Microsoft Azure 클라우드용 Cisco Firepower Threat Defense Virtual 빠른 시작 가이드

게시 날짜: 2017년 1월 23일

업데이트 날짜: 2017년 7월 13일 목요일

Microsoft Azure는 컴퓨팅, 분석, 스토리지 및 네트워킹을 위한 서비스를 포함하여 다양한 클라우드 서비스를 제공하는 개방형의 유연한 엔터프라이즈급 퍼블릭 클라우드 컴퓨팅 플랫폼입니다. 이러한 서비스 중 하나를 선택하여 퍼블릭 클라우드에서 새로운 애플리케이션을 개발하고 확장하거나 기존 애플리케이션을 실행할 수 있습니다.

이 문서에는 Azure에서 Firepower Threat Defense Virtual을 구축하는 방법이 나와 있습니다.

Microsoft Azure 클라우드에서의 구축 정보

Firepower Threat Defense Virtual은 Microsoft Azure 마켓플레이스에 통합됩니다. Firepower Management Center 관리 작업은 고객사 구내 Azure 외부에서 실행됩니다. Microsoft Azure의 Firepower Threat Defense Virtual은 두 가지 인스턴스 유형을 지원합니다.

- 표준 D3 - 4개의 vCPU, 14GB, 4vNIC
- 표준 D3_v2 - 4개의 vCPU, 14GB, 4vNIC

Firepower Threat Defense Virtual 및 Azure에 대한 사전 요구 사항 및 시스템 요구 사항

- Azure.com에서 어카운트를 생성합니다.

  Microsoft Azure에서 어카운트를 생성한 후 로그인하여 Cisco Firepower Threat Defense의 마켓플레이스를 검색하고 “Cisco Firepower Next Generation Firewall - 가상” 오퍼링을 선택할 수 있습니다.
- Cisco Smart Account. Cisco Software Central(https://software.cisco.com/)에서 어카운트를 생성할 수 있습니다.
- Firepower Threat Defense Virtual 라이선스를 얻습니다. 라이선스를 얻을 때까지 Firepower Threat Defense Virtual은 성능이 저하된 모드에서 실행되며, 100개의 연결과 100Kbps의 처리량만 허용합니다.
  - Firepower Management Center의 보안 서비스를 사용하려면 모든 라이선스 자격을 구성합니다.
  - 라이선스를 관리하는 방법에 대한 자세한 내용은 Firepower Management Center 컨피그레이션 가이드의 "Firepower System 라이선싱"을 참조하십시오.
- 통신 경로:
  - 관리 인터페이스 - Firepower Threat Defense Virtual을 Firepower Management Center에 연결하는 데 사용됩니다.
  - 진단 인터페이스 - 진단 및 보고에 사용되며, 통과하는 트래픽에는 사용할 수 없습니다.
  - 내부 인터페이스(필수) - Firepower Threat Defense Virtual을 내부 호스트에 연결하는 데 사용됩니다.
  - 외부 인터페이스(필수) - Firepower Threat Defense Virtual을 공용 네트워크에 연결하는 데 사용됩니다.
- Firepower Threat Defense Virtual 및 Firepower System 호환성에 대해서는 Cisco Firepower Threat Defense Virtual 호환성을 참조하십시오.

Firepower Threat Defense Virtual 및 Azure에 대한 지침 및 제한 사항

지원 기능

- Firepower Threat Defense Virtual만 Microsoft Azure 마켓플레이스에서 사용할 수 있습니다. Firepower Management Center는 Azure 외부에서 실행됩니다.
- 지원되는 Azure 인스턴스 - Standard_D3_V2(기본값) 및 Standard_D3. 두 인스턴스 모두 4vCPU, 14GB 메모리, 4vNIC를 지원합니다.
- 라이선싱 모드:
  - Smart License 전용
  - PLR은 지원되지 않음
- 네트워킹:
  - 라우팅 방화벽 모드 전용
- 공용 IP 주소 지정
  - 관리 0/0 및 GigabitEthernet0/0만 할당된 공용 IP 주소입니다.
- 인터페이스:
  - 4개의 인터페이스에서 Firepower Threat Defense Virtual을 구축합니다.

