ASA versie 9.x SSH en telnet op binnen- en buitenkant-interfaces

Inhoud

Inleiding

Dit document beschrijft hoe u Secure Shell (SSH) kunt configureren op de binnen- en externe interfaces van de Cisco Series security applicatie versies 9.x en hoger. Wanneer u de Cisco adaptieve security applicatie (ASA) extern met de CLI moet configureren en bewaken, is het gebruik van telnet of SSH vereist. Omdat de mededelingen van het telnet in duidelijke tekst worden verzonden, die wachtwoorden kan omvatten, wordt SSH zeer aanbevolen. Het SSH-verkeer is versleuteld in een tunnel en daardoor beschermt u wachtwoorden en andere gevoelige configuratieopdrachten tegen interceptie.

De ASA staat SSH-verbindingen met het beveiligingsapparaat toe voor beheerdoeleinden. Het security apparaat maakt maximaal vijf gelijktijdige SSH-verbindingen mogelijk voor elke beveiligingscontext, indien beschikbaar, en maximaal 100 verbindingen voor alle contexten samen.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de Cisco ASA Firewall software versie 9.1.5.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

> **Opmerking:** SSH versie 2 (SSHv2) wordt ondersteund in ASA versies 7.x en hoger.

Verwante producten

Deze configuratie kan ook worden gebruikt met de Cisco ASA 5500 Series security applicatie met softwareversies 9.x en hoger.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

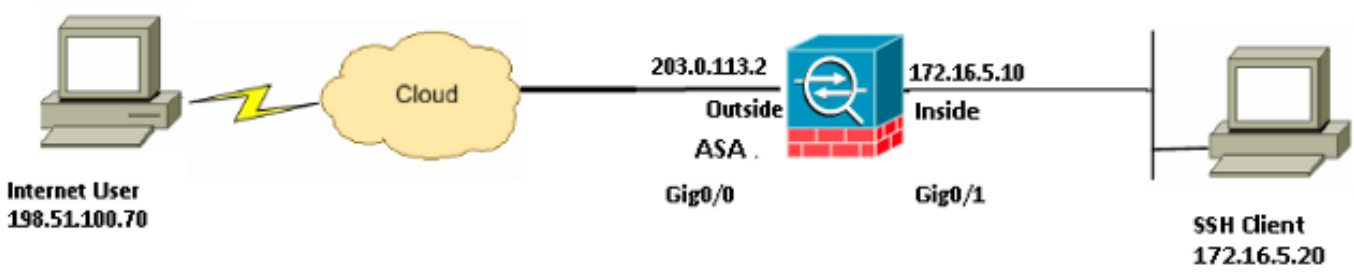
Configureren

Gebruik de informatie die in deze sectie wordt verschaft om de functies te configureren die in dit document worden beschreven.

> **Opmerking:** Elke configuratiestap die wordt beschreven geeft de informatie die nodig is om de CLI of de Adaptieve Security Devices Manager (ASDM) te gebruiken.

> **Opmerking:** Gebruik de Command Lookup Tool (alleen voor geregistreerde gebruikers) voor meer informatie over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram



In dit configuratievoorbeeld wordt de ASA beschouwd als de SSH server. Het verkeer van de SSH-clients (198.51.100.70/32 en 172.16.5.20/24) naar de SSH-server is versleuteld. Het beveiligingsapparaat ondersteunt de SSH-functionaliteit voor afstandsbediening die wordt geboden in SSH versies 1 en 2 en ondersteunt Data Encryption Standard (DES) en 3DES-ciphers. SSH versies 1 en 2 verschillen en zijn niet interoperabel.

SSH-configuraties

Dit document gebruikt deze configuraties:

- SSH-toegang tot de security applicatie
- Hoe een SSH-client wordt gebruikt
- ASA-configuratie

SSH-toegang tot de security applicatie

Volg deze stappen om de SSH-toegang tot het beveiligingsapparaat te configureren:

1. SSH-sessies vereisen altijd een vorm van verificatie, zoals een gebruikersnaam en wachtwoord. Er zijn twee methoden die je kunt gebruiken om aan deze eis te voldoen.

