페이스를 사용할 때는 DDNS가 지원되지 않습니다.

단계 **8** **Connect(**연결**)**를 클릭합니다. 등록 상태**(Registration Status)** 대화 상자는 management center/CDO 전환에 대한 현재 상태를 보여줍니다. **Saving Management Center/CDO Registration Settings(**관리 센터**/CDO** 등록 설정 저장**)** 단계에서 management center/CDO로 이동하여 방화벽을 추가합니다.

management center/CDO에 대한 전환을 취소하려면 **Cancel Registration(**등록 취소**)**을 클릭합니다. 아니면 **Saving Management Center/CDO Registration Settings(**관리 센터**/CDO** 등록 설정 저장**)** 단계까지 device manager 브라우저를 닫지 마십시오. 이렇게 하면 프로세스가 일시 중지되며, device manager에 다시 연결할 때만 재개됩니다.

Save Management Center/CDO Registration Settings(관리 센터**/CDO** 등록 설정 저장**)** 단계를 수행한 후 device manager에 연결된 상태로 유지되는 경우, 마지막으로 **Successful Connection with Management Center or CDO(**관리 센터 또는 **CDO**와의 연결 성공**)** 대화 상자가 표시된 뒤 device manager으로부터 연결이 해제됩니다.

그림 51: 연결 성공



Management Center에서 또는 CDO에서 Device Manager로 전환

대신 device manager를 사용하도록 온프레미스 또는 클라우드 제공management center에서 현재 관리 중인 threat defense 디바이스를 구성할 수 있습니다.

소프트웨어를 다시 설치하지 않고 management center에서 device manager로 전환할 수 있습니다. management center에서 device manager로 전환하기 전에 device manager에서 모든 구성 요건을 충족하는지 확인하십시오. device manager에서 management center로 전환하려면 Device Manager에서 Management Center 또는 CDO로 전환, 844 페이지의 내용을 참조하십시오.

⚠

주의 device manager 전환 시 디바이스 구성이 지워지며 시스템이 기본 구성으로 돌아갑니다. 하지만 관리 IP 주소 및 호스트 이름은 유지됩니다.

프로시저

단계 1 management center의 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** 페이지에서 방화벽을 삭제합니다.

단계 2 SSH 또는 콘솔 포트를 사용하여 threat defense CLI에 연결합니다. SSH의 경우 관리 **IP** 주소에 대한 연결을 열고, 관리자 사용자 이름(또는 관리자 권한이 있는 다른 사용자)을 사용하여 threat defense CLI에 로그인합니다.

콘솔 포트는 기본적으로 FXOS CLI를 사용합니다. **connect ftd** 명령을 사용하여 threat defense CLI에 연결합니다. SSH 세션은 threat defense CLI에 직접 연결됩니다.

관리 IP 주소에 연결할 수 없는 경우에는 다음 작업을 수행합니다.

- 관리 물리적 포트가 작동하는 네트워크에 유선 연결되어 있는지 확인합니다.
- 관리 네트워크에 대해 관리 IP 주소 및 게이트웨이가 구성되어 있는지 확인합니다. **configure network ipv4/ipv6 manual** 명령을 사용하십시오.

단계 **3** 현재 원격 관리 모드 상태인지 확인합니다.

show managers

예제:

```
> show managers
Type                        : Manager
Host                        : 10.89.5.35
Display name                : 10.89.5.35
Identifier                  : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration                : Completed
```

단계 **4** 원격 관리자를 삭제하고 관리자 없음 모드를 설정합니다.

configure manager delete *uuid*

원격 관리에서 로컬 관리로 직접 이동할 수는 없습니다.둘 이상의 관리자가 정의된 경우 식별자(UUID라고도 함, **show managers** 명령 참조)를 지정해야 합니다. 각 관리자 항목을 개별적으로 삭제합니다.

예제:

```
> configure manager delete
Deleting task list
Manager successfully deleted.

>
> show managers
No managers configured.
```

단계 **5** 로컬 관리자를 구성합니다.

configure manager local

이제 웹 브라우저를 사용하여 **https://***management-IP-address*에서 로컬 관리자를 열 수 있습니다.

예제:

```
> configure manager local
Deleting task list

> show managers
Managed locally.
```

TLS / SSL 암호 설정 설정

SSL 암호 설정은 디바이스에 대한 TLS/SSL 연결에 허용되는 TLS 버전 및 암호화 암호 그룹을 제어합니다. 특히 이러한 설정은 원격 액세스 VPN 연결을 설정할 때 클라이언트가 사용할 수 있는 암호를 제어합니다.

일반적으로 설정하는 암호 그룹에는 사용 가능한 암호화 암호 그룹이 두 개 이상 있어야 합니다. 시스템은 클라이언트 및 threat defense 디바이스가 모두 지원하는 가장 높은 TLS 버전을 확인한 다음 TLS 버전과 호환되는 두 가지를 모두 지원하는 암호 그룹을 선택합니다. 시스템은 사용자가 허용하는 암호 중에서 가장 안전한 연결을 보장하기 위해 두 엔드포인트 모두에서 지원하는 가장 강력한 TLS 버전 및 암호 그룹을 선택합니다.

시작하기 전에

기본적으로 시스템은 DefaultSSLCipher 개체를 사용하여 허용되는 암호 그룹을 정의합니다. 이 개체에 포함된 암호는 내보내기 제어 기능에 대해 스마트 라이선스 어카운트가 활성화되었는지 여부에 따라 달라집니다. 이 기본값은 가능한 많은 클라이언트가 연결을 완료할 수 있도록 낮은 보안 레벨을 설정합니다. 기본 Diffie-Hellman 그룹도 있습니다. 기본값이 요구 사항에 맞지 않는 경우에만 이러한 설정을 지정해야 합니다.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음, **System Settings(**시스템 설정**)** > **SSL Settings(SSL** 설정**)** 링크를 클릭합니다.

단계 **2** 다음 옵션을 구성합니다.

- **Ciphers(**암호**)** - 허용되는 TLS 버전 및 암호화 알고리즘을 정의하는 SSL 암호 개체를 선택합니다. DefaultSSLCipher 개체는 낮은 보안 레벨을 설정합니다. 더 높은 요구 사항을 구현하려면 이 개체를 CiscoRecommendedCipher 또는 맞춤형 암호 개체로 교체하십시오. 허용하려는 모든 TLS 버전과 암호만 포함하는 단일 개체를 생성하는 것이 이상적입니다.

  지금 개체를 생성해야 하는 경우 목록 하단에서 **Create New Cipher(**새 암호 생성**)**를 클릭합니다.

- **Ephemeral Diffie-Hellman Group(**일회성 **Diffie-Hellman** 그룹**)** - 일회성 암호화 알고리즘에 사용할 DH 그룹입니다. DH 그룹에 대한 설명은 사용할 Diffie-Hellman 모듈러스 그룹 결정, 682 페이지의 내용을 참조하십시오. 기본값은 14입니다.

- **Elliptical Curve DH Group(**타원 곡선 **DH** 그룹**)** - 타원 곡선 암호화 알고리즘에 사용할 DH 그룹입니다. 기본값은 19입니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

TLS / SSL 암호 개체 설정

SSL 암호 개체는 threat defense 디바이스에 대한 SSL 연결을 설정할 때 사용할 수 있는 보안 레벨, TLS/DTLS 프로토콜 버전 및 암호화 알고리즘의 조합을 정의합니다. **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **SSL Settings(SSL** 설정**)**에서 이러한 개체를 사용하여 상자에 SSL 연결을 수행하는 사용자에 대한 보안 요구 사항을 정의합니다.

선택할 수 있는 TLS 버전 및 암호는 스마트 라이선스 어카운트에 의해 제어됩니다. 내보내기 규정 준수 요건을 충족하는 경우 옵션의 조합을 선택할 수 있습니다. 라이선스가 내보내기를 준수하지 않는 경우 가장 낮은 보안 옵션인 TLSv1.0 및 DES-CDC-SHA로 제한됩니다. 평가 모드는 비호환 모드로 간주되므로 시스템 라이선스를 받을 때까지 옵션이 제한됩니다.

시스템에는 사전 정의된 개체가 여러 개 포함되어 있습니다. 사전 정의된 개체가 보안 요건에 맞지 않는 경우에만 새 개체를 생성해야 합니다. 개체는 다음과 같습니다.

- DefaultSSLCipher - 낮은 보안 레벨 그룹입니다. 가능한 많은 클라이언트가 시스템에 대한 연결을 완료할 수 있도록 SSL 설정에서 사용되는 기본값입니다. 여기에는 시스템에서 지원하는 모든 프로토콜 버전 및 암호가 포함됩니다.
- CiscoRecommendedCipher - 보안 레벨이 높은 그룹으로, 가장 안전한 암호 및 TLS 버전만 포함됩니다. 이 그룹은 가장 높은 보안을 제공하지만 클라이언트가 일치하는 암호를 사용할 수 있도록 해야 합니다. 암호 불일치 문제로 인해 일부 클라이언트가 연결을 완료할 수 없을 가능성이 더 높습니다.

프로시저

단계 **1** 콘텐츠 테이블에서 **Objects(**개체**)**를 선택하고 **SSL Ciphers(SSL** 암호**)**를 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 개체를 생성하려면 **+** 버튼을 클릭합니다.
- 개체를 수정하려면 개체의 수정 아이콘()을 클릭하십시오.

참조되지 않는 개체를 삭제하려면 해당 개체의 휴지통 아이콘()을 클릭합니다.

단계 **3** 개체의 **Name(**이름**)** 및 설명(선택 사항)을 입력합니다.

단계 **4** 다음 옵션을 구성합니다.

- **Security Level(**보안 레벨**)** - 개체의 상대적 보안 레벨입니다. 보안 레벨을 선택한 후 프로토콜 버전 또는 암호 그룹 목록을 수정하면 개체에서 제공하는 실제 보안 레벨이 보안 레벨과 일치하지 않을 수 있습니다. 다음 중 하나를 선택합니다.
  - **All(**모두**)** - 낮음부터 높음까지 개체의 모든 TLS 레벨 및 암호 그룹을 포함합니다.
  - **Low(**낮음**)** - 모든 TLS 버전 및 암호를 포함하므로 사용자가 최소 보안 암호로 연결을 완료할 수 있습니다. 내보내기 미준수 라이선스의 경우 TLSv1.0 및 DES-CBC-SHA가 포함됩니다.

- **Medium(**중간**)** - 모든 TLS 버전을 포함하지만 상대적으로 안전하지 않은 일부 암호를 제거합니다. 이 옵션과 Low(낮음)/All(모두) 옵션 사이에는 최소한의 차이만 있습니다. 내보내기 미준수 라이선스에 이 옵션을 사용할 수 없습니다.
- **High(**높음**)** - 최신 DTLS 및 TLS 버전과 이러한 버전에서 작동하는 암호만 허용합니다. 이 옵션은 현재 사용 가능한 가장 안전한 암호로 연결을 제한합니다. 내보내기 미준수 라이선스에 이 옵션을 사용할 수 없습니다.
- **Custom(**맞춤형**)** - TLS 버전과 암호를 개별적으로 선택하려면 이 옵션을 선택합니다. 선택하는 옵션에 따라 높거나 낮은 보안 암호화 설정을 정의할지 여부가 결정됩니다. 맞춤형 개체에 대한 기본값은 없지만 맞춤형을 선택하기 전에 다른 레벨을 선택한 경우 편의상 이전에 표시된 옵션이 선택된 상태로 유지됩니다.

- **Protocol Versions(**프로토콜 버전**)** - threat defense 디바이스에 대한 TLS/SSL 연결을 설정할 때 클라이언트에서 사용할 수 있는 TLS/DTLS 버전입니다. 맞춤형 개체의 경우 지원하고자 하는 버전을 선택합니다. 다른 보안 레벨의 경우에는 목록을 수정하지 않는 것이 좋지만 원하는 대로 버전을 추가 또는 제거할 수 있습니다.
- **Applicable Cipher Suites(**적용 가능한 암호 그룹**)** - 클라이언트가 사용할 수 있는 암호화 알고리즘입니다. **+**를 클릭하여 새 그룹을 추가하고, 그룹에서 **x**를 클릭하면 그룹을 제거합니다.

  선택한 프로토콜 버전은 이 목록에서 사용 가능한 그룹을 제어합니다. 프로토콜 버전을 변경하면 선택한 버전에서 더 이상 작동하지 않는 선택한 그룹에 플래그가 지정됩니다. 이러한 그룹을 제거하거나 필요한 프로토콜 버전을 다시 추가해야 합니다.

단계 **5** **OK(**확인**)**를 클릭합니다.

27 장

시스템 관리

다음 주제에서는 시스템 데이터베이스 업데이트, 시스템 백업 및 복원 등의 시스템 관리 작업을 수행하는 방법을 설명합니다.

소프트웨어 업데이트 설치

시스템 데이터베이스 및 시스템 소프트웨어에 업데이트를 설치할 수 있습니다. 다음 주제에서는 이러한 업데이트를 설치하는 방법을 설명합니다.

시스템 데이터베이스 및 피드 업데이트

시스템에서는 여러 데이터베이스 및 보안 인텔리전스 피드를 사용하여 고급 서비스를 제공합니다. Cisco에서는 보안 정책에서 최신 정보를 사용할 수 있도록 이러한 데이터베이스 및 피드에 대한 업데이트를 제공합니다.

시스템 데이터베이스 및 피드 업데이트 개요

Threat Defense는 다음 데이터베이스 및 피드를 사용하여 고급 서비스를 제공합니다.

침입 규칙

새로운 취약성이 알려지면 Cisco Talos Intelligence Group(Talos)에서 사용자가 가져올 수 있는 침입 규칙 업데이트를 릴리스합니다. 이러한 업데이트는 침입 규칙, 전처리기 규칙 및 규칙을 사용하는 정책에 영향을 줍니다.

침입 규칙은 업데이트된 새로운 침입 규칙과 전처리기 규칙, 기존 규칙의 수정된 상태, 수정된 기본 침입 정책 설정을 제공합니다. 규칙 업데이트는 또한 규칙을 삭제하고, 새로운 규칙 카테고리와 기본 변수를 제공하며, 기본 변수 값을 변경할 수 있습니다.

침입 규칙 업데이트를 통해 수행된 변경 사항을 적용하려면 컨피그레이션을 재구축해야 합니다.

침입 규칙 업데이트는 규모가 클 수 있으므로 네트워크 이용률이 낮은 시간 동안 규칙을 가져오십시오. 느린 네트워크에서는 업데이트 시도가 실패할 수 있는데, 이 경우 재시도해야 합니다.

GeoDB(Geolocation database)

Cisco Geolocation Database(GeoDB)는 라우팅 가능 IP 주소와 연결된 지리적 데이터(국가, 도시, 좌표 등)의 데이터베이스입니다.

GeoDB 업데이트는 물리적 위치의 업데이트된 정보를 제공하여 시스템이 라우팅 가능한 탐지된 IP 주소에 연결할 수 있습니다. 지리위치 데이터를 액세스 제어 규칙의 조건으로 사용할 수 있습니다.

GeoDB 업데이트에 필요한 시간은 어플라이언스에 따라 다릅니다. 설치하는 데 일반적으로 30~40분이 소요됩니다. GeoDB 업데이트를 수행해도 지리위치 정보의 지속적인 수집을 비롯한 기타 시스템 기능이 중단되지는 않지만, 업데이트를 완료하는 동안 시스템 리소스가 사용됩니다. 업데이트를 예약하는 경우 이를 고려하십시오.

VDB(Vulnerability Database)

Cisco VDB(Vulnerability Database)는 호스트가 영향을 받기 쉬운 알려진 취약점의 데이터베이스인 동시에 운영 체제, 클라이언트 및 애플리케이션의 지문이기도 합니다. 방화벽 시스템은 지문과 취약점의 상관관계를 지정하므로, 특정 호스트가 네트워크 보안 침해 위험을 증가시키는지를 쉽게 확인할 수 있습니다. Cisco Talos Intelligence Group(Talos)는 VDB에 주기적인 업데이트를 생성합니다.

취약성 매핑 업데이트에 걸리는 시간은 네트워크 맵에 있는 호스트의 수에 따라 달라집니다. 시스템 다운타임의 영향을 최소화하려면 시스템 사용량이 적은 시간에 업데이트를 예약할 수 있습니다. 네트워크에 있는 호스트의 수를 1000으로 나누면 업데이트를 수행하는 데 걸리는 대략적인 시간(분)이 나옵니다.

VDB를 업데이트한 후에는 컨피그레이션을 재구축해야 업데이트된 애플리케이션 탐지기 및 운영 체제 지문을 적용할 수 있습니다.

Cisco Talos Intelligence Group(Talos) 보안 인텔리전스 피드

Talos 에서는 보안 인텔리전스 정책에 사용하기 위해 정기적으로 업데이트되는 인텔리전스 피드에 액세스할 수 있도록 지원합니다. 악성코드, 스팸, 봇넷, 피싱과 같은 보안 위협을 나타내는 사이트는 맞춤형 컨피그레이션을 업데이트하고 구축하는 속도보다 빠르게 나타났다 사라질 수 있습니다. 이러한 피드에는 알려진 위협에 대한 주소 및 URL이 포함됩니다. 피드가 업데이트되면 재구축하지 않아도 됩니다. 이후의 연결 평가에는 새 목록이 사용됩니다.

URL 카테고리/평판 데이터베이스

시스템은 Cisco CSI(Collective Security Intelligence)에서 URL 카테고리 및 평판 데이터베이스를 가져옵니다. 카테고리 및 평판을 기준으로 필터링하는 URL 필터링 액세스 제어 규칙을 구성하는 경우에는 요청한 URL과 데이터베이스를 대조하여 일치 여부를 확인합니다. **System Settings(**시스템 설정**)** > **URL Filtering Preferences(URL** 필터링 환경 설정**)**에서 데이터베이스 업데이트 및

일부 기타 URL 필터링 환경 설정을 구성할 수 있습니다. URL 카테고리/평판 데이터베이스 업데이트는 다른 시스템 데이터베이스용 업데이트를 관리하는 것과 같은 방식으로 관리할 수 없습니다.

시스템 데이터베이스 업데이트

편의상 시스템 데이터베이스 업데이트를 수동으로 검색하여 적용할 수 있습니다. Cisco 지원 사이트에서 업데이트를 검색합니다. 따라서 시스템 관리 주소에서 인터넷으로 이동하는 경로가 있어야 합니다.

또는 인터넷에서 직접 업데이트 패키지를 검색한 다음, 워크스테이션에서 업로드할 수 있습니다. 이 방법은 주로 에어 갭(air-gapped) 네트워크를 위한 것으로, 이 네트워크 환경에는 Cisco에서 업데이트를 검색하기 위한 인터넷 경로가 없습니다. 시스템 소프트웨어 업그레이드를 다운로드할 수 있는 동일한 폴더에서 software.cisco.com의 업데이트를 다운로드합니다.

참고 2022년 5월에 GeoDB를 두 개의 패키지로 분할했습니다. IP 주소를 국가/대륙에 매핑하는 국가 코드 패키지와 라우팅 가능한 IP 주소와 관련된 추가 상황 데이터를 포함하는 IP 패키지입니다. device manager은 IP 패키지의 정보를 사용하거나 사용한 적이 없습니다. 이 분할은 로컬로 관리되는 threat defense 구축에서 상당한 디스크 공간을 절약합니다. Cisco에서 직접 GeoDB를 가져오는 경우 이전 통합형 패키지와 동일한 파일 이름을 가진 국가 코드 패키지(Cisco_GEODB_Update-*date-build*)를 가져와야 합니다.

데이터베이스 업데이트를 검색하고 적용하는 정기적인 일정을 설정할 수도 있습니다. 이러한 업데이트는 크기가 클 수 있으므로 네트워크 활동이 적은 시간에 예약합니다.

참고 데이터베이스 업데이트가 진행 중인 동안에는 사용자 인터페이스가 작업에 응답하는 속도가 느려질 수 있습니다.

시작하기 전에

보류 중인 변경 사항에 영향을 줄 가능성을 방지하려면 이러한 데이터베이스를 수동으로 업데이트하기 전에 컨피그레이션을 디바이스에 구축합니다.

VDB 및 URL 카테고리 업데이트에서 애플리케이션 또는 카테고리를 제거할 수 있다는 점에 유의하십시오. 변경 사항을 구축하기 전에 이러한 사용되지 않는 항목을 사용하는 액세스 제어 또는 SSL 암호 해독 규칙을 업데이트해야 합니다.

프로시저

단계 **1** 디바이스를 선택한 다음, Updates(업데이트) 요약에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

그러면 업데이트 페이지가 열립니다. 페이지의 정보에는 각 데이터베이스의 현재 버전과 각 데이터베이스가 업데이트된 마지막 날짜 및 시간이 표시됩니다.

단계 **2** 수동으로 데이터베이스를 업데이트하려면 해당 데이터베이스의 섹션에서 다음 옵션 중 하나를 클릭합니다.

- **Update from Cloud(**클라우드에서 업데이트**)** — device manager이 Cisco Cloud에서 업데이트 패키지를 검색하도록 합니다. 이 방법은 가장 쉽고 신뢰할 수 있는 방법이지만, 이를 사용하려면 인터넷에 연결할 경로가 있어야 합니다.
- **(**아래쪽 화살표**)** > 옵션 — 워크스테이션 또는 워크스테이션에 연결된 드라이브에서 업데이트 패키지를 선택합니다. 이 옵션은 다음 중 하나입니다.
  - **Select File(**파일 선택**)** — VDB 또는 지리위치 패키지를 선택합니다.
  - **Update to Newer Version(**새 버전으로 업데이트**)** — 현재 설치된 패키지보다 새로워진 침입 규칙 패키지를 선택합니다.
  - **Downgrade to Older Version(**이전 버전으로 다운그레이드**)** — 현재 설치된 패키지보다 이전의 침입 규칙 패키지를 선택합니다.

규칙 및 VDB 업데이트를 수행하려면 컨피그레이션 구축 시 이를 활성화해야 합니다. 클라우드에서 업데이트할 때 지금 구축할 것인지 묻는 메시지가 표시되면 **Yes(**예**)**를 클릭합니다. **No(**아니요**)**를 클릭하는 경우 가장 빠른 시일 내에 구축 작업을 시작해야 합니다.

자체 파일을 업로드할 경우에는 항상 수동으로 변경 사항을 구축해야 합니다.

참고 침입 규칙 패키지를 수동으로 업로드할 때는 Snort 버전에 적합한 패키지 유형(Snort 2의 경우 SRU, Snort 3의 경우 LSP)을 업로드해야 합니다. 비 액티브 Snort 버전용 패키지를 업로드할 수 있지만 버전을 전환하지 않으면 활성화되지 않습니다. Snort 버전 전환에 대한 자세한 내용은 Snort 2와 Snort 3 간 전환, 560 페이지를 참조하십시오.

단계 **3** (선택 사항) 정기적인 데이터베이스 업데이트 일정을 설정하려면 다음을 수행합니다.

a) 원하는 데이터베이스의 섹션에서 **Configure(**구성**)** 링크를 클릭합니다. 일정이 이미 있는 경우 **Edit(**편집**)**을 클릭합니다.

데이터베이스의 업데이트 일정은 별개이므로 별도로 일정을 정의해야 합니다.

b) 업데이트 시작 시간을 설정합니다.

- 업데이트 빈도(매일, 매주, 매월)
- 매주 또는 매월의 경우 업데이트를 수행할 요일이나 날짜
- 업데이트를 시작할 시간 지정하는 시간은 일광 절약 시간에 맞게 조정되므로 해당 지역에서 시간을 조정할 때마다 1시간 앞당겨지거나 늦춰집니다. 연중 내내 정확한 시간을 유지하려면 시간 변경에서 예약을 수정하십시오.

c) 규칙 또는 VDB 업데이트의 경우, 시스템에서 데이터베이스 업데이트 시 항상 컨피그레이션을 구축하도록 하려면 **Automatically Deploy the Update(**자동으로 업데이트 구축**)** 체크 박스를 선택합니다.

업데이트는 구축될 때까지 적용되지 않습니다. 자동 구축 시에는 아직 구축되지 않은 다른 컨피그레이션 변경 사항도 구축됩니다.

d) **Save(**저장**)**를 클릭합니다.

참고 반복 예약을 제거하려면 **Edit(**수정**)** 링크를 클릭하여 예약 대화 상자를 연 다음 **Remove(**제거**)** 버튼을 클릭합니다.

Cisco 보안 인텔리전스 피드 업데이트

Cisco Talos Intelligence Group(Talos) 에서는 정기적으로 업데이트되는 보안 인텔리전스 피드에 액세스할 수 있도록 지원합니다. 악성코드, 스팸, 봇넷, 피싱과 같은 보안 위협을 나타내는 사이트는 맞춤형 컨피그레이션을 업데이트하고 구축하는 속도보다 빠르게 나타났다 사라질 수 있습니다. 피드가 업데이트되면 재구축하지 않아도 됩니다. 이후의 연결 평가에는 새 목록이 사용됩니다.

시스템이 인터넷에서 피드를 업데이트할 때 엄격한 제어를 원할 경우, 해당 피드에 대한 자동 업데이트를 비활성화할 수 있습니다. 그러나 자동 업데이트는 가장 연관성 있는 최신 데이터를 지원합니다.

프로시저

단계 **1** 디바이스를 선택한 다음 Updates(업데이트) 요약에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

그러면 업데이트 페이지가 열립니다. 페이지의 정보에는 **Security Intelligence Feeds(**보안 인텔리전스 피드**)**의 현재 버전과 피드가 업데이트된 마지막 날짜 및 시간이 표시됩니다.

단계 **2** 피드를 수동으로 업데이트하려면 **Security Intelligence Feeds(**보안 인텔리전스 피드**)** 그룹에서 **Update Now(**지금 업데이트**)**를 클릭합니다.

고가용성 그룹의 유닛 하나에서 피드를 수동으로 업데이트하는 경우에는 일관성을 유지하기 위해 다른 유닛에서도 피드를 수동으로 업데이트해야 합니다.

단계 **3** (선택 사항). 정기적인 업데이트 빈도를 구성하려면 다음을 수행합니다.

a) Cisco Feeds(Cisco 피드)의 섹션에서 **Configure(**구성**)** 링크를 클릭합니다. 일정이 이미 있는 경우 **Edit(**편집**)**을 클릭합니다.

b) 원하는 빈도를 선택합니다.

기본값은 **Hourly(**매시간**)**입니다. **Daily(**매일**)** 업데이트(시간 지정) 또는 **Weekly(**매주**)** 업데이트(요일 및 시간 선택)로 설정할 수도 있습니다. 지정하는 시간은 일광 절약 시간에 맞게 조정되므로 해당 지역에서 시간을 조정할 때마다 1시간 앞당겨지거나 늦춰집니다. 연중 내내 정확한 시간을 유지하려면 시간 변경에서 예약을 수정하십시오.

자동 업데이트되지 않도록 하려면 **Delete(**삭제**)**를 클릭합니다.

c) **OK(**확인**)**를 클릭합니다.

Threat Defense 소프트웨어 업그레이드

threat defense 소프트웨어 업그레이드는 사용 가능 시 설치할 수 있습니다.

업그레이드는 주 버전(A.x), 유지 보수 릴리스(Axy) 또는 패치(Axyz)일 수 있습니다. 또한 긴급한 특정 문제를 해결하는 사소한 업데이트인 핫픽스도 제공할 수 있습니다. 핫픽스는 시스템 재부팅이 필요하지 않을 수도 있지만 다른 업그레이드 시에는 재부팅이 필요합니다. 재부팅이 필요하면 설치 후에 시스템이 자동으로 재부팅됩니다. 업데이트를 설치할 때는 트래픽이 중단될 수 있으므로 시스템 사용량이 적을 때 설치를 수행하십시오.

섀시에서 FXOS 소프트웨어도 업그레이드해야 하는 경우 이 절차를 수행하기 전에 FXOS 업그레이드를 설치합니다.

고가용성 그룹의 유닛을 업그레이드하는 경우에는 스탠바이 디바이스를 업그레이드하고 모드를 전환하여 액티브/스탠바이 유닛을 교체한 다음 새 스탠바이 디바이스에 업그레이드를 설치합니다. 자세한 내용은 HA 디바이스에서 소프트웨어 업그레이드 설치, 242 페이지를 참조하십시오.

이 절차를 통해 디바이스를 재이미징하거나 ASA 소프트웨어에서 threat defense 소프트웨어로 마이그레이션할 수는 없습니다.

참고 업데이트를 설치하기 전에 보류 중인 모든 변경 사항을 구축해야 합니다. 또한 백업을 실행하고 백업 복사본을 다운로드해야 합니다. 핫픽스를 제외한 모든 업그레이드는 시스템에 보관된 모든 백업 파일을 삭제합니다.

시작하기 전에

작업 목록을 확인하고 실행 중인 작업이 없는지 확인하십시오. 데이터베이스 업데이트 등 모든 작업이 완료될 때까지 대기했다가 업그레이드를 설치하십시오. 예약된 작업도 모두 확인하십시오. 예약 작업이 업그레이드 작업과 중복되지 않게 하십시오.

업데이트를 수행하기 전에 더 이상 사용되지 않는 애플리케이션이 애플리케이션 필터, 액세스 규칙 또는 SSL 암호 해독 규칙에 없는지 확인하십시오. 이러한 애플리케이션의 이름 뒤에는 "(사용되지 않음)"이라고 적혀 있습니다. 이러한 개체에는 더 이상 사용되지 않는 애플리케이션을 추가할 수 없으며, 후속 VDB 업데이트를 수행하면 이전에 유효했던 애플리케이션이 더 이상 사용되지 않게 될 수 있습니다. 이러한 상황이 발생하면 업그레이드에 실패하고 디바이스는 사용할 수 없는 상태가 됩니다.

Cisco 지원 및 다운로드 사이트에서 https://www.cisco.com/go/ftd-software 업그레이드 파일을 다운로드합니다.

- 제품군 또는 시리즈의 모든 모델에 동일한 업그레이드 패키지를 사용하십시오. 올바른 버전을 찾으려면 모델을 선택하거나 검색한 다음 해당 버전의 소프트웨어 다운로드 페이지로 이동합니다. 파일 유형이 REL.tar인 적절한 업그레이드 파일을 다운로드해야 합니다. 시스템 소프트웨어 패키지 또는 부트 이미지를 다운로드하지 마십시오.
- 업그레이드 파일의 이름을 바꾸지 마십시오. 이름이 바뀐 파일은 유효하지 않은 것으로 간주됩니다.

- 다운그레이드하거나 패치를 제거할 수는 없습니다.
- 업그레이드에 필요한 베이스라인 이미지를 실행 중인지 확인합니다. 호환성 정보는 *Cisco Secure Firewall* 호환성 가이드 http://www.cisco.com/c/en/us/td/docs/security/firepower/compatibility/firepower-compatibility.html을 참조하십시오.
- 새 버전의 릴리스 노트를 확인합니다. 릴리스 노트는 http://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-release-notes-list.html에서 확인할 수 있습니다.

프로시저

단계 **1** **Device(**디바이스**)**를 선택한 다음 업데이트 요약에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

시스템 업그레이드 섹션에는 현재 실행 중인 소프트웨어 버전과 이미 업로드한 업데이트가 표시됩니다.

단계 **2** 업그레이드 파일을 업로드합니다.

- 업그레이드 파일을 아직 업로드하지 않은 경우 **Browse(**찾아보기**)**를 클릭하고 파일을 선택합니다. 업로드가 완료되면 **Run Upgrade Immediately on Upload(**업로드 즉시 업그레이드 실행**)** 옵션을 선택하여 설치를 시작할 수 있습니다.
- 업로드한 파일이 이미 있지만 다른 파일을 업로드하려는 경우에는 **Upload Another File(**다른 파일 업로드**)** 링크를 클릭합니다. 파일은 하나만 업로드할 수 있습니다. 새 파일을 업로드하면 이전 파일이 교체됩니다.
- 파일을 제거하려면 삭제 아이콘( )을 클릭합니다.

단계 **3** (선택 사항). 업그레이드 준비도 확인을 실행합니다.

수동으로 확인을 실행하지 않는 경우 설치를 시작할 때 자동으로 실행됩니다. 확인에 실패하면 업그레이드가 취소됩니다. 자세한 내용은 업그레이드 준비도 확인 실행, 862 페이지를 참고하십시오.

단계 **4** 설치 프로세스를 시작합니다.

