Firepower Threat Defense Virtual 및 AWS 시작하기

Amazon VPC(Amazon Virtual Private Cloud)를 통해 사용자가 정의한 가상 네트워크에서 AWS(Amazon Web Services) 리소스를 실행할 수 있습니다. 자체 데이터 센터에서 운영할 수 있는 기존 네트워크와 매우 유사한 이 가상 네트워크는 확장 가능한 AWS 인프라 사용 시의 이점도 제공합니다.

이 문서에서는 AWS에 Firepower Threat Defense Virtual을 구축하는 방법을 설명합니다.

- FTDv 및 AWS 클라우드, 1 페이지
- Firepower 디바이스 관리 방법, 2 페이지
- AWS 솔루션 개요, on page 3
- Firepower Threat Defense Virtual 사전 요건, on page 3
- 지원되는 기능 및 제한 사항, on page 4
- AWS 환경 구성, on page 5

FTDv 및 AWS 클라우드

AWS는 퍼블릭 클라우드 환경입니다. Firepower Threat Defense Virtual은 다음 인스턴스 유형의 AWS 환경에서 게스트로 실행됩니다.

참고 Firepower 버전 6.6에서는 다음 표에 나와 있는 C5 인스턴스 유형에 대한 지원이 추가되었습니다. 인스턴스 유형이 클수록 AWS VM에 더 많은 CPU 리소스를 제공하여 성능을 높이고 일부는 더 많은 네트워크 인터페이스를 허용합니다.

표 *1: FTDv*에 대한 *AWS* 지원 인스턴스

인스턴스 유형	**vCPU**	메모리**(RAM)**	**vNics**
C5.xlarge	4	8GB	4
C5.2xlarge	8	16GB	4

인스턴스 유형	**vCPU**	메모리**(RAM)**	**vNics**
C5.4xlarge	16	32GB	8
C4.xlarge	4	7.5GB	4
C3.xlarge	4	7.5GB	4

Firepower 디바이스 관리 방법

두 가지 옵션을 통해 Firepower Threat Defense 디바이스를 관리할 수 있습니다.

Firepower Device Manager

Firepower Device Manager(FDM) 온보드 통합 관리자.

FDM은(는) 일부 Firepower Threat Defense 디바이스에 포함된 웹 기반 구성 인터페이스입니다. FDM은(는) 소규모 네트워크에서 가장 흔히 사용되는 소프트웨어의 기본 기능을 구성하도록 합니다. Firepower Device Manager는 디바이스를 하나 또는 몇 개만 포함하는 네트워크 용도로 특별히 설계되어 고성능 다중 디바이스 관리자를 사용해 여러 Firepower Threat Defense 디바이스가 포함된 대규모 네트워크를 제어하기를 원하지 않을 경우에 유용합니다.

참고 FDM을 지원하는 Firepower Threat Defense 디바이스 목록은 Firepower Device Manager용 Cisco Firepower Threat Defense 구성 가이드을 참조하십시오.

Firepower Management Center

Cisco Firepower Management Center(FMC)

다수의 디바이스를 관리하거나 Firepower Threat Defense에서 허용하는 더 복잡한 기능 및 구성을 사용하려는 경우에는 통합형 FDM 대신 FMC을(를) 사용하여 디바이스를 구성하십시오.

중요 Firepower 디바이스를 관리할 때 FDM와(과) FMC을(를) 동시에 사용할 수 없습니다. FDM 통합 관리가 활성화되면 로컬 관리를 사용하지 않도록 설정하고 FMC을(를) 사용하도록 재구성하기 전에는 FMC을(를) 사용해 Firepower 디바이스를 관리할 수 없습니다. 반면 FMC에 Firepower 디바이스를 등록하면 FDM 온보드 관리 서비스가 비활성화됩니다.

주의 현재 Cisco에는 FDM Firepower 구성을 FMC로, 또는 그 반대로 마이그레이션할 수 있는 옵션이 없습니다. Firepower 디바이스를 구성할 때는 이를 고려해 관리 유형을 선택해야 합니다.

