AWS 클라우드에 ASA 가상 구축

AWS(Amazon Web Sources) 클라우드에 ASA 가상을 구축할 수 있습니다.

중요 9.13(1)부터 모든 ASA 가상 라이선스는 지원되는 모든 ASA 가상 vCPU/메모리 구성에서 사용할 수 있습니다. 따라서 ASA 가상 고객은 다양한 VM 리소스 사용 공간에서 실행할 수 있습니다. 또한 지원되는 AWS 인스턴스 유형의 수가 증가합니다.

AWS Cloud에 ASA 가상 구축 정보

ASA 가상은 물리적 ASA 와 동일한 소프트웨어를 실행하여 가상 폼 팩터에서 검증된 보안 기능을 제공합니다. ASA 가상은 퍼블릭 AWS 클라우드에 구축할 수 있습니다. 그러면 시간이 경과함에 따라 해당 위치를 확장, 축소 또는 이동하는 가상 및 물리적 데이터 센터 워크로드를 보호하기 위한 구성이 가능하게 됩니다.

ASA 가상은 다음 AWS 인스턴스 유형을 지원합니다.

표 ***1: AWS*** 지원 인스턴스 유형

Instance	특성		인터페이스
	vCPUs	메모리**(GB)**	
c5.xlarge	4	8	4
c5.2xlarge	8	16	4

Instance	특성		인터페이스
	vCPUs	메모리(GB)	
c4.large	2	3.75	3
c4.xlarge	4	7.5	4
c4.2xlarge	8	15	4
c3.large	2	3.75	3
c3.xlarge	4	7.5	4
c3.2xlarge	8	15	4
m4.large	2	4	3
m4.xlarge	4	16	4
m4.2xlarge	8	32	4
c5a.large	2	4	3
c5a.xlarge	4	8	4
c5a.2xlarge	8	16	4
c5a.4xlarge	16	32	8
c5ad.large	2	4	3
c5ad.xlarge	4	8	4
c5ad.2xlarge	8	16	4
c5ad.4xlarge	16	32	8
c5d.large	2	4	3
c5d.xlarge	4	8	4
c5d.2xlarge	8	16	4
c5d.4xlarge	16	32	8
g4ad.4xlarge	16	64	3
g4dn.xlarge	4	16	3
g4dn.2xlarge	8	32	3
g4dn.4xlarge	16	64	3
i3en.large	2	16	3
i3en.xlarge	4	32	4
i3en.2xlarge	8	64	4
i3en.3xlarge	12	96	4

Instance	특성		인터페이스
	vCPUs	메모리(GB)	
inf1.xlarge	4	8	4
inf1.2xlarge	8	16	4
m5.large	2	8	3
m5.xlarge	4	16	4
m5.2.xlarge	8	32	4
m5.4xlarge	16	64	8
m5a.large	2	8	3
m5a.xlarge	4	16	4
m5a.2xlarge	8	32	4
m5a.4xlarge	16	64	8
m5ad.large	2	8	3
m5ad.xlarge	4	16	4
m5ad.2xlarge	8	32	4
m5ad.4xlarge	16	64	8
m5d.large	2	8	3
m5d.xlarge	4	16	4
m5d.2xlarge	8	32	4
m5d.4xlarge	16	64	8
m5dn.xlarge	2	8	3
m5dn.xlarge	4	16	4
m5dn.2xlarge	8	32	4
m5dn.4xlarge	16	64	8
m5n.large	2	8	3
m5n.xlarge	4	16	4
m5n.2xlarge	8	32	4
m5n.4xlarge	16	64	8
m5zn.large	2	8	3
m5zn.xlarge	4	16	4
m5zn.2xlarge	8	32	4
m5zn.3xlarge	12	48	8
r5.large	2	16	3