지원되지 않는 기능

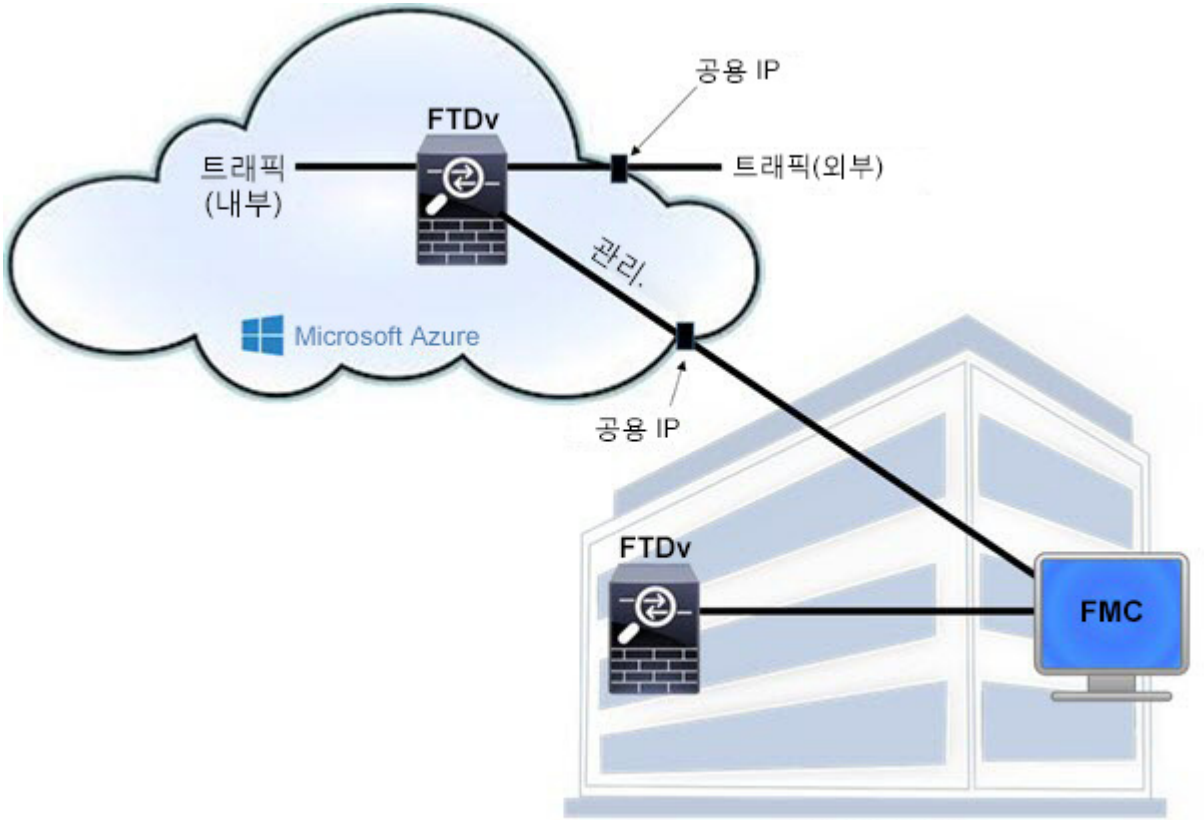
- 라이선싱
  - PAYG(용량 확장에 따른 지불) 라이선싱
  - PLR(Permanent License Reservation: 영구 라이선스 예약)
- 네트워킹(다음 중 대부분이 Microsoft Azure 제한 사항에 해당함)
  - 점보 프레임
  - IPv6
  - 802.1Q VLANs
  - 투명 모드 및 기타 레이어 2 기능: 브로드캐스트 없음, 멀티캐스트 없음
  - 디바이스가 Azure 측면에서 소유하고 있지 않은 IP 주소에 대한 프록시 ARP(일부 NAT 기능에 영향을 줌)
  - 프로미스큐어스 모드(서브넷 트래픽 캡처 없음)
  - 인라인 집합 모드, 패시브 모드

    참고: Azure 정책은 인터페이스가 프로미스큐어스 모드에서 동작하는 것을 허용하지 않으므로 Firepower Threat Defense Virtual이 투명 방화벽 또는 인라인 모드에서 동작하는 것을 방지합니다.
  - ERSPAN(Azure에서 전달되지 않는 GRE 사용)
- 관리
  - 콘솔 액세스: Firepower Management Center를 사용하여 네트워크를 통해 관리 기능이 수행됨(SSH는 일부 설치 및 유지 보수 활동에 사용 가능)
  - Azure 포털 "비밀번호 재설정" 기능
  - 콘솔 기반 비밀번호 복구: 사용자가 콘솔에 대한 실시간 액세스 권한이 없으므로 비밀번호를 복구할 수 없으며, 비밀번호 복구 이미지를 부팅할 수 없습니다. 유일한 방법은 새로운 Firepower Threat Defense Virtual VM을 구축하는 것입니다.
- 고가용성(액티브/스탠바이)
- 클러스터링
- VM 가져오기/내보내기
- Firepower Device Manager 사용자 인터페이스

Azure에서의 Firepower Threat Defense Virtual에 대한 샘플 네트워크 토폴로지

다음 그림은 Azure 내부 라우팅 방화벽 모드에서의 Firepower Threat Defense Virtual에 대한 일반적인 토폴로지를 보여줍니다. 첫 번째 정의된 인터페이스는 항상 관리 인터페이스이며 관리 0/0과 GigabitEthernet0/0만 할당된 공용 IP 주소입니다.