AWS 솔루션 개요

AWS는 클라우드 컴퓨팅 플랫폼을 구성하는 원격 컴퓨팅 서비스(웹 서비스라고도 함) 컬렉션으로 Amazon.com에서 제공합니다. 이러한 서비스는 전 세계 11개 지역에서 운영됩니다. Firepower Management Center Virtual 및 Firepower Threat Defense Virtual을 구축할 때는 일반적으로 다음의 AWS 서비스를 숙지해야 합니다.

- Amazon EC2(Elastic Compute Cloud) - Amazon의 데이터 센터에서 방화벽 등의 자체 애플리케이션 및 서비스를 실행하고 관리하기 위한 가상 컴퓨터를 임대할 수 있는 웹 서비스입니다.
- Amazon VPC(Virtual Private Cloud) - Amazon 퍼블릭 클라우드 내에 격리된 프라이빗 네트워크를 구성하는 데 사용할 수 있는 웹 서비스입니다. EC2 인스턴스는 VPC 내에서 실행할 수 있습니다.
- Amazon S3(Simple Storage Service) - 데이터 스토리지 인프라를 제공하는 웹 서비스입니다.

AWS에서 어카운트를 생성하고, AWS 마법사 또는 수동 컨피그레이션을 사용하여 VPC 및 EC2 구성 요소를 설정하고, AMI(Amazon Machine Image) 인스턴스를 선택합니다. AMI는 인스턴스 실행에 필요한 소프트웨어 컨피그레이션을 포함한 템플릿입니다.

Note AMI 이미지는 AWS 환경이 아닌 곳에서 다운로드할 수 없습니다.

Firepower Threat Defense Virtual 사전 요건

- Amazon 어카운트는 http://aws.amazon.com/에서 생성할 수 있습니다.
- FTDv 콘솔에 액세스하려면 SSH 클라이언트(예: Windows의 PuTTY 또는 Macintosh의 터미널)가 필요합니다.
- Cisco Smart Account는 Cisco Software Central에서 생성할 수 있습니다. https://software.cisco.com/
- Firepower Threat Defense Virtual 라이선스
  - Firepower Management Center의 보안 서비스에 대해 모든 라이선스 권한을 구성합니다.
  - 라이선스를 관리하는 방법에 대한 자세한 내용은 Firepower Management Center 컨피그레이션 가이드의 "Firepower System 라이선싱"을 참조하십시오.
- Firepower Threat Defense Virtual 인터페이스 요구 사항:
  - 관리 인터페이스(2 - 첫째는 Firepower Threat Defense Virtual을 Firepower Management Center에 연결하는 데 사용되고, 둘째는 진단용으로 사용되며, 통과 트래픽에는 사용할 수 없습니다.

    6.7 이상 버전에서는 선택적으로 관리 인터페이스 대신 FMC 관리용 데이터 인터페이스를 구성할 수 있습니다. 관리 인터페이스는 데이터 인터페이스 관리를 위한 전제 조건이므로 초기 설정에서 구성해야합니다. 데이터 인터페이스에서의 FMC 액세스는 고 가용성 구축에

서 지원되지 않습니다. FMC 액세스를 위한 데이터 인터페이스 구성에 대한 자세한 내용은 FTD command reference에서 **configure network management-data-interface** 명령을 참조하십시오.

- 트래픽 인터페이스 (2) - Firepower Threat Defense Virtual을 내부 호스트 및 공용 네트워크에 연결하는 데 사용됩니다.

- 통신 경로:
  - Firepower Threat Defense Virtual 액세스를 위한 Public/elastic IP

지원되는 기능 및 제한 사항

지원 기능

- VPC(Virtual Private Cloud)에 구축
- 확장 네트워킹(SR-IOV) - 사용 가능한 경우
- Amazon Marketplace에서 구축
- 인스턴스당 최대 4개의 vCPU
- L3 네트워크의 사용자 구축
- 라우팅 모드(기본값)
- ERSPAN을 통한 패시브 모드

Firepower Threat Defense Virtual 제한 사항

- c4.xlarge가 권장되는 인스턴스입니다. c3.xlarge 인스턴스는 AWS 지역 전체에서 가용성이 제한됩니다.
- 시작하는 동안 2개의 관리 인터페이스를 구성해야 합니다.
- 시작하려면 트래픽 인터페이스 2개와 관리 인터페이스 2개, 즉 총 4개의 인터페이스가 있어야 합니다.