Instance	특성		인터페이스
	vCPUs	메모리(GB)	
r5.xlarge	4	32	4
r5.2.xlarge	8	64	4
r5.4xlarge	16	128	8
r5a.large	2	16	3
r5a.xlarge	4	32	4
r5a.2xlarge	8	64	4
r5a.4xlarge	16	128	8
r5ad.large	2	16	3
r5ad.xlarge	4	32	4
r5ad.2xlarge	8	64	4
r5ad.4xlarge	16	128	8
r5b.large	2	16	3
r5b.xlarge	4	32	4
r5b.2xlarge	8	64	4
r5b.4xlarge	16	128	8
r5d.large	2	16	3
r5d.xlarge	4	32	4
r5d.2xlarge	8	64	4
r5d.4xlarge	16	128	8
r5dn.large	2	16	3
r5dn.xlarge	4	32	4
r5dn.2xlarge	8	64	4
r5dn.4xlarge	16	128	8
r5n.large	2	16	3
r5n.xlarge	4	32	4
r5n.2xlarge	8	64	4
r5n.4xlarge	16	128	8
z1d.large	2	16	3
z1d.xlarge	4	32	4
z1d.2xlarge	8	64	4
z1d.3xlarge	12	96	8

팁 M4 또는 C4 인스턴스 유형을 사용하는 경우, 성능 향상을 위해 Nitro 하이퍼바이저 및 ENA(Elastic Network Adapter) 인터페이스 드라이버를 사용하는 C5 또는 M5 인스턴스 유형으로 마이그레이션하는 것이 좋습니다.

AWS에서 계정을 생성하고, AWS 마법사를 사용하여 ASA 가상을 설정하고, AMI(Amazon Machine Image)를 선택합니다. AMI는 인스턴스 실행에 필요한 소프트웨어 컨피그레이션을 포함한 템플릿입니다.

중요 AMI 이미지는 AWS 환경이 아닌 곳에서 다운로드할 수 없습니다.

ASA 가상 및 AWS 사전 요건

- aws.amazon.com에서 계정을 생성합니다.
- ASA 가상에 라이선스를 부여합니다. ASA 가상 라이선스를 등록하기 전에는 저성능 모드에서 실행됩니다. 이 모드에서는 100개의 연결 및 100Kbps의 처리량만 허용됩니다. ASA 가상에 대한 라이선싱의 내용을 참조하십시오.
- 인터페이스 요건:
  - 관리 인터페이스
  - 내부 및 외부 인터페이스
  - (선택 사항) 추가 서브넷(DMZ)
- 통신 경로:
  - 관리 인터페이스 - ASA 가상을 ASDM에 연결할 때 사용합니다. 통과 트래픽에는 사용할 수 없습니다.
  - 내부 인터페이스(필수)—ASA 가상를 내부 호스트에 연결하는 데 사용합니다.
  - 외부 인터페이스(필수)—ASA 가상를 공용 네트워크에 연결하는 데 사용합니다.
  - DMZ 인터페이스(선택 사항)—c3.xlarge 인터페이스 사용 시 ASA 가상을 DMZ 네트워크에 연결하는 데 사용합니다.
- ASA 가상 시스템 요구 사항은 Cisco Secure Firewall ASA호환성을 참조하십시오.

ASA 가상 및 AWS에 대한 지침과 제한 사항

지원 기능

AWS의 ASA 가상은 다음 기능을 지원합니다.

- Amazon EC2 컴퓨팅 최적화 인스턴스 제품군의 차세대 버전인 Amazon EC2 C5 인스턴스를 지원합니다.
- VPC(Virtual Private Cloud)에 구축
- 확장 네트워킹(SR-IOV) - 사용 가능한 경우
- Amazon Marketplace에서 구축
- L3 네트워크의 사용자 구축
- 라우팅 모드(기본값)
- Amazon CloudWatch

지원되지 않는 기능

AWS의 ASA 가상은 다음을 지원하지 않습니다.

- 콘솔 액세스(네트워크 인터페이스를 통해 SSH 또는 ASDM을 사용하여 관리 수행)
- VLAN
- 프로미스큐어스 모드(스니핑 또는 투명 모드 방화벽 지원 없음)
- 다중 컨텍스트 모드
- 클러스터링
- ASA 가상 기본 HA
- EtherChannel은 직접 물리적 인터페이스에서만 지원됨
- VM 가져오기/내보내기
- 하이퍼바이저 독립적 패키징
- VMware ESXi
- 브로드캐스트/멀티캐스트 메시지

  이러한 메시지는 AWS 내에서 전파되지 않으므로 브로드캐스트/멀티캐스트가 필요한 라우팅 프로토콜은 AWS에서 정상적으로 작동하지 않게 됩니다. VXLAN은 고정 피어에서만 작동할 수 있습니다.
- 불필요한/원치 않는 ARP

이러한 ARPS는 AWS 내에서 허용되지 않으므로 불필요한 ARP 또는 원치 않는 ARP가 필요한 NAT 구성은 정상적으로 작동하지 않게 됩니다.