그림 1 Azure 구축에서의 샘플 Firepower Threat Defense Virtual



구축 시 생성되는 리소스

Azure에서 Firepower Threat Defense Virtual을 구축할 때 다음과 같은 리소스가 생성됩니다.

- Firepower Threat Defense VM(Virtual Machine)
- 리소스 그룹
  - Firepower Threat Defense Virtual은 항상 새 리소스 그룹에 구축됩니다. 그러나 다른 리소스 그룹에 있는 기존 가상 네트워크에 연결할 수 있습니다.
- *VM 이름*-Nic0, *VM 이름*-Nic1, *VM 이름*-Nic2, *VM 이름*-Nic3으로 명명된 4개의 NICS

  이러한 NIC는 Firepower Threat Defense Virtual 인터페이스 관리, 진단 0/0, GigabitEthernet0/0 및 GigabitEthernet0/1에 각각 매핑됩니다.

- *VM 이름*-mgmt-SecurityGroup으로 명명된 보안 그룹

  보안 그룹은 VM의 Nic0에 연결되며 이는 Firepower Threat Defense Virtual 관리 인터페이스에 매핑됩니다.

  보안 그룹에는 SSH(TCP 포트 22) 및 Firepower Management Center 인터페이스(TCP 포트 8305)용 관리 트래픽을 허용하는 규칙이 포함되어 있습니다. 이러한 값은 구축 후 수정할 수 있습니다.
- 공용 IP 주소(구축 시 선택한 값에 따라 명명됨)

  공용 IP 주소는 VM Nic0에 연결되며 이는 관리에 매핑됩니다.

  참고: 공용 IP 주소(신규 또는 기존)를 선택해야 합니다. NONE(없음) 옵션은 지원되지 않습니다.
- 4개의 서브넷이 있는 가상 네트워크는 새로운 네트워크 옵션을 선택할 경우 생성됩니다.
- 각 서브넷에 대한 라우팅 테이블(이미 있는 경우 업데이트됨)

  테이블 이름은 "*서브넷 이름*"-FTDv-RouteTable입니다.

  각 라우팅 테이블에는 다음 홉으로 Firepower Threat Defense Virtual IP 주소를 사용하는 다른 3개의 서브넷에 대한 경로가 포함되어 있습니다. 트래픽이 다른 서브넷 또는 인터넷에 도달해야 하는 경우 기본 경로를 추가하도록 선택할 수 있습니다.
- 선택한 스토리지 어카운트의 부팅 진단 파일

  부팅 진단 파일은 Blob(binary large object)에 포함됩니다.
- Blob 및 컨테이너 VHD 아래에서 선택된 스토리지 어카운트의 파일 2개(*VM 이름*-disk.vhd 및 *VM 이름*-<uuid>.status)
- 스토리지 어카운트(기존 스토리지 어카운트를 선택하지 않는 경우)

  참고: VM을 삭제하는 경우 각 리소스를 개별적으로 삭제해야 합니다(유지할 리소스는 제외).

Azure 라우팅

Azure 가상 네트워크 서브넷에서 라우팅은 서브넷의 효과적인 라우팅 테이블에 의해 결정됩니다. 효과적인 라우팅 테이블은 기본 제공 시스템 경로 및 UDR(User Defined Route) 테이블의 경로를 조합한 것입니다.

참고: VM NIC 속성에서 효과적인 라우팅 테이블을 볼 수 있습니다.

사용자 정의 라우팅 테이블을 보고 편집할 수 있습니다. 시스템 경로 및 사용자 정의 경로가 효과적인 라우팅 테이블을 구성하기 위해 결합된 경우, 가장 구체적인 경로를 얻고 결합하여 사용자 정의 라우팅 테이블로 이동합니다. 시스템 라우팅 테이블에는 Azure의 가상 네트워크 인터넷 게이트웨이를 가리키는 기본 경로(0.0.0.0/0)가 포함되어 있습니다. 시스템 라우팅 테이블에는 또한 Azure의 가상 네트워크 인프라 게이트웨이를 가리키는 다음 홉과 함께 정의된 다른 서브넷에 대한 구체적인 경로가 포함되어 있습니다.

Firepower Threat Defense Virtual을 통해 트래픽을 라우팅하려면 각 데이터 서브넷과 연결된 사용자 정의 라우팅 테이블에서 경로를 추가/업데이트해야 합니다. 관심 있는 트래픽은 해당 서브넷에서 다음 홉으로 Firepower Threat Defense Virtual IP 주소를 사용하여 라우팅해야 합니다. 또한, 필요한 경우 0.0.0.0/0에 대한 기본 경로를 Firepower Threat Defense Virtual IP의 다음 홉과 함께 추가할 수 있습니다.

