구성ASA 가상

ASA 가상 구축에서는 ASDM 액세스를 사전에 구성합니다. 웹 브라우저를 사용하여, 구축 중에 지정한 클라이언트 IP 주소에서 ASA 가상 관리 IP 주소에 연결할 수 있습니다. 이 장에서는 다른 클라이언트에서 ASDM에 액세스하도록 허용하는 방법 및 CLI 액세스(SSH 또는 텔넷)를 허용하는 방법에 대해서도 설명합니다. 이 장에서 다루는 그 밖의 필수 컨피그레이션 작업에는 ASDM에서 마법사를 통해 제공되는 라이센스 설치 및 일반 컨피그레이션 작업이 포함됩니다.

ASDM 시작

단계 **1** ASDM 클라이언트로 지정한 PC에서 다음 URL을 입력합니다.

https://*asa_ip_address*/**admin**

다음 버튼이 있는 ASDM 시작 창이 나타납니다.

- **Install ASDM Launcher and Run ASDM(ASDM Launcher** 설치 및 **ASDM** 실행**)**
- **Run ASDM(ASDM** 실행**)**
- **Run Startup Wizard(**시작 마법사 실행**)**

단계 **2** Launcher를 다운로드하려면

a) **Install ASDM Launcher and Run ASDM(ASDM Launcher** 설치 및 **ASDM** 실행**)**을 클릭합니다.

b) 사용자 이름 및 비밀번호 필드를 비어 있는 상태로 두고(새로 설치하는 경우) **OK(**확인**)**를 클릭합니다. 어떤 HTTPS 인증도 구성되지 않았으므로 사용자 이름 없이, **enable** 비밀번호(기본적으로 비어 있음)를 사용하여 ASDM에 액세스할 수 있습니다. HTTPS 인증을 활성화한 경우 사용자 이름과 관련 비밀번호를 입력합니다.

c) 설치 프로그램을 PC에 저장한 다음 시작합니다. 설치가 완료되면 ASDM-IDM Launcher가 자동으로 열립니다.

d) 관리 IP 주소를 입력한 후 사용자 이름과 비밀번호를 비어 있는 상태로 두고(새로 설치하는 경우) **OK(**확인**)**를 클릭합니다. HTTPS 인증을 활성화한 경우 사용자 이름과 관련 비밀번호를 입력합니다.

단계 3 Java Web Start를 사용하려면

a) **Run ASDM(ASDM 실행)** 또는 **Run Startup Wizard(**시작 마법사 실행**)**를 클릭합니다.
b) 프롬프트에 따라 바로가기를 컴퓨터에 저장합니다. 저장하지 않고 열 수도 있습니다.
c) 바로가기에서 Java Web Start를 시작합니다.
d) 표시되는 대화 상자의 안내에 따라 인증서를 승인합니다. Cisco ASDM-IDM Launcher가 나타납니다.
e) 사용자 이름과 비밀번호를 비어 있는 상태로 두고(새로 설치하는 경우) **OK(**확인**)**를 클릭합니다. HTTPS 인증을 활성화한 경우 사용자 이름과 관련 비밀번호를 입력합니다.

ASDM을 사용하여 초기 컨피그레이션 수행

다음 ASDM 마법사 및 절차를 사용하여 초기 컨피그레이션을 수행할 수 있습니다.

- 시작 마법사 실행
- (선택 사항) ASA 가상 뒤에 있는 공용 서버에 대한 액세스 허용
- (선택 사항) VPN 마법사 실행
- (선택 사항) ASDM에서 다른 마법사 실행

CLI 컨피그레이션에 대해서는 Cisco Secure Firewall ASA Series CLI 컨피그레이션 가이드를 참조하십시오.

시작 마법사 실행

Startup Wizard(시작 마법사**)**를 실행하여 구축에 맞게 보안 정책을 사용자 정의합니다.

단계 1 **Wizards(**마법사**)** > **Startup Wizard(**시작 마법사**)**를 선택합니다.

단계 2 구축에 맞게 보안 정책을 사용자 지정합니다. 다음을 설정할 수 있습니다.

- 호스트 이름
- 도메인 이름
- 관리 비밀번호
- 인터페이스
- IP 주소
- 정적 경로
- DHCP 서버
- NAT(Network Address Translation) 규칙

• 기타 등등...