System Upgrade(시스템 업그레이드) 섹션에는 최신 threat defense 버전 및 해당하는 경우 FXOS 버전과 FXOS 호환성에 대한 정보 링크가 표시됩니다. threat defense 업그레이드를 설치하기 전에 적절한 FXOS 버전이 이미 설치되어 있는지 확인하십시오. 이 페이지에서는 FXOS 업그레이드를 설치할 수 없습니다. 섀시 모델에서 소프트웨어를 업그레이드하는 방법에 대한 자세한 내용은 FXOS 설명서를 참조하십시오.

설치 버튼 옆의 정보는 디바이스가 설치 중에 재부팅되는지 여부를 나타냅니다. 디바이스가 재부팅되면 시스템에서 자동으로 로그아웃됩니다. 설치에는 30분 이상 소요될 수 있습니다.

a) **Upgrade Now(**지금 업그레이드**)**를 클릭하여 설치 프로세스를 시작합니다.

작업을 확인하라는 메시지가 나타납니다.

b) (선택 사항). Confirmation System Upgrade(시스템 업그레이드 확인) 대화 상자에서 **Automatically cancel on upgrade failure and roll back to the previous version(**업그레이드 실패 시 자동으로 취소하고 이전 버전으로 롤백**)**을 선택합니다. 이 옵션은 주요 및 유지 보수 릴리스 업그레이드에만 사용할 수 있습니다. 이 범주는 기본적으로 활성화되어 있습니다.

이 옵션을 선택하고 업그레이드에 실패하면 업그레이드를 시작할 때 디바이스의 이전 상태로 돌아갑니다.

이 옵션을 선택하지 않으면 설치 프로세스가 실패할 경우 설치 프로세스를 재시작할 수 있습니다. 여전히 수동으로 이전 릴리스로 되돌릴 수 있는 옵션이 있으므로 이 대화 상자의 설정에 따라 되돌리기가 자동으로 수행되는지 여부가 결정됩니다.

c) **Continue(**계속**)**를 클릭하여 설치 작업을 시작합니다.

자동으로 로그오프되고 상태 페이지로 이동되며, 여기서 설치 진행 상황을 확인할 수 있습니다. 이 페이지에는 설치를 취소하는 옵션이 포함되어 있습니다. 재부팅이 필요한 경우 재부팅 중에 페이지에 액세스할 수 없게 됩니다. 그러나 페이지를 다시 로드하지 않을 경우 페이지가 계속 작동하여 결국 로그인 페이지로 자동 재로드됩니다.

설치에 실패하면 상태 페이지는 설치를 다시 시도하거나 실패한 작업을 취소하여 이전의 주 버전으로 되돌리는 옵션을 제공합니다.

단계 **5** (선택 사항). 시스템 데이터베이스를 업데이트합니다.

지리위치, 규칙 및 VDB(Vulnerability Database)에 대해 자동 업데이트 작업을 구성하지 않으면 지금 이러한 항목을 업데이트하는 것이 좋습니다.

업그레이드 준비도 확인 실행

시스템은 업그레이드를 설치하기 전에 준비도 확인을 실행하여 시스템에 대해 업그레이드가 유효한지 확인하고, 업그레이드에 방해가 되는 다른 항목을 확인합니다. 준비도 확인에서 실패하면 설치를 다시 시도하기 전에 문제를 해결해야 합니다. 확인에 실패하면 다음에 설치를 시도할 때 실패 메시지가 표시되며, 원하는 경우 강제 설치 옵션이 제공됩니다.

업그레이드를 시작하기 전에 이 절차에서 설명한 대로 준비도 확인을 수동으로 실행할 수도 있습니다.

시작하기 전에

확인할 업그레이드 패키지를 업로드합니다.

프로시저

단계 **1** **Device(**디바이스**)**를 선택한 다음 업데이트 요약에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

시스템 업그레이드 섹션에는 현재 실행 중인 소프트웨어 버전과 이미 업로드한 업데이트가 표시됩니다.

단계 **2** **Readiness Check(**준비도 확인**)** 섹션을 참조하십시오.

- 업그레이드 확인을 아직 수행하지 않은 경우, **Run Upgrade Readiness Check(**업그레이드 준비도 확인 실행**)** 링크를 클릭합니다. 이 영역에 확인 진행 상황이 표시됩니다. 프로세스를 완료하는 데 약 20초가 소요됩니다.
- 업그레이드 확인이 이미 실행된 경우, 이 섹션에 성공 또는 실패 여부가 표시됩니다. 확인이 실패할 경우, **See Details(**세부 사항 보기**)**를 클릭하면 준비도 확인에 대한 추가 정보가 표시됩니다. 문제를 해결한 후 다시 확인을 실행합니다.

단계 **3** 준비도 확인이 실패하는 경우, 업그레이드를 설치하기 전에 문제를 해결해야 합니다. 세부 정보에는 표시된 문제를 해결하는 방법에 대한 도움말이 포함되어 있습니다. 실패한 스크립트의 경우, **Show Recovery Message(**복구 메시지 표시**)**를 클릭하여 정보를 확인합니다.

다음은 몇 가지 일반적인 문제입니다.

- FXOS 버전 비호환 - FXOS 업그레이드를 별도로 설치하는 시스템(예: Firepower 4100/9300)에서 업그레이드 패키지에 현재 실행 중인 threat defense 소프트웨어 버전과 다른 최소 FXOS 버전이 필요할 수 있습니다. 이 경우, threat defense 소프트웨어를 업그레이드하려면 먼저 FXOS를 업그레이드해야 합니다.
- 지원되지 않는 디바이스 모델 - 이 디바이스에는 업그레이드 패키지를 설치할 수 없습니다. 잘못된 패키지를 업로드했거나 디바이스가 새 threat defense 소프트웨어 버전에서 더 이상 지원되지 않는 이전 모델입니다. 디바이스 호환성을 확인하고 사용 가능하면 지원되는 패키지를 업로드하십시오.
- 디스크 공간 부족 - 사용 가능한 공간이 충분하지 않으면 시스템 백업 등을 통해 불필요한 파일을 삭제하십시오. 직접 생성한 파일만 삭제합니다.

업그레이드 상태 모니터링 및 소프트웨어 업그레이드 취소 또는 재시작

다음 방법을 사용하여 threat defense 소프트웨어 업그레이드의 상태를 확인할 수 있습니다.

- device manager 로그인 화면에는 업그레이드 실패 여부를 포함하여 현재 업그레이드 상태가 표시됩니다. 이 화면에서 **Cancel Upgrade(**업그레이드 취소**)**를 클릭하여 진행 중인 주요 업그레이드를 취소할 수 있습니다. 업그레이드가 실패할 경우 **Cancel Upgrade(**업그레이드 취소**)**를 클릭하여 작업을 중지하고 업그레이드 전의 디바이스의 상태로 돌아갈 수 있습니다. 또는 **Continue(**계속**)**를 클릭하여 업그레이드를 재시작합니다. 업그레이드 취소는 유지 보수 또는 패치 업그레이드가 아닌 주요 업그레이드에만 사용할 수 있습니다.
- threat defense 명령줄에 대한 SSH 세션에서 **show upgrade status** 명령을 사용할 수 있습니다. 만들어진 로그 항목을 확인하려면 **continuous** 키워드를 추가하고 자세한 정보를 보려면 **detail** 키워드를 추가합니다. 두 키워드를 모두 추가하여 지속적인 상세정보를 얻을 수 있습니다.

- 업그레이드를 취소하려면 **upgrade cancel** 명령을 사용합니다. 업그레이드 취소는 유지 보수 또는 패치 업그레이드가 아닌 주요 업그레이드에만 사용할 수 있습니다.
- 업그레이드를 재시도하려면 **upgrade retry** 명령을 사용합니다.
- 디바이스의 이전 상태로 되돌리려면 **upgrade revert** 명령을 사용합니다. 어떤 버전으로 되돌릴지 확인하려면 **show upgrade revert-info** 명령을 사용합니다. 명령에 "No revert information available(사용 가능한 되돌리기 정보 없음)"이 표시되면 되돌릴 수 있는 버전이 없는 것입니다.

완료된 **Threat Defense** 소프트웨어 업그레이드 되돌리기

설치된 주요 업그레이드가 예상대로 작동하지 않는 것으로 확인되면 업그레이드 직전의 상태로 디바이스를 되돌릴 수 있습니다.

프로세스가 완료되면 되돌리기된 릴리스를 설치한 후 변경한 컨피그레이션을 다시 실행해야 합니다.

다음 절차에서는 device manager에서 되돌리는 방법을 설명합니다. device manager을 시작할 수 없는 경우, **upgrade revert** 명령을 사용하여 SSH 세션의 threat defense 명령줄에서 되돌릴 수 있습니다. **show upgrade revert-info** 명령을 사용하여 시스템이 어떤 버전으로 되돌아갈지 확인할 수 있습니다.

시작하기 전에

유닛이 고가용성 쌍의 일부인 경우 두 개의 유닛을 모두 되돌려야 합니다. 페일오버 문제 없이 컨피그레이션을 되돌릴 수 있도록 두 개의 유닛에서 동시에 되돌리기를 시작하는 것이 가장 좋습니다. 두 개의 유닛으로 세션을 열고 각 유닛에서 되돌리기가 가능한지 확인한 다음 프로세스를 시작합니다. 되돌리기 중에는 트래픽이 중단되므로, 가능하면 바쁘지 않은 시간에 수행하십시오.

Firepower 4100/9300 섀시의 경우, 주요 Firepower 버전에는 특별히 검증 및 권장된 컴패니언 FXOS 버전이 있습니다. 즉, threat defense 소프트웨어를 되돌린 후에는 권장되지 않는 버전의 FXOS(너무 새로운 버전)를 실행 중일 수 있습니다. 최신 버전의 FXOS는 이전 버전의 threat defense 버전과 호환되지만, 권장되는 조합에 대해서는 향상된 테스트가 실시됩니다. FXOS를 다운그레이드할 수는 없습니다. 따라서 이러한 상황에 처한 경우 권장 조합을 실행하려면 디바이스에서 이미지를 재설치해야 합니다.

프로시저

단계 **1** 디바이스를 선택한 다음 **Updates(**업데이트**)** 요약에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

단계 **2** **System Upgrade(**시스템 업그레이드**)** 섹션에서 **Revert Upgrade(**업그레이드 되돌리기**)** 링크를 클릭합니다.

현재 버전 및 시스템이 되돌아갈 버전을 보여주는 확인 대화 상자가 표시됩니다. 되돌아갈 버전이 없으면 **Revert Upgrade(**업그레이드 되돌리기**)** 링크가 없습니다.

단계 **3** 대상 버전이 마음에 들고 사용 가능한 경우 **Revert(**되돌리기**)**를 클릭합니다.

되돌린 후에는 Smart Software Manager에 디바이스를 다시 등록해야 합니다.

디바이스 재이미징

디바이스를 재이미징할 때는 디바이스 컨피그레이션을 없애고 새 소프트웨어 이미지를 설치합니다. 재이미징은 공장 기본 컨피그레이션을 사용하여 소프트웨어를 새로 설치하기 위한 작업입니다.

다음과 같은 상황에서 디바이스를 재이미징합니다.

- 시스템을 ASA 소프트웨어에서 threat defense 소프트웨어로 변환하려는 경우. ASA 이미지를 실행하는 디바이스를 threat defense 이미지를 실행하는 디바이스로 업그레이드할 수는 없습니다.
- 디바이스가 정상적으로 작동하지 않으며 모든 컨피그레이션을 수정하려는 시도에 실패한 경우

디바이스를 재이미징하는 방법에 대한 자세한 내용은 사용 중인 디바이스 모델의 *Cisco ASA* 또는 *Threat Defense* 디바이스 재이미징 또는 *Threat Defense* 빠른 시작 가이드를 참조하십시오. 이러한 가이드는 http://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-guides-list.html 에서 확인할 수 있습니다.

시스템 백업 및 복원

잘못된 후속 컨피그레이션 또는 물리적 사고로 인해 컨피그레이션이 손상된 경우 디바이스를 복구할 수 있도록 시스템 컨피그레이션을 백업할 수 있습니다.

두 디바이스가 동일한 모델이며 동일한 버전의 소프트웨어(같은 시기에 릴리스되었을 뿐만 아니라 빌드 번호도 동일해야 함)를 실행하는 경우에만 교체 디바이스에 백업을 복원할 수 있습니다. 백업 및 복원 프로세스를 사용하여 어플라이언스 간에 컨피그레이션을 복사하지 마십시오. 백업 파일은 어플라이언스를 고유하게 식별하는 정보를 포함하므로 이러한 방식을 통해 공유할 수 없습니다.

참고 백업에는 관리 IP 주소 컨피그레이션이 포함되지 않습니다. 따라서 백업 파일을 복원할 때는 관리 주소가 백업 복사본에서 대체되지 않습니다. 이로 인해 주소에 대해 수행하는 변경 사항이 유지되며, 다른 네트워크 세그먼트의 다른 디바이스에서도 컨피그레이션을 복원할 수도 있습니다. 또한 백업에는 라이선싱 또는 클라우드 등록 정보도 포함되지 않으므로 복구 시 존재하는 모든 라이선스 또는 클라우드 등록 상태가 유지됩니다.

백업은 컨피그레이션만 포함하며 시스템 소프트웨어는 포함하지 않습니다. 디바이스를 재이미징해야 하는 경우에는 소프트웨어를 다시 설치해야 하며, 그 이후에 백업을 업로드하고 컨피그레이션을 복구할 수 있습니다.

컨피그레이션 데이터베이스는 백업하는 동안 잠겨 있습니다. 백업 중에는 정책, 대시보드 등을 볼 수는 있지만 컨피그레이션을 변경할 수는 없습니다. 복원 중에는 시스템을 완전히 사용할 수 없게 됩니다.

백업 및 복원 페이지의 표에는 시스템에서 사용 가능한 모든 기존 백업 복사본과 백업의 파일 이름, 백업이 생성된 날짜와 시간 및 파일 크기가 나열됩니다. 백업의 유형(수동, 예약, 반복)은 해당 백업 복사본을 생성하도록 시스템에 명령한 방법을 기준으로 합니다.

팁 백업 복사본은 시스템 자체에 생성됩니다. 수동으로 백업 복사본을 다운로드하여 안전한 서버에 저장해야 재해 복구에 필요한 백업 복사본을 사용할 수 있습니다. 시스템은 디바이스에 최대 3개의 백업 복사본을 유지합니다. 새 백업이 가장 오래된 백업을 대체합니다.

다음 항목에서는 백업 및 복원 작업을 관리하는 방법을 설명합니다.

시스템 즉시 백업

언제든지 원할 때 백업을 시작할 수 있습니다.

프로시저

단계 **1** 디바이스를 클릭한 다음 Backup and Restore(백업 및 복원) 요약에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

그러면 백업 및 복원 페이지가 열립니다. 테이블에는 시스템에서 사용 가능한 모든 기존 백업 복사본이 나열됩니다.

단계 **2** **Manual Backup(**수동 백업**)** > **Back Up Now(**지금 백업**)**를 클릭합니다.

단계 **3** 백업의 이름과 설명(선택 사항)을 입력합니다.

백업을 즉시 수행하지 않고 나중에 수행하려는 경우에는 **Schedule(**일정**)**을 대신 클릭하면 됩니다.

단계 **4** (선택 사항). 백업 파일을 암호화하려면 **Encrypt file(**파일 암호화**)** 옵션을 선택합니다.

이 옵션을 선택하는 경우 백업 파일을 복원하는 데 필요한 **Password(**비밀번호**)**(및 **Confirm Password(**비밀번호 확인**)**)를 입력해야 합니다.

단계 **5** (ISA 3000에만 해당.) **Location of Backup Files(**백업 파일의 위치**)**를 선택합니다.

Local Hard Disk(로컬 하드 디스크**)** 또는 **SD Card(SD** 카드**)**에 백업을 생성할 수 있습니다. SD 카드 사용의 장점은 SD 카드를 사용하여 컨피그레이션을 교체 디바이스에 복구할 수 있다는 것입니다.

단계 **6** **Back Up Now(**지금 백업**)**를 클릭합니다.

시스템에서 백업 프로세스를 시작합니다. 백업이 완료되면 백업 파일이 테이블에 표시됩니다. 그러면 백업 복사본을 시스템에 다운로드하고 원하는 경우 다른 위치에 저장할 수 있습니다.

백업을 시작한 후에는 백업 및 복원 페이지에서 나가도 됩니다. 그러나 시스템 속도가 느려질 가능성이 있으므로 백업을 완료할 수 있도록 작업을 일시 중지하는 것을 고려해야 합니다.

또한 백업 중 일부 또는 전체를 수행하는 동안에는 구성 데이터베이스가 잠기므로 백업 프로세스 기간을 변경하는 것을 방지할 수 있습니다.

예약한 시간에 시스템 백업

예약 백업을 설정하여 향후의 특정 날짜와 시간에 시스템을 백업할 수 있습니다. 예약 백업은 한 번만 수행됩니다. 정기적으로 백업을 생성하는 백업 일정을 생성하려면 예약 백업 대신 반복 백업을 구성합니다.

참고 이후 백업 일정을 삭제하려면 일정을 수정하고 **Remove(**제거**)**를 클릭합니다.

프로시저

단계 **1** 디바이스를 클릭한 다음 Backup and Restore(백업 및 복원) 요약에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

단계 **2** **Scheduled Backup(**예약 백업**)** > **Schedule a Backup(**백업 예약**)**을 클릭합니다.

이미 예약한 백업이 있는 경우 **Scheduled Backup(**예약 백업**)** > **Edit(**수정**)**을 클릭합니다.

단계 **3** 백업의 이름과 설명(선택 사항)을 입력합니다.

단계 **4** 백업의 날짜와 시간을 선택합니다.

단계 **5** (선택 사항). 백업 파일을 암호화하려면 **Encrypt file(**파일 암호화**)** 옵션을 선택합니다.

이 옵션을 선택하는 경우 백업 파일을 복원하는 데 필요한 **Password(**비밀번호**)**(및 **Confirm Password(**비밀번호 확인**)**)를 입력해야 합니다.

단계 **6** (ISA 3000에만 해당.) **Location of Backup Files(**백업 파일의 위치**)**를 선택합니다.

Local Hard Disk(로컬 하드 디스크**)** 또는 **SD Card(SD** 카드**)**에 백업을 생성할 수 있습니다. SD 카드 사용의 장점은 SD 카드를 사용하여 컨피그레이션을 교체 디바이스에 복구할 수 있다는 것입니다.

단계 **7** **Schedule(**예약**)**을 클릭합니다.

선택한 날짜와 시간이 되면 시스템이 백업을 수행합니다. 백업이 완료되면 백업 복사본이 백업 테이블에 나열됩니다.

반복 백업 일정 설정

반복 백업을 설정하여 정기적인 일정으로 시스템을 백업할 수 있습니다. 예를 들어 매주 금요일 자정에 백업을 만들 수 있습니다. 반복 백업 일정을 사용하는 경우 항상 최신 백업 집합을 적용할 수 있습니다.

참고 반복 일정을 삭제하려면 일정을 수정하고 **Remove(**제거**)**를 클릭합니다.

프로시저

단계 **1** 디바이스를 클릭한 다음 Backup and Restore(백업 및 복원) 요약에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

단계 **2** **Recurring Backup(**반복 백업**)** > **Configure(**구성**)**를 클릭합니다.

이미 반복 백업을 구성한 경우 **Recurring Backup(**반복 백업**)** > **Edit(**수정**)**을 클릭합니다.

단계 **3** 백업의 이름과 설명(선택 사항)을 입력합니다.

단계 **4** 빈도 및 관련 일정을 선택합니다.

- **Daily(**매일**)** - 시간을 선택합니다. 이 경우 매일 예약된 시간에 백업을 만듭니다.
- **Weekly(**매주**)** - 요일과 시간을 선택합니다. 이 경우 매 날짜의 예약된 시간에 백업을 만듭니다. 예를 들어 매주 월요일, 수요일, 금요일 23:00(오후 11시)에 백업을 예약할 수 있습니다.
- **Monthly(**매월**)** - 날짜와 시간을 선택합니다. 이 경우 매 날짜의 예약된 시간에 백업을 만듭니다. 예를 들어 매월 1일, 15일, 28일 23:00(오후 11시)에 백업을 예약할 수 있습니다.

지정하는 시간은 일광 절약 시간에 맞게 조정되므로 해당 지역에서 시간을 조정할 때마다 1시간 앞당겨지거나 늦춰집니다. 연중 내내 정확한 시간을 유지하려면 시간 변경에서 예약을 수정하십시오.

단계 **5** (선택 사항). 백업 파일을 암호화하려면 **Encrypt file(**파일 암호화**)** 옵션을 선택합니다.

이 옵션을 선택하는 경우 백업 파일을 복원하는 데 필요한 **Password(**비밀번호**)**(및 **Confirm Password(**비밀번호 확인**)**)를 입력해야 합니다.

단계 **6** (ISA 3000에만 해당.) **Location of Backup Files(**백업 파일의 위치**)**를 선택합니다.

Local Hard Disk(로컬 하드 디스크**)** 또는 **SD Card(SD** 카드**)**에 백업을 생성할 수 있습니다. SD 카드 사용의 장점은 SD 카드를 사용하여 컨피그레이션을 교체 디바이스에 복구할 수 있다는 것입니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

선택한 날짜와 시간이 되면 시스템에서 백업을 만듭니다. 백업이 완료되면 백업 복사본이 백업 테이블에 나열됩니다.

반복 일정을 변경하거나 제거할 때까지 해당 일정에 따라 백업이 계속 만들어집니다.

백업 복원

디바이스에서 백업 수행 시 실행하고 있었던 소프트웨어 버전(빌드 번호 포함)과 동일한 버전을 실행하는 한, 필요에 따라 백업을 복원할 수 있습니다. 두 디바이스가 동일한 모델이며 동일한 버전의 소프트웨어(빌드 번호 포함)를 실행하는 경우에만 교체 디바이스에 백업을 복원할 수 있습니다.

그러나 디바이스가 고가용성 쌍의 일부인 경우 백업을 복원할 수 없습니다. 먼저 **Device(**디바이스**)** > **High Availability(**고가용성**)** 페이지에서 HA를 해제해야 백업을 복원할 수 있습니다. 백업이 HA 컨피그레이션을 포함하는 경우 디바이스가 HA 그룹에 다시 조인합니다. 두 유닛에서 동일한 백업을 복원하지 마십시오. 이렇게 하면 두 유닛이 모두 액티브로 설정됩니다. 대신 액티브로 설정할 유닛에서 백업을 먼저 복원한 후에 다른 유닛에서 해당하는 백업을 복원합니다.

복원하려는 백업 복사본이 디바이스에 아직 없으면 복원 전에 백업을 먼저 업로드해야 합니다.

복원 중에는 시스템을 완전히 사용할 수 없게 됩니다.

참고 백업에는 관리 IP 주소 컨피그레이션이 포함되지 않습니다. 따라서 백업 파일을 복원할 때는 관리 주소가 백업 복사본에서 대체되지 않습니다. 이로 인해 주소에 대해 수행하는 변경 사항이 유지되며, 다른 네트워크 세그먼트의 다른 디바이스에서도 컨피그레이션을 복원할 수도 있습니다. 또한 백업에는 라이선싱 또는 클라우드 등록 정보도 포함되지 않으므로 복구 시 존재하는 모든 라이선스 또는 클라우드 등록 상태가 유지됩니다.

시작하기 전에

예를 들어 디바이스를 교체할 때와 같이 다른 시스템에서 백업을 복원하는 경우에는 먼저 디바이스를 등록하고 백업 파일에 구성된 기능에 필요한 선택적 라이선스를 활성화하는 것이 가장 좋습니다. 백업 파일에는 라이선스 또는 클라우드 서비스 정보가 포함되지 않으므로 복구 전에 변경한 라이선스 또는 클라우드 등록은 유지됩니다.

프로시저

단계 **1** 디바이스를 클릭한 다음 Backup and Restore(백업 및 복원) 요약에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

그러면 백업 및 복원 페이지가 열립니다. 테이블에는 시스템에서 사용 가능한 모든 기존 백업 복사본이 나열됩니다.

단계 **2** 복원하려는 백업 복사본이 사용 가능한 백업 목록에 없으면 **Upload(**업로드**)** > **Browse(**찾아보기**)**를 클릭하여 백업 복사본을 업로드합니다.

단계 **3** 파일의 복원 아이콘( )을 클릭합니다.

복원을 확인하라는 메시지가 나타납니다. 기본값으로, 복원 후에 백업 복사본이 삭제되지만, 복원을 계속하기 전에 복원 후 백업을 제거하면 안 됨을 선택하여 백업을 유지할 수 있습니다.

백업 파일이 암호화된 경우 파일을 열고 암호를 해독하는 데 필요한 **Password(**비밀번호**)**를 입력해야 합니다.

복원이 완료되고 나면 시스템이 재부팅됩니다.

참고 시스템은 재부팅된 후 VDB(Vulnerability Database), 지리위치 및 규칙 데이터베이스 업데이트를 자동으로 확인하여 필요한 경우 다운로드합니다. 이러한 업데이트는 규모가 클 수 있기 때문에 첫 시도는 실패할 수 있습니다. 작업 목록을 확인하고, 다운로드에 실패한 경우 시스템 데이터베이스 업데이트, 857 페이지에 설명된 대로 업데이트를 수동으로 다운로드합니다. 또한 정책도 재구축합니다. 업데이트가 성공할 때까지 모든 후속 구축은 실패합니다.

단계 **4** 필요한 경우 디바이스 > **Smart License(**스마트 라이선스**)** > **View Configuration(**컨피그레이션 보기**)**을 클릭하고, 디바이스를 재등록하고, 필요한 선택적 라이선스를 재활성화합니다.

백업에는 라이선스 또는 클라우드 등록 정보가 포함되지 않습니다. 따라서 새 시스템에 백업을 복구하는 경우(예 : 디바이스를 교체할 때 시스템이 평가 모드에 있는 경우) 이를 등록하고 필요한 라이선스를 활성화해야 합니다. 복구 전에 디바이스를 등록하고 라이선스를 활성화한 경우에는 추가 변경이 필요하지 않습니다.

이전 백업을 동일한 시스템으로 복구하는 경우에는 라이선스 또는 클라우드 등록을 변경할 필요가 없습니다. 그러나 백업이 생성된 후 비활성화한 라이선스가 필요한 기능을 백업에 포함할 수 있으므로 필요한 모든 선택적 라이선스가 활성화되었는지 확인합니다.

ISA 3000 디바이스 교체

ISA 3000에는 분리 후 다른 ISA 3000 디바이스에 삽입할 수 있는 SD 카드가 있습니다. SD 카드에 시스템 백업을 생성하는 경우에는 이 기능을 사용하여 디바이스를 쉽게 교체할 수 있습니다. 문제 있는 디바이스의 SD 카드를 분리하여 새 디바이스에 삽입하기만 하면 됩니다. 그러면 백업을 복원할 수 있게 됩니다.

필요한 백업을 사용할 수 있도록 하려면 SD 카드에 백업을 생성하는 백업 작업을 구성합니다.

백업 파일 관리

새 백업을 생성할 때 백업 파일은 백업 및 복원 페이지에 나열됩니다. 백업 복사본은 무기한 보존되지 않으며, 디바이스의 디스크 공간 사용량이 최대 임계값에 도달하면 새 백업 복사본을 위한 공간 확보를 위해 이전 백업 복사본이 삭제됩니다. 또한 핫픽스 이외의 업그레이드를 설치하면 모든 백업 파일이 삭제됩니다. 따라서 가장 보관 필요성이 높은 특정 백업 복사본을 보관할 수 있도록 백업 파일을 정기적으로 관리해야 합니다.

다음 작업을 수행하여 백업 복사본을 관리할 수 있습니다.

- 보안 스토리지에 파일 다운로드 - 워크스테이션에 백업 파일을 다운로드하려면 해당 파일의 다운로드 아이콘( )을 클릭합니다. 그러면 보안 파일 스토리지로 파일을 이동할 수 있습니다.
- 시스템에 백업 파일 업로드 - 디바이스에서 더 이상 사용할 수 없는 백업 복사본을 복원하려면 **Upload(**업로드**)** > **Browse File(**파일 찾아보기**)**을 클릭하고 워크스테이션에서 해당 복사본을 업로드합니다. 그러면 백업을 복원할 수 있습니다.

참고 업로드한 파일의 이름은 원본 파일 이름과 일치하도록 바꿀 수 있습니다. 또한, 시스템에 3개가 넘는 백업 복사본이 이미 있으면 업로드한 파일을 위한 공간 확보를 위해 가장 오래된 복사본이 삭제됩니다. 이전 소프트웨어 버전에서 생성한 파일은 업로드할 수 없습니다.

- 백업 복원 - 백업 사본을 복원하려면 해당 파일의 복원 아이콘()을 클릭합니다. 복원 중에는 시스템을 사용할 수 없으며 복원이 완료되면 시스템이 재부팅됩니다. 시스템이 가동 및 실행되고 나면 컨피그레이션을 구축해야 합니다.
- 백업 파일 삭제 - 특정 백업이 더 이상 필요하지 않은 경우, 해당 파일의 삭제 아이콘()을 클릭합니다. 그러면 삭제를 확인하라는 메시지가 나타납니다. 삭제한 백업 파일은 복구할 수 없습니다.

감사 및 변경 관리

시스템 이벤트 및 사용자가 수행한 작업에 대한 상태 정보를 확인할 수 있습니다. 이 정보를 참조하여 시스템을 감사하고 시스템이 적절하게 관리되고 있는지 확인할 수 있습니다.

감사 로그를 확인하려면 디바이스 > **Device Administration(**디바이스 관리**)** > **Audit Log(**감사 로그**)**를 클릭합니다. 또한 오른쪽 상단 모서리의 **Task List(**작업 목록**)** 또는 **Deployment(**구축**)** 아이콘 버튼을 클릭하여 시스템 관리 정보를 찾을 수도 있습니다.

다음 주제에서는 시스템 감사 및 변경 관리에 대한 몇 가지 주요 개념과 작업을 살펴봅니다.

감사 이벤트

감사 로그는 다음 유형의 이벤트를 포함할 수 있습니다.

Custom Feed Update Event(맞춤형 피드 업데이트 이벤트**), Custom Feed Update Failed(**맞춤형 피드 업데이트 실패**)**

이러한 이벤트는 성공적으로 완료되었거나 맞춤형 보안 인텔리전스 피드에 대한 업데이트가 실패했음을 나타냅니다. 세부 정보에는 업데이트를 시작한 사람과 업데이트 중인 피드에 대한 정보가 포함됩니다.

사용자 지정 규칙 파일 가져오기 요약 이벤트

이러한 이벤트는 하나 이상의 맞춤형 침입 규칙이 포함된 파일을 가져왔음을 나타냅니다. 이벤트에는 추가, 업데이트 및 삭제된 규칙 수의 요약과 가져온 규칙에 대한 세부 사항을 보여주는 차이점 보기가 포함됩니다.

Deployment Completed(구축 완료됨**), Deployment Failed(**구축 실패함**):** 작업 이름 또는 엔터티 이름

이러한 이벤트는 정상적으로 완료되었거나 실패한 구축 작업을 나타냅니다. 세부사항에는 작업을 시작한 사람과 작업 엔터티에 대한 정보가 포함됩니다. 실패한 작업에는 실패 관련 오류 메시지가 포함됩니다.

세부사항에는 **Differences View(**차이 보기**)** 탭도 포함되며, 이 탭에는 작업 시 디바이스에 구축된 변경 사항이 표시됩니다. 여기에는 구축된 엔터티의 모든 엔터티 변경 이벤트가 조합되어 있습니다.

이러한 이벤트를 기준으로 필터링하려는 경우 사전 정의된 **Deployment History(**구축 기록**)** 필터만 클릭하면 됩니다. 이러한 이벤트의 이벤트 유형은 Deployment Event(구축 이벤트)입니다. 완료된 이벤트 또는 실패한 이벤트만 기준으로 하여 필터링할 수는 없습니다.

이벤트 이름에는 사용자 정의 작업 이름(구성하는 경우) 또는 "User(사용자 이름) Triggered Deployment(사용자가 트리거한 구축)"가 포함됩니다. 디바이스 설정 마법사를 실행하는 중에 수행되는 "Device Setup Automatic Deployment(디바이스 설정 자동 구축)" 및 "Device Setup Automatic Deployment (Final Step)(디바이스 설정 자동 구축(최종 단계))" 작업도 있습니다.