시스템 라우팅 테이블에 있는 기존의 구체적인 경로 때문에 다음 홉으로 Firepower Threat Defense Virtual을 가리키도록 사용자 정의 라우팅 테이블에 구체적인 경로를 추가해야 합니다. 그렇지 않으면 사용자 정의 테이블의 기본 경로보다 시스템 라우팅 테이블의 더 구체적인 경로가 우선시되어 트래픽이 Firepower Threat Defense Virtual을 우회합니다.

가상 네트워크에서의 VM에 대한 라우팅 컨피그레이션

Azure 가상 네트워크에서 라우팅은 클라이언트에서의 특정한 게이트웨이 설정이 아니라 효과적인 라우팅 테이블에 따라 결정됩니다. 가상 네트워크에서 실행 중인 클라이언트에는 개별 서브넷에서 .1 주소인 DHCP에 의해 경로가 지정될 수 있습니다. 이는 자리 표시자이며 가상 네트워크의 인프라 가상 게이트웨이로 패킷을 가져가기 위해서만 제공됩니다. 패킷이 VM에서 전송되면 효과적인 라우팅 테이블에 따라 사용자 정의 테이블에서 수정된 대로 라우팅됩니다. 효과적인 라우팅 테이블은 클라이언트가 .1 또는 Firepower Threat Defense Virtual 주소로 구성된 게이트웨이를 갖고 있는지와 관계없이 다음 홉을 결정합니다.

Azure VM ARP 테이블은 모든 알려진 호스트에 대해 동일한 MAC 주소(1234.5678.9abc)를 표시합니다. 이렇게 하면 Azure VM에서 전송되는 모든 패킷이 Azure 게이트웨이(효과적인 라우팅 테이블이 패킷의 경로를 결정하는 데 사용되는 위치)에 도달합니다.

IP 주소

다음은 Azure의 IP 주소에 해당하는 정보입니다.

- Firepower Threat Defense Virtual(관리에 매핑됨)의 첫 번째 NIC에는 연결된 서브넷의 개인 IP 주소가 지정됩니다.

  공용 IP 주소는 이 개인 IP 주소와 연결될 수 있으며 Azure 인터넷 게이트웨이는 NAT 변환을 처리합니다.

  Firepower Threat Defense Virtual이 구축된 이후에 공용 IP 주소를 데이터 인터페이스(예: GigabitEthernet0/0)에 연결할 수 있습니다.
- 동적 공용 IP 주소는 Azure 중지/시작 주기 동안 변경될 수 있습니다. 그러나 Azure가 재시작되고 Firepower Threat Defense Virtual이 다시 로드되는 동안에는 영구적입니다.
- 정적 공용 IP 주소는 Azure에서 이 주소를 변경할 때까지 변경되지 않습니다.
- Firepower Threat Defense Virtual 인터페이스는 DHCP를 사용하여 IP 주소를 설정할 수 있습니다. Azure 인프라에서는 Firepower Threat Defense Virtual 인터페이스가 Azure에서 설정된 IP 주소를 할당받습니다.

Firepower Threat Defense Virtual 구축

다음 절차는 Microsoft Azure 환경에서 Firepower Threat Defense Virtual을 설정하는 단계의 최상위 레벨 목록입니다. Azure 설정에 대한 자세한 단계는 Azure 시작을 참조하십시오.

Azure에서 Firepower Threat Defense Virtual을 구축하는 경우 리소스, 공용 IP 주소 및 경로 테이블 등 다양한 컨피그레이션이 자동으로 생성됩니다. 이러한 컨피그레이션은 구축 후 변경할 수 있습니다. 예를 들어 유휴 시간 초과 값을 기본값(낮은 시간 초과 값)에서 변경할 수 있습니다.

절차

1. ARM(Azure Resource Manager) 포털에 로그인합니다.

   Azure 포털에는 데이터 센터 위치와 관계없이 현재 어카운트 및 서브스크립션과 연결된 가상 요소가 표시됩니다.
2. **Azure Marketplace(Azure 마켓플레이스)** > **Virtual Machines(가상 머신)**를 선택합니다.
3. “Cisco Firepower Next Generation Firewall - 가상”의 마켓플레이스를 검색하고 오퍼링을 선택한 다음 **Create(생성)**를 클릭합니다.
4. 기본 설정을 구성합니다.

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

      참고: 기존 이름을 사용하지 마십시오. 그렇지 않으면 구축이 실패합니다.

   b. Firepower Threat Defense Virtual 관리자의 사용자 이름을 입력합니다.

      참고: "admin"이라는 이름은 Azure에서 예약되어 있으므로 사용할 수 없습니다.

c. 인증 유형을 비밀번호 또는 SSH 키 중에서 선택합니다.

   비밀번호를 선택하는 경우 비밀번호를 입력하고 확인합니다.

   SSH 키를 선택하는 경우 원격 피어의 RSA 공개 키를 지정합니다.

d. Firepower Threat Defense Virtual을 구성하기 위해 로그인할 경우 사용자 어카운트(**Admin**)와 함께 사용할 비밀번호를 생성합니다.

e. 서브스크립션 유형을 선택합니다.

f. 새 리소스 그룹을 생성합니다.

