PIX/ASA 7.x:내부 및 외부 인터페이스의 SSH/텔넷 컨피그레이션 예

목차

소개

이 문서에서는 Cisco Series Security Appliance 버전 7.x 이상의 내부 및 외부 인터페이스에서 SSH(Secure Shell)의 샘플 컨피그레이션을 제공합니다.명령줄을 사용하여 원격으로 Series Security Appliance를 구성하는 경우 텔넷 또는 SSH를 사용해야 합니다.텔넷 통신은 비밀번호를 포함하는 일반 텍스트로 전송되므로 SSH를 사용하는 것이 좋습니다.SSH 트래픽은 터널에서 암호화되므로 암호와 기타 컨피그레이션 명령을 가로채기에서 보호할 수 있습니다.

Security Appliance에서는 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.

이 컨피그레이션 예에서는 PIX Security Appliance가 SSH 서버로 간주됩니다.SSH 클라이언트

(10.1.1.2/24 및 172.16.1.1/16)에서 SSH 서버로의 트래픽은 암호화됩니다.보안 어플라이언스는 SSH 버전 1 및 2에서 제공하는 SSH 원격 셸 기능을 지원하며 DES(Data Encryption Standard) 및 3DES 암호를 지원합니다.SSH 버전 1과 2는 서로 다르며 상호 운용이 불가능합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 Cisco PIX Firewall Software 버전 7.1 및 8.0을 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: SSHv2는 PIX/ASA 버전 7.x 이상에서 지원되며 7.x 이전 버전에서는 지원되지 않습니다.

관련 제품

이 컨피그레이션은 소프트웨어 버전 7.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

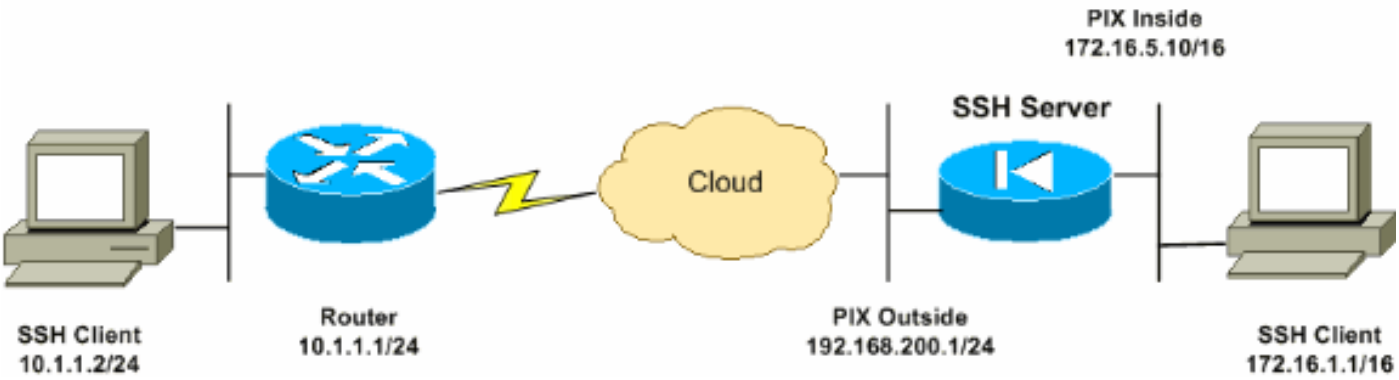
이 섹션에서는 이 문서에 설명된 기능을 구성하는 정보를 제공합니다.

참고: 각 컨피그레이션 단계에는 명령행 또는 ASDM(Adaptive Security Device Manager)을 사용하는 데 필요한 정보가 표시됩니다.

참고: 이 섹션에 사용된 명령에 대한 자세한 내용을 보려면 명령 조회 도구(등록된 고객만 해당)를 사용하십시오.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



SSH 구성

이 문서에서는 다음 구성을 사용합니다.

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

보안 어플라이언스에 대한 SSH 액세스

보안 어플라이언스에 대한 SSH 액세스를 구성하려면 다음 단계를 완료합니다.

1. SSH 세션에는 항상 인증을 위해 사용자 이름과 비밀번호가 필요합니다.이 요구 사항을 충족하는 두 가지 방법이 있습니다.사용자 이름 및 비밀번호를 구성하고 AAA를 사용합니다.구문:
   ```
   pix(config)#username username password password
   pix(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 지정하고 LOCAL(LOCAL은 대/소문자 구분)을 지정합니다. 보안 어플라이언스 프롬프트는 어떤 방법이 사용되는지 아무런 표시를 하지 않으므로 로컬 데이터베이스에서 AAA 서버와 동일한 사용자 이름과 비밀번호를 사용하는 것이 좋습니다.**참고:** 예:
   ```
   pix(config)#aaa authentication ssh console TACACS+ LOCAL
   ```

   참고: 대체(fallback) 없이 로컬 데이터베이스를 기본 인증 방법으로 사용할 수도 있습니다.이렇게 하려면 LOCAL만 입력합니다.예:
   ```
   pix(config)#aaa authentication ssh console LOCAL
   ```

   또는cisco의 기본 사용자 이름 및 기본 텔넷 비밀번호를 **사용합니다**.다음 명령을 사용하여 텔넷 비밀번호를 변경할 수 있습니다.
   ```
   pix(config)#passwd password
   ```

   참고: password 명령도 이 상황에서 사용할 수 있습니다.두 명령 모두 동일한 작업을 수행합니다.
2. SSH에 필요한 PIX 방화벽에 대한 RSA 키 쌍을 생성합니다.
   ```
   pix(config)#crypto key generate rsa modulus modulus_size
   ```

   참고: modulus _size(비트)는 512, 768, 1024 또는 2048이 될 수 있습니다.지정한 키 모듈러스 크기가 클수록 RSA 키 쌍을 생성하는 데 더 오래 걸립니다.1024 값을 사용하는 것이 좋습니다

.**참고:** RSA 키 쌍을 생성하는 데 사용되는 명령은 7.x 이전 버전의 PIX 소프트웨어에 대해 다릅니다.이전 버전에서는 키를 만들려면 먼저 도메인 이름을 설정해야 합니다.**참고:** 다중 컨텍스트 모드에서는 모든 컨텍스트에 대해 RSA 키를 생성해야 합니다.또한 crypto 명령은 시스템 컨텍스트 모드에서 지원되지 않습니다.

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 및 외부에 있는 하나의 호스트가 허용됩니다.

```
pix(config)#ssh 172.16.1.1 255.255.255.255 inside
pix(config)#ssh 10.1.1.2 255.255.255.255 outside
```

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

```
pix(config)# ssh version
```

참고: version_number는 1 또는 2일 수 있습니다.

5. **선택 사항:**기본적으로 SSH 세션은 5분 동안 활동이 없으면 닫힙니다.이 시간 제한은 1분에서 60분 동안 지속되도록 구성할 수 있습니다.

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

SSH 클라이언트 사용 방법

SSH 세션을 여는 동안 PIX 500 Series Security Appliance의 사용자 이름 및 로그인 비밀번호를 제공합니다.SSH 세션을 시작하면 SSH 사용자 인증 프롬프트가 표시되기 전에 점(.)이 보안 어플라이언스 콘솔에 표시됩니다.

```
hostname(config)# .
```

점 표시는 SSH 기능에 영향을 주지 않습니다.서버 키가 생성되거나 사용자 인증이 발생하기 전에 SSH 키 교환 중에 개인 키를 사용하여 메시지를 해독할 때 점이 콘솔에 나타납니다.이러한 작업은 최대 2분 이상 걸릴 수 있습니다.점은 보안 어플라이언스가 사용 중이고 정지되지 않았음을 확인하는 진행률 표시기입니다.

SSH 버전 1.x 및 2는 완전히 다른 프로토콜이며 호환되지 않습니다.호환되는 클라이언트를 다운로드합니다.자세한 내용은 Advanced Configurations의 Obtain an SSH Client 섹션을 참조하십시오.

PIX 컨피그레이션

이 문서에서는 다음 구성을 사용합니다.

PIX 컨피그레이션

```
PIX Version 7.1(1)
!
hostname pix
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0
 nameif outside
 security-level 0
```

```
 ip address 192.168.200.1 255.255.255.0
!
interface Ethernet1
 nameif inside
 security-level 100
 ip address 172.16.5.10 255.255.0.0
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
pager lines 24
mtu outside 1500
mtu inside 1500
no failover
icmp permit any outside
no asdm history enable
arp timeout 14400
route outside 10.1.1.0 255.255.255.0 192.168.200.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute

!--- AAA for the SSH configuration username ciscouser
password 3USUcOPFUiMCO4Jk encrypted
aaa authentication ssh console LOCAL

http server enable
http 172.16.0.0 255.255.0.0 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 10.1.1.2 255.255.255.255 outside

