PIX/ASA 7.x: SSH/Telnet auf der internen und externen Schnittstelle - Konfigurationsbeispiel

Inhalt

Einführung

Dieses Dokument enthält eine Beispielkonfiguration von Secure Shell (SSH) auf den Innen- und Außenschnittstellen der Cisco Series Security Appliance Version 7.x und höher. Bei der Remote-Konfiguration der Security Appliance mit der Befehlszeile wird Telnet oder SSH verwendet. Da Telnet-Kommunikation in Klartext mit Kennwörtern versendet wird, wird SSH dringend empfohlen. SSH-Datenverkehr wird in einem Tunnel verschlüsselt und schützt so Kennwörter und andere Konfigurationsbefehle vor Abfangen.

Die Sicherheits-Appliance ermöglicht zu Verwaltungszwecken SSH-Verbindungen mit der Sicherheits-Appliance. Die Sicherheits-Appliance ermöglicht maximal fünf gleichzeitige SSH-Verbindungen für jeden Sicherheitskontext, sofern verfügbar, und ein globales Maximum von 100 Verbindungen für alle Kontexte zusammen.

In diesem Konfigurationsbeispiel wird die PIX Security Appliance als SSH-Server angesehen. Der Datenverkehr von SSH-Clients (10.1.1.2/24 und 172.16.1.1/16) zum SSH-Server wird verschlüsselt. Die Sicherheits-Appliance unterstützt die SSH-Remote-Shell-Funktionalität der SSH-Versionen 1 und 2 und unterstützt DES- (Data Encryption Standard) und 3DES-Verschlüsselungen. SSH-Versionen 1 und 2 sind unterschiedlich und nicht interoperabel.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der Cisco PIX Firewall Software, Version 7.1 und 8.0.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hinweis: SSHv2 wird in PIX/ASA Version 7.x und höher unterstützt und in Versionen vor 7.x nicht unterstützt.

Zugehörige Produkte

Diese Konfiguration kann auch mit der Cisco Security Appliance der Serie ASA 5500 mit den Softwareversionen 7.x und höher verwendet werden.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Konfigurieren

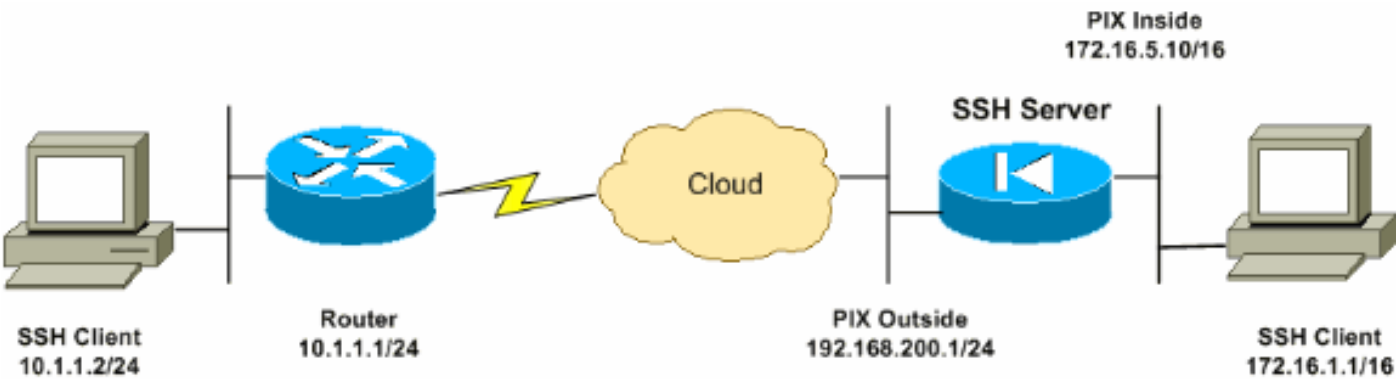
In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Jeder Konfigurationsschritt enthält die erforderlichen Informationen für die Verwendung der Befehlszeile oder des Adaptive Security Device Manager (ASDM).

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



SSH-Konfigurationen

In diesem Dokument werden folgende Konfigurationen verwendet:

- SSH-Zugriff auf die Sicherheits-Appliance
- Verwenden eines SSH-Clients
- PIX-Konfiguration

SSH-Zugriff auf die Sicherheits-Appliance

Gehen Sie wie folgt vor, um den SSH-Zugriff auf die Sicherheits-Appliance zu konfigurieren:

1. SSH-Sitzungen erfordern für die Authentifizierung immer einen Benutzernamen und ein Kennwort. Es gibt zwei Möglichkeiten, diese Anforderung zu erfüllen.Konfigurieren Sie einen Benutzernamen und ein Kennwort, und verwenden Sie AAA:Syntax:
   ```
   pix(config)#username username password password
   pix(config)#aaa authentication {telnet | ssh | http | serial} console {LOCAL |
   server_group [LOCAL]}
   ```

   Hinweis: Wenn Sie eine TACACS+- oder RADIUS-Servergruppe für die Authentifizierung verwenden, können Sie die Sicherheits-Appliance so konfigurieren, dass sie die lokale Datenbank als Fallbackmethode verwendet, wenn der AAA-Server nicht verfügbar ist. Geben Sie den Namen der Servergruppe und anschließend LOCAL an (LOCAL ist Groß- und Kleinschreibung zu beachten). Es wird empfohlen, in der lokalen Datenbank denselben Benutzernamen und dasselbe Kennwort wie beim AAA-Server zu verwenden, da bei der Aufforderung zur Sicherheitsappliance nicht angegeben wird, welche Methode verwendet wird.**Hinweis:** Beispiel:
   ```
   pix(config)#aaa authentication ssh console TACACS+ LOCAL
   ```

   Hinweis: Alternativ können Sie die lokale Datenbank als Hauptauthentifizierungsmethode ohne Fallback verwenden. Geben Sie dazu nur LOCAL ein.Beispiel:
   ```
   pix(config)#aaa authentication ssh console LOCAL
   ```

   ODERVerwenden Sie den Standardbenutzernamen **pix** und das Telnet-Standardkennwort von **cisco**. Sie können das Telnet-Kennwort mit dem folgenden Befehl ändern:
   ```
   pix(config)#passwd password
   ```

   Hinweis: In dieser Situation kann der Befehl **password** verwendet werden. Beide Befehle tun dasselbe.

2. Generieren Sie ein RSA-Schlüsselpaar für die PIX-Firewall, das für SSH erforderlich ist:
   `pix(config)#crypto key generate rsa modulus modulus_size`

   Hinweis: Die `modulus_size` (in Bits) kann 512, 768, 1024 oder 2048 sein. Je größer die Modulusgröße, desto länger dauert die Generierung des RSA-Schlüsselpaars. Der Wert von 1024 wird empfohlen.**Hinweis:** Der Befehl zum Generieren eines RSA-Schlüsselpaars unterscheidet sich für PIX-Softwareversionen vor 7.x. In früheren Versionen muss ein Domänenname festgelegt werden, bevor Schlüssel erstellt werden können.**Hinweis:** Im Mehrfachkontextmodus müssen Sie die RSA-Schlüssel für jeden Kontext generieren. Darüber hinaus werden Krypto-Befehle im Systemkontextmodus nicht unterstützt.
3. Geben Sie die Hosts an, die eine Verbindung zur Sicherheits-Appliance herstellen dürfen.Mit diesem Befehl werden die Quelladresse, die Netzmaske und die Schnittstelle des Hosts angegeben, der bzw. die eine Verbindung mit SSH herstellen darf. Sie kann für mehrere Hosts, Netzwerke oder Schnittstellen mehrfach eingegeben werden. In diesem Beispiel ist ein Host auf der Innenseite und ein Host auf der Außenseite zulässig.
   ```
   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. **Optional:** Standardmäßig ist die Sicherheits-Appliance für SSH-Version 1 und -Version 2 zulässig. Geben Sie diesen Befehl ein, um Verbindungen auf eine bestimmte Version zu beschränken:
   `pix(config)# ssh version`

   Hinweis: Die `Versionsnummer` kann 1 oder 2 sein.
5. **Optional:** Standardmäßig werden SSH-Sitzungen nach fünf Minuten Inaktivität geschlossen. Diese Zeitüberschreitung kann so konfiguriert werden, dass sie 1 bis 60 Minuten lang andauert.
   `pix(config)#ssh timeout minutes`

Verwenden eines SSH-Clients

Geben Sie beim Öffnen der SSH-Sitzung den Benutzernamen und das Anmeldekennwort der Sicherheitslösung der Serie PIX 500 an. Wenn Sie eine SSH-Sitzung starten, wird in der Konsole der Sicherheitslösung ein Punkt (.) angezeigt, bevor die Aufforderung zur SSH-Benutzerauthentifizierung angezeigt wird:

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

Die Anzeige des Punkts hat keinen Einfluss auf die Funktionalität von SSH. Der Punkt wird an der Konsole angezeigt, wenn ein Serverschlüssel generiert oder eine Nachricht mit privaten Schlüsseln entschlüsselt wird, bevor die Benutzerauthentifizierung erfolgt. Diese Aufgaben können bis zu zwei Minuten oder länger dauern. Der Punkt ist eine Fortschrittsanzeige, die überprüft, ob die Sicherheits-Appliance besetzt ist und nicht geklingelt hat.

SSH-Versionen 1.x und 2 sind völlig unterschiedliche Protokolle und nicht kompatibel. Laden Sie einen kompatiblen Client herunter. Weitere Informationen finden Sie im Abschnitt SSH-Client im Abschnitt Erweiterte Konfigurationen.

PIX-Konfiguration

In diesem Dokument wird diese Konfiguration verwendet:

PIX-Konfiguration