   Firepower Threat Defense Virtual은 새 리소스 그룹에 구축해야 합니다. 기존 리소스 그룹에 구축하는 옵션은 기존 리소스 그룹이 비어 있는 경우에만 동작합니다.

   그러나 나중 단계에서 네트워크 옵션을 구성하는 경우 다른 리소스 그룹에 있는 기존의 가상 네트워크에 FTDv를 연결할 수 있습니다.

g. 지리적 위치를 선택합니다. 위치는 이 구축에서 사용되는 모든 리소스(예: ASAv, 네트워크, 스토리지 어카운트)에서 동일해야 합니다.

h. **OK(확인)**를 클릭합니다.

5. Firepower Threat Defense Virtual의 초기 컨피그레이션을 완료합니다.

   a. 가상 머신 크기를 선택합니다.

   b. 스토리지 어카운트를 선택합니다.

      참고: 기존의 스토리지 어카운트를 사용하거나 새로운 어카운트를 생성할 수 있습니다. 스토리지 어카운트 이름에는 소문자와 숫자만 포함할 수 있습니다.

   c. **Name(이름)** 필드에 IP 주소의 레이블을 입력하여 공용 IP 주소를 요청한 다음 **OK(확인)**를 클릭합니다.

      참고: 이 단계에서 설정한 동적/정적 선택 사항과 관계없이 Azure는 동적 공용 IP 주소를 생성합니다. 공용 IP는 VM이 중지되었다가 재시작될 때 변경될 수 있습니다. 고정 IP 주소를 선호하는 경우 구축 후 생성한 공용 IP를 열고 동적 주소에서 정적 주소로 변경할 수 있습니다.

   d. 필요한 경우 DNS 레이블을 추가합니다.

      참고: FQDN(Fully Qualified Domain Name)은 DNS 레이블에 Azure URL을 더한 것입니다(예: <dnslabel>.<location>.cloudapp.azure.com).

   e. 기존의 가상 네트워크를 선택하거나 새로 생성합니다.

   f. Firepower Threat Defense Virtual 네트워크 인터페이스에 대해 4개의 서브넷을 구성합니다.

      - **FTDv 관리** 인터페이스는 "첫 번째 서브넷"에 연결됩니다.

      - **FTDv 진단** 인터페이스는 "두 번째 서브넷"에 연결됩니다.

      - **FTDv Gig0/0** 인터페이스는 "세 번째 서브넷"에 연결됩니다.

      - **FTDv Gig0/1** 인터페이스는 "네 번째 서브넷"에 연결됩니다.

   g. **OK(확인)**를 클릭합니다.

6. 컨피그레이션 요약을 확인한 다음 **OK(확인)**를 클릭합니다.
7. 이용 약관을 확인한 다음 **Purchase(구매)**를 클릭합니다.

   Azure에서 구축 시간은 다양합니다. Azure가 Firepower Threat Defense Virtual VM이 실행 중이라고 보고할 때까지 기다립니다.

향후 작업

- Azure에서 Firepower Threat Defense Virtual의 IP 컨피그레이션을 업데이트합니다.

공용 IP 주소 컨피그레이션 업데이트

절차

1. **Virtual Machine(가상 머신)** 목록에서 Firepower Threat Defense Virtual VM을 선택합니다.
2. **Overview(개요)**를 클릭합니다.
3. **Public IP address/DNS name label(공용 IP 주소/DNS 이름 레이블)** 아래에서 파란색 IP와 DNS 이름을 클릭합니다.
4. **Configuration(컨피그레이션)**을 클릭합니다.
   - IP 주소를 사용하여 연결하려면 할당의 **Static(정적)**을 선택합니다.
   - DNS 이름을 사용하여 연결하려면 DNS 이름 레이블을 입력합니다.
   - (선택사항) 편의를 위해 **Idle Timeout(유휴 시간 초과)**을 최대 범위인 30분으로 늘릴 수 있습니다. 이렇게 하면 관리 SSH 세션에서 시간이 너무 빨리 초과되는 것이 방지됩니다.
5. **Save(저장)**를 클릭합니다.

향후 작업

- 경우에 따라 데이터 인터페이스에 공용 IP 주소를 추가합니다.
- Firepower Management Center에서의 관리를 위해 Firepower Threat Defense Virtual을 구성합니다.

