내부 및 외부 인터페이스의 ASA 버전 9.x SSH 및 텔넷 컨피그레이션 예

목차

소개

이 문서에서는 Cisco Series Security Appliance 버전 9.x 이상의 내부 및 외부 인터페이스에서 SSH(Secure Shell)를 구성하는 방법에 대해 설명합니다. CLI를 사용하여 Cisco ASA(Adaptive Security Appliance)를 원격으로 구성 및 모니터링해야 하는 경우 텔넷 또는 SSH를 사용해야 합니다. 텔넷 통신은 비밀번호를 포함할 수 있는 일반 텍스트로 전송되므로 SSH를 사용하는 것이 좋습니다. SSH 트래픽은 터널에서 암호화되므로 암호 및 기타 민감한 구성 명령을 가로채기에서 보호할 수 있습니다.

ASA는 관리 목적으로 보안 어플라이언스에 대한 SSH 연결을 허용합니다. 보안 어플라이언스는 각 보안 컨텍스트에 대해 최대 5개의 동시 SSH 연결(사용 가능한 경우)을 허용하고, 결합된 모든 컨텍스트에 대해 전역 최대 100개의 연결을 허용합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 Cisco ASA Firewall 소프트웨어 버전 9.1.5을 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

> **참고:** SSH 버전 2(SSHv2)는 ASA 버전 7.x 이상에서 지원됩니다.

관련 제품

이 컨피그레이션은 소프트웨어 버전 9.x 이상에서 Cisco ASA 5500 Series Security Appliance와 함께 사용할 수도 있습니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

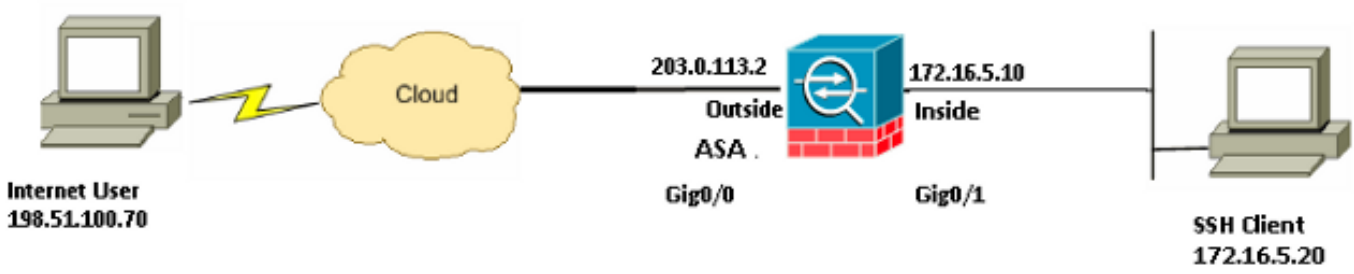
구성

이 문서에 설명된 기능을 구성하려면 이 섹션에서 제공하는 정보를 사용합니다.

> **참고:** 설명된 각 컨피그레이션 단계에서는 CLI 또는 ASDM(Adaptive Security Device Manager)을 사용하기 위해 필요한 정보를 제공합니다.

> **참고:** 이 섹션에 사용된 명령에 대한 자세한 내용을 보려면 Command Lookup Tool(등록된 고객만 해당)을 사용합니다.

네트워크 다이어그램



이 컨피그레이션 예에서는 ASA가 SSH 서버로 간주됩니다. SSH 클라이언트(198.51.100.70/32 및 172.16.5.20/24)에서 SSH 서버로의 트래픽은 암호화됩니다. 보안 어플라이언스는 SSH 버전 1 및 2에서 제공되는 SSH 원격 셸 기능을 지원하며 DES(Data Encryption Standard) 및 3DES 암호를 지원합니다. SSH 버전 1과 2는 서로 다르며 상호 운용이 불가능합니다.

SSH 구성

이 문서에서는 다음 구성을 사용합니다.

- 보안 어플라이언스에 대한 SSH 액세스
- SSH 클라이언트 사용 방법
- ASA 컨피그레이션

보안 어플라이언스에 대한 SSH 액세스

보안 어플라이언스에 대한 SSH 액세스를 구성하려면 다음 단계를 완료합니다.

1. SSH 세션에는 항상 사용자 이름 및 비밀번호와 같은 인증 형식이 필요합니다. 이 요구 사항을 충족하기 위해 사용할 수 있는 두 가지 방법이 있습니다.

   이 요구 사항을 충족하기 위해 사용할 수 있는 **첫 번째 방법은** AAA(Authentication, Authorization, and Accounting)를 사용하여 사용자 이름과 비밀번호를 구성하는 것입니다.

   ```
   ASA(config)#username username password password
   ASA(config)#aaa authentication {telnet | ssh | http | serial} console
   {LOCAL | server_group [LOCAL]}
   ```

   참고: 인증에 TACACS+ 또는 RADIUS 서버 그룹을 사용하는 경우 AAA 서버를 사용할 수 없는 경우 로컬 데이터베이스를 대체 방법으로 사용하도록 보안 어플라이언스를 구성할 수 있습니다. 서버 그룹 이름을 지정한 다음 **LOCAL**(**LOCAL**은 대/소문자 구분)을 지정합니다. 보안 어플라이언스 프롬프트는 사용하는 방법을 나타내지 않으므로 로컬 데이터베이스와 AAA 서버에서 동일한 사용자 이름과 비밀번호를 사용하는 것이 좋습니다.TACACS+용 **로컬** 백업을 지정하려면 **SSH** 인증에 이 컨피그레이션을 사용합니다.

   ```
   ASA(config)#aaa authentication ssh console TACACS+ LOCAL
   ```

   대체 방법 없이 로컬 데이터베이스를 기본 인증 방법으로 사용할 수도 있습니다. 이렇게 하려면 LOCAL만 **입력합니다**.