```
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, !-
```

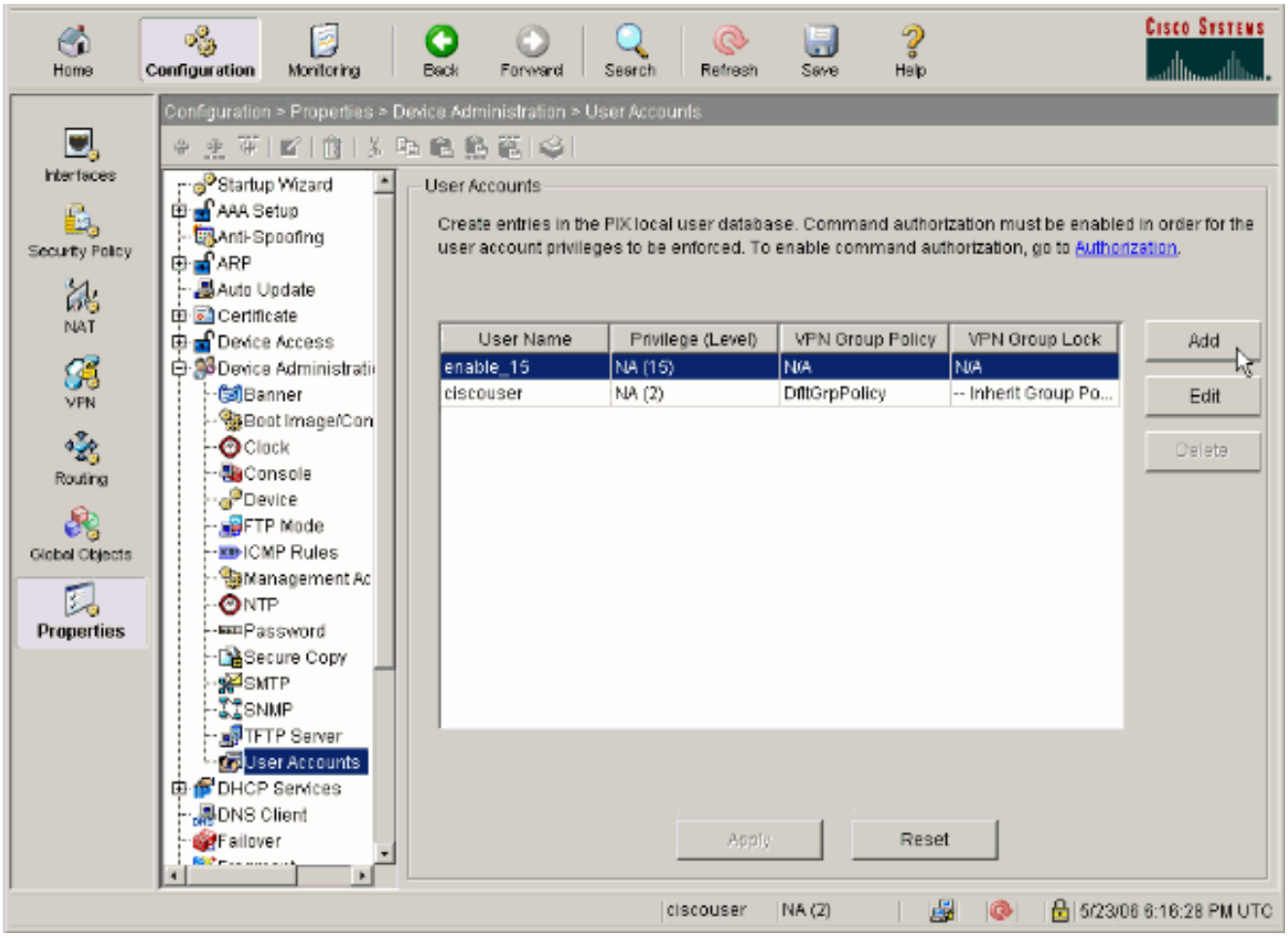
```
-- before the security appliance disconnects the
session. ssh timeout 60