Entity Created(엔터티 생성됨**), Entity Updated(**엔터티 업데이트됨**), Entity Deleted(**엔터티 삭제됨**):** 엔터티 이름**(**엔터티 유형**)**

이러한 이벤트는 식별된 엔터티나 개체가 변경되었음을 나타냅니다. 엔터티 세부사항에는 변경을 수행한 사람과 엔터티 이름, 유형, ID가 포함됩니다. 이러한 항목을 기준으로 엔터티를 필터링할 수 있습니다. 세부사항에는 **Differences View(**차이 보기**)** 탭도 포함되며, 이 탭에는 개체에 적용된 변경 사항이 표시됩니다.

HA Action Event(HA 작업 이벤트**)**

이러한 이벤트는 고가용성 컨피그레이션에 대한 작업(사용자가 시작한 작업 또는 시스템이 시작한 작업)과 관련되어 있습니다. 이벤트 유형은 HA Action Event(HA 작업 이벤트)이지만 이벤트 이름은 다음 중 하나입니다.

- **HA Suspended(HA** 일시 중단됨**)** - 시스템에서 HA를 의도적으로 일시 중단했습니다.
- **HA Resumed(HA** 다시 시작됨**)** - 시스템에서 HA를 의도적으로 다시 시작했습니다.
- **HA Reset(HA** 재설정됨**)** - 시스템에서 HA를 의도적으로 재설정했습니다.
- **HA Failover: Unit Switched Modes(HA** 페일오버**:** 유닛 모드 전환됨**)** - 모드를 의도적으로 전환했거나 상태 메트릭 위반으로 인해 시스템에서 페일오버를 실행하였습니다. 메시지에는 액티브 피어가 스탠바이 피어로 전환되었거나 스탠바이 피어가 액티브 피어로 전환되었음이 표시됩니다.

고가용성 동기화 완료됨

액티브 유닛에서 스탠바이 유닛에 컨피그레이션을 동기화했습니다. 이벤트에는 동기화된 버전과 비교한 이전 버전의 변경 정보가 포함됩니다.

Interface List Scanned(스캔된 인터페이스 목록**)**

이 이벤트는 인터페이스 인벤토리에서 변경 사항을 스캔했음을 나타냅니다.

Pending Changes Discarded(보류 중인 변경 사항 취소됨**)**

이 이벤트는 보류 중인 모든 변경 사항을 삭제했음을 나타냅니다. 이 이벤트와 이전 Deployment Completed(구축 완료됨) 이벤트 사이의 Entity Created(엔터티 생성됨), Entity Updated(엔터티 업데이트됨), Entity Deleted(엔터티 삭제됨) 이벤트에 표시된 모든 변경 사항은 제거되며, 영향을 받은 개체의 상태는 마지막으로 구축된 버전으로 되돌아갑니다.

Rules Update Event(규칙 업데이트 이벤트**)**

Snort 3을 실행할 때 LSPUpdateServer 엔티티의 이 이벤트는 새 침입 규칙 패키지를 다운로드하여 설치할 때 추가, 제거 또는 변경된 침입 규칙에 대한 세부 정보를 표시합니다. 이벤트는 100개 규칙으로 제한되므로, 100개보다 많은 항목이 추가, 제거 또는 변경되면 이벤트에 완전한 정보가 포함되지 않습니다. 이 이벤트는 Snort 2 업데이트에는 표시되지 않습니다.

Task Started(작업 시작됨**), Task Completed(**작업 완료됨**), Task Failed(**작업 실패함**)**

작업 이벤트는 시스템이나 사용자가 시작한 작업의 시작과 종료를 나타냅니다. 이 두 이벤트는 작업 목록에서 단일 작업으로 통합됩니다. 이 작업 목록은 오른쪽 상단 모서리에 있는 **Task List(**작업 목록**)** 버튼을 클릭하면 볼 수 있습니다.

작업에는 구축 작업과 수동 또는 예약된 데이터베이스 업데이트와 같은 작업이 포함됩니다. 작업 목록에 있는 모든 항목은 감사 로그의 두 작업 이벤트(작업 시작 표시 및 성공적인 완료 또는 실패)에 부합합니다.

User Logged In(사용자 로그인함**), User Logged Out(**사용자 로그아웃함**):** 사용자 이름

이러한 이벤트에는 사용자의 device manager 로그인 및 로그아웃 시간과 소스 IP 주소가 표시됩니다. User Logged Out(사용자 로그아웃함) 이벤트는 활성 로그아웃과 유휴 시간 초과로 인한 자동 로그아웃 모두에 대해 발생합니다.

이러한 이벤트는 디바이스와 연결을 설정하는 RA VPN 사용자와는 관계가 없습니다. 또한 디바이스 CLI 로그인/로그아웃도 포함하지 않습니다.

감사 로그 보기 및 분석

감사 로그에는 구축 작업, 데이터베이스 업데이트, device manager 로그인/로그아웃과 같은 시스템 시작/사용자 시작 이벤트에 대한 정보가 포함됩니다.

로그에서 확인할 수 있는 이벤트 유형의 설명은 감사 이벤트, 871 페이지의 내용을 참조하십시오.

프로시저

단계 **1** 디바이스를 클릭한 다음 **Device Administration(**디바이스 관리**) > View Configuration(**컨피그레이션 보기**)** 링크를 클릭합니다.

단계 **2** 목차에서 **Audit Log(**감사 로그**)**를 아직 선택하지 않은 경우 클릭합니다.

이벤트는 날짜를 기준으로 그룹화되며 한 날짜 안에서는 시간을 기준으로 그룹화됩니다. 날짜/시간이 가장 최근인 이벤트가 목록 맨 위에 표시됩니다. 처음에는 각 이벤트가 축소되어 있으므로 시간, 이벤트 이름, 이벤트를 시작한 사용자 및 사용자의 소스 IP 주소만 표시됩니다. 사용자 및 IP 주소가 "System(시스템)"이면 디바이스 자체에서 이벤트를 시작한 것입니다.

다음을 수행할 수 있습니다.

- 이벤트 이름 옆의 >를 클릭하여 이벤트를 열고 이벤트 세부사항을 확인합니다. 아이콘을 다시 클릭하면 이벤트가 닫힙니다. 대다수 이벤트에는 이벤트 유형, 사용자 이름, 소스 IP 주소 등의

이벤트 특성이 포함된 단순 목록이 있습니다. 하지만 Entity(엔터티) 및 Deployment(구축) 이벤트에는 다음의 두 탭이 있습니다.

- **Summary(요약)** - 기본적인 이벤트 특성이 표시됩니다.
- **Differences View(차이 보기)** - 이벤트의 일부분으로 수행된 변경과 기존의 "구축된" 컨피그레이션을 비교한 내용이 표시됩니다. 구축 작업의 경우에는 이 보기가 길어서 스크롤해야 할 수도 있습니다. 이 보기에는 구축 작업의 일부로 수행된 Entity(엔터티) 이벤트 변경 사항의 모든 차이가 통합 표시됩니다.

- 필터 필드 오른쪽의 드롭다운 목록에서 다른 시간 범위를 선택합니다. 기본적으로는 지난 2주 동안의 이벤트가 표시되지만 지난 24시간, 7일, 1개월 또는 6개월 동안의 이벤트가 표시되도록 변경할 수 있습니다. **Custom(맞춤형)**을 클릭하고 시작 및 종료 날짜와 시간을 입력해 정확한 범위를 지정합니다.
- 로그의 링크를 클릭하여 해당 항목에 대한 검색 필터를 추가합니다. 그러면 해당 항목을 포함하는 이벤트만 표시되도록 목록이 업데이트됩니다. 또한 **Filter(필터)** 상자만 클릭하면 필터를 직접 작성할 수도 있습니다. 필터 상자 아래에는 사전 정의된 필터 몇 개가 있습니다. 이러한 필터를 클릭하면 관련 필터 기준을 로드할 수 있습니다. 이벤트 필터링에 대한 세부 정보는 감사 로그 필터링, 874 페이지의 내용을 참조하십시오.
- 브라우저 페이지를 다시 로드하여 최신 이벤트로 로그를 새로 고칩니다.

감사 로그 필터링

특정 유형의 메시지만 표시되도록 보기의 범위를 좁히기 위해 감사 로그에 필터를 적용할 수 있습니다. 필터의 각 요소는 정확하고 완전한 일치 항목입니다. 예를 들어 "User = admin"을 사용하는 경우 이름이 **admin**인 사용자가 시작한 이벤트만 표시됩니다.

다음과 같은 기술을 단독으로 사용하거나 조합하여 필터를 작성할 수 있습니다. 필터 요소를 추가할 때마다 목록은 자동으로 업데이트됩니다.

사전 정의된 필터 클릭

Filter(필터) 필드 아래에는 사전 정의된 필터가 있습니다. 링크만 클릭하면 해당 필터가 로드됩니다. 그러면 필터를 확인하라는 메시지가 표시됩니다. 이미 필터를 적용한 경우에는 추가되지 않고 대체됩니다.

강조 표시된 항목 클릭

필터를 작성하는 가장 쉬운 방법은 로그 테이블의 항목 또는 필터링 기준으로 사용할 값이 포함된 이벤트 세부사항을 클릭하는 것입니다. 항목을 클릭하면 해당 값 및 요소의 조합에 대해 올바르게 작성된 요소로 **Filter(필터)** 필드가 업데이트됩니다. 그러나 이 기술을 사용하려면 기존 이벤트 목록에 원하는 값이 포함되어 있어야 합니다.

항목에 대해 필터 요소를 추가할 수 있는 경우 해당 항목 위에 마우스를 가져가면 항목에 밑줄이 표시되며 **Click to Add to Filter(필터에 추가하려면 클릭)** 명령이 나타납니다.

원자성 요소 선택

Filter(필터**)** 필드를 클릭하고 드롭다운 목록에서 원하는 원자성 요소를 선택한 다음 등호 뒤에 일치 값을 입력하고 Enter 키를 눌러 필터를 작성할 수도 있습니다. 필터링 기준으로 사용할 수 있는 요소가 아래에 나와 있습니다. 모든 요소가 모든 이벤트 유형과 관련되어 있는 것은 아닙니다.

- **Event Type(**이벤트 유형**)** - 일반적으로(항상은 아님) 이벤트 이름과 같지만 엔터티 이름이나 사용자 등의 변수 한정자는 없습니다. 구축 이벤트의 경우 이벤트 유형은 Deployment Event(구축 이벤트)입니다. 이벤트 유형에 대한 설명은 감사 이벤트, 871 페이지의 내용을 참조하십시오.
- **User(**사용자**)** - 이벤트를 시작한 사용자의 이름입니다. 시스템 사용자의 경우 모두 대문자로 표시됩니다(예: SYSTEM).
- **Source IP(**소스 **IP)** - 사용자가 이벤트를 시작한 IP 주소입니다. 시스템에서 시작된 이벤트의 소스 IP 주소는 SYSTEM입니다.
- **Entity ID(**엔터티 **ID)** - 엔터티나 개체의 UUID로, 8e7021b4-2e1e-11e8-9e5d-0fc002c5f931과 같이 읽을 수 없는 긴 문자열입니다. 일반적으로 이 필터를 사용하려면 이벤트 세부사항에서 엔터티 ID를 클릭하거나 REST API를 사용하여 관련 GET 호출을 하여 필요한 ID를 검색해야 합니다.
- **Enntity Name(**엔터티 이름**)** - 엔터티 또는 개체의 이름입니다. 사용자 생성 엔터티의 경우에는 보통 개체에 지정한 이름(예: 네트워크 개체의 경우 InsideNetwork)입니다. 시스템 생성 엔터티나 일부 사용자 정의 엔터티의 경우에는 사전 정의되었으나 이해 가능한 이름입니다. 예를 들어 명시적으로 이름을 지정하지 않은 구축 작업의 경우 "User (admin) Triggered Deployment(사용자(관리자)가 트리거한 구축)"입니다.
- **Enntity Type(**엔터티 유형**)** - 엔터티 또는 개체의 종류입니다. 사전 정의되었으나 이해 가능한 이름입니다(예: Network Object(네트워크 개체)). 관련 개체 모델에서 "type(유형)" 값을 확인하여 API Explorer에서 엔터티 유형을 찾을 수 있습니다. API 유형은 일반적으로 모두 소문자이며 공백이 없습니다. 모델에 표시된 것과 똑같이 유형을 입력하는 경우, Enter 키를 누르면 문자열이 더 쉽게 읽을 수 있는 형식으로 변경됩니다. 둘 중 어떤 형식을 입력해도 됩니다. API Explorer를 열려면 More options(추가 옵션) 버튼(⋮)을 클릭하고 **API Explorer**를 선택합니다.

복잡한 감사 로그 필터에 대한 규칙

여러 원자성 요소가 포함된 복잡한 필터를 작성할 때는 다음 규칙에 주의하십시오.

- 유형이 같은 요소의 경우 해당 유형의 모든 값 간에 OR 관계가 설정됩니다. 예를 들어 "User = admin"과 "User = SYSTEM"을 포함하면 두 사용자 중 한 명이 시작한 이벤트가 일치 항목으로 표시됩니다.
- 유형이 다른 요소의 경우 AND 관계가 설정됩니다. 예를 들어 "Event Type = Entity Updated" 및 "User = SYSTEM"을 포함하면 활성 사용자가 아닌 시스템이 엔터티를 업데이트한 이벤트만 표시됩니다.
- 와일드카드, 정규식, 부분 일치 또는 단순 텍스트 문자열 일치는 사용할 수 없습니다.

구축 및 엔터티 변경 기록 확인

구축 및 엔터티 이벤트의 이벤트 세부사항에는 **Differences View(**차이 보기**)** 탭이 포함되어 있습니다. 이 탭에는 이전 컨피그레이션과 변경 사항을 비교한 내용이 색상 코드가 적용된 상태로 표시됩니다.

- 구축 작업의 경우 구축 전에 디바이스에서 실행 중이었던 컨피그레이션과 실제로 구축된 변경 사항을 비교한 내용이 표시됩니다.
- 엔터티 이벤트의 경우에는 개체의 이전 버전에 적용된 컨피그레이션 변경 사항이 표시됩니다. 이전 버전은 디바이스에서 실제로 사용되었던 버전일 수도 있고 아직 구축되지 않은 개체의 변경 사항일 수도 있습니다.

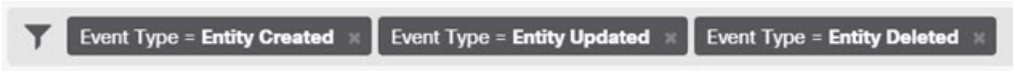
프로시저

단계 **1** 디바이스를 클릭한 다음 **Device Administration(**디바이스 관리**)** > **View Configuration(**컨피그레이션 보기**)** 링크를 클릭합니다.

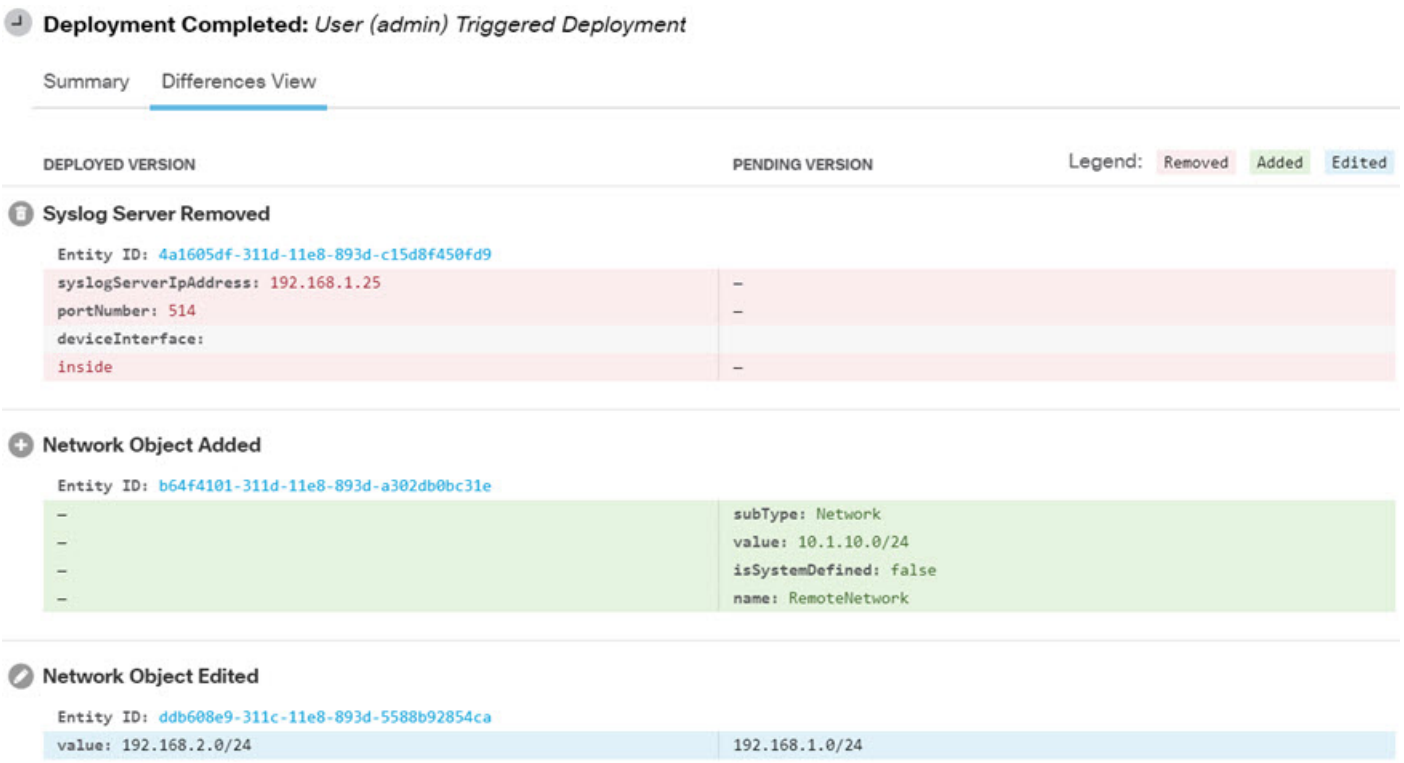
단계 **2** 목차에서 **Audit Log(**감사 로그**)**를 아직 선택하지 않은 경우 클릭합니다.

단계 **3** (선택 사항). 메시지를 필터링합니다.

- 구축 이벤트 - 필터 상자 아래에서 사전 정의된 **Deployment History(**구축 기록**)** 필터를 클릭합니다.
- 엔터티 변경 이벤트 - 원하는 변경 유형에 대해 Event Type(이벤트 유형) 요소를 사용하여 필터를 수동으로 생성합니다. 모든 엔터티 변경 사항을 확인하려면 Entity Created(엔터티 생성됨), Entity Updated(엔터티 업데이트됨) 및 Entity Deleted(엔터티 삭제됨)에 해당하는 3가지 사양을 포함합니다. 그러면 필터가 다음과 같이 표시됩니다.



단계 **4** 이벤트를 열고 **Differences View(**차이 보기**)** 탭을 클릭합니다.



변경 사항에는 색상 코드가 적용되며, 머리글에는 개체 유형과 개체에 대해 수행된 작업 Added(추가됨)(생성됨), Removed(제거됨)(삭제됨) 또는 Edited(수정됨)(업데이트됨)이 표시됩니다. 수정된 개체의 경우 개체에서 변경되었거나 삭제된 특성만 표시됩니다. 구축 작업의 경우에는 변경된 각 엔터티에 대해 개별 머리글이 있습니다. 이 머리글은 개체의 엔터티 유형을 나타냅니다.

모든 보류 중인 변경 사항 취소

아직 구축하지 않은 컨피그레이션 변경 사항이 만족스럽지 않다면 보류 중인 모든 변경 사항을 취소할 수 있습니다. 이렇게 하면 모든 기능이 디바이스에 있는 상태로 되돌아갑니다. 그리고 나면 컨피그레이션 변경을 다시 시작할 수 있습니다.

프로시저

단계 **1** 웹 페이지의 오른쪽 상단에 있는 **Deploy Changes(**변경 사항 구축**)** 아이콘을 클릭합니다.

보류 중인 변경 사항이 있으면 아이콘이 점으로 강조 표시됩니다.

단계 **2** **More Options(**기타 옵션**)** > **Discard All(**모두 취소**)**을 클릭합니다.

단계 **3** 확인 대화 상자에서 **OK(**확인**)**를 클릭합니다.

시스템이 변경 사항을 취소하며, 프로세스 완료 시에 보류 중인 변경 사항이 없다는 메시지가 표시됩니다. 그리고 Pending Changes Discarded(보류 중인 변경 사항 취소됨) 이벤트가 감사 로그에 추가됩니다.

디바이스 컨피그레이션 내보내기

현재 구축된 컨피그레이션의 복사본을 JSON 형식으로 내보낼 수 있습니다. 해당 파일은 보관 또는 기록 보존용으로 사용할 수 있습니다. 비밀번호 및 비밀 키와 같은 민감한 데이터는 마스크 처리됩니다.

이 디바이스 또는 다른 디바이스로 파일을 가져올 수는 없습니다. 이 기능을 시스템 백업 대신 사용할 수는 없습니다.

구축 작업을 한 번 이상 성공적으로 완료해야 컨피그레이션을 다운로드할 수 있습니다.

프로시저

단계 **1** 디바이스를 선택한 다음 **Device Administration(**디바이스 관리**)** 그룹에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

단계 **2** 목차에서 **Download Configuration(**컨피그레이션 다운로드**)**을 클릭합니다.

단계 **3** **Get Device Configuration(**디바이스 컨피그레이션 가져오기**)**을 클릭하여 파일을 생성하는 작업을 시작합니다.

이전에 파일을 생성한 경우 다운로드 버튼과 **File is ready to download(**파일 다운로드가 준비됨**)** 메시지 및 파일 생성 날짜가 표시됩니다.

컨피그레이션의 크기에 따라서는 파일을 생성하는 데 몇 분 정도 걸릴 수도 있습니다. Export Config(컨피그레이션 내보내기) 작업이 완료되고 파일이 생성될 때까지 작업 목록 또는 감사 로그를 확인하거나 이 페이지를 주기적으로 다시 방문합니다.

단계 **4** 파일이 생성되면 이 페이지로 돌아와 **Download the Configuration File(**컨피그레이션 파일 다운로드**)** 버튼( )을 클릭하여 파일을 워크스테이션에 저장합니다.

Device Manager 및 Threat Defense 사용자 액세스 관리

사용자가 threat defense(HTTPS 액세스)에 로그인할 수 있도록 외부 인증 및 권한 부여 소스를 컨피그레이션할 수 있습니다. 외부 서버는 로컬 사용자 데이터베이스 및 시스템 정의 관리 사용자와 함께 사용하거나 대신 사용할 수 있습니다. device manager 액세스에 대해서는 추가 로컬 사용자 어카운트를 생성할 수는 없습니다.

컨피그레이션을 변경할 수 있는 외부 device manager 사용자 계정이 여러 개일 수는 있지만 이러한 변경 사항을 사용자가 추적할 수는 없습니다. 한 사용자가 변경 사항을 구축하면 모든 사용자가 적용한 변경 사항이 구축됩니다. 잠금은 적용되지 않습니다. 즉, 두 명 이상의 사용자가 같은 개체를 동시에 업데이트하려고 하면 한 사용자만 변경 사항을 저장할 수 있습니다. 또한 사용자를 기준으로 변경 사항을 취소할 수도 없습니다.

device manager에서는 동시 사용자 세션 5개를 허용합니다. 6번째 사용자가 로그인하면 가장 오래된 사용자 세션이 자동으로 로그오프됩니다. 또한 유휴 시간 제한도 적용되므로 20분이 지나면 비활성 사용자가 로그아웃됩니다.

threat defense CLI에 대한 SSH 액세스를 위해 외부 인증 및 권한 부여를 컨피그레이션할 수도 있습니다. 로컬 데이터베이스는 외부 소스를 사용하기 전에 항상 확인되므로 페일세이프 액세스에 대해 추가 로컬 사용자를 생성할 수 있습니다. 로컬 및 외부 소스 모두에서 중복 사용자를 생성하지 마십시오. 관리 사용자를 제외하면 CLI와 device manager에서 겹치는 사용자는 없으며 사용자 어카운트는 완전히 별개입니다.

참고 외부 서버를 사용 중인 경우, 별도 RADIUS 서버 그룹을 설정하거나 특정 threat defense 디바이스 IP 주소에 대해서만 사용자 액세스를 허용하는 RADIUS 서버 내 인증/권한 부여 정책을 생성하여 디바이스의 하위 집합에 대한 사용자의 액세스를 제어할 수 있습니다.

다음 주제에서는 device manager 사용자 액세스와 CLI 사용자 액세스를 컨피그레이션하고 관리하는 방법을 설명합니다.

Device Manager(HTTPS) 사용자를 위한 외부 권한 부여(AAA) 컨피그레이션

외부 RADIUS 서버에서 device manager에 HTTPS 액세스 권한을 제공할 수 있습니다. RADIUS 인증 및 권한 부여를 활성화하면 각기 다른 액세스 권한 레벨을 제공할 수 있으며, 모든 사용자가 로컬 관리자 어카운트를 통해 로그인하지 못하게 할 수 있습니다.

이러한 외부 사용자는 threat defense API 및 API Explorer에 대한 권한을 부여받습니다.

RBAC(역할 기반 액세스 제어)를 제공하려면 RADIUS 서버에서 사용자 어카운트를 업데이트하여 **cisco-av-pair** 특성을 정의합니다. 이는 ISE에서 해당하며, 무료 RADIUS에서는 해당 특성의 철자가 Cisco-AVPair이므로 시스템에서 철자가 올바른지 확인하십시오. 사용자 어카운트에 대해 이러한 속성을 정확하게 정의해야 합니다. 그렇지 않으면 해당 사용자의 device manager 액세스가 거부됩니다. **cisco-av-pair** 특성에 대해 지원되는 값은 다음과 같습니다.

- **fdm.userrole.authority.admin**은 전체 관리자 액세스를 제공합니다. 이러한 사용자는 로컬 관리 사용자가 수행할 수 있는 모든 작업을 수행할 수 있습니다.
- **fdm.userrole.authority.rw**는 읽기-쓰기 액세스를 제공합니다. 이러한 사용자는 읽기 전용 사용자가 수행할 수 있는 모든 작업을 수행할 수 있으며 컨피그레이션 수정 및 구축도 수행할 수 있습니다. 업그레이드 설치, 백업 생성 및 복원, 감사 로그 확인, device manager 사용자의 세션 종료를 포함하는 시스템의 중요 작업만 제한됩니다.

- **fdm.userrole.authority.ro**는 읽기 전용 액세스를 제공합니다. 이러한 사용자는 대시보드 및 컨피그레이션을 볼 수는 있지만 변경할 수는 없습니다. 사용자가 변경을 시도하면 권한이 없음을 설명하는 오류 메시지가 표시됩니다.

사용자가 device manager에 로그인할 때는 페이지 오른쪽 상단에 사용자 이름과 역할이 표시됩니다. 역할은 Administrator(관리자), Read-Write User(읽기-쓰기 사용자) 또는 Read-Only User(읽기 전용 사용자) 중 하나입니다.

RADIUS 서버에서 어카운트를 설정하고 나면 다음 절차를 수행하여 관리 액세스용으로 해당 어카운트를 활성화할 수 있습니다.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 후 **System Settings(**시스템 설정**)** > **Management Access(**관리 액세스**)** 링크를 클릭합니다.

System Settings(시스템 설정) 페이지가 이미 열려 있는 경우 목차에서 **Management Access(**관리 액세스**)**를 클릭하면 됩니다.

단계 **2** **AAA Configuration(AAA** 컨피그레이션**)** 탭을 아직 선택하지 않은 경우 클릭합니다.

단계 **3** **HTTPS Connection(HTTPS** 연결**)** 옵션을 다음과 같이 컨피그레이션합니다.

- **Server Group for Management/REST API(**관리**/REST API**용 서버 그룹**)** - 기본 인증 소스로 사용할 RADIUS 서버 그룹 또는 로컬 사용자 데이터베이스(LocalIdentitySource)를 선택합니다. 외부 인증을 사용하려는 경우 RADIUS 서버 그룹을 선택해야 합니다.

  서버 그룹이 아직 없으면 **Create New RADIUS Server Group(**새 **RADIUS** 서버 그룹 생성**)** 링크를 클릭하여 지금 생성합니다. 각 서버에 대해 RADIUS 서버 개체도 생성하여 그룹에 추가해야 합니다. 하지만 이 작업은 서버 그룹을 정의할 때 수행할 수 있습니다. RADIUS에 대한 자세한 정보는 RADIUS 서버 및 그룹, 182 페이지의 내용을 참조하십시오.

- **Authentication with LOCAL(**로컬로 인증**)** — 외부 서버 그룹을 선택하는 경우 로컬 관리 사용자 어카운트를 포함하는 로컬 ID 소스를 사용하는 방법을 지정할 수 있습니다. 다음 중 하나를 선택합니다.

  - **Before External Server(**외부 서버 전**)** — 시스템이 로컬 소스를 먼저 대조하여 사용자 이름과 비밀번호를 확인합니다.
  - **After External Server(**외부 서버 후**)** — 외부 소스를 사용할 수 없거나 외부 소스에 사용자 어카운트가 없는 경우에만 로컬 소스를 확인합니다.
  - **Never(**사용 안 함**)** — (권장되지 않음.) 로컬 소스를 사용하지 않습니다. 따라서 관리 사용자로 로그인할 수 없습니다.

  주의 **Never(**사용 안 함**)**를 선택하는 경우 관리자 어카운트를 사용하여 device manager에 로그인할 수 없습니다. RADIUS 서버를 사용할 수 없게 되거나 RADIUS 서버에서 어카운트를 잘못 구성하는 경우에는 시스템에서 해당 어카운트를 차단합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

Threat Defense CLI(SSH) 사용자를 위한 외부 권한 부여(AAA) 구성

외부 RADIUS 서버에서 threat defense CLI에 SSH 액세스 권한을 제공할 수 있습니다. RADIUS 인증 및 권한 부여를 활성화하면 각 디바이스에 별도 로컬 사용자 계정을 정의하는 대신에 단일 인증 소스에서 다양한 수준의 액세스 권한을 제공할 수 있습니다.

이러한 SSH 외부 사용자는 threat defense API 및 API Explorer에 대한 권한을 부여받지 못합니다. SSH에 대한 권한 부여를 정의하는 데 사용하는 메커니즘은 HTTPS 액세스에 필요한 메커니즘과는 다릅니다. 그러나 SSH 및 HTTPS 두 프로토콜을 통해 특정 사용자가 시스템에 액세스할 수 있도록 SSH 및 HTTPS 권한 부여 기준 모두에서 동일한 RADIUS 사용자를 컨피그레이션할 수 있습니다.

SSH 액세스에 RBAC(Role-Based Access Control)를 제공하려면 RADIUS 서버에서 사용자 계정을 업데이트하여 **Service-Type(**서비스 유형**)** 속성을 정의합니다. 사용자 계정에서 이 속성을 정의해야 합니다. 그러지 않으면 디바이스에 대한 사용자의 SSH 액세스가 거부됩니다. **Service-Type(**서비스 유형**)** 속성에 지원되는 값은 다음과 같습니다.

- **Administrative(**관리**)(6)** — CLI에 대한 **config** 액세스 권한을 제공합니다. 이러한 사용자는 CLI에서 모든 명령을 사용할 수 있습니다.
- **NAS Prompt(NAS** 프롬프트**) (7)** 또는 6 이외의 모든 레벨 - CLI에 대한 기본 액세스 권한을 제공합니다. 이러한 사용자는 모니터링 및 문제 해결을 위해 **show** 명령 같은 읽기 전용 명령을 사용할 수 있습니다.

RADIUS 서버에서 계정을 올바르게 설정하고 나면 이 절차를 수행하여 SSH 관리 액세스용으로 해당 계정을 활성화할 수 있습니다.

참고 로컬 및 외부 소스 모두에서 중복 사용자를 생성하지 마십시오. 중복 사용자 이름을 생성하는 경우, 이 사용자 이름에 동일한 권한 부여 권한이 있는지 확인하십시오. 로컬 사용자 계정에서 권한 부여 권한이 다른 경우에는 외부 버전 사용자 계정의 암호로는 로그인할 수 없고 로컬 암호로만 로그인할 수 있습니다. 권한이 동일한 경우, 사용하는 암호를 통해 외부 사용자와 로컬 사용자 중 어느 사용자로 로그인했는지 알 수 있습니다(암호가 서로 다르다고 가정함). 로컬 데이터베이스를 먼저 검사한다고 하더라도 로컬 데이터베이스에 사용자 이름이 있지만 암호가 올바르지 않을 경우, 외부 서버를 검사합니다. 외부 소스에 대한 암호가 올바른 경우에는 로그인에 성공합니다.

