Azure에서 Threat Defense Virtual 구축

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

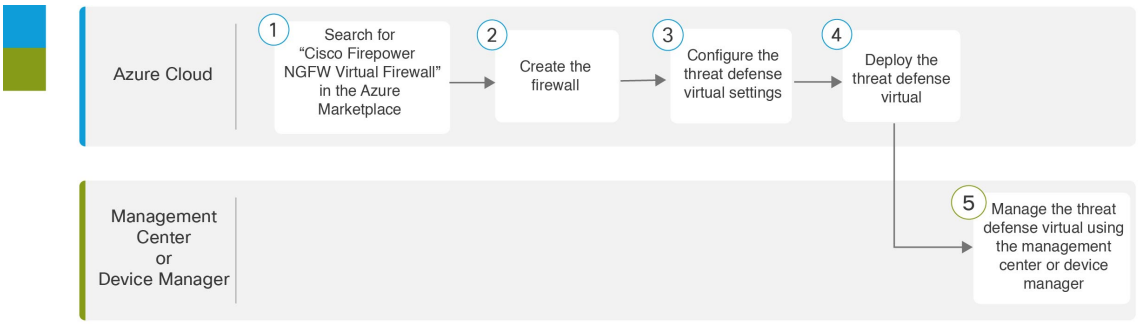
Azure 구축

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 3를 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 6를 참조하십시오.

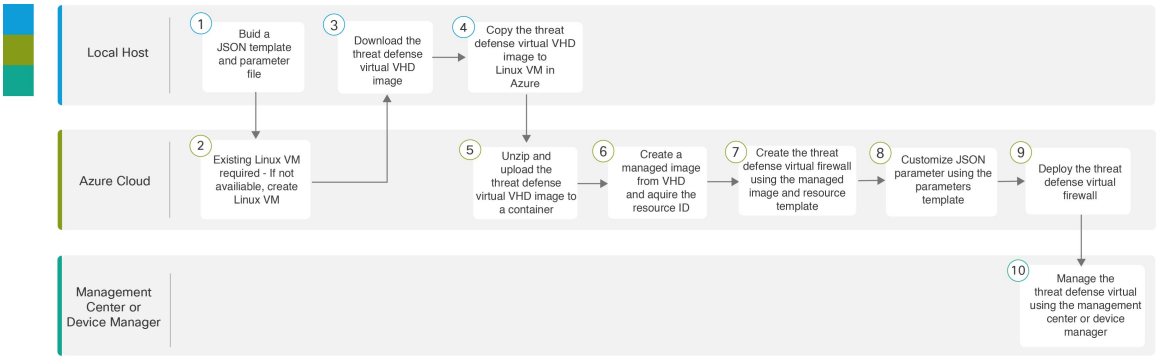
엔드 투 엔드 절차

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: • Management Center로 Threat Defense Virtual 관리 • Device Manager로 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, 6 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: • Management Center로 Threat Defense Virtual 관리 • Device Manager로 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 6를 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. FMC로 FTDv 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. FDM으로 FTDv 관리를 참조하십시오.

관리 옵션을 선택하는 방법에 대한 개요는 Secure Firewall Threat Defense Virtual 디바이스 관리 방법을 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.