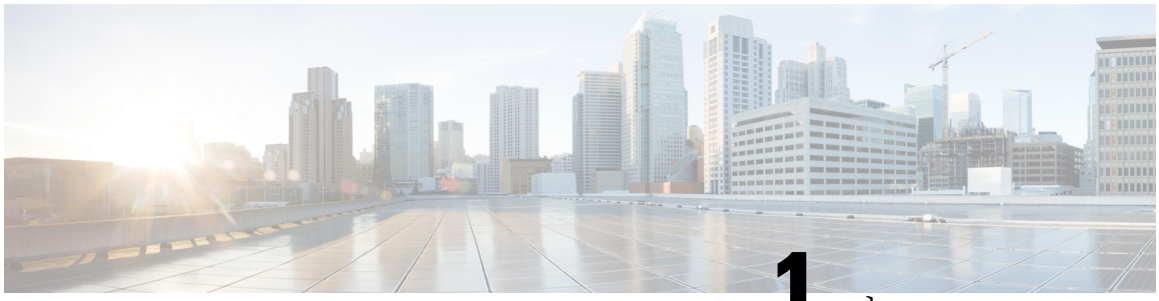
Microsoft Azure Cloud용 Cisco Secure Firewall Threat Defense Virtual 시작 가이드

초판: 2018년 8월 23일

최종 변경: 2022년 5월 31일

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



1 장

Secure Firewall Threat Defense Virtual 및 Azure 시작하기

Secure Firewall Threat Defense Virtual(이전 Firepower Threat Defense Virtual)는 Cisco의 Firepower NGFW(Next-Generation Firewall) 기능을 가상화된 환경으로 가져와 일관된 보안 정책으로 물리, 가상 및 클라우드 환경 전반 및 클라우드 간 워크로드를 준수하도록 합니다.

이 장에서는 기능 지원, 시스템 요구 사항, 지침, 제한 사항 등 Azure 마켓플레이스 내에서의 threat defense virtual 기능에 대해 설명합니다. 이 장에서는 threat defense virtual을(를) 관리하기 위한 옵션에 대해서도 설명합니다.

구축을 시작하기 전에 관리 옵션을 이해하는 것이 중요합니다. Secure Firewall Management Center(이전 Firepower Management Center) 또는 Secure Firewall device manager(이전 Firepower Device Manager)를 사용하여 threat defense virtual를 관리하고 모니터링할 수 있습니다. 다른 관리 옵션을 사용할 수도 있습니다.

Threat Defense Virtual 및 Microsoft Azure Cloud

Secure Firewall Threat Defense Virtual는 Microsoft Azure 마켓플레이스에 통합되며 다음 인스턴스 유형을 지원합니다.

- Standard D3—4 vCPUs, 14 GB, 4vNICs

- Standard D3_v2—4 vCPUs, 14 GB, 4vNICs
- Standard D4_v2—8 vCPUs, 28 GB, 8vNICs (버전 **6.5**의 신규 유형)
- Standard D5_v2—16 vCPUs, 56 GB, 8vNICs (버전 **6.5**의 신규 유형)
- Standard_D8s_v3—8 vCPU, 32GB, 4vNIC(버전 7.1의 새로운 기능)
- Standard_D16s_v3—16 vCPU, 64GB, 8vNIC(버전 7.1의 새로운 기능)
- Standard_F8s_v2—8 vCPUs, 16 GB, 4vNICs (버전 **7.1**의 새로운 기능)
- Standard_F16s_v2—16 vCPU, 32GB, 4vNIC(버전 7.1의 새로운 기능)

Threat Defense Virtual 및 Azure의 사전 요건과 일반 요건

사전 요건

- Microsoft Azure 계정. https://azure.microsoft.com/en-us/에서 하나를 생성할 수 있습니다.

  Azure에서 계정을 생성한 후에 로그인하여 마켓플레이스에서 Cisco Firepower Threat Defense를 검색하고 Cisco Firepower NGFW Virtual(NGFWv) 제품을 선택할 수 있습니다.

- Cisco Smart Account는 Cisco Software Central에서 생성할 수 있습니다.

  threat defense virtual의 라이선스, Cisco Firepower System 기능 라이선스에서 유용한 링크를 포함해 방화벽 시스템의 기능 라이선스 개요를 확인할 수 있습니다.

- threat defense virtual 및 시스템 호환성에 대해서는 Threat Defense Virtual 호환성을 참조하십시오.

통신 경로

- 관리 인터페이스—threat defense virtual을 보안 방화벽 관리 센터에 연결하는 데 사용합니다.

Note 6.7 이상 버전에서는 선택적으로 관리 인터페이스 대신 management center 관리용 데이터 인터페이스를 구성할 수 있습니다. 관리 인터페이스는 데이터 인터페이스 관리를 위한 전제 조건이므로 초기 설정에서 구성해야합니다. management center 액세스를 위한 데이터 인터페이스 구성에 대한 자세한 내용은 Secure Firewall Threat Defense 명령 참조에서 **configure network management-data-interface** 명령을 참조하십시오.

- 진단 인터페이스—진단 및 보고에 사용되며 통과 트래픽에는 사용할 수 없습니다.
- 내부 인터페이스(필수)—threat defense virtual를 내부 호스트에 연결하는 데 사용합니다.
- 외부 인터페이스(필수)—threat defense virtual를 공용 네트워크에 연결하는 데 사용합니다.

Threat Defense Virtual 및 Azure에 대한 지침과 제한

지원 기능

- 라우팅된 방화벽 모드만 해당
- Azure Accelerated Networking(AN)
- IPv6
- 관리 모드, 두 가지 중 하나:
  - 보안 방화벽 관리 센터를 사용하여 threat defense virtual를 관리할 수 있습니다. 보안 방화벽 관리 센터로 Secure Firewall Threat Defense Virtual 관리를 참조하십시오.
  - 통합 Secure Firewall device manager을 사용하여 threat defense virtual를 관리할 수 있습니다. Secure Firewall device manager로 Secure Firewall Threat Defense Virtual 관리를 참조하십시오.
- 공용 IP 주소 지정 - 공용 IP 주소를 Management 0/0 및 GigabitEthernet0/0에 할당합니다.

  필요에 따라 공용 IP 주소를 다른 인터페이스에 할당 할 수 있습니다. 공용 IP 주소를 생성, 변경 또는 삭제하는 방법을 비롯하여 퍼블릭 IP와 관련된 Azure 지침은 Public IP addresses를 참조하십시오.
- 인터페이스:
  - threat defense virtual 기본적으로 4개의 vNIC로 구축합니다.
  - 더 큰 인스턴스 지원을 통해 최대 8개의 vNIC로 threat defense virtual를 구축할 수 있습니다.
  - 추가 vNIC를 threat defense virtual 구축에 추가하려면 Microsoft의 Add network interfaces to or remove network interfaces from virtual machines에서 제공하는 지침을 따르십시오.
  - 관리자를 사용하여 threat defense virtual 인터페이스를 구성합니다. 인터페이스 지원 및 구성에 대한 자세한 내용은 관리 플랫폼, 즉 management center 또는 device manager에 대한 구성 지침서를 참조하십시오.

라이선싱

- Cisco Smart License 계정을 사용하는 BYOL(Bring Your Own License)
- PAYG(Pay As You Go) 라이선싱 - Cisco Smart Licensing을 구매하지 않고도 고객이 threat defense virtual을 실행할 수 있는 사용 기반 청구 모델입니다. 모든 라이선스 기능(악성 코드 / 위협 / URL 필터링 / VPN 등)은 등록된 PAYG threat defense virtual 디바이스에 대해 활성화됩니다. 라이선스가 있는 기능은 management center에서 수정하거나 변경할 수 없습니다. (버전 6.5 이상)

Note PAYG 라이선싱은 device manager 모드로 구축된 threat defense virtual 디바이스에서 지원되지 않습니다.

threat defense virtual 디바이스 라이선싱에 대한 지침은 보안 방화벽 관리 센터 관리 가이드의 "라이선싱" 장을 참조하십시오.

Threat Defense Virtual 스마트 라이선싱의 성능 계층

threat defense virtual에서는 구축 요건에 따라 다양한 처리량 레벨 및 VPN 연결 제한을 제공하는 성능 계층 라이선싱을 지원합니다.

Table 1: 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 / 34GB	16Gbps	10,000

성능 최적화

threat defense virtual에서 최상의 성능을 얻으려면 VM과 호스트를 모두 조정할 수 있습니다. 자세한 내용은 Azure에서의 가상화 조정 및 최적화를 참조하십시오.

Receive Side Scaling — threat defense virtual는 RSS(Receive Side Scaling)를 지원합니다. RSS는 네트워크 수신 트래픽을 여러 프로세서 코어로 분산하기 위해 네트워크 어댑터에서 활용하는 기술입니다. 버전 7.0 이상에서 지원됩니다. 자세한 내용은 RSS(Receive Side Scaling)를 위한 다중 RX 대기열을 참조하십시오.

지원되지 않는 기능

- 라이선싱:
  - PLR(영구 라이선스 예약)
  - PAYG(Pay As You Go)(버전 6.4 이하)
- 네트워킹(이러한 제한의 많은 수는 Microsoft Azure 제한임):

- 점보 프레임
- 802.1Q VLAN
- 투명 모드 및 기타 레이어 2 기능, 브로드 캐스트도 없고 멀티 캐스트도 없습니다.
- Azure의 관점에서는 디바이스 소유가 아닌 IP 주소에 대한 프록시 ARP(일부 NAT 기능에 영향을 미침)
- 프로미스큐어스 모드(서브넷 트래픽 캡처 없음)
- 인라인 설정 모드, 패시브 모드

Note Azure 정책에서는 threat defense virtual가 투명 방화벽 모드에서 작동할 수 없습니다. 이 모드에서는 인터페이스가 프로미스큐어스 모드에서 작동할 수 없기 때문입니다.

- ERSPAN(Azure에서 전달되지 않는 GRE 사용)

- 관리:
  - 콘솔 액세스; 관리는 management center를 사용하여 네트워크를 통해 수행됩니다(일부 설정 및 유지 보수 활동에 SSH 사용 가능).
  - Azure Portal "비밀번호 재설정" 기능
  - 콘솔 기반 비밀번호 복구: 사용자는 콘솔에 실시간으로 액세스할 수 없으므로 비밀번호를 복구할 수 없습니다. 비밀번호 복구 이미지는 부팅할 수 없습니다. 유일한 방법은 새 threat defense virtual VM을 구축하는 것입니다.
- 고가용성(활성-대기)
- 클러스터링
- VM 가져오기/내보내기
- Device Manager 사용자 인터페이스(버전 6.4 이하)

Azure DDoS 보호 기능

Microsoft Azure의 Azure DDoS Protection은 threat defense virtual의 최전선에서 구현되는 추가 기능입니다. 가상 네트워크에서 이 기능을 활성화하면 네트워크 예상 트래픽의 초당 패킷 수에 따라 일반적인 네트워크 레이어 공격으로부터 애플리케이션을 방어할 수 있습니다. 네트워크 트래픽 패턴에 따라 이 기능을 맞춤화할 수 있습니다.

Azure DDoS Protection 기능에 대한 자세한 내용은 Azure DDoS Protection 표준 개요를 참고하십시오.

Snort

- Snort를 종료하는 데 시간이 오래 걸리거나, VM이 일반적으로 느려지거나, 특정 프로세스가 실행되는 등의 비정상적인 동작이 관찰되는 경우 threat defense virtual 및 VM 호스트에서 로그를 수집합니다. 전체 CPU 사용량, 메모리, I/O 사용량 및 읽기/쓰기 속도 로그를 수집하면 문제를 해결하는 데 도움이 됩니다.
- Snort가 종료될 때 높은 CPU 및 I/O 사용량이 관찰됩니다. 메모리가 충분하지 않고 전용 CPU가 없는 단일 호스트에서 여러 threat defense virtual 인스턴스가 생성된 경우 Snort가 종료되는 데 시간이 오래 걸리므로 Snort 코어가 생성됩니다.

Secure Firewall Threat Defense Virtual 디바이스 관리 방법

두 가지 옵션을 통해 Secure Firewall Threat Defense Virtual 디바이스를 관리할 수 있습니다.

보안 방화벽 관리 센터

다수의 디바이스를 관리하거나 threat defense에서 허용하는 더 복잡한 기능 및 구성을 사용하려는 경우에는 통합형 device manager 대신 management center를 사용하여 디바이스를 구성하십시오.

중요 device manager와 management center를 모두 사용하여 threat defense 디바이스를 관리할 수는 없습니다. device manager 통합 관리가 활성화되면 로컬 관리를 사용하지 않도록 설정하고 management center를 사용하도록 재구성하기 전에는 management center를 사용해 threat defense 디바이스를 관리할 수 없습니다. 반면 management center에 threat defense 디바이스를 등록하면 device manager 온보드 관리 서비스가 비활성화됩니다.

주의 현재 Cisco에서는 device manager 구성을 management center로, 또는 그 반대로 마이그레이션 할 수 있는 옵션이 없습니다. threat defense 디바이스를 구성할 때는 이를 고려해 관리 유형을 선택해야 합니다.

Secure Firewall device manager

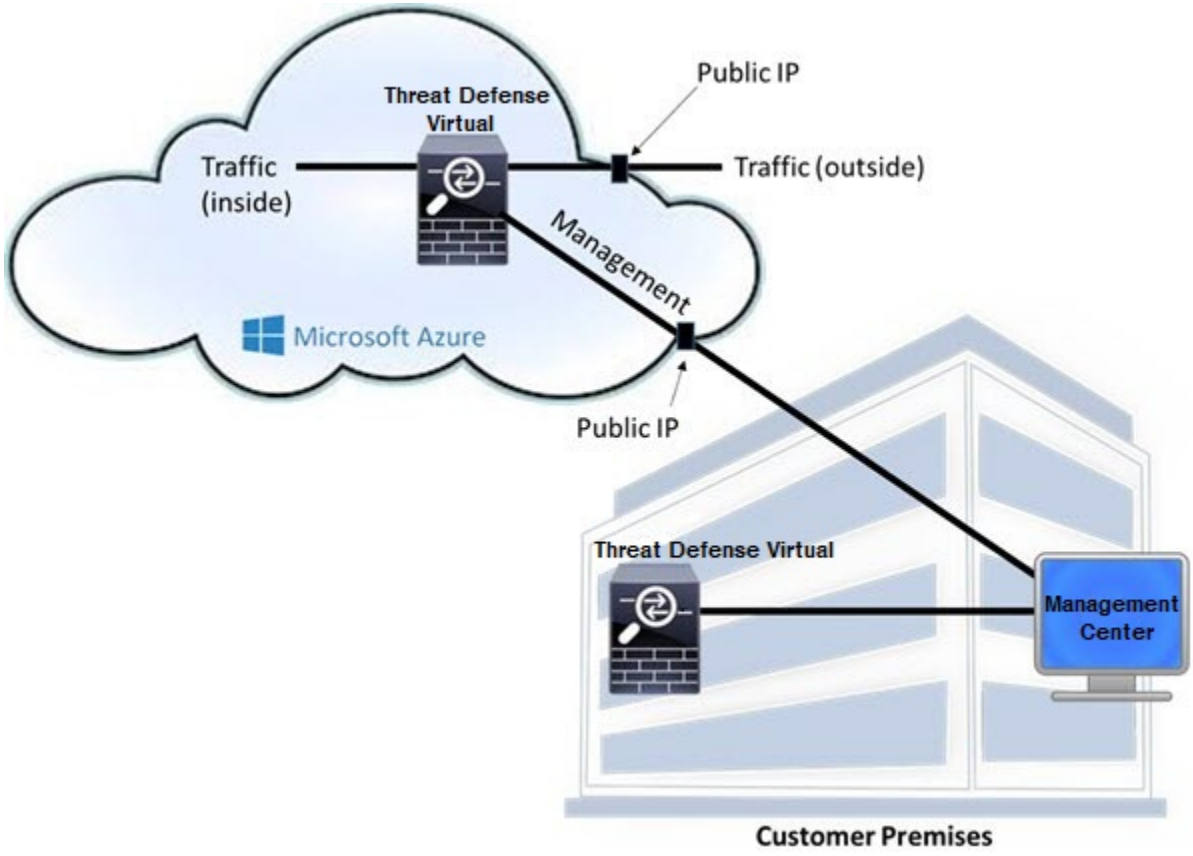
device manager은 온보드 통합 관리자입니다.

device manager는 일부 threat defense 디바이스에 포함된 웹 기반 구성 인터페이스입니다. device manager 사용을 통해 소규모 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.

참고 device manager을 지원하는 threat defense 디바이스 목록은 Cisco Secure Firewall Device Manager 구성 가이드을 참조하십시오.

Azure에서 Threat Defense Virtual를 위한 네트워크 토폴로지 샘플

다음 그림에는 Azure 내 라우팅 방화벽 모드의 threat defense virtual에 대한 일반적인 토폴로지가 나와 있습니다. 첫 번째로 정의된 인터페이스는 항상 관리 인터페이스이며 Management 0/0 및 GigabitEthernet0 / 0에만 공용 IP 주소가 할당됩니다.



구축 중에 생성된 리소스

Azure에서 Secure Firewall Threat Defense Virtual를 구축할 때 다음 리소스가 생성됩니다.

- threat defense virtual 머신(VM)

- 리소스 그룹
  - threat defense virtual는 항상 새 리소스 그룹에 구축됩니다. 그러나 다른 리소스 그룹의 기존 가상 네트워크에 연결할 수 있습니다.

- 4개의 NIC - *vm name*-Nic0, *vm name*-Nic1, *vm name*-Nic2, *vm name*-Nic3

Note 요구 사항에 따라 IPv4 전용 또는 듀얼 스택 (IPv4 및 IPv6 활성화)을 사용하여 VNet을 생성할 수 있습니다.

이러한 NIC는 threat defense virtual interfaces Management, 진단 0/0, GigabitEthernet 0/0 및 GigabitEthernet 0/1에 각각 매핑됩니다.

- *vm name* -mgmt-SecurityGroup으로 명명된 보안 그룹

  보안 그룹이 VM의 Nic0에 매핑되며 이는 threat defense virtual 관리 인터페이스에 매핑됩니다.

  보안 그룹에는 SSH (TCP 포트 22) 및 management center인터페이스 (TCP 포트 8305)의 관리 트래픽을 허용하는 규칙이 포함되어 있습니다. 구축 후에 이 값을 수정할 수 있습니다.

- 공용 IP 주소(구축 중에 선택한 값에 따라 이름이 지정됩니다)

  공용 IP 주소를 다른 인터페이스에 할당할 수 있습니다. 공용 IP 주소를 생성, 변경 또는 삭제하는 방법을 비롯하여 퍼블릭 IP와 관련된 Azure 지침은 Public IP addresses를 참조하십시오.

- New Network(새 네트워크) 옵션을 선택하면 서브넷이 4개인 가상 네트워크가 생성됩니다.
- 각 서브넷에 대한 라우팅 테이블(이미 있을 경우 업데이트됨)

  이 테이블의 이름은 "*subnet name* "-FTDv-RouteTable입니다.

  각 라우팅 테이블에는 다른 3개 서브넷에 대한 경로가 포함되며 threat defense virtual IP 주소가 다음 홉입니다. 트래픽이 다른 서브넷 또는 인터넷에 도달해야 하는 경우 기본 경로 추가를 선택할 수 있습니다.

- 선택된 스토리지 계정의 부팅 진단 파일

  부팅 진단 파일은 Blob(binary large object)에 포함됩니다.

- Blob과 컨테이너 VHD인 *vm name*-disk.vhd 및 *vm name*-<uuid>.status에 속한 선택된 스토리지 계정의 파일 2개
- 스토리지 계정(기존 스토리지 계정을 선택하지 않은 경우)

Note VM을 삭제할 경우 이 리소스에서 유지할 것을 제외하고 각각을 개별적으로 삭제해야 합니다.

Accelerated Networking(AN)

Azure의 AN(Accelerated Networking) 기능은 VM에 대한 SR-IOV(Single Root I / O Virtualization)를 활성화합니다. 그러면 VM NIC가 하이퍼바이저를 우회하여 PCIe 카드로 바로 이동할 수 있습니다. AN은 VM의 처리량 성능을 크게 향상시키며 추가 코어(예: 더 큰 VM)로 확장됩니다.

기본적으로 비활성화되어 있습니다. Azure는 사전 프로비저닝된 가상 머신에서 AN 활성화를 지원합니다. Azure에서 VM을 중지하고 네트워크 카드 속성을 업데이트하여 *enableAcceleratedNetworking* 매개 변수를 true로 설정하기만 하면 됩니다. Microsoft 문서 Enable accelerated networking on existing VMs를 참조하십시오. 그런 다음 VM을 다시 시작합니다.

Azure 라우팅

Azure 가상 네트워크 서브넷의 라우팅은 해당 서브넷의 유효 라우팅 테이블에 따라 결정됩니다. 유효 라우팅 테이블은 기존 시스템 라우팅 테이블과 사용자 정의 라우팅 테이블의 조합입니다.

Note VM NIC 속성 아래에서 유효 라우팅 테이블을 볼 수 있습니다.

사용자 정의 라우팅 테이블은 보고 수정할 수 있습니다. 시스템 테이블과 사용자 정의 테이블의 조합으로 유효 라우팅 테이블이 구성될 경우 가장 구체적인 경로가 선택되며 동등할 때는 사용자 정의 라우팅 테이블이 적용됩니다. 시스템 라우팅 테이블은 Azure의 가상 네트워크 인터넷 게이트웨이를 가리키는 기본 경로(0.0.0.0/0) IPv4 또는 [::/0] IPv6를 포함합니다. 시스템 라우팅 테이블은 나머지 정의된 서브넷에 대한 경로도 포함하는데, 다음 홉은 Azure의 가상 네트워크 인프라 게이트웨이를 가리킵니다.

Azure 라우팅 threat defense virtual을 통해 트래픽을 라우팅하려면 각 데이터 서브넷과 연결된 사용자 정의 라우팅 테이블에서 경로를 추가/업데이트해야 합니다. 관심 트래픽은 해당 서브넷의 threat defense virtual IP 주소를 다음 홉으로 사용하여 라우팅해야 합니다. 또한 필요한 경우 threat defense virtual IP의 다음 홉과 함께 0.0.0.0/0 IPv4 또는 [::/0] IPv6의 기본 경로를 추가할 수 있습니다.

시스템 라우팅 테이블의 기존 경로 때문에 threat defense virtual를 다음 홉으로 가리키는 경로를 사용자 정의 라우팅 테이블에 추가해야 합니다. 그렇지 않으면 사용자 정의 테이블의 기본 경로가 시스템 라우팅 테이블의 더 구체적인 경로에 밀려 트래픽이 threat defense virtual를 우회하게 됩니다.

가상 네트워크의 VM을 위한 라우팅 컨피그레이션

Azure 가상 네트워크의 라우팅은 클라이언트의 특정 게이트웨이 설정이 아니라 유효 라우팅 테이블에 따라 달라집니다. 가상 네트워크에서 실행 중인 클라이언트는 DHCP에서 경로를 지정할 수도 있습니다. 이는 해당 서브넷의 1번 주소입니다. 이는 자리 표시자이며 가상 네트워크의 인프라 가상 게이트웨이에 패킷을 보내는 기능만 할 뿐입니다. 패킷이 VM을 떠나면 유효 라우팅 테이블에 따라 (사용자 정의 테이블에서 수정한 대로) 라우팅됩니다. 클라이언트가 .1 또는 threat defense virtual 주소로 구성된 경우에도 유효 라우팅 테이블에 따라 다음 홉이 결정됩니다.

Azure VM ARP 테이블에서는 모든 확인된 호스트에 대해 동일한 MAC 주소(1234.5678.9abc)를 표시합니다. 그러면 Azure VM을 떠나는 모든 패킷이 Azure 게이트웨이에 도달하며, 여기서 유효 라우팅 테이블을 사용하여 패킷의 경로를 결정합니다.

IP 주소

다음 정보가 Azure의 IP 네트워크에 적용됩니다.

- threat defense virtual의 첫 NIC(Management에 매핑됨)는 연결된 서브넷에서 전용 IP 주소를 받습니다.

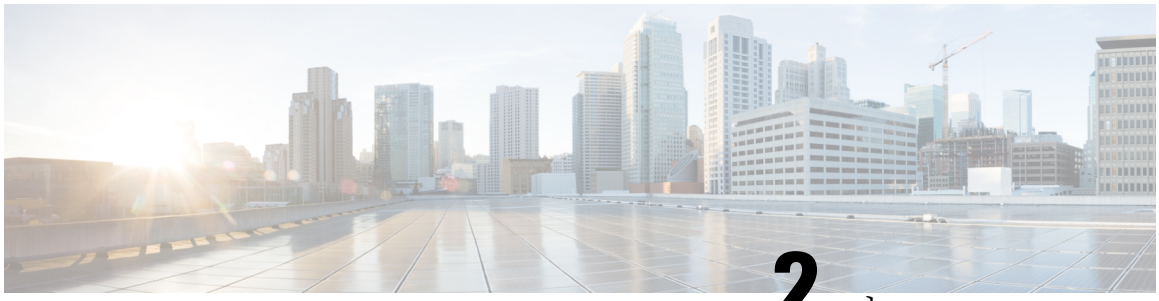
  공용 IP 주소를 이 전용 IP 주소와 연결할 수 있으며 Azure Internet 게이트웨이에서 NAT 변환을 처리합니다.

  threat defense virtual이 구축된 후 공용 IP 주소를 데이터 인터페이스(예: GigabitEthernet0/0)와 연결할 수 있습니다. 공용 IP 주소를 생성, 변경 또는 삭제하는 방법을 비롯하여 공용 IP와 관련된 Azure 지침은 Public IP addresses를 참조하십시오.

- 공용 IP 주소(IPv4 및 IPv6)는 동적이며 Azure 중지/시작 사이클 중 변경될 수 있습니다. 그러나 Azure가 재시작하고 threat defense virtual가 다시 로드될 때는 유지됩니다. IPv6 공용 IP 주소 표준을 참조하십시오.

- 고정 상태의 공용 IP 주소는 Azure에서 변경하지 않는 한 바뀌지 않습니다.

- Threat Defense Virtual 인터페이스에서 IP 주소 설정에 DHCP를 사용할 수 있습니다. Azure 인프라는 Azure에서 설정된 IP 주소가 threat defense virtual 인터페이스에 지정되게 합니다.



2 장

Azure에서 Threat Defense Virtual 구축

이 장에서는 Azure 포털에서 Secure Firewall Threat Defense Virtual를 구축하는 방법을 설명합니다.

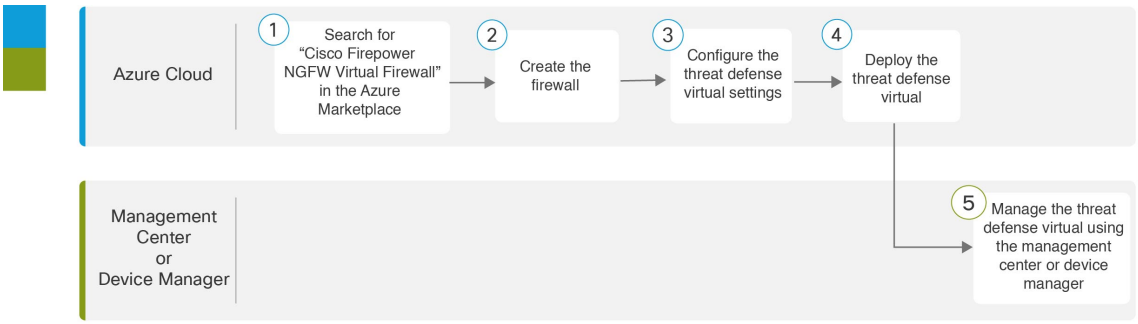
Azure 구축

템플릿을 사용하여 Azure에서 threat defense virtual를 구축할 수 있습니다. Cisco는 다음과 같은 두 가지 템플릿을 제공합니다.

- **Azure Marketplace**의 솔루션 템플릿 - Azure Marketplace에서 사용 가능한 솔루션 템플릿을 사용하여 Azure Portal을 사용하여 threat defense virtual를 구축합니다. 기존 리소스 그룹 및 스토리지 어카운트를 사용하거나 새로 생성하여 가상 어플라이언스를 구축할 수 있습니다. 솔루션 템플릿을 사용하려면 솔루션 템플릿을 사용한 Azure Marketplace에서의 구축, on page 13를 참조하십시오.
- **VHD**에서 관리되는 이미지를 사용하는 맞춤형 템플릿(https://software.cisco.com/download/home에서 사용 가능)-Cisco는 Marketplace 기반 구축 외에 Azure에 threat defense virtual를 구축하는 프로세스를 간소화하기 위해 Azure에 업로드할 수 있는 압축된 VHD(Virtual Hard Disk)를 제공합니다. 관리 이미지와 두 개의 JSON 파일(템플릿 파일 및 매개 변수 파일)을 사용하면 threat defense virtual를 위해 단일 리소스로 모든 리소스를 구축하고 프로비저닝 할 수 있습니다. 맞춤형 템플릿을 사용하려면 VHD 및 리소스 템플릿을 사용해서 Azure에서 구축, on page 16를 참조하십시오.