- IPv6

구성 마이그레이션 및 SSH 인증

SSH 공개 키 인증 사용 시 업그레이드가 미치는 영향 — SSH 인증에 대한 업데이트 때문에 SSH 공개 키 인증을 활성화하려면 추가 구성이 필요합니다. 따라서 공개 키 인증을 사용하는 기존 SSH 구성은 업그레이드 후 더 이상 작동하지 않습니다. 공개 키 인증은 AWS(Amazon Web Services)에서 ASA 가상에 대한 기본값이므로 AWS 사용자에게 이 문제가 표시됩니다. SSH 연결이 손실되는 것을 방지하기 위해 업그레이드하기 전에 구성을 업데이트할 수 있습니다. 또는 업그레이드 후에 ASDM을 사용하여(ASDM 액세스를 활성화한 경우) 구성을 수정할 수 있습니다.

다음은 "admin" 사용자 이름의 샘플 원본 구성입니다.

```
username admin nopassword privilege 15
username admin attributes
  ssh authentication publickey 55:06:47:eb:13:75:fc:5c:a8:c1:2c:bb:
  07:80:3a:fc:d9:08:a9:1f:34:76:31:ed:ab:bd:3a:9e:03:14:1e:1b hashed
```

ssh authentication 명령을 사용하려면 업그레이드하기 전에 다음 명령을 입력합니다.

```
aaa authentication ssh console LOCAL
username admin password <password> privilege 15
```

nopassword 키워드가 있는 경우 이를 유지하지 않고 사용자 이름에 비밀번호를 설정하는 것이 좋습니다. **nopassword**키워드는 어떤 비밀번호든지 입력할 수 있지만 비밀번호를 비워둘 수는 없다는 뜻입니다. 9.6(2) 이전 버전의 경우 **aaa** 명령이 SSH 공개 키 인증에 필요하지 않았으므로 **nopassword** 키워드가 트리거되지 않았습니다. **aaa** 명령이 필요해짐에 따라 **password**(또는 **nopassword**) 키워드가 있는 경우 자동으로 **username**에 대한 일반 비밀번호 인증도 허용됩니다.

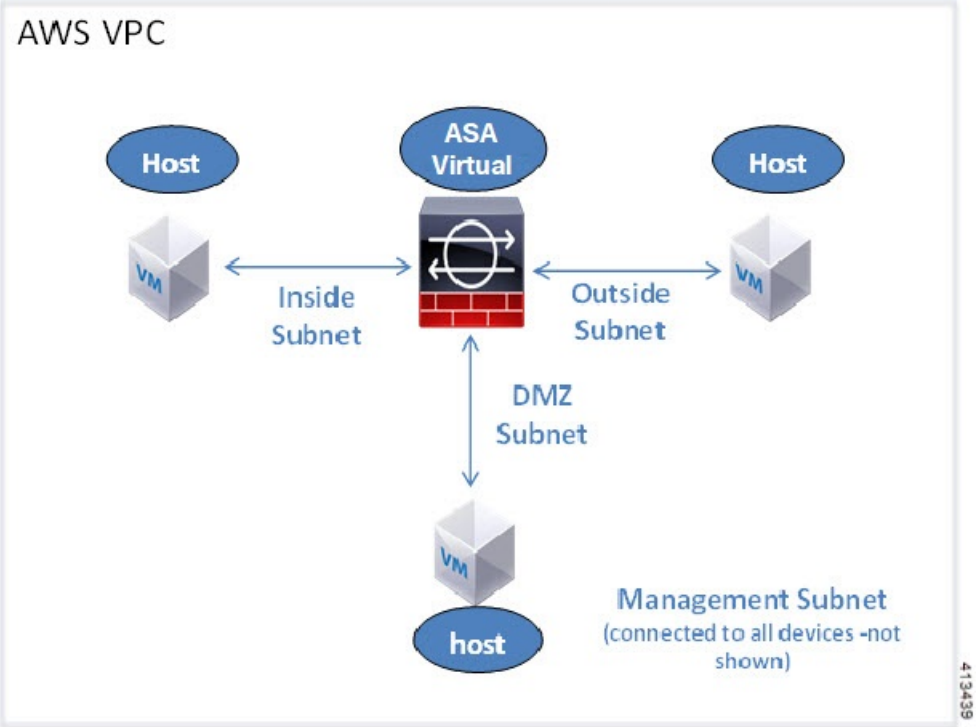
업그레이드를 하고 나면 **username** 명령에는 더 이상 **password** 또는 **nopassword** 키워드가 필요하지 않으므로 사용자가 비밀번호를 입력할 수 없도록 요청할 수 있습니다. 따라서 공개 키 인증만 강제로 적용하려면 **username** 명령을 다시 입력합니다.

```
username admin privilege 15
```