(선택사항) 데이터 인터페이스에 공용 IP 주소 추가

절차

1. **Virtual Machine(가상 머신)** 목록에서 Firepower Threat Defense Virtual VM을 선택합니다.
2. **Network interfaces(네트워크 인터페이스)**를 클릭합니다.
3. IP 주소를 추가할 데이터 인터페이스를 선택합니다.
   - Firepower Management Center에서 확인된 경우 Nic2(세 번째 NIC)가 GigabitEthernet0/0에 매핑됩니다. 이는 첫 번째 데이터 NIC입니다.
   - Firepower Management Center에서 확인된 경우 Nic3(네 번째 NIC)가 GigabitEthernet 0/1에 매핑됩니다. 이는 두 번째 데이터 NIC입니다.
4. **IP Configuration(IP 컨피그레이션)**을 클릭합니다.
5. **Add(추가)**를 클릭합니다.
6. 오른쪽에 있는 목록에서 **IPConfig-1**을 선택합니다.
7. **IPConfig-1** 컨피그레이션 블레이드에서 **Public IP address(공용 IP 주소)**를 **Enabled(활성화됨)**로 전환합니다.

8. **Create new(새로 생성)** 대화 상자를 사용하여 새 공용 IP 주소를 생성합니다.

   참고: 정적 또는 동적 IP 주소를 생성할 수 있습니다. 동적 IP 주소를 생성할 경우 IP 주소 대신 DNS 이름을 사용하여 항상 이 인터페이스에 액세스해야 합니다.

9. **OK(확인)**를 클릭합니다.

   컨피그레이션 변경이 처리될 때까지 기다린 다음 **Network interfaces(네트워크 인터페이스)** 목록을 검사하여 공용 IP 주소가 데이터 인터페이스에 추가되었는지 확인합니다.

   참고: 인터넷 트래픽이 데이터 인터페이스와 연결된 공용 IP 주소로 향하는 경우, 트래픽은 Azure 게이트웨이에서 대상 NATed가 되며 패킷의 새로운 대상 IP는 공용 IP와 연결된 Firepower Threat Defense Virtual 인터페이스의 개인 IP가 됩니다. Firepower Threat Defense Virtual은 대상 IP를 내부 서브넷에 있는 일부 리소스의 IP로 변환하기 위해 NAT로 구성해야 합니다.

10. **Save(저장)**를 클릭합니다.

향후 작업

- Firepower Management Center에서의 관리를 위해 Firepower Threat Defense Virtual을 구성합니다.

Firepower Management용 Firepower Threat Defense Virtual 구성

Firepower Threat Defense Virtual은 디바이스를 Firepower Management Center에 등록하는 데 필요한 네트워킹 정보를 사용하여 구성해야 합니다.

FMC가 Firepower Threat Defense Virtual을 디바이스로 추가할 수 있도록 구성하려면 **configure manager add** 명령을 사용하십시오. 디바이스를 Firepower Management Center에 등록하려면 항상 자체 생성된 고유한 영숫자 등록 키가 필요합니다. 등록 키는 사용자가 지정할 수 있는 간단한 키이며, 라이선스 키와는 다릅니다.

구내에서 Azure 가상 네트워크로 Express Route를 연결한 경우 Firepower Management Center의 IP 주소를 등록 키와 함께 제공할 수 있습니다. 예를 들면 다음과 같습니다.

```
configure manager add XXX.XXX.XXX.XXX my_reg_key
```

여기서 *XXX.XXX.XXX.XXX*는 관리하는 Firepower Management Center의 IP 주소이며 *my_reg_key*는 가상 디바이스의 사용자 정의 등록 키입니다.

그러나 공용 IP 주소를 사용하여 Firepower Threat Defense Virtual을 등록하려는 경우 고유한 NAT ID를 등록 키와 함께 입력하고 IP 주소 대신 DONTRESOLVE를 지정해야 합니다. 예를 들면 다음과 같습니다.

```
configure manager add DONTRESOLVE my_reg_key my_nat_id
```

여기서 *my_reg_key*는 사용자 정의 등록 키이며 *my_nat_id*는 가상 디바이스의 사용자 정의 NAT ID입니다.

절차

1. 공용 IP 주소를 사용하는 Firepower Threat Defense Virtual에 대한 SSH는 Azure에서 제공됩니다.
2. 사용자 이름 **admin** 및 비밀번호 **Admin123**으로 로그인합니다.
3. 화면에 표시되는 대로 컨피그레이션을 완료합니다.

   먼저 EULA(End User License Agreement, 최종 사용자 라이선스 계약)를 읽고 내용에 동의해야 합니다. 그런 다음 관리자 비밀번호를 변경하고 표시되는 프롬프트에 따라 관리 주소, DNS 설정 및 방화벽 모드(라우팅)를 구성합니다.
4. 기본 시스템 컨피그레이션이 처리될 때까지 기다립니다. 이 작업은 몇 분 정도 걸릴 수 있습니다.
5. **configure manager add** 명령을 사용하여 이 디바이스를 관리할 Firepower Management Center 어플라이언스를 식별합니다.

   > **configure manager add** {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} *reg_key* [*nat_id*]

참고: 등록 키는 사용자가 정의한 일회용 키로, 37자를 초과하지 않아야 합니다. 여기에는 영숫자(A–Z, a–z, 0–9)와 하이픈(-)을 사용할 수 있습니다. 디바이스를 Firepower Management Center에 추가할 때 이 등록 키를 기억해야 합니다.