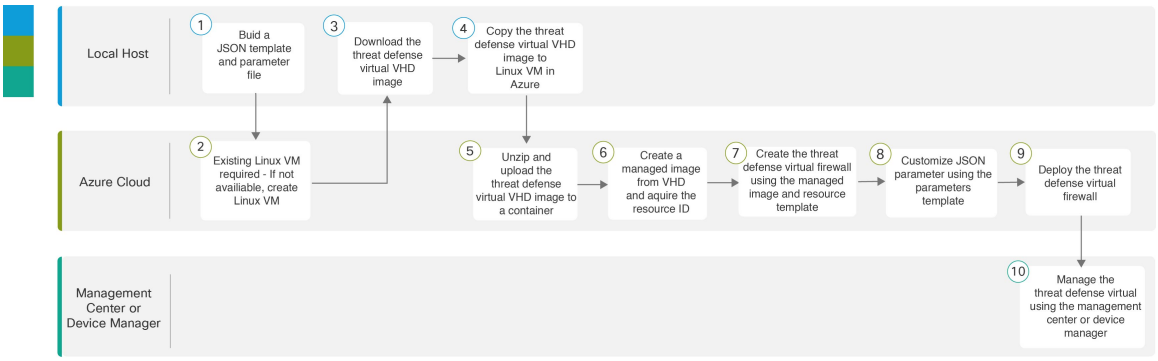
엔드 투 엔드 절차

다음 순서도에서는 솔루션 템플릿을 사용하여 Microsoft Azure에서 threat defense virtual를 구축하는 워크플로를 보여줍니다.



	업무 환경	단계
1	Azure Cloud	솔루션 템플릿을 사용한 Azure Marketplace에서의 구축: Azure Marketplace에서 "Cisco Firepower NGFW Virtual Firewall"을 검색합니다.
2	Azure Cloud	솔루션 템플릿을 사용한 Azure Marketplace에서의 구축: 방화벽을 생성합니다.
3	Azure Cloud	솔루션 템플릿을 사용한 Azure Marketplace에서의 구축: threat defense virtual 설정을 구성합니다.
4	Azure Cloud	솔루션 템플릿을 사용한 Azure Marketplace에서의 구축: threat defense virtual를 구축합니다.
5	Management Center 또는 Device Manager	threat defense virtual 관리: • 보안 방화벽 관리 센터로 Secure Firewall Threat Defense Virtual 관리 • Secure Firewall device manager로 Secure Firewall Threat Defense Virtual 관리

다음 순서도에서는 VHD 및 리소스 템플릿을 사용하여 Microsoft Azure에서 threat defense virtual를 구축하는 워크플로를 보여줍니다.



	업무 환경	단계
1	로컬 호스트	VHD 및 리소스 템플릿을 사용해서 Azure에서 구축: JSON 템플릿 및 파라미터 파일을 빌드합니다.
2	Azure Cloud	VHD 및 리소스 템플릿을 사용해서 Azure에서 구축: 기존 Linux VM 필요 - 사용할 수 없는 경우 Linux VM을 생성합니다. • Azure CLI를 사용하여 Linux 가상 시스템 생성 • Azure Portal을 사용하여 Linux 가상 시스템 생성
3	로컬 호스트	VHD 및 리소스 템플릿을 사용해서 Azure에서 구축: Cisco Download Software(Cisco 소프트웨어 다운로드) 페이지에서 threat defense virtual VHD 이미지를 다운로드합니다.
4	로컬 호스트	VHD 및 리소스 템플릿을 사용해서 Azure에서 구축: threat defense virtual VHD 이미지를 Azure의 Linux VM에 복사합니다.
5	Azure Cloud	VHD 및 리소스 템플릿을 사용해서 Azure에서 구축: threat defense virtual VHD 이미지의 압축을 풀고 컨테이너에 업로드합니다.
6	Azure Cloud	VHD 및 리소스 템플릿을 사용해서 Azure에서 구축: VHD에서 매니지드 이미지를 생성하고 해당 이미지의 리소스 ID를 가져옵니다.
7	Azure Cloud	VHD 및 리소스 템플릿을 사용하여 Azure에서 구축: 관리되는 이미지 및 리소스 템플릿을 사용하여 방화벽을 생성합니다.VHD 및 리소스 템플릿을 사용해서 Azure에서 구축, 16 페이지threat defense virtual
8	Azure Cloud	VHD 및 리소스 템플릿을 사용해서 Azure에서 구축: 파라미터 템플릿을 사용하여 JSON 파라미터를 사용자 지정합니다.
9	Azure Cloud	VHD 및 리소스 템플릿을 사용해서 Azure에서 구축: threat defense virtual 방화벽을 구축합니다.
10	Management Center 또는 Device Manager	threat defense virtual 관리: • 보안 방화벽 관리 센터로 Secure Firewall Threat Defense Virtual 관리 • Secure Firewall device manager로 Secure Firewall Threat Defense Virtual 관리

솔루션 템플릿을 사용한 Azure Marketplace에서의 구축

다음 지침에서는 Azure Marketplace에서 제공되는 threat defense virtual에 대한 솔루션 템플릿을 구축하는 방법을 보여줍니다. 이 목록은 Microsoft Azure 환경에서 threat defense virtual를 설정하는 단계의

최상위 목록입니다. Azure 설정 단계에 대한 자세한 내용은 Getting Started with Azure를 참조하십시오.

Azure에서 threat defense virtual를 구축할 경우 리소스, 공용 IP 주소(IPv4 및 IPv6), 경로 테이블과 같은 다양한 컨피그레이션이 자동으로 생성됩니다. 구축 후에 이 컨피그레이션을 추가로 관리할 수 있습니다. 이를테면 유휴 시간 초과 값을 낮게 설정된 기본값에서 변경할 수 있습니다.

Note GitHub 리포지토리에서 사용 가능한 맞춤형 ARM 템플릿을 사용하려면 VHD 및 리소스 템플릿을 사용해서 Azure에서 구축, on page 16를 참조하십시오.

Procedure

단계 **1** ARM(Azure Resource Manager) 포털에 로그인합니다.

Azure 포털에서는 데이터 센터 위치와 상관없이 현재 계정 및 서브스크립션의 가상 요소를 보여줍니다.

단계 **2** **Azure Marketplace(Azure** 마켓플레이스**)> Virtual Machines(**가상 시스템**)**를 선택합니다.

단계 **3** Marketplace에서 "Cisco Firepower NGFW Virtual (Threat Defense Virtual)"을 검색하고 제품을 선택한 다음 **Create(**생성**)**를 클릭합니다.

단계 **4** 기본 설정을 구성합니다.

a) 가상 시스템의 이름을 입력합니다. 이 이름은 Azure 서브스크립션 내에서 고유해야 합니다.

Important 기존 이름을 사용하면 구축이 실패하므로 주의합니다.

b) 라이선싱 방법을 **BYOL** 또는 **PAYG** 중에서 선택합니다.

Cisco Smart License 계정을 사용하려면 **BYO**L(Bring Your Own License)을 선택합니다.

Cisco Smart Licensing을 구매하지 않고도 사용량 기준 청구 모델을 사용하려면 **PAYG**(Pay As You Go) 라이선싱을 선택합니다.

Important management center를 사용하여 threat defense virtual를 관리하는 경우에만 **PAYG**를 사용할 수 있습니다.

c) threat defense virtual 관리자에 대해서 사용자 이름을 입력합니다.

Note 이름 "admin"은 Azure에 예비되어 있으므로 사용할 수 없습니다.

d) 권한 부여 유형을 비밀번호 또는 SSH 공용 키 중 하나로 선택합니다.

비밀번호를 선택할 경우 비밀번호를 입력하고 커밋합니다.

SSH 키를 선택하면 원격 피어의 RSA 공용 키를 지정합니다.

e) 로그인하여 threat defense virtual를 구성할 때 관리자 사용자 계정에 사용할 비밀번호를 생성합니다.

f) 구독 유형을 선택합니다.

g) 새로운 리소스 그룹을 생성합니다.

threat defense virtual를 새 리소스 그룹에 구축해야 합니다. 기존 리소스 그룹에 구축하는 옵션은 기존 리소스 그룹이 비어 있는 경우에만 작동합니다.

그러나 나중 단계에서 네트워크 옵션을 구성할 때 다른 리소스 그룹의 기존 가상 네트워크에 threat defense virtual를 연결할 수 있습니다.

h) 지리적 위치을 선택합니다. 이는 이 구축에 사용된 모든 리소스(예: Threat Defense Virtual, 네트워크, 스토리지 계정)에 대해 동일해야 합니다.

i) **OK(**확인**)**를 클릭합니다.

단계 **5** threat defense virtual 설정을 구성합니다.

a) 가상 시스템 크기를 선택합니다.

b) 스토리지 계정을 선택합니다.

Note 기존 스토리지 계정을 사용하거나 새로 만들 수 있습니다. 스토리지 계정 이름은 소문자와 숫자만 포함할 수 있습니다.

c) 공용 IP 주소를 선택합니다.

선택한 구독 및 위치에 사용 가능한 공용 IP 주소를 선택하거나 **Create new(**새로 만들기**)**를 클릭할 수 있습니다.

새 공용 IP 주소를 만들면 Microsoft가 소유한 IP 주소 블록에서 하나를 가져오므로 특정 주소를 선택할 수 없습니다. 인터페이스에 할당할 수 있는 최대 공용 IP 주소 수는 Azure 구독을 기반으로 합니다.

Important Azure는 기본적으로 동적 공용 IP 주소를 생성합니다. VM을 중지했다가 다시 시작하면 공용 IP가 변경될 수 있습니다. 고정 IP 주소를 선호하는 경우 고정 주소를 생성해야 합니다. 구축 후 공용 IP 주소를 수정하고 동적 주소에서 고정 주소로 변경할 수도 있습니다.

VM에서 공용 IPv6 주소를 할당해야 하는 경우 IPv6 표준 IPv6 공용 IP 주소 표준을 참조하십시오.

d) DNS 레이블을 추가합니다.

Note FQDN(fully qualified domain name)은 DNS 레이블 + Azure URL이 됩니다. 즉 <dnslabel>.<location>.cloupapp.azure.com입니다.

e) 가상 네트워크를 선택합니다.

기존 VNet(Azure Virtual Network)을 선택하거나 새로 생성하고 VNet의 IP 주소 공간을 입력할 수 있습니다. 기본적으로 CIDR(Classless Inter-Domain Routing) IP 주소는 10.0.0.0/16입니다.

IPv6 주소 지정에 가상 머신이 필요한 경우 가상 네트워크에서 활성화해야 합니다. 예: 기본적으로 CIDR IPv6 주소는 [ace:cab:deca::/48]입니다.

Note 가상 네트워크, 서브넷, 인터페이스 등은 IPv6만 사용해 생성할 수 없습니다. IPv4가 기본적으로 사용되며, IPv6와 함께 활성화할 수 있습니다. IPv6에 대한 자세한 내용은 Azure IPv6 개요를 참조하십시오.

f) threat defense virtual 네트워크 인터페이스에 4개의 서브넷을 구성합니다.

- Azure의 Nic0에 연결된 **FTDv Management** 인터페이스, “첫 번째 서브넷”
- **FTDv Diagnostic** 인터페이스, Azure의 Nic1에 연결됨, "두 번째 서브넷"
- **FTDv Outside** 인터페이스, Azure의 Nic2에 연결, “세 번째 서브넷”
- **FTDv Inside** 인터페이스, Azure의 Nic3에 연결, "네 번째 서브넷"

Note 위의 서브넷에 대해 서브넷을 생성하는 동안 IPv6 구성이 필요한 경우 IPv6 옵션을 선택하고 인터페이스에 대한 IPv6 서브넷을 구성합니다.

g) **OK(**확인**)**를 클릭합니다.

단계 **6** 컨피그레이션 요약을 본 다음 **OK(**확인**)**를 클릭합니다.

단계 **7** 이용 약관을 보고 **Purchase(**구매**)**를 클릭합니다.

Azure에서는 구축 시간이 다양합니다. Azure가 threat defense virtual VM이 실행 중임을 보고할 때까지 기다립니다.

What to do next

다음 단계는 선택한 관리 모드에 따라 달라집니다.

- **Enable Local Manager(**로컬 매니저 활성화**)**에 대해 **No(**아니요**)**를 선택한 경우 보안 방화벽 관리 센터을 사용해 threat defense virtual를 관리할 수 있습니다. 보안 방화벽 관리 센터로 Secure Firewall Threat Defense Virtual 관리를 참조하십시오.
- **Enable Local Manager(**로컬 매니저 활성화**)**에 대해 **Yes(**예**)**를 선택한 경우 통합 Secure Firewall Device Manager을 사용해 threat defense virtual를 관리할 수 있습니다. 보안 방화벽 관리 센터로 Secure Firewall Threat Defense Virtual 관리를 참조하십시오.

관리 옵션을 선택하는 방법에 대한 개요는 Secure Firewall Threat Defense Virtual 디바이스 관리 방법, on page 6을 참조하십시오.

VHD 및 리소스 템플릿을 사용해서 Azure에서 구축

이제 Cisco에서 사용 가능한 압축된 VHD 이미지를 사용하여 Azure에서 고유한 맞춤형 threat defense virtual 이미지를 생성할 수 있습니다. VHD 이미지를 사용하여 구축하려면 Azure 스토리지 계정에 VHD 이미지를 업로드합니다. 그런 다음, 업로드된 디스크 이미지 및 Azure Resource Manager 템플릿을 사용하여 매니지드 이미지를 생성할 수 있습니다. Azure 템플릿은 리소스 설명 및 파라미터 정의를 포함하는 JSON 파일입니다.

시작하기 전에

- threat defense virtual 템플릿 구축을 위한 JSON 템플릿 및 해당 JSON 매개변수 파일이 필요합니다. 템플릿 및 매개변수 파일을 구축하는 방법에 대한 지침을 제공하는 Github에서 VHD 및 업데이트된 ARM 템플릿을 사용하는 Azure threat defense virtual 구축용 샘플을 참조하십시오.
- 이 절차를 수행하려면 Azure의 기존 Linux VM이 필요합니다. 압축된 VHD 이미지를 Azure에 업로드하려면 임시 Linux VM(예: Ubuntu 16.04)을 사용하는 것이 좋습니다. 이 이미지는 압축을 풀 때 약 50GB의 스토리지가 필요합니다. 또한 Azure의 Linux VM에서 Azure 스토리지로의 업로드 시간이 더 빨라집니다.

  VM을 생성해야 하는 경우 다음 방법 중 하나를 사용합니다.

  - Azure CLI를 사용하여 Linux 가상 시스템 생성
  - Azure Portal을 사용하여 Linux 가상 시스템 생성

- Azure 구독에서 threat defense virtual를 구축하려는 위치에서 사용 가능한 스토리지 계정이 있어야 합니다.

프로시저

단계 **1** Cisco Download Software(소프트웨어 다운로드) 페이지에서 threat defense virtual 압축된 VHD 이미지를 다운로드합니다.

a) **Products(**제품**)** > **Security(**보안**)** > **Firewalls(**방화벽**)** > **Next-Generation Firewalls(NGFW)(**차세대 방화벽**)** > **Firepower NGFW Virtual**로 이동합니다.

b) **Firepower Threat Defense Software**를 클릭합니다.

지침에 따라 다운로드합니다.

예: Cisco_Firepower_Threat_Defense_Virtual-7.1.0-92.vhd.bz2

단계 **2** 압축된 VHD 이미지를 Azure의 Linux VM에 복사합니다.

파일을 Azure로 또는 Azure에서 아래로 이동하는 데 사용할 수 있는 여러 옵션이 있습니다. 이 예에서는 SCP 또는 보안 복사본을 보여줍니다.

```
# scp /username@remotehost.com/dir/Cisco_Firepower_Threat_Defense_Virtual-7.1.0-92.vhd.bz2
 <linux-ip>
```

단계 **3** Azure에서 Linux VM에 로그인하고 압축된 VHD 이미지를 복사한 디렉터리로 이동합니다.

단계 **4** threat defense virtual VHD 이미지의 압축을 풉니다.

파일의 압축을 풀거나 압축을 풀 때 사용할 수 있는 여러 옵션이 있습니다. 이 예에서는 Bzip2 유틸리티를 보여 주지만, 작동하는 Windows 기반 유틸리티도 있습니다.

```
# bunzip2 Cisco_Firepower_Threat_Defense_Virtual-7.1.0-92.vhd.bz2
```

단계 **5** Azure 스토리지 계정의 컨테이너에 VHD를 업로드합니다. 기존 스토리지 계정을 사용하거나 새로 만들 수 있습니다. 스토리지 계정 이름은 소문자와 숫자만 포함할 수 있습니다.

스토리지 계정에 VHD를 업로드하는 데 사용할 수 있는 여러 옵션(AzCopy, Azure Storage Copy Blob API, Azure Storage Explorer, Azure CLI 또는 Azure Portal)이 있습니다. threat defense virtual VHD만큼 큰 파일에는 Azure Portal을 사용하지 않는 것이 좋습니다.

다음 예에서는 Azure CLI를 사용하는 구문을 보여줍니다.

```
azure storage blob upload \
       --file <unzipped vhd> \
       --account-name <azure storage account> \
       --account-key yX7txxxxxxxx1dnQ== \
       --container <container> \
       --blob <desired vhd name in azure> \
       --blobtype page
```

단계 **6** VHD에서 관리되는 이미지 생성:

a) Azure Portal에서 **Images(**이미지**)**를 선택합니다.
b) **Add(**추가**)**를 클릭하여 새 엔트리를 만듭니다.
c) 다음 정보를 제공합니다.

- **Name(**이름**)**-관리되는 이미지의 사용자 정의 이름을 입력합니다.
- **Subscription(**구독**)**-드롭 다운 목록에서 구독을 선택합니다.
- **Resource group(**리소스 그룹**)**-기존 리소스 그룹을 선택하거나 새 리소스 그룹을 생성합니다.
- **OS disk(OS** 디스크**)**-OS 유형으로 Linux를 선택합니다.
- **Storage blob(**스토리지 블롭**)**-스토리지 계정을 찾아 업로드된 VHD를 선택합니다.
- **Account type(**계정 유형**)**-드롭 다운 목록에서 표준(HDD)을 선택합니다.
- **Host caching(**호스트 캐싱**)**-드롭 다운 목록에서 Read/write(읽기/쓰기)를 선택합니다.
- **Data Disk(**데이터 디스크**)**-기본값을 그대로 둡니다. 데이터 디스크를 추가하지 마십시오.

d) **Create(**생성**)**를 클릭합니다.

Notifications(알림**)** 탭 아래에서 정상적으로 생성된 이미지 메시지를 기다립니다.

참고 관리되는 이미지가 생성되면 업로드된 VHD 및 업로드 스토리지 계정을 제거할 수 있습니다.

단계 **7** 새로 생성한 관리 이미지의 리소스 ID를 가져옵니다.

내부적으로 Azure는 모든 리소스를 리소스 ID와 연결합니다. 이 관리되는 이미지에서 새 threat defense virtual 방화벽을 구축할 때는 리소스 ID가 필요합니다.

a) Azure Portal에서 **Images(**이미지**)**를 선택합니다.
b) 이전 단계에서 생성한 관리 이미지를 선택합니다.
c) 이미지 속성을 보려면 **Overview(**개요**)**를 클릭합니다.
d) 리소스 **ID**를 클립 보드에 복사합니다.

리소스 **ID**의 형식은 다음과 같습니다.

/subscriptions/<subscription-id>/resourceGroups/<resourceGroup>/providers/Microsoft.Compute/<container>/<vhdname>

단계 **8** 관리되는 이미지 및 리소스 템플릿을 사용하여 threat defense virtual 방화벽을 구축합니다.

a) **New(**새로 만들기**)**를 선택하고 옵션에서 선택할 수 있을 때까지 **Template Deployment(**템플릿 구축**)**를 검색합니다.

b) **Create(**생성**)**을 선택합니다.

c) **Build your own template in the editor(**편집기에서 자체 템플릿 구축**)**를 선택합니다.

맞춤화할 수 있는 빈 템플릿이 있습니다. 템플릿 및 매개변수 파일을 구축하는 방법에 대한 지침을 제공하는 Github에서 VHD 및 ARM 템플릿을 사용하는 Azure threat defense virtual 구축용 샘플을 참조하십시오.

d) 맞춤화된 JSON 템플릿 코드를 창에 붙여넣은 다음 **Save(**저장**)**를 클릭합니다.

e) 드롭 다운 목록에서 **Subscription(**구독**)**을 선택합니다.

f) 기존 **Resource group(**리소스 그룹**)**을 선택하거나 새 리소스 그룹을 생성합니다.

g) 드롭다운 목록에서 **Location(**위치**)**를 선택합니다.

h) 이전 단계의 관리 이미지 리소스 **ID**를 **Vm** 관리 이미지 **ID** 필드에 붙여 넣습니다.

단계 **9** **Custom deployment(**맞춤형 구축**)** 페이지 상단에서 **Edit parameters(**매개 변수 수정**)**를 클릭합니다. 맞춤화할 수 있는 매개변수 템플릿이 있습니다.

a) **Load file(**파일 로드**)**을 클릭하고 사용자 맞춤화된 threat defense virtual 매개변수 파일을 찾습니다. 템플릿 및 매개변수 파일을 구축하는 방법에 대한 지침을 제공하는 Github에서 VHD 및 ARM 템플릿을 사용하는 Azure threat defense virtual 구축용 샘플을 참조하십시오.

b) 사용자 맞춤화된 JSON 매개변수 코드를 창에 붙여 넣은 다음 **Save(**저장**)**를 클릭합니다.

단계 **10** 맞춤형 구축 세부 정보를 검토합니다. **Basics(**기본**)** 및 **Settings(**설정**)**의 정보가 리소스 **ID**를 포함하여 예상되는 구축 컨피그레이션과 일치하는지 확인합니다.

단계 **11** 약관을 검토하고 위에 명시된 약관에 동의합니다 확인란을 선택합니다.

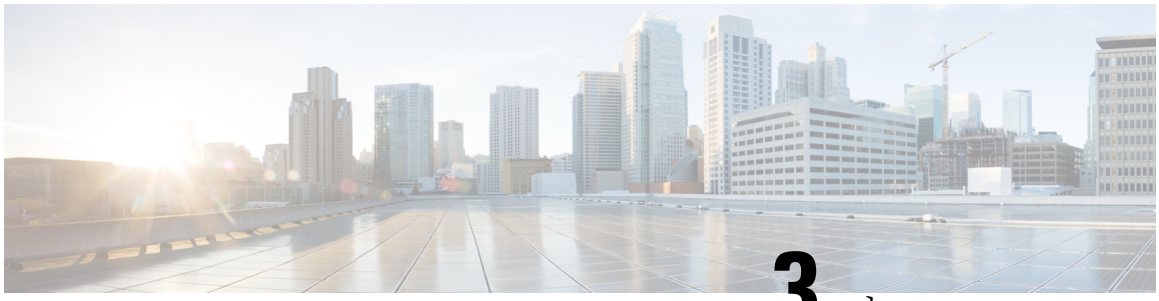
단계 **12** 관리 이미지 및 맞춤형 템플릿을 사용하여 방화벽을 구축하려면 Purchase (구매)를 클릭합니다.threat defense virtual

템플릿 및 매개변수 파일에 충돌이 없는 경우 구축이 성공적으로 이루어지게 됩니다.

Managed Image(관리 이미지)는 동일한 구독 및 지역 내의 여러 구축에 사용할 수 있습니다.

다음에 수행할 작업

- Azure에서 threat defense virtual의 IP 컨피그레이션을 업데이트합니다.



3 장

Secure Firewall Threat Defense Virtual Auto Scale for Azure 구축

Azure의 Threat Defense Virtual용 Auto Scale 솔루션

Auto Scale 솔루션

위협 대응 가상 Auto Scale for Azure는 Azure에서 제공하는 서버리스 인프라(논리 앱, Azure 기능, 로드 밸런서, 보안 그룹, 가상 시스템 확장 집합 등)를 사용하며 완벽환 서버리스 방식으로 구현됩니다.

Azure용 위협 대응 가상 Auto Scale 구현의 몇 가지 주요 기능은 다음과 같습니다.

- ARM(Azure Resource Manager) 템플릿 기반 구축
- CPU 및 메모리(RAM) 기반의 메트릭 확장 지원:

참고 자세한 내용은 Auto Scale 논리, 57 페이지를 참조하십시오.

- 위협 대응 가상 구축 및 다중 가용성 영역 지원
- 완전 자동화된 threat defense virtual 인스턴스 등록 및 management center 등록 취소.
- 확장된 threat defense virtual 인스턴스에 자동으로 적용되는 NAT 정책, 액세스 정책 및 경로.
- 로드 밸런서 및 다중 가용성 영역 지원
- Auto Scale 기능 활성화 및 비활성화 지원
- management center에서만 작동하며 device manager는 지원하지 않습니다.
- PAYG 또는 BYOL 라이선싱 모드로 threat defense virtual 구축 지원 PAYG는 threat defense virtual 소프트웨어 버전 6.5 이상에만 적용됩니다. 지원되는 소프트웨어 플랫폼, 22 페이지의 내용을 참조하십시오.

- Cisco에서는 구축을 쉽게 수행할 수 있도록 Azure용 Auto Scale 구축 패키지를 제공합니다.

지원되는 소프트웨어 플랫폼

threat defense virtual Auto Scale 솔루션은 management center에서 관리하는 threat defense virtual에 적용 가능하며 소프트웨어 버전과 무관합니다. Cisco FirePOWER 호환성 가이드는 운영 체제 및 호스팅 환경 요구 사항을 포함해서 소프트웨어 및 하드웨어 호환성에 대한 내용을 제공합니다.

- Management Center의 가상 테이블은 management center virtual에 필요한 호환성 및 가상 호스팅 환경 요구 사항을 표시합니다.
- Threat Defense Virtual 호환성 테이블은 Azure의 threat defense virtual에 필요한 호환성 및 가상 호스팅 환경 요구 사항을 표시합니다.

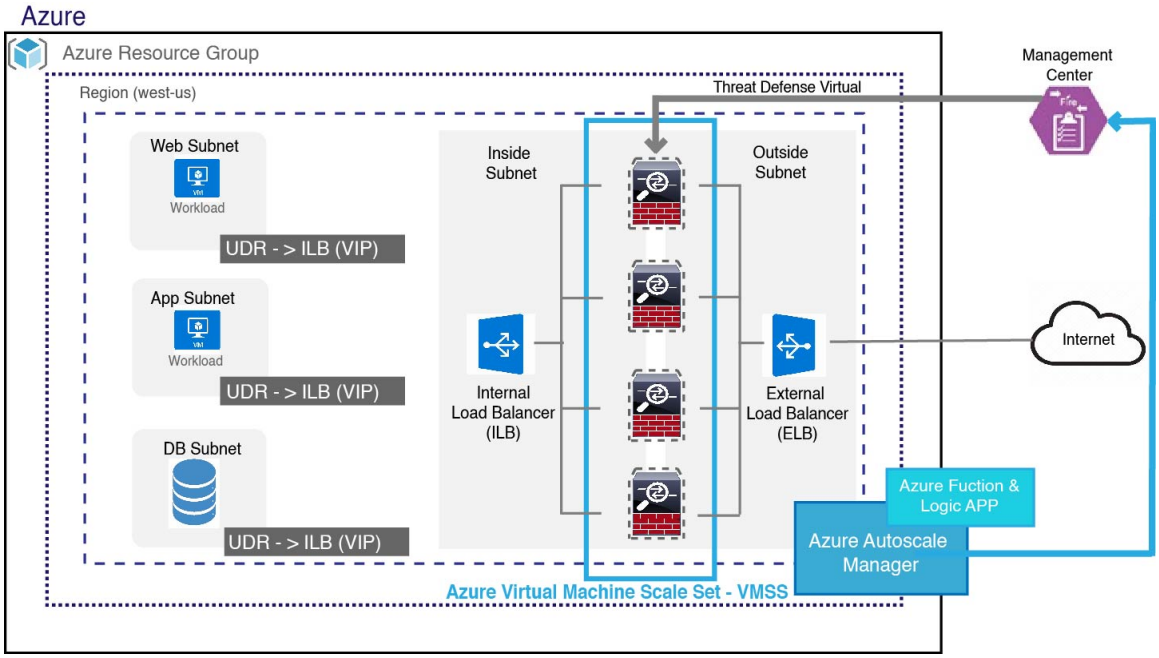
참고 Azure Auto Scale 솔루션 구축을 위해 Azure에서 threat defense virtual에 대해 지원되는 최소 버전은 버전 6.4입니다.

Auto Scale 사용 사례

Azure용 threat defense virtual Auto Scale은 Azure 내부 로드 밸런서(ILB)와 Azure 외부 로드 밸런서(ELB) 사이에 threat defense virtual 확장 집합을 배치하는 자동화된 수평 확장 솔루션입니다.

- ELB는 확장 집합에서 인터넷에서 threat defense virtual 인스턴스로 트래픽을 분산합니다. 그러면 방화벽이 애플리케이션에 트래픽을 전달합니다.
- ILB는 애플리케이션의 아웃 바운드 인터넷 트래픽을 확장 집합의 threat defense virtual 인스턴스로 분산합니다. 그러면 방화벽이 트래픽을 인터넷으로 전달합니다.
- 네트워크 패킷은 단일 연결에서 내부 및 외부 로드 밸런서를 모두 통과하지 않습니다.
- 확장 집합의 threat defense virtual 인스턴스 수는 로드 조건에 따라 자동으로 조정 및 구성됩니다.