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
```

Hinweis: Führen Sie folgenden Befehl aus, um über SSH auf die Verwaltungsschnittstelle von ASA/PIX zuzugreifen: `SSH 172.16.16.160 Verwaltung 255.255.255.255`

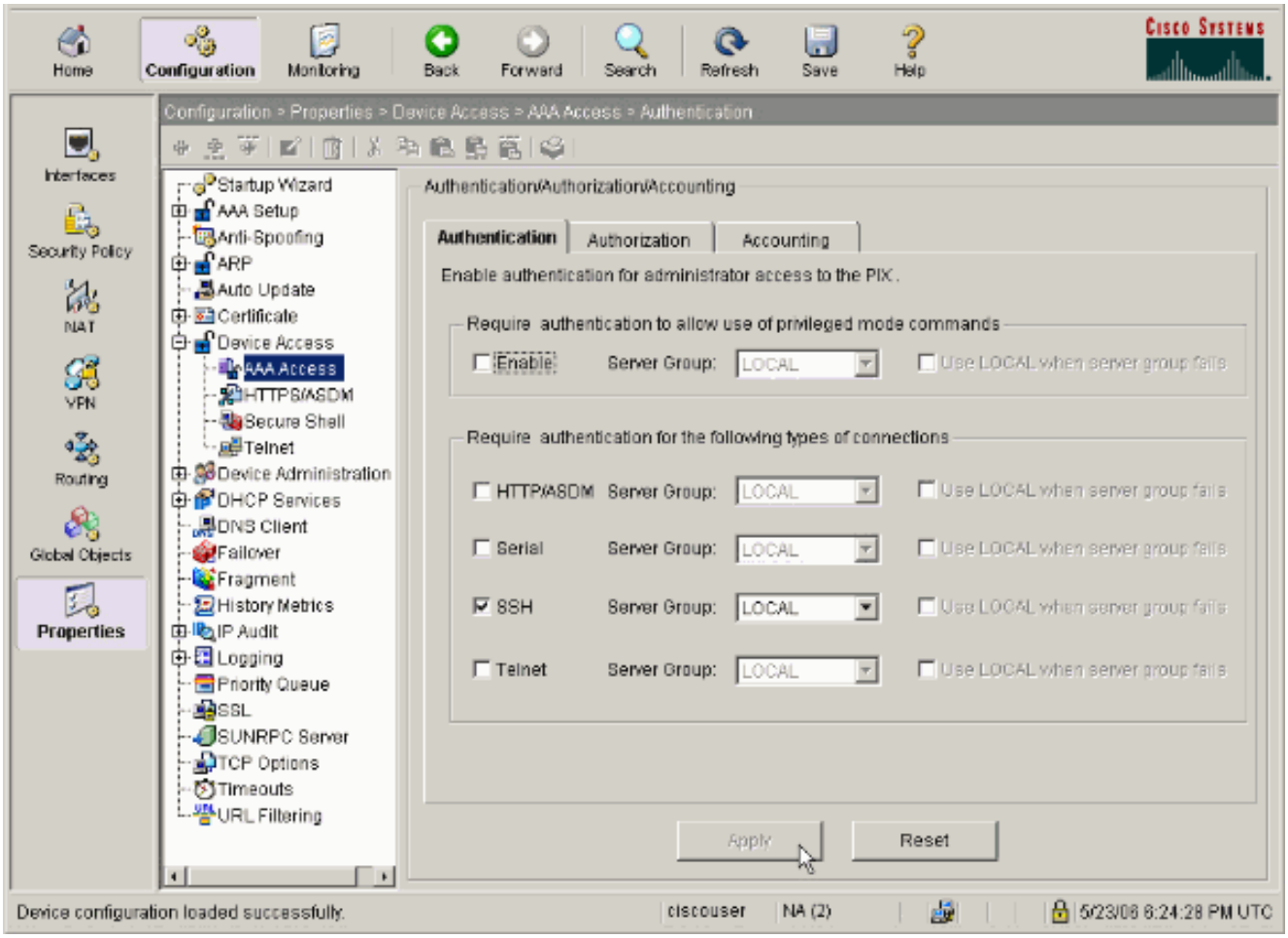
Konfiguration mit ASDM 5.x

Gehen Sie wie folgt vor, um das Gerät für SSH mithilfe von ASDM zu konfigurieren:

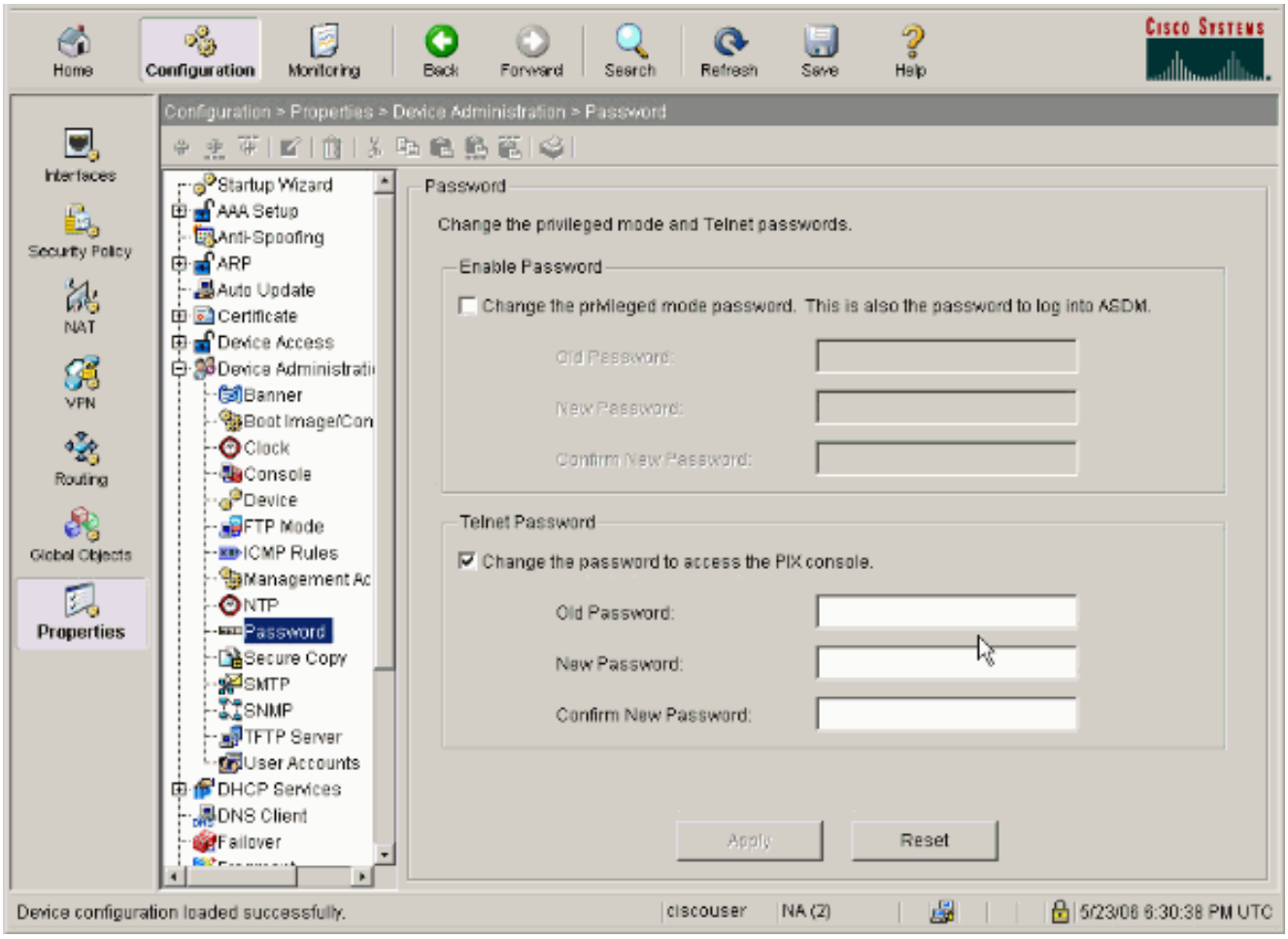
1. Wählen Sie **Configuration > Properties > Device Administration > User Accounts (Konfiguration > Eigenschaften > Geräteverwaltung > Benutzerkonten)**, um einen Benutzer mit ASDM
   hinzuzufügen.



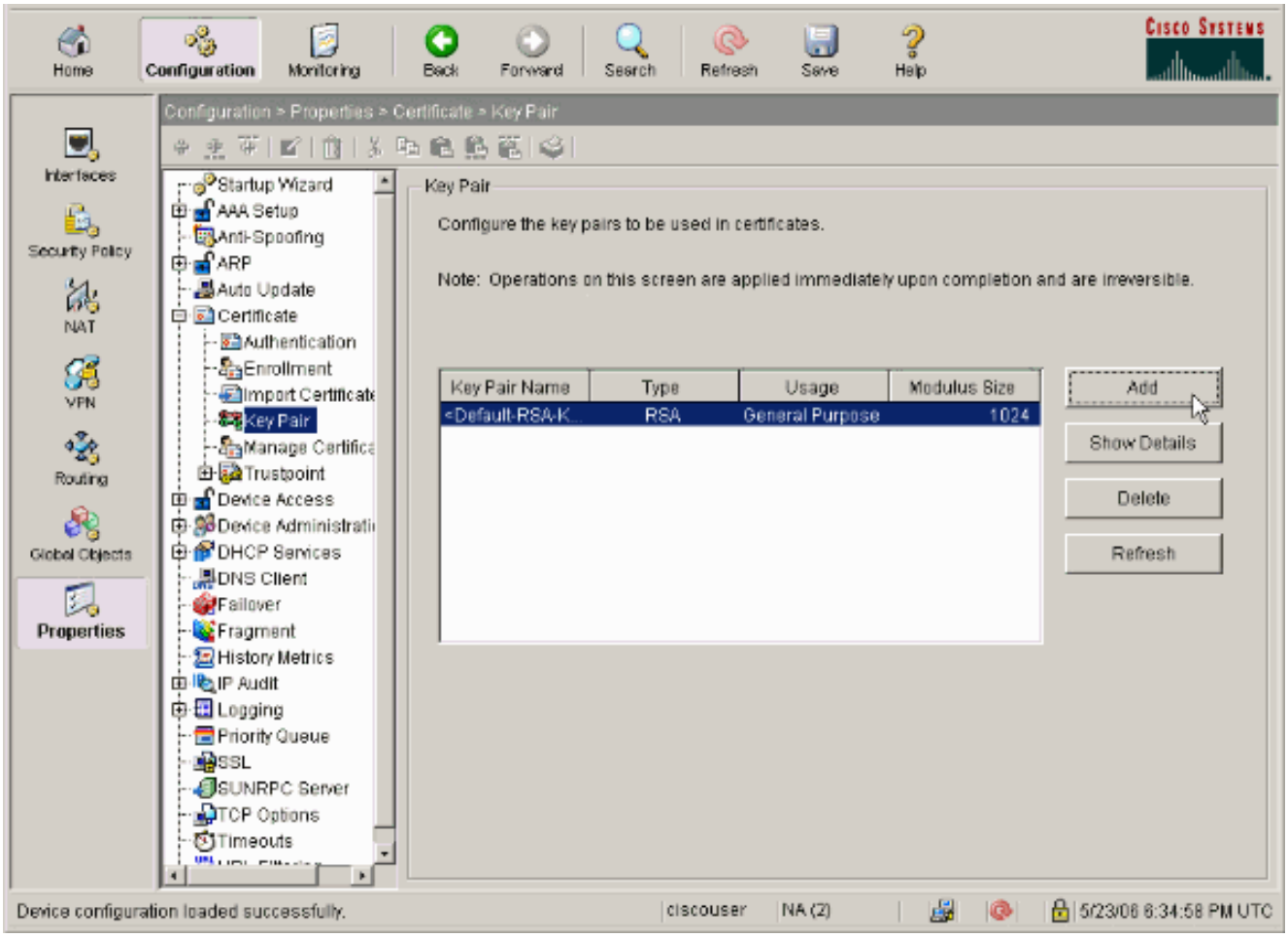
2. Wählen Sie **Configuration > Properties > Device Access > AAA Access > Authentication**, um die AAA-Authentifizierung für SSH mit ASDM einzurichten.



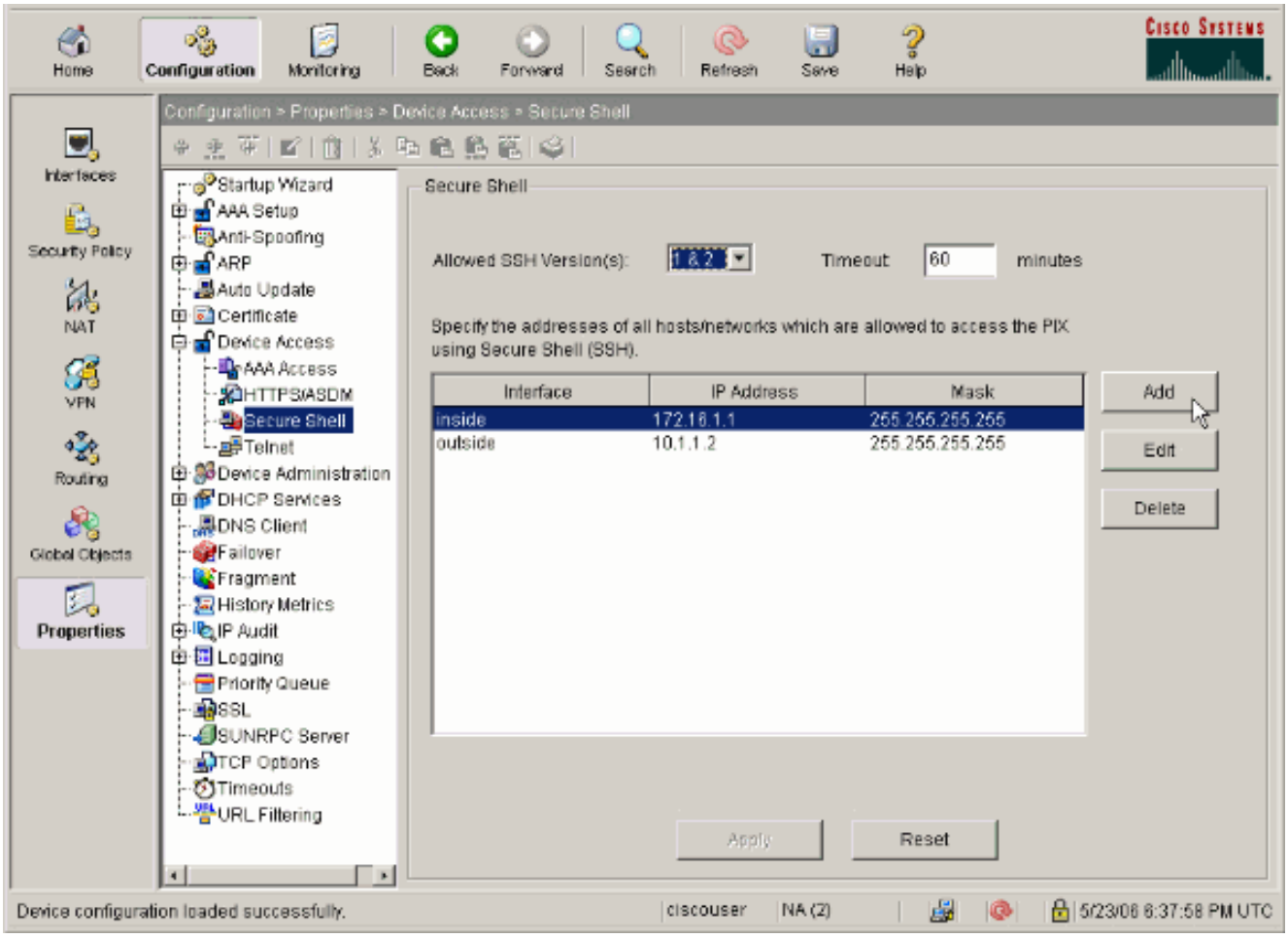
3. Wählen Sie **Configuration > Properties > Device Administration > Password (Konfiguration > Eigenschaften > Geräteverwaltung > Kennwort)**, um das Telnet-Kennwort mit ASDM zu ändern.