!--- Allows the users on the host 172.161.1.1 !--- to
access the security appliance !--- on the inside
interface. ssh 172.16.1.1 255.255.255.255 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
Cryptochecksum:a6b05fd04f9fbd0a39f1ca7328de91f7
: end
```

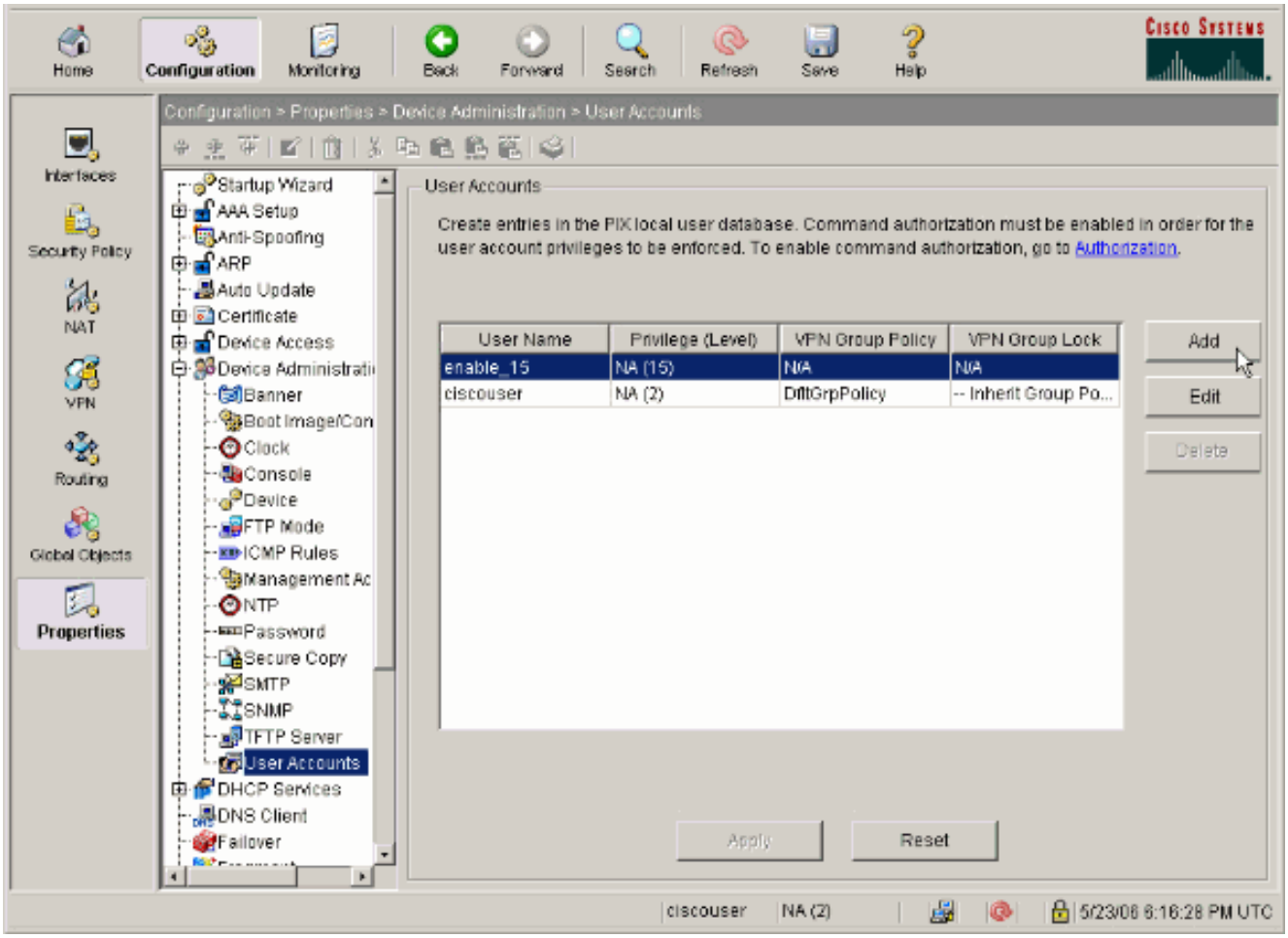
참고: SSH를 사용하여 ASA/PIX의 관리 인터페이스에 액세스하려면 다음 명령을 실행합니다.`ssh 172.16.16.160 255.255.255.255`

ASDM 5.x를 사용한 구성

ASDM을 사용하여 SSH용 디바이스를 구성하려면 다음 단계를 완료합니다.

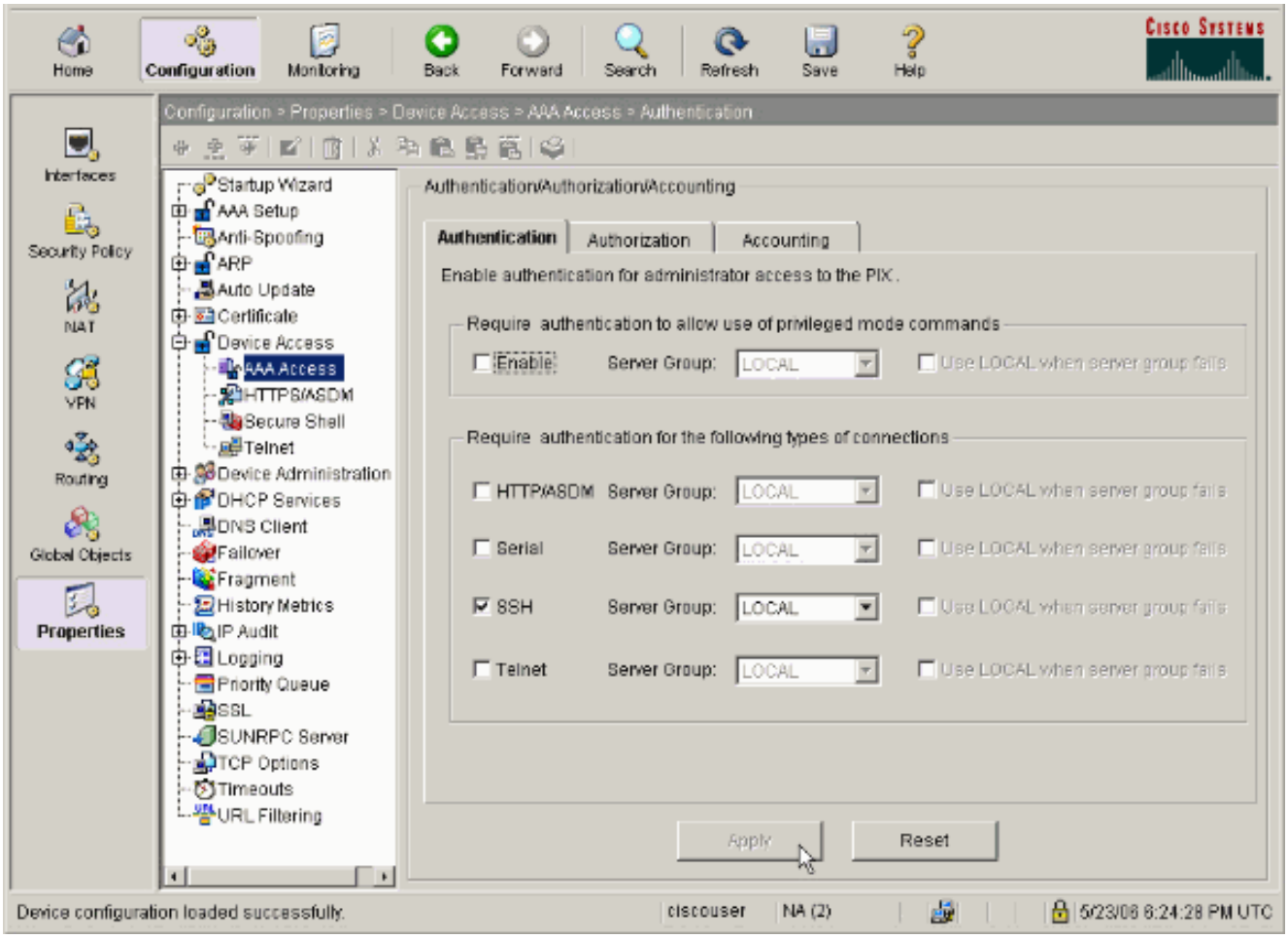
1. ASDM을 사용하는 사용자를 추가하려면 Configuration > Properties > Device Administration > User Accounts를 선택합니다

.



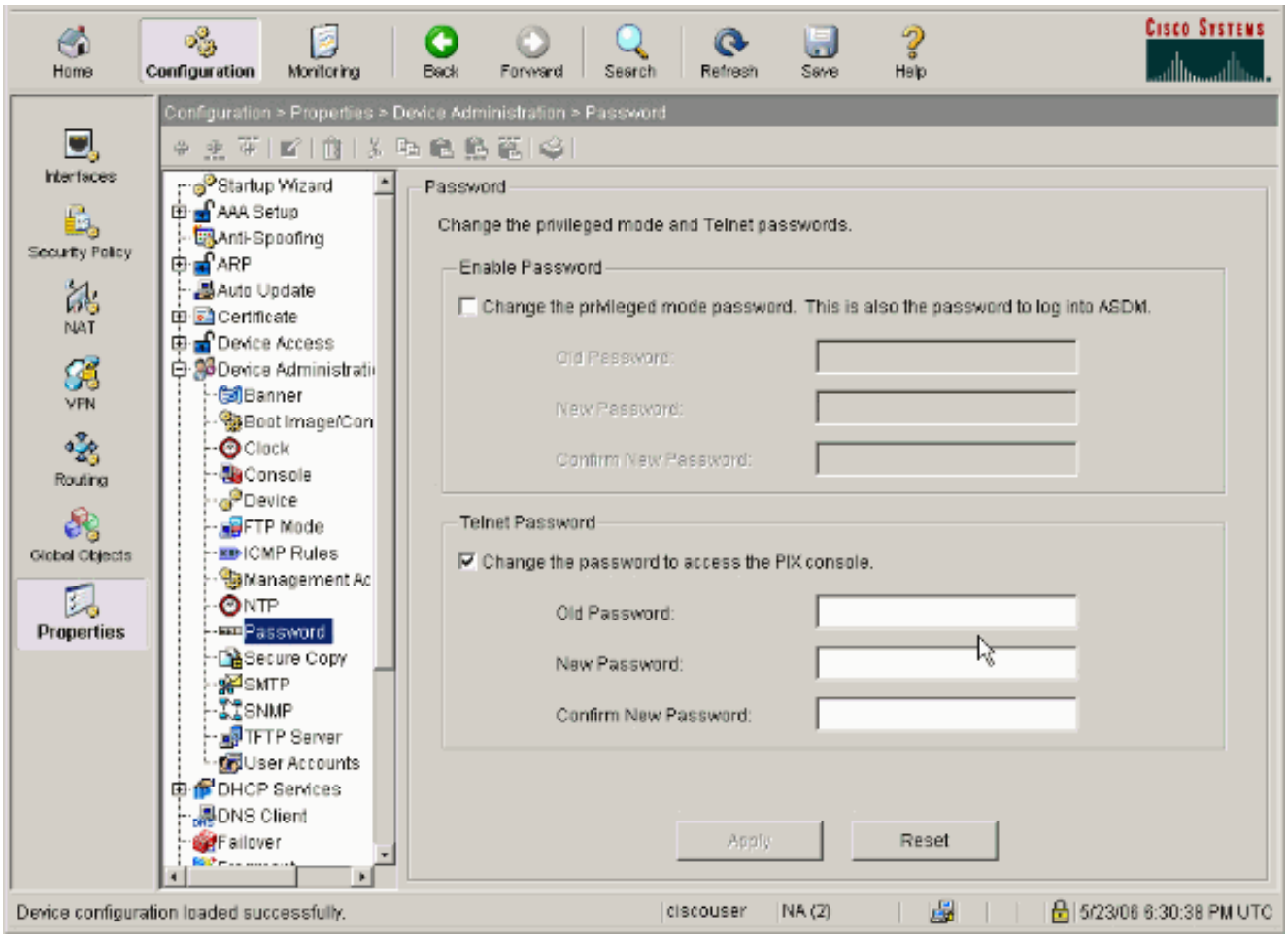
2. ASDM을 사용하는 SSH에 대한 AAA 인증을 설정하려면 Configuration > Properties > Device Access > AAA Access > Authentication을 선택합니다

.

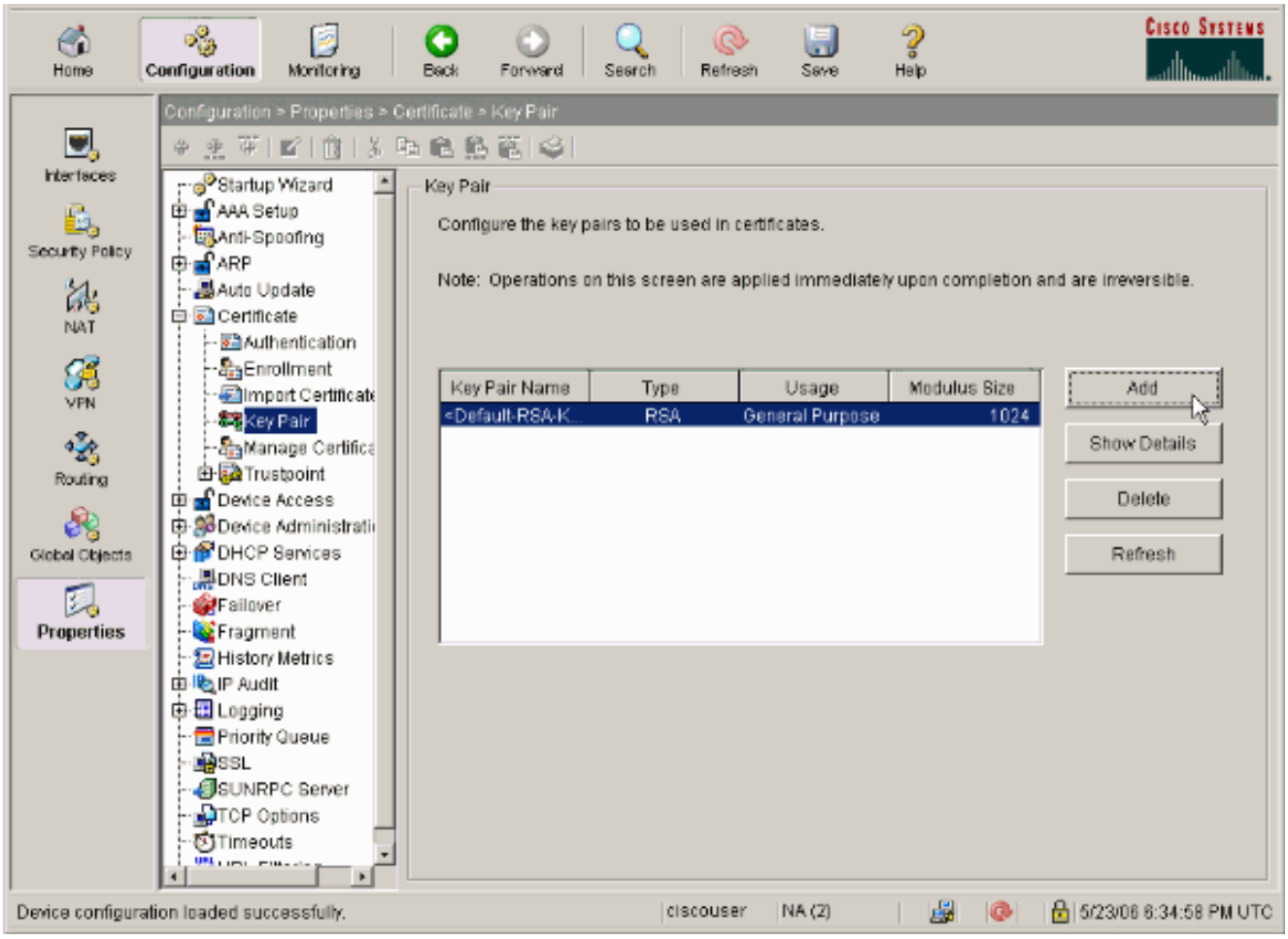


3. ASDM을 사용하여 텔넷 비밀번호를 변경하려면 Configuration > Properties > Device Administration > Password를 선택합니다