그림 *1: Threat Defense Virtual Auto Scale* 사용 사례 다이어그램



범위

이 문서에서는 위협 대응 가상 Auto Scale for Azure 솔루션의 서버리스 구성 요소를 구축하는 자세한 절차를 설명합니다.

중요

- 구축을 시작하기 전에 전체 문서를 읽어보십시오.
- 구축을 시작하기 전에 전제 조건이 충족되었는지 확인합니다.
- 여기에 설명된 대로 단계 및 실행 순서를 따라야 합니다.

구축 패키지 다운로드

Azure용 위협 대응 가상 Auto Scale 솔루션은 Azure에서 제공하는 서버리스 인프라(논리 앱, Azure Functions, 로드 밸런서, 가상 시스템 확장 집합 등)를 활용하는 ARM(Azure Resource Manager) 템플릿 기반 구축입니다.

Azure용 위협 대응 가상 Auto Scale 솔루션을 시작하는 데 필요한 파일을 다운로드합니다. 사용자 버전의 구축 스크립트 및 템플릿은 GitHub 리포지토리에서 제공됩니다.

- GitHub Autoscale

주의 Cisco에서 제공하는 자동 확장용 구축 스크립트 및 템플릿은 오픈 소스 예시로 제공되며 일반적인 Cisco TAC 지원 범위에서는 다루지 않습니다. GitHub에서 정기적으로 업데이트 및 ReadMe 지침을 확인하십시오.

ASM_Function.zip 패키지를 구축하는 방법에 대한 지침은 소스 코드로 Azure 기능 빌드, 60 페이지를 참고하십시오.

Auto Scale 솔루션 구성 요소

다음 구성 요소는 Azure용 위협 대응 가상 Auto Scale 솔루션을 구성합니다.

Azure Functions(Function 앱)

Function 앱은 Azure 함수의 집합입니다. 기본 기능은 다음과 같습니다.

- Azure 메트릭을 주기적으로 통신/프로브합니다.
- 위협 대응 가상 로드를 모니터링하고 축소/확장(Scale In/Scale Out 작업을 트리거합니다.
- 새 threat defense virtual를 management center에 등록합니다.
- management center를 통해 새 threat defense virtual를 구성합니다.
- management center에서 확장된 threat defense virtual을 등록 취소(제거)합니다.

이들 함수는 압축된 Zip 패키지 형식으로 제공됩니다(Azure Function 앱 패키지 빌드, 26 페이지 참조). 함수는 특정 작업을 수행하기 위해 가능한 한 개별적으로 유지되며, 개선 사항 및 새로운 릴리스 지원을 위해 필요에 따라 업그레이드할 수 있습니다.

오케스트레이터(Logic 앱)

Auto Scale Logic App은 하나의 워크플로우, 즉 시퀀스 단계 모음입니다. Azure 함수는 독립적인 엔터티이므로 서로 통신할 수 없습니다. 이 오케스트레이터는 이러한 함수의 실행을 시퀀싱하고 함수간 정보를 교환합니다.

- Logic App은 Auto Scale Azure 함수 간에 정보를 오케스트레이션하고 전달하는 데 사용됩니다.
- 각 단계는 Auto Scale Azure 함수 또는 기본 제공 표준 논리를 나타냅니다.
- Logic 앱은 JSON 파일로 제공됩니다.
- Logic 앱은 GUI 또는 JSON 파일을 통해 맞춤화할 수 있습니다.

VMSS(Virtual Machine Scale Set)

VMSS는 위협 대응 가상 디바이스와 같은 균일한 가상 시스템의 모음입니다.

- VMSS는 해당 집합에 동일한 새 VM을 추가할 수 있습니다.

- VMSS에 추가된 새 VM은 로드 밸런서, 보안 그룹 및 네트워크 인터페이스에 자동으로 연결됩니다.
- VMSS에는 Azure 위협 대응 가상용으로 사용하지 않도록 설정된 Auto Scale 기능이 내장되어 있습니다.
- VMSS에서 위협 대응 가상 인스턴스를 수동으로 추가하거나 삭제해서는 안 됩니다.

ARM(Azure Resource Manager) 템플릿

ARM 템플릿은 Azure용 위협 대응 가상 Auto Scale 솔루션에 필요한 리소스를 구축하는 데 사용됩니다.

ARM 템플릿은 다음을 포함하여 Auto Scale Manager 구성 요소에 대한 입력을 제공합니다.

- Azure Function 앱
- Azure Logic 앱
- VMSS(Virtual Machine Scale Set)
- 내부/외부 로드 밸런서
- 구축에 필요한 보안 그룹 및 기타 기타 구성 요소

중요 ARM 템플릿은 사용자 입력 검증과 관련하여 제한 사항이 있으므로 구축 중에 입력을 검증해야 합니다.

Auto Scale 솔루션 사전 요건

Azure 리소스

리소스 그룹

이 솔루션의 모든 구성 요소를 구축하려면 기존 또는 새로 생성 된 리소스 그룹이 필요합니다.

참고 나중에 사용할 수 있도록 리소스 그룹 이름, 리소스 그룹이 생성된 지역 및 Azure 구독 ID를 기록합니다.

네트워킹

가상 네트워크가 사용 가능/생성되었는지 확인합니다. Auto Scale 구축에서는 네트워킹 리소스를 생성, 변경 또는 관리하지 않습니다.

위협 대응 가상에는 4 개 네트워크 인터페이스가 필요하므로 가상 네트워크에는 4 개 서브넷이 필요합니다.

1. 관리 트래픽
2. 진단 트래픽
3. 내부 트래픽
4. 외부 트래픽

서브넷이 연결된 네트워크 보안 그룹에서 다음 포트를 열어야 합니다.

- SSH(TCP/22)

  로드 밸런서와 위협 대응 가상 사이의 상태 프로브에 필요합니다.

  서버리스 함수와 위협 대응 가상 간의 통신에 필요합니다.

- TCP/8305

  threat defense virtual와 management center 간 통신에 필요합니다.

- HTTPS(TCP/443)

  서버리스 구성 요소와 management center 간의 통신에 필요합니다.

- 애플리케이션별 프로토콜/포트

  모든 사용자 애플리케이션(예: TCP/80)에 필요합니다.

참고 가상 네트워크 이름, 가상 네트워크 CIDR, 4 개 서브넷의 이름, 외부 및 내부 서브넷의 게이트웨이 IP 주소를 기록합니다.

Azure Function 앱 패키지 빌드

위협 대응 가상 Auto Scale 솔루션은 아카이브 파일인 *ASM_Function.zip* 빌드가 필요하며, 이 파일은 압축된 ZIP 패키지로 개별 Azure 기능을 제공합니다.

ASM_Function.zip 패키지를 구축하는 방법에 대한 지침은 소스 코드로 Azure 기능 빌드, 60 페이지를 참고하십시오.

이들 함수는 특정 작업을 수행하기 위해 가능한 한 개별적이며, 개선 사항 및 새로운 릴리스 지원을 위해 필요에 따라 업그레이드할 수 있습니다.

Management Center 준비

모든 기능을 갖춘 멀티 디바이스 관리자인 management center를 사용해 threat defense virtual을 관리할 수 있습니다. threat defense virtual은 threat defense virtual 장비에 할당한 관리 인터페이스의 management center로 등록 및 통신합니다.

디바이스 그룹을 포함해 threat defense virtual 설정 및 관리를 위해 필요한 모든 객체를 생성하면 여러 디바이스에 정책을 쉽게 배포하고 업데이트를 설치할 수 있습니다. 디바이스 그룹에 적용되는 모든 설정은 threat defense virtual 인스턴스에 푸시됩니다.

다음 섹션에서는 management center 준비를 위한 기본 단계를 간략히 소개합니다. 자세한 내용은 Firepower Management Center Configuration Guide를 참조하세요. management center를 준비할 때는 다음 정보를 기록하십시오.

- management center 공용 IP 주소.
- management center 사용자 이름/비밀번호.
- 보안 정책 이름
- 내부 및 외부 보안 영역 개체 이름
- 디바이스 그룹 이름

새 **Management Center** 사용자 생성

AutoScale Manager에서만 사용할 관리자 권한이 있는 management center의 새 사용자를 생성합니다.

중요 다른 management center 세션과의 충돌을 방지하려면 threat defense virtual Auto Scale 솔루션 전용 management center 사용자 계정이 있어야 합니다.

프로시저

단계 **1** management center에서 관리자 권한으로 새 사용자를 생성합니다. **System(**시스템**)** > **Users(**사용자**)**를 선택하고 **Create User(**사용자 생성**)**를 클릭합니다.

사용자 이름은 다음과 같은 Linux 기준을 준수해야 합니다.

- 최대 32개의 영숫자 문자와 하이픈(-) 및 밑줄(_)
- 모두 소문자
- 하이픈(-)으로 시작할 수 없으며, 숫자만으로 구성할 수 없고, 마침표(.), 단가 기호(@) 또는 슬래시(/)를 포함할 수 없음

단계 **2** 환경에 필요한 대로 사용자 옵션을 완료합니다. 자세한 내용은 Cisco Secure Firewall Management Center 관리 가이드를 참조하십시오.

액세스 제어 구성

액세스 제어를 내부에서 외부로 향하는 트래픽을 허용하도록 구성합니다. 액세스 제어 정책 내에서 액세스 제어 규칙은 여러 매니지드 디바이스에서 네트워크 트래픽을 처리하는 세분화된 방법을 제

공합니다. 효과적인 구축을 위해서는 규칙을 올바르게 구성하고 그 순서를 지정해야 합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드의 "액세스 제어 모범 사례"를 참고하십시오.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)**을 선택합니다.

단계 **2** **New Policy(**새로운 정책**)**를 클릭합니다.

단계 **3** 고유한 **Name(**이름**)**을 입력하고, 필요한 경우 **Description(**설명**)**을 입력합니다.

단계 **4** 고급 보안 설정 및 규칙을 구성하려면 Cisco Secure Firewall Management Center 디바이스 구성 가이드를 참고하십시오.

라이선싱 구성

모든 라이선스는 management center를 통해 threat defense에 제공됩니다. 선택적으로 다음 기능 라이선스를 구매할 수 있습니다.

- **Secure Firewall Threat Defense IPS** - 보안 인텔리전스 및 Cisco Secure IPS
- **Secure Firewall Threat Defense Malware Defense** - 악성코드 방어
- **Secure Firewall Threat Defense URL** 필터링 - 필터링
- **RA VPN**—AnyConnect Plus, AnyConnect Apex 또는 AnyConnect VPN 전용입니다.

참고 IPS, 악성코드 디펜스 또는 URL 필터링 라이선스를 구매하고 1년, 3년 또는 5년 동안 업데이트에 액세스하려면 그에 대응하는 구독 라이선스도 필요합니다.

시작하기 전에

- Cisco Smart Software Manager에서 마스터 계정을 만듭니다.

  아직 어카운트가 없는 경우 새 어카운트 설정 링크를 클릭합니다. Smart Software Manager에서 조직의 마스터 계정을 만들 수 있습니다.

- Cisco Smart Software Licensing 계정은 일부 기능(export-compliance 플래그를 사용하여 활성화됨)을 사용하려면 강력한 암호화(3DES/AES) 라이선스 자격을 얻어야 합니다.

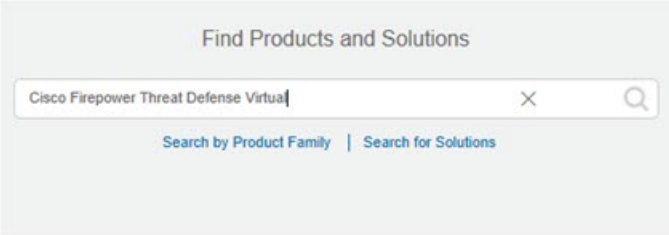
프로시저

단계 **1** Smart Licensing 계정에서 필요한 라이선스가 사용 가능한지 확인합니다.

Cisco 또는 리셀러에서 디바이스를 구매한 경우 라이선스는 Smart Software License 계정에 연결되어 있어야 합니다. 그러나 라이선스를 직접 추가해야 하는 경우 Cisco Commerce Workspace에서 **Find**

Products and Solutions(제품 및 솔루션 찾기**)** 검색 필드를 사용합니다. 다음 라이선스 PID를 검색합니다.

그림 *2:* 라이선스 검색



참고 PID를 찾을 수 없는 경우 주문에 수동으로 PID를 추가할 수 있습니다.

단계 **2** 아직 등록하지 않은 경우 management center을 Smart Licensing 서버에 등록합니다.

등록하려면 Smart Software Manager에서 등록 토큰을 생성해야 합니다. 자세한 지침은 Cisco Secure Firewall Management Center 관리 가이드 항목을 참조하십시오.

보안 영역 개체 생성

구축을 위해 내부 및 외부 보안 영역 개체를 생성합니다.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택합니다.
단계 **2** 개체 유형 목록에서 **Interface(**인터페이스**)**를 선택합니다.
단계 **3** **Add** > **Security Zone(**보안 영역 추가**)**을 클릭합니다.
단계 **4** 이름을 입력합니다(예: *inside*, *outside*).
단계 **5** 인터페이스 유형으로 라우팅을 선택합니다.
단계 **6** **Save(**저장**)**를 클릭합니다.

디바이스 그룹 생성

디바이스 그룹을 사용하면 쉽게 정책을 할당하고 여러 디바이스에 업데이트를 설치할 수 있습니다.

프로시저

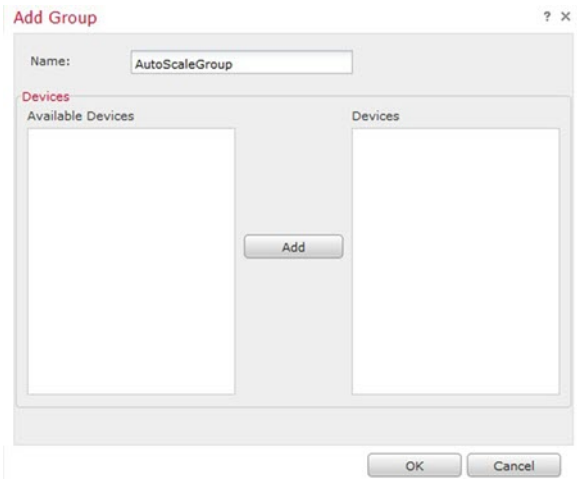
단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택합니다.

그림 *3:* 디바이스 관리

단계 **2** 드롭다운 메뉴의 **Add(**추가**)**에서 **Add Group(**그룹 추가**)**를 선택합니다.

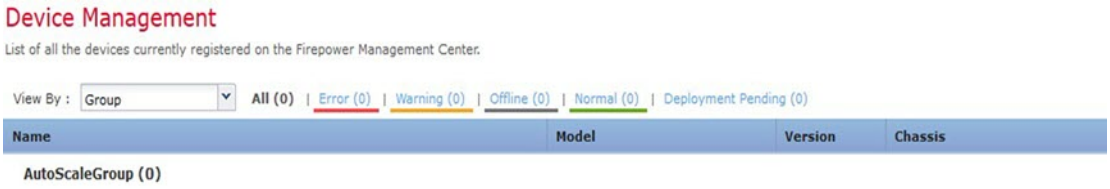
단계 **3** **Name(**이름**)**을 입력합니다. 예를 들면 *AutoScaleGroup*.

그림 *4:* 디바이스 그룹 추가



단계 **4** 디바이스 그룹에 추가하려면 **OK(**확인**)**를 클릭합니다.

그림 *5:* 디바이스 그룹 추가됨



보안 쉘 액세스 구성

threat defense 디바이스의 플랫폼 설정은 값을 여러 디바이스 간에 공유하려고 할 수 있는 비 관련 기능을 구성합니다. Threat Defense Virtual Auto Scale for Azure이 내부/외부 영역의 SSH 및 Auto Scale 그룹에 대해 생성된 디바이스 그룹을 허용하려면 threat defense 플랫폼 설정 정책이 필요합니다. 이는 threat defense virtual의 데이터 인터페이스가 로드 밸런서에서 상태 프로브에 응답할 수 있도록 하는 데 필요합니다.

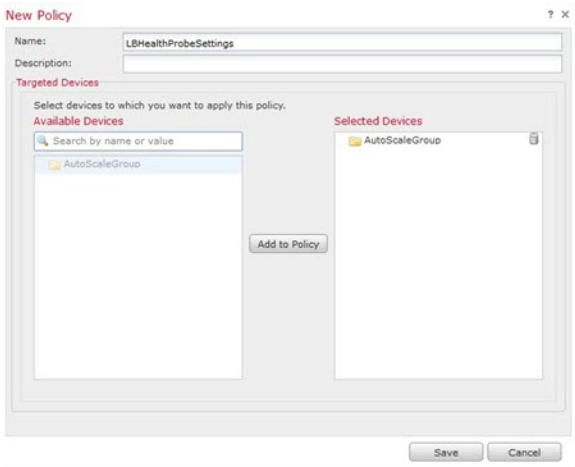
시작하기 전에

- 디바이스에 SSH 연결을 허용할 호스트 또는 네트워크를 정의하는 네트워크 개체가 필요합니다. 이 절차의 일부로 개체를 추가할 수 있지만 개체 그룹을 사용하여 IP 주소 그룹을 식별하려면 규칙에 필요한 그룹이 이미 있는지 확인합니다. **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택하여 개체를 설정합니다. 예를 들어 다음 절차의 *azure-utility-ip(168.63.129.16)* 개체를 참조하십시오.

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 threat defense 정책을(예: *LBHealthProbeSettings*) 생성하거나 수정합니다.

그림 ***6: Threat Defense*** 플랫폼 설정 정책



단계 **2** **Secure Shell**을 선택합니다.

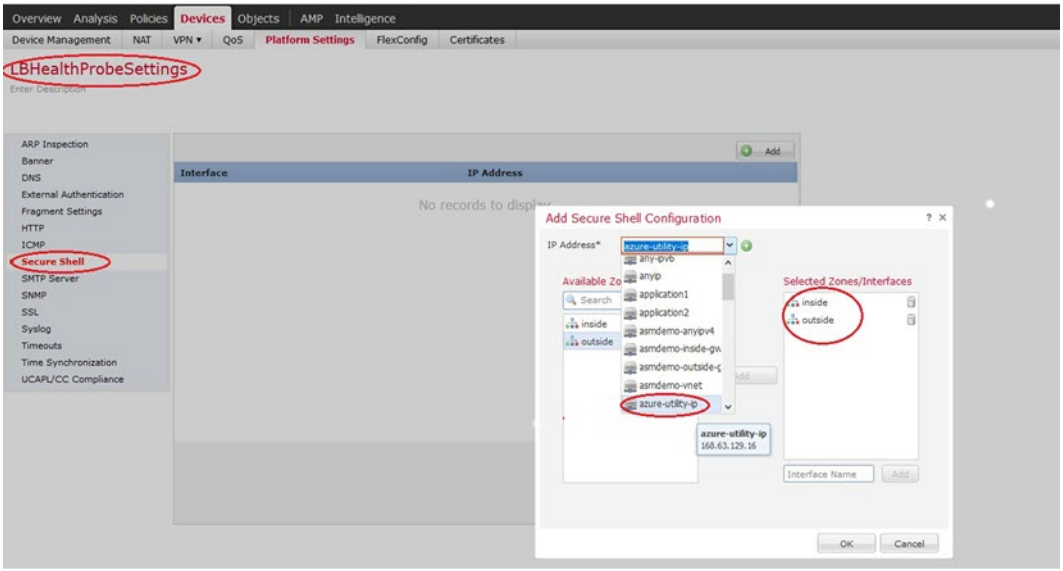
단계 **3** SSH 연결을 허용하는 인터페이스와 IP 주소를 확인합니다.

a) **Add(**추가**)**를 클릭해 새 규칙을 추가하거나, **Edit(**편집**)**을 클릭해 기존 규칙을 편집합니다.

b) 규칙 속성을 구성합니다.

- **IP Address(IP** 주소**)** - SSH 연결을 허용하는 호스트 또는 네트워크를 식별하는 네트워크 개체입니다(예: *azure-utility-ip (168.63.129.16)*). 드롭다운 메뉴에서 개체를 선택하거나 +를 클릭하여 새 네트워크 개체를 추가합니다.
- **Security Zones(**보안 영역**)** - SSH 연결을 허용할 인터페이스가 포함된 영역을 추가합니다. 예를 들어 내부 인터페이스는 내부 영역에, 외부 인터페이스는 외부 영역에 할당할 수 있습니다. management center의 개체 페이지에서 보안 영역을 생성할 수 있습니다. 보안 영역에 대한 자세한 내용은 Cisco Secure Firewall Management Center 디바이스 구성 가이드를 참조하십시오.
- **OK(**확인**)**를 클릭합니다.

그림 *7: Threat Defense Virtual Auto Scale*을 위한 *SSH* 액세스



단계 **4** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

NAT 구성

NAT 정책을 생성하고 외부 인터페이스에서 애플리케이션으로 트래픽을 전달하는 데 필요한 NAT 규칙을 생성하고 이 정책을 자동 확장을 위해 생성한 디바이스 그룹에 연결합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **NAT**를 선택합니다.

단계 **2** **New Policy(**새 정책**)** 드롭다운 목록에서 **Threat Defense NAT**를 선택합니다.

단계 **3** 고유한 **Name(**이름**)**을 입력합니다.

단계 **4** 필요한 경우 **Description(**설명**)**을 입력합니다.

단계 **5** NAT 규칙을 구성합니다. NAT 규칙을 생성하고 NAT 정책을 적용하는 방법에 대한 지침은 Cisco Secure Firewall Management Center 디바이스 구성 가이드의 "Configure NAT for Threat Defense" 절차를 참조하십시오. 다음 그림에는 기본 접근 방식이 나와 있습니다.

그림 ***8: NAT*** 정책 예

참고 따라서 변환 문제와 까다로운 트러블슈팅 상황을 방지하기 위해 규칙을 최대한 단순하게 유지하는 것이 좋습니다. 그리고 NAT를 구현하기 전에 면밀한 계획을 세워야 합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

입력 매개변수

다음 표에서는 템플릿 매개 변수를 정의하고 일 예를 제공합니다. 이러한 값을 결정하고 나면 Azure 구독에 ARM 템플릿을 구축할 때 이러한 매개 변수를 사용하여 위협 대응 가상 디바이스를 생성할 수 있습니다. Auto Scale ARM 템플릿 구축, 41 페이지의 내용을 참조하십시오.

표 ***2:*** 템플릿 매개변수

매개 변수 이름	허용되는 값 / 유형	설명	리소스 생성 유형
resourceNamePrefix	문자열 * (3 ~ 10 자)	모든 리소스는 이 접두사를 포함하는 이름으로 생성됩니다. 참고: 소문자만 사용하십시오. 예: ftdv	New
virtualNetworkRg	문자열	가상 네트워크 리소스 그룹 이름입니다. 예: cisco-virtualnet-rg	기존
virtualNetworkName	문자열	가상 네트워크 이름(이미 생성됨) 예: cisco-virtualnet	기존
virtualNetworkCidr	CIDR 형식 x.x.x.x/y	가상 네트워크의 CIDR(이미 생성됨)	기존
mgmtSubnet	문자열	관리 서브넷 이름(이미 생성됨) 예: cisco-mgmt-subnet	기존

매개 변수 이름	허용되는 값 / 유형	설명	리소스 생성 유형
diagSubnet	문자열	진단 서브넷 이름(이미 생성됨) 예: cisco-diag-subnet	기존
insideSubnet	문자열	내부 서브넷 이름(이미 생성됨) 예: cisco-inside-subnet	기존
internalLbIp	문자열	내부 서브넷(이미 생성됨)의 내부 로드 밸런서 IP 주소입니다. 예: 1.2.3.4.	기존
insideNetworkGatewayIp	문자열	내부 서브넷 게이트웨이 IP 주소(이미 생성됨)	기존
outsideSubnet	문자열	외부 서브넷 이름(이미 생성됨) 예: cisco-outside-subnet	기존
outsideNetworkGatewayIp	문자열	외부 서브넷 게이트웨이 IP(이미 생성됨)	기존
deviceGroupName	문자열	management center의 디바이스 그룹(이미 생성됨)	기존
insideZoneName	문자열	management center의 내부 영역 이름(이미 생성됨)	기존
outsideZoneName	문자열	management center의 외부 영역 이름(이미 생성됨)	기존
softwareVersion	문자열	위협 대응 가상 버전(구축 중 드롭 다운에서 선택)	기존
vmSize	문자열	위협 대응 가상 인스턴스의 크기(구축 중 드롭 다운에서 선택).	해당 없음
ftdLicensingSku	문자열	Threat Defense Virtual 라이선싱 모드(PAYG / BYOL) 참고: PAYG는 버전 6.5 이상에서 지원됩니다.	해당 없음
licenseCapability	쉼표로 구분된 문자열	기본, 악성코드, URL 필터링, 위협	해당 없음

매개 변수 이름	허용되는 값 / 유형	설명	리소스 생성 유형
ftdVmManagementUserName	문자열*	threat defense virtual VM 관리 관리자 사용자 이름입니다. 이는 관리자가 될 수 없습니다. Azure for VM administrator user name guidelines를 참조하십시오.	New
ftdVmManagementUserPassword	문자열*	threat defense virtual VM 관리 관리자 사용자의 비밀번호입니다. 비밀번호는 12 ~ 72자여야 하며 소문자, 대문자, 숫자 및 특수 문자를 포함해야 합니다. 같은 문자를 세 번 이상 반복해서 사용할 수 없습니다. 참고 템플릿에는 이에 대한 규정 준수 확인이 없습니다.	New
fmcIpAddress	문자열 x.x.x.x	management center의 공용 IP 주소(이미 생성됨)	기존
fmcUserName	문자열	관리자 권한이 있는 Management Center 사용자 이름(이미 생성됨)	기존
fmcPassword	문자열	위의 management center 사용자 이름에 대한 Management Center 비밀번호(이미 생성됨)	기존
policyName	문자열	management center에서 생성된 보안 정책(이미 생성됨)	기존

매개 변수 이름	허용되는 값 / 유형	설명	리소스 생성 유형
scalingPolicy	POLICY-1 / POLICY-2	**POLICY-1**: 어떤 위협 대응 가상 평균로드가 구성된 기간 동안 확장 임계값을 초과하면 확장(Scale-Out)이 트리거됩니다. **POLICY-2**: 자동 확장 그룹 내의 모든 위협 대응 가상 평균로드가 구성된 기간 동안 확장 임계값을 초과하면 확장(Scale-Out)이 트리거됩니다. 두 경우 모두 축소(Scale-In) 논리는 동일하게 유지됩니다. 모든 위협 대응 가상 디바이스의 평균로드가 구성된 기간 동안 축소 임계값 미만이 되면 축소가 트리거됩니다.	해당 없음
scalingMetricsList	문자열	스케일링 결정을 내리는 데 사용되는 메트릭입니다. 허용됨: CPU CPU, 메모리 기본값: CPU	해당 없음
cpuScaleInThreshold	문자열	CPU 메트릭에 대한 축소 임계값입니다. 기본값: 10 위협 대응 가상 메트릭이 이 값보다 작으면 축소(Scale-In)가 트리거됩니다. Auto Scale 논리, 57 페이지의 내용을 참조하십시오.	해당 없음

매개 변수 이름	허용되는 값 / 유형	설명	리소스 생성 유형
cpuScaleOutThreshold	문자열	CPU 메트릭의 확장 임계값입니다. 기본값: 80 메트릭이이 값을 초과하면 스케일 아웃이 트리거됩니다.위협 대응 가상 'cpuScaleOutThreshold'는 항상 'cpuScaleInThreshold' 보다 커야 합니다. Auto Scale 논리, 57 페이지의 내용을 참조하십시오.	해당 없음
memoryScaleInThreshold	문자열	메모리 메트릭에 대한 축소(Scale-In) 임계값(%)입니다. 기본값: 0 위협 대응 가상 메트릭이 이 값보다 작으면 축소(Scale-In)가 트리거됩니다. Auto Scale 논리, 57 페이지의 내용을 참조하십시오.	해당 없음
memoryScaleOutThreshold	문자열	메모리 메트릭에 대한 확장(Scale-Out) 임계값(%)입니다. 기본값: 0 위협 대응 가상 메트릭이 이 값을 초과하면 확장(Scale-Out)이 트리거됩니다. 'memoryScaleOutThreshold'는 항상'memoryScaleInThreshold'보다 커야 합니다. Auto Scale 논리, 57 페이지의 내용을 참조하십시오.	해당 없음
minFtdCount	정수	지정된 시간에 설정된 확장 집합에서 사용 가능한 최소 위협 대응 가상 인스턴스. 예: 2	해당 없음

매개 변수 이름	허용되는 값 / 유형	설명	리소스 생성 유형
maxFtdCount	정수	확장 집합에서 허용되는 최대 위협 대응 가상 인스턴스 수입니다. 예: 10 참고 이 수는 management center 용량에 의해 제한됩니다. Auto Scale 논리는 이 변수의 범위를 확인하지 않으므로 신중하게 입력하십시오.	해당 없음
metricsAverageDuration	정수	드롭다운에서 선택 이 숫자는 메트릭이 평균화되는 시간(분)을 나타냅니다. 이 변수의 값이 5(즉, 5)인 경우, Auto Scale Manager가 예약되면 메트릭의 지난 5분 평균을 확인하고 이를 기반으로 하여 확장 결정을 내립니다. 참고 Azure 제한으로 인해 숫자 1, 5, 15, 30만 유효합니다.	해당 없음

매개 변수 이름	허용되는 값 / 유형	설명	리소스 생성 유형
initDeploymentMode	일괄(BULK) / 단계별(STEP)		

매개 변수 이름	허용되는 값 / 유형	설명	리소스 생성 유형
		기본적으로 첫 번째 구축 또는 확장 집합에 위협 대응 가상 인스턴스가 포함되지 않은 경우에 적용됩니다. 일괄(BULK): Aucto Scale Manager가 한 번에 'minFtdCount '개의 위협 대응 가상 인스턴스 수를 동시에 구축하려고 시도합니다. 참고 실행은 동시에 진행되지만 management center에 등록하는 것은 management center 제한으로 인해 순차적입니다. 단계별(STEP): Auto Scale Manager는 예약된 간격마다 하나씩 'minFtdCount '개의 위협 대응 가상 디바이스를 구축합니다. 참고 단계별 옵션은 'minFtdCount' 인스턴스가 management center와 함께 시작 및 구성되고 작동 상태가 되지만 디버깅에 유용할 때까지 시간이 오래 걸립니다. 일괄 옵션은 하나의 threat defense virtual 실행이 병렬로 실행되기 때문에 threat defense virtual의 'minFtdCount'개 전부를 시작하는 데 동일한 시간이 걸리지만 management center 등록은 순차적입니다. threat defense virtual의 'minFtdCount'개를 구축	

매개 변수 이름	허용되는 값 / 유형	설명	리소스 생성 유형
		하는 데 걸리는 총 시간 = (1개 threat defense virtual를 실행하는 시간 + 1개 threat defense virtual를 등록/구성하는 시간 * minFtdCount).	
* Azure에는 새 리소스의 명명 규칙에 제한 사항이 있습니다. 제한 사항을 검토하거나 간단히 모두 소문자를 사용하십시오. 공백이나 특수 문자는 사용하지 마십시오.			