Note Firepower Threat Defense Virtual은 4개의 인터페이스 없이는 실행되지 않습니다.

- AWS에서 트래픽 인터페이스를 구성할 때는“Change Source / Dest. Check” 옵션을 선택해제해야 합니다.

- 모든 IP 주소 컨피그레이션(CLI 또는 Firepower Management Center의 컨피그레이션)은 AWS 콘솔에서 생성된 컨피그레이션과 일치해야 하며, 구축 중에 컨피그레이션 정보를 적어 두어야 합니다.
- Firepower Threat Defense Virtual을 등록한 후에는 인터페이스를 수정하여 Firepower Management Center에서 활성화해야 합니다. IP 주소는 AWS에서 구성한 인터페이스와 일치해야 합니다.
- IPv6은 현재 지원되지 않습니다.
- 투명 / 인라인 / 패시브 모드는 현재 지원되지 않습니다.
- 인터페이스를 수정하려면 AWS 콘솔에서 변경해야 합니다.
  - Firepower Management Center에서 등록 해제
  - AWS AMI 사용자 인터페이스를 통해 인스턴스를 중지합니다.
  - AWS AMI 사용자 인터페이스를 통해 변경하려는 인터페이스를 분리합니다.
  - 새 인터페이스를 연결합니다(시작하려면 트래픽 인터페이스 2개와 관리 인터페이스 2개가 있어야 합니다).
  - AWS AMI 사용자 인터페이스를 통해 인스턴스를 시작합니다.
  - Firepower Management Center에 재등록합니다.
  - Firepower Management Center에서 디바이스 인터페이스를 수정하고 AWS 콘솔을 통해 변경한 내용과 일치하도록 IP 주소 및 기타 매개 변수를 수정합니다.
- 부팅 후에는 인터페이스를 추가할 수 없습니다.
- 복제/스냅샷은 현재 지원되지 않습니다.

AWS 환경 구성

AWS에 Firepower Threat Defense Virtual을 구축하려면 구축 관련 요구 사항과 설정을 사용하여 Amazon VPC를 구성해야 합니다. 대부분의 상황에서는 설정 마법사가 설정 과정을 안내합니다. AWS는 소개 정보에서 고급 기능에 이르기까지 서비스와 관련한 여러 가지 유용한 정보를 찾을 수 있는 온라인 설명서를 제공합니다. 자세한 내용은 https://aws.amazon.com/documentation/gettingstarted/를 참조하십시오.

AWS 설정을 더 세부적으로 제어할 수 있도록 Firepower Threat Defense Virtual 인스턴스를 실행하기 전에 다음과 같은 섹션에서 VPC 및 EC2 구성을 안내합니다.

- VPC 생성, on page 6
- 인터넷 게이트웨이 추가, on page 6
- 서브넷 추가, on page 7
- 라우트 테이블 추가, on page 8
- 보안 그룹 생성, on page 9
- 네트워크 인터페이스 생성, on page 9

- 탄력적 IP 생성, on page 10

시작하기 전에

- AWS 어카운트를 생성합니다.
- Firepower Threat Defense Virtual 인스턴스에 AMI를 사용할 수 있는지 확인합니다.

VPC 생성

VPC(Virtual Private Cloud)는 AWS 어카운트 전용 가상 네트워크이며, AWS Cloud의 다른 가상 네트워크와 논리적으로 격리되어 있습니다. Firepower Threat Defense Virtual 인스턴스 등의 AWS 리소스를 VPC에서 실행할 수 있습니다. VPC의 IP 주소 범위를 선택하고, 서브넷을 생성하고, 라우트 테이블, 네트워크 게이트웨이, 보안 설정을 구성하여 VPC를 구성할 수 있습니다.

Procedure

단계 **1** http://aws.amazon.com/에 로그인하고 지역을 선택합니다.

AWS는 여러 지역으로 나뉘며, 이 지역은 상호 격리되어 있습니다. 화면의 우측 상단에 지역이 표시됩니다. 한 지역의 리소스가 다른 지역에는 나타나지 않습니다. 원하는 지역에 있는지 정기적으로 확인합니다.