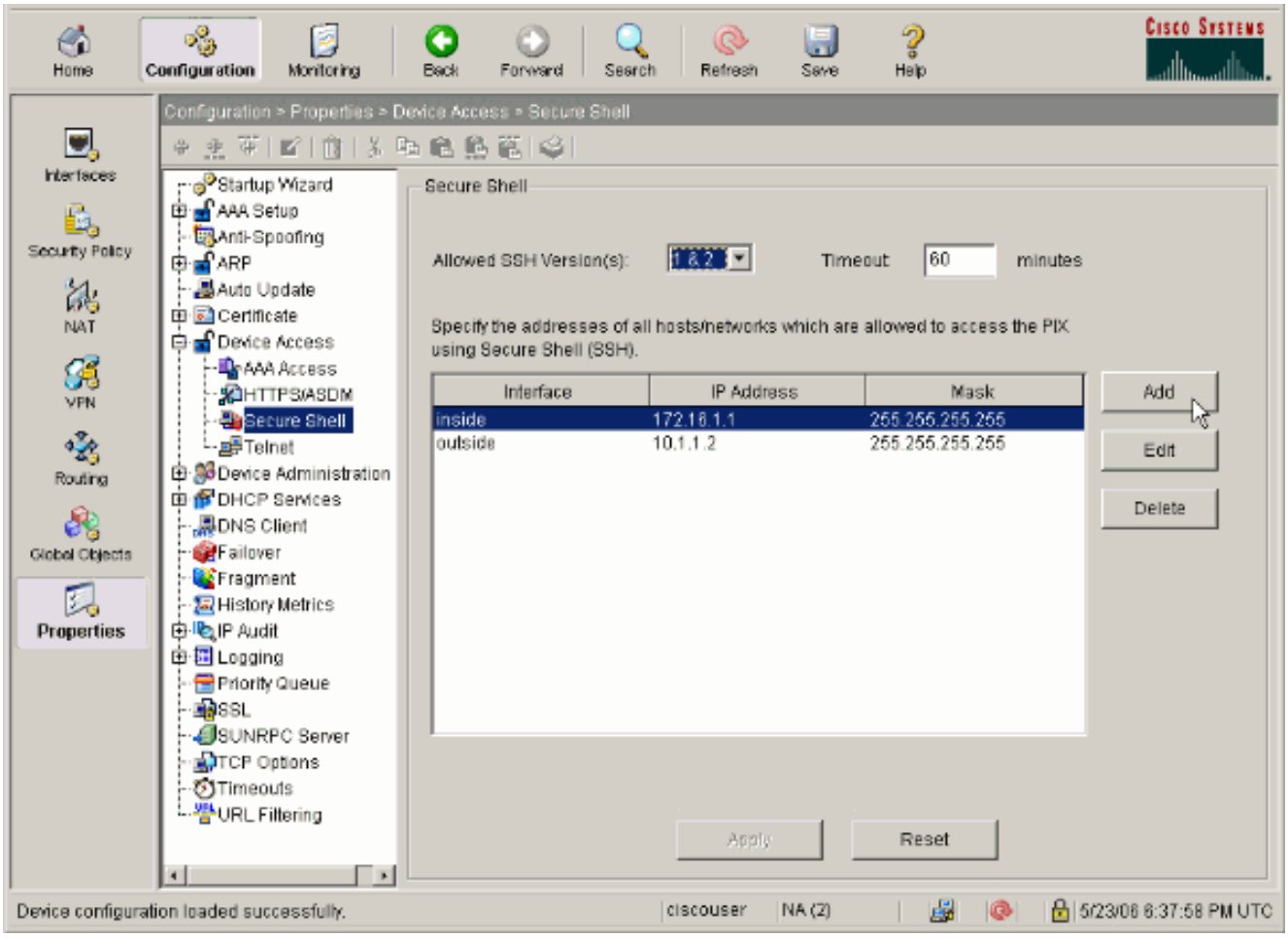
.



4. Configuration(**구성) > Properties(속성) > Certificate(인증서) > Key Pair(키 쌍)를** 선택하고 **Add(추가)**를 클릭하고 ASDM과 동일한 RSA 키를 생성하려면 제공된 기본 옵션을 사용합니다
.

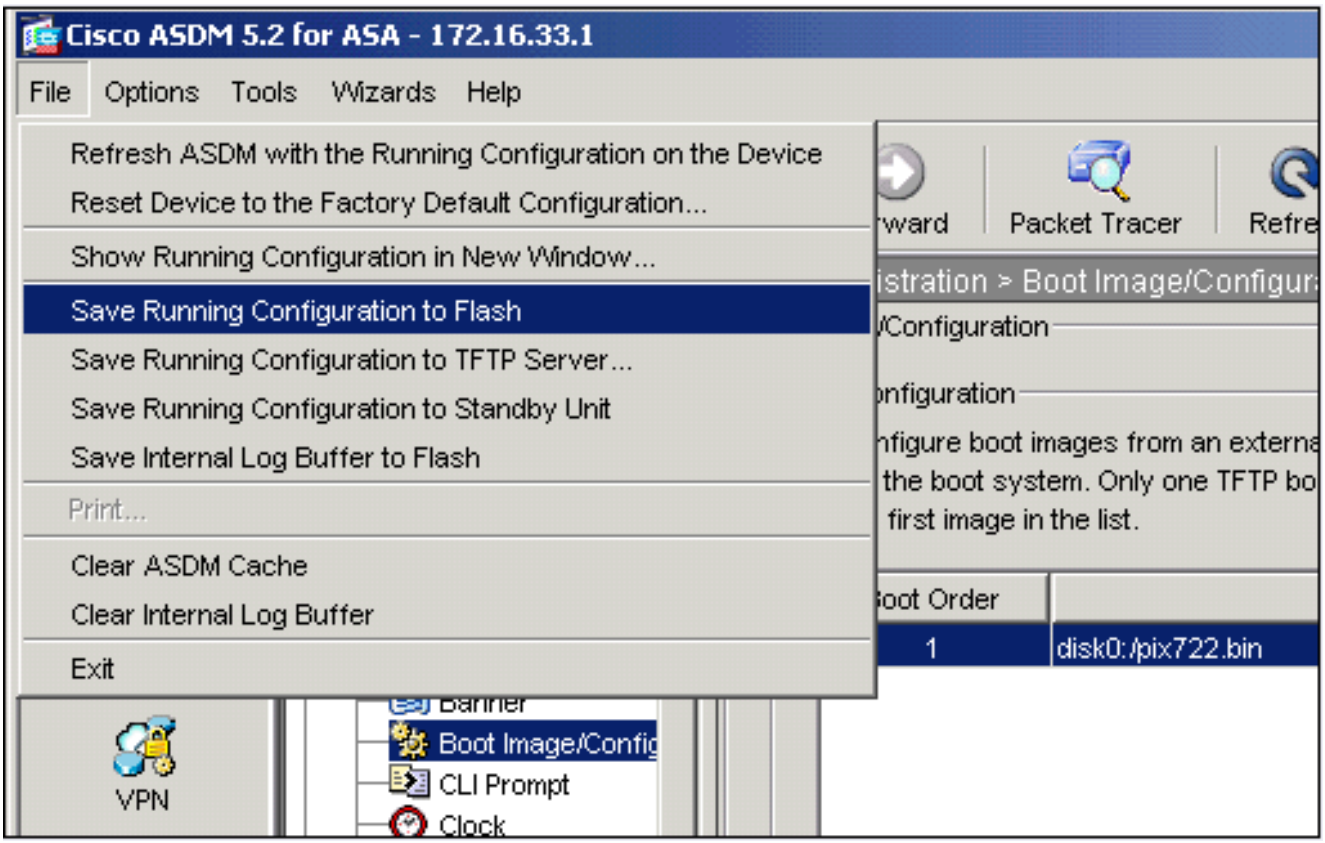


5. ASDM을 사용하여 SSH와 연결할 수 있는 호스트를 지정하고 버전 및 시간 제한 옵션을 지정하려면 Configuration **> Properties > Device Access > Secure Shell**을 선택합니다
.



6. 컨피그레이션을 저장하려면 **File(파일) > Save Running Configuration to Flash(실행 중인 컨피그레이션을 플래시에 저장)**를 클릭합니다

.

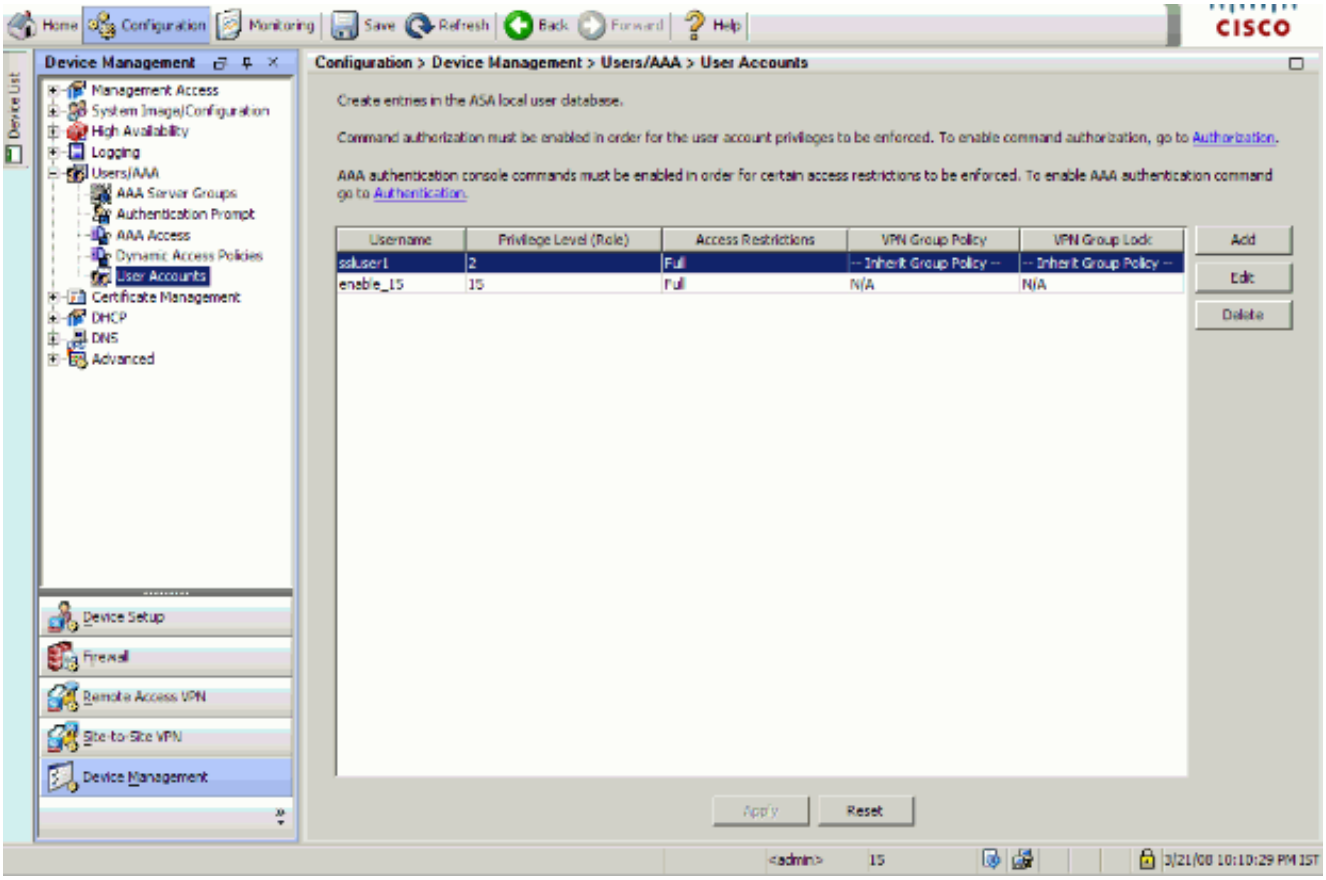


ASDM 6.x를 사용한 구성

다음 단계를 완료하십시오.

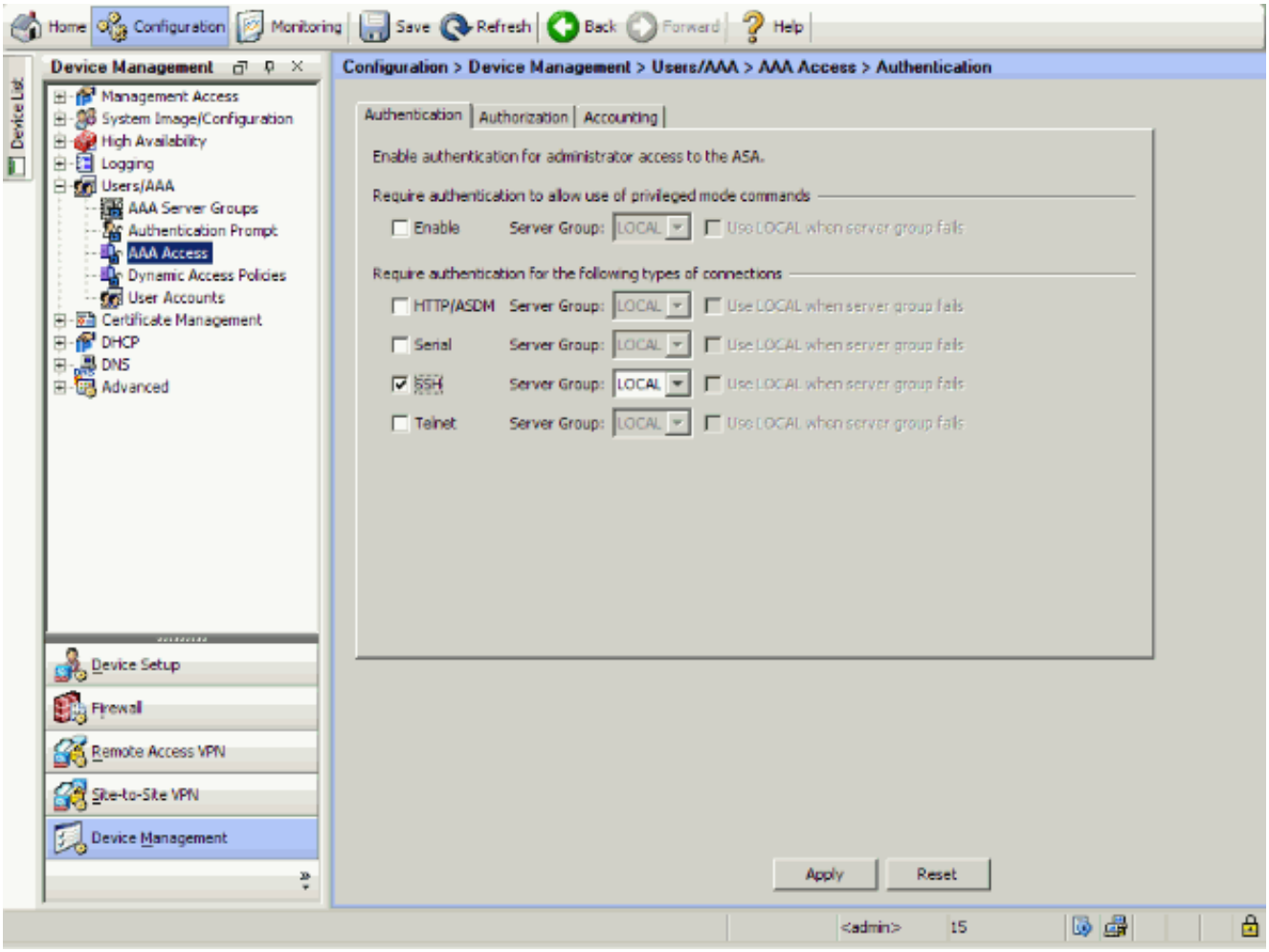
1. ASDM을 사용하는 사용자를 추가하려면 Configuration > Device Management > Users/AAA > User Accounts를 선택합니다

.



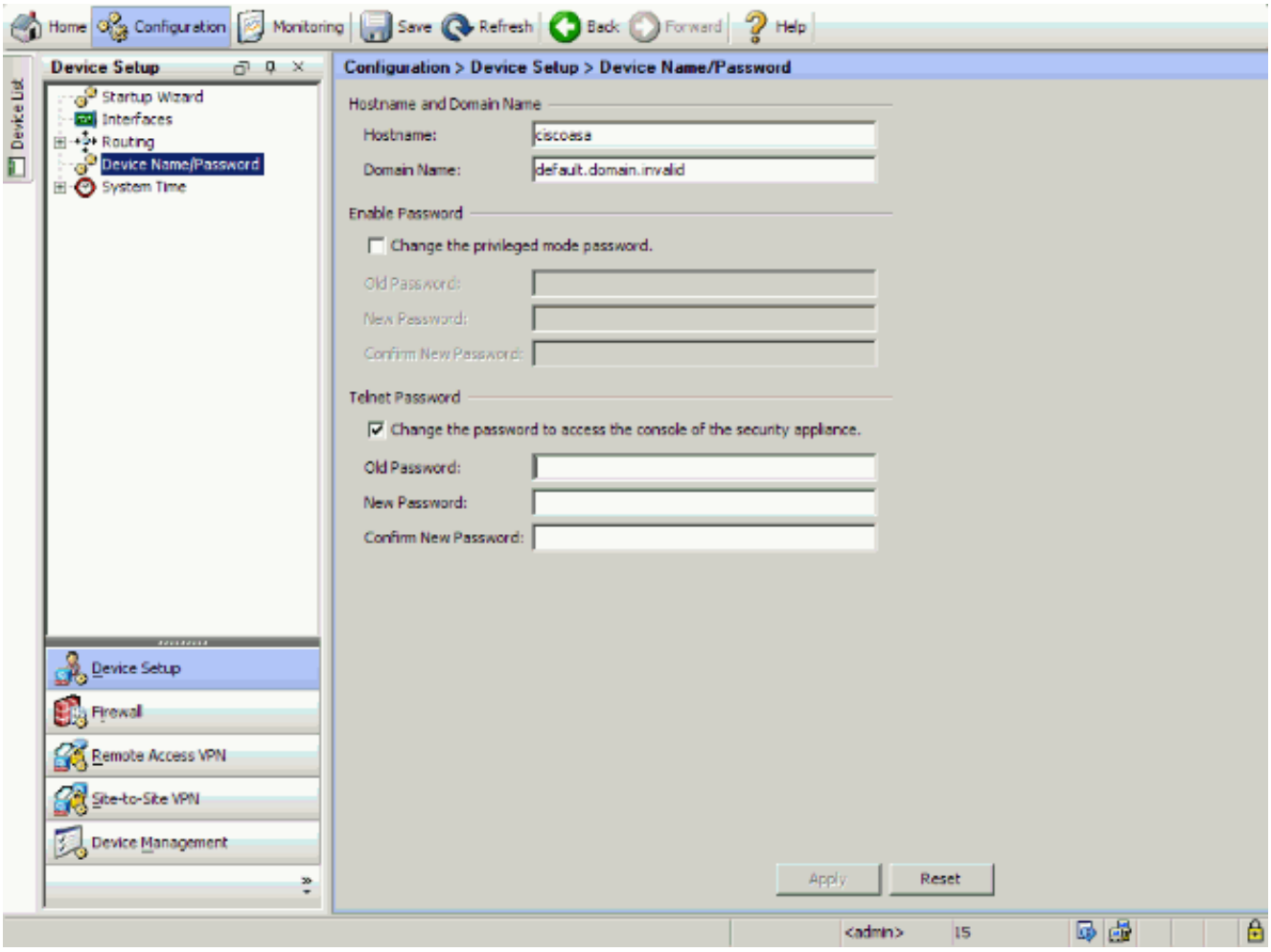
2. ASDM을 통한 SSH에 대한 AAA 인증을 설정하려면 **Configuration > Device Management > Users/AAA > AAA Access > Authentication**을 선택합니다

.



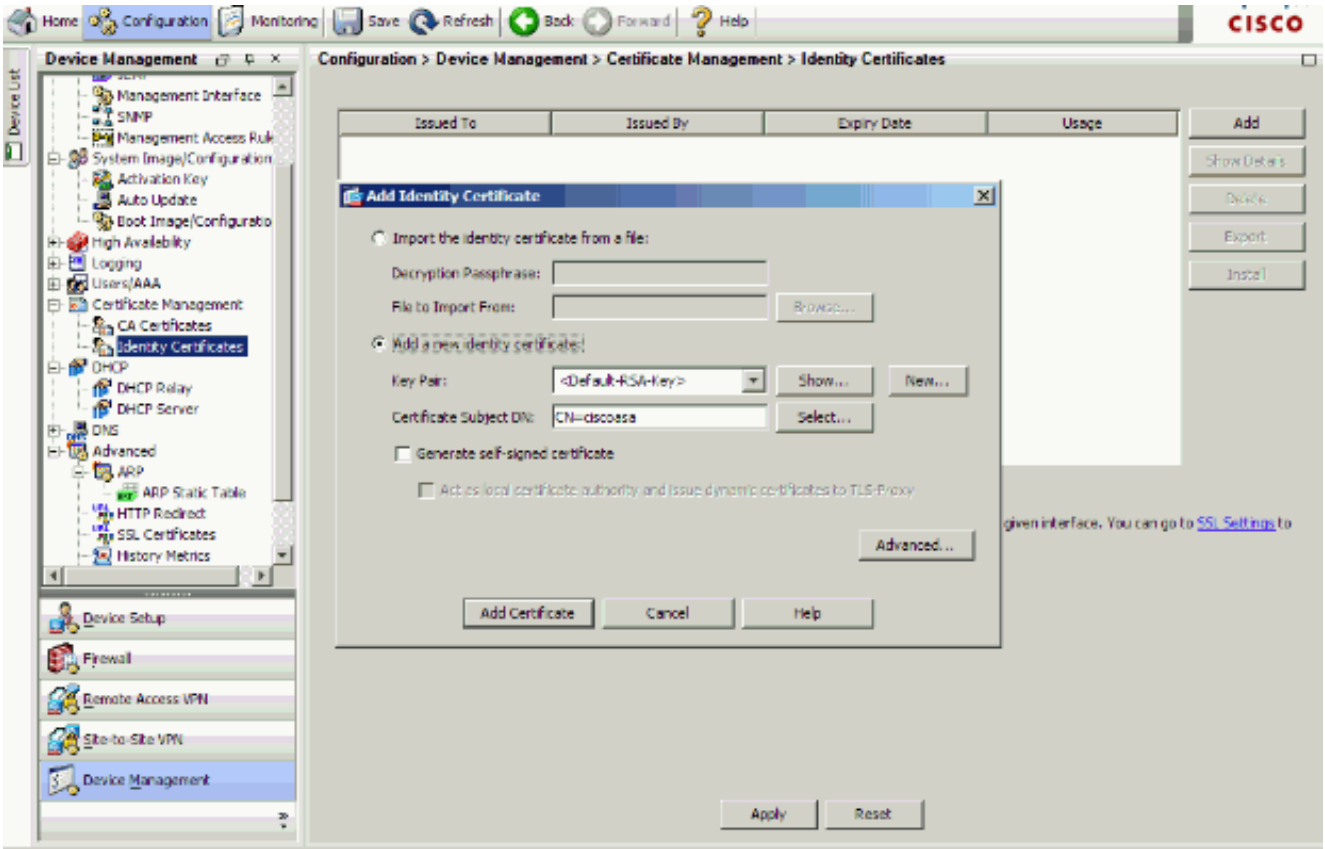