Auto Scale 구축

구축 패키지 다운로드

Azure용 위협 대응 가상 Auto Scale 솔루션은 Azure에서 제공하는 서버리스 인프라(논리 앱, Azure Functions, 로드 밸런서, 가상 시스템 확장 집합 등)를 활용하는 ARM(Azure Resource Manager) 템플릿 기반 구축입니다.

Azure용 위협 대응 가상 Auto Scale 솔루션을 시작하는 데 필요한 파일을 다운로드합니다. 사용자 버전의 구축 스크립트 및 템플릿은 GitHub 리포지토리에서 제공됩니다.

- GitHub Autoscale

주의 Cisco에서 제공하는 자동 확장용 구축 스크립트 및 템플릿은 오픈 소스 예시로 제공되며 일반적인 Cisco TAC 지원 범위에서는 다루지 않습니다. GitHub에서 정기적으로 업데이트 및 ReadMe 지침을 확인하십시오.

ASM_Function.zip 패키지를 구축하는 방법에 대한 지침은 소스 코드로 Azure 기능 빌드, 60 페이지를 참고하십시오.

Auto Scale ARM 템플릿 구축

ARM 템플릿은 위협 대응 가상 Auto Scale for Azure에 필요한 리소스를 구축하는 데 사용됩니다. 지정된 리소스 그룹 내에서 ARM 템플릿 구축은 다음을 생성합니다.

- VMSS(Virtual Machine Scale Set)
- 외부 로드 밸런서
- 내부 로드 밸런서
- Azure Function 앱

- Logic 앱
- 보안 그룹 (데이터 및 관리 인터페이스용)

시작하기 전에

- GitHub 리포지토리(https://github.com/CiscoDevNet/cisco-ftdv/tree/master/autoscale/azure)에서 ARM 템플릿 *azure_ ftdv _autoscale.json*을 다운로드합니다.

프로시저

단계 **1** 여러 Azure 영역에서 위협 대응 가상 인스턴스를 구축해야 하는 경우 구축 영역에서 사용 가능한 영역을 기준으로 하여 ARM 템플릿을 편집합니다.

예제:

```
"zones": [
    "1",
    "2",
    "3"
],
```

이 예에서는 3개의 영역이 있는“Central US” 지역을 보여줍니다.

단계 **2** 외부 로드 밸런서에 필요한 트래픽 규칙을 수정합니다. 이 'json' 어레이를 확장하여 원하는 수의 규칙을 추가할 수 있습니다.

예제:

```
{
 "type": "Microsoft.Network/loadBalancers",
 "name": "[variables('elbName')]",
 "location": "[resourceGroup().location]",
 "apiVersion": "2018-06-01",
 "sku": {
   "name": "Standard"
 },
 "dependsOn": [
   "[concat('Microsoft.Network/publicIPAddresses/', variables('elbPublicIpName'))]"

 ],
 "properties": {
   "frontendIPConfigurations": [
     {
       "name": "LoadBalancerFrontEnd",
         "properties": {
           "publicIPAddress": {
             "id": "[resourceId('Microsoft.Network/publicIPAddresses/',
variables('elbPublicIpName'))]"
           }
         }
     }
   ],
   "backendAddressPools": [
     {
```

```
            "name": "backendPool"
          }
        ],
        "loadBalancingRules": [
          {
            "properties": {
              "frontendIPConfiguration": {
                "Id": "[concat(resourceId('Microsoft.Network/loadBalancers',
variables('elbName')), '/frontendIpConfigurations/LoadBalancerFrontend')]"
              },
              "backendAddressPool": {
                "Id": "[concat(resourceId('Microsoft.Network/loadBalancers',
variables('elbName')), '/backendAddressPools/BackendPool')]"
              },
              "probe": {
                "Id": "[concat(resourceId('Microsoft.Network/loadBalancers',
variables('elbName')), '/probes/lbprobe')]"
              },
              "protocol": "TCP",
              "frontendPort": "80",
              "backendPort": "80",
              "idleTimeoutInMinutes": "[variables('idleTimeoutInMinutes')]"
            },
            "Name": "lbrule"
          }
        ],
```

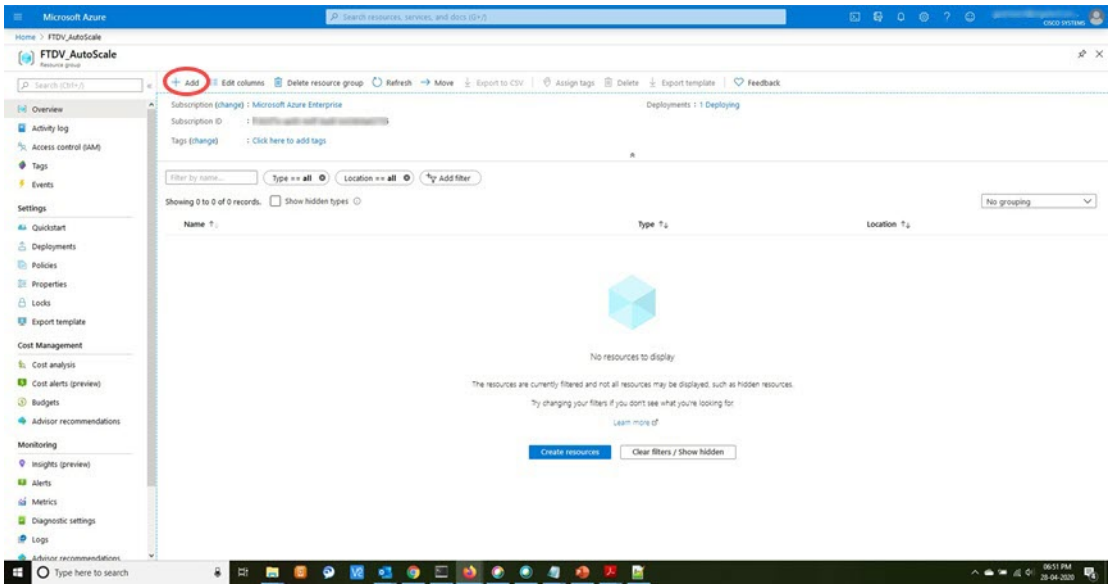
참고 이 파일을 편집하지 않으려는 경우 Azure 포털 구축후(post-deployment)에서 이를 편집할 수도 있습니다.

단계 **3** Microsoft 계정 사용자 이름 및 비밀번호를 사용하여 Microsoft Azure 포털에 로그인합니다.

단계 **4** 서비스 메뉴에서 **Resource groups(**리소스 그룹**)**를 클릭하여 리소스 그룹 블레이드에 액세스합니다. 블레이드에 나열된 구독의 모든 리소스 그룹이 표시됩니다.

새 리소스 그룹을 생성하거나 기존의 빈 리소스 그룹을 선택합니다(예:위협 대응 가상 *_AutoScale*).

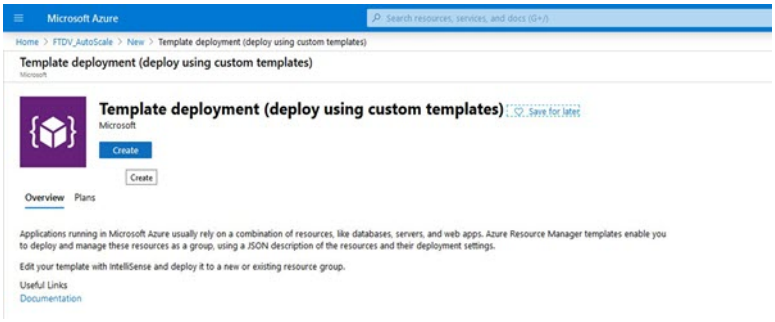
그림 ***9: Azure Portal***



단계 **5** **Create a resource(**리소스 생성**)(+)**를 클릭하여 템플릿 구축을 위한 새 리소스를 생성합니다. Create Resource Group(리소스 그룹 생성) 블레이드가 나타납니다.

단계 **6** **Search the Marketplace(**마켓플레이스 검색**)**에서 **Template deployment(**구축 **(**맞춤형 템플릿 사용**))**를 입력한 다음 **Enter** 키를 누릅니다.

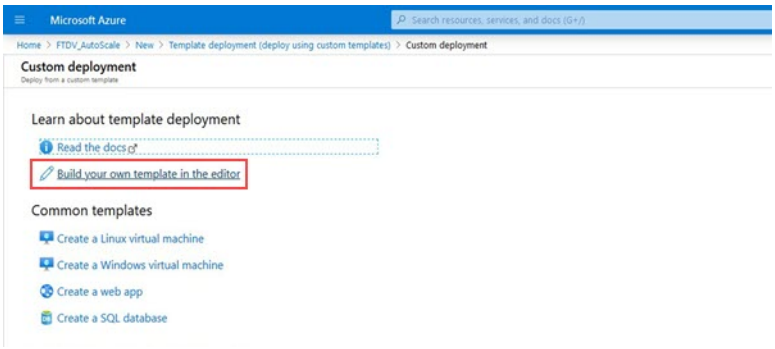
그림 ***10:*** 맞춤형 템플릿 구축



단계 **7** **Create(**생성**)**를 클릭합니다.

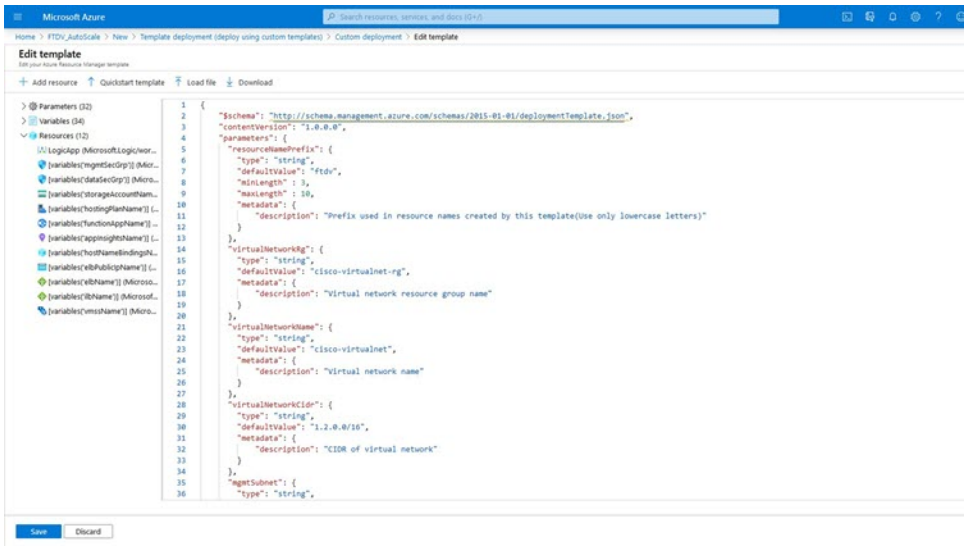
단계 **8** 템플릿을 생성하기 위한 몇 가지 옵션이 있습니다. **Build your own template in editor(**편집기에서 자체 템플릿 구축**)**를 선택합니다.

그림 ***11:*** 자체 템플릿 만들기



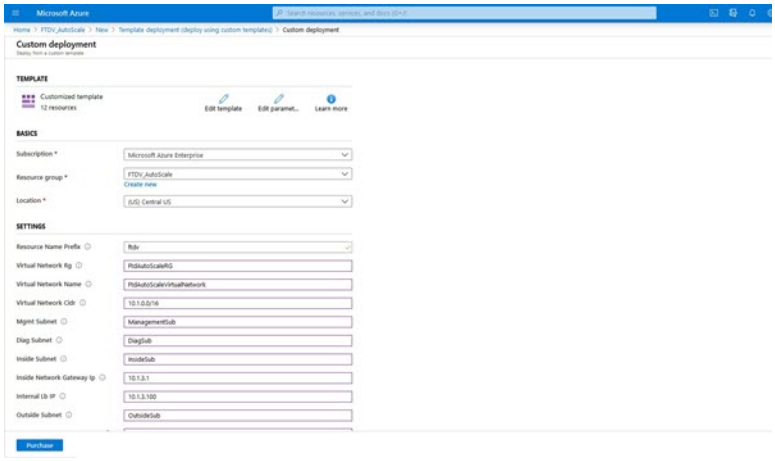
단계 **9** **Edit template(**템플릿 편집**)** 창에서 모든 기본 콘텐츠를 삭제하고 업데이트된 *azure_ ftdv _autoscale.json* 에서 콘텐츠를 복사하고 **Save(**저장**)**를 클릭합니다.

그림 *12:* 템플릿 수정



단계 **10** 다음 섹션에서 모든 매개변수를 입력합니다. 각 매개변수에 대한 자세한 내용은 입력 매개변수, 33 페이지를 참조한 다음 **Purchase(**구매**)**를 클릭하십시오.

그림 *13: ARM* 템플릿 매개변수

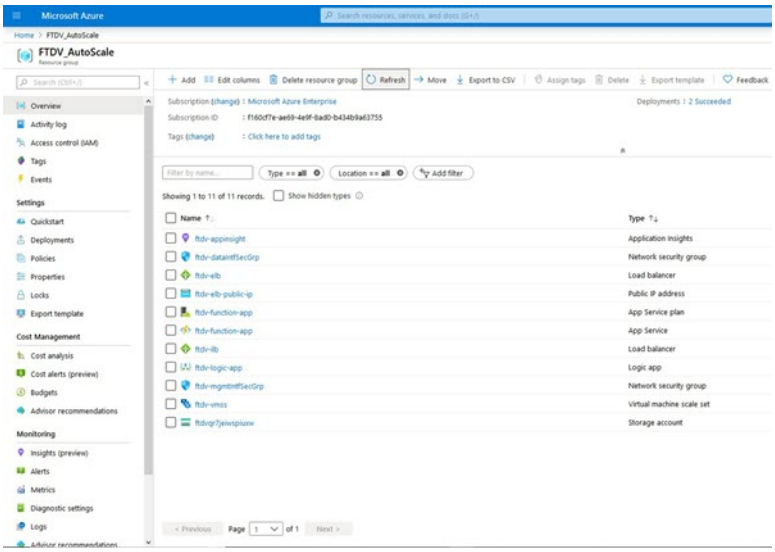


참고 **Edit Parameters(**매개변수 편집**)**를 클릭하고 JSON 파일을 편집하거나 미리 채워진 내용을 업로드할 수도 있습니다.

ARM 템플릿은 입력 검증 기능이 제한되어 있으므로 올바른 입력 검증을 제공하는 것은 사용자의 책임입니다.

단계 **11** 템플릿 구축이 성공하면 Azure용 위협 대응 가상 Auto Scale 솔루션에 필요한 모든 리소스가 생성됩니다. 다음 그림의 리소스를 참조하십시오. Type(유형) 열은 논리 앱, VMSS, 로드 밸런서, 공용 IP 주소 등 각 리소스에 대해 설명합니다.

그림 *14: Threat Defense Virtual Auto Scale Template* 구축



Azure Function 앱 구축

ARM 템플릿을 구축할 때 Azure는 기본 Function 앱을 생성합니다. 그러면 Auto Scale Manager 논리에 필요한 함수를 사용하여 수동으로 업데이트하고 구성해야 합니다.

시작하기 전에

- *ASM_Function.zip* 패키지를 빌드합니다. 소스 코드로 Azure 기능 빌드, 60 페이지의 내용을 참조하십시오.

프로시저

단계 **1** ARM 템플릿을 구축할 때 생성한 Function 앱으로 이동하여 함수가 없는지 확인합니다. 브라우저에서 다음 URL로 이동합니다.

https://<Function App Name>.scm.azurewebsites.net/DebugConsole

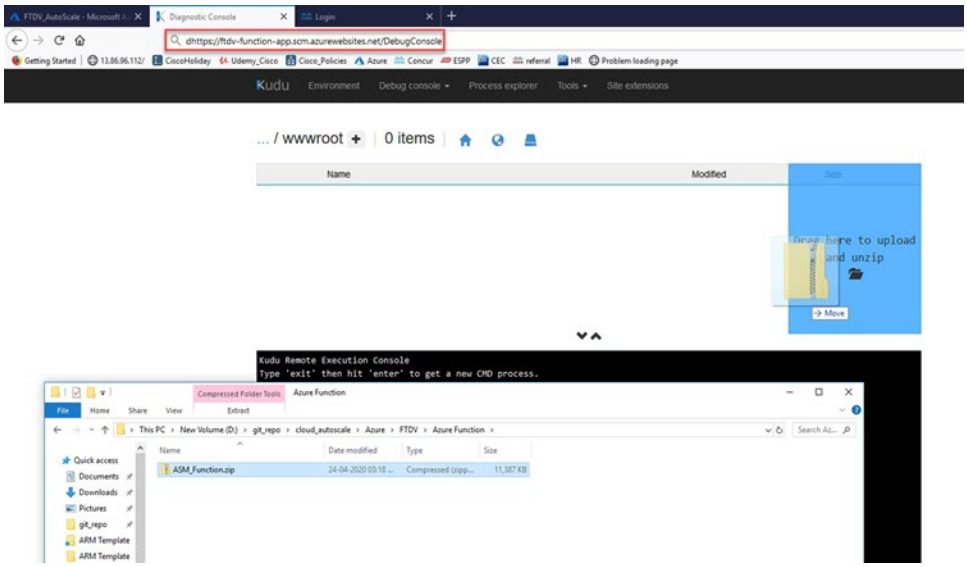
Auto Scale ARM 템플릿 구축, 41 페이지의 예:

https://ftdv-function-app.scm.azurewebsites.net/DebugConsole

단계 **2** 파일 탐색기에서 **site/wwwroot**로 이동합니다.

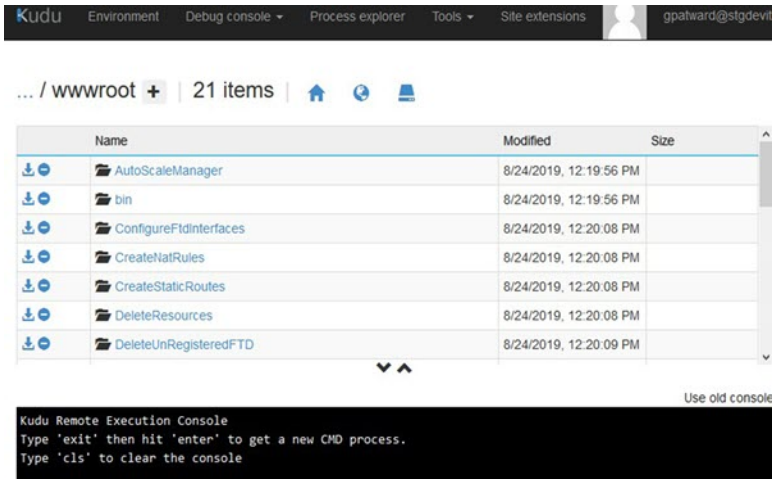
단계 **3** **ASM_Function.zip**을 파일 탐색기의 오른쪽 모서리로 끌어다 놓습니다.

그림 ***15: Threat Defense Virtual Auto Scale*** 기능 업로드



단계 **4** 업로드에 성공하면 모든 서버리스 함수가 표시됩니다.

그림 ***16: Threat Defense*** 가상 서버리스 기능

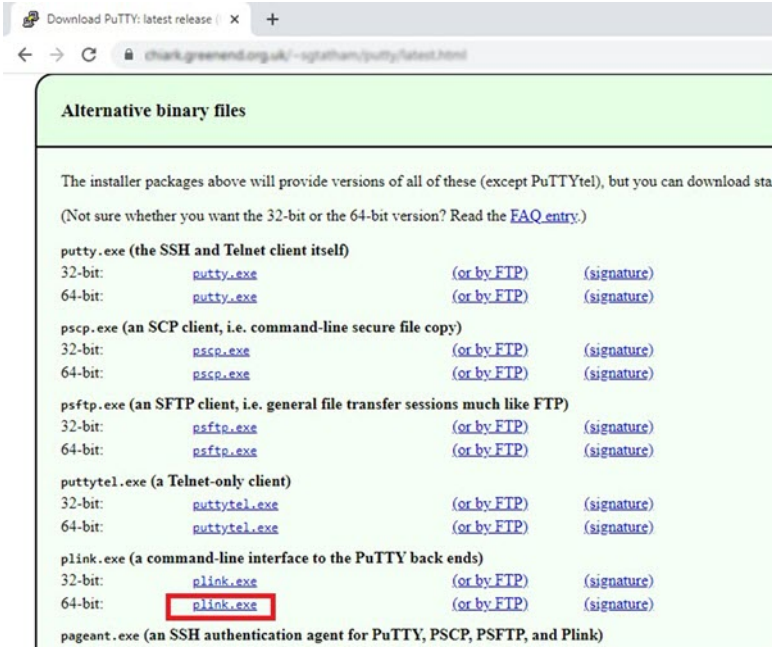


단계 **5** PuTTY SSH 클라이언트를 다운로드합니다.

Azure 함수는 SSH 연결을 통해 위협 대응 가상에 액세스해야 합니다. 그러나 서버리스 코드에서 사용되는 오픈 소스 라이브러리는 위협 대응 가상에서 사용하는 SSH 키 교환 알고리즘을 지원하지 않습니다. 따라서 사전 구축된 SSH 클라이언트를 다운로드해야 합니다.

www.putty.org에서 PuTTY 명령줄 인터페이스를 PuTTY 백엔드(*plink.exe*)에 다운로드합니다.

그림 *17: PuTTY* 다운로드



단계 **6** SSH 클라이언트 실행 파일의 이름 **plink.exe**를 **ftdssh.exe** 로 변경합니다.

단계 **7** 파일 탐색기의 오른쪽 모서리, 즉 이전 단계에서 **ASM_Function.zip**이 업로드된 위치에 **ftdssh.exe** 를 끌어다 놓습니다.

단계 **8** SSH 클라이언트에 해당 함수 애플리케이션이 있는지 확인합니다. 필요한 경우 페이지를 새로 고칩니다.

컨피그레이션 조정

Auto Scale Manager를 조정하거나 디버깅에 사용할 수 있는 몇 가지 컨피그레이션이 있습니다. 이러한 옵션은 ARM 템플릿에 표시되지 않지만 Function 앱 아래에서 수정할 수 있습니다.

시작하기 전에

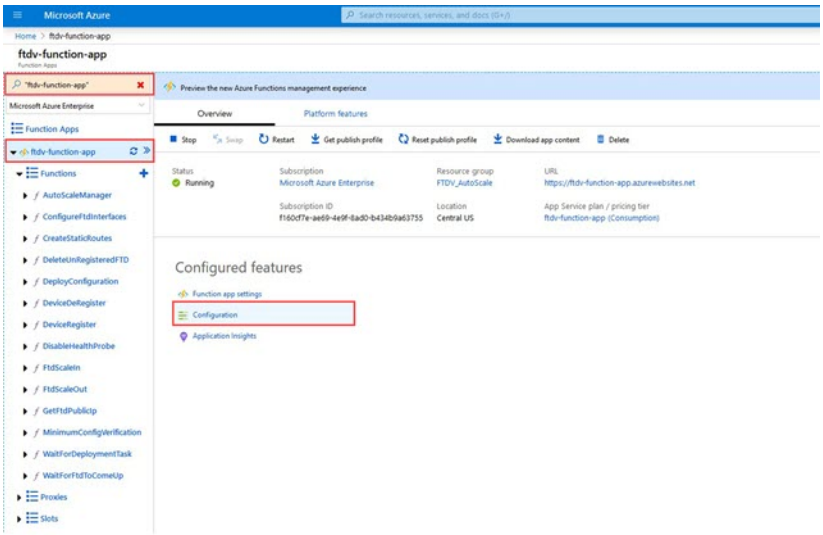
참고 이즌 언제든지 수정할 수 있습니다. 컨피그레이션을 수정하려면 이 순서를 따릅니다.

- Function 앱을 비활성화합니다.
- 기존의 예약된 작업이 완료 될 때까지 기다립니다.
- 컨피그레이션을 수정하고 저장합니다.
- Function 앱을 활성화합니다.

프로시저

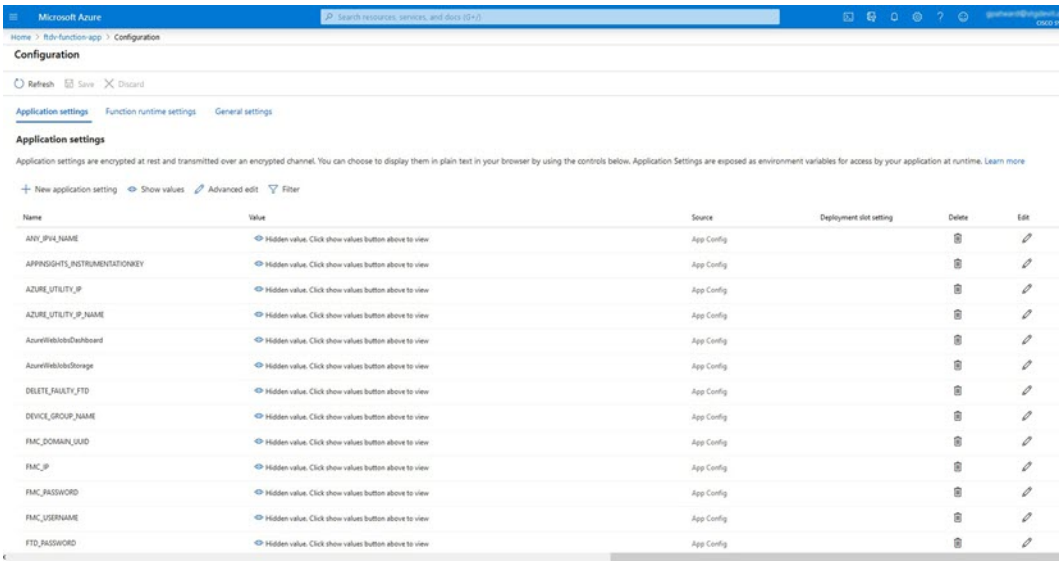
단계 **1** Azure Portal에서 위협 대응 가상 함수 애플리케이션을 검색하여 선택합니다.

그림 ***18: Threat Defense*** 가상 기능 애플리케이션



단계 **2** 여기서는 ARM 템플릿을 통해 전달된 컨피그레이션을 수정할 수도 있습니다. 변수 이름은 ARM 템플릿과 다르게 표시될 수 있지만 이러한 변수의 용도를 해당 이름에서 쉽게 식별할 수 있습니다.

그림 ***19:*** 애플리케이션 설정



대부분의 옵션은 이름에 그 설명을 담고 있습니다. 대표적인 예는 다음과 같습니다.

- 컨피그레이션 이름: “DELETE_FAULTY_FTD”(기본값: YES)

확장 중에 새 위협 대응 가상 인스턴스가 시작되고 management center에 등록됩니다. 등록 이 실패할 경우 이 옵션을 기반으로 Auto Scale Manager는 해당 위협 대응 가상 인스턴스를 유지하거나 삭제할지 결정합니다. (예: 결함 위협 대응 가상 삭제 / 아니요: management center에 등록하지 못하더라도 위협 대응 가상 인스턴스를 유지합니다.)