단계 **2** **Services(**서비스**)** > **VPC**를 클릭합니다.

단계 **3** **VPC Dashboard(VPC** 대시보드**)** > 사용자 **VPC**를 클릭합니다.

단계 **4** **Create VPC(VPC** 생성**)**를 클릭합니다.

단계 **5** **Create VPC(VPC** 생성**)** 대화 상자에 다음 정보를 입력합니다.

a) VPC를 식별하기 위한 사용자 정의 **Name tag(**이름 태그**)**.

b) IP 주소의 **CIDR block(CIDR** 블록**)**. CIDR(Classless Inter-Domain Routing) 표기법은 IP 주소와 관련 라우팅 접두사를 축약한 표현입니다. 예를 들면 10.0.0.0/24와 같습니다.

c) **Tenancy(**테넌시**)** 설정을 Default(기본값)로 설정하면 이 VPC에서 실행되는 인스턴스가 실행 시에 지정된 테넌시 특성을 사용합니다.

단계 **6** VPC를 생성하려면 **Yes, Create(**예**,** 생성합니다**)**를 클릭합니다.

What to do next

다음 섹션의 설명에 따라 VPC에 인터넷 게이트웨이를 추가합니다.

인터넷 게이트웨이 추가

VPC를 인터넷에 연결하기 위해 인터넷 게이트웨이를 추가할 수 있습니다. VPC 외부의 IP 주소에 대한 트래픽을 인터넷 게이트웨이로 라우팅할 수 있습니다.

시작하기 전에

- Firepower Threat Defense Virtual 인스턴스용으로 VPC를 생성합니다.

Procedure

단계 **1** **Services(**서비스**) > VPC**를 클릭합니다.

단계 **2** **VPC Dashboard(VPC** 대시보드**) > Internet Gateways(**인터넷 게이트웨이**)**를 클릭하고 **Create Internet Gateway(**인터넷 게이트웨이 생성**)**를 클릭합니다.

단계 **3** 게이트웨이 식별을 위한 사용자 정의 **Name tag(**이름 태그**)**를 입력한 후, 게이트웨이를 생성하려면 **Yes, Create(**예**,** 생성합니다**)**를 클릭합니다.

단계 **4** 이전 단계에서 생성한 게이트웨이를 선택합니다.

단계 **5** **Attach to VPC(VPC**에 연결**)**를 클릭하고 이전에 생성한 VPC를 선택합니다.

단계 **6** VPC에 게이트웨이를 연결하려면 **Yes, Attach(**예**,** 연결합니다**)**를 클릭합니다.

기본적으로 VPC에서 실행되는 인스턴스는 게이트웨이를 생성하여 VPC에 연결할 때까지 인터넷과 통신할 수 없습니다.

What to do next

다음 섹션의 설명에 따라 VPC에 서브넷을 추가합니다.

서브넷 추가

Firepower Threat Defense Virtual 인스턴스를 연결할 수 있는 VPC의 IP 주소 범위를 세그먼트로 지정할 수 있습니다. 보안 및 운영 요구 사항에 따라 서브넷을 생성하여 인스턴스를 그룹화할 수 있습니다. Firepower Threat Defense Virtual의 경우에는 트래픽용 서브넷과 관리용 서브넷을 모두 생성해야 합니다.

시작하기 전에

- Firepower Threat Defense Virtual 인스턴스용으로 VPC를 생성합니다.

Procedure

단계 **1** **Services(**서비스**) > VPC**를 클릭합니다.

단계 **2** **VPC Dashboard(VPC** 대시보드**) > Subnets(**서브넷**)**를 클릭하고 **Create Subnet(**서브넷 생성**)**을 클릭합니다.

단계 **3** **Create Subnet(**서브넷 생성**)** 대화 상자에 다음 정보를 입력합니다.

a) 서브넷을 식별하기 위한 사용자 정의 **Name tag(**이름 태그**)**.

b) 이 서브넷에 사용할 **VPC**.

c) 이 서브넷이 상주할 **Availability Zone(**가용성 영역**)**. Amazon이 해당 영역을 선택할 수 있게 하려면 **No Preference(**환경 설정 없음**)**를 선택합니다.
d) IP 주소의 **CIDR block(CIDR** 블록**)**. 서브넷의 IP 주소 범위는 VPC의 IP 주소 범위의 하위 집합이어야 합니다. 블록 크기는 /16 네트워크 마스크와 /28 네트워크 마스크 사이여야 합니다. 서브넷의 크기는 VPC의 크기와 같아도 됩니다.