3. ASDM을 사용하여 텔넷 비밀번호를 변경하려면 Configuration **> Device Setup > Device Name/Password**를 선택합니다

.



4. Configuration(**구성**) > **Device Management(디바이스 관리)** > **Certificate Management(인증서 관리)** > **Identity Certificates(ID 인증서)**를 선택하고 **Add(추가)**를 클릭하고 제공된 기본 옵션을 사용하여 ASDM과 동일한 RSA 키를 생성합니다

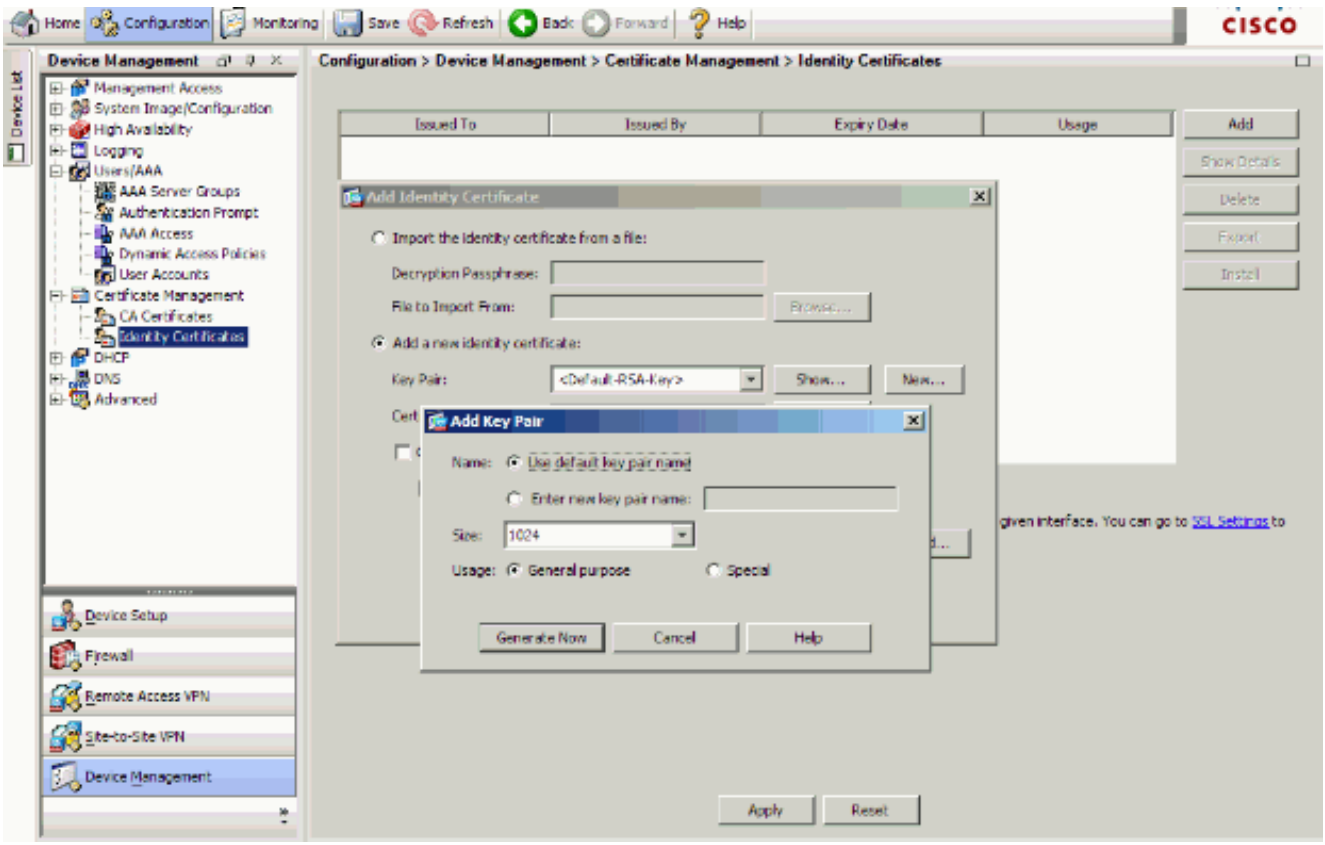
.



5. Add **a new Identity certificate(새 ID 인증서 추가)**에서 **New(새로 만들기)**를 클릭하여 기본 키

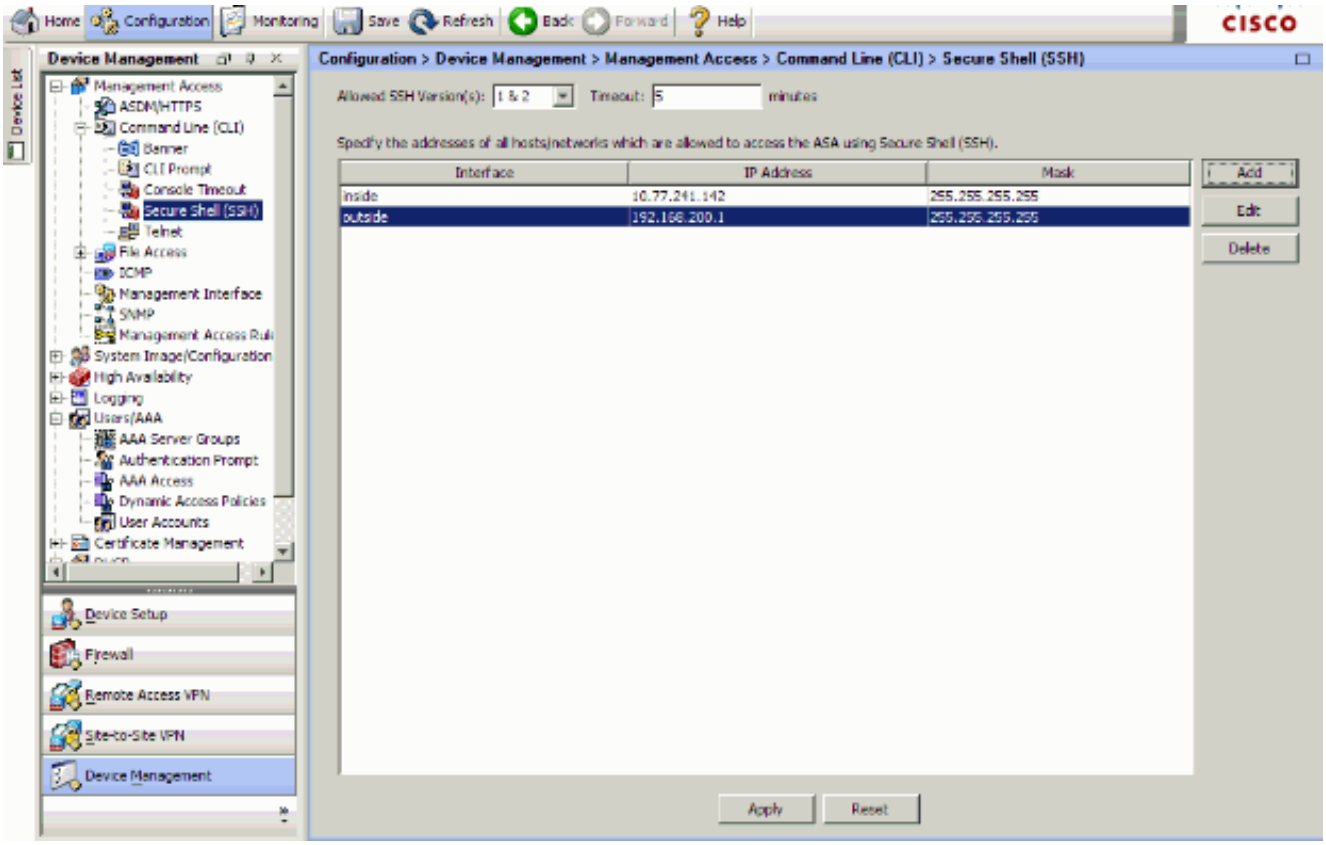
쌍이 없는 경우 기본 키 쌍을 추가합니다.그런 다음 Generate Now(**지금 생성)를 클릭합니다**

.



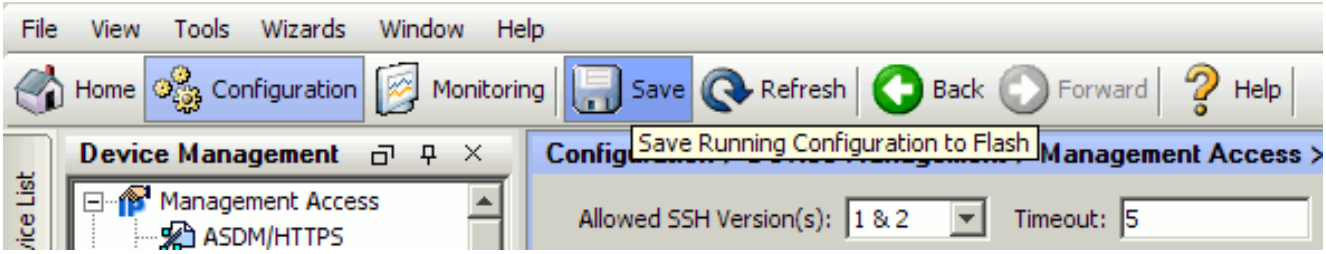
6. ASDM을 사용하여 SSH와 연결할 수 있는 호스트를 지정하고 버전 및 시간 제한 옵션을 지정하려면 Configuration **> Device Management > Management Access > Command Line (CLI) > Secure Shell (SSH)**을 선택합니다

.



7. 구성을 저장하려면 창 상단에 있는 저장을 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 실행합니다.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 텔넷으로 보안 어플라이언스 콘솔에 액세스할 수 있는 호스트를 지정할 수 있습니다.