   ```
   ASA(config)#aaa authentication ssh console LOCAL
   ```

   이 요구 사항을 충족하기 위해 사용할 수 있는 **두 번째 방법은 ASA**의 기본 사용자 이름과 **cisco**의 기본 텔넷 비밀번호를 사용하는 것입니다. 다음 명령을 사용하여 텔넷 비밀번호를 변경할 수 있습니다.

```
ASA(config)#passwd password
```

참고: 두 명령 모두 마찬가지로 작동하므로 이 경우에도 password 명령을 사용할 수 있습니다.

2. SSH에 필요한 ASA 방화벽에 대한 RSA 키 쌍을 생성합니다.

```
ASA(config)#crypto key generate rsa modulusmodulus_size
```

참고: modulus_size(비트)는 512, 768, 1024 또는 2048일 수 있습니다. 지정한 키 모듈러스 크기가 클수록 RSA 키 쌍을 생성하는 데 더 오래 걸립니다. 2048 값을 사용하는 것이 좋습니다. RSA 키 쌍을 생성하는 데 사용되는 명령은 버전 7.x 이전 버전의 ASA 소프트웨어 버전과 다릅니다. 이전 버전에서는 키를 만들려면 도메인 이름을 설정해야 합니다. 다중 컨텍스트 모드에서는 모든 컨텍스트에 대해 RSA 키를 생성해야 합니다.

3. 보안 어플라이언스에 연결할 수 있는 호스트를 지정합니다. 이 명령은 SSH로 연결할 수 있는 호스트의 소스 주소, 넷마스크 및 인터페이스를 지정합니다. 여러 호스트, 네트워크 또는 인터페이스에 대해 여러 번 입력할 수 있습니다. 이 예에서는 내부 호스트 하나와 외부 호스트 하나가 허용됩니다.

```
ASA(config)#ssh 172.16.5.20 255.255.255.255 inside
ASA(config)#ssh 198.51.10.70 255.255.255.255 outside
```

4. 이 단계는 선택 사항입니다. 기본적으로 보안 어플라이언스는 SSH 버전 1과 버전 2를 모두 허용합니다. 특정 버전으로 연결을 제한하려면 이 명령을 입력합니다.

```
ASA(config)# ssh version
```

참고: version_number는 1 또는 2일 수 있습니다.

5. 이 단계는 선택 사항입니다. 기본적으로 SSH 세션은 5분 동안 활동이 없으면 닫힙니다. 이 시간 제한은 1~60분 동안 지속되도록 구성할 수 있습니다.

```
ASA(config)#ssh timeout minutes
```

ASA 컨피그레이션

ASA를 구성하려면 다음 정보를 사용합니다.

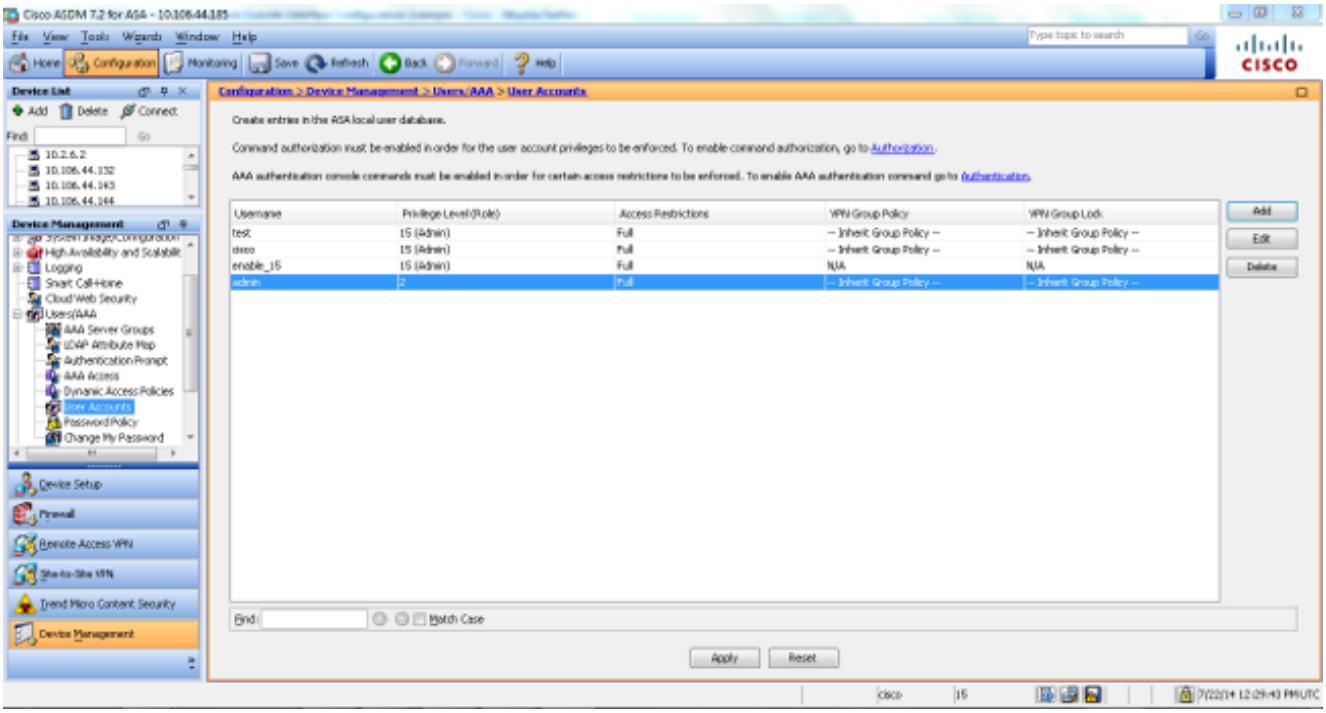
```
ASA Version 9.1(5)2
!
hostname ASA
domain-name cisco.com

interface GigabitEthernet0/0
 nameif inside
 security-level 100
 ip address 172.16.5.10 255.255.255.0
!
interface GigabitEthernet0/1
 nameif outside
 security-level 0
 ip address 203.0.113.2 255.255.255.0

!--- AAA for the SSH configuration

username ciscouser password 3USUcOPFUiMCO4Jk encrypted
aaa authentication ssh console LOCAL

http server enable
http 172.16.5.0 255.255.255.0 inside
```

```
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstar
telnet timeout 5

!--- Enter this command for each address or subnet
!--- to identify the IP addresses from which
!--- the security appliance accepts connections.
!--- The security appliance accepts SSH connections from all interfaces.

ssh 172.16.5.20 255.255.255.255 inside
ssh 198.51.100.70 255.255.255.255 outside

!--- Allows the users on the host 172.16.5.20 on inside
!--- Allows SSH access to the user on internet 198.51.100.70 on outside
!--- to access the security appliance
!--- on the inside interface.

ssh 172.16.5.20 255.255.255.255 inside

!--- Sets the duration from 1 to 60 minutes
!--- (default 5 minutes) that the SSH session can be idle,
!--- before the security appliance disconnects the session.

ssh timeout 60

console timeout 0
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map global_policy
class inspection_default
inspect dns maximum-length 512
inspect ftp
inspect h323 h225
inspect h323 ras
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
!
service-policy global_policy global
```