Firepower Management Center의 주소를 직접 지정할 수 없으면 DONTRESOLVE를 사용합니다.

참고: NAT ID는 위에서 설명한 등록 키와 동일한 규칙을 따르는 선택적인 사용자 정의 영숫자 문자열입니다. 호스트 이름을 DONTRESOLVE로 설정하는 경우 반드시 필요합니다. 디바이스를 Firepower Management Center에 추가할 때 이 NAT ID를 기억해야 합니다.

Firepower Management Center의 IP 주소가 Azure에 대한 NATed가 될 가능성이 있습니다. NAT ID는 필수입니다. 예를 들면 다음과 같습니다.

```
configure manager add DONTRESOLVE 1234 ABCD
```

향후 작업

- Azure 보안 그룹을 업데이트합니다.

보안 그룹 업데이트

보안 그룹은 특정 인터페이스에 대해 허용/거부하는 포트/대상 Azure를 제어합니다. Firepower Threat Defense Virtual에 대한 SSH 액세스와 Firepower Management Center에서의 SSH 액세스를 확보하려면 VM의 기본 인터페이스에 있는 보안 그룹에 규칙을 추가해야 합니다. TCP 포트 22는 SSH에 필요하며 TCP 포트 8305는 등록 및 진단에 필요합니다.

절차

1. 새로 구축된 Firepower Threat Defense Virtual의 VM 정보 페이지를 엽니다.
2. **Network Interfaces(네트워크 인터페이스)**를 선택합니다.
3. **Nic0**을 선택합니다.
4. **Essentials(필수 사항)** 창에서 네트워크 보안 그룹을 찾습니다. 파란색 네트워크 보안 그룹 이름을 클릭합니다. 이름은 *<VM 이름>-SSH-SecurityGroup*과 유사한 규칙을 따라야 합니다.
5. **Inbound security rules(인바운드 보안 규칙)**를 클릭합니다.
6. 서비스 = SSH를 허용하는 SSH 규칙이 있는지 확인하고 없는 경우 규칙을 하나 추가합니다.

   SSH를 통해 Firepower Threat Defense Virtual에 연결할 때 사용할 것으로 예상하는 IP 주소로 소스 주소 범위를 제한하는 것이 좋습니다. 그렇지 않으면 SSH가 인터넷에 개방됩니다.
7. 다음과 같이 진단 인터페이스에 대한 보안 그룹 규칙을 추가합니다.
   a. Name(이름) - 인바운드 규칙 이름(예: *sf-tunnel*)
   b. Priority(우선 순위) - 기본값 유지
   c. Source(소스) - CIDR로 변경하고 Firepower Management Center가 전송되기 시작하는 서브넷을 입력
   d. Service(서비스) - Custom(맞춤설정)
   e. Protocol(프로토콜) - TCP
   f. Port range(포트 범위) - 8305
   g. Action(작업) - Allow(허용)
8. **OK(확인)**를 클릭합니다.

향후 작업

- Firepower Threat Defense Virtual을 Firepower Management Center에 등록합니다.

Firepower Management Center에 등록

첫 번째 인터페이스와 관리 서브넷의 보안 그룹이 Firepower Management Center 소스 주소의 모든 트래픽을 허용하는지 확인합니다. 이는 일반적으로 인터넷 연결 방화벽에서 풀의 주소입니다. 모든 트래픽은 일시적으로 허용할 수 있습니다. 그러나 Firepower Management Center의 연결이 시작되고 있는 IP 주소 블록을 발견하면 이러한 알려진 안전한 블록에서만 트래픽을 허용하도록 보안 그룹을 제한해야 합니다.

절차

시작하기 전에

- Firepower Threat Defense Virtual에는 스마트 소프트웨어 라이선싱이 필요하며 이는 Firepower Management Center에서 구성 가능합니다.
- 가상 어플라이언스의 시간 동기화 요구 사항을 결정합니다. 어플라이언스는 물리적 NTP 서버와 동기화하는 것이 좋습니다. 관리되는 디바이스를 가상 Firepower Management Center와 동기화하지 마십시오. 시간 동기화 요구 사항에 대해서는 Firepower Management Center 컨피그레이션 가이드를 참조하십시오.