참고: 모든 인터페이스에서 보안 어플라이언스에 텔넷을 활성화할 수 있습니다.그러나 보안 어플라이언스는 외부 인터페이스에 대한 모든 텔넷 트래픽을 IPsec으로 보호하도록 적용합니다.외부 인터페이스에 대한 텔넷 세션을 활성화하려면 보안 어플라이언스에서 생성된 IP 트래픽을 포함하도록 외부 인터페이스에서 IPsec을 구성하고 외부 인터페이스에서 텔넷을 활성화합니다.

참고: 일반적으로 보안 레벨이 다른 인터페이스보다 0 또는 낮은 인터페이스가 있으면 PIX/ASA에서 해당 인터페이스에 텔넷을 허용하지 않습니다.

참고: 텔넷 세션을 통해 보안 어플라이언스에 액세스하는 것은 권장되지 않습니다.비밀번호와 같은 인증 자격 증명 정보는 일반 텍스트로 전송됩니다.텔넷 서버 및 클라이언트 통신은 일반 텍스트로만 이루어집니다.Cisco에서는 더 안전한 데이터 통신을 위해 SSH를 사용하는 것이 좋습니다.

IP 주소를 입력할 경우 넷마스크도 입력해야 합니다.기본 넷마스크는 없습니다.내부 네트워크의 하위 네트워크 마스크를 사용하지 마십시오.넷마스크는 IP 주소의 비트 마스크입니다.단일 IP 주소에 대한 액세스를 제한하려면 각 8진에서 255를 사용합니다.예: 255.255.255.255.

IPsec이 작동하는 경우 비보안 인터페이스 이름(일반적으로 외부 인터페이스)을 지정할 수 있습니다.최소한 **telnet** 명령을 사용하여 인터페이스 이름을 지정하기 위해 **crypto map** 명령을 구성할 수 있습니다.

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

내부 인터페이스에 대한 텔넷 세션을 활성화하려면 다음 예를 검토하십시오.

예 1

다음 예에서는 호스트 10.1.1.1만 텔넷을 통해 보안 어플라이언스 콘솔에 액세스할 수 있도록 허용합니다.