(선택 사항) ASA 가상 뒤에 있는 공용 서버에 대한 액세스 허용

Configuration(컨피그레이션**)** > **Firewall(**방화벽**)** > **Public Servers(**공용 서버**)** 창에서는 인터넷을 통해 내부 서버에 액세스할 수 있도록 하는 보안 정책을 자동으로 구성합니다. 비즈니스 소유자는 웹 및 FTP 서버 등 외부 사용자가 사용할 수 있도록 해야 하는 내부 네트워크 서비스를 운영할 수 있습니다. 이러한 서비스를 ASA 가상 뒤에 있는 DMZ(Demilitarized Zone)라는 별도의 네트워크에 둘 수 있습니다. 공용 서버를 DMZ에 두면 공용 서버에 대해 실행된 어떤 공격도 내부 네트워크에 영향을 주지 않습니다.

(선택 사항) VPN 마법사 실행

다음 마법사를 사용하여 VPN을 구성할 수 있습니다(**Wizards(**마법사**)** > **VPN Wizards(VPN** 마법사**)**).

- Site-to-Site VPN Wizard(사이트 대 사이트 VPN 마법사) - ASA 가상 및 다른 VPN 지원 디바이스 사이에 IPsec 사이트 대 사이트 터널을 만듭니다.
- AnyConnect VPN Wizard(AnyConnect VPN 마법사) - Cisco AnyConnect VPN 클라이언트를 위한 SSL VPN 원격 액세스를 구성합니다. Secure Client는 기업 리소스에 대한 전체 VPN 터널링을 통해 원격 사용자에게 ASA에 대한 SSL 연결을 제공합니다 원격 사용자가 브라우저를 통해 처음 연결할 때 Secure Client를 다운로드하도록 ASA 정책을 구성할 수 있습니다. Secure Client 3.0 이상을 사용하면 클라이언트에서 SSL 또는 IPsec IKEv2 VPN 프로토콜을 실행할 수 있습니다.
- Clientless SSL VPN Wizard(클라이언트리스 SSL VPN 마법사) - 브라우저에 대한 클라이언트리스 SSL VPN 원격 액세스를 구성합니다. 클라이언트리스 브라우저 기반 SSL VPN을 통해 사용자는 웹 브라우저를 사용하여 ASA에 보안 원격 액세스 VPN 터널을 설정할 수 있습니다. 사용자는 인증 후 포털 페이지에 액세스하여 지원되는 특정 내부 리소스에 액세스할 수 있습니다. 네트워크 관리자는 사용자 그룹별로 리소스에 대한 액세스를 제공합니다. ACL을 적용하여 특정 회사 리소스에 대한 액세스를 제한하거나 허용할 수 있습니다.
- IPsec (IKEv1 or IKEv2) Remote Access VPN Wizard(IPsec(IKEv1 또는 IKEv2) 원격 액세스 VPN 마법사) - Cisco IPsec 클라이언트에 대한 IPsec VPN 원격 액세스를 구성합니다.

Azure에 대한 ASA 가상 IPsec VTI(Virtual Tunnel Interface) 연결을 구성하는 자세한 방법은 Azure에 대한 ASA IPsec VTI 연결 구성을 참고하십시오.

(선택 사항) ASDM에서 다른 마법사 실행

ASDM에서 다른 마법사를 실행하여 고가용성, VPN 클러스터 로드 밸런싱 및 패킷 캡처를 이용해 페일오버를 구성할 수 있습니다.

- High Availability and Scalability Wizard(고가용성 및 확장성 마법사) - 장애 조치 또는 VPN 로드 밸런싱을 구성합니다.

- Packet Capture Wizard(패킷 캡처 마법사) - 패킷 캡처를 구성하고 실행합니다. 이 마법사는 각 인그레스 및 이그레스 인터페이스에서 하나의 패킷 캡처를 실행합니다. 패킷 캡처가 완료되면 패킷 분석기에서 검사하고 재생하기 위해 패킷 캡처를 PC에 저장할 수 있습니다.

고급 컨피그레이션

ASA 가상을 계속 구성하려면 Cisco Secure Firewall ASA Series 설명서 탐색을 참조하십시오.