   De eerste methode die u kunt gebruiken om aan deze vereiste te voldoen is om een gebruikersnaam en wachtwoord te configureren met behulp van verificatie, autorisatie en accounting (AAA):

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

   Opmerking: Als u een TACACS+ of RADIUS-servergroep voor verificatie gebruikt, kunt u het security apparaat configureren zodat de lokale database als back-upmethode wordt gebruikt als de AAA-server niet beschikbaar is. Specificeer de naam van de servergroep en vervolgens **PLAATSELIJK** (**PLAATSELIJK** is hoofdlettergevoelig). Cisco raadt u aan dezelfde gebruikersnaam en wachtwoord te gebruiken in de lokale database en de AAA-server, omdat de melding van het beveiligingsapparaat geen indicatie geeft van de gebruikte methode.Om een **LOKALE** back-up voor **TACACS+** te specificeren, gebruikt u deze configuratie voor SSH-verificatie:

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

   U kunt de lokale database ook gebruiken als hoofdmethode voor verificatie zonder back-up. Voer daartoe alleen **LOCAL** in:

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

De tweede methode die u kunt gebruiken om aan dit vereiste te voldoen is de standaard gebruikersnaam van **ASA** en het standaard Telnet wachtwoord van **cisco** te gebruiken. U kunt het Telnet-wachtwoord met deze opdracht wijzigen:

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

Opmerking: De opdracht Wachtwoord kan ook in deze situatie worden gebruikt, aangezien beide opdrachten eveneens werken.

2. Genereert een RSA sleutelpaar voor de ASA Firewall, dat nodig is voor SSH:

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

Opmerking: The **modulus_size** (in bits) kan 512, 768, 1024 of 2048 zijn. Hoe groter de standaardgrootte die je specificeert, hoe langer het duurt om het RSA-sleutelpaar te genereren. Een waarde van 2048 wordt aanbevolen. De opdracht die wordt gebruikt om een RSA-sleutelpaar te genereren is anders voor ASA-softwareversies eerder dan versie 7.x. In eerdere versies moet een domeinnaam worden ingesteld voordat u de keys kunt maken. In meerdere context mode moet u de RSA keys voor elke context genereren.

3. Specificeer de hosts verbinding met het beveiligingsapparaat te maken. Deze opdracht specificeert het bronadres, netmask en interface van de host(s) die mag worden aangesloten bij SSH. Het kan meerdere keren zijn ingevoerd voor meerdere hosts, netwerken of interfaces. In dit voorbeeld, wordt één gastheer binnen en één gastheer op de buitenkant toegestaan:

```
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. Deze stap is optioneel. Met het beveiligingsapparaat kan standaard zowel versie 1 als versie 2 worden uitgevoerd. Voer deze opdracht in om de verbindingen tot een bepaalde versie te beperken:

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

Opmerking: Het **version_number** kan **1** of **2** zijn.

5. Deze stap is optioneel. Standaard worden de SSH-sessies gesloten na vijf minuten van inactiviteit. Deze tijdelijke versie kan worden ingesteld op een duur van 1 tot 60 minuten:

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

ASA-configuratie

Gebruik deze informatie om de ASA te configureren:

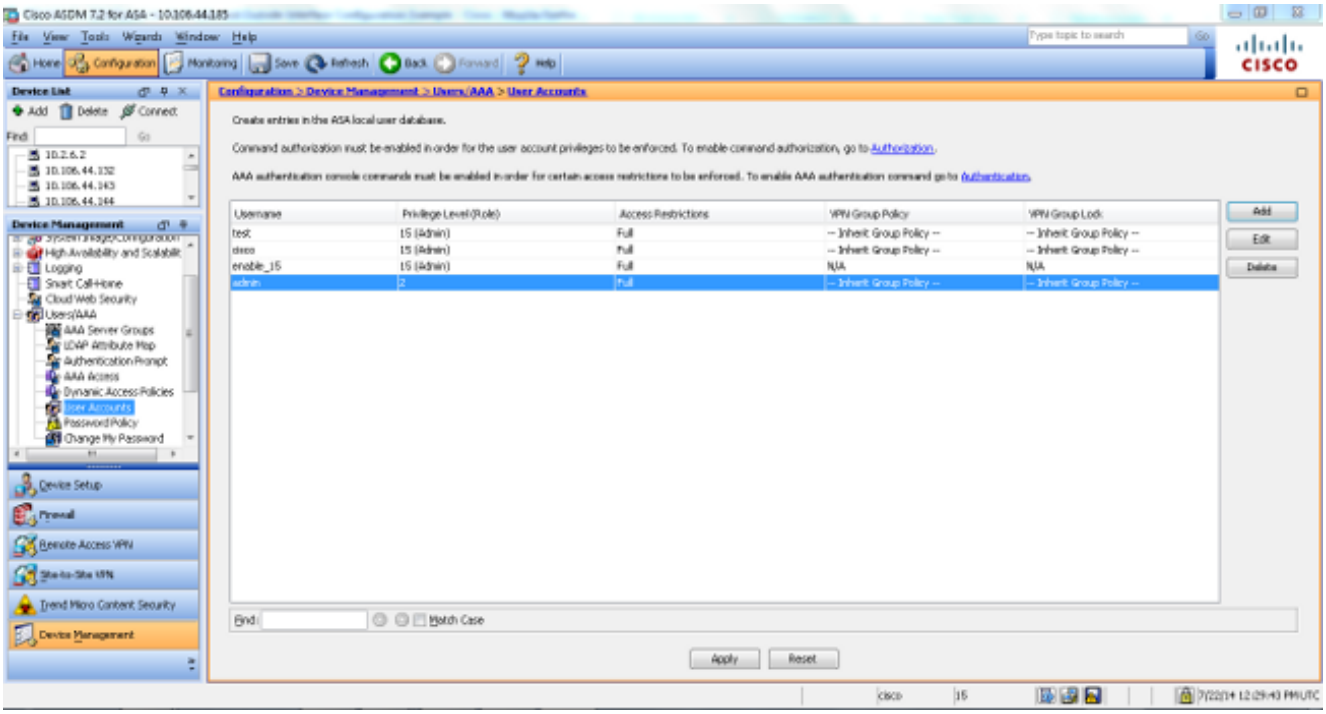
```
ASA Version 9.1(5)2
!
hostname ASA
domain-name cisco.com