AWS 기반 ASA 가상의 샘플 네트워크 토폴로지

다음 그림에서는 Routed Firewall Mode의 ASA 가상에 대한 권장 토폴로지와 ASA 가상에 대해 AWS에 구성된 4개의 서브넷(관리, 내부, 외부 및 DMZ)을 보여줍니다.

그림 *1: AWS* 구축 기반 샘플 *ASA* 가상



AWS에 ASA 가상 구축

다음 절차는 ASA 가상에 AWS를 설정하는 단계를 간략하게 정리한 것입니다. 자세한 설정 단계는 AWS 시작하기를 참조하십시오.

단계 **1** aws.amazon.com에 로그인하고 지역을 선택합니다.

참고 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** **My Account(**내 계정**)** > **AWS Management Console(AWS** 관리 콘솔**)**을 클릭하고 Networking(네트워킹)에서 **VPC** > **Start VPC Wizard(VPC** 마법사 시작**)**를 클릭한 다음 단일 공용 서브넷을 선택하여 VPC를 생성하고 다음과 같이 설정합니다. 달리 표시되지 않는 한 기본 설정을 사용할 수 있습니다.

- 내부 및 외부 서브넷—VPC 및 서브넷의 이름을 입력합니다.
- 인터넷 게이트웨이—인터넷을 통한 직접 연결을 활성화합니다. 인터넷 게이트웨이의 이름을 입력합니다.
- 외부 테이블—인터넷에 대한 아웃바운드 트래픽을 활성화하려면 항목을 추가합니다. 인터넷 게이트웨이에 0.0.0.0/0을 추가합니다.

단계 **3** **My Account(**내 계정**)** > **AWS Management Console(AWS** 관리 콘솔**)** > **EC2**를 클릭한 후, **Create an Instance(**인스턴스 생성**)**를 클릭합니다.

- AMI를 선택합니다(예: Ubuntu Server 14.04 LTS).

  이미지 전달 알림에 식별된 AMI를 사용합니다.

- ASA 가상에서 지원하는 인스턴스 유형(예: c3.large)을 선택합니다.

- 인스턴스를 구성합니다. CPU 및 메모리는 고정되어 있습니다.

- **Advanced Details(**고급 세부 정보**)** 섹션을 확장하고 **User data(**사용자 데이터**)** 필드에 Day 0 컨피그레이션을 입력할 수 있습니다. 이 컨피그레이션은 ASA 가상이 시작될 때 적용된 ASA 가상 컨피그레이션을 포함하는 텍스트 입력입니다. 추가 정보(예: 스마트 라이센싱)를 이용해 Day 0 컨피그레이션에 구성하는 방법과 절차는 Day 0 컨피그레이션 파일 준비를 참조하십시오.

  - **Management interface(**관리 인터페이스**)** - Day 0 컨피그레이션을 제공하도록 선택했다면 DHCP를 사용하도록 구성해야 하는 관리 인터페이스 세부 정보를 반드시 제공해야 합니다.

  - **Data interfaces(**데이터 인터페이스**)** - 데이터 인터페이스의 IP 주소는 Day 0 컨피그레이션의 일부로서 해당 정보를 제공하는 경우에만 할당 및 구성됩니다. DHCP를 사용하도록 데이터 인터페이스를 구성할 수 있습니다. 연결할 네트워크 인터페이스가 이미 생성되었고 IP 주소가 알려진 상태라면 Day 0 컨피그레이션에 IP 세부 정보를 제공해도 됩니다.