시작하기 전에

기대치를 적절하게 설정하려면 외부에서 정의한 사용자를 다음 동작에 알려주십시오.

- 외부 사용자가 처음 로그인하면 threat defense에서는 필수 구조를 생성합니다. 하지만 이와 동시에 사용자 세션을 생성할 수는 없습니다. 세션을 시작하려면 사용자는 다시 인증하기만 하면 됩니다. 사용자에게는 다음과 같은 메시지가 표시됩니다. "New external username identified(새 외부

사용자 이름이 식별됨). Please log in again to start a session(세션을 시작하려면 다시 로그인하십시오)."

- 이와 마찬가지로 Service-Type(서비스 유형)에 정의된 사용자의 권한 부여가 마지막 로그인 후 변경된 경우, 사용자는 다시 인증해야 합니다. 사용자에게는 다음과 같은 메시지가 표시됩니다. "Your authorization privilege has changed(귀하의 권한 부여 권한이 변경되었습니다). Please log in again to start a session(세션을 시작하려면 다시 로그인하십시오)."

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 후 **System Settings(**시스템 설정**)** > **Management Access(**관리 액세스**)** 링크를 클릭합니다.

System Settings(시스템 설정) 페이지가 이미 열려 있는 경우 목차에서 **Management Access(**관리 액세스**)**를 클릭하면 됩니다.

단계 **2** **AAA Configuration(AAA** 컨피그레이션**)** 탭을 아직 선택하지 않은 경우 클릭합니다.

단계 **3** **SSH Connection(SSH** 연결**)** 옵션을 다음과 같이 컨피그레이션합니다.

- **Server Group(**서버 그룹**)** - 기본 인증 소스로 사용할 RADIUS 서버 그룹 또는 로컬 사용자 데이터베이스(LocalIdentitySource)를 선택합니다. 외부 인증을 사용하려는 경우 RADIUS 서버 그룹을 선택해야 합니다.

  서버 그룹이 아직 없으면 **Create New RADIUS Server Group(**새 **RADIUS** 서버 그룹 생성**)** 링크를 클릭하여 지금 생성합니다. 각 서버에 대해 RADIUS 서버 개체도 생성하여 그룹에 추가해야 합니다. 하지만 이 작업은 서버 그룹을 정의할 때 수행할 수 있습니다. RADIUS에 대한 자세한 정보는 RADIUS 서버 및 그룹, 182 페이지의 내용을 참조하십시오.

  SSH 연결에서는 그룹에서만 첫 서버 2개를 사용한다는 점에 유의하십시오. 3개 이상의 서버에서 그룹을 사용하는 경우, 추가 서버는 시도되지 않습니다. 또한 **Dead Time(**비활성 시간**)** 및 **Maximum Failed Attempts(**최대 실패 시도**)** 그룹 속성은 사용되지 않습니다.

- **Authentication with LOCAL(**로컬로 인증**)** - 외부 서버 그룹을 선택하는 경우, 로컬 ID 소스를 사용하는 방법을 지정할 수 있습니다. SSH 액세스의 경우, 로컬 데이터베이스는 항상 외부 서버에 앞서 확인됩니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

Device Manager 사용자 세션 관리

Monitoring(모니터링**)** > **Sessions(**세션**)**를 선택하면 현재 device manager에 로그인되어 있는 사용자 목록을 확인할 수 있습니다. 목록에는 각 사용자가 현재 세션에 로그인되어 있었던 시간이 표시됩니다.

동일한 사용자 이름이 여러 번 표시되는 경우 해당 사용자가 각기 다른 소스 주소에서 세션을 연 것입니다. 사용자 이름과 소스 주소를 기준으로 하여 세션을 개별적으로 추적하며, 각 세션에는 고유한 타임스탬프가 있습니다.

시스템에서는 동시 사용자 세션 5개를 허용합니다. 6번째 사용자가 로그인하면 가장 오래된 현재 세션이 자동으로 로그아웃됩니다. 또한 20분 동안 아무 작업이 없으면 유휴 사용자는 자동으로 로그아웃됩니다.

device manager 사용자가 잘못된 비밀번호를 입력하고 3회 연속하여 로그인 시도에 실패할 경우, 5분 동안 사용자 어카운트가 잠깁니다. 사용자는 다시 로그인을 시도하기 전에 잠시 기다려야 합니다. device manager 사용자 어카운트의 잠금을 해제할 수 있는 방법은 없으며 재시도 횟수 또는 잠금 시간 제한을 조정할 수도 없습니다. SSH 사용자의 경우 이러한 설정을 조정하고 어카운트의 잠금을 해제할 수 있습니다.

필요한 경우 세션의 삭제 아이콘( )을 클릭하여 사용자 세션을 종료할 수 있습니다. 세션을 삭제하면 세션에서 로그아웃됩니다. 세션을 종료하는 경우의 잠금 기간은 없으며 사용자는 즉시 다시 로그인할 수 있습니다.

대기 HA 유닛에서 외부 사용자에 대한 Device Manager 액세스 활성화

device manager 사용자에 대한 외부 권한 부여를 컨피그레이션하는 경우, 해당 사용자는 고가용성 쌍의 활성 및 대기 유닛에 모두 로그인할 수 있습니다. 그러나 대기 유닛에 처음 로그인하려면 활성 유닛에 로그인하는 것에 비해 몇 가지 추가 단계가 필요합니다.

외부 사용자가 처음으로 활성 유닛에 로그인하면 시스템에서는 사용자 및 사용자의 액세스 권한을 정의하는 개체를 생성합니다. 이때 관리자 또는 읽기-쓰기 사용자는 대기 유닛에 표시할 사용자 개체에 대해 활성 유닛에서 컨피그레이션을 구축해야 합니다.

이러한 구축과 후속 컨피그레이션 동기화가 성공적으로 완료된 후에야 외부 사용자는 대기 유닛에 로그인할 수 있습니다.

관리자 및 읽기-쓰기 사용자는 활성 유닛에 로그인한 후 변경 사항을 구축할 수 있습니다. 그러나 읽기 전용 사용자는 컨피그레이션을 구축할 수 없습니다. 컨피그레이션을 구축하려면 적절한 권한이 있는 사용자에게 요청해야 합니다.

Threat Defense CLI용 로컬 사용자 계정 생성

threat defense 디바이스에서 CLI 액세스를 위한 사용자를 생성할 수 있습니다. 이 어카운트는 관리 애플리케이션에 대한 액세스는 허용하지 않으며 CLI에 대한 액세스만 허용합니다. CLI는 트러블슈팅 및 모니터링에 유용합니다.

로컬 사용자 계정은 한 번에 둘 이상의 디바이스에서 생성할 수 없습니다. 각 디바이스에는 일련의 고유 로컬 사용자 CLI 계정이 있습니다.

프로시저

단계 **1** config 권한이 있는 어카운트를 사용하여 디바이스 CLI에 로그인합니다.

관리자 사용자 어카운트는 필수 권한을 갖고 있지만, config 권한이 있는 모든 어카운트도 괜찮습니다. SSH 세션 또는 콘솔 포트를 사용할 수 있습니다.

특정 디바이스 모델의 경우, 콘솔 포트는 사용자를 FXOS CLI에 연결합니다. threat defense CLI로 이동하려면 **connect ftd** 명령을 사용하십시오.

단계 **2** 사용자 계정을 생성합니다.

configure user add *username* {**basic** | **config**}

다음 권한 레벨을 가진 사용자를 정의할 수 있습니다:

- **config**- 사용자에게 컨피그레이션 액세스 권한을 제공합니다. 이 명령은 사용자에게 모든 명령에 대한 전체 관리자 권한을 제공합니다.
- **basic**- 사용자에게 기본 액세스 권한을 제공합니다. 이 명령은 사용자가 컨피그레이션 명령을 입력하는 것을 허용하지 않습니다.

예제**:**

다음 예에서는 config 액세스 권한이 있는 joecool이라는 이름의 사용자 어카운트를 추가합니다. 입력하고 있으므로 비밀번호가 표시되지 않습니다.

```
> configure user add joecool config
Enter new password for user joecool: newpassword
Confirm new password for user joecool: newpassword
> show user
Login              UID   Auth Access  Enabled Reset    Exp Warn  Str Lock Max
admin             1000  Local Config  Enabled    No  Never  N/A  Dis   No N/A
joecool           1001  Local Config  Enabled    No  Never  N/A  Dis   No   5
```

참고 **configure password** 명령을 사용하여 암호를 변경할 수 있다고 사용자에게 알려주십시오.

단계 **3** (선택 사항). 보안 요건을 충족하도록 어카운트의 특성을 조정합니다.

다음 명령을 사용하여 기본 어카운트 동작을 변경할 수 있습니다.

- **configure user aging** *username max_days warn_days*

  사용자 비밀번호의 만료일을 설정합니다. 비밀번호가 유효한 최대 일수를 지정한 후 며칠 전부터 사용자에게 다가오는 만료일에 대해 경고할지 일수를 지정합니다. 두 값 모두 1~9999 범위이지만, 경고 일수는 최대 일수보다 작아야 합니다. 어카운트를 생성할 때 비밀번호 만료일이 없습니다.

- **configure user forcereset** *username*

  사용자가 다음 로그인 시 강제로 비밀번호를 변경하게 합니다.

- **configure user maxfailedlogins** *username number*

  어카운트를 잠그기 전에 허용되는 연속 실패 로그인의 최대 수를 1~9999 범위로 설정합니다. 계정의 잠금을 해제하려면 **configure user unlock** 명령을 사용하십시오. 새 어카운트에 대한 기본값은 로그인 5회 연속 실패입니다.

- **configure user minpasswdlen** *username number*

최소 비밀번호 길이를 1~127 범위로 설정합니다.

- **configure user strengthcheck** *username* {**enable** | **disable**}

  비밀번호 강도 검사를 활성화하거나 비활성화합니다. 이 경우 비밀번호를 변경할 때 사용자는 특정 비밀번호 기준을 충족해야 합니다. 사용자의 암호가 만료되거나 **configure user forcereset** 명령을 사용하는 경우, 이 요건은 사용자가 다음번 로그인할 때 자동으로 활성화됩니다.

단계 **4** 필요 시 사용자 어카운트를 관리합니다.

사용자가 자신의 어카운트를 잠글 수 있게 하거나, 어카운트를 제거하거나 다른 문제를 해결해야 합니다. 시스템에서 사용자 어카운트를 관리하려면 다음 명령을 사용합니다.

- **configure user access** *username* {**basic** | **config**}

  사용자 어카운트에 대한 권한을 변경합니다.

- **configure user delete** *username*

  지정된 어카운트를 삭제합니다.

- **configure user disable** *username*

  지정된 어카운트를 삭제하지 않고 비활성화합니다. 사용자는 어카운트를 활성화할 때까지 로그인할 수 없습니다.

- **configure user enable** *username*

  지정된 어카운트를 활성화합니다.

- **configure user password** *username*

  지정된 사용자에 대한 비밀번호를 변경합니다. 사용자는 일반적으로 **configure password** 명령을 사용하여 자신의 암호를 변경해야 합니다.

- **configure user unlock** *username*

  연속 실패 로그인 시도의 최대 횟수를 초과하므로 잠겨 있는 사용자 어카운트의 잠금을 해제합니다.

시스템 리부팅 또는 종료

필요한 경우 시스템을 리부팅하거나 종료할 수 있습니다.

아래 절차 외에, **reboot** 또는 **shutdown** 명령을 사용하여 SSH 세션 또는 device manager CLI 콘솔을 통해 이러한 작업을 수행할 수도 있습니다.

프로시저

단계 **1** 디바이스를 클릭한 다음, **System Settings(**시스템 설정**)** > **Reboot/Shutdown(**리부팅/종료**)** > 링크를 클릭합니다.

System Settings(시스템 설정) 페이지가 이미 열려 있는 경우 목차에서 **Reboot/Shutdown(**리부팅/종료**)**을 클릭하면 됩니다.

단계 **2** 필요한 기능을 수행하는 버튼을 클릭합니다.

- **Reboot(**리부팅**)** - 시스템이 올바르게 작동하지 않으며 문제를 해결하기 위한 다른 작업에 실패한 경우에는 디바이스를 리부팅할 수 있습니다. 또한 시스템 소프트웨어를 다시 로드하기 위해 디바이스를 리부팅하도록 요청하는 몇 가지 절차가 있을 수 있습니다.
- **Shut Down(**종료**)** - 전원을 제어되는 방식으로 끄려면 시스템을 종료합니다. 네트워크에서 디바이스를 제거하려는 경우(예: 교체하는 경우) 종료를 사용합니다. 디바이스를 종료한 후에는 하드웨어 On/Off(켜기/끄기) 스위치에서만 되돌릴 수 있습니다.

단계 **3** 작업이 완료될 때까지 기다립니다.

시스템이 리부팅되거나 종료되는 동안에는 device manager 또는 CLI에서 다른 작업을 수행할 수 없습니다.

리부팅이 완료되면 device manager 페이지가 새로 고침되며 로그인 페이지로 이동됩니다. 리부팅이 완료되기 전에 페이지를 새로 고치면 웹 브라우저에서는 해당 시점의 device manager 웹 서버의 작동 상태에 따라 503 또는 404 오류를 반환할 수 있습니다.

종료 시에는 시스템이 결국 전혀 응답할 수 없게 되며 404 오류가 발생합니다. 종료는 시스템을 완전히 끄는 것이기 때문에 이는 정상적인 결과입니다.

시스템 문제 해결

다음 항목에서는 일부 시스템 레벨 트러블슈팅 작업과 기능에 관해 설명합니다. 액세스 제어와 같은 특정 기능의 트러블슈팅에 대한 자세한 내용은 해당 기능 관련 장을 참조하십시오.

주소 **ping**을 통해 연결 테스트

ping은 특정 주소가 활성 상태이고 응답할 수 있는지 확인하는 간단한 명령입니다. 기본 연결이 작동 중인 것입니다. 그러나 디바이스에서 실행 중인 다른 정책 때문에 특정 트래픽 유형이 디바이스를 통과하지 못할 수도 있습니다. **ping** CLI 콘솔을 열거나 디바이스 CLI에 로그인하면 사용할 수 있습니다.

참고 시스템에는 여러 인터페이스가 있으므로 주소 ping에 사용되는 인터페이스를 제어할 수 있습니다. 중요한 연결을 테스트할 수 있도록 적절한 명령을 사용해야 합니다. 예를 들어 시스템에서는 가상 관리 인터페이스를 통해 Cisco 라이선스 서버에 연결할 수 있어야 하므로, **ping system** 명령을 사용하여 연결을 테스트해야 합니다. **ping**을 사용하는 경우에는 데이터 인터페이스를 통해 특정 주소에 연결할 수 있는지를 테스트하게 되므로 결과가 달라질 수도 있습니다.

일반 ping은 ICMP 패킷을 사용하여 연결을 테스트합니다. 네트워크에서 ICMP를 금지하는 경우에는 TCP ping을 대신 사용할 수 있습니다(데이터 인터페이스 ping에만 해당함).

IP 주소 또는 정규화된 호스트 이름(FQDN)을 ping할 수 있습니다. FQDN에서 ping이 작동하려면 관리 또는 데이터 인터페이스용으로 구성된 DNS 서버가 성공적으로 IP 주소를 반환해야 합니다. 관리 및 데이터 인터페이스에 대해 별도로 DNS 서버를 구성해야 합니다. 특정 인터페이스에 대해 DNS 서버가 구성되지 않은 경우 **dig** 명령을 사용하여 지정된 FQDN의 IP 주소를 조회합니다.

네트워크 주소 ping에 사용되는 주요 옵션은 다음과 같습니다.

가상 관리 인터페이스를 통해 주소 **ping**

ping system 명령을 사용하십시오.

ping system 호스트

호스트는 IP 주소일 수도 있고 www.example.com과 같은 FQDN(Fully-Qualified Domain Name)일 수도 있습니다. 데이터 인터페이스를 통해 수행하는 ping과는 달리 시스템 ping에는 기본 횟수가 없습니다. 즉, Ctrl+C를 사용하여 중지할 때까지 ping은 계속 실행됩니다. 예를 들면 다음과 같습니다.

```
> ping system www.cisco.com
PING origin-www.cisco.COM (72.163.4.161) 56(84) bytes of data.
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=1 ttl=242 time=10.6 ms
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=2 ttl=242 time=8.13 ms
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=3 ttl=242 time=8.51 ms
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=4 ttl=242 time=8.40 ms
^C
--- origin-www.cisco.COM ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 8.139/8.927/10.650/1.003 ms
>
```

라우팅 테이블을 사용하여 데이터 인터페이스를 통해 주소 **ping**

ping 명령을 사용하십시오. 이 경우 인터페이스를 지정하지 않고 시스템이 호스트에 대한 경로를 일반적으로 찾을 수 있는지를 테스트하게 됩니다. 시스템은 보통 이 방법을 통해 트래픽을 라우팅하므로 일반적으로 이 테스트를 수행하면 됩니다.

ping 호스트

예를 들면 다음과 같습니다.

```
> ping 171.69.38.1
Sending 5, 100-byte ICMP Echos to 171.69.38.1, timeout is 2 seconds:
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

참고 시간 제한, 반복 횟수, 패킷 크기 및 전송할 데이터 패턴을 지정할 수 있습니다. 사용 가능한 옵션을 확인하려면 CLI에서 도움말 표시기를 사용합니다.

특정 데이터 인터페이스를 통해 주소 **ping**

특정 데이터 인터페이스를 통한 연결을 테스트하려는 경우, **ping interface** *if_name* 명령을 사용합니다. 이 명령을 사용하여 진단 인터페이스를 지정할 수도 있지만, 가상 관리 인터페이스는 지정할 수 없습니다.

ping interface *if_name host*

예를 들면 다음과 같습니다.

```
> ping interface inside 171.69.38.1
Sending 5, 100-byte ICMP Echos to 171.69.38.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

TCP ping을 사용하여 데이터 인터페이스를 통해 주소 **ping**

ping tcp 명령을 사용하십시오. TCP ping은 SYN 패킷을 전송하며, 목적지에서 SYN-ACK 패킷을 전송하는 경우 ping에 성공한 것으로 간주합니다.

ping tcp [**interface** *if_name*] *host port*

호스트 및 TCP 포트를 지정해야 합니다.

원하는 경우 인터페이스(ping을 전송하는 데 사용할 인터페이스가 아닌 ping의 소스 인터페이스)를 지정할 수 있습니다. 이 ping 유형은 항상 라우팅 테이블을 사용합니다.

TCP ping은 SYN 패킷을 전송하며, 목적지에서 SYN-ACK 패킷을 전송하는 경우 ping에 성공한 것으로 간주합니다. 예를 들면 다음과 같습니다.

```
> ping tcp 10.0.0.1 21
Type escape sequence to abort.
No source specified. Pinging from identity interface.
Sending 5 TCP SYN requests to 10.0.0.1 port 21
from 10.0.0.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

참고 TCP ping의 시간 제한, 반복 횟수 및 소스 주소를 지정할 수도 있습니다. 사용 가능한 옵션을 확인하려면 CLI에서 도움말 표시기를 사용합니다.

호스트에 대한 경로 추적

어떤 IP 주소에 트래픽을 보내는 데 문제가 있을 경우 호스트까지의 경로를 추적하여 네트워크 경로에 문제가 있는지 확인할 수 있습니다. 경로 추적(traceroute)은 잘못된 포트의 UDP 패킷이나 ICMPv6 에코를 목적지로 전송하는 방식입니다. 이러한 패킷이나 에코를 목적지로 전송하는 과정에서 라우터는 ICMP 시간 초과 메시지로 응답하고 경로 추적에 해당 오류를 보고합니다. 각 노드는 3개의 패킷을 수신하므로 노드당 정보 결과를 가져올 수 있는 3번의 기회가 있습니다. **traceroute** CLI 콘솔을 열거나 디바이스 CLI에 로그인하면 사용할 수 있습니다.

참고 데이터 인터페이스(**traceroute**) 또는 가상 관리 인터페이스(**traceroute system**)를 통해 경로를 추적할 수 있는 별도의 명령이 있습니다. 경우에 따라 적절한 명령을 사용해야 합니다.

다음 표에는 출력에 표시될 수 있는 패킷별 결과에 대한 설명이 나와 있습니다.

출력 기호	설명
*	프로브에 대한 응답을 받지 못한 채 시간이 초과되었습니다.
nn msec	각 노드에서 지정된 수의 프로브가 왕복하는 데 걸린 시간(밀리초)입니다.
!N.	연결 불가한 ICMP 네트워크입니다.
!H	연결 불가한 ICMP 호스트입니다.
!P	ICMP 프로토콜에 연결할 수 없습니다.
!A	관리자가 ICMP를 금지했습니다.
?	알 수 없는 ICMP 오류입니다.

가상 관리 인터페이스를 통해 경로 추적

traceroute system 명령을 사용하십시오.

traceroute system *destination*

호스트는 IPv4/IPv6 주소일 수도 있고 www.example.com과 같은 FQDN(Fully Qualified Domain Name)일 수도 있습니다. 예를 들면 다음과 같습니다.

```
> traceroute system www.example.com
traceroute to www.example.com (172.163.4.161), 30 hops max, 60 byte packets
 1  192.168.0.254 (192.168.0.254)  0.213 ms  0.310 ms  0.328 ms
 2  10.88.127.1 (10.88.127.1)  0.677 ms  0.739 ms  0.899 ms
 3  lab-gw1.example.com (10.89.128.25)  0.638 ms  0.856 ms  0.864 ms
 4  04-bb-gw1.example.com (10.152.240.65)  1.169 ms  1.355 ms  1.409 ms
 5  wan-gw1.example.com (10.152.240.33)  0.712 ms  0.722 ms  0.790 ms
 6  wag-gw1.example.com (10.152.240.73)  13.868 ms  10.760 ms  11.187 ms
 7  rbb-gw2.example.com (172.30.4.85)  7.202 ms  7.301 ms  7.101 ms
 8  rbb-gw1.example.com (172.30.4.77)  8.162 ms  8.225 ms  8.373 ms
 9  sbb-gw1.example.com (172.16.16.210)  7.396 ms  7.548 ms  7.653 ms
10  corp-gw2.example.com (172.16.16.58)  7.413 ms  7.310 ms  7.431 ms
11  dmzbb-gw2.example.com (172.16.0.78)  7.835 ms  7.705 ms  7.702 ms
```

```
12  dmzdcc-gw2.example.com (172.16.0.190)  8.126 ms  8.193 ms  11.559 ms
13  dcz05n-gw1.example.com (172.16.2.106)  11.729 ms  11.728 ms  11.939 ms
14  www1.example.com (172.16.4.161)  11.645 ms  7.958 ms  7.936 ms
```

데이터 인터페이스를 통해 경로 추적

traceroute 명령을 사용하십시오.

traceroute *destination*

데이터 인터페이스에 대해 DNS 서버를 구성한 경우 호스트는 IPv4/IPv6 주소일 수도 있고 www.example.com과 같은 정규화된 호스트 이름(FQDN)일 수도 있습니다. 특정 인터페이스에 대해 DNS 서버가 구성되지 않은 경우 **dig** 명령을 사용하여 지정된 FQDN의 IP 주소를 조회합니다. 예를 들면 다음과 같습니다.

```
> traceroute 209.165.200.225
Tracing the route to 209.165.200.225
 1  10.83.194.1 0 msec 10 msec 0 msec
 2  10.83.193.65 0 msec 0 msec 0 msec
 3  10.88.193.101 0 msec 10 msec 0 msec
 4  10.88.193.97 0 msec 0 msec 10 msec
 5  10.88.239.9 0 msec 10 msec 0 msec
 6  10.88.238.65 10 msec 10 msec 0 msec
 7 172.16.7.221 70 msec 70 msec 80 msec
 8 209.165.200.225 70 msec 70 msec 70 msec
```

참고 시간 제한, TTL(Time to Live), 노드당 패킷 수 및 경로 추적의 출발지로 사용할 IP 주소나 인터페이스를 지정할 수 있습니다. 사용 가능한 옵션을 확인하려면 CLI에서 도움말 표시기를 사용합니다.

트레이스라우트(traceroute)에 Threat Defense 디바이스가 표시되도록 설정

기본적으로 threat defense 디바이스는 트레이스라우트에 홉으로 나타나지 않습니다. 디바이스를 표시하려면 디바이스를 통과하는 패킷에서 TTL(Time to Live)을 줄이고 ICMP 연결 불가 메시지의 속도 제한을 늘려야 합니다. 이렇게 하려면 필요한 서비스 정책 규칙과 기타 옵션을 구성하는 FlexConfig 개체를 생성해야 합니다.

서비스 정책 및 트래픽 클래스의 자세한 설명은 https://www.cisco.com/c/en/us/support/security/asa-firepower-services/products-installation-and-configuration-guides-list.html에서 제공되는 *Cisco ASA Series* 방화벽 컨피그레이션 가이드를 참조하십시오.

참고 TTL(time-to-live)을 줄이면 TTL이 1인 패킷이 삭제되지만, 연결이 더 큰 TTL이 있는 패킷을 포함할 수 있다는 가정하에 세션에 대한 연결이 열립니다. OSPF Hello 패킷과 같은 일부 패킷은 TTL 이 1로 전송되어 TTL을 줄이면 예기치 않은 결과가 발생할 수 있습니다. 트래픽 클래스를 정의할 때는 다음 사항을 고려하십시오.

프로시저

단계 **1** **Device(**디바이스**)** > **Advanced Configuration(**고급 컨피그레이션**)**에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

단계 **2** Advanced Configuration(고급 컨피그레이션) 목차에서 **FlexConfig** > **FlexConfig Objects(FlexConfig** 개체**)**를 클릭합니다.

단계 **3** TTL을 줄이는 개체를 생성합니다.

a) **+** 버튼을 클릭하여 새 개체를 생성합니다.

b) 개체의 이름을 입력합니다. 예를 들어 **Decrement_TTL**을 입력합니다.

c) **Template(**템플릿**)** 편집기에서 들여쓰기를 포함하여 다음 줄을 입력합니다.

```
icmp unreachable rate-limit 50 burst-size 1
policy-map global_policy
 class class-default
  set connection decrement-ttl
```

d) **Negate Template(**무효화 템플릿**)** 편집기에 이 컨피그레이션을 실행 취소하는 데 필요한 행을 입력합니다.

명령을 활성화하려면 상위 명령을 포함해 명령에 대해 정확한 하위 모드를 입력해야 하는 것과 마찬가지로, 무효화 템플릿에도 해당 명령을 포함해야 합니다.

무효화 템플릿은 이 개체를 정상적으로 구축한 후에 FlexConfig 정책에서 제거하는 경우에 적용되며, 실패한 구축 중에도 컨피그레이션을 이전 상태로 재설정하기 위해 적용됩니다.

그러므로 이 예시에서 무효화 템플릿은 다음과 같습니다.

```
no icmp unreachable rate-limit 50 burst-size 1
policy-map global_policy
 class class-default
  no set connection decrement-ttl
```

e) **OK(**확인**)**를 클릭하여 개체를 저장합니다.

단계 **4** FlexConfig 정책에 개체를 추가합니다.

FlexConfig 정책에서 선택한 개체만 구축됩니다.

a) 목차에서 **FlexConfig Policy(FlexConfig** 정책**)**를 클릭합니다.

b) Group List(그룹 목록)에서 **+**를 클릭합니다.

c) Decrement_TTL 개체를 선택하고 **OK(**확인**)**를 클릭합니다.

템플릿의 명령으로 미리보기가 업데이트됩니다. 올바른 명령이 표시되는지 확인합니다.

d) **Save(**저장**)**를 클릭합니다.

이제 정책을 구축할 수 있습니다.

NTP 트러블슈팅

시스템은 시스템이 올바르게 작동하고 이벤트 및 기타 데이터 포인트가 정확하게 처리되도록 정확하고 일관된 시간을 사용합니다. 시스템에서 항상 신뢰할 수 있는 시간 정보를 유지하려면 1개 이상의 NTP(Network Time Protocol) 서버(이상적으로는 3개)를 구성해야 합니다.

디바이스 요약 연결 다이어그램(기본 메뉴에서 **Device(**디바이스**)** 클릭)은 NTP 서버에 대한 연결 상태를 보여줍니다. 이 상태가 노란색 또는 주황색인 경우, 구성된 서버에 연결하는 데 문제가 있는 것입니다. 연결 문제가 지속될 경우(일시적인 문제가 아님), 다음을 수행하십시오.

- **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **NTP**에서 3개 이상의 NTP 서버를 구성합니다. 이것은 요건은 아니지만 3개 이상의 NTP 서버가 있는 경우 신뢰성이 매우 향상됩니다.
- **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Management Interface(**관리 인터페이스**)**에 정의되어 있는 관리 인터페이스 IP 주소와 NTP 서버 간의 네트워크 경로가 있는지 확인합니다.
  - 관리 인터페이스 게이트웨이가 데이터 인터페이스인 경우, 기본 경로가 적절하지 않으면 **Device(**디바이스**)** > **Routing(**라우팅**)**에서 NTP 서버에 대한 고정 경로를 구성할 수 있습니다.
  - 명시적 관리 인터페이스 게이트웨이를 설정한 경우, 디바이스 CLI에 로그인하고 **ping system** 명령을 사용하여 각 NTP 서버에 대한 네트워크 경로가 있는지 테스트합니다.
- 디바이스 CLI에 로그인하고 다음 명령을 사용하여 NTP 서버의 상태를 확인합니다.
  - **show ntp**— 이 명령은 NTP 서버와 가용성에 대한 기본 정보를 표시합니다. 단, device manager의 연결 상태는 상태를 나타내는 추가 정보를 사용합니다. 따라서 이 명령이 표시하는 항목과 연결 상태 다이어그램이 표시하는 항목 간에 불일치가 있을 수 있습니다. 이 명령은 CLI 콘솔에서도 실행할 수 있습니다.
  - **system support ntp** - 이 명령에는 **show ntp**의 출력과 함께 표준 NTP 명령인 **ntpq**의 출력(NTP 프로토콜에 문서화됨)도 포함됩니다. NTP 동기화를 확인해야 하는 경우 이 명령을 사용합니다.

    'ntpq -pn 결과' 섹션을 검색합니다. 예를 들면 다음과 같은 내용이 표시될 수 있습니다.

```
Results of 'ntpq -pn'
remote                    : +216.229.0.50
refid                     : 129.7.1.66
st                        : 2
t                         : u
when                      : 704
poll                      : 1024
reach                     : 377
delay                     : 90.455
offset                    : 2.954
jitter                    : 2.473
```

    이 예에서 NTP 서버 주소 앞에 있는 +는 잠재적인 후보임을 나타냅니다. 여기에서 별표 *는 현재 시간 소스 피어를 나타냅니다.

    NTPD(NTP 데몬)에서는 각 피어의 8개의 샘플로 구성된 슬라이딩 창을 사용하고 하나의 샘플을 선택하며, 클럭 선택에 따라 올바른 차이머와 잘못된 티커가 결정됩니다. 그런 다음 NTPD에서는 왕복 거리(후보의 오프셋은 왕복 지연의 1/2을 초과하지 않아야 함)를 결정합

니다. 연결 지연, 패킷 손실 또는 서버 문제로 인해 하나 또는 모든 후보가 거부되는 경우, 동기화 시 지연이 길어지며 조정에도 매우 긴 시간이 소요됩니다. 클럭 오프셋과 오실레이터 오류는 클럭 규칙 알고리즘으로 해결해야 하며 이 작업에는 몇 시간이 걸릴 수 있습니다.

참고 refid가 .LOCL인 경우, 이는 피어가 규칙이 없는 로컬 시계임을 나타냅니다. 즉, 시간을 설정하기 위해 로컬 시계만 사용하는 것을 의미합니다. 선택한 피어가 .LOCL인 경우 device manager는 항상 동기화되지 않은 NTP 연결을 노란색으로 표시합니다. 일반적으로, NTP는 더 나은 후보를 사용할 수 있는 경우 .LOCL 후보를 선택하지 않으므로 3개 이상의 서버를 구성해야 합니다.

관리 인터페이스용 **DNS** 문제 해결

관리 인터페이스에서 사용할 DNS 서버를 하나 이상 설정해야 합니다. 이 서버는 스마트 라이선싱, 데이터베이스 업데이트(예: GeoDB, 규칙 및 VDB), 그리고 도메인 이름을 확인해야 하는 기타 작업 등의 서비스에 대한 클라우드 연결용으로 필요합니다.

DNS 서버를 구성하는 과정은 비교적 간단합니다. 디바이스를 처음 구성할 때 사용하는 DNS 서버의 IP 주소만 입력하면 됩니다. 해당 IP 주소는 나중에 **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **DNS Server(DNS** 서버**)** 페이지에서 변경할 수 있습니다.

그러나 시스템은 네트워크 연결 문제 또는 DNS 서버 자체의 문제로 인해 FQDN(Fully Qualified Domain Name)을 확인하지 못할 수 있습니다. 시스템에서 DNS 서버를 사용할 수 없는 경우 문제 식별 및 해결을 위한 다음 작업을 고려하십시오. 일반 DNS 문제 문제 해결, 829 페이지도 참조하십시오.

프로시저

단계 **1** 문제가 있는지 확인합니다.

a) SSH를 사용하여 디바이스 CLI에 로그인합니다.

b) **ping system www.cisco.com**을 입력합니다. 다음과 같은 "unknown host(알 수 없는 호스트)" 메시지가 표시되는 경우 시스템이 도메인 이름을 확인할 수 없는 것입니다. ping이 성공하는 경우에는 확인이 완료되었으며 DNS가 작동 중인 것입니다. ping을 중지하려면 Ctrl+C를 누릅니다.