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
```

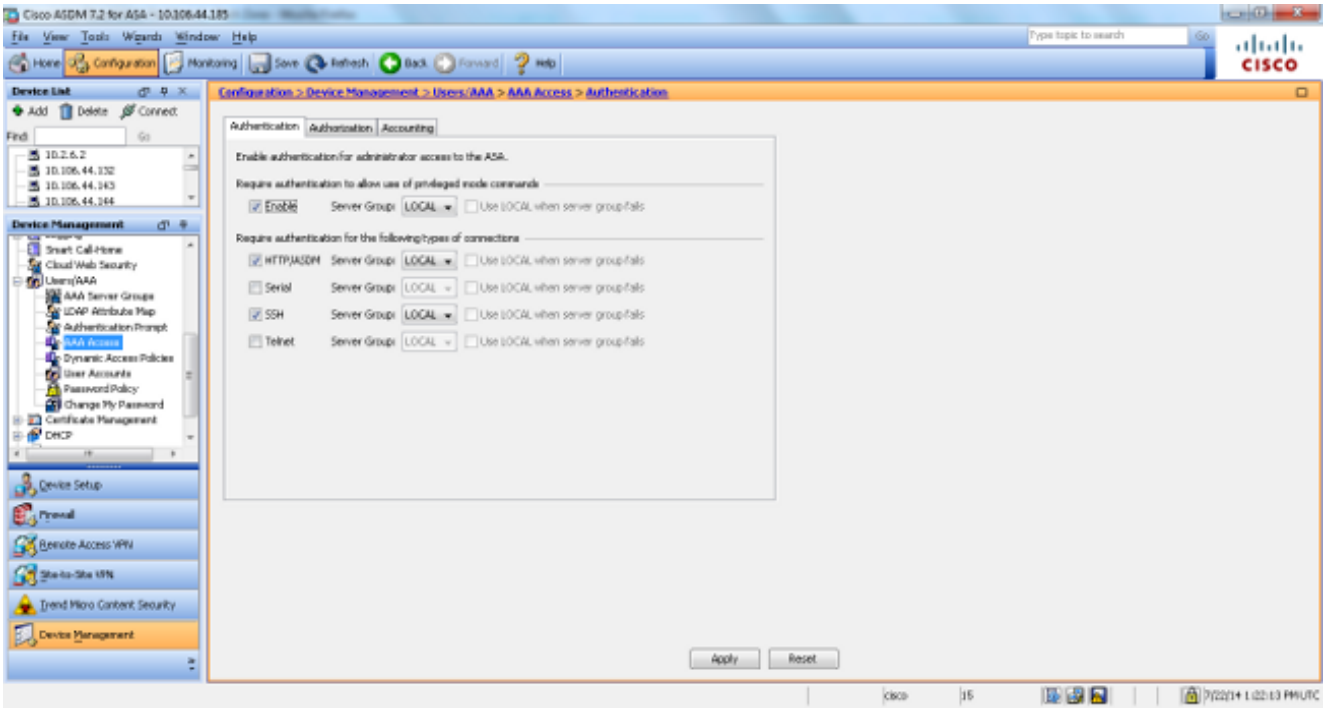
ASDM versie 7.2.1 Configuratie

Volg deze stappen om de ASDM versie 7.2.1 te configureren:

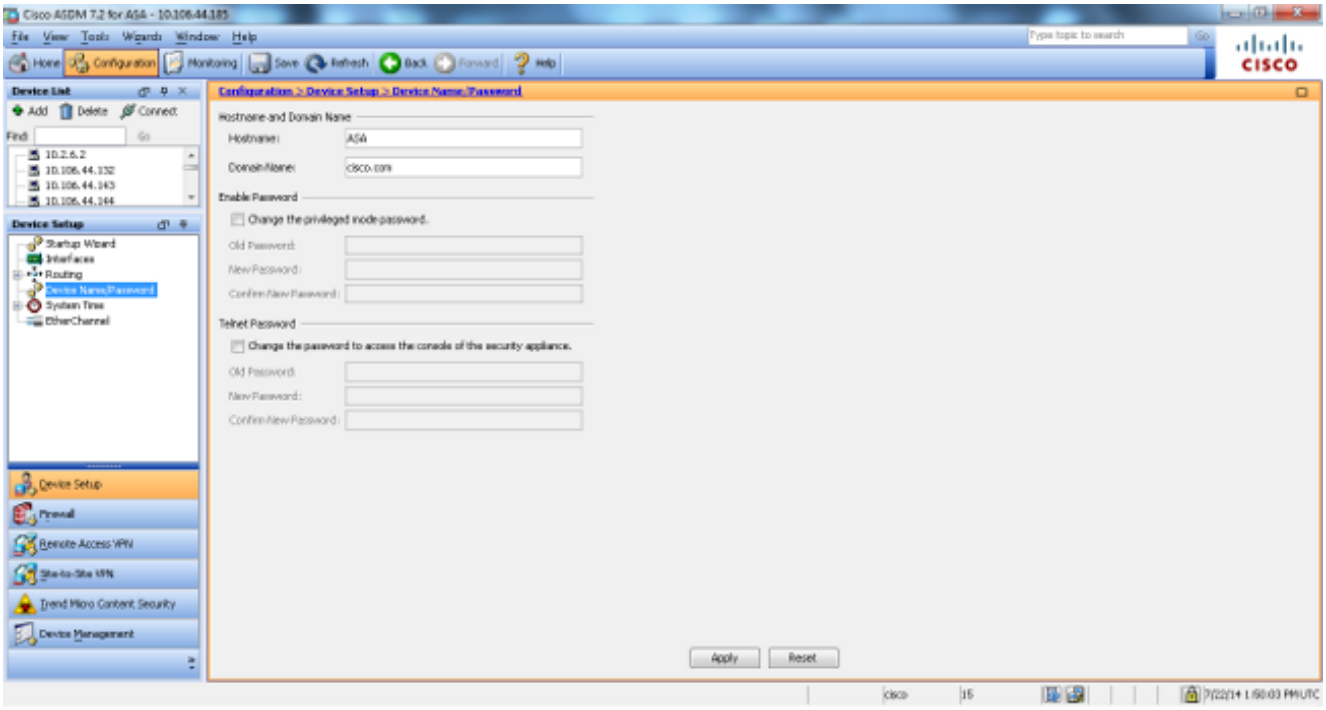
1. Navigeer naar **Configuratie > Apparaatbeheer > Gebruikers/AAA > Gebruikersrekeningen** om een gebruiker met ASDM toe te voegen.



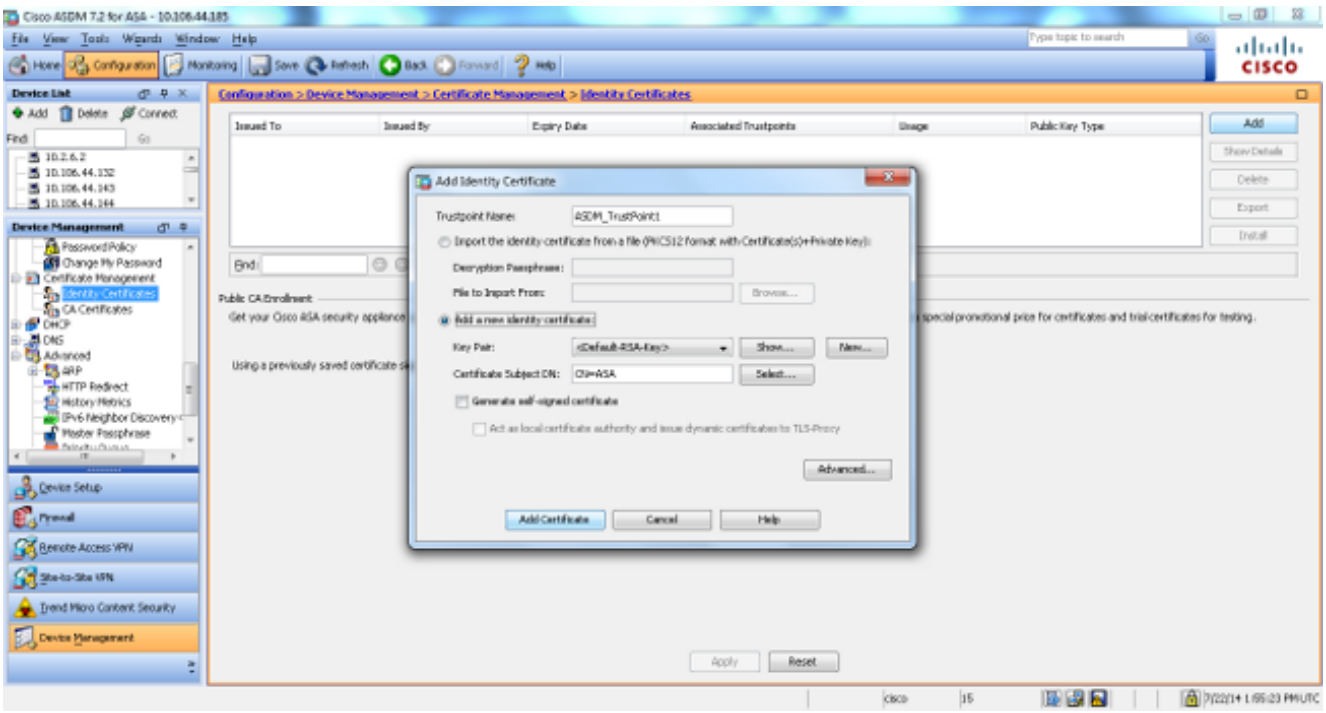
2. Navigeer naar **Configuratie > Apparaatbeheer > Gebruikers/AAA > Toegang > Verificatie** om AAA-verificatie in te stellen voor SSH met ASDM.