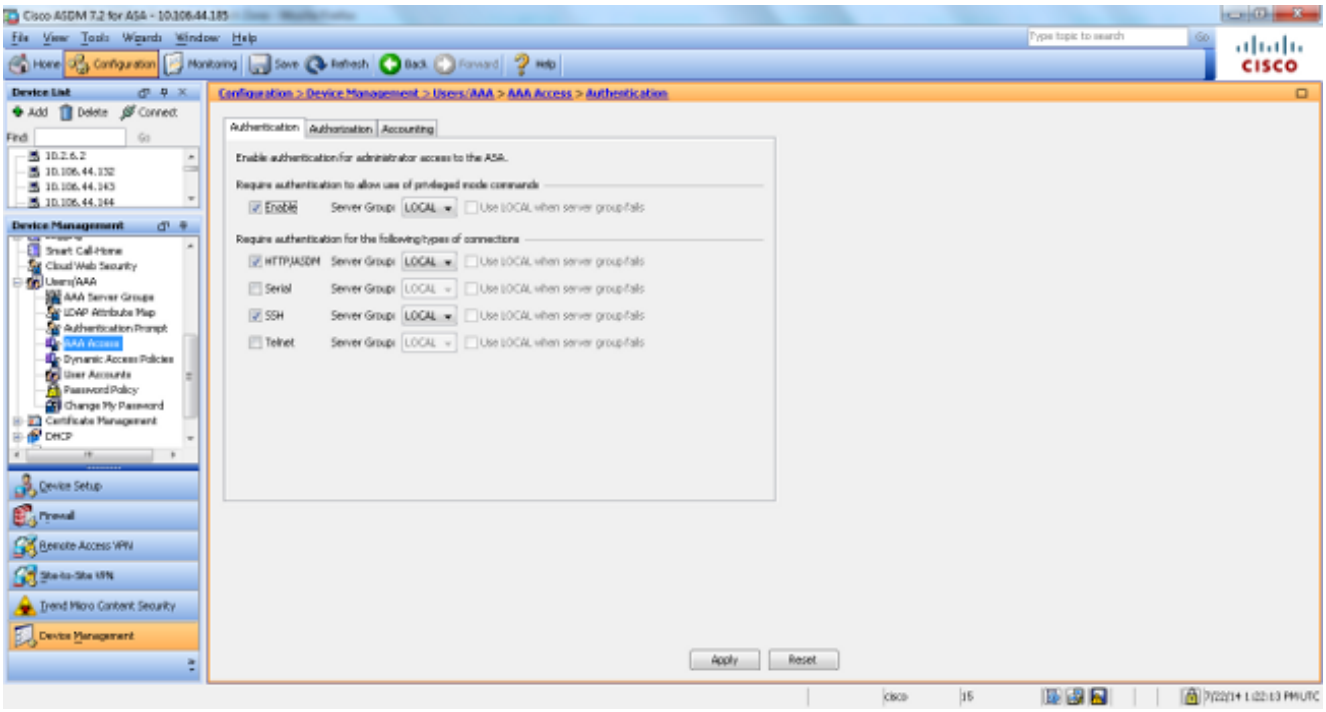
ASDM 버전 7.2.1 구성

ASDM 버전 7.2.1을 구성하려면 다음 단계를 완료합니다.