- Function 앱 설정에서는 Azure 구독에 대한 액세스 권한이 있는 사용자가 모든 변수('password'와 같은 보안 문자열을 포함하는 변수 포함)를 일반 텍스트 형식으로 볼 수 있습니다.

  사용자가 이에 대해 보안 문제가 있는 경우(예: 조직 내에서 권한이 낮은 사용자 간에 Azure 구독이 공유되는 경우) 사용자는 Azure의 *Key Vault* 서비스를 사용하여 비밀번호를 보호할 수 있습니다. 이 기능이 구성되면 기능 설정에서 일반 텍스트 '비밀번호'를 제공하는 대신 비밀번호가 저장된 키 저장소에서 생성된 보안 식별자를 제공해야 합니다.

  참고 Azure 문서를 검색하여 애플리케이션 데이터를 보호하는 모범 사례를 찾습니다.

가상 시스템 확장 집합의 IAM 역할 구성

Azure IAM (Identity and Access Management)은 사용자 ID를 관리하고 제어하기 위해 Azure Security and Access Control의 일부로 사용됩니다. Azure 리소스의 관리되는 ID는 Azure Active Directory의 자동으로 관리되는 ID를 Azure 서비스에 제공합니다.

이를 통해 Function 앱은 명시적 인증 자격 증명 없이 VMSS(Virtual Machine Scale Sets)를 제어할 수 있습니다.

프로시저

단계 **1** Azure 포털에서 VMSS로 이동합니다.

단계 **2** 액세스 제어**(IAM)**를 클릭합니다.

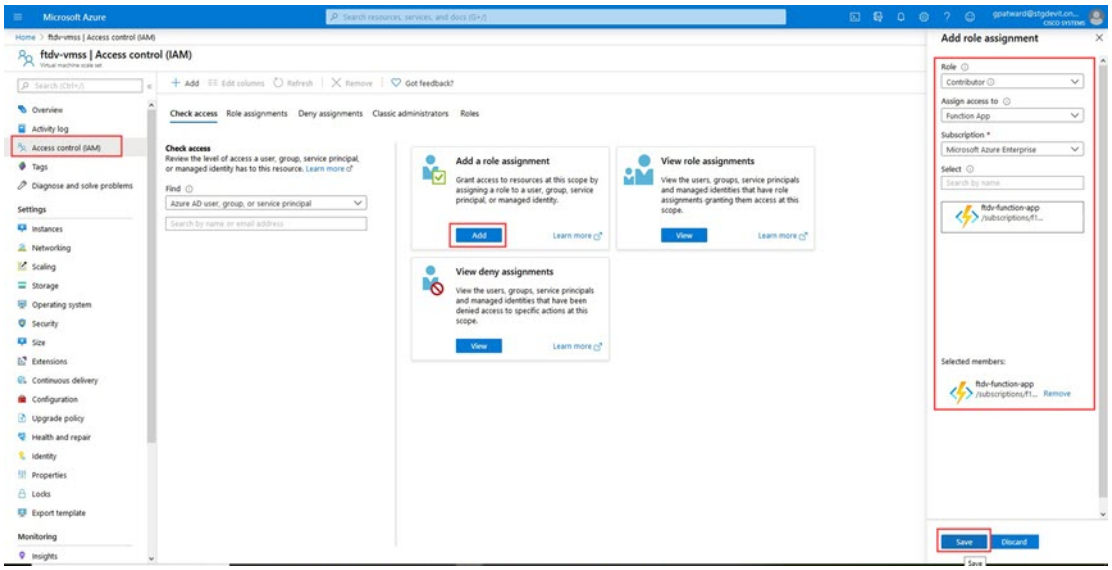
단계 **3** **Add(**추가**)**를 클릭하여 역할 할당을 추가합니다.

단계 **4** **Add role Assignment(**역할 할당 추가**)** 드롭 다운에서 **Contributor(**기여자**)**를 선택합니다.

단계 **5** **Assign access to(**액세스 할당 대상**)** 드롭 다운에서 **Function App(**기능 앱**)**을 선택합니다.

단계 **6** 위협 대응 가상 함수 애플리케이션을 선택합니다.

그림 ***20: AIM*** 역할 할당



단계 **7** **Save(**저장**)**를 클릭합니다.

참고 또한 아직 시작된 위협 대응 가상 인스턴스가 없는지 확인해야 합니다.

보안 그룹 업데이트

ARM 템플릿은 Management 인터페이스용과 데이터 인터페이스용의 두 가지 보안 그룹을 생성합니다. Management 보안 그룹은 위협 대응 가상 관리 활동에 필요한 트래픽만 허용합니다. 그러나 데이터 인터페이스 보안 그룹은 모든 트래픽을 허용합니다.

프로시저

구축의 토폴로지 및 애플리케이션 요구 사항에 따라 보안 그룹 규칙을 세부적으로 조정합니다.

참고 데이터 인터페이스 보안 그룹은 로드 밸런서의 최소 SSH 트래픽을 허용해야 합니다.

Azure Logic 앱 업데이트

Logic 앱은 Autoscale 기능의 오케스트레이터 역할을 합니다. ARM 템플릿은 기본 Logic 앱을 생성합니다. 그러면 Auto Scale 오케스트레이터로 작동하는 데 필요한 정보를 제공할 수 있도록 수동으로 업데이트해야 합니다.

프로시저

단계 **1** 리포지토리에서 *LogicApp.txt* 파일을 로컬 시스템으로 검색하고 아래 표시된 대로 수정합니다.

중요 계속하기 전에 이 단계를 모두 읽고 숙지하십시오.

이러한 수동 단계는 ARM 템플릿에서 자동화되지 않으므로 나중에 Logic 앱만 독립적으로 업그레이드 할 수 있습니다.

a) 필수: "SUBSCRIPTION_ID"의 모든 어커런스를 찾아서 구독 ID 정보로 교체합니다.
b) 필수: "RG_NAME" 어커런스를 모두 찾아서 리소스 그룹 이름으로 바꿉니다.
c) 필수: "FUNCTIONAPPNAME" 어커런스를 모두 찾아서 함수 앱 이름으로 바꿉니다.

다음 예에서는 *LogicApp.txt* 파일에서 이러한 행 중 일부를 보여줍니다.

```
  "AutoScaleManager": {
      "inputs": {
          "function": {
              "id":
"/subscriptions/SUBSCRIPTION_ID/resourceGroups/RG_NAME/providers/Microsoft.Web/sites/FUNCTIONAPPNAME/functions/AutoScaleManager"

          }
.
.
                      },
                      "Deploy_Changes_to_FTD": {
                          "inputs": {
                              "body": "@body('AutoScaleManager')",
                              "function": {
                                  "id":
"/subscriptions/SUBSCRIPTION_ID/resourceGroups/RG_NAME/providers/Microsoft.Web/sites/FUNCTIONAPPNAME/functions/DeployConfiguration"

                              }
.
.
                      "DeviceDeRegister": {
                          "inputs": {
                              "body": "@body('AutoScaleManager')",
                              "function": {
                                  "id":
"/subscriptions/SUBSCRIPTION_ID/resourceGroups/RG_NAME/providers/Microsoft.Web/sites/FUNCTIONAPPNAME/functions/DeviceDeRegister"

                              }
                          },
                          "runAfter": {
                              "Delay_For_connection_Draining": [
```

d) (선택 사항) 트리거 간격을 수정하거나 기본값(5)을 유지합니다. 이는 Autoscale 기능이 주기적으로 트리거되는 시간 간격입니다. 다음 예는 *LogicApp.txt* 파일에서 이러한 행을 보여줍니다.

```
        "triggers": {
            "Recurrence": {
                "conditions": [],
                "inputs": {},
                "recurrence": {
                    "frequency": "Minute",
                    "interval": 5
```

```
},
```

e) (선택 사항) 드레인 시간을 수정하거나 기본값(5)을 유지합니다. 이는 축소(Scale-In) 작업 중에 디바이스를 삭제하기 전에 위협 대응 가상에서 기존 연결을 드레 이닝하는 시간 간격입니다. 다음 예는 *LogicApp.txt* 파일에서 이러한 행을 보여줍니다.

```
"actions": {
     "Branch_based_on_Scale-In_or_Scale-Out_condition": {
         "actions": {
             "Delay_For_connection_Draining": {
                 "inputs": {
                     "interval": {
                         "count": 5,
                         "unit": "Minute"
                     }
```

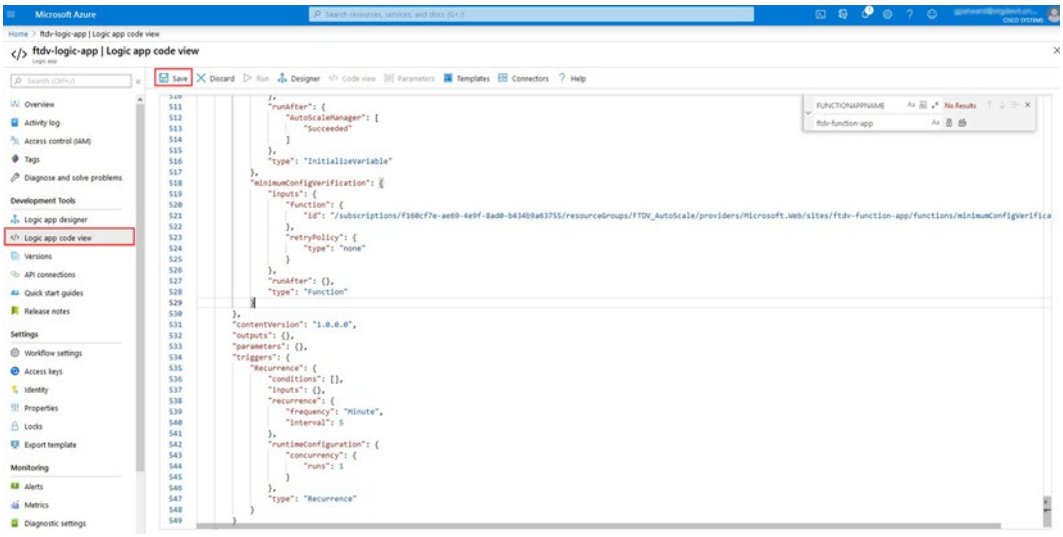
f) (선택 사항) 냉각 시간을 수정하거나 기본값(10)을 유지합니다. 이 시간은 확장(Scale-Out)이 완료된 후 작업 없음을 유지하는 시간입니다. 다음 예는 *LogicApp.txt* 파일에서 이러한 행을 보여줍니다.

```
"actions": {
    "Branch_based_on_Scale-Out_or_Invalid_condition": {
        "actions": {
            "Cooldown_time": {
                "inputs": {
                    "interval": {
                        "count": 10,
                        "unit": "Second"
                    }
```

참고 이러한 단계는 Azure 포털에서도 수행할 수 있습니다. 자세한 내용은 Azure 문서를 참조하십시오.

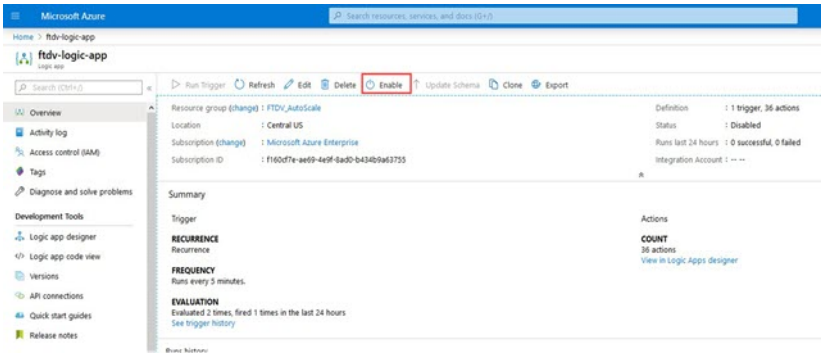
단계 **2** **Logic** 앱 코드 보기로 이동하여 기본 콘텐츠를 삭제하고 수정된 *LogicApp.txt* 파일에서 콘텐츠를 붙여넣고 **Save(**저장**)**을 클릭합니다.

그림 ***21: Logic*** 앱 코드 보기



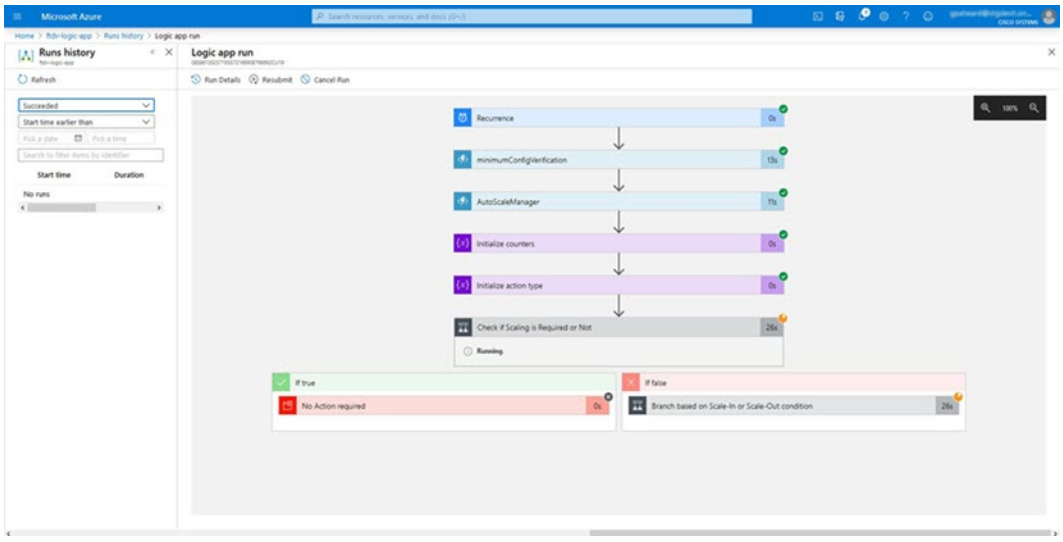
단계 **3** Logic 앱을 저장하면 '비활성화' 상태가 됩니다. Auto Scale Manager를 시작하려면 **Enable(**활성화**)**을 클릭합니다.

그림 ***22: Logic*** 앱 활성화



단계 **4** 활성화되면 작업이 실행되기 시작합니다. 활동을 보려면 '실행 중' 상태를 클릭하십시오.

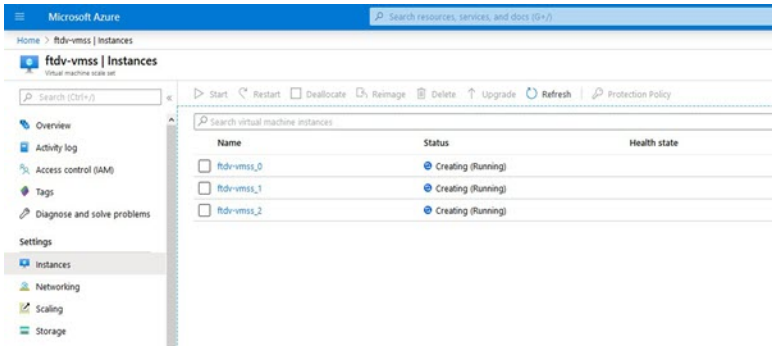
그림 *23: Logic* 앱 실행 상태



단계 **5** Logic 앱이 시작되면 모든 구축 관련 단계가 완료됩니다.

단계 **6** VMSS에서 위협 대응 가상 인스턴스가 생성되고 있는지 확인합니다.

그림 *24:* 실행 중인 *Threat Defense Virtual* 인스턴스



이 예에서는 ARM 템플릿 구축에서 'minFtdCount' 가 '3'으로, 'initDeploymentMode'가 'BULK'로 설정되었으므로 3개의 위협 대응 가상 인스턴스가 시작됩니다.

Threat Defense Virtual 업그레이드

위협 대응 가상 업그레이드는 VMSS(Virtual Machine Scale Set)의 이미지 업그레이드 형식으로만 지원됩니다. 따라서 Azure REST API 인터페이스를 통해 위협 대응 가상를 업그레이드합니다.

참고 모든 REST 클라이언트를 사용하여 위협 대응 가상를 업그레이드할 수 있습니다.

시작하기 전에

- 마켓플레이스에서 사용 가능한 새 위협 대응 가상 이미지 버전을 가져옵니다(예: 650.32.0).
- 원래 스케일 세트를 구축하는 데 사용된 SKU를 가져옵니다(예: ftdv -azure-byol).
- 리소스 그룹 및 가상 시스템 확장 집합 이름을 가져옵니다.

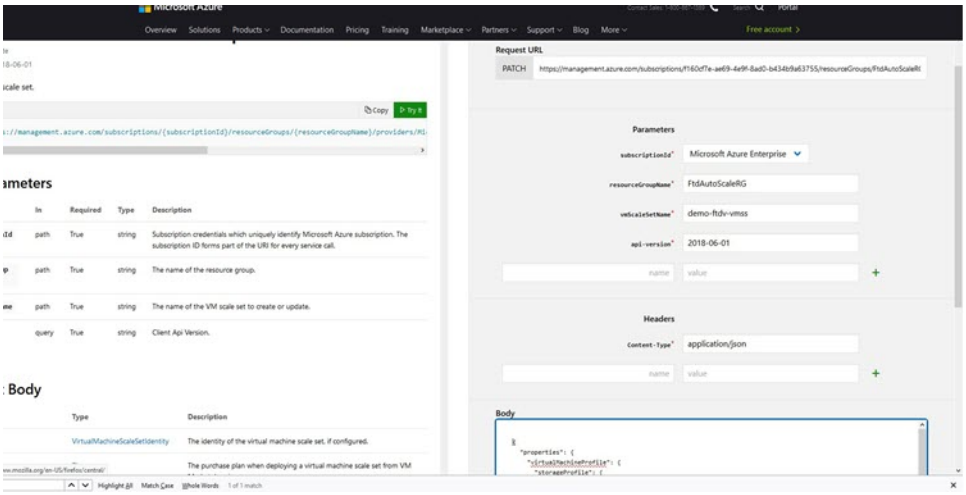
프로시저

단계 **1** 브라우저에서 다음 URL로 이동합니다.

https://docs.microsoft.com/en-us/rest/api/compute/virtualmachinescalesets/update#code-try-0

단계 **2** 매개변수 섹션에 세부 사항을 입력합니다.

그림 ***25: Threat Defense Virtual*** 업그레이드



단계 **3** 본문 섹션에 새로운 위협 대응 가상 이미지 버전, SKU 및 트리거 RUN을 포함하는 JSON 입력을 입력합니다.

```
{
 "properties": {
        "virtualMachineProfile": {
              "storageProfile": {
                     "imageReference": {
                          "publisher": "cisco",
                          "offer": "cisco-ftdv",
                          "sku": "ftdv-azure-byol",
                           "version": "650.32.0"
                     }
                },
            }
      }
}
```

단계 **4** Azure의 성공적인 응답은 VMSS가 변경 사항을 수락했음을 의미합니다.

새 위협 대응 가상 이미지는 새 인스턴스에서 사용되며, 이는 확장 작업의 일부로 시작됩니다.

- 기존 위협 대응 가상 인스턴스는 확장 집합에 있는 동안 기존 소프트웨어 이미지를 계속 사용합니다.
- 위의 동작을 재정의하고 기존 위협 대응 가상 인스턴스를 수동으로 업그레이드할 수 있습니다. 이렇게 하려면 VMSS에서 **Upgrade(**업그레이드**)** 버튼을 클릭합니다. 선택한 위협 대응 가상 인스턴스가 재부팅되고 업그레이드됩니다. 이러한 업그레이드된 위협 대응 가상 인스턴스를 수동으로 다시 등록하고 재구성해야 합니다. 이 방법은 권장되지 않습니다**.**

Auto Scale 논리

확장 메트릭

ARM 템플릿을 사용하여 threat defense virtual Auto Scale 솔루션에 필요한 리소스를 구축합니다. ARM 템플릿 구축 중에는 다음과 같은 확장 메트릭 옵션이 제공됩니다.

- CPU
- CPU, 메모리(버전 6.7 이상)

참고 CPU 메트릭은 Azure에서 수집되며 메모리 메트릭은 management center에서 수집됩니다.

확장 논리

- **POLICY-1**: 어떤 경우든 위협 대응 가상 평균로드가 구성된 기간 동안 확장 임계값을 초과하면 확장(Scale-Out)이 트리거됩니다. 'CPU, 메모리' 확장 메트릭을 사용하는 경우 확장 임계값은 확장 집합에 있는 모든 threat defense virtual의 평균 CPU 또는 메모리 사용률입니다.
- **POLICY-2**: 구성된 기간 동안 모든 위협 대응 가상 디바이스의 평균로드가 확장 임계값을 초과하면 확장(Scale-Out)이 트리거됩니다. 'CPU, 메모리' 확장 메트릭을 사용하는 경우 확장 임계값은 확장 집합에 있는 모든 threat defense virtual디바이스의 평균 CPU 또는 메모리 사용률입니다.

축소 논리

- 모든 위협 대응 가상 디바이스의 CPU 사용률이 구성된 기간 동안 구성된 축소 임계값 미만인 경우. 'CPU, 메모리' 확장 메트릭을 사용할 때 확장 집합의 모든 threat defense virtual 디바이스의 CPU 및 메모리 사용률이 구성된 기간 동안 구성된 축소 임계값 아래로 내려가면 CPU로드가 가장 적은 threat defense virtual가 종료되도록 선택됩니다.

참고

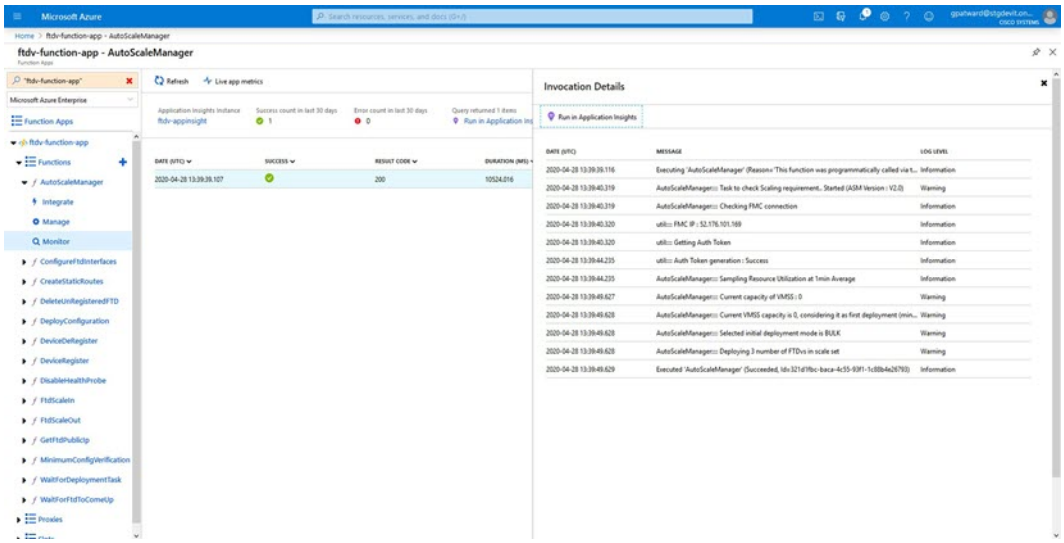
- 축소(Scale-In)/확장(Scale-Out)은 1단계로 수행됩니다(즉, 한 번에 1개 위협 대응 가상만 축소/확장).
- management center에서 수신한 메모리 사용량 메트릭은 시간 경과에 따라 계산된 평균 값이 아니라 순간 스냅 샷/샘플 값입니다. 따라서 메모리 메트릭만으로는 확장 결정을 내릴 수 없습니다. 구축 중에는 메모리 전용 메트릭을 사용할 수 있는 옵션이 없습니다.

Auto Scale 로깅 및 디버깅

서버리스 코드의 각 구성 요소에는 자체 로깅 메커니즘이 있습니다. 또한 로그는 애플리케이션 인사이트에 게시됩니다.

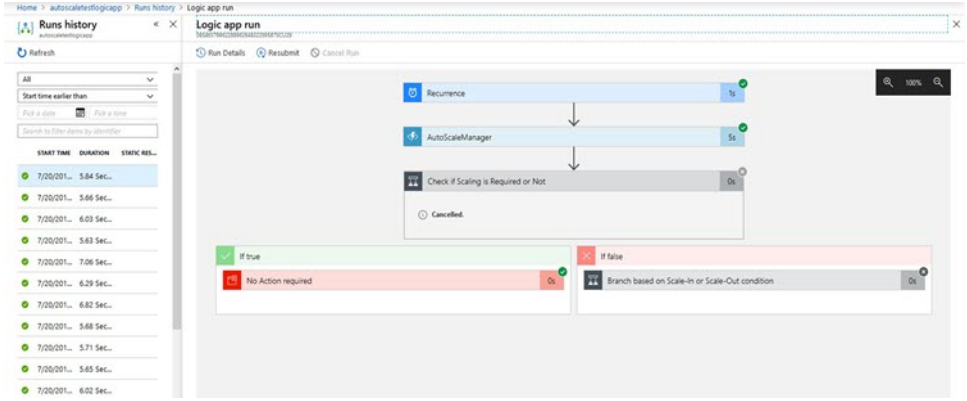
- 개별 Azure 함수의 로그를 볼 수 있습니다.

  그림 ***26: Azure Function*** 로그



- 각 Logic App 실행 및 해당 개별 구성 요소에 대한 유사한 로그를 볼 수 있습니다.

그림 ***27: Logic*** 앱 실행 로그



- 필요한 경우 Logic App에서 실행중인 작업을 언제든지 중지/종료할 수 있습니다. 그러나 현재 실행 중이거나 종료되는 위협 대응 가상 디바이스는 일관성이 없는 상태로 유지됩니다.
- 각 실행/개별 작업에 소요되는 시간은 Logic 앱에서 확인할 수 있습니다.
- 언제든지 새 zip을 업로드하여 Function 앱을 업그레이드할 수 있습니다. Function 앱을 업그레이드하기 전에 Logic 앱을 중지하고 모든 작업이 완료될 때까지 기다립니다.

Auto Scale 지침 및 제한 사항

위협 대응 가상 Auto Scale for Azure를 구축할 때 다음 지침 및 제한 사항에 유의하십시오.

- (버전 6.6 이하) 확장 결정은 CPU 사용률을 기반으로 합니다.
- (버전 6.7 이상) 확장 결정에서는 CPU 전용 사용률 또는 CPU 및 메모리 사용률을 사용할 수 있습니다.
- Management Center 관리가 필요합니다. Device Manager는 지원되지 않습니다.
- management center에는 공용 IP 주소가 있어야 합니다.
- 위협 대응 가상 Management 인터페이스가 공용 IP 주소를 갖도록 구성되었습니다.
- IPv4만 지원됩니다.
- Threat Defense Virtual Auto Scale for Azure는 액세스 정책, NAT 정책, 플랫폼 설정 등 디바이스 그룹에 적용되며 확장된 threat defense virtual 인스턴스에 전파되는 설정만을 지원합니다. management center을 사용한 디바이스 그룹 설정만을 수정할 수 있습니다. 디바이스별 컨피그레이션은 지원되지 않습니다.
- ARM 템플릿은 입력 검증 기능이 제한되어 있으므로 올바른 입력 검증을 제공하는 것은 사용자의 책임입니다.
- Azure 관리자는 Function 앱 환경 내에서 민감한 데이터(예: 관리자 로그인 자격 증명 및 비밀번호)를 일반 텍스트 형식으로 볼 수 있습니다. *Azure Key Vault* 서비스를 사용하여 민감한 데이터를 보호할 수 있습니다.

Auto Scale 문제 해결

다음은 일반적인 오류 시나리오 및 위협 대응 가상 Auto Scale for Azure에 대한 디버깅 팁입니다.

- management center에 연결 실패: management center IP / 자격 증명을 확인하십시오. management center에 결함이 있거나 연결할 수 없는지 확인합니다.
- 위협 대응 가상로 SSH할 수 없음 : 템플릿을 통해 복잡한 비밀번호가 위협 대응 가상에 전달되는지 확인합니다. 보안 그룹에서 SSH 연결을 허용하는지 확인하십시오.
- 로드 밸런서 상태 확인 실패: 위협 대응 가상에서 데이터 인터페이스의 SSH에 응답하는지 확인합니다. 보안 그룹 설정을 확인합니다.
- 트래픽 문제: 로드 밸런서 규칙, NAT 규칙 / 위협 대응 가상에 구성된 고정 경로를 확인합니다. 템플릿 및 보안 그룹 규칙에 제공된 Azure 가상 네트워크 / 서브넷 / 게이트웨이 세부 정보를 확인합니다.
- threat defense virtual가 management center에 등록 실패: 새 threat defense virtual 디바이스를 수용할 수 있도록 management center 용량을 확인하십시오. 라이선싱을 확인합니다. threat defense virtual 버전 호환성을 확인하십시오.
- Logic 앱이 VMSS에 액세스하지 못함: VMSS의 IAM 역할 컨피그레이션이 올바른지 확인하십시오.
- Logic 앱이 매우 오랫동안 실행 됨: 확장된 위협 대응 가상 디바이스에서 SSH 액세스를 확인합니다. management center에서 디바이스 등록 문제를 확인합니다. Azure VMSS에서 위협 대응 가상 디바이스의 상태를 확인합니다.
- 구독 ID와 관련된 오류 발생 Azure Function: 계정에서 기본 구독이 선택되었는지 확인하십시오.
- 축소(Scale-In) 작업 실패: 경우에 따라 Azure에서 인스턴스를 삭제하는 데 시간이 오래 걸리는 경우가 있습니다. 이러한 상황에서는 축소 작업이 시간 초과되고 오류를 보고할 수 있지만 결국엔 인스턴스가 삭제됩니다.
- 컨피그레이션 변경을 수행하기 전에 논리 애플리케이션을 비활성화하고 실행중인 모든 작업이 완료될 때까지 기다리십시오.