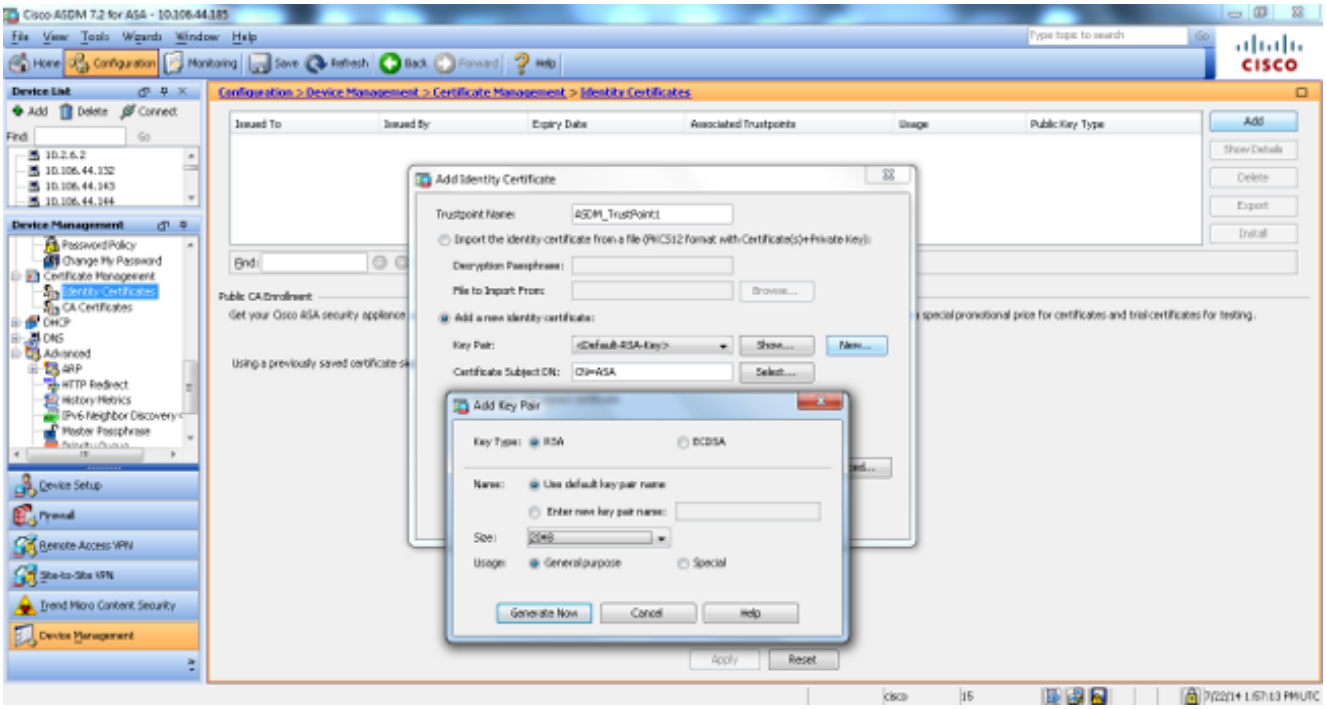
3. Navigeer naar **Configuratie > Instellen van het apparaat > Naam/Wachtwoord van het apparaat** om het Telnet wachtwoord met ASDM te veranderen.



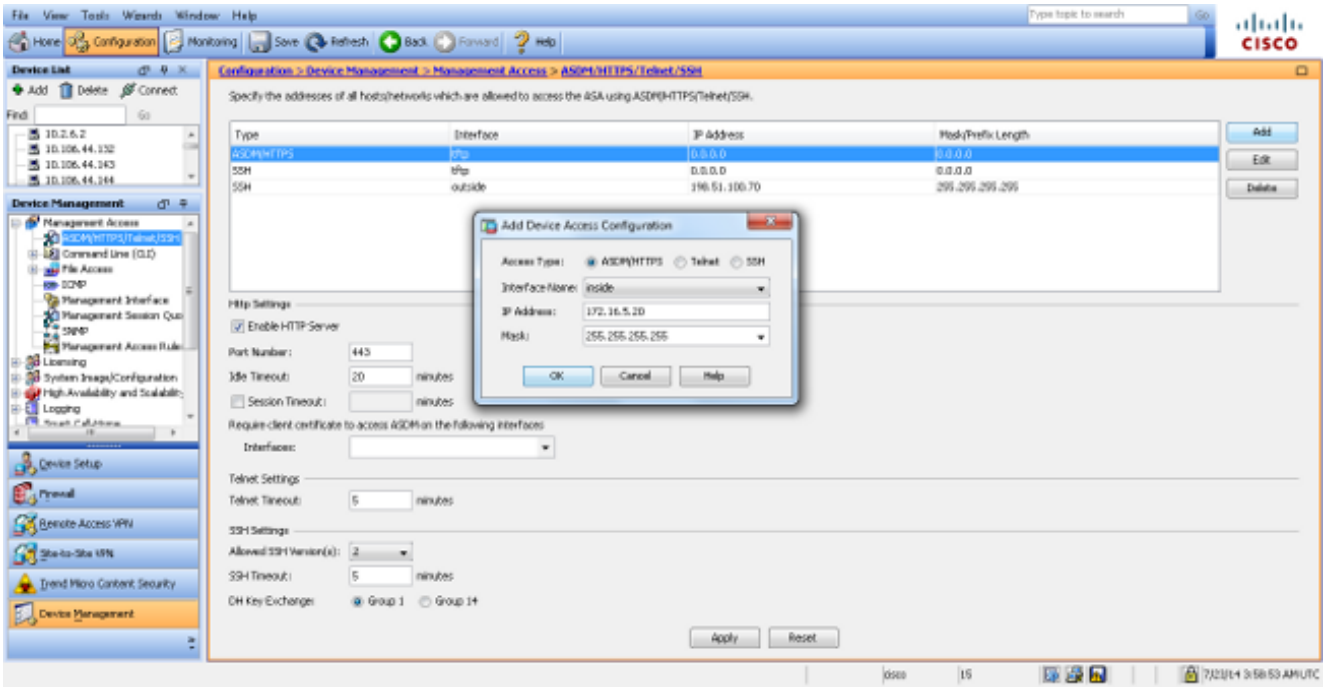
4. navigeren naar **Configuratie > Apparaatbeheer > Certificaatbeheer > Identity Certificaten**, klik op **Add** en gebruik de standaardopties die beschikbaar zijn om dezelfde RSA-toetsen met ASDM te genereren.



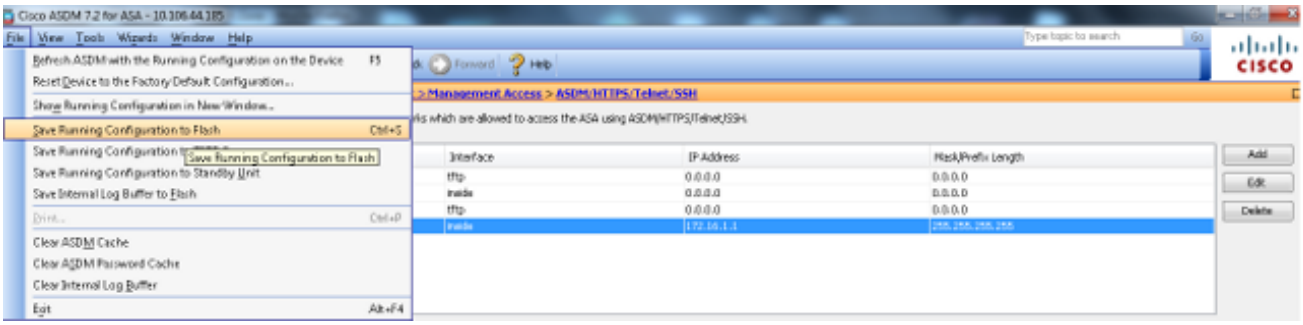
5. Klik op de radioknop **Add a new Identity Certificate** en klik op **New** om een standaardtoetsenbord toe te voegen indien dit niet bestaat. Klik na voltooiing **op Nu genereren**.



6. Navigeer naar **Configuratie > Apparaatbeheer > Toegang > Opdrachtlijn (CLI) > Secure Shell (SSH)** om ASDM te gebruiken zodat u de hosts kunt specificeren die toegang hebben tot verbinding met SSH en om de versie- en tijdelijke opties te specificeren.



7. Klik in het pop-upvenster op **Opslaan** om de configuratie op te slaan.



8. Wanneer gevraagd wordt de configuratie op flitser op te slaan, kies **Toepassen** om de configuratie op te slaan.

Telnet-configuratie

Om de toegang van het telnet aan de console toe te voegen en de nutteloze tijd in te stellen, voer het **telnet** bevel in globale configuratiewijze in. Telnet-sessies die gedurende vijf minuten stilstaand zijn, worden standaard door het security apparaat gesloten. Om de toegang van het telnet uit een eerder vastgesteld IP adres te verwijderen, gebruik de **geen** vorm van deze opdracht.