```
> ping system www.cisco.com
ping: unknown host www.cisco.com
```

참고 중요한 것은 **ping** 명령에 **system** 키워드가 포함되어야 한다는 것입니다. **system** 키워드에서는 관리 IP 주소(관리 DNS 서버를 사용하는 유일한 인터페이스)를 통해 ping을 전송합니다. www.cisco.com에 대해 ping을 실행하는 것도 유용한 옵션입니다. 스마트 라이선싱 및 업데이트를 수행하려면 해당 서버로의 경로가 필요하기 때문입니다.

단계 **2** 관리 인터페이스의 컨피그레이션을 확인합니다.

a) **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Management Interface(**관리 인터페이스**)** 다음을 확인합니다. 변경을 수행하는 경우 **Save(**저장**)**를 클릭하면 변경 사항이 즉시 적용됩니다. 관리 주소를 변경하는 경우 다시 연결하여 다시 로그인해야 합니다.

- 관리 네트워크에 대한 게이트웨이 IP 주소가 정확합니다. 게이트웨이로 데이터 인터페이스를 사용 중이라면 후속 단계에서는 해당 컨피그레이션을 확인합니다.
- 게이트웨이로 데이터 인터페이스를 사용하고 있지 않다면 관리 IP 주소/서브넷 마스크와 게이트웨이 IP 주소가 같은 서브넷에 있는지 확인합니다.

b) 이렇게 하려면 **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **DNS Server(DNS** 서버**)**를 클릭하고 올바른 DNS 서버가 구성되어 있는지 확인합니다.

네트워크 에지에서 디바이스를 구축하는 경우 사용 가능한 DNS 서버에 대한 서비스 제공자의 특정 요구 사항이 있을 수 있습니다.

c) 게이트웨이로 데이터 인터페이스를 사용 중이라면 필요한 경로가 있는지 확인합니다.

0.0.0.0의 경우 기본 경로가 필요합니다. 기본 경로에 대해 게이트웨이를 통해 DNS 서버를 사용할 수 없는 경우에는 추가 경로가 필요할 수 있습니다. 기본적으로 발생 가능한 상황은 다음의 두 가지입니다.

- DHCP를 사용하여 외부 인터페이스의 주소를 가져오는 경우 **Obtain Default Route using DHCP(DHCP**를 사용하여 기본 경로 얻기**)** 옵션을 선택했다면 device manager에 기본 경로가 표시되지 않습니다. SSH에서 **show route**(을)를 입력하고 0.0.0.0에 대한 경로가 있는지 확인합니다. 이 컨피그레이션은 외부 인터페이스의 기본 컨피그레이션이므로 기본적으로는 이 상황이 발생할 가능성이 높습니다. 외부 인터페이스의 컨피그레이션을 확인하려면 **Device(**디바이스**)** > **Interfaces(**인터페이스**)**로 이동합니다.
- 외부 인터페이스에서 고정 IP 주소를 사용 중이거나 DHCP에서 기본 경로를 얻지 않는 경우에는 **Device(**디바이스**)** > **Routing(**라우팅**)**을 엽니다. 기본 경로에 대해 정확한 게이트웨이를 사용하고 있는지 확인합니다.

기본 경로를 통해 DNS 서버에 연결할 수 없는 경우에는 **Routing(**라우팅**)** 페이지에서 해당 서버로의 정적 경로를 정의해야 합니다. 직접 연결된 네트워크(시스템의 데이터 인터페이스에 직접 연결된 네트워크)의 경우에는 경로를 추가하면 안 됩니다. 시스템은 해당 네트워크로 자동 라우팅할 수 있기 때문입니다.

또한 잘못된 인터페이스를 통해 서버로 트래픽을 잘못 전송하는 정적 경로가 없는지도 확인합니다.

d) 구축 버튼에 구축하지 않은 변경 사항이 있음이 표시되는 경우 지금 구축하고 구축이 완료될 때까지 기다립니다.

e) **ping system www.cisco.com**을 다시 테스트합니다. 문제가 계속 발생하면 다음 단계로 계속 진행합니다.

단계 **3** SSH 세션에서 **dig www.cisco.com**을 입력합니다.

- **dig** 실행 시 DNS 서버에서 응답을 받았음을 표시하는데 서버가 이름을 찾을 수 없는 경우, DNS는 정확하게 컨피그레이션되어 있지만 사용 중인 DNS 서버에 FQDN의 주소가 없는 것입니다. 이 오류는 NXDOMAIN 상태로 표시됩니다. 응답은 다음과 같이 표시됩니다.

```
> dig www.cisco.com

; <<>> DiG 9.11.4 <<>> www.cisco.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 43246
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
; COOKIE: 78b1c6b2b3ef5b689fc2f65260db9e9b36a7d9fefb301943 (good)
;; QUESTION SECTION:
;www.cisco.com.                 IN      A

;; AUTHORITY SECTION:
.                       3600    IN      SOA     a.root-servers.net.
nstld.verisign-grs.com. 2021062901 1800 900 604800 86400

;; Query time: 13 msec
;; SERVER: 10.163.47.11#53(10.163.47.11)
;; WHEN: Tue Jun 29 22:28:43 UTC 2021
;; MSG SIZE  rcvd: 145
```

  해결 방법: 이 경우 다른 DNS 서버를 구성하거나 확인해야 하는 FQDN을 확인할 수 있도록 현재 DNS 서버를 업데이트해야 합니다. 네트워크 관리자나 ISP와 협의하여 네트워크에 대해 작동하는 DNS 서버의 IP 주소를 얻으십시오.

- 연결 시간 초과가 발생한 경우 시스템이 DNS 서버에 연결할 수 없거나, 모든 DNS 서버가 현재 중단되어 응답하지 않는 것입니다(가능성은 낮음). 다음 단계를 계속합니다.

단계 **4** **traceroute system** *DNS_server_ip_address* 명령을 사용하여 DNS 서버로의 경로를 추적합니다.

예를 들어 DNS 서버가 10.100.10.1인 경우 다음 명령을 입력합니다.

```
> traceroute system 10.100.10.1
```

발생 가능한 결과는 다음과 같습니다.

- traceroute가 완료되고 DNS 서버에 연결됩니다. 이 경우 DNS 서버로의 경로가 실제로 있으며 시스템이 DNS 서버에 연결할 수 있는 것입니다. 따라서 라우팅 문제는 없습니다. 하지만 이 서버에 대한 DNS 요청에서 응답은 수신되지 않습니다.

  해결 방법: 경로 내에 있는 라우터나 방화벽이 UDP/53(DNS에 사용되는 포트) 트래픽을 삭제하고 있을 수 있습니다. 다른 네트워크 경로에서 DNS 서버에 연결해 볼 수 있습니다. 트래픽을 차단하는 노드를 확인한 다음 시스템 관리자와 협의하여 액세스 규칙을 변경해야 하므로, 이 문제는 해결하기가 어렵습니다.

- traceroute가 어떤 노드에도 연결할 수 없습니다. 이 경우 결과는 다음과 같이 표시됩니다.

```
> traceroute system 10.100.10.1
traceroute to 10.100.10.1 (10.100.10.1), 30 hops max, 60 byte packets
```

```
 1  * * *
 2  * * *
 3  * * *
(and so forth)
```

해결 방법: 이 경우에는 시스템 내에 라우팅 문제가 있는 것입니다. 게이트웨이 IP 주소에 **ping system**을 실행해 보십시오. 이전 단계에서 설명한 것처럼 관리 인터페이스의 컨피그레이션을 다시 확인하여 필요한 게이트웨이와 경로가 구성되어 있는지 확인합니다.

- traceroute가 노드 몇 개를 통과한 후 경로를 더 이상 확인하지 못합니다. 이 경우 결과는 다음과 같이 표시됩니다.

```
> traceroute system 10.100.10.1
traceroute to 10.100.10.1 (10.100.10.1), 30 hops max, 60 byte packets
 1  192.168.0.254 (192.168.0.254)  0.475 ms  0.532 ms  0.542 ms
 2  10.88.127.1 (10.88.127.1)  0.803 ms  1.434 ms  1.443 ms
 3  site04-lab-gw1.example.com (10.89.128.25)  1.390 ms  1.399 ms  1.435 ms
 4  * * *
 5  * * *
 6  * * *
```

해결 방법: 이 경우에는 마지막 노드에서 라우팅에 장애가 발생하는 것입니다. 그러므로 시스템 관리자와 협의하여 해당 노드에 정확한 경로를 설치해야 할 수 있습니다. 그러나 해당 노드를 통과하여 DNS 서버에 연결하는 경로를 의도적으로 삭제한 경우에는 게이트웨이를 변경하거나 DNS 서버로 트래픽을 라우팅할 수 있는 라우터를 가리키도록 정적 경로를 직접 생성해야 합니다.

CPU 및 메모리 사용량 분석

CPU 및 메모리 사용량에 대한 시스템 레벨 정보를 보려면 **Monitoring(**모니터링**)** > **System(**시스템**)**을 선택하고 CPU 및 메모리 막대 그래프를 찾습니다. 이 그래프에는 CLI에서 **show cpu system** 및 **show memory system** 명령을 사용해 수집한 정보가 표시됩니다.

CLI 콘솔을 열거나 CLI에 로그인하면 이러한 명령의 추가 버전을 사용하여 다른 정보를 확인할 수 있습니다. 일반적으로는 사용량과 관련하여 지속적인 문제가 발생하는 경우나 Cisco TAC(Technical Assistance Center)의 지침이 있는 경우에만 이 정보를 확인하면 됩니다. 자세한 정보는 대부분 복잡하므로 TAC의 해석이 필요합니다.

검사할 수 있는 몇 가지 주요 정보는 다음과 같습니다. 이러한 명령에 대한 자세한 내용은 http://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.html의 Cisco Firepower Threat Defense 명령 참조에서 확인할 수 있습니다.

- **show cpu** 데이터 플레인 CPU 사용률을 표시합니다.
- **show cpu core** 각 CPU 코어의 사용량을 개별적으로 표시합니다.
- **show cpu detailed** 코어당/전체 데이터 플레인 CPU 사용량을 추가로 표시합니다.
- **show memory** 데이터 플레인 메모리 사용량을 표시합니다.

참고 위에 나와 있지 않은 일부 키워드의 경우 **cpu** 또는 **memory** 명령을 사용하여 프로파일링 또는 기타 기능을 먼저 설정해야 합니다. 이러한 기능은 TAC 지침에 따라 사용하십시오.

로그 보기

시스템은 다양한 작업에 대한 정보를 로깅합니다. **system support view-files** 명령을 사용하여 시스템 로그를 열 수 있습니다. Cisco TAC(Technical Assistance Center)와 작업할 때 이 명령을 사용하면 TAC에서 출력 해석을 지원할 수 있으며 확인해야 하는 적절한 로그를 선택할 수 있습니다.

이 명령을 실행하면 로그 선택을 위한 메뉴가 표시됩니다. 다음 명령을 사용하여 마법사를 탐색합니다.

- 하위 디렉터리로 변경하려면 디렉터리의 이름을 입력하고 Enter 키를 누릅니다.
- 볼 파일을 선택하려면 프롬프트에서 **s**를 입력합니다. 그러면 파일 이름을 입력하라는 메시지가 표시됩니다. 대소문자를 구분하여 전체 이름을 입력해야 합니다. 파일 목록에는 로그의 크기가 표시됩니다. 매우 큰 로그의 경우 열기 전에 크기를 고려해야 합니다.
- --More(자세히)--가 표시될 때 스페이스바를 누르면 다음 로그 항목 페이지가 표시되고 Enter 키를 누르면 다음 로그 항목만 표시됩니다. 로그의 끝에 도달하면 메인 메뉴로 이동됩니다. --More(자세히)-- 줄에는 로그의 크기와 로그를 확인한 빈도가 표시됩니다. 전체 로그 페이지를 확인하지 않으려는 경우 **Ctrl+C**를 사용하여 로그를 닫고 명령을 종료합니다**.**
- 메뉴의 구조에서 한 레벨 위로 이동하려면 **b**를 입력합니다.

새로 추가되는 메시지를 확인할 수 있도록 로그를 열어 두려면 **system support view-files** 대신 **tail-logs** 명령을 사용합니다.

다음 예에서는 시스템 로그인 시도를 추적하는 cisco/audit.log 파일을 확인하는 방법을 보여줍니다. 파일 목록은 맨 위의 디렉터리에서 시작되며, 그 아래에는 현재 디렉터리의 파일 목록이 표시됩니다.

```
> system support view-files

===View Logs===

============================
Directory: /ngfw/var/log
----------sub-dirs----------
cisco
mojo
removed_packages
setup
connector
sf
scripts
packages
removed_scripts
httpd
-----------files------------
2016-10-14 18:12:04.514783 | 5371       | SMART_STATUS_sda.log
2016-10-14 18:12:04.524783 | 353        | SMART_STATUS_sdb.log
```

```
2016-10-11 21:32:23.848733 | 326517     | action_queue.log
2016-10-06 16:00:56.620019 | 1018       | br1.down.log

<list abbreviated>


([b] to go back or [s] to select a file to view, [Ctrl+C] to exit)
Type a sub-dir name to list its contents: cisco

============================
Directory: /ngfw/var/log/cisco
-----------files------------
2017-02-13 22:44:42.394907 | 472        | audit.log
2017-02-13 23:40:30.858198 | 903615     | ev_stats.log.0
2017-02-09 18:14:26.870361 | 0          | ev_stats.log.0.lck
2017-02-13 05:24:00.682601 | 1024338    | ev_stats.log.1
2017-02-12 08:41:00.478103 | 1024338    | ev_stats.log.2
2017-02-11 11:58:00.260805 | 1024218    | ev_stats.log.3
2017-02-09 18:12:13.828607 | 95848      | firstboot.ngfw-onbox.log
2017-02-13 23:40:00.240359 | 6523160    | ngfw-onbox.log

([b] to go back or [s] to select a file to view, [Ctrl+C] to exit)
Type a sub-dir name to list its contents: s

Type the name of the file to view ([b] to go back, [Ctrl+C] to exit)
> audit.log
2017-02-09 18:59:26 - SubSystem:LOGIN, User:admin, IP:10.24.42.205, Message:Login successful,

2017-02-13 17:59:28 - SubSystem:LOGIN, User:admin, IP:10.24.111.72, Message:Login successful,

2017-02-13 22:44:36 - SubSystem:LOGIN, User:admin, IP:10.24.111.72, Message:Login failed,
2017-02-13 22:44:42 - SubSystem:LOGIN, User:admin, IP:10.24.111.72, Message:Login successful,

2017-02-13 22:44:42 - SubSystem:LOGIN, User:admin, IP:10.24.111.72, Message:Unlocked account.,


<remaining log truncated>
```

트러블슈팅 파일 생성

문제 보고서를 제출할 때는 Cisco TAC(Technical Assistance Center) 담당자가 시스템 로그 정보 제출을 요청할 수 있습니다. 담당자는 이 정보를 통해 문제를 보다 쉽게 진단할 수 있습니다. 별도의 요청이 없으면 진단 파일을 제출하지 않아도 됩니다.

다음 절차에서는 진단 파일을 생성하고 다운로드하는 방법을 설명합니다.

프로시저

단계 **1** 디바이스를 클릭합니다.

단계 **2** **Troubleshooting(**트러블슈팅**)**에서 **Request file to be Created(**파일 생성 요청**)** 또는 **Re-Request File to be Created(**파일 생성 재요청**)**(이전에 파일 생성을 요청한 경우)를 클릭합니다.

시스템에서 진단 파일 생성이 시작됩니다. 다른 페이지로 이동했다가 돌아와서 상태를 확인할 수 있습니다. 파일이 준비되면 파일 생성 날짜와 시간이 다운로드 버튼과 함께 표시됩니다.

단계 **3** 파일이 준비되면 다운로드 버튼을 클릭합니다.

브라우저 표준 다운로드 방법을 통해 파일이 워크스테이션에 다운로드됩니다.

일반적이지 않은 관리 작업

다음 항목에서는 수행하더라도 자주 수행하지는 않는 작업에 관해 설명합니다. 이러한 모든 작업을 수행하면 디바이스 컨피그레이션이 지워집니다. 이러한 변경을 수행하기 전에 디바이스가 현재 프로덕션 네트워크에 중요한 서비스를 제공하고 있지 않은지 확인합니다.

방화벽 모드 변경

threat defense 방화벽은 라우팅 모드 또는 투명 모드에서 실행될 수 있습니다. 라우팅 모드 방화벽은 라우팅 홉이며, 해당 스크린드 서브넷 중 하나에 연결되는 호스트의 기본 게이트웨이 역할을 수행합니다. 이와 반대로 투명 방화벽은 "비활성 엔드포인트(bump in the wire)" 또는 "은폐형 방화벽(stealth firewall)" 같은 역할을 수행하는 레이어 2 방화벽이며, 연결된 디바이스에 대한 라우터 홉으로 표시되지 않습니다.

로컬 device manager는 라우팅 모드만 지원합니다. 그러나 투명 모드에서 디바이스를 실행해야 하는 경우에는 방화벽 모드를 변경하고 management center를 사용하여 디바이스 관리를 시작할 수 있습니다. 반면 투명 모드 디바이스는 라우팅 모드로 변환할 수 있으며, 그 후에는 로컬 관리자를 사용하여 해당 디바이스를 구성할 수 있습니다. management center를 사용하여 라우팅 모드 디바이스를 관리할 수도 있습니다.

로컬 또는 원격 관리와 관계없이 모드를 변경하려면 디바이스 CLI를 사용해야 합니다.

다음 절차에서는 로컬 관리자를 사용 중이거나 사용하려는 경우 모드를 변경하는 방법을 설명합니다.

⚠

주의 방화벽 모드를 변경하면 디바이스 컨피그레이션이 지워지며 시스템이 기본 컨피그레이션으로 돌아갑니다. 그러나, 관리 IP 주소 및 호스트 이름은 유지됩니다.

시작하기 전에

투명 모드로 변환하는 경우 방화벽 모드를 변경하기 전에 management center를 설치합니다.

기능 라이선스를 활성화한 경우에는 로컬 관리자를 삭제하고 원격 관리로 전환하기 전에 device manager에서 해당 라이선스를 비활성화해야 합니다. 이렇게 하지 않으면 해당 라이선스는 Cisco Smart Software Manager에서 디바이스에 할당된 상태로 유지됩니다. 선택 가능한 라이선스 활성화 또는 비활성화, 98 페이지의 내용을 참조하십시오.

디바이스가 고가용성으로 컨피그레이션된 경우에는 먼저 디바이스 관리자(사용 가능한 경우) 또는 **configure high-availability disable** 명령을 사용하여 고가용성 컨피그레이션을 해제해야 합니다. 액티브 유닛에서 HA를 해제하는 것이 가장 좋습니다.

프로시저

단계 **1** SSH 클라이언트를 사용하여 관리 **IP** 주소에 대한 연결을 열고 구성 CLI 액세스 권한이 있는 사용자 이름으로 디바이스 CLI에 로그인합니다. 예를 들어 관리자 사용자 이름을 사용합니다.

관리 IP 주소에 연결되어 있는 동안에는 이 프로세스를 따라야 합니다. device manager를 사용할 때는 데이터 인터페이스의 IP 주소를 통해 디바이스를 관리할 수 있습니다. 그러나 디바이스를 원격으로 관리하려면 관리 물리적 포트 및 관리 IP 주소를 사용해야 합니다.

관리 IP 주소에 연결할 수 없는 경우에는 다음 작업을 수행합니다.

- 관리 물리적 포트가 작동하는 네트워크에 유선 연결되어 있는지 확인합니다.
- 관리 네트워크에 대해 관리 IP 주소 및 게이트웨이가 구성되어 있는지 확인합니다. device manager의 **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Management Interface(**관리 인터페이스**)** 에서 주소와 게이트웨이를 구성합니다. (CLI에서는 **configure network ipv4/ipv6 manual** 명령을 사용하십시오.)

  참고 관리 IP 주소에 대해 외부 게이트웨이를 사용하고 있는지 확인합니다. 원격 관리자를 사용할 때는 데이터 인터페이스를 게이트웨이로 사용할 수 없습니다.

단계 **2** 라우팅 모드에서 투명 모드로 변경하고 원격 관리를 사용하려면 다음을 수행합니다.

a) 로컬 관리를 비활성화하고 관리자 모드로 진입하지 않습니다.

활성 관리자가 있으면 방화벽 모드를 변경할 수 없습니다. 관리자를 제거하려면 **configure manager delete** 명령을 사용합니다.

```
> configure manager delete
If you enabled any feature licenses, you must disable them in
Firepower Device Manager before deleting the local manager.
Otherwise, those licenses remain assigned to the device in
Cisco Smart Software Manager.
Do you want to continue[yes/no] yes
Deleting task list
Manager successfully deleted.

>
> show managers
No managers configured.
```

b) 방화벽 모드를 투명으로 변경합니다.

configure firewall transparent

예제:

```
> configure firewall transparent
This will destroy the current interface configurations,
are you sure that you want to proceed? [y/N] y
The firewall mode was changed successfully.
```

c) 원격 관리자를 구성합니다.

configure manager add {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} *regkey* [*nat_id*]

여기서 각 항목은 다음을 나타냅니다.

- {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**}에서는 이 디바이스를 관리하는 management center의 DNS 호스트 이름이나 IP 주소(IPv4 또는 IPv6)를 지정합니다. management center의 주소를 직접 지정할 수 없으면 **DONTRESOLVE**(을)를 사용합니다. **DONTRESOLVE**(을)를 사용하는 경우 *nat_id*가 필요합니다.
- *regkey*는 디바이스를 management center에 등록하는 데 필요한 고유 영숫자 등록 키입니다.
- *nat_id*는 management center와 장치 간의 등록 프로세스 동안 사용되는 선택적인 영숫자 문자열입니다. 호스트 이름을 DONTRESOLVE로 설정하는 경우 반드시 필요합니다.

예를 들어 등록 키 **secret**을 사용하여 192.168.0.123에서 관리자를 사용하려면 다음과 같이 입력합니다.

```
> configure manager add 192.168.0.123 secret
Manager successfully configured.
Please make note of reg_key as this will be required while adding
Device in FMC.

> show managers
Host                    : 192.168.0.123
Registration Key        : ****
Registration            : pending
RPC Status              :
```

d) management center에 로그인하여 디바이스를 추가합니다.

자세한 내용은 management center 온라인 도움말을 참조하십시오.

단계 **3** 투명 모드에서 라우팅 모드로 변경하고 로컬 관리로 변환하려면 다음을 수행합니다.

a) management center에서 디바이스를 등록 취소합니다.

b) threat defense 디바이스 CLI에 액세스합니다. 콘솔 포트에서 액세스하는 것이 좋습니다.

모드를 변경하면 컨피그레이션이 지워지므로 관리 IP 주소는 기본값으로 되돌아갑니다. 따라서 모드를 변경한 후에는 관리 IP 주소에 대한 SSH 연결이 끊길 수 있습니다.

c) 방화벽 모드를 라우팅으로 변경합니다.

configure firewall routed

예제**:**

```
> configure firewall routed
This will destroy the current interface configurations,
are you sure that you want to proceed? [y/N] y
The firewall mode was changed successfully.
```

d) 로컬 관리자를 활성화합니다.

configure manager local

예를 들면 다음과 같습니다.

```
> configure manager local
Deleting task list

> show managers
Managed locally.
```

이제 웹 브라우저를 사용하여 **https://***management-IP-address*에서 로컬 관리자를 열 수 있습니다.

컨피그레이션 재설정

컨피그레이션을 처음부터 다시 시작하려는 경우 시스템 컨피그레이션을 공장 기본값으로 재설정할 수 있습니다. 컨피그레이션을 직접 재설정할 수는 없지만 관리자를 삭제했다가 추가하면 컨피그레이션이 지워집니다.

컨피그레이션을 지우고 백업을 복구하려는 경우에는 복원할 백업 복사본을 이미 다운로드한 상태여야 합니다. 시스템을 재설정한 후에 백업을 복원할 수 있도록 해당 복사본을 업로드해야 합니다.

시작하기 전에

기능 라이선스를 활성화한 경우에는 로컬 관리자를 삭제하기 전에 device manager에서 해당 라이선스를 비활성화해야 합니다. 이렇게 하지 않으면 해당 라이선스는 Cisco Smart Software Manager에서 디바이스에 할당된 상태로 유지됩니다. 선택 가능한 라이선스 활성화 또는 비활성화, 98 페이지의 내용을 참조하십시오.

장치가 고가용성으로 구성된 경우에는 먼저 device manager(사용 가능한 경우) 또는 **configure high-availability disable** 명령을 사용하여 고가용성 구성을 해제해야 합니다. 액티브 유닛에서 HA를 해제하는 것이 가장 좋습니다.

프로시저

단계 **1** SSH 클라이언트를 사용하여 관리 IP 주소에 대한 연결을 열고 컨피그레이션 CLI 액세스 권한이 있는 사용자 이름으로 디바이스 CLI에 로그인합니다. 예를 들어 관리자 사용자 이름을 사용합니다.

단계 **2** 관리자를 제거하려면 **configure manager delete** 명령을 사용합니다.

```
> configure manager delete
If you enabled any feature licenses, you must disable them in
Device Manager before deleting the local manager.
Otherwise, those licenses remain assigned to the device in Cisco
Smart Software Manager.
Do you want to continue[yes/no] yes
Deleting task list
Manager successfully deleted.

>
> show managers
No managers configured.
```

단계 **3** 로컬 관리자를 구성합니다.

configure manager local

예를 들면 다음과 같습니다.

```
> configure manager local
Deleting task list

> show managers
Managed locally.
```

이제 웹 브라우저를 사용하여 **https://***management-IP-address*에서 로컬 관리자를 열 수 있습니다. 컨피그레이션을 지우면 디바이스 설정 마법사를 완료하라는 메시지가 표시됩니다.

Secure Firewall 3100에서 SSD 핫스왑

SSD 2개를 설치한 경우 부팅 시 RAID를 형성합니다. 방화벽의 전원이 켜져 있는 동안 threat defense CLI에서 다음 작업을 수행할 수 있습니다.

- SSD 중 하나를 핫 스왑 - SSD에 결함이 있는 경우 교체할 수 있습니다. SSD가 하나뿐인 경우 방화벽이 켜져 있는 동안에는 SSD를 제거할 수 없습니다.
- SSD 중 하나 제거 - SSD가 2개인 경우 하나를 제거할 수 있습니다.
- 두 번째 SSD 추가 - SSD가 한 개인 경우 두 번째 SSD를 추가하여 RAID를 구성할 수 있습니다.

⚠

주의 이 절차를 사용하여 RAID에서 SSD를 먼저 분리하지 않은 상태에서 SSD를 분리하지 마십시오. 데이터가 손실될 수 있습니다.

프로시저

단계 **1** SSD 중 하나를 분리합니다.

a) RAID에서 SSD를 분리합니다.

configure raid remove-secure local-disk {**1** | **2**}

remove-secure 키워드는 RAID에서 SSD를 제거하고, 자체 암호화 디스크 기능을 비활성화하며, SSD의 보안 기반 초기화를 수행합니다. RAID에서 SSD만 제거하고 데이터를 그대로 유지하려는 경우 **remove** 키워드를 사용할 수 있습니다.

예제**:**

```
> configure raid remove-secure local-disk 2
```

b) SSD가 인벤토리에 더 이상 표시되지 않을 때까지 RAID 상태를 모니터링합니다.

show raid

SSD가 RAID에서 제거되면 작동성 및 드라이브 상태가 저하됨으로 표시됩니다. 두 번째 드라이브는 더 이상 멤버 디스크로 나열되지 않습니다.

예제:

```
> show raid
Virtual Drive
ID:                          1
Size (MB):                   858306
Operability:                 operable
Presence:                    equipped
Lifecycle:                   available
Drive State:                 optimal
Type:                        raid
Level:                       raid1
Max Disks:                   2
Meta Version:                1.0
Array State:                 active
Sync Action:                 idle
Sync Completed:              unknown
Degraded:                    0
Sync Speed:                  none

RAID member Disk:
Device Name:                 nvme0n1
Disk State:                  in-sync
Disk Slot:                   1
Read Errors:                 0
Recovery Start:              none
Bad Blocks:
Unacknowledged Bad Blocks:

Device Name:                 nvme1n1
Disk State:                  in-sync
Disk Slot:                   2
Read Errors:                 0
Recovery Start:              none
Bad Blocks:
Unacknowledged Bad Blocks:

> show raid
Virtual Drive
ID:                          1
Size (MB):                   858306
Operability:                 degraded
Presence:                    equipped
Lifecycle:                   available
Drive State:                 degraded
Type:                        raid
Level:                       raid1
Max Disks:                   2
Meta Version:                1.0
Array State:                 active
Sync Action:                 idle
Sync Completed:              unknown
Degraded:                    1
Sync Speed:                  none