단계 **4** 서브넷을 생성하려면 **Yes, Create(**예**,** 생성합니다**)**를 클릭합니다.

단계 **5** 필요한 서브넷 수만큼 위의 단계를 반복합니다. 관리 트래픽용으로 별도의 서브넷을 생성하고, 데이터 트래픽용으로 필요한 수만큼의 서브넷을 생성합니다.

What to do next

다음 섹션의 설명에 따라 VPC에 라우트 테이블을 추가합니다.

라우트 테이블 추가

VPC용으로 구성한 게이트웨이에 라우트 테이블을 연결할 수 있습니다. 여러 서브넷을 단일 라우트 테이블과 연결할 수는 있지만, 각 서브넷은 한 번에 하나의 라우트 테이블에만 연결할 수 있습니다.

Procedure

단계 **1** **Services(**서비스**) > VPC**를 클릭합니다.

단계 **2** **VPC Dashboard(VPC** 대시보드**) > Route Tables(**라우트 테이블**)**를 클릭하고 **Create Route Tables(**라우트 테이블 생성**)**를 클릭합니다.

단계 **3** 라우트 테이블 식별을 위한 사용자 정의 **Name tag(**이름 태그**)**를 입력합니다.

단계 **4** 드롭다운 목록에서 이 라우트 테이블을 사용할 **VPC**를 선택합니다.

단계 **5** 라우트 테이블을 생성하려면 **Yes, Create(**예**,** 생성합니다**)**를 클릭합니다.

단계 **6** 방금 생성한 라우트 테이블을 선택합니다.

단계 **7** **Routes(**라우트**)** 탭을 클릭하여 상세 정보 창에 라우트 정보를 표시합니다.

단계 **8** **Edit(**수정**)**, **Add another route(**다른 라우트 추가**)**를 차례로 클릭합니다.

a) **Destination(**대상**)** 열에 **0.0.0.0/0**을 입력합니다.
b) **Target(**대상**)** 열에서 게이트웨이를 선택합니다.

단계 **9** **Save(**저장**)**를 클릭합니다.

What to do next

다음 섹션의 설명에 따라 보안 그룹을 생성합니다.

보안 그룹 생성

허용되는 프로토콜, 포트 및 소스 IP 범위를 지정하는 규칙을 사용하여 보안 그룹을 생성할 수 있습니다. 각 인스턴스에 할당할 수 있는 각기 다른 규칙을 사용해 여러 보안 그룹을 생성할 수 있습니다.

Procedure

단계 **1** **Services(**서비스**) > EC2**를 클릭합니다.

단계 **2** **EC2 Dashboard(EC2** 대시보드**) > Security Groups(**보안 그룹**)**를 클릭합니다.

단계 **3** **Create Security Group(**보안 그룹 생성**)**을 클릭합니다.

단계 **4** 다음을 보안 그룹 생성 대화 상자에 입력합니다.

a) 보안 그룹 식별을 위한 사용자 정의 **Security group name(**보안 그룹 이름**)**.

b) 이 보안 그룹에 대한 **Description(**설명**)**.

c) 이 보안 그룹과 연결된 **VPC**.

단계 **5** **Security group rules(**보안 그룹 규칙**)**를 구성합니다.

a) **Inbound(**인바운드**)** 탭을 클릭하고 **Add Rule(**규칙 추가**)**을 클릭합니다.

Note 외부 AWS에서 Firepower Management Center Virtual을 관리하려면 HTTPS 및 SSH 액세스가 필요합니다. 이에 따라 소스 IP 주소를 지정해야 합니다. 또한 AWS VPC 내에 Firepower Management Center Virtual과 Firepower Threat Defense Virtual을 모두 구성할 경우에는 개인 IP 관리 서브넷 액세스를 허용해야 합니다.

b) **Outbound(**아웃바운드**)** 탭을 클릭한 다음, **Add Rule(**규칙 추가**)**을 클릭하여 아웃바운드 트래픽용 규칙을 추가하거나, 기본값인 **All traffic(**모든 트래픽**)(Type(**유형**)**의 경우) 및 **Anywhere(**모든 위치**)(Destination(**대상**)**의 경우)를 그대로 유지합니다.