```
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}}
```

Met de opdracht **telnet** kunt u de hosts specificeren die toegang kunnen krijgen tot de console van het beveiligingsapparaat via telnet.

> **Opmerking:** U kunt telnet op alle interfaces naar het beveiligingsapparaat inschakelen. Het security apparaat vereist echter dat al het Telnet-verkeer naar de externe interface door IPsec wordt beschermd. Om een Telnet-sessie naar de externe interface mogelijk te maken, moet u IPsec op de externe interface configureren zodat deze het IP-verkeer omvat dat door het security apparaat gegenereerd wordt en telnet op de externe interface mogelijk maakt.

> **Opmerking:** In het algemeen, als om het even welke interface die een veiligheidsniveau van nul of lager dan om het even welke andere interface heeft, staat de ASA telnet aan die interface niet toe.

> **Opmerking:** Cisco raadt geen toegang tot het security apparaat aan via een telnet-sessie. De authenticatie crediteureninformatie, zoals het wachtwoord, wordt als duidelijke tekst verzonden. Cisco raadt u aan SSH te gebruiken voor een betere gegevenscommunicatie.

Voer de opdracht **Wachtwoord in** om een wachtwoord in te stellen voor de toegang tot de console van het telnet. Het standaardwachtwoord is **cisco**. Geef de **who** opdracht op om de IP-adressen te bekijken die momenteel toegang hebben tot de security wasmachine. Typ de opdracht **doden** om een actieve sessie van de Telnet-console te beëindigen.

Telnet-voorbeeldscenario's

Om een Telnet-sessie naar de interne interface mogelijk te maken, herzie de voorbeelden die in deze sectie worden gegeven.

Voorbeeld 1

In dit voorbeeld is alleen de host **172.16.5.20** toegestaan om via telnet toegang te krijgen tot de beveiligingswasmachineconnector:

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

Voorbeeld 2

Dit voorbeeld geeft alleen het netwerk **172.16.5.0/24** toegang tot de beveiligingswasmachineconnector door telnet:

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

Voorbeeld 3

In dit voorbeeld kunnen alle netwerken via telnet toegang krijgen tot de beveiligingsservicetechnicus:

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

Als u de opdracht AAA met het sleutelwoord gebruikt, moet de toegang tot de Telnet-console met een authenticatieserver geauthentiseerd zijn.

> **Opmerking:** Als u de opdracht AAA configureren om verificatie van het security apparaat en de toegang tot de Telnet-console nodig te hebben, en de aanmeldingsaanvraag voor de console uit te voeren, kunt u vanuit de seriële console toegang tot het security apparaat krijgen. Voer daartoe de gebruikersnaam voor het beveiligingsapparaat in en het wachtwoord dat is ingesteld met de opdracht **Wachtwoord** inschakelen.

Geef de opdracht voor **tijdelijke** installatie van telnet uit om de maximale tijd in te stellen die een sessie van telnet onklaar kan zijn voordat deze door het beveiligingsapparaat is uitgelogd. U kunt de **geen telnet** opdracht gebruiken met de opdracht **telnet timeout**.

Dit voorbeeld toont hoe om de maximum ongebruikte de zitting te veranderen:

```
hostname(config)#telnet timeout 10

hostname(config)#show running-config telnet timeout

telnet timeout 10 minutes
```

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

> **Opmerking:** Het Uitvoer Tolk (uitsluitend geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van de opdrachtoutput van de **show** te bekijken.

Debug SSH

Voer de opdracht **debug ssh** in om SSH-debuggen in te schakelen:

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

Deze uitvoer toont een SSH-poging van een binnen-IP-adres (172.16.5.20) naar de interne interface van de ASA. Deze cijfers tonen een succesvolle verbinding en authenticatie:

```
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
```

Als een verkeerde gebruikersnaam is ingevoerd, zoals **cisco1** in plaats van **cisco**, wijst de ASA Firewall de verificatie af. Dit debug uitvoer toont de mislukte authenticatie:

```
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.
```

Evenzo, als het onjuiste wachtwoord wordt verstrekt, faalt de authenticatie. Dit debug uitvoer toont de mislukte authenticatie:

```
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.
```

Actieve SSH-sessies bekijken

Voer deze opdracht in om het aantal SSH-sessies dat is aangesloten (en de verbindingsstaat) op de ASA te controleren:

```
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
```

Navigeer naar **bewaking > Eigenschappen > Apparaattoegang > Secure Shell-sessies** om de

sessies met ASDM te bekijken.

Voer de opdracht **Show asp table socket in** om te controleren of de TCP-sessie is ingesteld:

```
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
```

Openbare RSA-toetsen bekijken

Typ deze opdracht om het openbare gedeelte van de RSA-toetsen op het security apparaat te bekijken:

```
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
```

Navigeer naar **Configuration > Properties > certificaatnummer > Key Pair** en klik op **Show Details** om de RSA-toetsen met ASDM te bekijken.

Problemen oplossen

Deze sectie verschaft informatie die u kunt gebruiken om problemen met uw configuratie op te lossen.

Verwijder de RSA-toetsen van de ASA

In bepaalde situaties, zoals wanneer u de ASA-software upgrade of wijziging van de SSH-versie in de ASA-software, kan het zijn dat u de RSA-toetsen verwijdert en opnieuw maakt. Voer deze opdracht in om het RSA-sleutelpaar van de ASA te verwijderen:

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

navigeren naar **Configuratie > Eigenschappen > Certificaat > Belangrijkste paneel** en klik **Verwijderen** om de toetsen RSA met ASDM te verwijderen.

SSH-verbinding is mislukt

U ontvangt deze foutmelding in de ASA:

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

Dit is de foutmelding die in de SSH-client wordt weergegeven:

```
Selected cipher type
```

Om dit probleem op te lossen, verwijdert en herstelt u de RSA-toetsen. Voer deze opdracht in om het RSA-sleutelpaar van de ASA te verwijderen:

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

Typ deze opdracht om de nieuwe toets te genereren:

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