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 업로드의 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, 9 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 구성의 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 구성의 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 구성를 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, 13 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 소스의 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 구성의 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 구성의 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, 5 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, 6 페이지의 내용을 참조하십시오.
비밀 키	스마트 CLI 및 FlexConfig 정책	비밀 키 개체는 암호화하여 숨기려는 비밀번호 또는 기타 인증 문자열을 정의합니다. 비밀 키 개체 구성의 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, 8 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, 15 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 컨피그레이션의 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 설정의 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, 13 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, 11 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 구성의 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 호스트 주소(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 컨피그레이션를 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 방법를 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 구성의 내용을 참조하십시오.

단계 **5** **OK(**확인**)**를 클릭합니다.