소스 코드로 Azure 기능 빌드

시스템 요구 사항

- Microsoft Windows 데스크톱 / 노트북
- Visual Studio(Visual Studio 2019 버전 16.1.3에서 테스트)

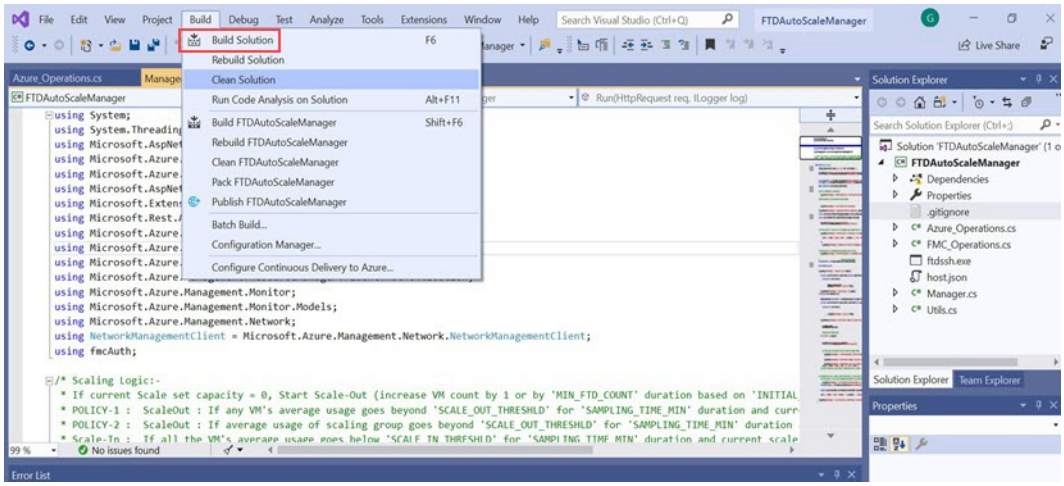
참고 Azure 함수는 C#을 사용하여 작성됩니다.

- "Azure 개발" 워크로드를 Visual Studio에 설치해야 합니다.

Visual Studio로 빌드

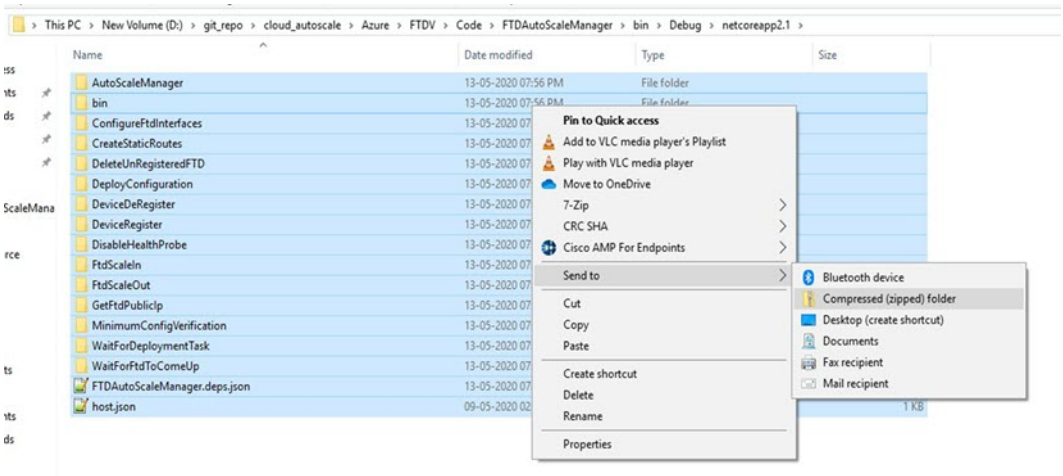
1. 'code' 폴더를 로컬 시스템에 다운로드합니다.
2. 'FTDAutoScaleManager '폴더로 이동합니다.
3. Visual Studio에서 'FTDAutoScaleManager ' 프로젝트 파일을 엽니다.
4. Visual Studio 표준 절차를 사용하여 정리 및 빌드합니다.

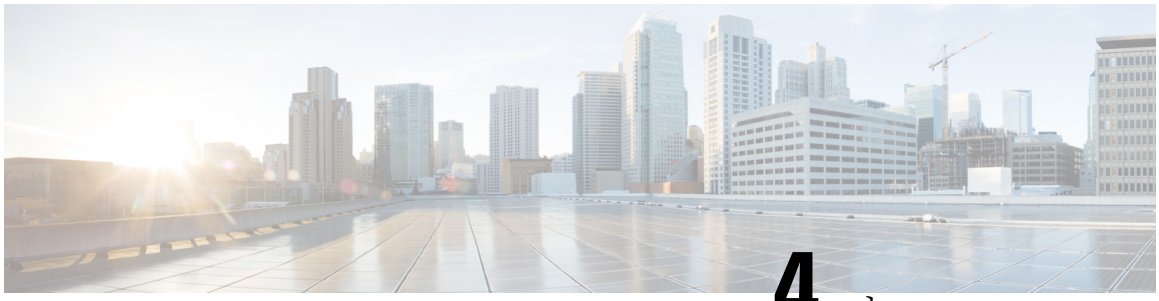
그림 ***28: Visual Studio*** 빌드



5. 빌드가 성공적으로 컴파일되면 **\bin\Release\netcoreapp2.1** 폴더로 이동합니다.
6. 모든 내용을 선택하고 **Send to** > **Compressed(zipped)(**압축 폴더로 전송**)**을 클릭하고 ZIP 파일을 *ASM_Function.zip*으로 저장합니다.

그림 ***29: Build ASM_Function.zip***





4 장

Threat Defense Virtual 이미지 스냅샷

Azure 포털에서 스냅샷 이미지를 사용하여 threat defense virtual를 생성하고 구축할 수 있습니다. 이미지 스냅샷은 상태 데이터가 없는 복제된 threat defense virtual 이미지 인스턴스입니다.

Threat Defense Virtual 이미지 스냅샷

Azure 포털에서 스냅샷 이미지를 사용하여 threat defense virtual를 생성하고 구축할 수 있습니다. 이미지 스냅샷은 상태 데이터가 없는 복제된 threat defense virtual 이미지 인스턴스입니다.

Threat Defense Virtual 스냅샷 개요

threat defense virtual 인스턴스의 스냅샷 이미지를 생성하는 프로세스는 threat defense virtual 및 FSIC에 대해 수행되는 첫 번째 부팅 절차를 건너뛰어 초기 시스템 초기화 시간을 최소화하는 데 도움이 됩니다. 스냅샷 이미지는 미리 채워진 데이터베이스 및 threat defense virtual 초기 부팅 프로세스로 구성되며, 이를 통해 이미지는 management center 또는 다른 관리 센터의 시스템 ID와 관련된 고유 ID(UUID, 일련 번호)를 다시 생성할 수 있습니다. 이 프로세스는 threat defense virtual의 부팅 시간을 단축하는 데 도움이 되며, 이는 자동 확장 구축에서 필수적입니다.

관리되는 이미지에서 Threat Defense Virtual 스냅샷 이미지 생성

Threat Defense Virtual 이미지 스냅샷 생성은 Azure 포털에서 threat defense virtual 인스턴스의 기존 관리 이미지를 복제하는 프로세스입니다.

Before you begin

Azure 포털에서 Linux VM의 Azure 스토리지 계정에 있는 컨테이너에 크기가 조정된 VHD 이미지를 업로드하여 threat defense virtual 버전 7.2 이상의 관리되는 이미지를 생성해야 합니다. 크기가 조정된 VHD 이미지를 생성하는 방법에 대한 자세한 내용은 VHD 및 리소스 템플릿을 사용하여 Azure에서 구축을 참고하십시오.

이미지 스냅샷을 준비 중인 threat defense virtual 인스턴스를 management center 또는 device manager 같은 관리자에 등록해서는 안 됩니다.

Procedure

단계 1 threat defense virtual 인스턴스의 관리되는 이미지를 생성한 Azure 포털로 이동합니다.

Note 복제하려는 threat defense virtual 인스턴스가 management center에 등록되거나 다른 로컬 관리자에 구성되지 않았는지 또는 어떤 구성과도 적용되지 않았는지 확인합니다.

단계 2 **Resource Group(**리소스 그룹**)**으로 이동하여 threat defense virtual 인스턴스를 선택합니다.

단계 3 threat defense virtual 인스턴스의 탐색 페이지에서 **Serial Console(**시리얼 콘솔**)**을 클릭합니다.

단계 4 다음 스크립트를 사용하여 전문가 셸에서 사전 스냅샷 프로세스를 실행합니다.

```
> expert
admin@FTDvbaseimg:~$ Sudo su
root@firepower:/ngfw/var/common# prepare_snapshot
Do you want to continue [Y/N]:
```

스크립트에서 `prepare_snapshot` 명령을 사용하는 경우 스크립트를 실행할지 확인하는 중간 메시지가 나타납니다. **Y**를 눌러 스크립트를 실행합니다.

또는 `root@firepower:/ngfw/var/common# prepare_snapshot -f`와 같이 이 명령에 `-f`를 추가하여 사용자 확인 메시지를 건너뛰고 스크립트를 직접 실행할 수 있습니다.

이 스크립트는 모든 라인 컨피그레이션, 구축된 정책, 구성된 관리자, threat defense virtual 인스턴스와 연결된 UUID를 제거합니다. 처리가 완료되면 threat defense virtual 인스턴스가 종료됩니다.

단계 5 **Capture(**캡처**)**를 클릭합니다.

단계 6 **Create image(**이미지 생성**)** 페이지에서 기존 리소스 그룹을 선택하거나 **Resource Group(**리소스 그룹**)** 드롭다운 목록에서 새 리소스 그룹을 생성합니다.

단계 7 관리되는 이미지만 생성하려면 **Instance Details(**인스턴스 세부 정보**)** 섹션에서 **No, capture only a managed image(**아니요, 관리되는 이미지만 캡처**)**를 클릭합니다.

단계 8 threat defense virtual 인스턴스의 관리되는 이미지를 사용하여 생성하는 스냅샷 이미지의 이름을 제공합니다.

단계 9 **Review+Create(**검토+생성**)**를 클릭하여 threat defense virtual 인스턴스의 새 스냅샷 이미지를 생성합니다.

What to do next

스냅샷 이미지를 사용하여 threat defense virtual 인스턴스를 구축합니다. 스냅샷 이미지를 사용하여 Threat Defense Virtual 인스턴스 구축을 참조하십시오.

스냅샷 이미지를 사용하여 Threat Defense Virtual 인스턴스 구축

Before you begin

다음 작업을 수행하는 것이 좋습니다.

- threat defense virtual 인스턴스에 대해 스냅샷 이미지를 사용할 수 있는지 확인합니다.

Procedure

단계 **1** Azure 포털에 로그인합니다.

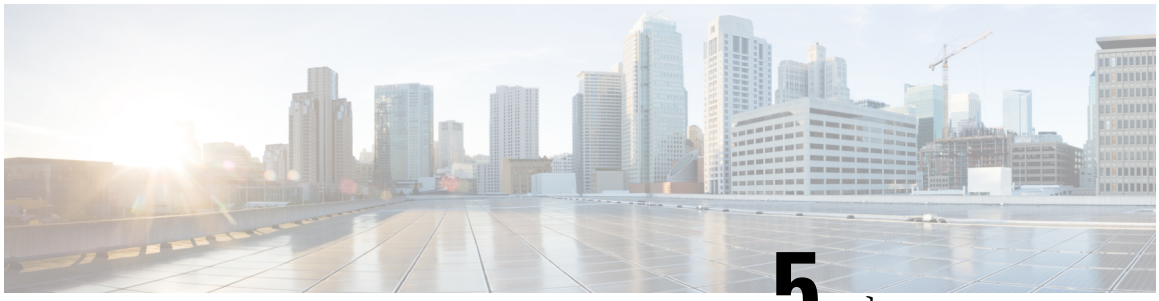
단계 **2** 새로 생성한 스냅샷 이미지의 리소스 ID를 복사합니다.

Note Azure는 모든 리소스(스냅샷 이미지)를 리소스 ID에 연결합니다. 새 threat defense virtual 인스턴스를 구축하려면 스냅샷 이미지의 리소스 ID가 필요합니다.

a) Azure Portal에서 **Images(**이미지**)**를 선택합니다.
b) 관리되는 이미지를 사용하여 생성한 스냅샷 이미지를 선택합니다.
c) 이미지 속성을 보려면 **Overview(**개요**)**를 클릭합니다.
d) 리소스 **ID**를 클릭 보드에 복사합니다. 리소스 **ID**의 구문은 다음과 같습니다: **/subscriptions/<subscription-id>/resourceGroups/<resourceGroup>/providers/Microsoft.Compute/<container>/<vhdname>**

단계 **3** 스냅샷 이미지를 사용하여 threat defense virtual 인스턴스를 계속 구축합니다. VHD 및 리소스 템플릿을 사용해서 Azure에서 구축을 참고하십시오.

Note threat defense virtual 콘솔에서 CLI 명령 **show version** 및 **show snapshot detail**을 실행하여 새로 구축된 threat defense virtual 인스턴스의 버전 및 세부 정보를 확인할 수 있습니다.



5 장

보안 방화벽 관리 센터로 Secure Firewall Threat Defense Virtual 관리

이 장에서는 management center로 관리되는 독립형 threat defense virtual 디바이스를 구축하는 방법을 설명합니다.

참고 이 문서에서는 최신 threat defense virtual 버전의 기능 이전 버전의 소프트웨어를 사용할 경우에는 해당 버전에 대한 management center 설정 가이드의 절차를 참조하십시오.

보안 방화벽 관리 센터를 사용하는 Secure Firewall Threat Defense Virtual 정보

Secure Firewall Threat Defense Virtual은(는) Cisco NGFW 솔루션의 가상화된 구성 요소입니다. threat defense virtual은 스테이트풀 방화벽, 라우팅, NGIPS(Next-Generation Intrusion Prevention System), AVC(Application Visibility and Control), URL 필터링, 악성코드 디펜스와 같은 차세대 방화벽 서비스를 제공합니다.

전체 기능을 갖춘 별도 서버의 다중 디바이스 관리자인 management center을 사용해 threat defense virtual을 관리할 수 있습니다. management center 설치에 대한 자세한 내용은 Cisco Firepower Management Center 1600, 2600 및 4600 하드웨어 설치 가이드를 참고하십시오.

threat defense virtual은 threat defense virtual 장비에 할당한 관리 인터페이스의 management center로 등록 및 통신합니다.

문제 해결을 위해 관리 인터페이스에서 SSH를 사용해 threat defense CLI에 액세스하거나, management center CLI에서 threat defense에 연결할 수 있습니다.

보안 방화벽 관리 센터에 로그인

management center을 사용해 threat defense를 구성하고 모니터링합니다.

시작하기 전에

지원되는 브라우저에 대한 자세한 내용은 사용 중인 버전의 릴리스 노트를 참조하십시오 (https://www.cisco.com/go/firepower-notes 참조).

프로시저

단계 **1** 지원되는 브라우저를 사용해 다음 URL을 입력합니다.

https://*fmcv_ip_address*

*fmc_ip_address*는 management center의 IP 주소 또는 호스트 이름을 식별합니다.

참고 https://[fmcv_ipv6_public_address] IPv6에 지정

단계 **2** 사용자 이름 및 비밀번호를 입력합니다.

단계 **3** **Log In(**로그인**)**을 클릭합니다.

디바이스를 보안 방화벽 관리 센터에 등록

시작하기 전에

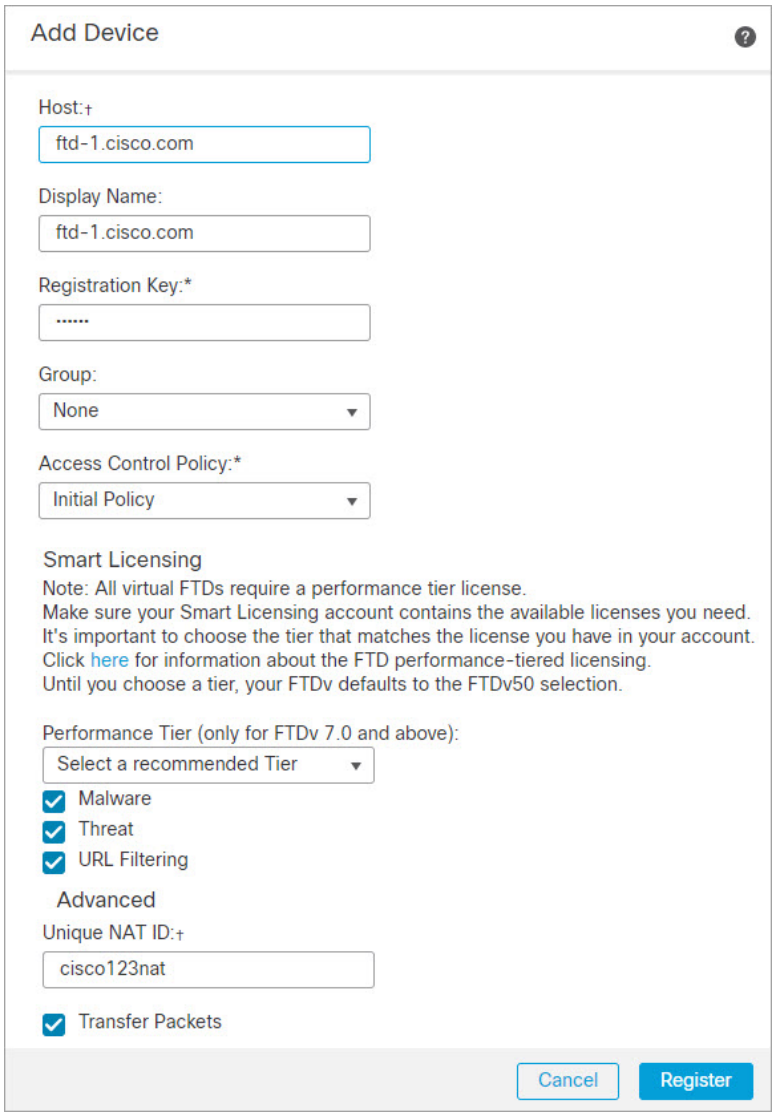
threat defense virtual 머신이 성공적으로 구축되었으며, 전원이 켜져 있고 첫 번째 부팅 절차를 완료했는지 확인하십시오.

참고 이 절차는 day0/부트스트랩을 통해서 management center에 대한 등록 정보가 제공된 것으로 가정합니다. 그러나 이러한 모든 설정은 **configure network(**네트워크 구성**)** 명령을 사용하여 CLI에서 나중에 변경할 수 있습니다. Secure Firewall Threat Defense 명령 참조를 참조하십시오.

프로시저

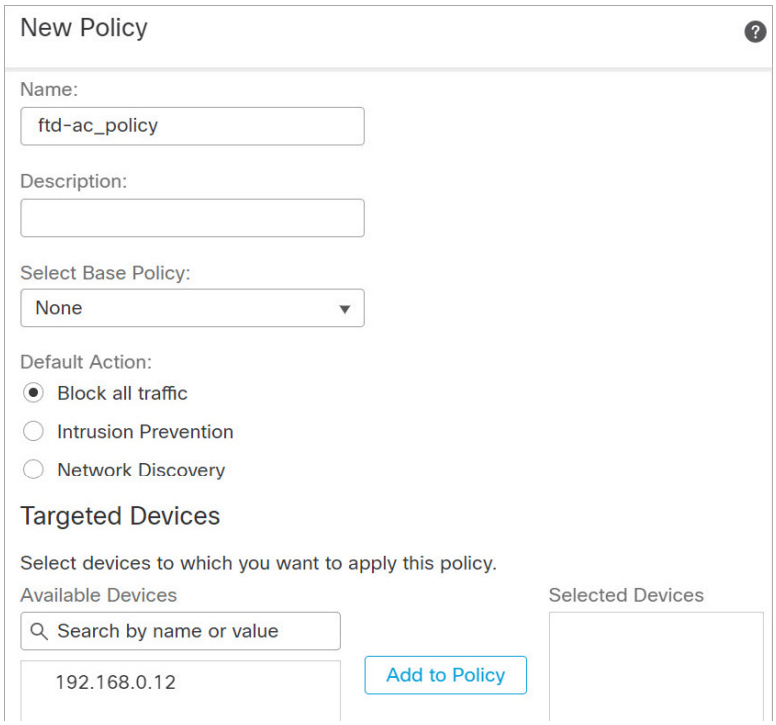
단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택합니다.

단계 **2** **Add(**추가**)** 드롭다운 목록에서 **Add device(**디바이스 추가**)**를 선택하고 다음 매개변수를 입력합니다.



- **Host(**호스트**)**—추가할 디바이스의 IP 주소(IPv4 및 IPv6)를 입력합니다. IPv6 활성화 설정의 경우 호스트 이름에 Ipv4 또는 Ipv6을 포함할 수 있습니다.
- **Display Name(**표시 이름**)**—management center에 표시하고자 하는 디바이스 이름을 입력합니다.
- **Registration key(**등록 키**)** - threat defense virtual 부트스트랩 구성에서 지정한 것과 동일한 등록 키를 입력합니다.
- **Domain(**도메인**)** - 멀티 도메인 환경이 있는 경우 리프 도메인에 디바이스를 할당합니다.
- **Group(**그룹**)** - 그룹을 사용하는 경우 디바이스 그룹에 할당합니다.
- **Access Control Policy(**액세스 제어 정책**)** - 초기 정책을 선택합니다. 사용해야 하는 맞춤형 정책이 이미 있는 경우가 아니라면 **Create new policy(**새 정책 생성**)**, **Block all traffic(**모든 트래픽 차

단)을 선택합니다. 나중에 트래픽을 허용하도록 변경할 수 있습니다. 액세스 제어 구성, 81 페이지을 참조하십시오.



- **Smart license (**스마트 라이선싱**)** - 구축하려는 기능에 필요한 스마트 라이선스(악성코드 디펜스 검사를 사용하려는 경우 **Malware(**악성코드**)**, 침입 방지를 사용하려는 경우 **Threat(**위협**)**, 카테고리 기반 URL 필터링을 구현하려는 경우 **URL**)를 할당합니다.
- **Unique NAT ID(**고유 **NAT ID)** - threat defense virtual 부트스트랩 구성에서 지정한 NAT ID를 지정합니다.
- **Transfer Packets(**패킷 전송**)** - 디바이스가 management center에 패킷을 전송하도록 허용합니다. 이 옵션이 활성화되어 IPS 또는 Snort 같은 이벤트가 트리거되면 디바이스는 검사를 위해 이벤트 메타데이터 정보 및 패킷 데이터를 management center에 전송합니다. 비활성화하면 management center에 이벤트 정보만 전송하고 패킷 데이터는 전송하지 않습니다.

단계 **3** **Register(**등록**)**를 클릭하여 성공적인 등록을 확인합니다.

등록에 성공하면 디바이스가 목록에 추가됩니다. 오류가 발생하면 오류 메시지가 표시됩니다. threat defense virtual 등록에 실패하면 다음 항목을 확인하십시오.

- Ping - 다음 명령을 사용해 threat defense CLI(Secure Firewall Threat Defense CLI에 액세스, 83 페이지)에 액세스하고 management center IP 주소에 Ping을 보냅니다.

  ping system *ip_address*

  Ping이 실패하는 경우 **show network** 명령을 사용해 네트워크 설정을 확인합니다. threat defense IP 주소를 변경해야 하는 경우 **configure network** {**ipv4** | **ipv6**} **manual or DHCP** 명령을 사용합니다.

- NTP - NTP 서버가 **System(**시스템**)** > **Configuration(**설정**)** > **Time Synchronization(**시간 동기화**)** 페이지에서 설정한 management center 서버와 일치하는지 확인합니다.
- 등록 키, NAT ID 및 management center IP 주소 - 두 디바이스에서 동일한 등록 키 및 NAT ID가 사용되고 있는지 확인합니다. **configure manager add DONTRESOLVE<registrationkey> <NATID>** 명령을 사용해 threat defense virtual에서 등록 키 및 NAT ID를 설정할 수 있습니다. 이 명령을 사용해 management center IP 주소를 변경할 수도 있습니다.

기본 보안 정책 구성

이 섹션에서는 다음 설정을 사용해 기본 보안 정책을 구성하는 방법에 대해 설명합니다.

- 내부 및 외부 인터페이스 - 내부 인터페이스에 고정 IP 주소를 할당하고, 외부 인터페이스에 DHCP를 사용합니다.
- DHCP Server(DHCP 서버) - 클라이언트용 내부 인터페이스에서 DHCP 서버를 사용합니다.
- Default route(기본 경로) - 외부 인터페이스를 통해 기본 경로를 추가합니다.
- NAT - 외부 인터페이스에서 인터페이스 PAT를 사용합니다.
- Access control(액세스 제어) - 내부에서 외부로 향하는 트래픽을 허용합니다.

프로시저

단계 **1** 인터페이스 구성, 71 페이지
단계 **2** DHCP 서버 구성, 75 페이지
단계 **3** 기본 경로 추가, 76 페이지
단계 **4** NAT 구성, 78 페이지
단계 **5** 액세스 제어 구성, 81 페이지
단계 **6** 구성 구축, 82 페이지

인터페이스 구성

threat defense virtual 인터페이스를 활성화하고, 보안 영역에 이를 할당하며, IP 주소를 설정합니다. 일반적으로 시스템이 의미 있는 트래픽을 전달하도록 최소 2개 이상의 인터페이스를 구성해야 합니다. 일반적으로 업스트림 라우터 또는 인터넷과 만나는 외부 인터페이스와 조직 네트워크에서 사용하는 하나 이상의 내부 인터페이스를 사용합니다. 이런 인터페이스의 일부는 웹 서버와 같이 공개적으로 액세스할 수 있는 에셋을 배치하는 '비무장지대(DMZ)'로 사용하게 됩니다.

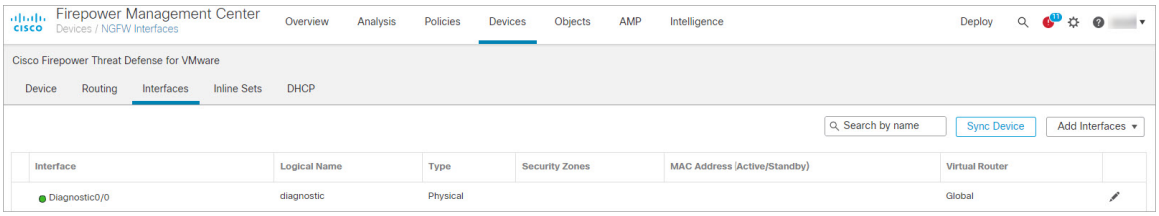
일반적인 에지 라우팅 상황의 경우, 내부 인터페이스에서 정적 주소를 정의하는 반면 ISP에서 온 DHCP를 통해 외부 인터페이스 주소를 가져옵니다.

다음 예에서는 DHCP를 사용하는 외부 인터페이스에서 고정 주소 및 라우팅 모드를 사용하여 인터페이스 내부에 라우팅 모드를 구성합니다.

프로시저

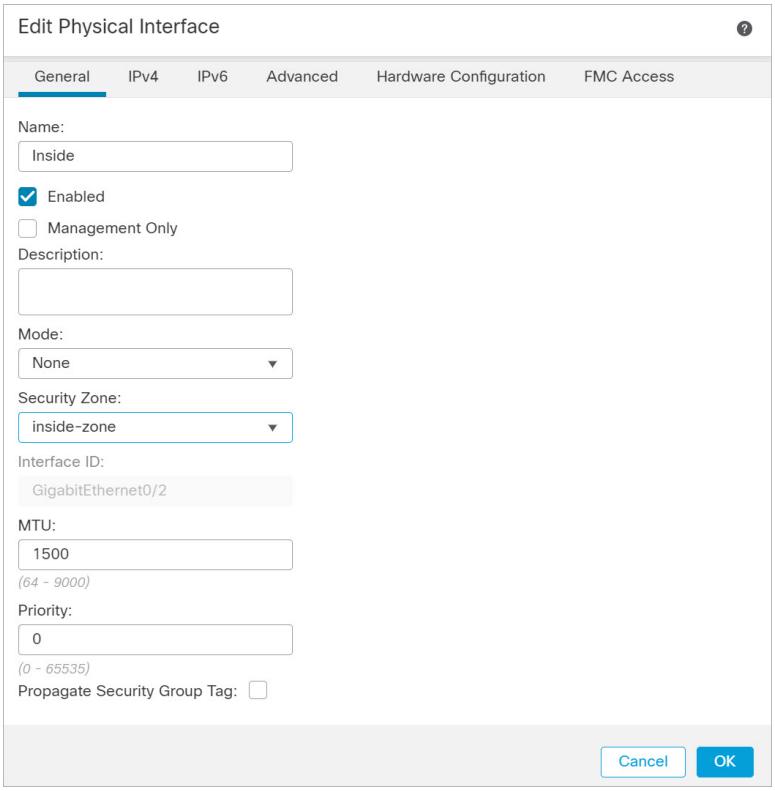
단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 디바이스의 수정( )을 클릭합니다.