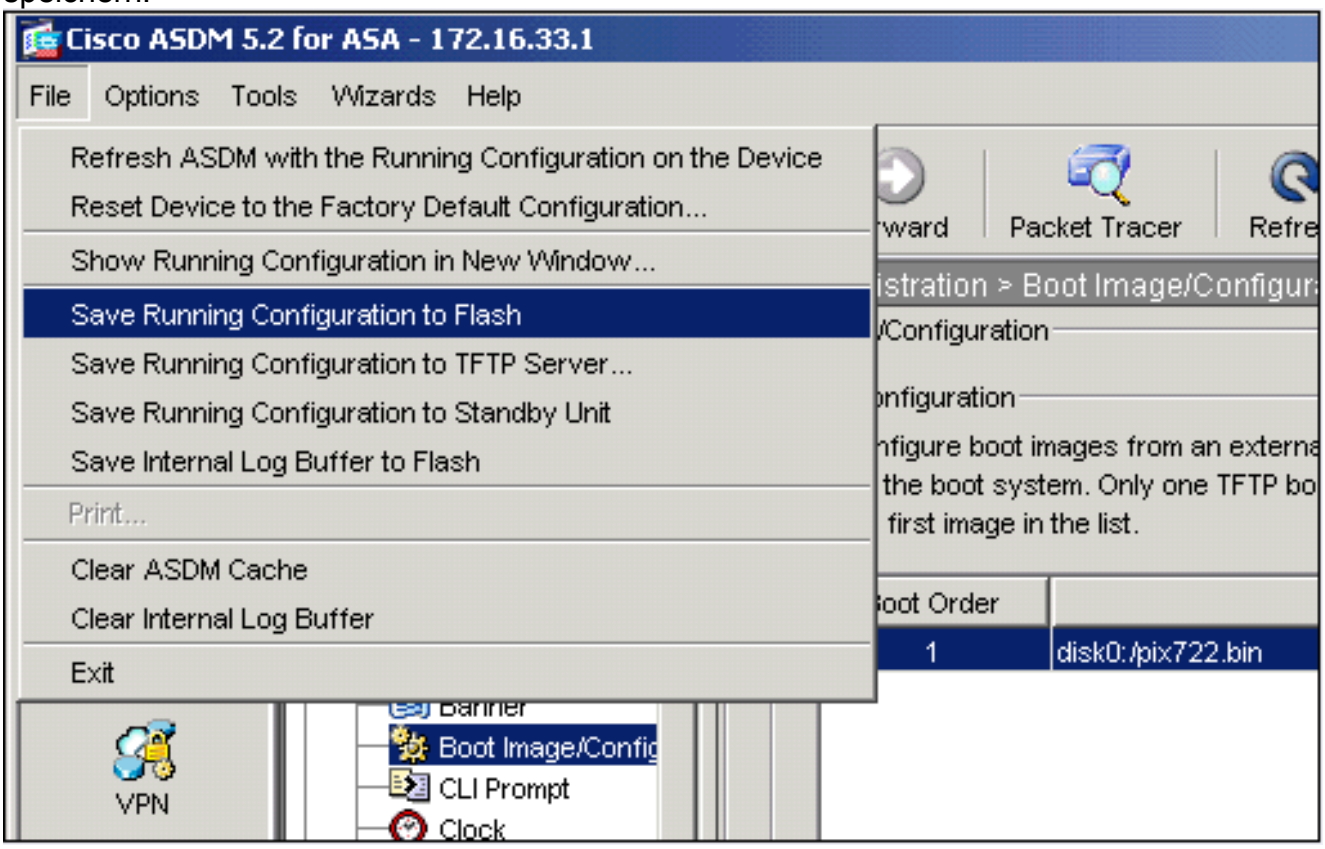
4. Wählen Sie **Konfiguration > Eigenschaften > Zertifikat > Schlüsselpaar**, klicken Sie auf **Hinzufügen**, und verwenden Sie die angezeigten Standardoptionen, um die gleichen RSA-Schlüssel mit ASDM zu
generieren.



5. Wählen Sie **Configuration > Properties > Device Access > Secure Shell**, um ASDM zum Festlegen von Hosts zu verwenden, die eine Verbindung mit SSH herstellen dürfen, und um die Version und die Timeout-Optionen anzugeben.



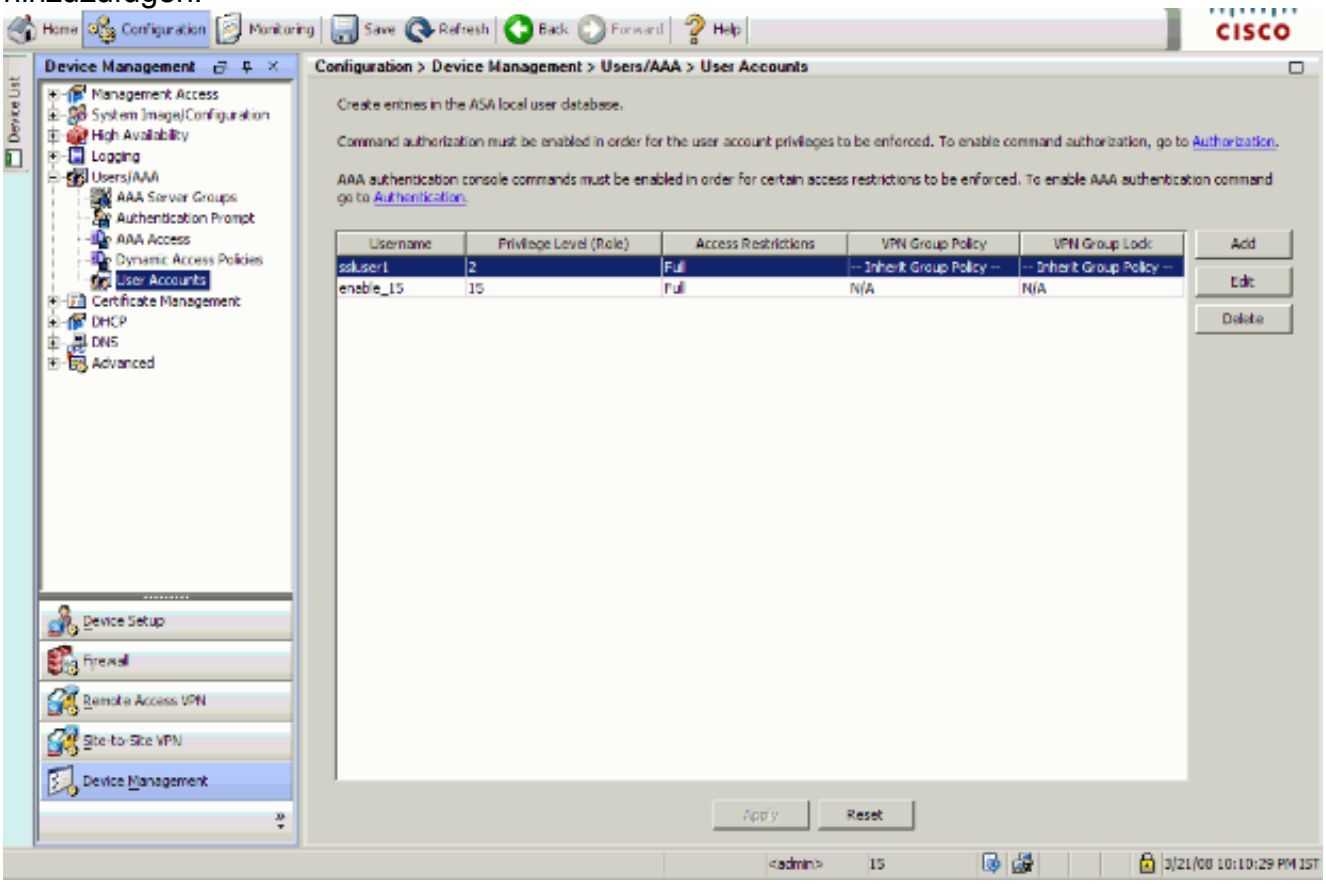
6. Klicken Sie auf **Datei > Running Configuration in Flash speichern**, um die Konfiguration zu speichern.



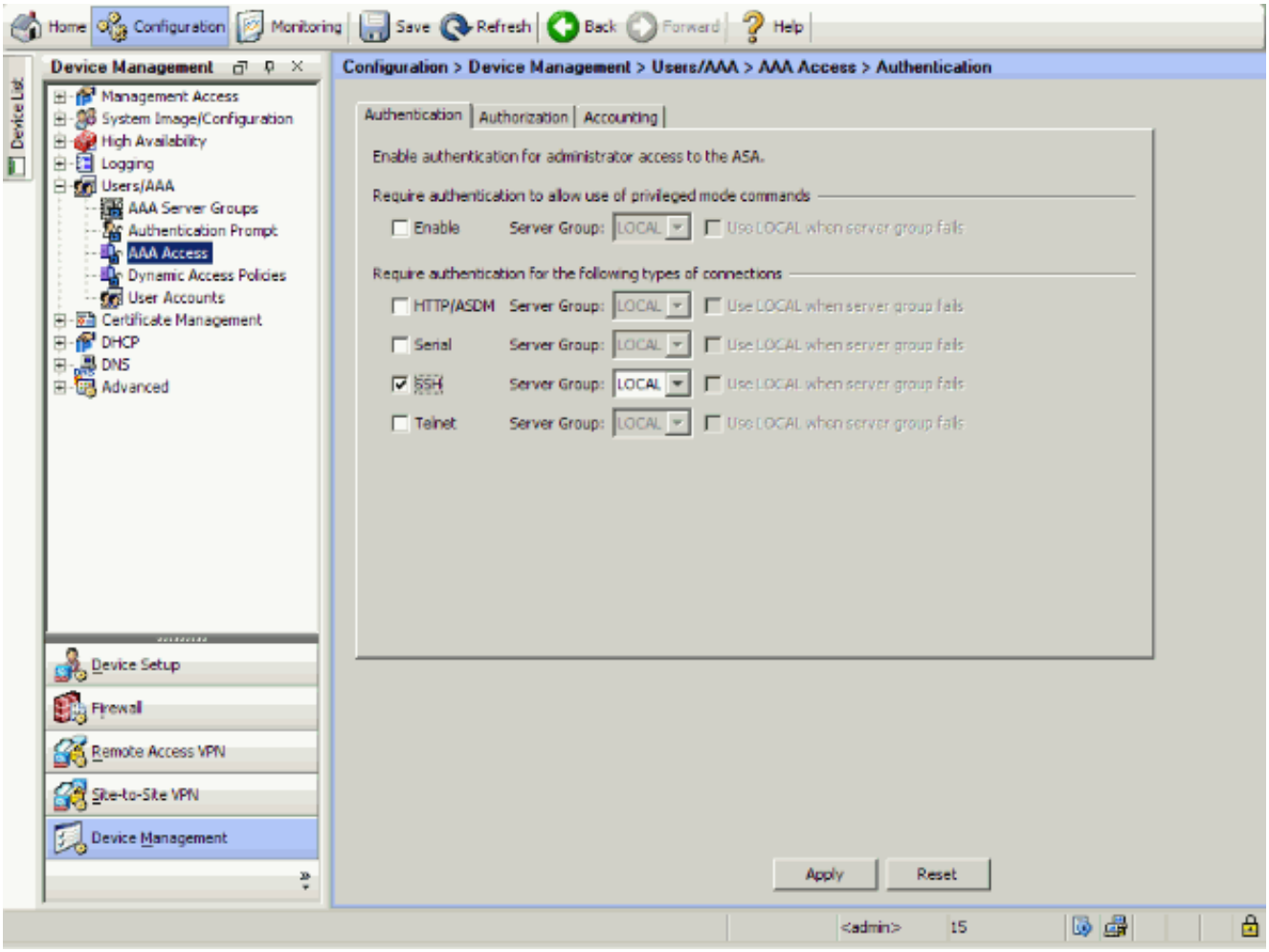
Konfiguration mit ASDM 6.x

Gehen Sie wie folgt vor:

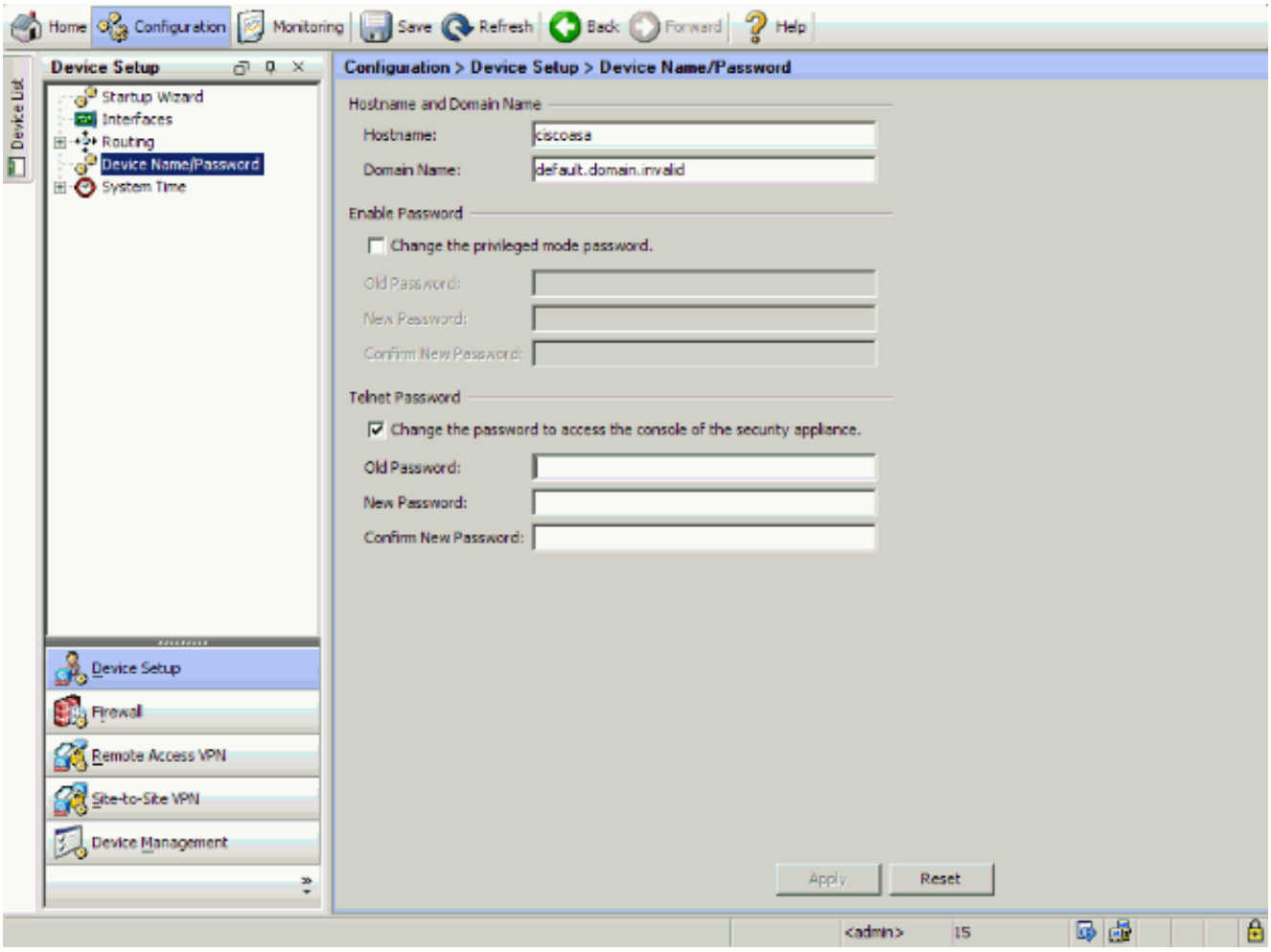
1. Wählen Sie **Configuration > Device Management > Users/AAA > User Accounts**, um einen Benutzer mit ASDM hinzuzufügen.