절차

1. 호스트 이름 또는 구성된 Firepower Management Center의 주소를 사용하여 브라우저에서 HTTPS 연결을 사용하는 Firepower Management Center에 로그인합니다. 구성된 주소의 예는 https://MC.example.com과 같습니다.
2. Management Center에 대한 웹 인터페이스에서 **Devices(디바이스)** > **Device Management(디바이스 관리)**를 선택합니다.
3. **Add(추가)** 드롭다운 목록에서 **Add Device(디바이스 추가)**를 선택합니다.
4. **Host(호스트)** 필드에서 다음 작업을 수행합니다.
   a. 공용 IP 주소를 사용하는 인터넷을 통해 연결하려면 Firepower Threat Defense Virtual의 관리 인터페이스에 연결된 공용 IP를 입력합니다.
   b. Azure ExpressRoute를 통해 연결하려면 Firepower Threat Defense Virtual의 관리 인터페이스에 연결된 개인 IP를 입력합니다.
5. **Display Name(이름 표시)** 필드에 Management Center에서 표시하고 싶은 대로 보안 모듈의 이름을 입력합니다.
6. **Registration Key(등록 키)** 필드에 Firepower Management용 Firepower Threat Defense Virtual을 구성했을 때 사용한 것과 동일한 등록 키를 입력합니다.
7. 다중 도메인 환경에서 디바이스를 추가 중인 경우 **Domain(도메인)** 드롭다운 목록에서 값을 선택하여 디바이스를 리프 도메인에 할당합니다.

   현재 도메인이 리프 도메인인 경우 디바이스는 현재 도메인에 자동으로 추가됩니다.
8. 경우에 따라 디바이스를 디바이스 **Group(그룹)**에 추가합니다.
9. **Access Control Policy(액세스 제어 정책)** 드롭다운 목록에서 보안 모듈에 구축할 초기 컨피그레이션을 선택합니다.
   - **Default Access Control(기본 액세스 제어)** 정책은 모든 트래픽이 네트워크로 들어오는 것을 차단합니다.
   - **Default Intrusion Prevention(기본 침입 방지)** 정책은 균형 보안 및 연결 침입 정책에 의해서도 전달되는 모든 트래픽을 허용합니다.
   - **Default Network Discovery(기본 네트워크 검색)** 정책은 모든 트래픽을 허용하며, 이때 트래픽은 네트워크 검색만 사용하여 검사됩니다.
   - 어떠한 기존 사용자 정의 액세스 제어 정책이든 선택할 수 있습니다. 자세한 내용은 *Firepower Management Center 컨피그레이션 가이드*에서 "액세스 제어 정책 관리"를 참조하십시오.

10. 디바이스에 적용할 라이선스를 선택합니다.

    참고: 제어, 악성코드 및 URL 필터링 라이선스에는 보호 라이선스가 필요합니다. 자세한 내용은 Firepower Management Center 컨피그레이션 가이드를 참조하십시오.

11. 디바이스를 Firepower Management Center에서 관리하도록 구성할 때 디바이스를 식별하기 위해 NAT ID를 사용한 경우 **Advanced(고급)** 섹션을 펼치고 Unique NAT ID(고유한 NAT ID) 필드에 동일한 NAT ID를 입력합니다.

    참고: 관리 공용 IP를 사용하는 인터넷을 통해 Firepower Threat Defense Virtual에 연결할 경우 NAT ID를 사용해야 합니다. Azure ExpressRoute를 통해 연결하는 경우 NAT ID를 사용할 필요가 없습니다.

12. **Register(등록)**를 클릭하여 등록에 성공했는지 확인합니다.

    Firepower Management Center가 디바이스의 하트비트를 확인하고 통신을 설정하려면 최대 2분이 걸릴 수 있습니다.

향후 작업

- 두 개의 데이터 인터페이스를 활성화 및 구성합니다.

디바이스 설정 구성

Firepower Threat Defense Virtual을 관리하는 Firepower Management Center에 등록한 후에는 두 개의 데이터 인터페이스를 활성화 및 구성해야 합니다.

절차

1. **Devices(디바이스)** > **Device Management(디바이스 관리)**를 선택합니다.
2. 인터페이스를 구성하려는 Firepower Threat Defense Virtual 디바이스 옆의 편집 아이콘을 클릭합니다.

   다중 도메인 구축 시 리프 도메인에 있지 않은 경우 전환하라는 프롬프트가 표시됩니다.
3. GigabitEthernet0/0 인터페이스 옆에 있는 편집 아이콘을 클릭합니다.
   a. **Mode(모드)** 드롭다운 목록에서 **None(없음)**을 선택하여 인터페이스를 라우팅 모드로 남겨둡니다.
   b. **IPv4** 탭을 클릭하여 해당 **IP Address(IP 주소)**가 Azure에서 구축 시 인터페이스에 부여된 주소와 일치하는지 확인합니다.
   c. **OK(확인)**를 클릭합니다.
4. GigabitEthernet0/1 인터페이스에 대해서도 동일한 단계를 반복합니다.
5. **Save(저장)**를 클릭합니다.

향후 작업

- Firepower Management Center 사용자 인터페이스를 사용하여 액세스 제어 정책 및 기타 관련된 정책을 구성 및 적용하여 Firepower Threat Defense Virtual 인스턴스를 사용하는 트래픽을 관리할 수 있습니다. *Firepower Management Center 컨피그레이션 가이드* 또는 온라인 도움말을 참조하십시오 .