```
pix(config)#telnet 10.1.1.1 255.255.255.255 inside
```

예: 2:

다음 예에서는 텔넷을 통해 보안 어플라이언스 콘솔에 액세스할 수 있도록 네트워크 10.0.0.0/8만 허용합니다.

```
pix(config)#telnet 10.0.0.0 255.0.0.0 inside
```

예: 3:

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

```
pix(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 텔넷 콘솔 액세스에 대한 인증을 요구하기 위해 aaa 명령을 구성한 경우 콘솔 로그인 요청 시간이 초과되면 직렬 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
```

ACS 4.x의 SSH/텔넷 지원

RADIUS 기능을 보면 SSH 기능에 RADIUS를 사용할 수 있습니다.

텔넷, SSH, HTTP 또는 시리얼 콘솔 연결을 사용하여 보안 어플라이언스에 액세스하려고 시도했지만 트래픽이 인증 문과 일치하면 보안 어플라이언스는 사용자 이름과 비밀번호를 요청합니다.그런 다음 이러한 자격 증명을 RADIUS(ACS) 서버로 전송하고 서버의 응답을 기반으로 CLI 액세스를 허용하거나 거부합니다.

자세한 내용은 AAA 서버 구성 및 로컬 데이터베이스의 AAA 서버 및 로컬 데이터베이스 지원 섹션을 참조하십시오.

예를 들어, ASA 보안 어플라이언스 7.0에는 보안 어플라이언스가 연결을 허용하는 IP 주소가 필요합니다. 이를테면 다음과 같습니다.