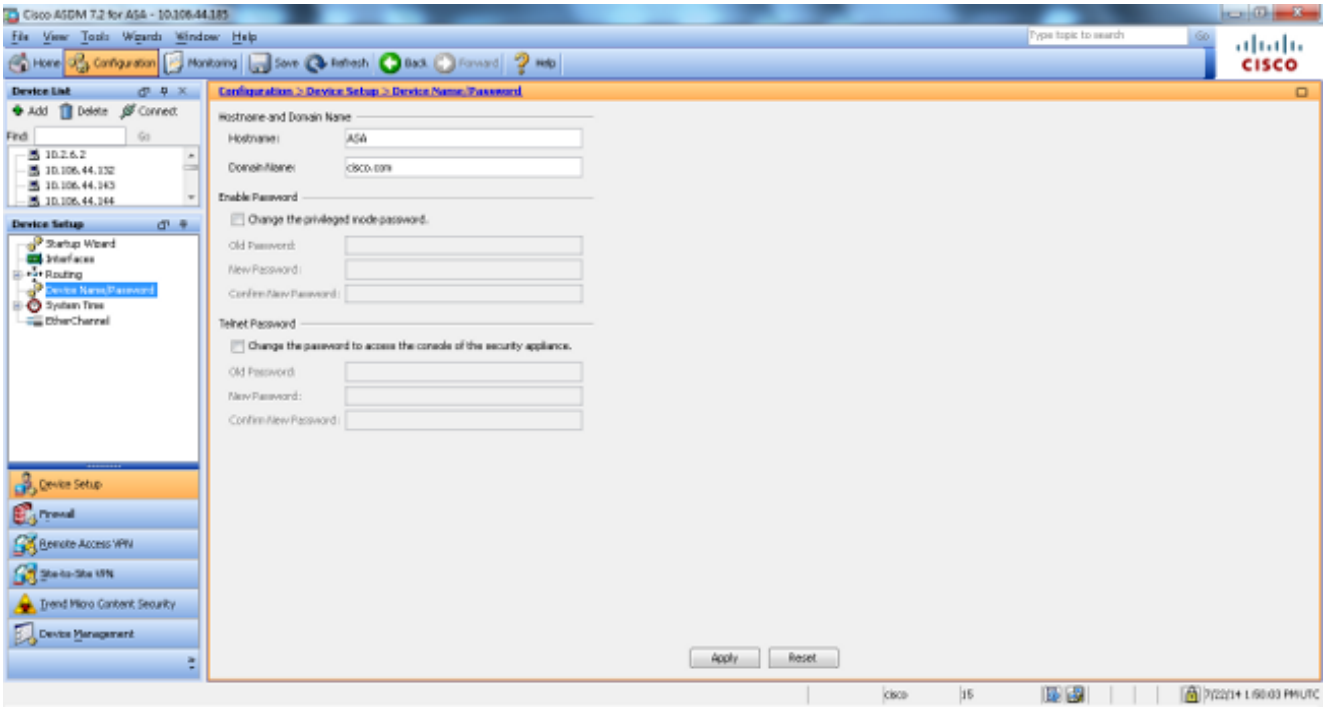
1. ASDM이 있는 사용자를 추가하려면 **Configuration > Device Management > Users/AAA > User Accounts**로 이동합니다.



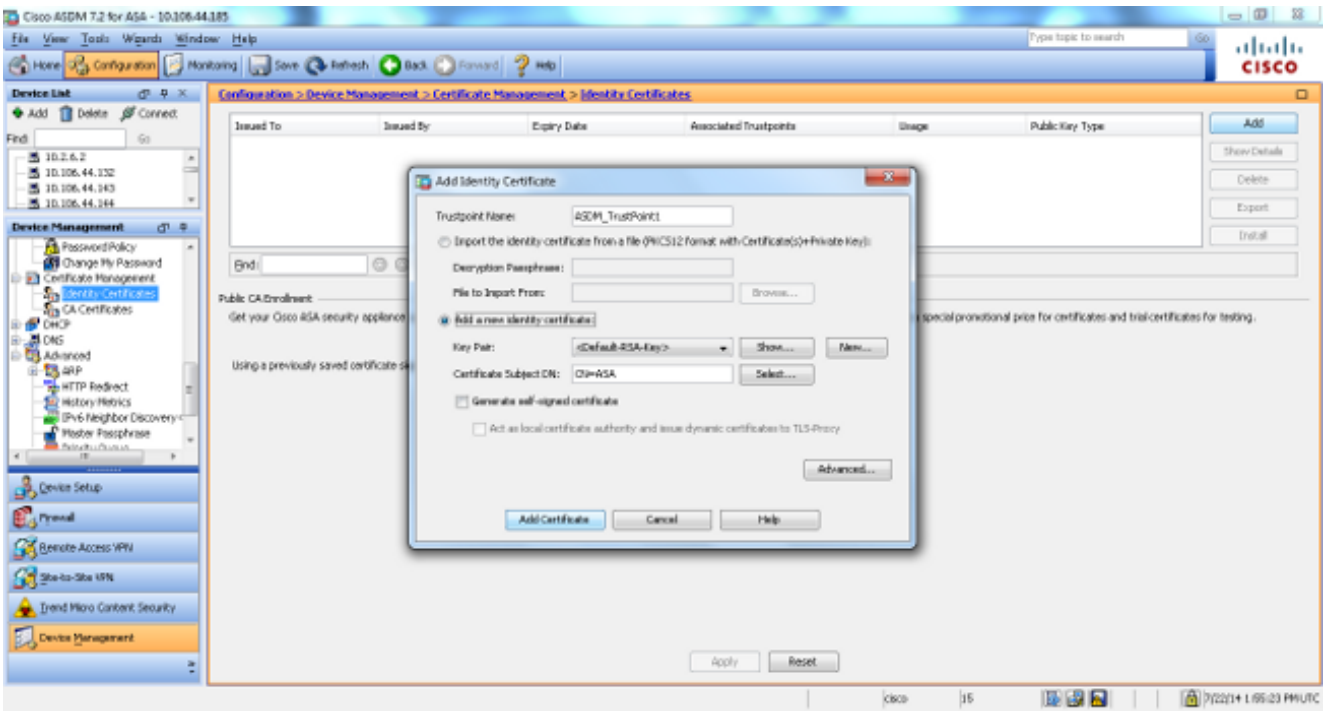
2. ASDM을 사용하여 SSH에 대한 AAA 인증을 설정하려면 Configuration **> Device Management > Users/AAA > AAA Access > Authentication**으로 이동합니다.