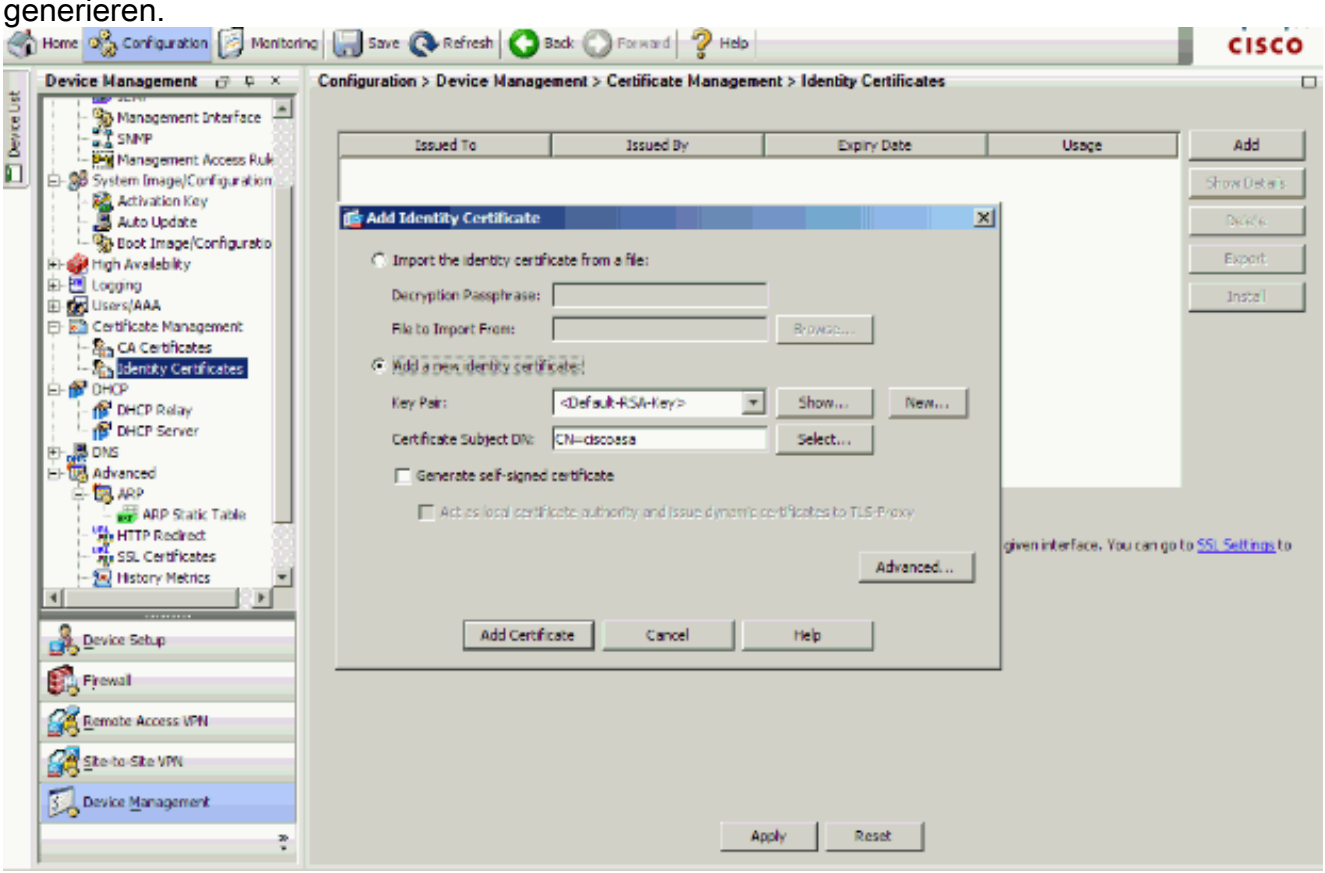
2. Wählen Sie **Configuration > Device Management > Users/AAA > AAA Access > Authentication** aus, um die AAA-Authentifizierung für SSH mit ASDM einzurichten.



3. Wählen Sie **Configuration > Device Setup > Device Name/Password (Konfiguration > Geräteeinrichtung > Gerätename/Kennwort)**, um das Telnet-Kennwort mit ASDM zu ändern.

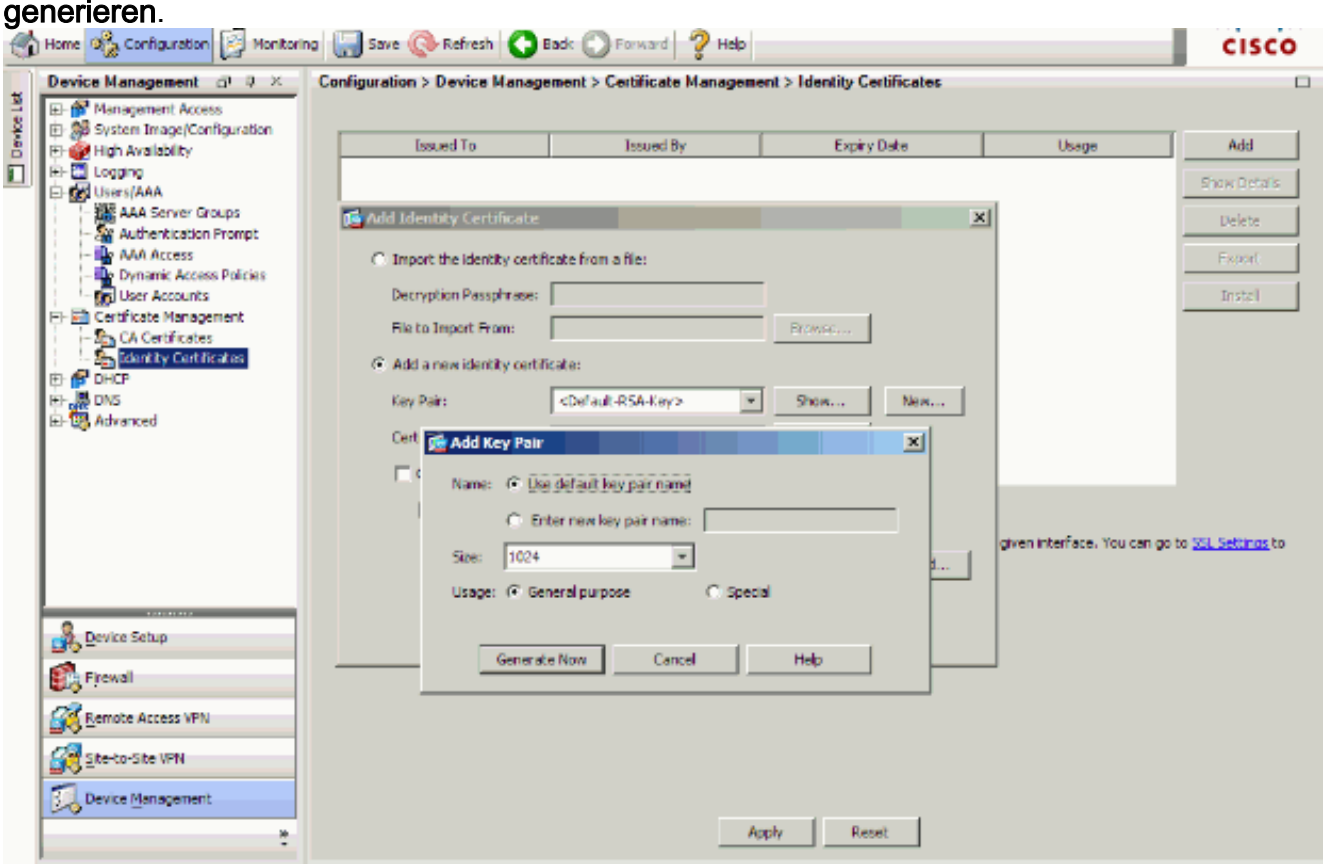


4. Wählen Sie **Konfiguration > Gerätemanagement > Zertifikatsverwaltung > Identitätszertifikate**, klicken Sie auf **Hinzufügen**, und verwenden Sie die angegebenen Standardoptionen, um dieselben RSA-Schlüssel mit ASDM zu generieren.

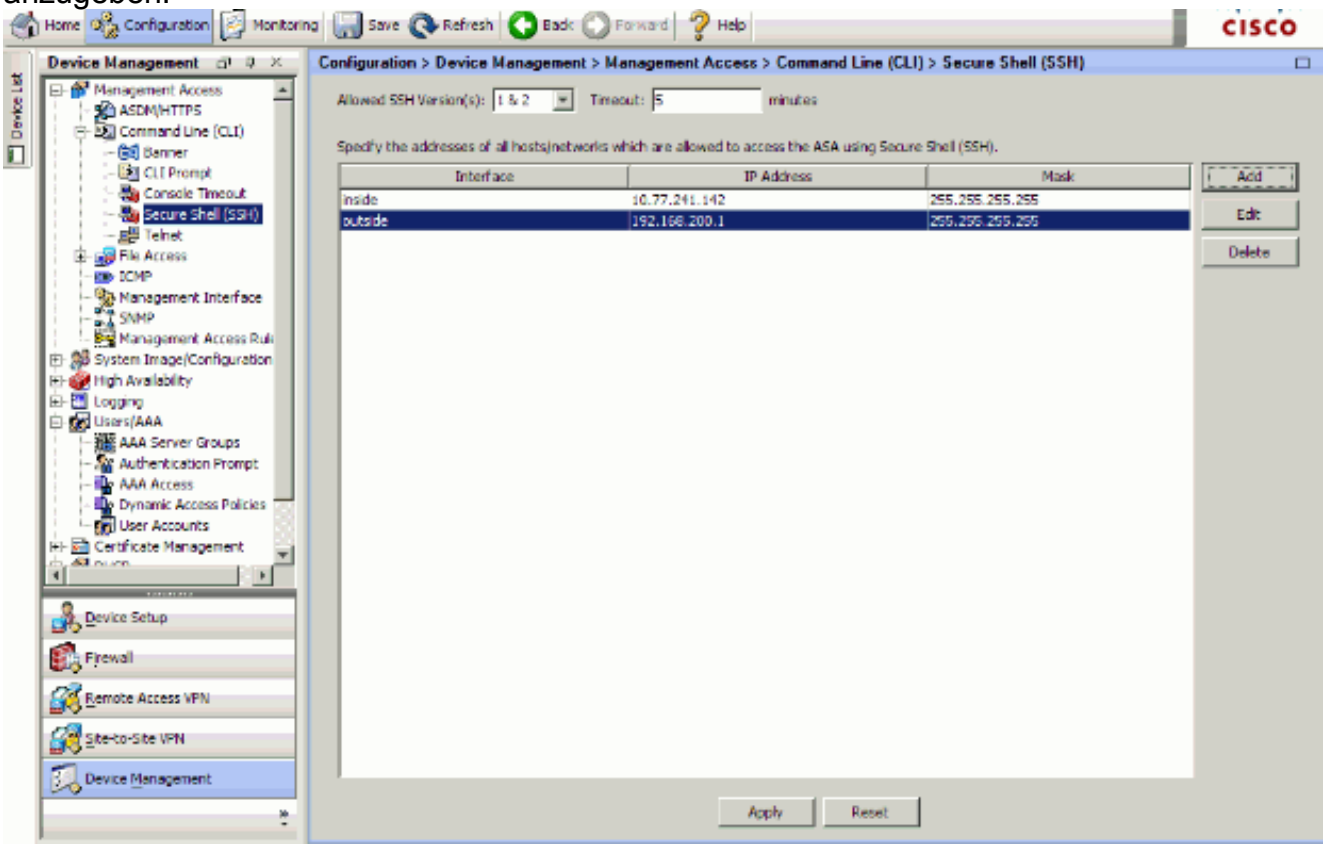


5. Klicken Sie unter **Neues Identitätszertifikat hinzufügen** auf **Neu**, um ein standardmäßiges

Schlüsselpaar hinzuzufügen, falls es kein solches nicht gibt. Klicken Sie anschließend auf **Jetzt generieren**.

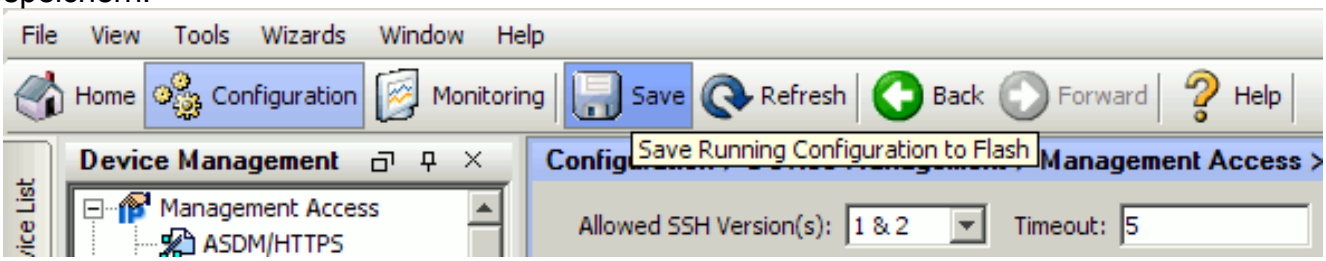


6. Wählen Sie **Configuration > Device Management > Management Access > Command Line (CLI) > Secure Shell (SSH)**, um ASDM zum Festlegen von Hosts zu verwenden, die eine Verbindung mit SSH herstellen dürfen, und um die Version- und Timeout-Optionen anzugeben.



7. Klicken Sie oben im Fenster auf **Speichern**, um die Konfiguration zu

speichern.



8. Wenn Sie dazu aufgefordert werden, die Konfiguration im Flash-Speicher zu speichern, wählen Sie **Apply (Übernehmen)**, um die Konfiguration zu speichern.

Telnet-Konfiguration

Führen Sie den Befehl **telnet** im globalen Konfigurationsmodus aus, um der Konsole Telnet-Zugriff hinzuzufügen und die Leerlaufzeitüberschreitung festzulegen. Standardmäßig werden Telnet-Sitzungen, die fünf Minuten lang im Leerlauf verbleiben, von der Sicherheits-Appliance geschlossen. Um den Telnet-Zugriff von einer zuvor festgelegten IP-Adresse zu entfernen, verwenden Sie die *no*-Form dieses Befehls.