RAID member Disk:
```

```
Device Name:                nvme0n1
Disk State:                 in-sync
Disk Slot:                  1
Read Errors:                0
Recovery Start:             none
Bad Blocks:
Unacknowledged Bad Blocks:
```

c) 섀시에서 SSD를 물리적으로 분리합니다.

단계 **2** SSD를 추가합니다.

a) SSD를 빈 슬롯에 물리적으로 추가합니다.

b) RAID에 SSD를 추가합니다.

configure raid add local-disk {**1** | **2**}

방화벽이 완전히 작동하는 동안 새 SSD를 RAID에 동기화하는 작업을 완료하는 데 몇 시간이 걸릴 수 있습니다. 재부팅해도 전원이 켜지면 동기화가 계속됩니다. **show RAID** 명령을 사용하여 상태를 표시합니다.

이전에 다른 시스템에서 사용된 SSD를 설치했지만 여전히 잠겨 있는 경우 다음 명령을 입력합니다.

configure raid add local-disk {**1** | **2**} *psid*

*PSID*는 SSD 후면에 부착된 레이블에 인쇄되어 있습니다. 또는 시스템을 재부팅할 수 있습니다. 그러면 SSD가 다시 포맷되고 RAID에 추가됩니다.

A 부록

고급 컨피그레이션

일부 디바이스 기능은 ASA 컨피그레이션 명령을 사용하여 구성됩니다. device manager는 명령 기반 기능을 많이 구성할 수 있지만 이를 모두 지원하지는 않습니다. device manager에서 달리 지원되지 않는 이러한 ASA 기능 중 일부를 사용해야 하는 경우, 스마트 CLI 또는 FlexConfig를 사용하여 기능을 수동으로 구성할 수 있습니다.

다음 주제에서는 이러한 유형의 고급 컨피그레이션에 대해 자세히 설명합니다.

스마트 CLI 및 FlexConfig 정보

Threat Defense ASA 구성 명령을 사용하여 일부 기능(모든 기능이 아님)을 구현합니다. threat defense 구성 명령의 고유 집합은 없습니다.

다음 방법으로 CLI를 사용하여 기능을 구성할 수 있습니다.

- 스마트 **CLI** — (기본 방법) 스마트 CLI 템플릿은 특정 기능에 대해 사전 정의된 템플릿입니다. 이 기능에 필요한 모든 명령은 제공되므로 변수의 값을 선택하기만 하면 됩니다. 시스템에서 선택 항목을 검증해 주기 때문에 기능을 더욱 올바르게 구성할 수 있습니다. 원하는 기능에 해당하는 스마트 CLI 템플릿이 있는 경우, 해당 스마트 CLI를 사용해야 합니다.

- **FlexConfig** — FlexConfig 정책은 FlexConfig 개체의 모음입니다. FlexConfig 개체는 스마트 CLI 템플릿보다 자유 형식으로 이용할 수 있으며, 시스템에서 CLI, 변수 또는 데이터 검증을 수행하지 않습니다. 유효한 명령 시퀀스를 생성하기 위해서는 ASA 컨피그레이션 명령을 알아야 하며 ASA 컨피그레이션 가이드를 준수해야 합니다.

스마트 CLI 및 FlexConfig를 사용하면 device manager 정책 및 설정을 통해 직접 지원되지 않는 기능을 구성할 수 있습니다.

주의 ASA에 대한 강력한 배경 지식을 보유하고 있으며 사용에 대한 전적인 책임을 질 수 있는 고급 사용자인 경우에만 스마트 CLI 및 FlexConfig를 사용하는 것이 좋습니다. 금지되지 않은 모든 명령을 구성할 수 있습니다. 스마트 CLI와 FlexConfig를 통해 기능을 활성화하는 경우, 구성되어 있는 다른 기능과 함께 의도하지 않은 결과를 초래할 수 있습니다.

구성한 스마트 CLI 및 FlexConfig 개체와 관련된 지원을 받기 위해 Cisco TAC(Technical Assistance Center)에 문의할 수 있습니다. Cisco TAC(Technical Assistance Center)에서는 고객을 대신하여 맞춤형 컨피그레이션을 설계하거나 작성하지 않습니다. Cisco에서는 올바른 작동이나 기타 threat defense 기능과의 상호운용성에 대해 어떠한 보증도 명시하지 않습니다. 스마트 CLI 및 FlexConfig 기능은 언제든지 사용이 중지될 수 있습니다. 완벽하게 보장되는 기능을 지원받으려면 device manager의 지원을 기다려야 합니다. 의심스러운 경우에는 스마트 CLI 또는 FlexConfig를 사용하지 마십시오.

다음 주제에서는 이러한 기능에 대해 자세히 설명합니다.

스마트 **CLI** 및 **FlexConfig**에 대한 권장 사용 방법

FlexConfig에는 다음과 같이 권장되는 주요 사용 방법이 두 가지 있습니다.

- ASA에서 threat defense로 마이그레이션하는 중이며 device manager에서 직접 지원하지 않는 호환 가능한 기능을 현재 사용 중이고 계속 사용해야 하는 경우입니다. 이 경우, ASA에서 **show running-config** 명령을 사용하여 해당 기능에 대한 컨피그레이션을 확인하고 FlexConfig 개체를 생성하여 해당 기능을 구현하십시오. 두 디바이스에서 **show running-config** 출력을 비교하여 확인합니다.
- threat defense를 사용 중이지만 구성해야 하는 설정 또는 기능이 있는 경우(예: Cisco TAC(Technical Assistance Center)에서 발생한 특정 문제를 해결하려면 특정 설정이 필요하다고 알려주는 경우), 복잡한 기능에 대해서는 랩 디바이스를 사용하여 FlexConfig를 테스트하고 정상적으로 작동하는지 확인합니다.

ASA 컨피그레이션을 재생성하려면 먼저 표준 정책에서 동일한 기능을 구성할 수 있는지 확인합니다. 예를 들어, 액세스 제어 정책에 침입 탐지 및 방지, HTTP 및 기타 프로토콜 검사 유형, URL 필터링, 애플리케이션 필터링, 액세스 제어(ASA에서는 별도의 기능을 사용하여 구현함)가 포함된 경우, 많은 기능이 CLI 명령을 사용하여 컨피그레이션된 것이 아니므로 **show running-config**의 출력 내에 모든 정책이 표시되지는 않습니다.

참고 ASA와 threat defense는 일대일로 중복되지 않는다는 점을 항상 기억해야 합니다. threat defense 디바이스에서 ASA 컨피그레이션을 완벽하게 재생성하려고 시도하지 마십시오. FlexConfig를 사용하여 구성하는 모든 기능은 신중히 테스트해야 합니다.

스마트 CLI 및 FlexConfig 개체의 CLI 명령

threat defense 는 ASA 구성 명령을 사용하여 일부 기능을 구성합니다. 모든 ASA 기능이 threat defense 에서 호환되는 것은 아니지만, threat defense에서는 작업 가능하나 device manager 정책에서는 구성할 수 없는 기능도 일부 있습니다. 스마트 CLI 및 FlexConfig 개체를 사용하여 이러한 기능을 구성하는 데 필요한 CLI를 지정할 수 있습니다.

스마트 CLI 또는 FlexConfig를 사용하여 기능을 수동으로 구성하려는 경우, 적절한 구문에 따라 명령을 파악하고 구현해야 합니다. FlexConfig는 CLI 명령 구문을 검증하지 않습니다. 적절한 구문 및 CLI 명령 구성에 대한 자세한 내용을 확인하려면 ASA 설명서를 참조하십시오.

- ASA CLI 컨피그레이션 가이드에서는 기능을 구성하는 방법에 대해 설명합니다. 가이드 위치: http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html
- ASA 명령 참조에서는 명령 이름을 기준으로 정렬된 추가 정보를 제공합니다. 참조 위치: http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-command-reference-list.html

다음 주제에서는 컨피그레이션 명령에 대해 자세히 설명합니다.

소프트웨어 업그레이드가 FlexConfig 정책에 미치는 영향

threat defense 소프트웨어의 각 새 버전을 설치할 때마다 device manager의 기능 구성을 위한 지원이 추가됩니다. 이러한 새 기능이 이전에 FlexConfig를 사용하여 구성한 기능과 겹치는 경우도 있습니다.

업그레이드 후에는 FlexConfig 정책 및 개체를 검사해야 합니다. device manager 또는 스마트 CLI 내에 추가된 지원으로 인해 금지된 명령을 포함하는 정책이나 개체가 있는 경우, 개체 목록의 아이콘과 메시지에 해당 문제가 표시됩니다. 이러한 경우에는 시간을 할애하여 컨피그레이션을 다시 수행하십시오. 금지된 명령 목록을 사용하면 해당 명령을 구성해야 하는 위치를 확인하는 데 도움이 됩니다.

FlexConfig 정책에 연결된 FlexConfig 개체에 새롭게 금지된 명령이 포함되어 있어도 변경 사항을 구축할 수는 있습니다. 하지만 FlexConfig 정책에 나와 있는 모든 문제를 해결할 때까지 새 스마트 CLI 개체를 생성할 수는 없습니다.

디바이스 컨피그레이션에 능동적으로 구축 중인 개체에만 제한이 적용되므로, 문제가 있는 개체를 FlexConfig 정책에서 제거하기만 하면 됩니다. 따라서 개체를 제거한 다음, 해당하는 스마트 CLI 또는 통합 device manager 컨피그레이션을 생성할 때 참조로 사용할 수 있습니다. 새 컨피그레이션에 만족하는 경우에는 개체만 삭제하면 됩니다. 제거된 개체에 금지되지 않은 일부 요소가 포함된 경우에는 해당 개체를 수정하여 지원되지 않은 명령을 제거한 후 FlexConfig 정책에 개체를 다시 연결할 수 있습니다.

ASA 소프트웨어 버전 및 현재 CLI 컨피그레이션 확인

시스템이 ASA 소프트웨어 명령을 사용하여 일부 기능을 구성하므로 threat defense 디바이스에서 실행 중인 소프트웨어에서 사용되는 현재 ASA 버전을 확인해야 합니다. 이 버전 번호에 따라 기능 구성 시 어떤 ASA CLI 컨피그레이션 가이드를 참조해야 하는지 알 수 있습니다. 또한 현재 CLI 기반 컨피그레이션을 확인하고, 구현하려는 ASA 컨피그레이션과 이를 비교합니다.

모든 ASA 컨피그레이션은 threat defense 컨피그레이션과 매우 다릅니다. threat defense 정책은 CLI 외부에서 구성되는 경우가 많아서 명령을 보고 컨피그레이션을 확인할 수가 없습니다. ASA와 threat defense 컨피그레이션 간에 일대일 대응 관계를 생성하지 마십시오.

이 정보를 확인하려면 device manager에서 CLI 콘솔을 열거나 디바이스 관리 인터페이스에 대한 SSH 연결을 설정하고 다음 명령을 실행합니다.

- **show version system** Cisco Adaptive Security Appliance 소프트웨어 버전 번호를 찾습니다.
- **show running-config** 현재 CLI 컨피그레이션을 확인합니다.
- **show running-config all** 현재 CLI 구성의 모든 기본 명령을 포함합니다.

금지된 **CLI** 명령

스마트 CLI와 FlexConfig의 목적은 device manager를 사용하여 threat defense 디바이스에서는 구성할 수 없으나 ASA 디바이스에서는 사용 가능한 기능을 구성하는 것입니다.

따라서 device manager에서 동일한 역할을 하는 ASA 기능을 구성할 수 없습니다. 다음 표에는 이러한 금지된 명령 영역 중 일부가 나와 있습니다. 이 목록에는 컨피그레이션 모드를 시작하는 상위 명령이 여러 개 포함되어 있습니다. 상위 명령의 금지 사항에는 하위 명령의 금지 사항이 포함됩니다. 여기에는 명령의 **no** 버전과 그와 연관된 **clear** 명령도 포함되어 있습니다.

FlexConfig 개체 편집기를 사용하면 개체에 이러한 명령을 포함할 수 없습니다. 스마트 CLI 템플릿에는 유효하게 구성할 수 있는 명령만 포함되어 있으므로 이 목록이 적용되지 않습니다.

금지된 **CLI** 명령	참고
aaa	**Objects(**개체**)** > **Identity Sources(ID** 소스**)**를 사용합니다.
aaa-server	**Objects(**개체**)** > **Identity Sources(ID** 소스**)**를 사용합니다.
access-group	**Policies(**정책**)** > **Access Control(**액세스 제어**)**을 사용하여 액세스 규칙을 구성합니다.
access-list	부분적으로 차단되었습니다. • **ethertype** 액세스 목록을 생성할 수 있습니다. • **extended** 및 **standard** 액세스 목록은 생성할 수 없습니다. 스마트 CLI 확장 액세스 목록 또는 표준 액세스 목록 개체를 사용하여 이러한 ACL을 생성합니다. 그런 다음, 서비스 정책 트래픽 클래스용 확장 ACL을 사용하는 **match access-list** 등의 개체 이름으로 ACL을 참조하는 FlexConfig 지원 명령에서 이러한 ACL을 사용할 수 있습니다. • 시스템에서 **access-group** 명령과 함께 사용하는 **advanced** 액세스 목록은 생성할 수 없습니다. 대신, **Policies(**정책**)** > **Access Control(**액세스 제어**)**을 사용하여 액세스 규칙을 구성합니다. • **webtype** 액세스 목록은 생성할 수 없습니다.

금지된 **CLI** 명령	참고
anyconnect-custom-data	**Device(**디바이스**)** > **Remote Access VPN(**원격 액세스 **VPN)**을 사용하여 Secure Client를 구성합니다.
asdm	이 기능은 threat defense 시스템에 적용되지 않습니다.
as-path	스마트 CLI AS 경로 개체를 생성한 다음, 스마트 CLI BGP 개체에 이를 사용하여 자동 시스템 경로 필터를 구성할 수 있습니다.
attribute	—
auth-prompt	이 기능은 threat defense 시스템에 적용되지 않습니다.
boot	—
call-home	—
captive-portal	**Policies(**정책**)** > **Identity(ID)**를 사용하여 활성 인증에 사용되는 종속 포털을 구성합니다.
clear	—
client-update	—
clock	**Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **NTP**를 사용하여 시스템 시간을 구성합니다.
cluster	—
command-alias	—
community-list	스마트 CLI 확장 커뮤니티 목록 또는 표준 커뮤니티 목록 개체를 생성한 다음, 스마트 CLI BGP 개체에 이를 사용하여 커뮤니티 목록 필터를 구성할 수 있습니다.
compression	—
configure	—
crypto	**Objects(**개체**)** 페이지에서 **Certificates(**인증서**)**, **IKE Policies(IKE** 정책**)** 및 **IPSec Proposals(IPSec** 제안**)**를 사용합니다.
ddns	**Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **DDNS Service(DDNS** 서비스**)**를 사용하여 동적 DNS를 설정합니다.
dhcp-client	—
dhcpd	**Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **DHCP Server(DHCP** 서버**)**를 사용합니다. 그러나 이 **dhcpd option** 명령은 허용됩니다.

금지된 **CLI** 명령	참고
dhcprelay	대신 위협 방어 API에서 dhcprelayservices 리소스를 사용하십시오.
dns	**Objects(**개체**)** > **DNS Groups(DNS** 그룹**)**를 사용하여 DNS 그룹을 구성한 다음, **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **DNS Server(DNS** 서버**)**를 사용하여 그룹을 할당합니다.
dns-group	**Objects(**개체**)** > **DNS Groups(DNS** 그룹**)**를 사용하여 DNS 그룹을 구성한 다음, **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **DNS Server(DNS** 서버**)**를 사용하여 그룹을 할당합니다.
domain-name	**Objects(**개체**)** > **DNS Groups(DNS** 그룹**)**를 사용하여 DNS 그룹을 구성한 다음, **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **DNS Server(DNS** 서버**)**를 사용하여 그룹을 할당합니다.
dynamic-access-policy-config **dynamic-access-policy-record**	—
enable	—
event	—
failover	—
fips	—
firewall	Device Manager에서는 라우팅 방화벽 모드만 지원합니다.
hostname	**Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Hostname(**호스트 이름**)**을 사용합니다.
hpm	이 기능은 threat defense 시스템에 적용되지 않습니다.
http	**Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Management Access(**관리 액세스**)**의 **Data Interfaces(**데이터 인터페이스**)** 탭을 사용합니다.
inline-set	—

금지된 **CLI** 명령	참고
interface (BVI, 관리, 이더넷, GigabitEthernet 및 하위 인터페이스용)	부분적으로 차단되었습니다. **Device(**디바이스**)** > **Interfaces(**인터페이스**)** 페이지에서 물리적 인터페이스, 하위 인터페이스 및 브리지 가상 인터페이스를 구성합니다. 그러면 FlexConfig를 사용하여 추가 옵션을 구성할 수 있습니다. 그러나 다음과 같은 **interface** 모드 명령은 이러한 유형의 인터페이스에 대해 금지되어 있습니다. **cts** **ip address** **ip address dhcp** **ipv6 address** **ipv6 enable** **ipv6 nd dad** **ipv6 nd suppress-ra** **mode** **nameif** **security-level** **shutdown** **zone-member**
vni, **redundant**, **tunnel**용 **interface**	**Device(**디바이스**)** > **Interfaces(**인터페이스**)**페이지에서 인터페이스를 구성합니다. Device Manager에서는 이러한 유형의 인터페이스를 지원하지 않습니다.
ip audit	이 기능은 threat defense 시스템에 적용되지 않습니다. 대신, 액세스 제어 규칙을 사용하여 침입 정책을 적용합니다.
ip-client	데이터 인터페이스를 관리 게이트웨이로 사용하도록 시스템을 구성하려면 **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Management Interface(**관리 인터페이스**)**를 사용합니다.
ip local pool	주소 풀을 구성하려면 **Device(**디바이스**)** > **Remote Access VPN(**원격 액세스 **VPN)**을 사용합니다.
ipsec	—
ipv6	스마트 CLI IPv6 접두사 목록 개체를 생성한 다음, 스마트 CLI BGP 개체에 이를 사용하여 IPv6용 접두사 목록 필터링을 구성할 수 있습니다.
ipv6-vpn-addr-assign	주소 풀을 구성하려면 **Device(**디바이스**)** > **Remote Access VPN(**원격 액세스 **VPN)**을 사용합니다.

금지된 **CLI** 명령	참고
isakmp	**Device(**디바이스**)** > **Site-to-Site VPN(**사이트 대 사이트 **VPN)**을 사용합니다.
jumbo-frame	어떤 인터페이스든지 MTU를 기본값인 1500을 넘도록 증가시키는 경우, 시스템에서는 점보 프레임 지원을 자동으로 활성화합니다.
ldap	—
license-server	**Device(**디바이스**)** > **Smart License(**스마트 라이선스**)**를 사용합니다.
logging	**Objects(**개체**)** > **Syslog Servers(Syslog** 서버**)** 및 **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Logging Settings(**로깅 설정**)**를 사용합니다. 그러나 **logging history** 명령은 FlexConfig에서 컨피그레이션할 수 있습니다.
management-access	—
migrate	**Device(**디바이스**)** > **Remote Access VPN(**원격 액세스 **VPN)** 및 **Device(**디바이스**)** > **Site-to-Site VPN(**사이트 대 사이트 **VPN)**을 사용하여 IKEv2 지원을 활성화합니다.
mode	Device Manager은 단일 컨텍스트 모드만 지원합니다.
mount	—
mtu	**Device(**디바이스**)** > **Interfaces(**인터페이스**)**에서 인터페이스당 MTU를 구성합니다.
nat	**Policies(**정책**)** > **NAT**를 사용합니다.
ngips	—
ntp	**Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **NTP**를 사용합니다.
object-group network **object network**	**Objects(**개체**)** > **Network(**네트워크**)**를 사용합니다. FlexConfig에서 네트워크 개체 또는 그룹을 생성할 수는 없지만, 템플릿 내부에서 개체 관리자에 정의되어 있는 네트워크 개체 및 그룹을 변수로 사용할 수는 있습니다.

금지된 **CLI** 명령	참고
object service |natorigsvc **object service |natmappedsvc**	**object service** 명령은 일반적으로 허용되지만 이름이 |natorigsvc 또는 |natmappedsvc로 지정된 내부 개체는 편집할 수 없습니다. 이러한 이름에서 세로 막대는 제한된 개체 이름의 첫 번째 문자로, 의도적으로 사용되는 것입니다.
passwd **password**	—
password-policy	—
policy-list	스마트 CLI 정책 목록 개체를 생성한 다음, 스마트 CLI BGP 개체에 이를 사용하여 정책 목록을 구성할 수 있습니다.
policy-map 하위 명령	다음 명령은 정책 맵에서 구성할 수 없습니다. **priority** **police** **match tunnel-group**
prefix-list	스마트 CLI IPv4 접두사 목록 개체를 생성한 다음, 스마트 CLI OSPF 또는 BGP 개체에 이를 사용하여 IPv4용 접두사 목록 필터링을 구성할 수 있습니다.
priority-queue	—
privilege	—
reload	reload 명령은 예약할 수 없습니다. 시스템에서는 **reload** 명령이 아닌 **reboot** 명령을 사용해 재시작합니다.
rest-api	이 기능은 threat defense 시스템에 적용되지 않습니다. REST API는 항상 설치 및 활성화되어 있습니다.
route	**Device(**디바이스**)** > **Routing(**라우팅**)**을 사용하여 정적 경로를 구성합니다.
route-map	스마트 CLI 경로 맵 개체를 생성한 다음, 스마트 CLI OSPF 또는 BGP 개체에 이를 사용하여 경로 맵을 구성할 수 있습니다.
router bgp	BGP용 스마트 CLI 템플릿을 사용합니다.
router eigrp	EIGRP용 스마트 CLI 템플릿을 사용합니다.
router ospf	OSPF용 스마트 CLI 템플릿을 사용합니다.
scansafe	이 기능은 threat defense 시스템에 적용되지 않습니다. 대신, 액세스 제어 규칙에서 URL 필터링을 구성합니다.

금지된 **CLI** 명령	참고
setup	이 기능은 threat defense 시스템에 적용되지 않습니다.
sla	—
snmp-server	FTP API SNMP 리소스를 사용하여 SNMP를 구성합니다.
ssh	**Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Management Access(**관리 액세스**)**의 **Data Interfaces(**데이터 인터페이스**)** 탭을 사용합니다.
ssl	**Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **SSL Settings(SSL** 설정**)**를 사용합니다.
telnet	Threat Defense는 텔넷 연결을 지원하지 않습니다. 텔넷 대신 SSH를 사용하여 디바이스 CLI에 액세스합니다.
time-range	—
tunnel-group	**Device(**디바이스**)** > **Remote Access VPN(**원격 액세스 **VPN)** 및 **Device(**디바이스**)** > **Site-to-Site VPN(**사이트 대 사이트 **VPN)**을 사용합니다.
tunnel-group-map	**Device(**디바이스**)** > **Remote Access VPN(**원격 액세스 **VPN)** 및 **Device(**디바이스**)** > **Site-to-Site VPN(**사이트 대 사이트 **VPN)**을 사용합니다.
user-identity	**Policies(**정책**)** > **Identity(ID)**를 사용합니다.
username	CLI 사용자를 생성하려면 디바이스에 대한 SSH 또는 콘솔 세션을 열고 **configure user** 명령을 사용합니다.
vpdn	—
vpn	—
vpn-addr-assign	—
vpnclient	—
vpn-sessiondb	—
vpnsetup	—
webvpn	—
zone	—
zonelabs-integrity	이 기능은 threat defense 시스템에 적용되지 않습니다.

스마트 CLI 템플릿

다음 표에서는 기능을 기반으로 스마트 CLI 템플릿을 설명합니다.

참고 또한 Smart CLI 템플릿을 사용하여 OSPF 및 BGP를 구성합니다. 그러나 이러한 템플릿은 Advanced Configuration(고급 구성) 페이지가 아닌 **Device(**디바이스**)** > **Routing(**라우팅**)** 페이지를 통해 사용할 수 있습니다.

기능	템플릿	설명
개체: AS 경로	ASPath	라우팅 프로토콜 개체에 사용할 ASPath 개체를 생성합니다.
개체: 액세스 목록	확장 액세스 목록 표준 액세스 목록	라우팅 개체에 사용할 확장 또는 표준 ACL을 생성합니다. ACL을 사용하는 허용된 명령을 구성하는 FlexConfig 개체에서 이러한 개체를 이름으로 참조할 수도 있습니다.
개체: 커뮤니티 목록	확장 커뮤니티 목록 표준 커뮤니티 목록	라우팅 개체에 사용할 확장 또는 표준 커뮤니티 목록을 생성합니다.
개체: 접두사 목록	IPV4 접두사 목록 IPV6 접두사 목록	라우팅 개체에 사용할 IPv4 또는 IPv6 접두사 목록을 생성합니다.
개체: 정책 목록	정책 목록	라우팅 개체에 사용할 정책 목록을 생성합니다.
개체: 경로 맵	경로 맵	라우팅 개체에 사용할 경로 맵을 생성합니다.

스마트 CLI 및 FlexConfig에 대한 지침 및 제한 사항

스마트 CLI 또는 FlexConfig를 통해 기능을 구성하는 경우 다음 사항에 유의하십시오.

- FlexConfig 개체에 정의된 명령은 스마트 CLI를 포함하여 기능에 대한 모든 명령이 device manager를 통해 정의된 이후에 구축됩니다. 따라서 이러한 명령이 디바이스에 실행되기 전에 구성 중인 개체, 인터페이스 등을 사용할 수 있습니다. 스마트 CLI 템플릿에서 FlexConfig 구축 항목을 사용해야 하는 경우, 스마트 CLI 템플릿을 생성 및 구축하기 전에 FlexConfig를 생성 및 구축하십시오. 예를 들어, OSPF 스마트 CLI 템플릿을 사용하여 EIGRP 경로를 재배포하려면 먼저 FlexConfig를 사용하여 EIGRP를 구성한 다음 OSPF 스마트 CLI 템플릿을 생성하십시오.
- FlexConfig를 통해 구성한 기능 또는 기능 중 일부를 제거하고 싶지만 스마트 CLI 템플릿이 이 기능을 참조하는 경우, 먼저 이 기능을 사용하는 스마트 CLI 템플릿에서 명령을 제거해야 합니다. 그런 다음 스마트 CLI 구성 기능이 이 기능을 더 이상 참조하지 않도록 컨피그레이션을 구축합니다. 그러면 FlexConfig에서 기능을 제거하고 컨피그레이션을 다시 구축하여 이 기능을 완전히 제거할 수 있습니다.

스마트 CLI 개체 구성

스마트 CLI 개체는 device manager의 다른 위치에서는 구성할 수 없는 기능을 정의합니다. 스마트 CLI 개체는 기능 구성에 대한 한 가지 수준의 지침을 제공합니다. 지정된 기능(템플릿)의 경우, 가능한 명령은 모두 사전 로드되며 입력하는 변수는 검증됩니다. 따라서 계속 CLI 명령을 사용하여 기능을 구성하더라도 스마트 CLI 개체는 FlexConfig 개체와 같은 자유 형식으로 사용할 수 없습니다.

스마트 CLI 템플릿에서 한 가지 수준의 지침을 제공하긴 하지만, 네트워크에 대해 올바르게 작동하는 값을 선택하려면 여전히 ASA 컨피그레이션 가이드 및 명령 참조를 읽어 명령 사용 방법을 파악해야 합니다. 작업할 ASA 컨피그레이션이 이미 있고 스마트 CLI 개체에서 동일한 명령 시퀀스를 구축하기만 하면 되는 것이 가장 좋습니다.

스마트 CLI 개체는 기능 영역에 따라 그룹화됩니다.

참고 정의하는 스마트 CLI 개체는 모두 구축됩니다. FlexConfig와 달리 여러 스마트 CLI 개체를 생성한 다음 구축할 개체를 선택할 수 없습니다. 구성하려는 기능에 대해서만 스마트 CLI 개체를 생성하십시오.

프로시저

단계 **1** **Device(**디바이스**)** > **Advanced Configuration(**고급 컨피그레이션**)**에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

단계 **2** Advanced Configuration(고급 컨피그레이션) 목차의 **Smart CLI(**스마트 **CLI)** 아래에서 적절한 기능 영역을 클릭합니다.

단계 **3** 다음 중 하나를 수행합니다.

- 개체를 생성하려면 **+** 버튼을 클릭합니다.
- 개체를 수정하려면 개체의 수정 아이콘()을 클릭하십시오.

개체를 삭제하려면 해당 개체의 휴지통 아이콘()을 클릭합니다.

단계 **4** 개체의 Name(이름) 및 설명(선택 사항)을 입력합니다.

단계 **5** 구성 중인 기능에 대해 **CLI Template(CLI** 템플릿**)**을 선택합니다.

시스템에서 **Template(**템플릿**)** 창에 명령 템플릿을 로드합니다. 처음에는 필수 명령만 표시됩니다. 이 명령은 템플릿에 필요한 최소 컨피그레이션을 나타냅니다.

단계 **6** 템플릿에서 필요에 따라 변수를 입력하고 명령을 추가합니다.

ASA 또는 threat defense 디바이스(management center에서 관리되는 디바이스)의 기존 컨피그레이션으로 작업하는 것이 가장 좋습니다. 컨피그레이션을 사용할 수 있는 경우, IP 주소 및 인터페이스 이름 등의 변수를 네트워크의 이 특정 디바이스 위치에 적절하게 변경하여 템플릿이 해당 컨피그레이션을 따르도록 설정하기만 하면 됩니다.

템플릿 내용 입력에 대한 몇 가지 팁은 다음과 같습니다.

- 변수의 값을 선택하려면 변수를 클릭하고 적절한 값을 입력하거나 목록에서 선택합니다(값이 열거된 경우). 입력해야 하는 변수 위에 마우스를 올려놓으면 숫자 범위와 같이 해당 옵션에 대해 유효한 값이 표시됩니다. 권장 값이 표시되는 경우도 있습니다.

  예를 들어 OSPF 템플릿에서 필수 명령인 **router ospf** *process-id* 위에 마우스를 올려놓으면 "Process ID (1-65535)(프로세스 ID(1-65535))"가 표시되며, *process-id*를 클릭하면 이 필드가 강조 표시됩니다. 원하는 숫자를 입력하기만 하면 됩니다.

- 변수의 옵션을 선택할 때 옵션 구성에 사용 가능한 추가 명령이 있는 경우, 이러한 명령은 자동으로 표시되며 적절하게 비활성화 또는 활성화됩니다. 이러한 추가 명령을 확인합니다.

- 템플릿 위에 있는 **Show**/**Hide Disabled(**비활성화된 항목 표시/숨기기**)** 링크를 사용하여 보기를 제어합니다. 비활성화된 명령은 구성되지 않으며, 구성하려면 이러한 명령을 표시해야 합니다. 전체 템플릿을 보려면 템플릿 위에 있는 **Show Disabled(**비활성화된 항목 표시**)** 링크를 클릭합니다. 구성되는 명령만 보려면 표 위에 있는 **Hide Disabled(**비활성화된 항목 숨기기**)** 링크를 클릭합니다.

- 개체를 마지막으로 저장한 이후에 편집한 내용을 모두 지우려면 템플릿 위에 있는 **Reset(**재설정**)** 링크를 클릭합니다.

- 선택 사항 명령을 활성화하려면 줄 번호의 왼쪽에서 **+** 버튼을 클릭합니다.

- 선택 사항 명령을 비활성화하려면 줄 번호의 왼쪽에서 **-** 버튼을 클릭합니다. 줄을 편집한 경우 편집한 내용은 삭제되지 않습니다.

- 명령을 중복하려면 Options(옵션)의 **...** 버튼을 클릭하고 **Duplicate(**중복**)**를 선택합니다. 두 번 이상 명령을 입력하는 것이 유효한 경우에만 명령 중복이 허용됩니다.

- 중복된 명령을 삭제하려면 Options(옵션)의 **...** 버튼을 클릭하고 **Delete(**삭제**)**를 선택합니다. 기본 템플릿에 포함되어 있는 명령은 삭제할 수 없습니다.

단계 **7** **OK(**확인**)**를 클릭합니다.

FlexConfig 정책 구성

FlexConfig 정책은 간단히 말해 디바이스 컨피그레이션에 구축하려는 FlexConfig 개체의 목록입니다. 정책에 포함된 개체만 구축되며 다른 개체는 모두 간단히 정의되고 사용되지 않습니다.

FlexConfig 개체에 정의된 명령은 스마트 CLI를 포함하여 기능에 대한 모든 명령이 device manager를 통해 정의된 이후에 구축됩니다. 따라서 이러한 명령이 디바이스에 실행되기 전에 구성 중인 개체, 인터페이스 등을 사용할 수 있습니다. 스마트 CLI 템플릿에서 FlexConfig 구축 항목을 사용해야 하는 경우, 스마트 CLI 템플릿을 생성 및 구축하기 전에 FlexConfig를 생성 및 구축하십시오. 예를 들어, OSPF 스마트 CLI 템플릿을 사용하여 EIGRP 경로를 재배포하려면 먼저 FlexConfig를 사용하여 EIGRP를 구성한 다음 OSPF 스마트 CLI 템플릿을 생성하십시오.

참고 기능에 스마트 CLI 템플릿이 있는 경우, FlexConfig를 사용해서는 이를 구성할 수 없으므로 스마트 CLI 개체를 사용해야 합니다.

시작하기 전에

FlexConfig 개체를 생성합니다. 다음 주제를 참조하십시오.

- FlexConfig 개체 구성, 921 페이지
- FlexConfig 개체에서 변수 생성, 923 페이지
- 비밀 키 개체 구성, 931 페이지

프로시저

단계 **1** **Device(**디바이스**)** > **Advanced Configuration(**고급 컨피그레이션**)**에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

단계 **2** Advanced Configuration(고급 컨피그레이션) 목차에서 **FlexConfig** > **FlexConfig Policy(FlexConfig** 정책**)**를 클릭합니다.

단계 **3** **Group List(**그룹 목록**)**에서 개체 목록을 관리합니다.

- 개체를 추가하려면 **+** 버튼을 클릭합니다. 개체가 아직 없으면 **Create New FlexConfig Object(**새 **FlexConfig** 개체 생성**)**를 클릭하여 개체를 정의합니다.
- 개체를 삭제하려면 개체 항목의 오른쪽에서 **X** 버튼을 클릭합니다.

참고 각 개체는 완전히 독립적이며 다른 FlexConfig 개체에 정의되어 있는 컨피그레이션의 영향을 받지 않는 것이 좋습니다. 그러면 다른 개체에 영향을 주지 않고 개체를 추가하거나 제거할 수 있습니다.

단계 **4** **Preview(**미리보기**)** 창에서 제안된 명령을 평가합니다.

Expand(펼치기**)** 버튼을 클릭하면 화면을 넓혀 긴 명령을 더 자세히 확인할 수 있습니다(확인 후에는 **Collapse(**접기**)**를 클릭).

미리보기는 변수를 평가하고 실행할 올바른 명령을 생성하므로 이러한 명령이 올바르고 유효한지 확인합니다. 명령으로 인해 디바이스를 사용할 수 없게 만드는 오류 또는 불량한 컨피그레이션이 발생하지 않는지 확인해야 합니다.

주의 시스템에서는 명령을 검증하지 않습니다. 따라서 유효하지 않은 명령이나 디바이스를 파괴하는 명령을 구축하게 될 수도 있습니다. 변경 사항을 구축하기 전에 매우 신중하게 미리보기를 확인하십시오.

단계 **5** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

FlexConfig 정책을 편집하고 나서 다음 구축 결과를 주의 깊게 검토합니다. 오류가 있으면 개체에서 CLI를 수정합니다. FlexConfig 정책 트러블슈팅, 932 페이지의 내용을 참조하십시오.

FlexConfig 개체 구성

FlexConfig 개체에는 device manager를 사용하여 달리 구성할 수 없는 특정 기능을 구성하는 데 필요한 ASA 명령이 포함되어 있습니다. 오타 없이 올바른 명령 시퀀스를 입력해야 합니다. 시스템에서는 FlexConfig 개체의 콘텐츠를 검증하지 않습니다.

구성하려는 각 일반 기능에 대해 별도의 개체를 생성하는 것이 좋습니다. 예를 들어, 배너를 정의하고 RIP 라우팅 프로토콜도 구성하려면 별도의 개체 2개를 사용합니다. 별도의 개체에서 기능을 분리하면 구축할 개체를 더 쉽게 선택할 수 있으며 트러블슈팅도 더 간단히 수행할 수 있습니다.

참고 **enable** 및 **configure terminal** 명령은 포함하지 마십시오. 시스템에서 컨피그레이션 명령에 대해 올바른 모드를 자동으로 시작합니다.

프로시저

단계 **1** **Device(**디바이스**)** > **Advanced Configuration(**고급 컨피그레이션**)**에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

단계 **2** Advanced Configuration(고급 컨피그레이션) 목차에서 **FlexConfig** > **FlexConfig Objects(FlexConfig** 개체**)**를 클릭합니다.

단계 **3** 다음 중 하나를 수행합니다.

- 개체를 생성하려면 + 버튼을 클릭합니다.
- 개체를 수정하려면 개체의 수정 아이콘( )을 클릭하십시오.

참조되지 않는 개체를 삭제하려면 해당 개체의 휴지통 아이콘( )을 클릭합니다.

단계 **4** 개체의 Name(이름) 및 설명(선택 사항)을 입력합니다.

단계 **5** **Variables(**변수**)** 섹션에서 개체 본문에 사용할 변수를 생성합니다.

생성해야 하는 유일한 변수는 device manager 내에 정의되어 있는 개체를 가리키는 변수입니다(특히, 네트워크, 포트 및 암호 키 변수 유형 또는 이름이 지정된 인터페이스를 가리키는 인터페이스 변수). 다른 변수 유형의 경우 간단히 개체 본문에 값을 입력하면 됩니다.

변수 생성 및 사용에 대한 자세한 내용은 FlexConfig 개체에서 변수 생성, 923 페이지를 참조하십시오.

단계 **6** **Template(**템플릿**)** 섹션에서 기능을 구성하는 데 필요한 ASA 명령을 입력합니다.

기능을 구성하기 위해서는 올바른 순서로 명령을 입력해야 합니다. ASA CLI 컨피그레이션 가이드를 사용하여 명령을 입력하는 방법에 대해 알아봅니다. 참조로 사용할 수 있는 ASA 또는 다른 threat defense 디바이스의 사전 테스트된 컨피그레이션 파일이 있는 것이 가장 좋습니다.

Mustache 표기법을 사용하여 변수를 참조하고 처리할 수도 있습니다. 자세한 내용은 FlexConfig 변수 참조 및 값 검색, 924 페이지를 참조하십시오.

개체 본문 생성에 대한 몇 가지 팁은 다음과 같습니다.

- 줄을 추가하려면 줄 끝에 커서를 놓고 Enter 키를 누릅니다.
- 변수를 사용하려면 이중 중괄호 사이에 변수 이름을 입력합니다(예: {{*variable_name*}}). 개체를 참조하는 변수의 경우, 검색 중인 값의 특성을 포함해야 합니다(예: {{*variable_name.attribute*}}). 사용 가능한 특성은 개체 유형에 따라 달라집니다. 자세한 내용은 변수 참조: {{variable}} 또는 {{{variable}}}, 924 페이지를 참조하십시오.
- 스마트 CLI 개체를 사용하려면 개체의 이름을 입력합니다. 스마트 CLI에 구성된 라우팅 프로세스를 참조해야 하는 경우 프로세스 식별자를 입력합니다. FlexConfig 개체의 스마트 CLI 개체 참조, 929 페이지를 참조하십시오.
- 본문의 크기를 더 키우거나 줄이려면 템플릿 본문 위의 **Expand/Collapse(**펼치기/접기**)** 링크를 클릭합니다.
- 개체를 마지막으로 저장한 이후에 변경한 사항을 지우려면 **Reset(**재설정**)** 링크를 클릭합니다.

단계 **7** **Negate Template(**무효화 템플릿**)** 섹션에서 개체 본문에 구성되어 있는 명령을 제거하거나 되돌리는 데 필요한 명령을 입력합니다.

Negate(무효화) 섹션은 매우 중요하며 다음의 두 가지 목적을 위해 사용됩니다.

- 구축을 간소화합니다. 본문에서 명령을 재구축하기 전에 시스템에서는 이러한 명령을 사용하여 먼저 컨피그레이션을 지우거나 실행 취소합니다. 이렇게 하면 구축이 정상적으로 이루어집니다.
- FlexConfig 정책에서 개체를 제거하여 이 기능을 제거하려는 경우, 시스템에서는 이러한 명령을 사용하여 디바이스에서 명령을 제거합니다.

개체 본문에서 CLI를 무효화하거나 되돌리는 데 필요한 명령을 제공하지 않으면 구축 시 개체 내의 명령뿐만 아니라 전체 디바이스의 컨피그레이션을 지우고 모든 정책을 재구축해야 할 수 있습니다. 이 경우, 구축에 더 오랜 시간이 걸리고 트래픽을 방해하게 됩니다. 개체 본문에 정의된 컨피그레이션을 취소하는 데 필요한 명령만 모두 사용했는지 확인합니다. 무효화 명령은 일반적으로 템플릿에 포함된 명령의 **no** 또는 **clear** 형식이지만 이미 활성화된 기능을 실제로 끄는 경우 "negate" 명령은 명령의 긍정 형식(기능을 활성화하는 형식)입니다.

ASA 컨피그레이션 가이드 및 명령 참조를 사용하여 적절한 명령을 파악합니다. 경우에 따라 단일 명령으로 컨피그레이션을 취소할 수 있습니다. 예를 들어 RIP를 컨피그레이션하는 개체에서 간단한 **no router rip** 명령은 하위 명령을 포함한 전체 **router rip** 컨피그레이션을 제거합니다.

마찬가지로 여러 줄로 된 배너를 생성하기 위해 여러 **banner login** 명령을 입력한 경우, 단일 **no banner login** 명령은 전체 로그인 배너를 무효화합니다.

템플릿이 여러 중첩 개체를 생성하는 경우 무효화 템플릿은 개체를 반대 순서로 제거해야 합니다. 즉, 개체를 삭제하기 전에 개체에 대한 참조를 먼저 제거해야 합니다. 예를 들어 ACL을 먼저 생성한 다

음 트래픽 클래스에서 참조하고, 정책 맵에서 해당 트래픽 클래스를 참조하고, 마지막으로 서비스 정책을 사용해 정책 맵을 활성화하는 경우 무효화 템플릿은 서비스 정책, 정책 맵, 트래픽 클래스, ACL을 차례로 제거하여 컨피그레이션을 실행 취소해야 합니다.

단계 **8** **OK(**확인**)**를 클릭합니다.

다음에 수행할 작업

FlexConfig 개체를 생성하기만 하면 이 개체가 구축되지 않으므로 개체를 FlexConfig 정책에 추가해야 합니다. 이때, FlexConfig 정책의 개체만 구축되기 때문에 FlexConfig 개체를 재정의할 수 있으며, 모든 개체를 자동으로 구축하지 않고 일부를 특별한 용도에 맞게 준비할 수 있습니다. FlexConfig 정책 구성, 919 페이지의 내용을 참조하십시오.

FlexConfig 개체에서 변수 생성

FlexConfig 개체 내에서 사용하는 변수는 해당 개체 자체 내에서 정의되며, 별도의 변수 목록은 없습니다. 따라서 변수를 정의한 다음 별도의 FlexConfig 개체에서 이를 사용할 수 없습니다.

변수는 다음과 같은 주요 이점을 제공합니다.

- 변수를 사용하면 device manager를 사용하여 정의된 개체를 가리킬 수 있습니다. 변수에는 네트워크, 포트 및 비밀 키 개체가 포함됩니다.
- 변수는 개체 본문에서 변경될 수 있는 값을 분리합니다. 따라서 값을 변경해야 하는 경우 해당 변수만 편집하면 되고 개체 본문을 편집할 필요는 없습니다. 변수는 특히 여러 명령줄에서 개체를 참조해야 하는 경우에 유용합니다.

이 절차에서는 FlexConfig 개체에 변수를 추가하는 프로세스에 대해 설명합니다.

프로시저

단계 **1** **Device(**디바이스**) > Advanced Configuration(**고급 컨피그레이션**)** 페이지에서 FlexConfig 개체를 편집하거나 생성합니다.

FlexConfig 개체 구성, 921 페이지의 내용을 참조하십시오.

단계 **2** **Variables(**변수**)** 섹션에서 다음 작업 중 하나를 수행합니다.

- 변수를 추가하려면 **+** 버튼을 클릭합니다(아직 정의된 변수가 없는 경우에는 **Add Variable(**변수 추가**)**을 클릭).
- 변수를 편집하려면 해당 변수의 편집 아이콘( )을 클릭합니다.

변수를 삭제하려면 해당 변수의 휴지통 아이콘( )을 클릭합니다. 템플릿 본문의 해당 변수 참조를 모두 제거합니다.

단계 **3** 변수의 이름과 설명(선택 사항)을 입력합니다.

단계 **4** 변수의 데이터 **Type(**유형**)**을 선택한 다음 값을 입력하거나 선택합니다.

다음과 같은 유형의 변수를 생성할 수 있습니다. 변수를 사용할 명령의 데이터 요건에 맞는 유형을 선택합니다.

- **String(**문자열**)** — 텍스트 문자열입니다. 예를 들어, 호스트 이름, 사용자 이름 등이 있습니다.
- **Numeric(**숫자**)** — 정수입니다. 쉼표, 10진수, 기호(예: 음수) 또는 16진수 표기법을 포함하지 마십시오. 정수가 아닌 경우에는 문자열 변수를 사용합니다.
- **Boolean(**부울**)** — 논리적 true/false입니다. True 또는 False 중 하나를 선택합니다.
- **Network(**네트워크**)** — Objects(개체) 페이지에 정의되어 있는 네트워크 개체 또는 그룹입니다. 네트워크 개체 또는 그룹을 선택합니다.
- **Port(**포트**)** — Objects(개체) 페이지에 정의되어 있는 TCP 또는 UDP 포트 개체입니다. 포트 개체를 선택합니다. 그룹을 선택하거나 다른 프로토콜에 대한 개체를 선택할 수는 없습니다.
- **Interface(**인터페이스**)** — Device(디바이스) > Interfaces(인터페이스) 페이지에 정의되어 있는 이름이 지정된 인터페이스입니다. 인터페이스를 선택합니다. 이름이 없는 인터페이스는 선택할 수 없습니다.
- **IP** — 넷마스크 또는 접두사 길이를 포함하지 않는 단일 IPv4 또는 IPv6 IP 주소입니다.
- **Secret(**비밀**)** — FlexConfig에 대해 정의된 비밀 키 개체입니다. 개체를 선택합니다. 비밀 키 개체 생성에 대한 자세한 내용은 비밀 키 개체 구성, 931 페이지를 참조하십시오.

단계 **5** Variable(변수) 대화 상자에서 **Add(**추가**)** 또는 **Save(**저장**)**를 클릭합니다.

이제 FlexConfig 개체의 본문 내에 변수를 사용할 수 있습니다. 변수를 참조하는 방법은 변수 유형에 따라 달라집니다. 이러한 변수를 사용하는 방법에 대한 내용은 다음 주제를 참조하십시오.

- 변수 참조: {{variable}} 또는 {{{variable}}}, 924 페이지
- 섹션 {{#key}} {{/key}} 및 역 섹션 {{^key}} {{/key}}, 928 페이지

단계 **6** FlexConfig Object(FlexConfig 개체) 대화 상자에서 **OK(**확인**)**를 클릭합니다.

FlexConfig 변수 참조 및 값 검색

FlexConfig는 Mustache를 템플릿 언어로 사용하지만 다음 섹션에 설명된 기능만 지원합니다. 이러한 기능을 사용하여 변수를 참조하고 해당 값을 검색 및 처리합니다.

변수 참조: {{variable}} 또는 {{{variable}}}

FlexConfig 개체 내에서 정의하는 변수를 참조하려면 다음 표기법을 사용합니다.

{{*variable_name*}}

또는

{{{*variable_name*}}}

이 표기법은 **Numeric(**숫자**)**, **String(**문자열**)**, **Boolean(**부울**)**, **IP** 유형의 변수를 포함하며 단일 값인 간단한 변수에 사용하기에 충분합니다. 변수에 &와 같은 특수 문자가 포함된 경우, 3중 괄호를 사용하십시오. 또는 모든 변수에 대해 항상 3중 괄호를 사용할 수 있습니다.

그러나 컨피그레이션 데이터베이스에서 개체로 모델링되는 요소를 가리키는 변수의 경우, 점 표기법을 사용하고 검색하려는 개체 특성의 이름을 포함해야 합니다. 이러한 특성 이름은 API Explorer에서 관련 개체 유형에 대해 모델을 검사하여 찾을 수 있습니다. **Secret(**비밀**)**, **Network(**네트워크**)**, **Port(**포트**)**, **Interface(**인터페이스**)** 유형의 변수를 사용하려면 다음과 같은 표기법을 사용해야 합니다.

{{*variable_name.attribute*}}

예를 들어, net-object1(네트워크 그룹이 아니라 네트워크 개체를 가리킴)이라는 이름의 네트워크 변수에서 주소를 검색하려면 다음과 같은 표기법을 사용합니다.

{{net-object1.value}}

개체 내에서 개체의 특성 값을 검색하려는 경우, 일련의 점으로 구분된 특성을 사용하여 원하는 값으로 드릴다운해야 합니다. 예를 들어, 인터페이스의 IP 주소는 인터페이스 개체에 대해 ipv4와 ipv6라는 이름의 하위 개체로 모델링됩니다. 따라서 int-inside(내부 인터페이스를 가리킴)라는 이름의 인터페이스 변수에 대한 IPv4 주소 및 서브넷 마스크를 검색하려면 다음과 같은 표기법을 사용합니다.

{{int-inside.ipv4.ipAddress.ipAddress}} {{int-inside.ipv4.ipAddress.netmask}}

참고 API Explorer를 열려면 More options(추가 옵션) 버튼( )을 클릭하고 **API Explorer**를 선택합니다.

다음 표에는 변수 유형, 변수 유형을 참조하는 방법, 그리고 개체의 경우, API 모델의 이름과 사용할 가능성이 가장 높은 참조가 나와 있습니다.

변수 유형	참조 모델	설명

부울
(간단한 변수)
	변수**:**
	{{*variable_name*}}
	섹션**:**
	`{{#variable_name}}`
	`commands`
	`{{/variable_name}}`
	역 섹션**:**
	`{{^variable_name}}`
	`commands`
	`{{/variable_name}}`
		논리적 true/false입니다. 부울 변수는 주로 섹션 또는 역 섹션에 사용합니다. 예를 들어 기능을 주기적으로 또는 특별한 상황에서만 활성화해야 하는 경우, 부울 변수를 편집하여 명령 섹션을 설정 또는 해제할 수 있습니다.
		일부 개체의 경우 모델에 부울 특성도 있으며, 이를 사용하여 선택적으로 섹션을 처리할 수 있습니다.

변수 유형	참조 모델	설명

인터페이스
(개체 변수: API 모델이 인터페이스임)
	변수:
	{{*variable_name*.*attribute*}}
	섹션:
	`{{#variable_name.attribute}}`
	`commands`
	`{{/variable_name.attribute}}`
	역 섹션:
	`{{^variable_name.attribute}}`
	`commands`
	`{{/variable_name.attribute}}`
		Device(디바이스) > Interfaces(인터페이스) 페이지에 정의되어 있는 이름이 지정된 인터페이스입니다. 이름이 없는 인터페이스는 가리킬 수 없습니다.
		인터페이스 모델에서 사용할 수 있는 특성은 다양합니다. 또한, 인터페이스 모델은 예를 들어 IP 주소의 하위 개체를 포함합니다.
		유용하게 활용할 수 있는 몇 가지 주요 특성은 다음과 같습니다.
		• *variable_name*.**name**에서는 인터페이스의 논리적 이름을 반환합니다.
		• *variable_name*.**hardwareName**에서는 GigabitEthernet1/8과 같은 인터페이스 포트 이름을 반환합니다.
		• *variable_name*.**managementOnly**은 부울 값입니다. TRUE는 인터페이스가 관리 전용으로 정의되어 있음을 의미합니다. FALSE는 인터페이스가 디바이스를 통과하는 트래픽용임을 의미합니다. 이 옵션은 섹션 키로 사용할 수 있습니다.
		• *variable_name*.**ipv4.ipAddress.ipAddress**에서는 인터페이스의 IPv4 주소를 반환합니다.
		• *variable_name*.**ipv4.ipAddress.netmask**에서는 인터페이스의 IPv4 주소에 대한 서브넷 마스크를 반환합니다.

IP (간단한 변수)	변수: {{*variable_name*}}	넷마스크 또는 접두사 길이를 포함하지 않는 단일 IPv4 또는 IPv6 IP 주소입니다.

변수 유형	참조 모델	설명
네트워크 (개체 변수: API 모델이 네트워크 개체임)	변수**(**네트워크 개체**):** {{*variable_name*.*attribute*}} 섹션**(**그룹 개체**):** {{#*variable_name*.**networkObjects**}} commands referring to one of {{**value**}} {{**name**}} {{/*variable_name*.**networkObjects**}}	Objects(개체) 페이지에 정의되어 있는 네트워크 개체 또는 그룹입니다. 섹션을 사용하여 네트워크 그룹을 처리할 수 있습니다. 유용하게 활용할 수 있는 주요 특성은 다음과 같습니다. • {{*variable_name*.**name**}}에서는 네트워크 개체 또는 그룹의 이름을 반환합니다. • {{*variable_name*.**value**}}에서는 네트워크 개체(네트워크 그룹이 아님)의 IP 주소 콘텐츠를 반환합니다. 지정된 명령에 대해 콘텐츠 유형이 적절한 네트워크 개체를 사용해야 합니다(예: 서브넷 주소 대신 호스트 주소). • {{*variable_name*.**groups**}}에서는 네트워크 그룹에 포함된 네트워크 개체의 목록을 반환합니다. 이 특성은 네트워크 그룹을 가리키는 변수에만 사용하고, 섹션 태그에서 사용하여 그룹의 콘텐츠를 반복적으로 처리하십시오. {{**value**}} 또는 {{**name**}}(을)를 사용하여 각 네트워크 개체의 콘텐츠를 차례대로 검색하십시오.
숫자 (간단한 변수)	변수**:** {{*variable_name*}}	정수 숫자입니다. 쉼표, 10진수, 기호(예: 음수) 또는 16진수 표기법을 포함하지 마십시오. 정수가 아닌 경우에는 문자열 변수를 사용합니다.
Port(포트) (개체 변수: API 모델이 포트 개체, TCP 포트 또는 UDP 포트임)	변수**:** {{*variable_name*.*attribute*}}	Objects(개체) 페이지에 정의되어 있는 TCP 또는 UDP 포트 개체입니다. 이는 포트 그룹이 아니라 포트 개체여야 합니다. 유용하게 활용할 수 있는 주요 특성은 다음과 같습니다. • {{*variable_name*.**port**}}에서는 포트 번호를 반환합니다. 프로토콜은 포함되지 않습니다. • {{*variable_name*.**name**}}에서는 포트 개체의 이름을 반환합니다.
기밀 (개체 변수: API 모델이 비밀임)	변수**:** {{*variable_name*.**password**}} 또는 {{{*variable_name*.**password**}}}	FlexConfig용으로 정의되어 있는 비밀 키 개체입니다. 암호화된 문자열을 반환하는 **password** 속성에 대한 참조만 수행해야 합니다. 암호에 &와 같은 특수 문자가 포함된 경우, 3중 괄호를 사용하십시오.
문자열 (간단한 변수)	변수**:** {{*variable_name*}}	텍스트 문자열입니다. 예를 들어, 호스트 이름, 사용자 이름 등이 있습니다.

섹션 {{#key}}{{/key}} 및 역 섹션 {{^key}}{{/key}}

섹션 또는 역 섹션은 키를 처리 기준으로 사용하는, 섹션 시작과 끝 태그 사이의 명령 블록입니다. 섹션 처리 방법은 일반 섹션 또는 역 섹션 중 어느 것인지에 따라 달라집니다.

- 일반 섹션(또는 간단하게 섹션)은 키가 TRUE이거나 콘텐츠가 비어 있지 않은 경우 처리됩니다. 키가 FALSE이거나 개체에 콘텐츠가 없는 경우 섹션의 명령은 구성되지 않으며, 섹션은 우회됩니다.

  일반 섹션의 구문은 다음과 같습니다.