```
hostname(config)#ssh source_IP_address mask source_interface
```

자세한 내용은 AAA 서버 구성 및 로컬 데이터베이스의 SSH 액세스 허용 섹션을 참조하십시오.

PIX/ASA 참조:TACACS+ 및 RADIUS 서버 컨피그레이션을 사용한 네트워크 액세스용 컷스루 프록시 ACS 인증을 사용하여 PIX에 대한 SSH/텔넷 액세스를 구성하는 방법에 대한 자세한 내용은 Cut-through Proxy for Network Access의 예를 참조하십시오.

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

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

디버그 SSH

SSH 디버깅을 켜려면 debug ssh 명령을 실행합니다.

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

이 출력은 호스트 10.1.1.2(외부에서 PIX로)에서 "pix"로 인증 요청이 성공했음을 보여줍니다.

```
pix#
Device ssh opened successfully.
   SSH0: SSH client: IP = '10.1.1.2' interface # = 1
   SSH: host key initialised
   SSH0: starting SSH control process
   SSH0: Exchanging versions - SSH-1.99-Cisco-1.25
SSH0: send SSH message: outdata is NULL
server version string:SSH-1.99-Cisco-1.25SSH0: receive SSH message: 83 (83)
   SSH0: client version is - SSH-1.99-3.2.0 SSH Secure Shell for Windows
client version string:SSH-1.99-3.2.0 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 receivedSSH(pix): user authen method is
'no AAA', aaa server group ID = 0
   SSH(pix): user authen method is 'no AAA', aaa server group ID = 0
```

SSH2 0: authentication successful for pix
!--- Authentication for the PIX 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

사용자가 잘못된 사용자 이름(예: "pix" 대신 "pix1")을 지정하면 PIX 방화벽은 인증을 거부합니다.이 디버그 출력은 실패한 인증을 보여줍니다.