  - **Without Day 0 Configuration(Day 0** 컨피그레이션 없음**)** - Day 0 컨피그레이션 없이 ASA 가상을 배포하는 경우, ASA 가상은 ASA 가상 컨피그레이션을 적용하여 AWS 메타데이터 서버에서 연결된 인터페이스의 IP를 가져오며 IP 주소를 할당합니다(데이터 인터페이스에서 IP를 할당하지만 ENI는 다운됩니다). Management0/0 인터페이스가 작동하며 DHCP 주소로 구성한 IP를 가져옵니다. Amazon EC2 및 Amazon VPC IP 주소 지정에 대한 자세한 내용은 VPC에서의 IP 주소 지정을 참조하십시오.

- **Sample Day 0 Configuration(**샘플 **Day 0** 컨피그레이션**)** -

```
! ASA Version 9.x.1.200
!
interface management0/0
management-only
nameif management
security-level 100
ip address dhcp setroute

no shutdown
!
crypto key generate rsa modulus 2048
ssh 0 0 management
ssh ::/0 management
ssh timeout 60
ssh version 2
username admin password Q1w2e3r4 privilege 15
username admin attributes
service-type admin
aaa authentication ssh console LOCAL
!
same-security-traffic permit inter-interface
same-security-traffic permit intra-interface
access-list allow-all extended permit ip any any
access-list allow-all extended permit ip any6 any6
```

```
access-group allow-all global
!
interface G0/0
nameif outside
ip address dhcp setroute

no shutdown
!
interface G0/1
nameif inside
ip address dhcp

no shutdown
!
```

- 스토리지(기본값 적용)
- 태그 인스턴스—다수의 태그를 생성하여 디바이스를 분류할 수 있습니다. 손쉽게 찾을 수 있도록 이름을 지정합니다.
- 보안 그룹—보안 그룹을 생성하고 이름을 지정합니다. 보안 그룹은 인바운드 및 아웃바운드 트래픽을 제어하기 위한 인스턴스에 대한 가상 방화벽입니다.

  기본적으로 보안 그룹은 모든 주소에 개방되어 있습니다. ASA 가상 액세스에 사용하는 주소의 SSH만 허용하도록 규칙을 변경합니다.
- 컨피그레이션을 검토하고 **Launch(**실행**)**를 클릭합니다.

단계 **4** 키 쌍을 생성합니다.

주의 키 쌍을 인식할 수 있는 이름을 지정하고 안전한 곳에 키를 다운로드합니다. 키는 다시 다운로드할 수 없습니다. 키 쌍을 잃어버릴 경우 인스턴스를 삭제하고 다시 구축해야 합니다.

단계 **5** **Launch Instance(**인스턴스 실행**)**를 클릭하여 ASA 가상을 구축합니다.

단계 **6** **My Account(**내 계정**)** > **AWS Management Console(AWS** 관리 콘솔**)** > **EC2** > **Launch an Instance(**인스턴스 실행**)** > **My AMIs(**내 **AMI)**를 클릭합니다.

단계 **7** ASA 가상에 대한 인터페이스 각각에서 Source/Destination Check(소스/대상 확인)가 비활성화되었는지 확인합니다.

AWS 기본 설정에서는 인스턴스가 관련 IP 주소(IPv4)에 대한 트래픽만 수신하도록 허용하고, 인스턴스가 자체 IP 주소(IPv4)에서 오는 트래픽만 전송하도록 허용합니다. ASA 가상이 라우팅 홉의 역할을 할 수 있으려면 ASA 가상 트래픽 인터페이스(내부, 외부, DMZ) 각각에서 소스/대상 확인을 비활성화해야 합니다.

AWS의 ASA 가상에 대한 성능 조정

VPN 최적화

AWS c5 인스턴스는 이전 c3, c4 및 m4 인스턴스보다 훨씬 뛰어난 성능을 제공합니다. c5 인스턴스 제품군의 대략적인 RA VPN 처리량(AES-CBC 암호화를 통한 450B TCP 트래픽을 사용하는 DTLS)은 다음과 같아야 합니다.

- c5.large에서는 0.5Gbps
- c5.xlarge에서는 1Gbps
- c5.2xlarge에서는 2Gbps