  ```
  {{#key}}
  one or more commands
  {{/key}}
  ```

- 역 섹션은 섹션과 반대로 키가 FALSE이거나 개체에 콘텐츠가 없는 경우 처리됩니다. 키가 TRUE이거나 개체에 콘텐츠가 있는 경우, 역 섹션은 우회됩니다.

  역 섹션의 구문은 다음과 같습니다. 차이점은 해시 태그가 캐럿 기호로 바뀐 것뿐입니다.

  ```
  {{^key}}
  one or more commands
  {{/key}}
  ```

다음 주제에서는 섹션 및 역 섹션의 주요 활용 사례에 대해 설명합니다.

다중 값 변수를 처리하는 방법

다중 값 변수 처리의 기본 예는 네트워크 그룹을 가리키는 네트워크 변수입니다. 그룹에는 여러 개체(**objects** 속성 아래)가 포함되어 있으므로 네트워크 그룹에서 값을 반복적으로 검토하여 동일한 명령을 다양한 값으로 여러 번 컨피그레이션할 수 있습니다.

개체 그룹은 개체 속성 내에 포함된 네트워크 개체를 정의하지만, 해당 개체는 포함된 개체의 콘텐츠를 포함하지 않습니다. 대신 **networkObjects** 속성을 사용하여 포함된 개체의 콘텐츠를 가져옵니다.

예를 들어 호스트 192.168.10.0, 192.168.20.0 및 192.168.30.0을 사용하는 net-group이라는 이름의 네트워크 그룹이 있는 경우, 다음 기술을 사용하여 RIP 라우팅의 각 주소에 대해 네트워크 명령을 구성할 수 있습니다. 섹션 시작 **value**에서 사용하면 멤버 개체에서 **net-group.networkObjects** 값 속성을 가져옴을 나타내므로 네트워크 개체의 속성만 사용합니다. FlexConfig 개체 내에서 "값" 특성에 대해 별도의 변수를 생성하지 마십시오.

```
router rip
{{#net-group.networkObjects}}
 network {{value}}
{{/net-group.networkObjects}}
```

시스템은 섹션 구조를 다음과 같이 변환합니다.

```
router rip
   network 192.168.10.0
   network 192.168.20.0
```

```
network 192.168.30.0
```

부울 값 또는 빈 개체를 기준으로 선택적 처리를 수행하는 방법

참고 이 항목의 예시는 설명만을 목적으로 합니다. 예를 들어, FlexConfig를 사용하여 버전 6.7 이상의 SNMP를 설정할 수 없습니다. 대신 threat defense API SNMP 리소스를 사용해야 합니다.

섹션이 섹션 시작 태그의 변수 콘텐츠가 TRUE이거나 개체가 비어 있지 않은 경우에는 처리되고, 부울 값이 FALSE이거나 비어 있는 경우(예: 빈 개체)에는 우회됩니다.

이 기능은 주로 부울 값에 사용됩니다. 예를 들어 부울 변수를 생성하고 이 변수가 적용되는 섹션 내에 명령을 입력할 수 있습니다. 그러면 FlexConfig 개체에서 명령의 섹션을 활성화 또는 비활성화해야 하는 경우, 단순히 부울 변수의 값만 변경하면 되며 코드에서 해당 줄을 삭제하지 않아도 됩니다. 따라서 이 기능은 켜거나 끄기가 쉽습니다.

예를 들어 FlexConfig를 사용하여 SNMP를 활성화하는 경우, SNMP 트랩을 해제할 수 있습니다. 즉, enable-traps라는 이름의 부울 변수를 생성하고 처음에 TRUE로 설정하고 나서 트랩을 해제해야 하는 경우 변수를 편집하여 FALSE로 변경하고 개체를 저장한 다음 컨피그레이션을 다시 구축하기만 하면 됩니다. 명령 시퀀스는 다음과 같이 표시됩니다.

```
snmp-server enable
snmp-server host inside 192.168.1.5
snmp-server community clearTextString
{{#enable-traps}}
snmp-server enable traps all
{{/enable-traps}}
```

또한, 개체 내의 부울 값을 기반으로 이러한 유형의 처리를 수행할 수 있습니다. 예를 들어 인터페이스에 일부 특성을 구성하기 전에 인터페이스가 관리 전용인지를 확인할 수 있습니다. 다음 예에서 int-inside는 inside라는 이름의 인터페이스를 가리키는 인터페이스 변수입니다. FlexConfig는 인터페이스가 관리 전용으로 설정되지 않은 경우에만 인터페이스에 EIGRP 관련 인터페이스 옵션을 구성합니다. 부울 값이 FALSE인 경우에만 명령이 구성되도록 역 섹션을 사용할 수 있습니다.

```
router eigrp 2
 network 192.168.1.0 255.255.255.0
{{^int-inside.managementOnly}}
interface {{int-inside.hardwareName}}
 hello interval eigrp 2 60
 delay 200
{{/int-inside.managementOnly}}
```

FlexConfig 개체의 스마트 CLI 개체 참조

FlexConfig 개체를 생성할 때는 변수를 사용해 device manager 내에서 구성할 수 있는 개체를 가리킬 수 있습니다. 예를 들어 인터페이스 요소 또는 네트워크 개체를 가리키는 변수를 생성할 수 있습니다.

그러나 같은 방식으로 스마트 CLI 개체를 가리킬 수는 없습니다.

대신 FlexConfig 정책에서 사용해야 하는 스마트 CLI 개체를 생성하는 경우 적절한 위치에 스마트 CLI 개체의 이름만 입력하면 됩니다.

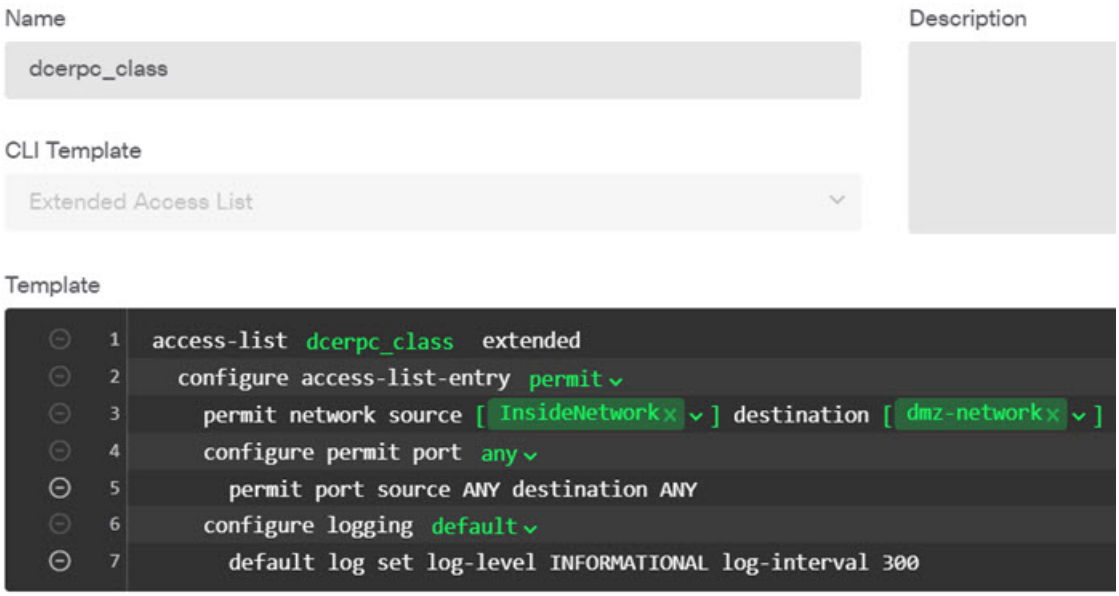
프로토콜 검사를 구성할 때 확장된 액세스 목록을 트래픽 클래스로 사용하려는 경우를 예로 들어 보겠습니다. 확장된 액세스 목록용 스마트 CLI 개체가 있으므로 해당 스마트 CLI 개체를 사용하여 ACL을 생성해야 하며, FlexConfig 개체에서 **access-list** 명령을 사용할 수는 없습니다.

예를 들어 192.168.1.0/24 및 192.168.2.0/24 네트워크 간에 DCERPC 검사를 전역적으로 활성화하려는 경우 다음을 수행합니다.

프로시저

단계 **1** 두 네트워크용으로 각기 별도의 네트워크 개체를 생성합니다. 예를 들어 InsideNetwork 및 dmz-network를 생성합니다.

단계 **2** 스마트 CLI 확장된 액세스 목록 개체에서 이러한 개체를 사용합니다.



단계 **3** 이름을 기준으로 스마트 CLI 개체를 가리키는 FlexConfig 개체를 생성합니다.

예를 들어 개체 이름이 "dcerpc_class"인 경우 FlexConfig 개체는 다음과 같을 수 있습니다. 무효화 템플릿에서는 스마트 CLI 개체를 통해 생성한 액세스 목록을 무효화하지 않습니다. 해당 개체는 실제로 FlexConfig를 통해 생성된 것이 아니기 때문입니다.

Template

```
1  class-map dcerpc_inspection
2   match access-list dcerpc_class
3  policy-map global_policy
4   class dcerpc_inspection
5    inspect dcerpc
```

Negate Template