단계 **2** **Interfaces(**인터페이스**)**를 클릭합니다.



단계 **3** 내부에 사용할 인터페이스의 수정( )를 클릭합니다.

General(일반**)** 탭이 표시됩니다.



a) **Name(**이름**)** 필드에 이름을 48자 이내로 입력합니다.

예를 들어 인터페이스에 **inside**라는 이름을 지정합니다.

b) **Enable(**활성화**)** 확인란을 선택합니다.

c) **Mode(**모드**)**는 **None(**없음**)** 상태로 남겨둡니다.

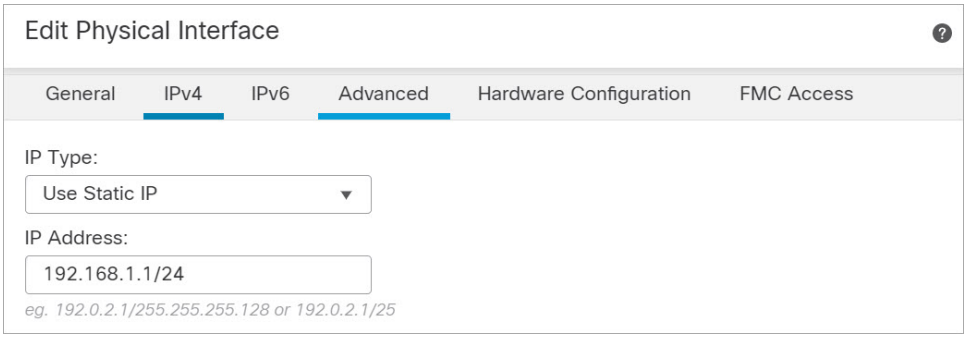
d) **Security Zone(**보안 영역**)** 드롭다운 목록에서 기존의 내부 보안 영역을 선택하거나 **New(**새로 만들기**)**를 클릭하여 새 보안 영역을 추가합니다.

예를 들어 **inside_zone**이라는 영역을 추가합니다. 각 인터페이스는 보안 영역 및/또는 인터페이스 그룹에 할당되어야 합니다. 인터페이스는 하나의 보안 영역에만 속할 수 있지만, 여러 인터페이스 그룹에 속할 수도 있습니다. 영역 또는 그룹을 기준으로 보안 정책을 적용합니다. 예를 들어 내부 인터페이스는 내부 영역에, 외부 인터페이스는 외부 영역에 할당할 수 있습니다. 트래픽이 내부에서 외부로는 이동하지만 외부에서 내부로는 이동할 수 없도록 액세스 제어 정책을 구성할 수 있습니다. 대부분의 정책은 보안 영역만 지원합니다. NAT 정책, 사전 필터 정책, QoS 정책에서 영역이나 인터페이스 그룹을 사용할 수 있습니다.

e) **IPv4** 및/또는 **IPv6** 탭을 클릭 합니다.

- **IPv4**—드롭다운 목록에서 **Use Static IP(**고정 **IP** 사용**)**를 선택하고 슬래시(/) 표기 또는 DHCP 옵션으로 IP 주소와 서브넷 마스크를 입력합니다.

  예를 들어 **192.168.1.1/24** 를 입력합니다.

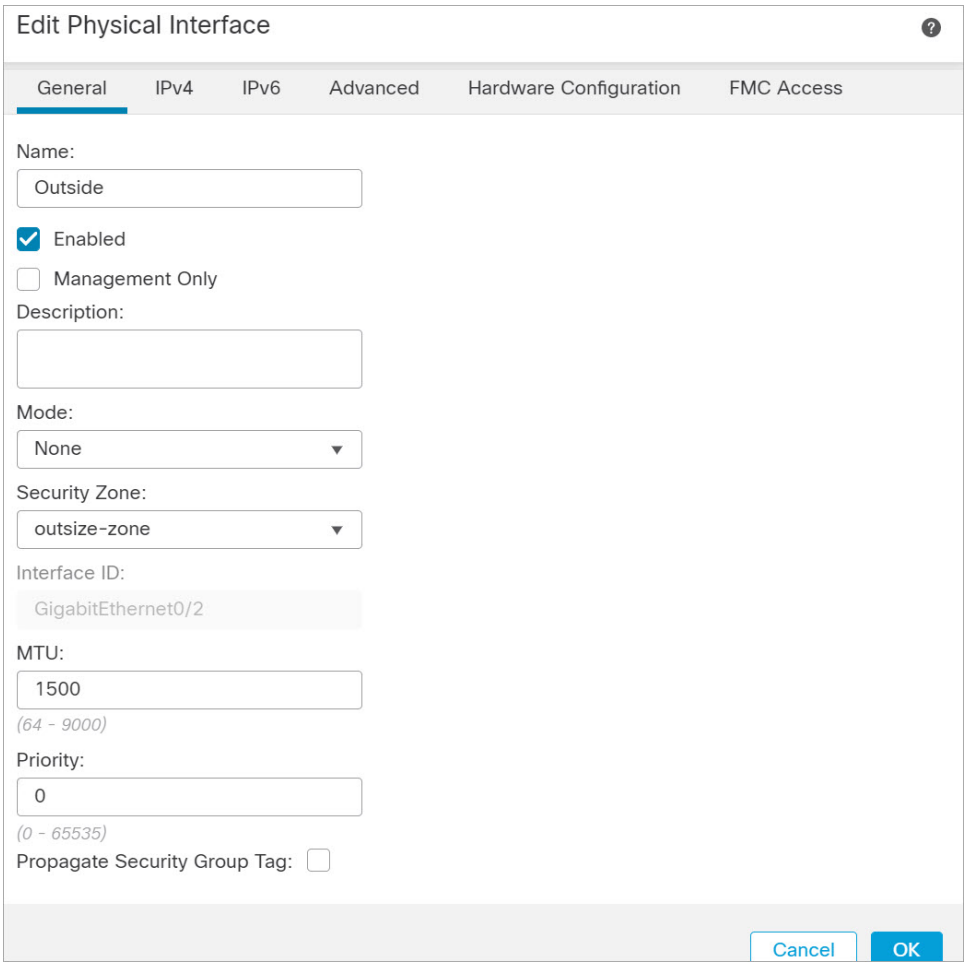


- **IPv6**—상태 비저장 자동 구성 및 IPv6 DHCP 또는 정적 구성의 경우 **Autoconfiguration(**자동 구성**)** 확인란을 선택하여 인터페이스를 활성화합니다.

f) **OK(**확인**)**를 클릭합니다.

단계 **4** 외부에서 사용하려는 인터페이스의 수정( )를 클릭합니다.

General(일반**)** 탭이 표시됩니다.



a) **Name(**이름**)** 필드에 이름을 48자 이내로 입력합니다.

예를 들어, 인터페이스에 **outside**라는 이름을 지정합니다.

b) **Enable(**활성화**)** 확인란을 선택합니다.

c) **Mode(**모드**)**는 **None(**없음**)** 상태로 남겨둡니다.

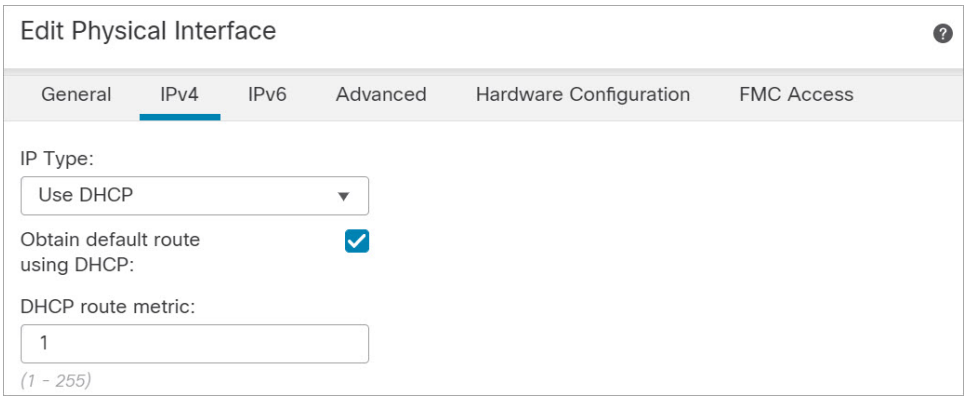
d) **Security Zone(**보안 영역**)** 드롭다운 목록에서 기존의 외부 보안 영역을 선택하거나 **New(**새로 만들기**)**를 클릭하여 새 보안 영역을 추가합니다.

예를 들어 **outside_zone**이라는 영역을 추가합니다.

e) **IPv4** 및/또는 **IPv6** 탭을 클릭 합니다.

참고 Google Cloud Platform의 VPC 네트워크는 IPv6를 지원하지 않습니다.

- **IPv4 - Use DHCP(DHCP** 사용**)**를 선택하여 다음 옵션 매개변수를 구성합니다.
  - **DHCP**에서 기본 경로 가져오기 - DHCP 서버에서 기본 경로를 가져옵니다.
  - **DHCP** 경로 메트릭 - 파악된 경로에 대해 1과 255 사이의 관리 거리를 할당합니다. 파악된 경로의 기본 관리 거리는 1입니다.



- **IPv6** - 상태 비저장 자동 구성을 하려면 **Autoconfiguration(**자동 구성**)** 확인란을 선택합니다.

f) **OK(**확인**)**를 클릭합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

DHCP 서버 구성

참고 AWS, Azure, GCP, OCI 등의 퍼블릭 클라우드 환경에 구축하는 경우 이 절차를 건너 뜁니다.

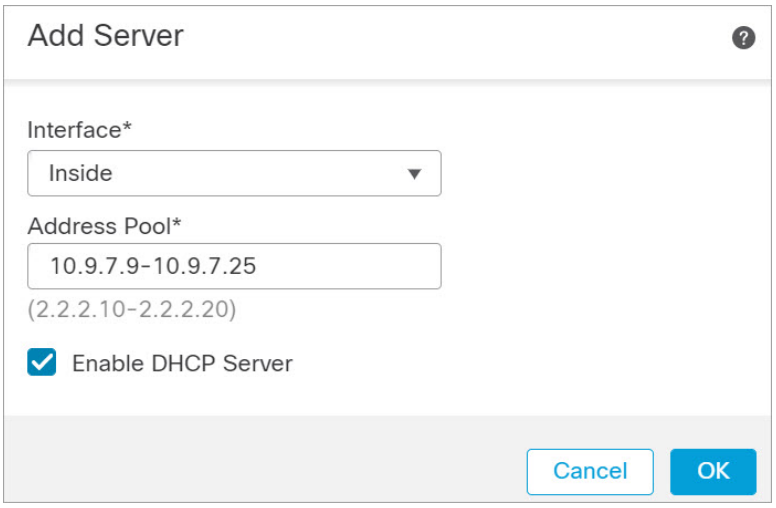
클라이언트가 DHCP를 사용하여 threat defense virtual에서 IP 주소를 가져오게 하려면 DHCP 서버를 활성화합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 디바이스의 수정( )을 클릭합니다.

단계 **2** **DHCP** > **DHCP Server(DHCP** 서버**)**를 선택합니다.

단계 **3** 서버 페이지에서 **Add(**추가**)**를 클릭하고 다음 옵션을 설정합니다.



- 인터페이스 - 드롭다운 목록에서 인터페이스를 선택합니다.
- **Address Pool(**주소 풀**)** - DHCP 서버에서 사용되는 최소 및 최대 IP 주소 범위를 설정합니다. 이 IP 주소 범위는 선택된 인터페이스와 동일한 서브넷에 있어야 하며, 인터페이스 자체의 IP 주소는 포함할 수 없습니다.
- **Enable DHCP Server(DHCP** 서버 활성화**)** - 선택한 인터페이스에서 DHCP 서버를 활성화합니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

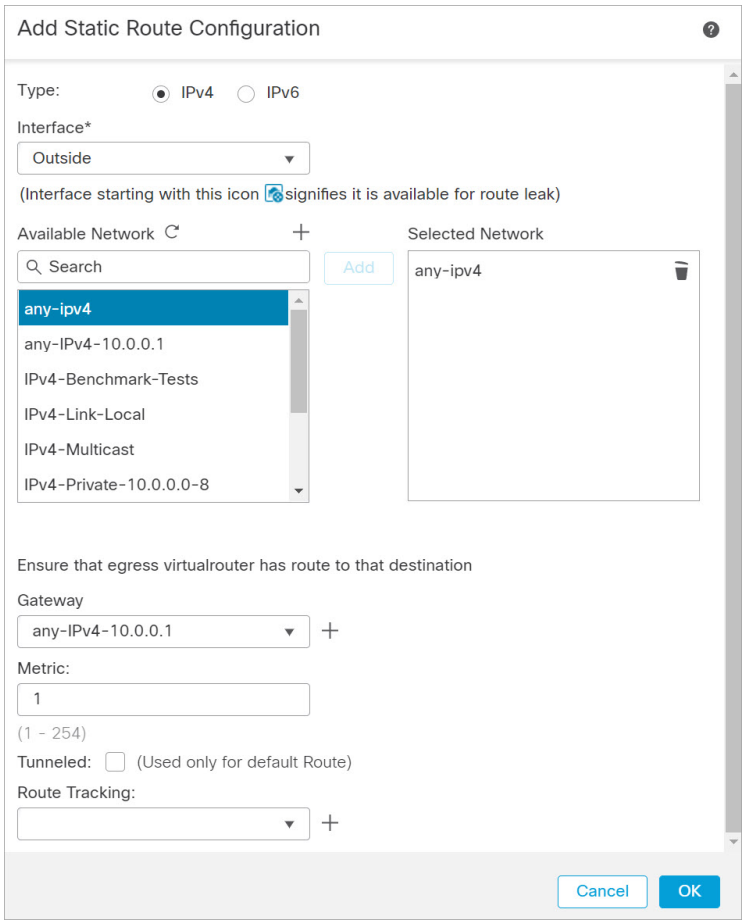
기본 경로 추가

기본 경로는 일반적으로 외부 인터페이스에서 접근 가능한 업스트림 라우터를 가리킵니다. 외부 인터페이스에 DHCP를 사용하는 경우 디바이스가 이미 기본 경로를 수신했을 수 있습니다. 수동으로 경로를 추가해야 하는 경우 이 절차를 완료합니다. DHCP 서버에서 기본 경로를 수신한 경우, **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Routing(**라우팅**)** > **Static Route(**정적 경로**)** 페이지의 **IPv4 Routes(IPv4** 경로**)** 또는 **IPv6 Routes(IPv6** 경로**)** 테이블에 표시됩니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 디바이스의 수정( )을 클릭합니다.

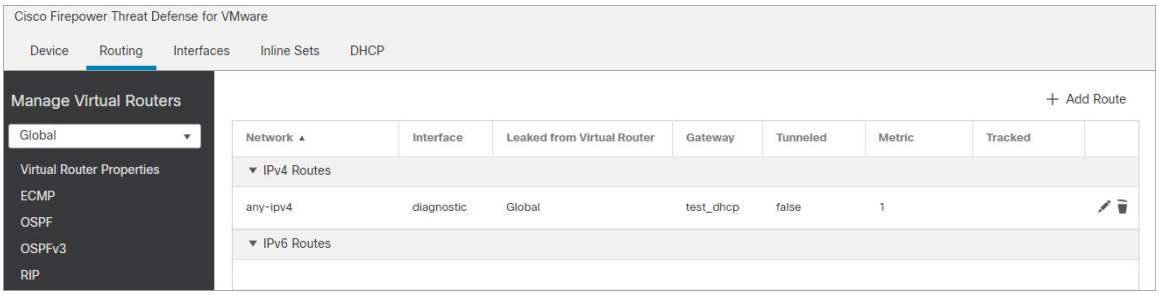
단계 **2** **Routing(**라우팅**)** > **Static Route(**정적 경로**)**를 선택하고 **Add Route(**경로 추가**)**를 클릭해 다음을 설정합니다.



- **Type(**유형**)** - 추가하려는 정적 경로 유형에 따라 **IPv4** 또는 **IPv6** 라디오 버튼을 클릭합니다.
- **Interface(**인터페이스**)** - 이그레스 인터페이스를 선택합니다. 일반적으로 외부 인터페이스입니다.
- **Available Network(**사용 가능한 네트워크**)** - IPv4 기본 경로에 대해 **any-ipv4**를 선택하거나, IPv6 기본 경로에 대해 **any-ipv6**를 선택합니다.
- **Gateway(**게이트웨이**)** 또는 **IPv6 Gateway(IPv6** 게이트웨이**)** - 이 경로의 다음 홉인 게이트웨이 라우터를 입력 또는 선택합니다. IP 주소 또는 네트워크/호스트 개체를 제공할 수 있습니다.
- **Metric(**메트릭**)** - 대상 네트워크 홉 수를 입력합니다. 유효한 범위는 1~255이고 기본값은 1입니다.

단계 **3** **OK(**확인**)**를 클릭합니다.

경로가 고정 경로 테이블에 추가됩니다.



단계 **4** **Save(**저장**)**를 클릭합니다.

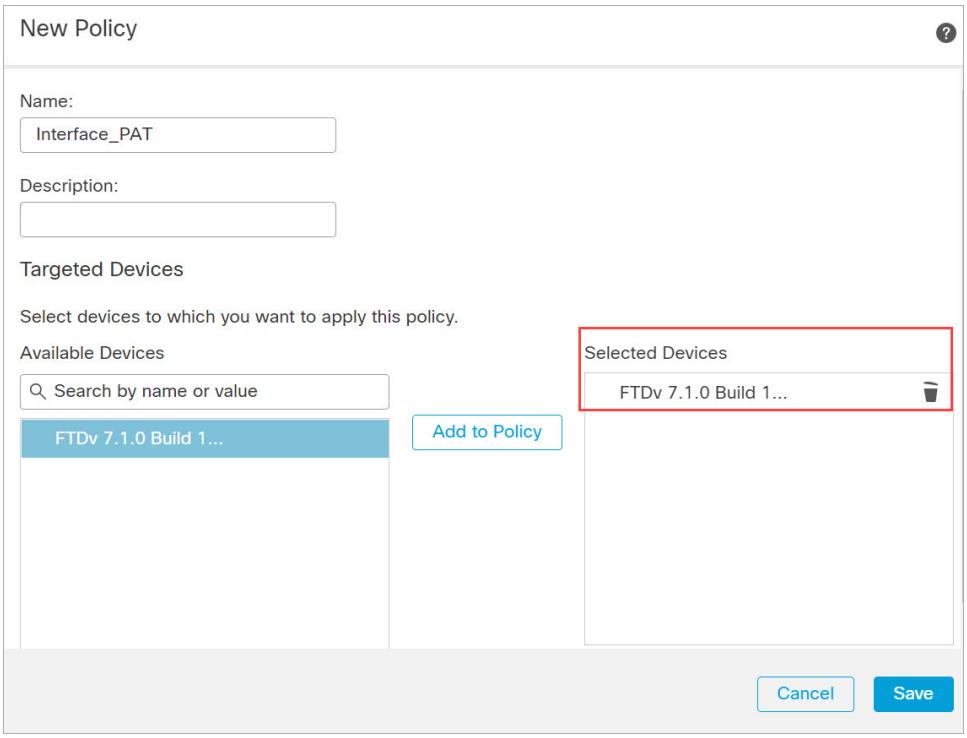
NAT 구성

일반적인 NAT 규칙은 내부 주소를 외부 인터페이스 IP 주소의 포트로 변환합니다. 이러한 유형의 NAT 규칙을 인터페이스 포트 주소 변환*(PAT)*이라고 합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **NAT**를 선택하고, **New Policy(**새 정책**)** > **Threat Defense NAT**를 클릭합니다.

단계 **2** 정책 이름을 지정하고, 정책을 사용할 디바이스를 선택한 뒤 **Save(**저장**)**를 클릭합니다.

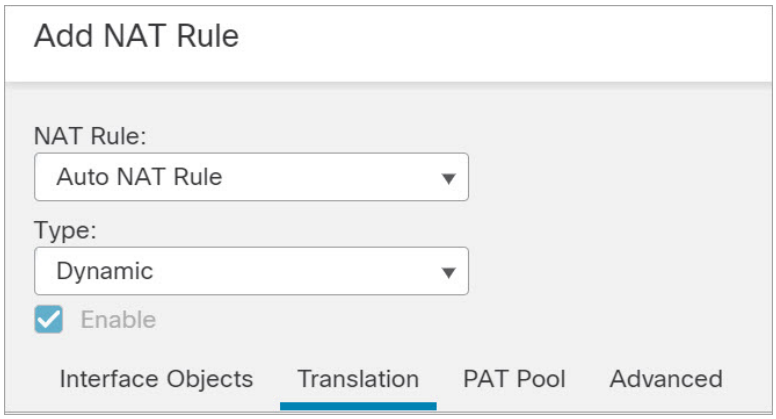


정책이 management center을 추가합니다. 계속해서 정책에 규칙을 추가해야 합니다.

단계 **3** **Add Rule(**규칙 추가**)**을 클릭합니다.

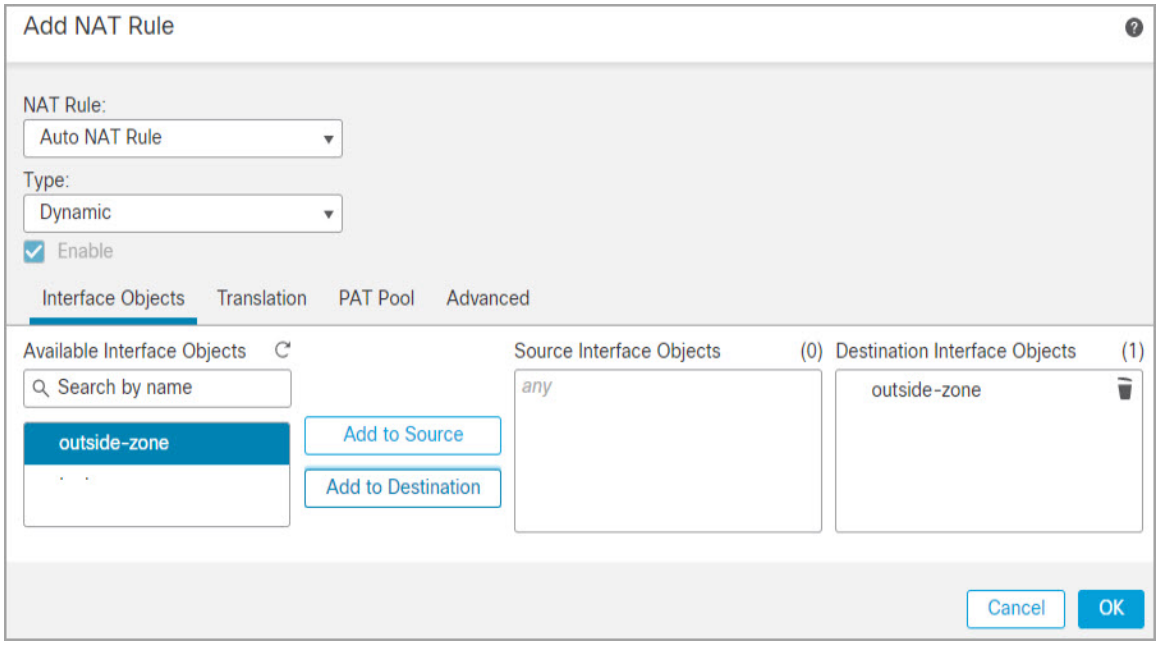
Add NAT Rule(NAT 규칙 추가**)** 대화 상자가 나타납니다.

단계 **4** 기본 규칙 옵션을 구성합니다.

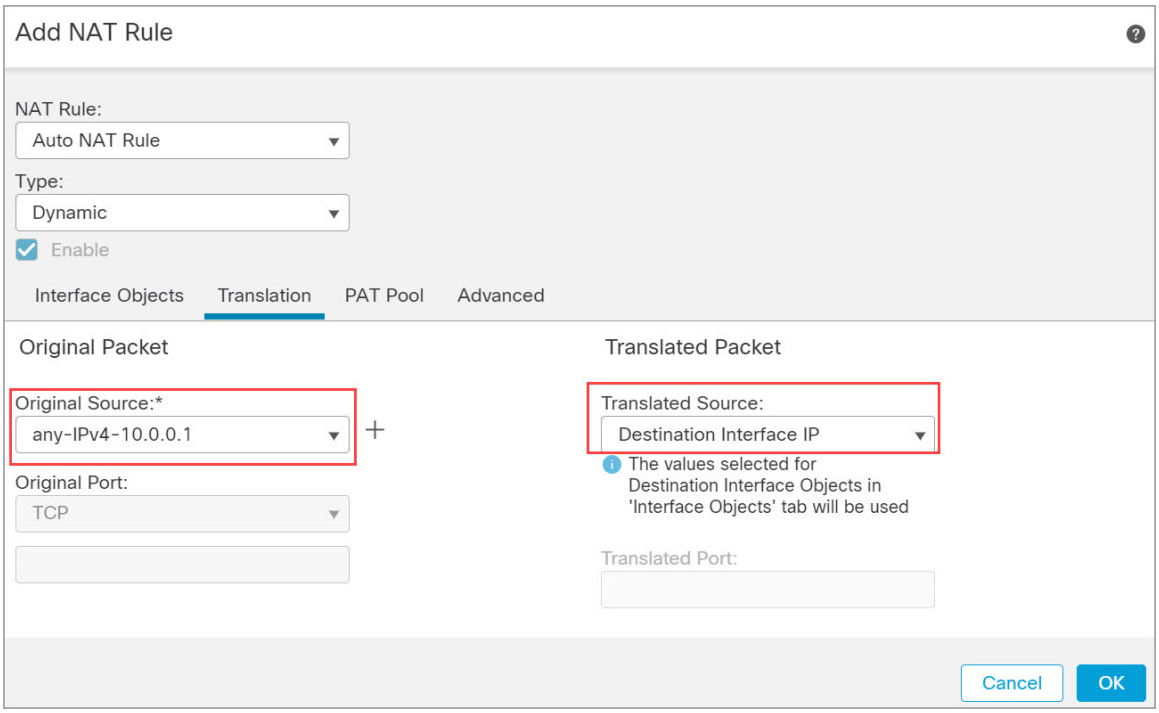


- **NAT Rule(NAT** 규칙**) - Auto NAT Rule(**자동 **NAT** 규칙**)**을 선택합니다.
- **Type(**유형**) - Dynamic(**동적**)**을 선택합니다.

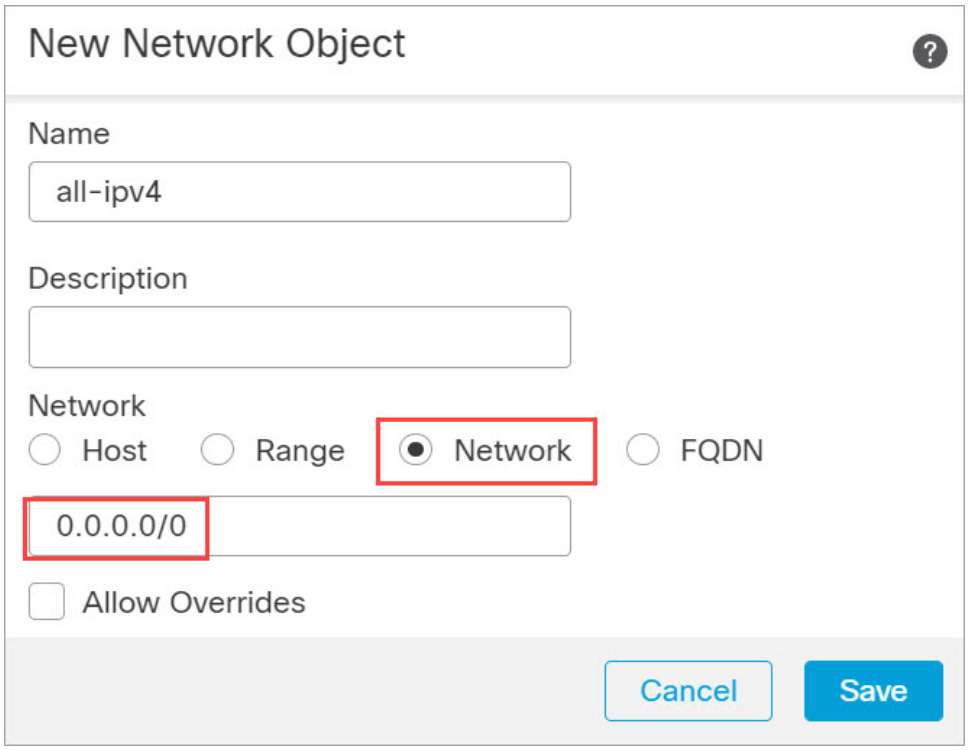
단계 **5** **Interface Objects(**인터페이스 개체**)** 페이지에서 **Available Interface Objects(**사용 가능한 인터페이스 개체**)** 영역의 외부 영역을 **Destination Interface objects(**대상 인터페이스 개체**)** 영역에 추가합니다.