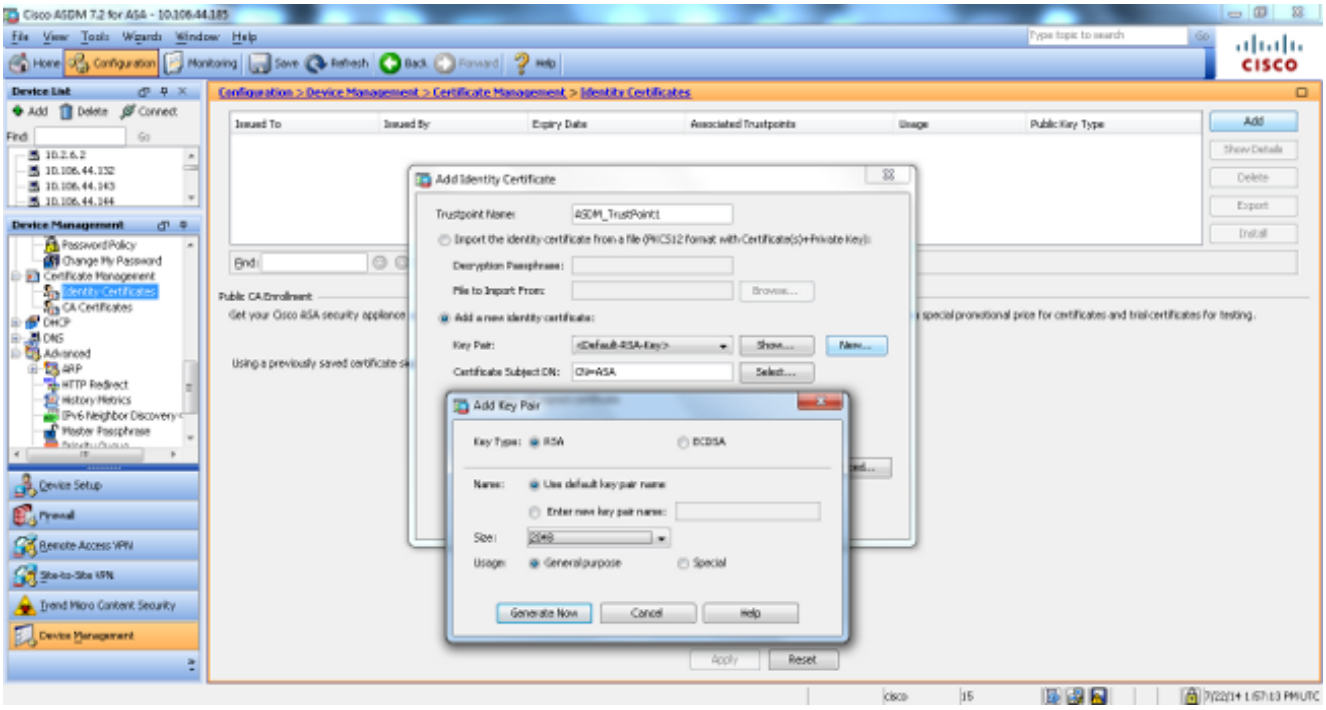
3. Configuration(컨피그레이션) **> Device Setup(디바이스 설정) > Device Name/Password(디바이스 이름/비밀번호)**로 이동하여 ASDM과의 텔넷 비밀번호를 변경합니다.



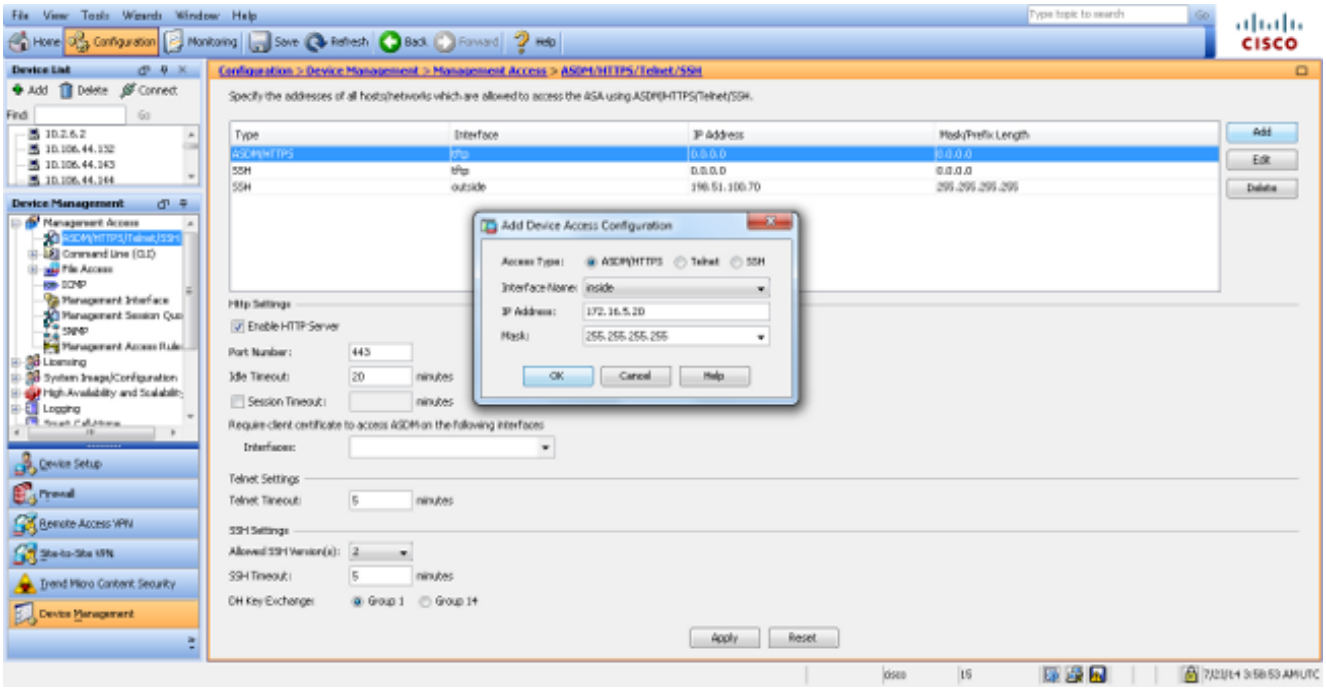
4. Configuration(**구성) > Device Management(디바이스 관리) > Certificate Management(인증서 관리) > Identity Certificates(ID 인증서)로 이동하고 Add(추가)를** 클릭하고 ASDM과 동일한 RSA 키를 생성하기 위해 사용 가능한 기본 옵션을 사용합니다.