```
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}}
```

Mit dem **Telnet-**Befehl können Sie festlegen, welche Hosts mit Telnet auf die Konsole der Sicherheitsanwendung zugreifen können.

Hinweis: Sie können Telnet für die Sicherheits-Appliance an allen Schnittstellen aktivieren. Die Sicherheits-Appliance erzwingt jedoch, dass der gesamte Telnet-Datenverkehr zur externen Schnittstelle durch IPsec geschützt wird. Um eine Telnet-Sitzung mit der externen Schnittstelle zu aktivieren, konfigurieren Sie IPsec auf der externen Schnittstelle so, dass der von der Sicherheits-Appliance generierte IP-Datenverkehr enthalten ist, und aktivieren Sie Telnet auf der externen Schnittstelle.

Hinweis: Wenn eine Schnittstelle im Allgemeinen eine Sicherheitsstufe von 0 oder niedriger als jede andere Schnittstelle hat, lässt PIX/ASA Telnet für diese Schnittstelle nicht zu.

Hinweis: Es wird nicht empfohlen, über eine Telnet-Sitzung auf die Sicherheits-Appliance zuzugreifen. Die Anmeldeinformationen für die Authentifizierung, z. B. das Kennwort, werden als Klartext gesendet. Die Telnet-Server- und Client-Kommunikation erfolgt nur mit dem Klartext. Cisco empfiehlt, SSH für eine sicherere Datenkommunikation zu verwenden.

Wenn Sie eine IP-Adresse eingeben, müssen Sie auch eine Netzmaske eingeben. Es gibt keine Standard-Netzmaske. Verwenden Sie nicht die Subnetzmaske des internen Netzwerks. Die Netzmaske ist nur eine Bitmaske für die IP-Adresse. Um den Zugriff auf eine einzelne IP-Adresse zu beschränken, verwenden Sie in jedem Oktett 255. z. B. 255.255.255.255.

Wenn IPsec ausgeführt wird, können Sie einen unsicheren Schnittstellennamen angeben, der in der Regel die externe Schnittstelle ist. Sie können mindestens den Befehl **crypto map**

konfigurieren, um einen Schnittstellennamen mit dem Befehl **telnet** anzugeben.

Geben Sie den Befehl **password** ein, um ein Kennwort für den Telnet-Zugriff auf die Konsole festzulegen. Der Standardwert ist "cisco". Geben Sie den Befehl "**wer**" ein, um anzuzeigen, welche IP-Adressen derzeit auf die Konsole der Sicherheitslösung zugreifen. Führen Sie den Befehl **kill** aus, um eine aktive Telnet-Konsolensitzung zu beenden.

Um eine Telnet-Sitzung auf der internen Schnittstelle zu aktivieren, sehen Sie sich die folgenden Beispiele an:

Beispiel 1

In diesem Beispiel kann nur der Host 10.1.1.1 über Telnet Zugriff auf die Konsole der Sicherheits-Appliance erhalten:

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

Beispiel 2

In diesem Beispiel kann nur das Netzwerk 10.0.0.0/8 über Telnet Zugriff auf die Konsole der Security Appliance erhalten:

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

Beispiel 3

In diesem Beispiel können alle Netzwerke über Telnet auf die Konsole der Sicherheits-Appliance zugreifen:

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

Wenn Sie den **aaa**-Befehl mit dem console-Schlüsselwort verwenden, muss der Telnet-Konsolenzugriff mit einem Authentifizierungsserver authentifiziert werden.

Hinweis: Wenn Sie den **aaa-**Befehl konfiguriert haben, um eine Authentifizierung für den Telnet-Konsolenzugriff der Sicherheitsappliance zu erfordern und die Konsolenanmeldung das Zeitlimit überschreitet, können Sie von der seriellen Konsole aus auf die Sicherheitsappliance zugreifen. Geben Sie dazu den Benutzernamen und das Kennwort der Security Appliance ein, die mit dem Befehl **enable password** festgelegt wurden.

Geben Sie den Befehl **telnet timeout** ein, um die maximale Zeit festzulegen, die eine Telnet-Konsolensitzung inaktiv sein kann, bevor sie von der Sicherheits-Appliance abgemeldet wird. Der Befehl **no telnet** kann mit dem Befehl **telnet timeout** nicht verwendet werden.

In diesem Beispiel wird veranschaulicht, wie die maximale Leerlaufdauer einer Sitzung geändert wird:

```
hostname(config)#telnet timeout 10

hostname(config)#show running-config telnet timeout

telnet timeout 10 minutes
```

SSH/Telnet-Unterstützung in ACS 4.x

Wenn Sie sich die RADIUS-Funktionen anschauen, können Sie den RADIUS für die SSH-Funktion verwenden.

Wenn versucht wird, über Telnet, SSH, HTTP oder eine serielle Konsolenverbindung auf die Security Appliance zuzugreifen und der Datenverkehr mit einer Authentifizierungsanweisung übereinstimmt, fordert die Security Appliance einen Benutzernamen und ein Kennwort an. Diese Anmeldeinformationen werden dann an den RADIUS-Server (ACS) gesendet, und der CLI-Zugriff wird basierend auf der Antwort des Servers gewährt oder verweigert.

Weitere Informationen finden Sie im Abschnitt AAA-Server- und lokaler Datenbanksupport zum Konfigurieren von AAA-Servern und der lokalen Datenbank.

Beispielsweise benötigt Ihre ASA Security Appliance 7.0 eine IP-Adresse, von der die Sicherheits-Appliance Verbindungen akzeptiert, z. B.:

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

Weitere Informationen finden Sie im Abschnitt Zulassen von SSH-Zugriff unter Konfigurieren von AAA-Servern und in der lokalen Datenbank.

Weitere Informationen finden Sie unter PIX/ASA: Cut-Through-Proxy für Netzwerkzugriff mit TACACS+ und RADIUS-Server-Konfigurationsbeispiel für weitere Informationen zum Konfigurieren des SSH/Telnet-Zugriffs auf PIX mit ACS-Authentifizierung.

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show** anzuzeigen.

Debug-SSH

Führen Sie den Befehl **debug ssh aus**, um das SSH-Debuggen zu aktivieren.

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

Diese Ausgabe zeigt, dass die Authentifizierungsanfrage von Host 10.1.1.2 (außerhalb von PIX) zu "pix" erfolgreich ist:

```
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
```

Wenn ein Benutzer einen falschen Benutzernamen angibt, z. B. "pix1" statt "pix", lehnt die PIX-Firewall die Authentifizierung ab. Diese Debug-Ausgabe zeigt die fehlgeschlagene Authentifizierung an:

```
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.
```

Wenn der Benutzer das falsche Kennwort bereitstellt, wird in diesem Debugausgang auch die fehlgeschlagene Authentifizierung angezeigt.

```
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.
```

Aktive SSH-Sitzungen anzeigen

Geben Sie diesen Befehl ein, um die Anzahl der mit dem PIX verbundenen SSH-Sitzungen und den Verbindungsstatus zu überprüfen:

```
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
```

Wählen Sie **Monitoring > Properties > Device Access > Secure Shell Sessions** aus, um die Sitzungen mit ASDM anzuzeigen.

Öffentlichen RSA-Schlüssel anzeigen

Geben Sie diesen Befehl ein, um den öffentlichen Teil der RSA-Schlüssel auf der Sicherheits-Appliance anzuzeigen:

```
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
```

Wählen Sie **Konfiguration > Eigenschaften > Zertifikat > Schlüsselpaar aus**, und klicken Sie auf **Details anzeigen**, um RSA-Schlüssel mit ASDM anzuzeigen.

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Entfernen der RSA-Schlüssel aus dem PIX

In bestimmten Situationen, z. B. wenn Sie die PIX-Software aktualisieren oder die SSH-Version im PIX ändern, müssen Sie möglicherweise RSA-Schlüssel entfernen und neu erstellen. Geben Sie diesen Befehl ein, um das RSA-Schlüsselpaar aus dem PIX zu entfernen:

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

Wählen Sie **Konfiguration > Eigenschaften > Zertifikat > Schlüsselpaar aus**, und klicken Sie auf **Löschen**, um RSA-Schlüssel mit ASDM zu entfernen.

SSH-Verbindung fehlgeschlagen

Fehlermeldung auf PIX/ASA:

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

Die entsprechende Fehlermeldung auf dem SSH-Client-Computer:

```
Selected cipher type
```

Um dieses Problem zu beheben, entfernen und erstellen Sie die RSA-Schlüssel erneut. Führen Sie diesen Befehl aus, um das RSA-Schlüsselpaar aus der ASA zu entfernen:

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

Geben Sie diesen Befehl ein, um den neuen Schlüssel zu generieren:

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

Zugriff auf ASA mit SSH nicht möglich

Fehlermeldung:

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

Gehen Sie wie folgt vor, um dieses Problem zu beheben:

1. Laden Sie entweder die ASA neu, oder entfernen Sie alle SSH-bezogenen Konfigurationen und RSA-Schlüssel.
2. Konfigurieren Sie die SSH-Befehle neu, und generieren Sie die RSA-Schlüssel neu.

Zugriff auf sekundäre ASA mit SSH nicht möglich

Wenn sich ASA im Failover-Modus befindet, ist eine SSH-Verbindung zum Standby-ASA über den VPN-Tunnel nicht möglich. Der Grund hierfür ist, dass der Antwortverkehr für das SSH die externe Schnittstelle der Standby-ASA übernimmt.

Zugehörige Informationen

- Cisco Security Appliances der Serie PIX 500
- Cisco Adaptive Security Appliances der Serie ASA 5500
- Cisco PIX Firewall-Software
- Cisco Secure PIX Firewall - Befehlsreferenzen
- Konfigurieren von SSH-Verbindungen - Cisco Router und Cisco Concentrators
- Anforderungen für Kommentare (RFCs)
- Technischer Support und Dokumentation - Cisco Systems