```
pix#
Device ssh opened successfully.
SSH0: SSH client: IP = '10.1.1.2' interface # = 1
SSH: host key initialised
SSH0: starting SSH control process
SSH0: Exchanging versions - SSH-1.99-Cisco-1.25
SSH0: send SSH message: outdata is NULL
server version string:SSH-1.99-Cisco-1.25SSH0: receive SSH message: 83 (83)
SSH0: client version is - SSH-1.99-3.2.0 SSH Secure Shell for Windows client version
    string:SSH-1.99-3.2.0 SSH Secure Shell for WindowsSSH0: begin server key generation
SSH0: complete server key generation, elapsed time = 1960 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 receivedSSH(pix1): user authen method is
'no AAA', aaa server group ID = 0
SSH(pix1): user authen method is 'no AAA', aaa server group ID = 0
SSH2 0: authentication failed for pix1
!--- Authentication for pix1 was not successful due to the wrong username.
```

마찬가지로 사용자가 잘못된 비밀번호를 제공할 경우 이 디버그 출력에는 실패한 인증이 표시됩니다.

```
pix#
Device ssh opened successfully.
SSH0: SSH client: IP = '10.1.1.2'  interface # = 1
SSH: host key initialised
SSH0: starting SSH control process
SSH0: Exchanging versions - SSH-1.99-Cisco-1.25
SSH0: send SSH message: outdata is NULL server version string:
SSH-1.99-Cisco-1.25SSH0: receive      SSH message: 83 (83)
SSH0: client version is - SSH-1.99-3.2.0 SSH Secure Shell for
Windows client version string:SSH-1.99-3.2.0
SSH Secure Shell for WindowsSSH0: begin server key generation
SSH0: complete server key generation, elapsed time = 1920 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 receivedSSH(pix): user authen method
is 'no AAA', aaa server group ID = 0
     SSH(pix): user authen method is 'no AAA', aaa server group ID = 0
SSH2 0: authentication failed for pixSSH(pix): user authen method
is 'no AAA', aaa server group ID = 0
SSH2 0: authentication failed for pix
!--- Authentication for PIX was not successful due to the wrong password.
```

활성 SSH 세션 보기

연결된 SSH 세션 수 및 PIX에 대한 연결 상태를 확인하려면 다음 명령을 실행합니다.

```
pix#show ssh session

SID Client IP       Version Mode Encryption Hmac     State            Username
0   10.1.1.2        1.99    IN   aes128-cbc md5      SessionStarted   pix
                            OUT  aes128-cbc md5      SessionStarted   pix
```

ASDM을 **사용하는** 세션을 보려면 **Monitoring > Properties > Device Access > Secure Shell Sessions**를 선택합니다.

공용 RSA 키 보기

보안 어플라이언스에서 RSA 키의 공용 부분을 보려면 다음 명령을 실행합니다.

```
pix#show crypto key mypubkey rsa

Key pair was generated at: 19:36:28 UTC May 19 2006
Key name: <Default-RSA-Key>
 Usage: General Purpose Key
 Modulus Size (bits): 1024
 Key Data:

  30819f30 0d06092a 864886f7 0d010101 05000381 8d003081 89028181 00c172f4
  95f66c34 2c2ced37 aa3442d8 12158c93 131480dd 967985ab 1d7b92d9 5290f695
  8e9b5b0d d88c0439 6169184c d8fb951c 19023347 d6b3f939 99ac2814 950f4422
  69b67328 f64916b1 82e15341 07590da2 390fbefd 38758888 7319196c de61aef1
  165c4bab 03d081d5 ddaf15cc c9ddb204 c2b451e0 f19ce0f3 485b1d69 8b020301 0001
```

ASDM이 있는 RSA 키**를 보려면 Configuration > Properties > Certificate > Key Pair**를 선택하고 **Show Details**를 클릭합니다.

문제 해결

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

PIX에서 RSA 키를 제거하는 방법

PIX 소프트웨어를 업그레이드하거나 PIX에서 SSH 버전을 변경하는 경우 RSA 키를 제거하고 다시 생성해야 하는 경우가 있습니다.PIX에서 RSA 키 쌍을 제거하려면 다음 명령을 실행합니다.

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

Configuration > **Properties > Certificate > Key Pair**를 선택하고 **Delete**를 클릭하여 ASDM과 함께 RSA 키를 제거합니다.

SSH 연결 실패

PIX/ASA의 오류 메시지:

```
%PIX|ASA-3-315004: Fail to establish SSH session because RSA host key retrieval failed.
```

SSH 클라이언트 시스템의 해당 오류 메시지:

```
Selected cipher type
```

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

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

새 키를 생성하려면 다음 명령을 실행합니다.

```
ASA(config)# crypto key generate rsa modulus 1024
```

SSH로 ASA에 액세스할 수 없음

오류 메시지:

```
ssh_exchange_identification: read: Connection reset by peer
```

이 문제를 해결하려면 다음 단계를 완료하십시오.

1. ASA를 다시 로드하거나 모든 SSH 관련 컨피그레이션 및 RSA 키를 제거합니다.
2. SSH 명령을 재구성하고 RSA 키를 재생성합니다.

SSH를 사용하여 보조 ASA에 액세스할 수 없음

ASA가 장애 조치 모드에 있는 경우 VPN 터널을 통해 대기 ASA에 SSH를 연결할 수 없습니다.이는 SSH에 대한 응답 트래픽이 대기 ASA의 외부 인터페이스를 사용하기 때문입니다.

관련 정보

- Cisco PIX 500 Series 보안 어플라이언스
- Cisco ASA 5500 Series Adaptive Security Appliance
- Cisco PIX 방화벽 소프트웨어
- Cisco Secure PIX Firewall 명령 참조
- SSH 연결 구성 - Cisco 라우터 및 Cisco Concentrator
- RFC(Request for Comments)
- 기술 지원 및 문서 – Cisco Systems