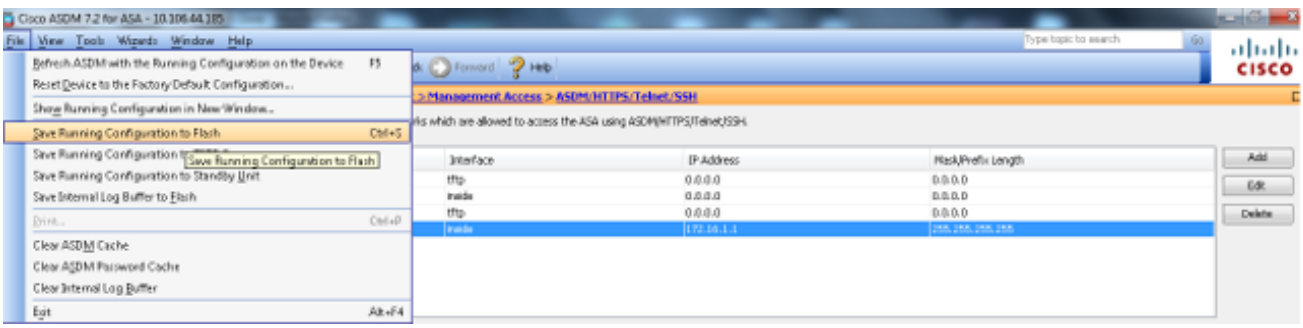
5. Add a **new Identity certificate(새 ID 인증서 추가)** 라디오 버튼**을 클릭하고 New(새로 만들기)**를 클릭하여 기본 키 쌍을 추가합니다(없는 경우). 완료되면 Generate Now(지금 **생성)를 클릭합니다**.



6. ASDM을 사용하여 SSH와 연결할 수 있는 호스트를 지정하고 버전 및 시간 제한 옵션을 지정하기 위해 ASDM을 사용하려면 Configuration **> Device Management > Management Access > Command Line (CLI) > Secure Shell (SSH)**로 이동합니다.



7. 컨피그레이션을 저장하려면 팝업 창에서 Save(저장)를 클릭합니다.



8. 플래시에 컨피그레이션을 저장하라는 메시지가 표시되면 **Apply**를 선택하여 컨피그레이션을 저장합니다.

텔넷 컨피그레이션

콘솔에 텔넷 액세스를 추가하고 유휴 시간 제한을 설정하려면 전역 컨피그레이션 모드에서 **telnet** 명령을 입력합니다. 기본적으로 5분 동안 유휴 상태로 남아 있는 텔넷 세션은 보안 어플라이언스에 의해 닫힙니다. 이전에 설정된 IP 주소에서 텔넷 액세스를 제거하려면 이 명령의 **no** 형식을 사용합니다.

```
telnet {{hostname | IP_address mask interface_name} | {IPv6_address
interface_name} | {timeout number}}
no telnet {{hostname | IP_address mask interface_name} | {IPv6_address
interface_name} | {timeout number}}
```

telnet 명령을 사용하면 텔넷을 통해 보안 어플라이언스 콘솔에 액세스할 수 있는 호스트를 지정할 수 있습니다.

> **참고:** 모든 인터페이스에서 보안 어플라이언스에 텔넷을 활성화할 수 있습니다. 그러나 보안 어플라이언스에서는 외부 인터페이스에 대한 모든 텔넷 트래픽을 IPsec으로 보호해야 합니다. 외부 인터페이스에 대한 텔넷 세션을 활성화하려면 보안 어플라이언스에서 생성된 IP 트래픽을 포함하도록 외부 인터페이스에서 IPsec을 구성하고 외부 인터페이스에서 텔넷을 활성화합니다.

> **참고:** 일반적으로 보안 레벨이 0이거나 다른 인터페이스보다 낮은 인터페이스가 있으면 ASA는 해당 인터페이스에 대한 텔넷을 허용하지 않습니다.

> **참고:** Cisco는 텔넷 세션을 통해 보안 어플라이언스에 대한 액세스를 권장하지 않습니다. 비밀번호와 같은 인증 자격 증명 정보는 일반 텍스트로 전송됩니다. Cisco에서는 보다 안전한 데이터 통신을 위해 SSH를 사용하는 것이 좋습니다.

콘솔에 대한 텔넷 액세스를 위한 비밀번호를 설정하려면 **password** 명령을 입력합니다. 기본 비밀번호는 **cisco입니다**. 현재 보안 어플라이언스 콘솔에 액세스하는 IP 주소를 보려면 **who** 명령을 입력합니다. 활성 텔넷 콘솔 세션을 종료하려면 **kill** 명령을 입력합니다.

텔넷 예제 시나리오

내부 인터페이스에 대한 텔넷 세션을 활성화하려면 이 섹션에서 제공하는 예를 검토하십시오.