단계 **6** 보안 그룹을 생성하려면 **Create(**생성**)**를 클릭합니다.

What to do next

다음 섹션의 설명에 따라 네트워크 인터페이스를 생성합니다.

네트워크 인터페이스 생성

고정 IP 주소를 사용하여 Firepower Threat Defense Virtual용 네트워크 인터페이스를 생성할 수 있습니다. 특정 구축에 필요한 만큼 네트워크 인터페이스(외부 및 내부)를 생성합니다.

Procedure

단계 **1** **Services(**서비스**) > EC2**를 클릭합니다.

단계 **2** **EC2 Dashboard(EC2** 대시보드**) > Network Interfaces(**네트워크 인터페이스**)**를 클릭합니다.

단계 **3** **Create Network Interface(**네트워크 인터페이스 생성**)**를 클릭합니다.

단계 **4** **Create Network Interface(**네트워크 인터페이스 생성**)** 대화 상자에 다음 정보를 입력합니다.

a) 네트워크 인터페이스에 대한 사용자 정의 **Description(**설명**)**(선택 사항)

b) 드롭다운 목록에서 **Subnet(**서브넷**)**을 선택합니다. Firepower Threat Defense Virtual 인스턴스를 생성할 VPC의 서브넷을 선택해야 합니다.

c) **Private IP(**개인 **IP)** 주소를 입력합니다. **auto-assign(**자동 할당**)**보다는 고정 IP 주소를 사용하는 것이 좋습니다.

d) 하나 이상의 **Security groups(**보안 그룹**)**를 선택합니다. 보안 그룹의 필수 포트가 모두 열려 있는지 확인합니다.

단계 **5** 네트워크 인터페이스를 생성하려면 **Yes, Create(**예**,** 생성합니다**)**를 클릭합니다.

단계 **6** 방금 생성한 네트워크 인터페이스를 선택합니다.

단계 **7** 마우스 오른쪽 버튼을 클릭하고 **Change Source/Dest. Check(**소스/대상 확인 변경**)** 를 선택합니다.

단계 **8** **Edit(**수정**)**, **Add another route(**다른 라우트 추가**)**를 차례로 클릭합니다.

단계 **9** **Disable(**비활성화**)**을 선택합니다. 생성하는 모든 네트워크 인터페이스에 대해 이 단계를 반복합니다.

What to do next

다음 섹션의 설명에 따라 탄력적 IP 주소를 생성합니다.

탄력적 IP 생성

인스턴스를 생성하면 공용 IP 주소가 인스턴스와 연결됩니다. 해당 공용 IP 주소는 인스턴스를 중지하고 시작할 때 자동으로 변경됩니다. 이 문제를 해결하려면 탄력적 IP 주소를 사용하여 인스턴스에 영구적 공용 IP 주소를 할당합니다. 탄력적 IP는 Firepower Threat Defense Virtual 및 기타 인스턴스의 원격 액세스에 사용되는 예약된 공용 IP입니다.

Note 최소한 Firepower Threat Defense Virtual 관리 및 진단 인터페이스용으로 탄력적 IP 주소를 생성할 수 있습니다.

Procedure

단계 **1** **Services(**서비스**) > EC2**를 클릭합니다.

단계 **2** **EC2 Dashboard(EC2** 대시보드**) > Elastic IPs(**탄력적 **IP)**를 클릭합니다.

단계 **3** **Allocate New Address(**새 주소 할당**)**를 클릭합니다.

단계 **4** 필요한 수만큼의 탄력적/공용 IP에 대해 이 단계를 반복합니다.

단계 **5** 탄력적 IP를 생성하려면 **Yes, Allocate(**예**,** 할당합니다**)**를 클릭합니다.

단계 **6** 구축에 필요한 탄력적 IP 수만큼 위의 단계를 반복합니다.

What to do next

다음 섹션에 설명된 Firepower Threat Defense Virtual 구축