```
1  policy-map global_policy
2   no class dcerpc_inspection
3  no class-map dcerpc_inspection
```

단계 **4** FlexConfig 정책에 개체를 추가합니다.

비밀 키 개체 구성

비밀 키 개체는 비밀번호 또는 민감한 문자열이 명확하게 표시되지 않게 하기 위해 사용됩니다. FlexConfig 개체 또는 스마트 CLI 템플릿에 사용된 문자열을 누군가가 보지 못하게 하려면 해당 문자열에 대해 비밀 키 개체를 생성합니다.

프로시저

단계 **1** 목차에서 **Objects(**개체**)**와 **Secret Keys(**비밀 키**)**를 차례로 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 개체를 생성하려면 + 버튼을 클릭합니다.
- 개체를 수정하려면 개체의 수정 아이콘()을 클릭하십시오.

참조되지 않는 개체를 삭제하려면 해당 개체의 휴지통 아이콘()을 클릭합니다.

단계 **3** 개체의 Name(이름) 및 설명(선택 사항)을 입력합니다.

단계 **4** **Password(**비밀번호**)** 및 **Confirm Password(**비밀번호 확인**)** 필드에 비밀번호 또는 기타 비밀 문자열을 입력합니다.

그러면 입력한 텍스트가 명확하지 않게 표시됩니다.

단계 **5** **OK(**확인**)**를 클릭합니다.

다음에 수행할 작업

- 새 개체의 경우 FlexConfig에서 이를 사용하려면 FlexConfig 개체를 편집하고 비밀 키 유형의 변수를 생성한 다음 해당 개체를 선택합니다. 그런 다음 개체 본문 내의 변수를 참조하십시오. 자세한 내용은 FlexConfig 개체에서 변수 생성, 923 페이지의 내용을 참고하십시오.
- FlexConfig 정책의 일부인 FlexConfig 개체에서 사용된 기존 개체를 편집하는 경우, 컨피그레이션을 구축하여 디바이스를 새로운 문자열로 업데이트해야 합니다.
- 스마트 CLI 템플릿에서 명령에 비밀 키가 필요한 경우 관련 속성을 편집할 때 해당하는 개체의 목록이 표시됩니다. 이에 맞게 적절한 키를 선택합니다.

FlexConfig 정책 트러블슈팅

FlexConfig 정책을 편집하고 나서 다음 구축 결과를 주의 깊게 검토합니다. Pending Changes(보류 중인 변경 사항) 대화 상자에 "Last Deployment Failed(마지막 구축 실패함)" 메시지가 표시되면 **See Details(**세부 사항 참조**)** 링크를 클릭합니다. 이 링크를 클릭하면 감사 로그로 이동하여 실패한 구축 작업을 찾을 수 있습니다. 특정 오류 메시지를 찾으려면 해당 작업을 엽니다.

FlexConfig 문제로 인해 구축에 실패한 경우, 세부 사항에서는 올바르지 않은 명령을 사용하는 FlexConfig 개체에 대해 언급하며 실패한 명령을 표시합니다. 이 정보를 사용하여 개체를 수정하고 다시 구축을 시도합니다. 개체 이름은 링크이므로, 이 링크를 클릭하여 개체에 대한 편집 대화 상자를 엽니다.

예를 들어 TCP MSS(최대 TCP 세그먼트 크기)를 구성하려는 경우, **sysopt connection tcpmss** 명령을 사용하여 이 설정을 제어할 수 있습니다. device manager에서 구성한 경우, 이 옵션에 대한 threat defense 기본값은 0입니다(ASA 기본값은 1380).

ASA 기본값은 기본 MTU(1500)를 사용하는 인터페이스에서 IPv4 VPN을 실행하는 경우 최적의 처리를 수행할 수 있도록 설계되어 있습니다. 시스템에서는 VPN 헤더에 120바이트를 필요로 합니다. IPv6의 경우, 시스템에서는 140바이트를 필요로 합니다. threat defense의 기본값인 0을 사용하면 엔드포인트에서 MSS를 협상할 수 있습니다. 이 설정은 정상적인 트래픽에 대해, 특히 1500을 넘는 MTU를 비롯하여 디바이스의 인터페이스 전체에서 서로 다른 MTU를 사용하는 경우, 이상적입니다. TCP MSS는 인터페이스별 설정이 아니라 글로벌 설정이므로 상당한 비율의 트래픽이 VPN을 통과하며 과도한 프래그멘테이션이 발생하는 경우에만 변경할 수 있습니다. 이 경우, TCP MSS를 MTU에서 120을 뺀 값(IPv4의 경우) 또는 MTU에서 140을 뺀 값(IPv6의 경우)으로 설정하고 모든 인터페이스에 대해 동일한 MTU를 사용할 수 있습니다. MSS를 명시적으로 설정하더라도 TLS/SSL 암호 해독 또는 서버 검색과 같은 구성 요소에 특정 MSS가 필요한 경우, 인터페이스 MTU를 기반으로 해당 MSS를 설정하고 MSS 설정을 무시합니다.

실례를 들기 위해 TCP MSS를 3바이트로 설정했다고 가정해 보겠습니다. 이 경우 명령에서 48바이트를 최솟값으로 사용하므로 다음과 유사한 구축 오류가 발생하게 됩니다.

오류는 다음과 같은 요소로 구성됩니다.

1. 구축 오류 메시지에는 오류를 야기한 FlexConfig 개체의 이름이 포함되어 있습니다. 개체 이름은 편집 대화 상자와 연결되므로 신속하게 개체를 열고 오류를 수정할 수 있습니다. 메시지의 첫 번째 문장에 이 내용이 포함됩니다.
2. "ERROR(오류):"로 시작되는 텍스트는 디바이스에서 반환된 메시지입니다. 이 메시지는 잘못된 명령을 입력한 경우 SSH 클라이언트를 포맷하지 않고 ASA가 대응하는 방식을 정확히 나타냅니다. 이 예에서 오류 메시지는 "ERROR: [3] is smaller than the minimum allowed MSS of 48 by RFC 791.(오류: [3]이 RFC 791에서 허용되는 최소 MSS 값인 48보다 작습니다.)"입니다. "Config Error(컨피그레이션 오류)"로 시작되는 텍스트에 오류 메시지를 생성한 특정 행이 나와 있습니다.
3. 검은색 텍스트는 오류를 야기한 FlexConfig 개체의 실제 줄이며, 이 줄은 수정해야 합니다. 이 예에서 MTU가 1500인 인터페이스(일반적인 상황)에서 IPv4 VPN 트래픽을 수용하려면 3을 1380으로 변경합니다.

   이 예를 수정할 때 CLI 콘솔을 열어 두고 **show running-config all sysopt**(을)를 사용하여 **sysopt** 명령 설정을 모두 확인할 수 있습니다. 대부분의 **sysopt** 명령에는 대부분의 용도에 적절한 기본 설정이 있으므로 실행 중인 컨피그레이션에는 기본 설정이 표시되지 않습니다. **all** 키워드를 사용하면 출력에 이러한 기본 설정이 포함됩니다.

FlexConfig의 예시

다음 주제에서는 FlexConfig를 사용하여 기능을 구성하는 몇 가지 예시를 제공합니다.

전역 기본 검사를 활성화/비활성화하는 방법

동적으로 할당된 포트의 개방형 보조 채널이나 사용자 데이터 패킷에 IP 주소 지정 정보를 포함하는 프로토콜도 있습니다. 이러한 프로토콜의 경우 NAT를 적용하고 보조 채널을 허용할 수 있도록 시스템이 심층 패킷 검사를 수행해야 합니다. 기본적으로 시스템에서는 몇 가지 일반적인 검사 엔진이 활성화되지만 네트워크에 따라 다른 엔진을 활성화하거나 기본 검사를 비활성화해야 할 수도 있습니다.

현재 활성화된 검사의 목록을 확인하려면 CLI 콘솔이나 SSH 세션에서 **show running-config policy-map** 명령을 사용합니다. 아래에는 검사 컨피그레이션을 변경하지 않은 시스템에서 이 명령을 실행하는 경우 표시되는 출력이 나와 있습니다. 이 출력의 끝에 나와 있는 **inspect** 명령의 목록에 활성화된 프로토콜 검사가 표시됩니다. 위의 명령은 inspection_default 트래픽 클래스(일반 프로토콜 및 해당하는 경우 검사되는 프로토콜의 포트 번호)에서 이러한 검사를 활성화합니다. 이 클래스는 service-policy 명령(출력에는 표시되지 않음)을 사용하여 모든 인터페이스에서 이러한 검사를 적용하는 global_policy 정책 맵의 일부분입니다. 예를 들어 ICMP 검사는 디바이스를 통과하는 모든 ICMP 트래픽에 대해 수행됩니다.

```
> show running-config policy-map
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
```

```
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
  inspect icmp
  inspect icmp error
!
```

참고 각 검사의 자세한 설명은 https://www.cisco.com/c/en/us/support/security/asa-firepower-services/products-installation-and-configuration-guides-list.html에서 제공되는 *Cisco ASA Series* 방화벽 컨피그레이션 가이드를 참조하십시오.

다음 절차에서는 전역적으로 적용된 이 기본 검사 클래스에서 검사를 활성화하거나 비활성화하는 방법을 보여줍니다. 이 방법을 설명하기 위해 예시에서는 다음을 수행합니다.

- PPTP(Point-to-Point Tunneling Protocol)를 활성화합니다. 이 프로토콜은 엔드포인트에 간의 지점 간 연결을 터널링하는 데 사용됩니다.
- SIP(Session Initiation Protocol)를 비활성화합니다. 일반적으로는 검사로 인해 네트워크에 문제가 발생하는 경우에만 SIP를 비활성화합니다. 그러나 SIP를 비활성화하는 경우에는 액세스 제어 정책이 SIP 트래픽(UDP/TCP 5060)과 동적으로 할당된 포트를 허용하며 SIP 연결에 대해 NAT 지원이 필요하지 않은지를 확인해야 합니다. 그리고 확인 결과에 따라 FlexConfig가 아닌 표준 페이지를 통해 액세스 제어 및 NAT 정책을 조정합니다.

시작하기 전에

적절한 계획을 세우면 FlexConfig를 효율적으로 사용할 수 있습니다. 이 예시에서는 동일 트래픽 클래스에서 서로 다르며 관련이 없는 두 검사를 변경합니다. 하지만 이러한 정책을 변경해야 하는 경우에는 독립적으로 변경하게 될 가능성이 높습니다.

따라서 이 예시의 각 검사에 대해 각기 별도의 FlexConfig 개체를 생성하는 것이 좋습니다. 이렇게 하면 다른 검사의 설정을 변경하지 않고도 한 검사의 설정을 쉽게 변경할 수 있으며, FlexConfig 개체를 수정할 필요도 없습니다.

프로시저

단계 **1** **Device(**디바이스**)** > **Advanced Configuration(**고급 컨피그레이션**)**에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

단계 **2** Advanced Configuration(고급 컨피그레이션) 목차에서 **FlexConfig** > **FlexConfig Objects(FlexConfig** 개체**)**를 클릭합니다.

단계 **3** PPTP 검사를 활성화하는 개체를 생성합니다.

a) **+** 버튼을 클릭하여 새 개체를 생성합니다.

b) 개체의 이름을 입력합니다. 예를 들어 **Enable_PPTP_Global_Inspection**을 입력합니다.

c) **Template(**템플릿**)** 편집기에서 들여쓰기를 포함하여 다음 줄을 입력합니다.

```
policy-map global_policy
 class inspection_default
  inspect pptp
```

d) **Negate Template(**무효화 템플릿**)** 편집기에 이 컨피그레이션을 실행 취소하는 데 필요한 행을 입력합니다.

명령을 활성화하려면 상위 명령을 포함해 명령에 대해 정확한 하위 모드를 입력해야 하는 것과 마찬가지로, 무효화 템플릿에도 해당 명령을 포함해야 합니다.

무효화 템플릿은 이 개체를 정상적으로 구축한 후에 FlexConfig 정책에서 제거하는 경우에 적용되며, 실패한 구축 중에도 컨피그레이션을 이전 상태로 재설정하기 위해 적용됩니다.

그러므로 이 예시에서 무효화 템플릿은 다음과 같습니다.

```
policy-map global_policy
 class inspection_default
  no inspect pptp
```

개체는 다음과 같이 표시됩니다.

고급 컨피그레이션

참고 inspection_default 클래스에는 다른 검사 명령이 활성화되어 있으므로 전체 클래스를 무효화해서는 안 됩니다. 마찬가지로 global_policy 정책 맵도 이러한 기타 검사가 포함되어 있으므로 정책 맵 역시 무효화하면 안 됩니다.

e) **OK(**확인**)**를 클릭하여 개체를 저장합니다.

단계 **4** SIP 검사를 비활성화하는 개체를 생성합니다.

a) + 버튼을 클릭하여 새 개체를 생성합니다.

b) 개체의 이름을 입력합니다. 예를 들어 **Disable_SIP_Global_Inspection**을 입력합니다.

c) **Template(**템플릿**)** 편집기에서 들여쓰기를 포함하여 다음 줄을 입력합니다.

```
policy-map global_policy
 class inspection_default
  no inspect sip
```

d) **Negate Template(**무효화 템플릿**)** 편집기에 이 컨피그레이션을 실행 취소하는 데 필요한 행을 입력합니다.

비활성화를 수행하는 "no" 명령에 대한 "negate" 명령이 기능을 활성화하는 명령입니다. 즉, "negate" 템플릿은 단지 기능을 비활성화하는 명령이 아니라 "positive" 템플릿에서 수행하는 모든 작업을 되돌리는 명령입니다. 이처럼 negate 템플릿의 핵심 기능은 변경 사항을 실행 취소하는 것입니다.

그러므로 이 예시에서 무효화 템플릿은 다음과 같습니다.

```
policy-map global_policy
 class inspection_default
  inspect sip
```

개체는 다음과 같이 표시됩니다.

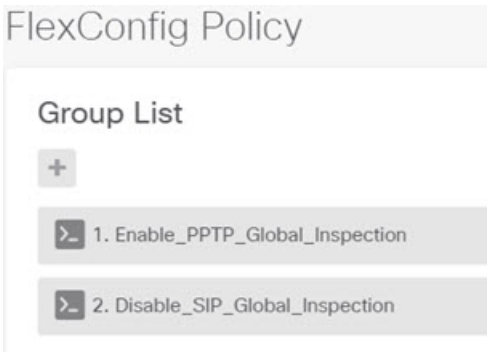
e) **OK(**확인**)**를 클릭하여 개체를 저장합니다.

단계 **5** FlexConfig 정책에 개체를 추가합니다.

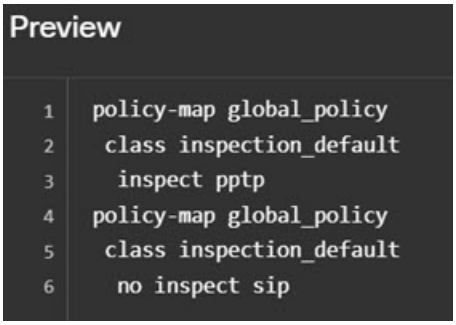
개체를 생성하는 것만으로는 충분하지 않습니다. 개체는 FlexConfig 정책에 추가하고 변경 사항을 저장해야 구축됩니다. 이렇게 하면 완료되지 않은 작업에서 구축 장애 발생 위험 없이 개체를 사용하여 실험을 하고 개체를 부분적으로 완성된 상태로 남겨 둘 수 있습니다. 그런 후에는 개체를 추가 및 제거만 하면 기능을 쉽게 켜거나 끌 수 있으며 매번 개체를 다시 생성할 필요가 없습니다.

a) 목차에서 **FlexConfig Policy(FlexConfig** 정책**)**를 클릭합니다.
b) Group List(그룹 목록)에서 +를 클릭합니다.
c) Enable_PPTP_Global_Inspection 및 Disable_SIP_Global_Inspection 개체를 선택하고 **OK(**확인**)**를 클릭합니다.

그룹 목록은 다음과 같이 표시됩니다.



템플릿의 명령으로 미리보기가 업데이트됩니다. 올바른 명령이 표시되는지 확인합니다.



d) **Save(**저장**)**를 클릭합니다.

이제 정책을 구축할 수 있습니다.

단계 **6** 변경 사항을 커밋합니다.

a) 웹 페이지의 오른쪽 상단에 있는 **Deploy Changes(**변경 사항 구축**)** 아이콘을 클릭합니다.

b) **Deploy Now(**지금 구축**)** 버튼을 클릭합니다.

구축이 완료될 때까지 기다리거나 **OK(**확인**)**를 클릭하고 나중에 작업 목록 또는 구축 기록을 확인할 수 있습니다.

단계 **7** CLI 콘솔 또는 SSH 세션에서 **show running-config policy-map** 명령을 사용하여 실행 중인 컨피그레이션에 정확한 변경 사항이 적용되었는지 확인합니다.

다음 출력에서는 **inspect pptp**(이)가 inspection_default 클래스 맵 아래에 추가되었으며 **inspect sip**(은)는 더 이상 클래스에 포함되어 있지 않다는 점에 유의하십시오. 즉, FlexConfig 개체에 정의된 변경 사항이 정상적으로 구축되었음을 확인할 수 있습니다.

```
> show running-config policy-map
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
```

```
  no tcp-inspection
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect netbios
  inspect tftp
  inspect ip-options
  inspect icmp
  inspect icmp error
  inspect pptp
!
```

FlexConfig 변경 사항을 실행 취소하는 방법

FlexConfig 개체에 정확한 무효화 템플릿을 입력하는 경우 해당 개체를 사용하여 적용한 변경 사항을 쉽게 제거할 수 있습니다. FlexConfig 정책에서 개체를 삭제하기만 하면 되며, 그러면 다음 구축에서 시스템이 무효화 템플릿을 사용하여 변경을 실행 취소합니다.

그러므로 변경을 실행 취소하기 위해 새 개체를 생성할 필요가 없습니다.

다음 예시에서는 전역 SIP 검사를 다시 활성화하는 방법을 보여 줍니다. 이 예시에서는 전역 기본 검사를 활성화/비활성화하는 방법, 933 페이지에서 설명하는 변경 사항을 되돌려 SIP 검사를 비활성화합니다.

시작하기 전에

FlexConfig 개체에 정확한 무효화 템플릿이 있는지 확인합니다. 정확한 무효화 템플릿이 없으면 무효화 템플릿이 정확해지도록 개체를 수정합니다.

프로시저

단계 **1** **Device(**디바이스**)** > **Advanced Configuration(**고급 컨피그레이션**)**에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

단계 **2** Advanced Configuration(고급 컨피그레이션) 목차에서 **FlexConfig** > **FlexConfig Policy(FlexConfig** 정책**)**를 클릭합니다.

단계 **3** FlexConfig 정책에서 **Disable_SIP_Global_Inspection** 개체 항목 오른쪽의 **X**를 클릭하여 정책에서 개체를 삭제합니다.

개체의 명령이 미리보기에서 제거됩니다. 무효화 명령은 미리보기에 추가되지 않으며 백그라운드에서 실행됩니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

단계 **5** 변경 사항을 커밋합니다.

a) 웹 페이지의 오른쪽 상단에 있는 **Deploy Changes(**변경 사항 구축**)** 아이콘을 클릭합니다.

b) **Deploy Now(**지금 구축**)** 버튼을 클릭합니다.

구축이 완료될 때까지 기다리거나 **OK(**확인**)**를 클릭하고 나중에 작업 목록 또는 구축 기록을 확인할 수 있습니다.

단계 **6** CLI 콘솔 또는 SSH 세션에서 **show running-config policy-map** 명령을 사용하여 실행 중인 컨피그레이션에 정확한 변경 사항이 적용되었는지 확인합니다.

다음 출력에서는 **inspect sip**(이)가 inspection_default 클래스 맵 아래에 추가되었습니다. 즉, FlexConfig 개체에 정의된 변경 사항이 정상적으로 구축되었음을 확인할 수 있습니다. (이 클래스에서 순서는 중요하지 않으므로 **inspect sip**(이)가 원래 위치가 아닌 끝에 있어도 상관없습니다.)

```
> show running-config policy-map
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect netbios
  inspect tftp
  inspect ip-options
  inspect icmp
  inspect icmp error
  inspect pptp
  inspect sip
!
```

고유한 트래픽 클래스에 대한 검사를 활성화하는 방법

이 예시에서는 특정 인터페이스의 두 엔드포인트 간 트래픽에 대해 PPTP 검사를 활성화합니다. 이렇게 하면 사이에 포인트 투 포인트 터널이 구성되어 있는 엔드포인트만 검사 대상으로 지정됩니다.

두 엔드포인트 간에 PPTP 검사를 활성화하는 데 필요한 CLI에는 다음 항목이 포함됩니다.

1. 소스와 대상이 엔드포인트 호스트의 IP 주소로 설정된 ACL.
2. 이 ACL을 참조하는 트래픽 클래스.
3. 트래픽 클래스를 포함하며 트래픽 클래스에 대해 PPTP 검사를 활성화하는 정책 맵.
4. 정책 맵을 원하는 인터페이스에 적용하는 서비스 정책. 이 단계에서 정책과 검사가 실제로 활성화됩니다.

참고 검사와 관련된 서비스 정책의 자세한 설명은 https://www.cisco.com/c/en/us/support/security/asa-firepower-services/products-installation-and-configuration-guides-list.html에서 제공되는 *Cisco ASA Series* 방화벽 컨피그레이션 가이드를 참조하십시오.

프로시저

단계 **1** **Device(**디바이스**)** > **Advanced Configuration(**고급 컨피그레이션**)**에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

단계 **2** Advanced Configuration(고급 컨피그레이션) 목차에서 **FlexConfig** > **FlexConfig Objects(FlexConfig** 개체**)**를 클릭합니다.

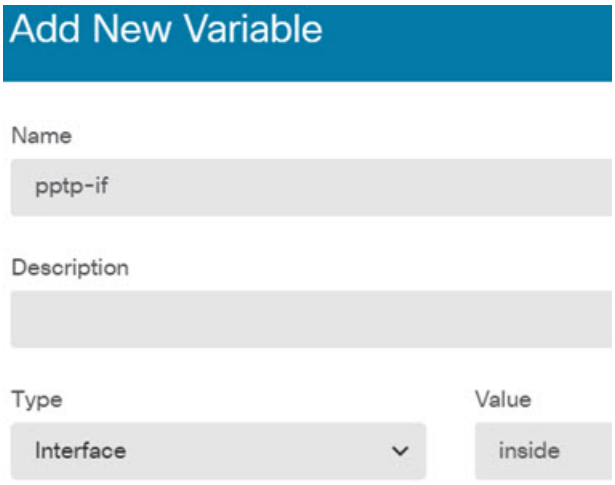
단계 **3** + 버튼을 클릭하여 새 개체를 생성합니다.

단계 **4** 개체의 이름을 입력합니다. 예를 들어 **Enable_PPTP_Inspection_on_Interface**를 입력합니다.

단계 **5** 내부 인터페이스에 대한 변수를 추가합니다.

a) Variables(변수) 목록 위의 +를 클릭합니다.
b) 변수의 이름을 **pptp-if**와 같이 입력합니다.
c) **Type(**유형**)**으로는 **Interface(**인터페이스**)**를 선택합니다.
d) **Value(**값**)**로는 **inside(**내부**)** 인터페이스를 선택합니다.

대화 상자는 다음과 같이 표시됩니다.



e) **Add(**추가**)**를 클릭합니다.

단계 **6** **Template(**템플릿**)** 편집기에서 들여쓰기를 포함하여 다음 줄을 입력합니다.

```
access-list MATCH_ACL permit ip host 192.168.1.55 host 198.51.100.1
class-map MATCH_CMAP
 match access-list MATCH_ACL
policy-map PPTP_POLICY
 class MATCH_CMAP
  inspect pptp
service-policy PPTP_POLICY interface {{pptp-if.name}}
```

변수를 사용하려면 이중 중괄호 사이에 변수 이름을 입력합니다. 또한 점 표기법을 사용하여 검색할 특성을 선택해야 합니다. 인터페이스를 정의하는 개체에는 여러 특성이 포함되어 있기 때문입니다. 인터페이스 이름은 "name" 특성에 포함되어 있으므로 **{{pptp-if.name}}**을 입력하면 변수에 할당된 인터페이스에 대한 name 특성의 값이 검색됩니다. PPTP 검사용 인터페이스를 변경해야 하는 경우 변수 정의에서 다른 인터페이스만 선택하면 됩니다.

단계 **7** **Negate Template(**무효화 템플릿**)** 편집기에 이 컨피그레이션을 실행 취소하는 데 필요한 행을 입력합니다.

이 예시의 경우 PPTP 검사 적용에만 사용되는 클래스 맵, 정책 맵 및 서비스 정책이 있다고 가정합니다. 따라서 무효화 템플릿에서 이러한 항목을 모두 제거할 것입니다.

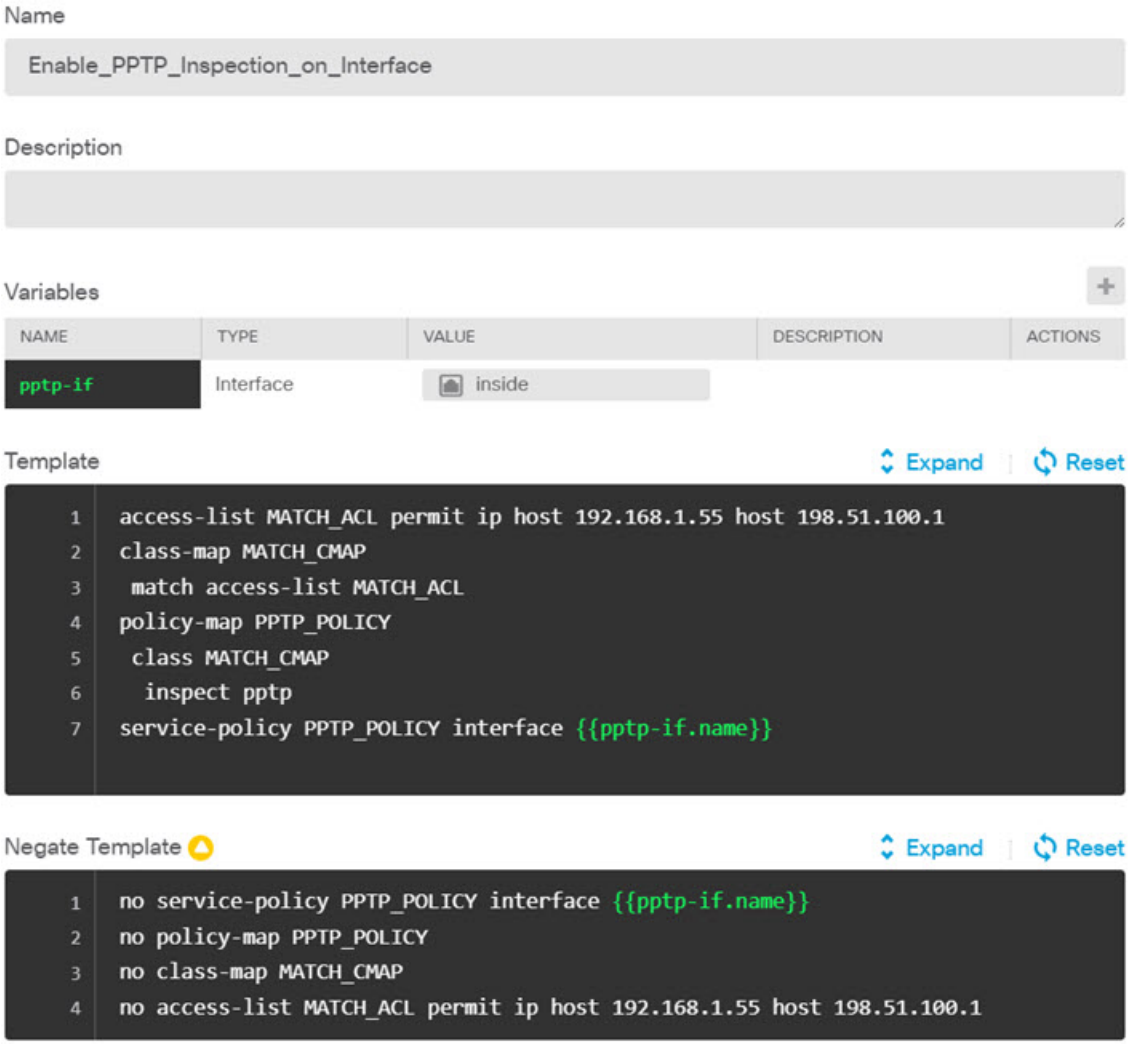
그러나 인터페이스의 기존 서비스 정책에 PPTP 검사를 실제로 추가하는 경우에는 정책 맵이나 서비스 정책을 무효화하지 않습니다. 정책 맵에서 클래스를 무효화하거나, 정책 맵에 포함된 클래스 내에서 검사만 끕니다. 무효화 템플릿 사용 시에 의도하지 않은 결과가 발생하지 않도록 다른 FlexConfig 개체에서 구현하는 내용을 명확하게 파악해야 합니다.

중첩된 항목을 삭제할 때는 해당 항목을 생성할 때와 반대 순서로 삭제해야 합니다. 따라서 먼저 서비스 정책부터 삭제하고 액세스 목록은 맨 끝에 삭제합니다. 이렇게 하지 않으면 사용 중인 개체 삭제를 시도하게 되므로 시스템에서 오류를 반환하며 개체를 삭제할 수 없습니다.

```
no service-policy PPTP_POLICY interface {{pptp-if.name}}
no policy-map PPTP_POLICY
no class-map MATCH_CMAP
```

```
no access-list MATCH_ACL permit ip host 192.168.1.55 host 198.51.100.1
```

개체는 다음과 같이 표시됩니다.



단계 **8** **OK(**확인**)**를 클릭하여 개체를 저장합니다.

단계 **9** FlexConfig 정책에 개체를 추가합니다.

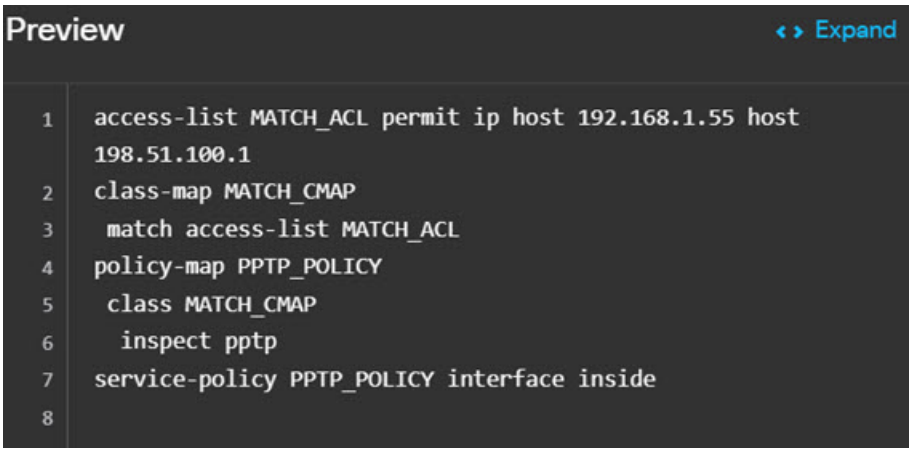
a) 목차에서 **FlexConfig Policy(FlexConfig** 정책**)**를 클릭합니다.

b) Group List(그룹 목록)에서 +를 클릭합니다.

c) **Enable_PPTP_Inspection_on_Interface** 개체를 선택하고 **OK(**확인**)**를 클릭합니다.

그룹 목록은 다음과 같이 표시됩니다.

템플릿의 명령으로 미리보기가 업데이트됩니다. 다음 그림에서와 같이 필요한 명령이 표시되는지 확인합니다. 인터페이스 변수는 미리보기에서 "inside"라는 이름으로 확인됩니다. 미리보기에서 정확하게 확인되지 않는 변수는 정확하게 구축되지 않으므로 변수를 자세히 확인하십시오. 미리보기에서 정확한 변수 변환이 표시될 때까지 FlexConfig 개체를 수정합니다.



d) **Save(**저장**)**를 클릭합니다.

이제 정책을 구축할 수 있습니다.

단계 **10** 변경 사항을 커밋합니다.

a) 웹 페이지의 오른쪽 상단에 있는 **Deploy Changes(**변경 사항 구축**)** 아이콘을 클릭합니다.

b) **Deploy Now(**지금 구축**)** 버튼을 클릭합니다.

구축이 완료될 때까지 기다리거나 **OK(**확인**)**를 클릭하고 나중에 작업 목록 또는 구축 기록을 확인할 수 있습니다.

단계 **11** CLI 콘솔 또는 SSH 세션에서 **show running-config** 명령의 변형을 사용하여 실행 중인 컨피그레이션에 정확한 변경 사항이 적용되었는지 확인합니다.

show running-config(을)를 입력하여 전체 CLI 컨피그레이션을 검사하거나 다음 명령을 사용하여 이 컨피그레이션의 각 부분을 확인할 수 있습니다.

- **show running-config access-list MATCH_ACL** ACL 확인.

- **show running-config class** 클래스 맵 확인. 이 명령을 실행하면 모든 클래스 맵이 표시됩니다.
- **show running-config policy-map PPTP_POLICY** 클래스 및 정책 맵 컨피그레이션 확인.
- **show running-config service-policy** 정책 맵이 인터페이스에 적용되었는지 확인. 이 명령을 실행하면 모든 서비스 정책이 표시됩니다.

이 명령의 시퀀스가 나와 있는 다음 출력을 통해 컨피그레이션이 정확하게 적용되었음을 확인할 수 있습니다.

```
> show running-config access-list MATCH_ACL
access-list MATCH_ACL extended permit ip host 192.168.1.55 host 198.51.100.1

> show running-config class
!
class-map MATCH_CMAP
 match access-list MATCH_ACL
class-map inspection_default
 match default-inspection-traffic
!

> show running-config policy-map PPTP_POLICY
!
policy-map PPTP_POLICY
 class MATCH_CMAP
  inspect pptp
!
> show running-config service-policy
service-policy global_policy global
service-policy PPTP_POLICY interface inside
```

고급 컨피그레이션