예 1

이 예에서는 호스트 **172.16.5.20만 텔넷을** 통해 보안 어플라이언스 콘솔에 액세스할 수 있습니다.

```
ASA(config)#telnet 172.16.5.20 255.255.255.255 inside
```

예 2

이 예에서는 텔넷을 통해 네트워크 **172.16.5.0/24**만 보안 어플라이언스 콘솔에 액세스할 수 있습니

다.

```
ASA(config)#telnet 172.16.5.0 255.255.255.0 inside
```

예 3

다음 예에서는 모든 네트워크에서 텔넷을 통해 보안 어플라이언스 콘솔에 액세스할 수 있도록 합니다.

```
ASA(config)#telnet 0.0.0.0 0.0.0.0 inside
```

console 키워드와 함께 **aaa** 명령을 사용하는 경우, 텔넷 콘솔 액세스는 인증 서버로 인증되어야 합니다.

> **참고:** 보안 어플라이언스 및 텔넷 콘솔 액세스에 대한 인증을 요구하기 위해 **aaa** 명령을 구성하고 콘솔 로그인 요청이 시간 초과되면 시리얼 콘솔에서 보안 어플라이언스에 액세스할 수 있습니다. 이렇게 하려면 보안 어플라이언스 사용자 이름 및 enable password 명령으로 설정된 비밀번호를 **입력합니다**.

보안 어플라이언스에서 로그오프하기 전에 콘솔 텔넷 세션이 유휴 상태일 수 있는 최대 시간을 설정하려면 telnet timeout 명령을 실행합니다. **telnet timeout** 명령과 함께 **no telnet** 명령을 사용할 수 없습니다.

다음 예에서는 최대 세션 유휴 기간을 변경하는 방법을 보여 줍니다.

```
hostname(config)#telnet timeout 10

hostname(config)#show running-config telnet timeout

telnet timeout 10 minutes
```

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

> **참고:** Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다. **show** 명령 출력의 분석을 보려면 OIT를 사용합니다.

디버그 SSH

SSH 디버깅을 활성화하려면 debug ssh 명령을 입력합니다.

```
ASA(config)#debug ssh
SSH debugging on
```

이 출력은 내부 IP 주소(172.16.5.20)에서 ASA의 내부 인터페이스로 SSH 시도를 보여줍니다. 다음 디버그는 성공적인 연결 및 인증을 나타냅니다.

```
Device ssh opened successfully.
SSH0: SSH client: IP = '172.16.5.20' interface # = 1
SSH: host key initialised
SSH0: starting SSH control process
SSH0: Exchanging versions - SSH-2.0-Cisco-1.25
SSH0: send SSH message: outdata is NULL
server version string:SSH-2.0-Cisco-1.25
SSH0: receive SSH message: 83 (83)
SSH0: client version is - SSH-2.0-PuTTY_Release_0.62
SSH Secure Shell for Windows
client version string:SSH-2.0-PuTTY_Release_0.62
SSH Secure Shell for WindowsSSH0: begin ser ver key generation
SSH0: complete server key generation, elapsed time = 1760 ms
SSH2 0: SSH2_MSG_KEXINIT sent
SSH2 0: SSH2_MSG_KEXINIT received
SSH2: kex: client->server aes128-cbc hmac-md5 none
SSH2: kex: server->client aes128-cbc hmac-md5 none
SSH2 0: expecting SSH2_MSG_KEXDH_INIT
SSH2 0: SSH2_MSG_KEXDH_INIT received
SSH2 0: signature length 143
SSH2: kex_derive_keys complete
SSH2 0: newkeys: mode 1
SSH2 0: SSH2_MSG_NEWKEYS sent
SSH2 0: waiting for SSH2_MSG_NEWKEYS
SSH2 0: newkeys: mode 0
SSH2 0: SSH2_MSG_NEWKEYS received
SSH(cisco): user authen method is 'use AAA', aaa server group ID = 1
SSH2 0: authentication successful for cisco

!--- Authentication for the ASA was successful.

SSH2 0: channel open request
SSH2 0: pty-req request
SSH2 0: requested tty: vt100, height 25, width 80
SSH2 0: shell request
SSH2 0: shell message received
```

잘못된 사용자 이름(예: **cisco** 대신 **cisco1)을** 입력하면 ASA 방화벽이 인증을 거부합니다. 이 디버그 출력은 실패한 인증을 보여줍니다.

```
Device ssh opened successfully.
SSH0: SSH client: IP = '172.16.5.20' interface # = 1
SSH: host key initialised
SSH0: starting SSH control process
SSH0: Exchanging versions - SSH-2.0-Cisco-1.25
SSH0: send SSH message: outdata is NULL
server version string:SSH-2.0-Cisco-1.25
SSH0: receive SSH message: 83 (83)
SSH0: client version is - SSH-2.0-PuTTY_Release_0.62
SSH Secure Shell for Windows
client version string:SSH-2.0-PuTTY_Release_0.62
SSH Secure Shell for WindowsSSH0: begin ser ver key generation
SSH0: complete server key generation, elapsed time = 1760 ms
SSH2 0: SSH2_MSG_KEXINIT sent
SSH2 0: SSH2_MSG_KEXINIT received
SSH2: kex: client->server aes128-cbc hmac-md5 none
SSH2: kex: server->client aes128-cbc hmac-md5 none
SSH2 0: expecting SSH2_MSG_KEXDH_INIT
SSH2 0: SSH2_MSG_KEXDH_INIT received
SSH2 0: signature length 143
SSH2: kex_derive_keys complete
SSH2 0: newkeys: mode 1
SSH2 0: SSH2_MSG_NEWKEYS sent
```

```
SSH2 0: waiting for SSH2_MSG_NEWKEYS
SSH2 0: newkeys: mode 0
SSH2 0: SSH2_MSG_NEWKEYS received
SSH(cisco): user authen method is 'use AAA', aaa server group ID = 1
SSH2 0: authentication failed for cisco1

!--- Authentication for ASA1 was not successful due to the wrong username.
```