단계 **6** **Translation(**변환**)** 페이지에서 다음 옵션을 설정합니다.



- **Original Source(**원본 소스**) -** 모든 IPv4 트래픽(0.0.0.0/0)에 대한 네트워크 개체를 추가하려면 추가(+)를 클릭합니다.



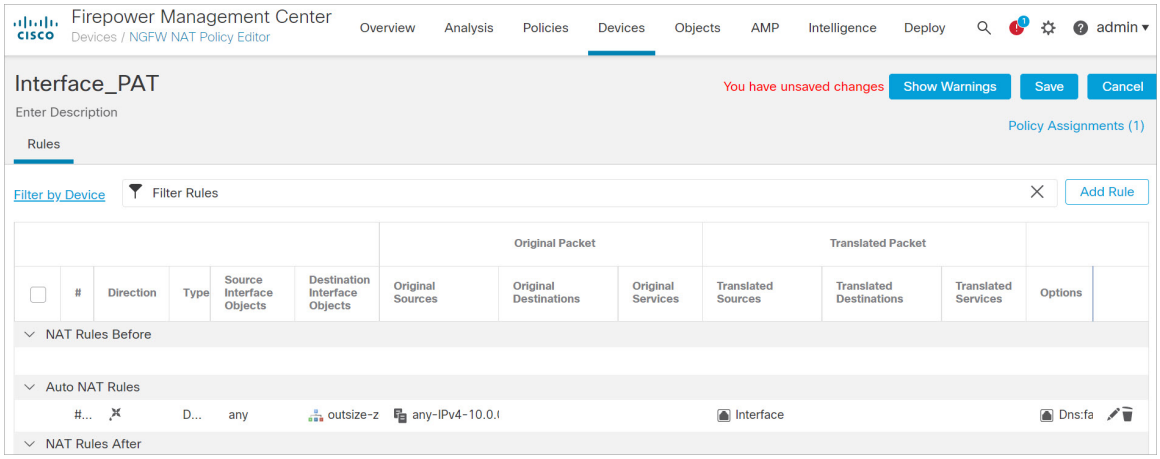
참고 자동 NAT 규칙은 개체 정의의 일부로 NAT를 추가하고 시스템 정의 개체를 수정할 수 없기 때문에 시스템에서 정의된 **any-ipv4** 개체를 사용할 수 없습니다.

마찬가지로, 모든 IPv6 트래픽에 대해 기본 호스트 네트워크 [::/0]를 사용하여 NAT 정책을 생성할 수 있습니다.

- **Translated Source(**변환된 소스**) - Destination Interface IP(**대상 인터페이스 **IP)**를 선택합니다.

단계 **7** **Save(**저장**)**를 클릭하여 규칙을 저장하십시오.

규칙이 **Rules(**규칙**)** 테이블에 저장됩니다.



단계 **8** 변경 사항을 저장하려면 **NAT** 페이지에서 **Save(**저장**)**를 클릭합니다.

액세스 제어 구성

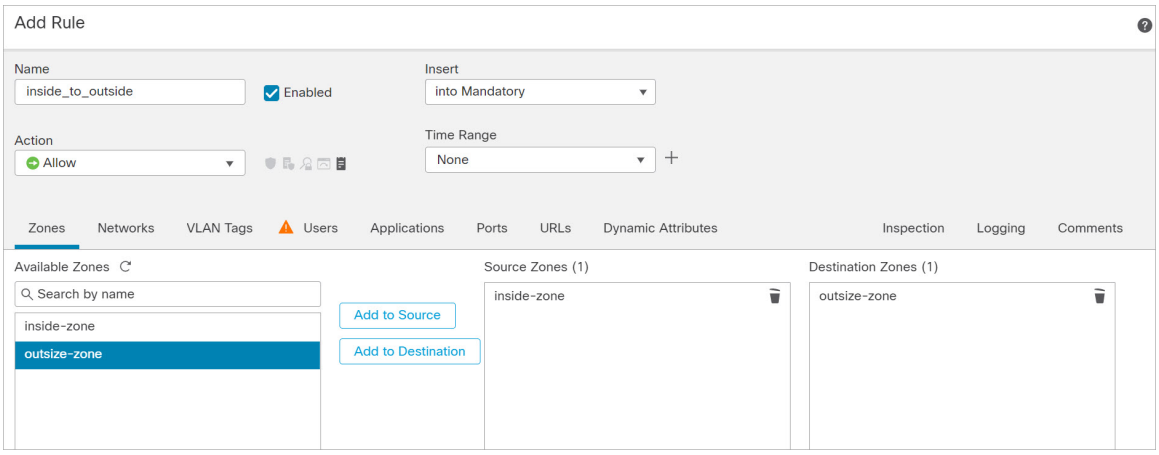
management center을 사용해 threat defense virtual를 등록할 때 기본 액세스 컨트롤 정책인 **Block all traffic(**모든 트래픽 차단**)**을 생성했다면, 디바이스에 트래픽을 허용하기 위해 정책에 규칙을 추가해야 합니다. 다음 절차에서는 내부 영역에서 외부 영역으로 향하는 트래픽을 허용하는 규칙을 추가합니다. 다른 영역이 있는 경우에는 적절한 네트워크에 대한 트래픽을 허용하는 규칙을 추가해야 합니다.

고급 보안 설정 및 규칙을 구성하려면 Firepower Management Center 구성 가이드 구성 가이드를 참조하십시오.

프로시저

단계 **1** **Policy(**정책**)** > **Access Policy(**액세스 정책**)** > **Access Policy(**액세스 정책**)**을 선택하고 threat defense에 할당된 액세스 컨트롤 정책에 대해 수정( )를 클릭합니다.

단계 **2** **Add Rule(**규칙 추가**)**을 클릭하고 다음 매개변수를 설정합니다.

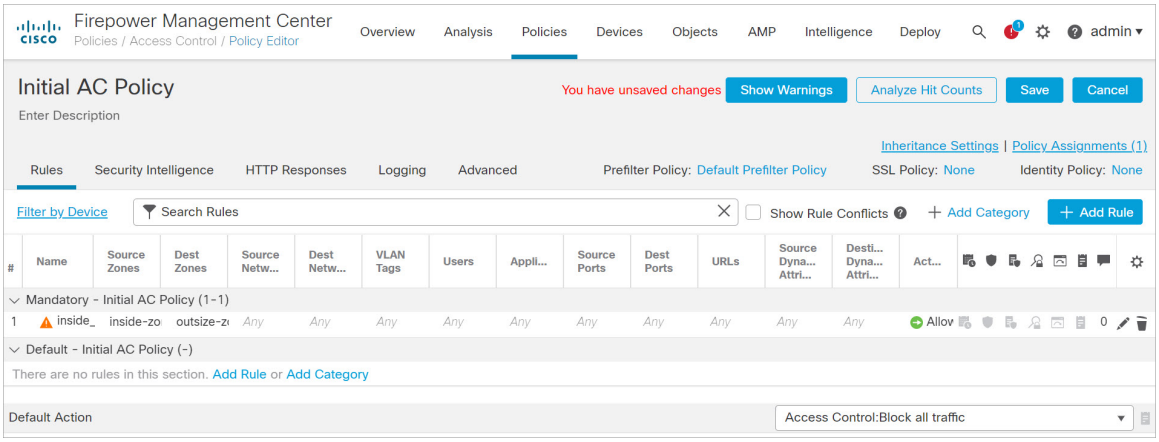


- **Name (**이름**)** - 예를 들어 이 규칙의 이름을 **inside_to_outside**로 지정합니다.
- **Source Zones(**원본 영역**)** - **Available Zones(**사용 가능한 영역**)**에서 내부 영역을 선택하고 **Add to Source(**원본에 추가**)**를 클릭합니다.
- **Destination Zones(**대상 영역**)** - **Available Zones(**사용 가능한 영역**)**에서 외부 영역을 선택하고 **Add to Destination(**대상에 추가**)**를 클릭합니다.

기타 설정은 변경하지 않습니다.

단계 **3** **Add(**추가**)**를 클릭합니다.

규칙이 **Rules(**규칙**)** 테이블에 추가됩니다.



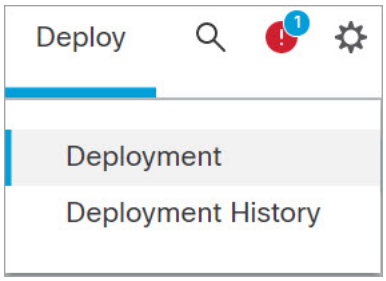
단계 **4** **Save(**저장**)**를 클릭합니다.

구성 구축

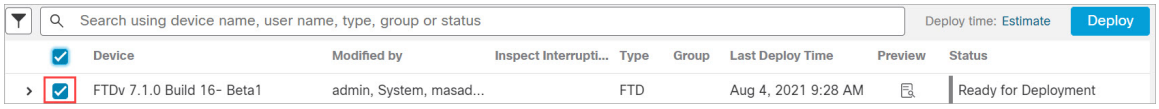
threat defense virtual에 설정 변경 사항을 구축합니다. 구축하기 전에는 디바이스에서 변경 사항이 활성 상태가 아닙니다.

프로시저

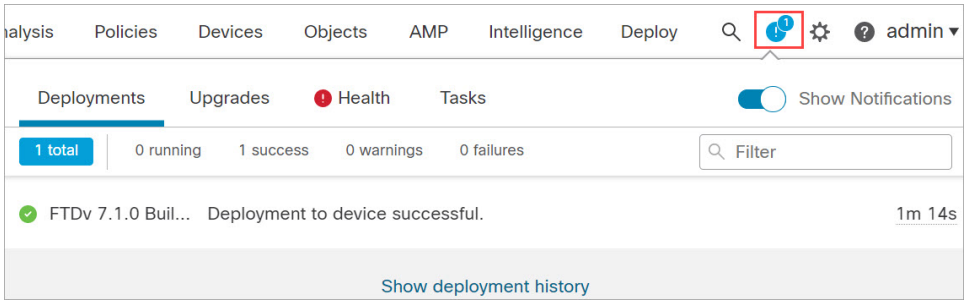
단계 1 우측 상단에서 **Deploy(구축)**를 클릭합니다.



단계 2 **Deploy policy(정책 구축)** 대화 상자에서 디바이스를 선택한 다음 **Deploy(구축)**를 클릭합니다.



단계 3 구축이 성공하는지 확인합니다. 메뉴 모음의 **Deploy(구축)** 버튼 오른쪽에 있는 아이콘을 클릭하여 구축 상태를 확인합니다.



Secure Firewall Threat Defense CLI에 액세스

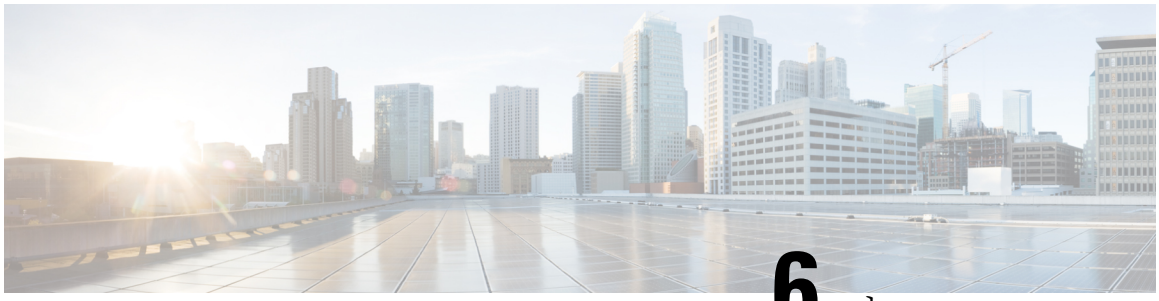
threat defense virtual CLI를 사용하여 관리 인터페이스 매개변수를 변경하고 문제를 해결할 수 있습니다. SSH를 사용하여 관리 인터페이스에 액세스하거나 VMware 콘솔에서 연결하여 CLI에 액세스할 수 있습니다.

프로시저

단계 1 (옵션 1) threat defense virtual 관리 인터페이스 IP 주소로 직접 SSH.

가상 머신을 구축할 때 관리 IP 주소를 설정합니다. 초기 구축 시 **admin** 계정 및 비밀번호를 사용해 threat defense virtual에 로그인합니다.

단계 **2** (옵션 2) VMware 콘솔을 열고 초기 구축 과정에 설정한 **admin** 계정의 기본 이름과 비밀번호를 사용해 로그인합니다.



6 장

Secure Firewall device manager로 Secure Firewall Threat Defense Virtual 관리

이 장에서는 device manager로 관리되는 독립형 threat defense virtual 디바이스를 구축하는 방법을 설명합니다. 고가용성 쌍을 구축하려면 Cisco Secure Firewall Device Manager 구성 가이드 설정 가이드를 참조하십시오.

Secure Firewall device manager를 사용하는 Secure Firewall Threat Defense Virtual 정보

Secure Firewall Threat Defense Virtual은(는) Cisco NGFW 솔루션의 가상화된 구성 요소입니다. threat defense virtual은 스테이트풀 방화벽, 라우팅, NGIPS(Next-Generation Intrusion Prevention System), AVC(Application Visibility and Control), URL 필터링, 악성코드 디펜스와 같은 차세대 방화벽 서비스를 제공합니다.

일부 threat defense 모델에 포함된 웹 기반 디바이스 설정 마법사인 Secure Firewall device manager을 사용하여 threat defense virtual를 관리할 수 있습니다. device manager 사용을 통해 소규모 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 구성을 사용하려는 경우에는 통합형 device manager 대신 management center를 사용하여 디바이스를 구성하십시오. 자세한 내용은 보안 방화벽 관리 센터로 Secure Firewall Threat Defense Virtual 관리, 67 페이지를 참조하십시오.

문제 해결을 위해 관리 인터페이스에서 SSH를 사용해 threat defense CLI에 액세스하거나, device manager CLI에서 threat defense에 연결할 수 있습니다.

기본 구성

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.

threat defense virtual은(는) 전원이 공급되는 첫 부팅 시 최소 4개의 인터페이스를 사용해야 합니다.

- 가상 머신의 첫 번째 인터페이스는 관리 인터페이스(Management0-0)입니다.
- 가상 머신의 두 번째 인터페이스는 진단 인터페이스(Diagnostic0-0)입니다.
- 가상 머신의 세 번째 인터페이스(GigabitEthernet0-0)는 외부 인터페이스입니다.
- 가상 머신의 네 번째 인터페이스(GigabitEthernet0-1)는 내부 인터페이스입니다.

데이터 트래픽의 경우 최대 6개 이상의 인터페이스를 추가하여 총 8개의 데이터 인터페이스를 사용할 수 있습니다. 추가 데이터 인터페이스의 경우 소스 네트워크가 올바른 대상 네트워크에 매핑되는지, 또한 각 데이터 인터페이스가 고유한 서브넷 또는 VLAN에 매핑되는지 확인합니다. VMware 인터페이스 구성을 참조하십시오.

초기 구성

네트워크에 보안 어플라이언스를 삽입하고 인터넷 또는 기타 업스트림 라우터에 연결하는 데 필요한 주소 구성을 포함한 threat defense virtual 기능이 네트워크에서 올바르게 작동하는 초기 구성을 완료해야 합니다. 다음 두 가지 방법 중 하나로 시스템의 초기 구성을 수행할 수 있습니다.

- device manager 웹 인터페이스(권장)를 사용합니다. Device Manager는 웹 브라우저에서 실행됩니다. 이 인터페이스를 사용하여 시스템을 구성, 관리 및 모니터링합니다.
- CLI(명령줄 인터페이스) 설정 마법사를 사용합니다(선택). 초기 구성에 device manager 대신 CLI 설정 마법사를 사용할 수 있으며, 문제 해결에도 CLI를 사용할 수 있습니다. device manager 사용해 여전히 시스템을 구성, 관리, 모니터링할 수 있습니다. (선택 사항) threat defense CLI 마법사 시작을 참조하십시오.

다음 주제에서는 이런 인터페이스를 사용해 시스템의 초기 구성을 수행하는 방법을 설명합니다.

실행 Device Manager

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

프로시저

단계 **1** 브라우저를 열고 device manager에 로그인합니다. CLI에서 초기 컨피그레이션을 수행하지 않았다고 가정하고 **https://FTDv** 공용 **IPv4** 주소 또는 **[FTDv IPv6** 공용 주소**]**에서 device manager를 엽니다.

단계 **2** 사용자 이름 **admin** 및 비밀번호 **Admin123**으로 로그인합니다.

단계 **3** 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 **4** 외부 및 관리 인터페이스에 대해 다음 옵션을 구성하고 **Next(**다음**)**를 클릭합니다.

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

a) **Outside Interface(**외부 인터페이스**)** - 게이트웨이 모드 또는 라우터에 연결한 데이터 포트입니다. 초기 디바이스 설정 중에는 대체 외부 인터페이스를 선택할 수 없습니다. 첫 번째 데이터 인터페이스가 기본 외부 인터페이스입니다.

IPv4 구성 - 외부 인터페이스의 IPv4 주소를 구성합니다. DHCP를 사용하거나 수동으로 고정 IP 주소, 서브넷 마스크 및 게이트웨이를 입력할 수 있습니다. *끄기*를 선택하여 IPv4 주소를 구성하지 않을 수도 있습니다.

IPv6 구성 - 외부 인터페이스의 IPv6 주소를 구성합니다. DHCP를 사용하거나 수동으로 고정 IP 주소, 접두사 및 게이트웨이를 입력할 수 있습니다. *끄기*를 선택하여 IPv6 주소를 구성하지 않을 수도 있습니다.

b) 관리 인터페이스

DNS 서버 - 시스템 관리 주소용 DNS 서버를 지정합니다. 이름 확인을 위해 DNS 서버의 주소를 하나 이상 입력합니다. 기본값은 OpenDNS 공개 DNS 서버입니다. 필드를 수정하여 기본값으로 되돌리려면 **OpenDNS(OpenDNS** 사용**)**를 클릭하여 적절한 IP 주소를 필드에 다시 로드합니다.

방화벽 호스트 이름 - 시스템 관리 주소용 호스트 이름을 지정합니다.

참고 디바이스 설정 마법사를 사용해 threat defense 디바이스를 구성할 때 시스템은 아웃바운드 및 인바운드 트래픽에 대해 두 가지 기본 액세스 규칙을 제공합니다. 초기 설정 후에 다시 돌아가 이 액세스 규칙을 편집할 수 있습니다.

단계 **5** 시스템 시간 설정을 구성하고 **Next(**다음**)**를 클릭합니다.

a) 표준 시간대 - 시스템의 표준 시간대를 선택합니다.

b) **NTP** 시간 서버 - 기본 NTP 서버를 사용할지 아니면 NTP 서버의 주소를 수동으로 입력할지를 선택합니다. 백업을 제공하기 위해 여러 서버를 추가할 수 있습니다.

단계 **6** 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 링크를 클릭하여 Smart Software Manager 어카운트에 로그인한 다음 새 토큰을 생성해 수정 상자에 복사합니다.

평가 라이선스를 사용하려면 등록 없이 **90**일 평가 기간 시작을 선택합니다. 나중에 디바이스를 등록하고 스마트 라이선스를 가져오려면 메뉴의 디바이스 이름을 클릭한 다음 **Device Dashboard(**디바이스 대시보드**)**로 이동해 **Smart Licenses(**스마트 라이선스**)** 그룹에서 링크를 클릭합니다.

단계 **7** **Finish(**마침**)**를 클릭합니다.

다음에 수행할 작업

- device manager을 사용해 디바이스 설정은 Secure Firewall device manager에서 디바이스를 구성하는 방법, 88 페이지를 참고하십시오.

Secure Firewall device manager에서 디바이스를 구성하는 방법

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

- 내부 및 외부 인터페이스용 보안 영역
- 내부에서 외부로 이동하는 모든 트래픽을 신뢰하는 액세스 규칙
- 내부에서 외부로 이동하는 모든 트래픽을 외부 인터페이스의 IP 주소에 있는 고유한 포트로 변환하는 인터페이스 NAT 규칙입니다.
- 내부 인터페이스 또는 브리지 그룹에서 실행 중인 DHCP 서버

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

프로시저

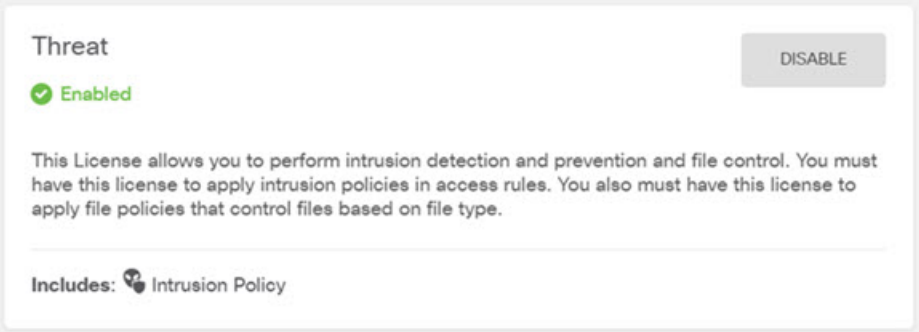
단계 **1** **Device(**디바이스**)**를 선택한 다음 **Smart License(**스마트 라이선스**)** 그룹에서 **View Configuration(**컨피그레이션 보기**)**를 클릭합니다.

사용할 각 라이선스 옵션(IPS, 악성코드 방어, URL 필터링)에 대해 **Enable(**활성화**)**을 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. **Request Register(**등록 요청**)**를 클릭하고 지침을 따릅니다. 평가 라이선스가 만료되기 전에 등록하십시오.

예를 들어, 활성화된 IPS 라이선스는 다음과 같이 표시됩니다.

그림 *30:* 활성화된 *IPS* 라이선스

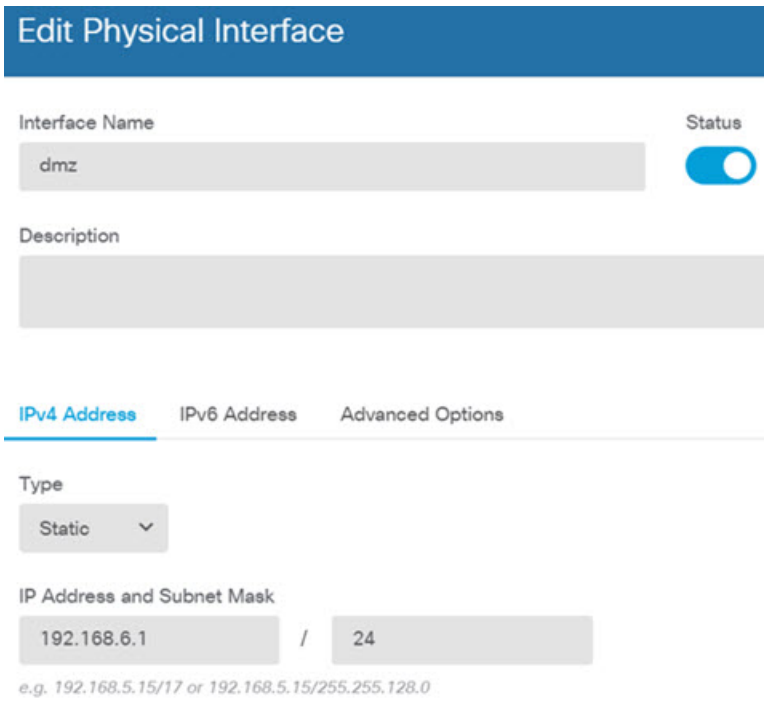


단계 **2** 다른 인터페이스를 구성한 경우 **Device(**디바이스**)**를 선택하고 **Interfaces(**인터페이스**)** 그룹에서 **View Configuration(**컨피그레이션 보기**)**를 클릭한 뒤 각 인터페이스를 구성합니다.

다른 인터페이스용 브리지 그룹을 생성하거나, 별도의 네트워크를 구성하거나 이 두 방법을 조합해 사용할 수 있습니다. 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.

그림 *31:* 인터페이스 수정



참고 IPv6 주소를 활성화하려면 IPv6 탭을 선택하고 고정 또는 DHCP를 사용하여 IPv6 주소를 구성합니다.

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.

그림 ***32:*** 보안 영역 개체

단계 **4** 내부 클라이언트가 DHCP를 사용해 디바이스에서 IP 주소를 가져오도록 하려면 **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **DHCP Server(DHCP** 서버**)**을 선택하고 **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.

그림 ***33: DHCP*** 서버

단계 **5** **Device(**디바이스**)**를 선택한 후 **Routing(**라우팅**)** 그룹에서 **View Configuration(**컨피그레이션 보기**)**(또는 **Create First Static Route(**첫 번째 정적 경로 생성**)**)을 클릭하고 기본 경로를 컨피그레이션합니다.

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.

참고 이 페이지에서 정의하는 경로는 데이터 인터페이스 전용입니다. 이러한 경로는 관리 인터페이스에 영향을 주지 않습니다. **Device(**디바이스**)** > **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.

그림 *34:* 기본 라우터

참고 마찬가지로 IPv6 라디오 버튼을 선택하여 IPv6 경로를 구성할 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.

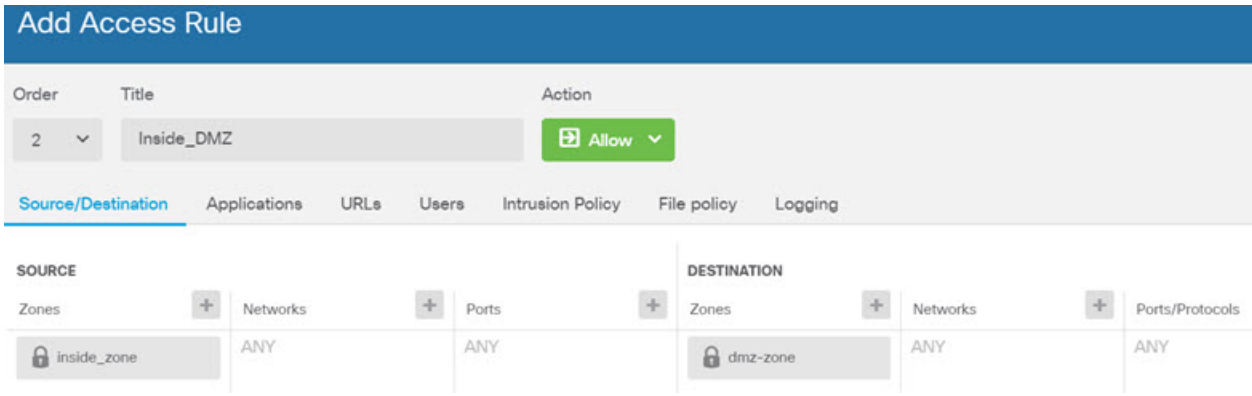
- **SSL Decryption(SSL** 암호 해독**)** — 침입, 악성코드 등에 대한 암호화된 연결(예: HTTPS)을 검사하려는 경우, 연결을 암호 해독해야 합니다. SSL 암호 해독 정책을 사용하여 어떤 연결을 암호 해독해야 할지 확인합니다. 시스템은 검사를 수행한 후에 연결을 다시 암호화합니다.
- **Identity(ID)** — 네트워크 활동과 개인 사용자의 상관관계를 분석하거나 사용자 또는 사용자 그룹 멤버십을 기반으로 네트워크 액세스를 제어하려면 ID 정책을 사용하여 지정된 소스 IP 주소와 연결된 사용자를 확인합니다.
- **Security Intelligence(**보안 인텔리전스**)** — 보안 인텔리전스 정책을 사용하여 블랙리스트에 추가된 IP 주소 또는 URL를 오가는 연결을 신속하게 삭제합니다. 알려진 유해 사이트를 블랙리스트에 추가함으로써 해당 사이트를 액세스 제어 정책에서 고려할 필요가 없습니다. Cisco는 알려진

유해 주소 및 URL에 대해 정기적으로 업데이트된 피드를 제공하므로 보안 인텔리전스 블랙리스트가 동적으로 업데이트됩니다. 피드를 사용하는 경우에는 블랙리스트에서 항목을 추가하거나 제거하기 위해 정책을 편집할 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.

그림 ***35:*** 액세스 제어 정책



단계 **7** **Device(디바이스)**를 선택한 다음 **Updates(업데이트)** 그룹에서 **View Configuration(구성 보기)**를 클릭하고 시스템 데이터베이스에 대한 업데이트 일정을 구성합니다.

침입 정책을 사용하는 경우 규칙 및 VDB 데이터베이스에 대한 정기 업데이트를 설정합니다. 보안 인텔리전스 피드를 사용하는 경우 피드의 업데이트 일정을 설정합니다. 모든 보안 정책의 일치 기준으로 지리적 위치를 사용하는 경우 해당 데이터베이스에 대한 업데이트 일정을 설정합니다.

단계 **8** 메뉴에서 **Deploy(구축)** 버튼을 클릭한 다음 지금 구축 버튼( )을 클릭하여 디바이스에 변경 사항을 구축합니다.

변경 사항은 구축할 때까지 디바이스에서 활성화되지 않습니다.

다음에 수행할 작업

device manager로 threat defense virtual을 관리하는 방법에 대한 자세한 내용은 Firepower Device Manager용 Cisco Firepower Threat Defense 구성 가이드 또는 Secure Firewall device manager 온라인 도움말을 참조하십시오.