마찬가지로, 잘못된 비밀번호를 입력하면 인증이 실패합니다. 이 디버그 출력은 실패한 인증을 보여줍니다.

```
Device ssh opened successfully.
SSH0: SSH client: IP = '172.16.5.20' interface # = 1
SSH: host key initialised
SSH0: starting SSH control process
SSH0: Exchanging versions - SSH-2.0-Cisco-1.25
SSH0: send SSH message: outdata is NULL
server version string:SSH-2.0-Cisco-1.25
SSH0: receive SSH message: 83 (83)
SSH0: client version is - SSH-2.0-PuTTY_Release_0.62
SSH Secure Shell for Windows
client version string:SSH-2.0-PuTTY_Release_0.62
SSH Secure Shell for WindowsSSH0: begin ser ver key generation
SSH0: complete server key generation, elapsed time = 1760 ms
SSH2 0: SSH2_MSG_KEXINIT sent
SSH2 0: SSH2_MSG_KEXINIT received
SSH2: kex: client->server aes128-cbc hmac-md5 none
SSH2: kex: server->client aes128-cbc hmac-md5 none
SSH2 0: expecting SSH2_MSG_KEXDH_INIT
SSH2 0: SSH2_MSG_KEXDH_INIT received
SSH2 0: signature length 143
SSH2: kex_derive_keys complete
SSH2 0: newkeys: mode 1
SSH2 0: SSH2_MSG_NEWKEYS sent
SSH2 0: waiting for SSH2_MSG_NEWKEYS
SSH2 0: newkeys: mode 0
SSH2 0: SSH2_MSG_NEWKEYS received
SSH(cisco): user authen method is 'use AAA', aaa server group ID = 1
SSH2 0: authentication failed for cisco1

!--- Authentication for ASA was not successful due to the wrong password.
```

활성 SSH 세션 보기

ASA에 연결된 SSH 세션 수(및 연결 상태)를 확인하려면 다음 명령을 입력합니다.

```
ASA(config)# show ssh sessions

SID Client IP    Version Mode Encryption Hmac State           Username
0   172.16.5.20 2.0     IN   aes256-cbc sha1 SessionStarted  cisco
                        OUT  aes256-cbc sha1 SessionStarted  cisco
```

ASDM과의 세션을 **보려면 Monitoring > Properties > Device Access > Secure Shell Sessions**로 이동합니다.

TCP 세션이 **설정되었는지** 확인하려면 show asp table socket 명령을 입력합니다.

```
ASA(config)# show asp table socket
```

```
Protocol Socket State Local Address Foreign Address

SSL 02444758 LISTEN 203.0.113.2:443 0.0.0.0:*
TCP 02448708 LISTEN 203.0.113.2:22 0.0.0.0:*
SSL 02c75298 LISTEN 172.16.5.10:443 0.0.0.0:*
TCP 02c77c88 LISTEN 172.16.5.10:22 0.0.0.0:*
TCP      02d032d8  ESTAB    172.16.5.10:22     172.16.5.20:52234
```

공용 RSA 키 보기

보안 어플라이언스에서 RSA 키의 공용 부분을 보려면 다음 명령을 입력합니다.

```
ASA(config)# show crypto key mypubkey rsa
Key pair was generated at: 23:23:59 UTC Jul 22 2014
Key name: <Default-RSA-Key>
 Usage: General Purpose Key
 Modulus Size (bits): 2048
 Key:

 30820122 300d0609 2a864886 f70d0101 01050003 82010f00 3082010a 02820101
 00aa82d1 f61df1a4 7cd1ae05 c92322c1 1ce490e3 c9db00fd d75afe77 1ea0b2c2
 3325576f a7dc5ffe a6166bf5 7f0f2551 25b8cb23 a8908b49 81c42618 c98e3aea
 ce6f9e42 367974d1 5c2ea6b1 e7aac40b 44a6c0a5 23c4d845 a57d4c04 6de49dbb
 2c6f074e 25e3b19e 7c5da809 ac7d775c 0c01bb9d 211b7078 741094b4 94056e75
 72d5e938 c59baaec 12285005 ee6abf81 90822610 cf7ee4c1 ae8093d9 6943bde3
 16d8748c d86b5f66 1a6ccf33 9cde0432 b3cabab5 938b1874 c3d7c13e 43a95a8f
 ed36db2e f9ca5d2c 0c65858e 3e513723 2d362b47 7984d845 faf22579 654113d1
 24d59f27 55d2ddf3 20af3b65 62f039cb a3aafc31 d92a3d9b 14966eb3 cb6ca249
 55020301 0001
```

Configuration(컨피그레이션) > Properties(속성) > Certificate(인증서) > Key Pair(키 쌍)로 이동하고 Show Details(세부사항 표시)를 클릭하여 ASDM과 함께 RSA 키를 확인합니다.

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

ASA에서 RSA 키 제거

ASA 소프트웨어를 업그레이드하거나 ASA에서 SSH 버전을 변경하는 경우 RSA 키를 제거하고 다시 생성해야 하는 경우가 있습니다. ASA에서 RSA 키 쌍을 제거하려면 다음 명령을 입력합니다.

```
ASA(config)#crypto key zeroize rsa
```

Configuration(컨피그레이션) > Properties(속성) > Certificate(인증서) > Key Pair(키 쌍)로 이동하고 Delete(삭제)를 클릭하여 ASDM과 함께 RSA 키를 제거합니다.

SSH 연결 실패

ASA에서 다음 오류 메시지가 표시됩니다.

%ASA-3-315004: Fail to establish SSH session because RSA host key retrieval failed.
SSH 클라이언트 시스템에 나타나는 오류 메시지입니다.

Selected cipher type

이 문제를 해결하려면 RSA 키를 제거하고 다시 만드십시오. ASA에서 RSA 키 쌍을 제거하려면 다음 명령을 입력합니다.

ASA(config)#**crypto key zeroize rsa**
새 키를 생성하려면 다음 명령을 입력합니다.

ASA(config)# **crypto key generate rsa modulus 2048**