ASA Connection-problemen met Cisco adaptieve security apparaat Manager

Inhoud

Inleiding

Dit document biedt de methodologie voor het opsporen en verhelpen van problemen die nodig zijn om te onderzoeken wanneer u toegang hebt tot/de Cisco adaptieve security applicatie (ASA) kunt configureren met Cisco Adaptieve Security Devices Manager (ASDM). ASDM levert beveiligingsbeheer- en bewakingsdiensten voor beveiligingsapparaten via een grafische beheerinterface.

Voorwaarden

Vereisten

De scenario's, symptomen en stappen in dit document worden geschreven voor problemen bij het oplossen van problemen nadat de eerste configuratie is ingesteld op de ASA. Raadpleeg voor de eerste configuratie het gedeelte ASDM Access-configureren voor applicaties van de Cisco ASA Series General Operations ASDM Configuration Guide, 7.1.

Dit document gebruikt de ASA CLI voor het oplossen van problemen, wat Secure Shell (SSH)/telnet/console toegang tot de ASA vereist.

Gebruikte componenten

De informatie in dit document is gebaseerd op ASDM en ASA.

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.

Methode voor probleemoplossing

Er zijn drie belangrijke mislukkingspunten waarop dit document voor het oplossen van problemen is gericht. Als u zich houdt aan het algemene proces voor het oplossen van problemen in deze volgorde, zou dit document u moeten helpen om het nauwkeurige probleem met ASDM gebruik/toegang te bepalen.

- **ASA-configuratie**
- **Netwerkconnectiviteit**
- **Toepassingssoftware**

ASA-configuratie

Er zijn drie essentiële configuraties aanwezig op de ASA die nodig zijn om succesvol toegang te krijgen tot de ASDM:

- ASDM-afbeelding in Flitser
- ASDM-afbeelding in gebruik
- HTTP-serverbeperkingen

ASDM-afbeelding in Flitser

Zorg dat de gewenste versie van de ASDM in de flitser wordt geüpload. Het kan worden geüpload met de momenteel uitgevoerde versie van de ASDM of met andere conventionele methoden voor bestandsoverdracht naar de ASA, zoals TFTP.

Geef **flitser op** op de ASA CLI om u te helpen om de bestanden op het ASA flash-geheugen op te sommen. Controleer op aanwezigheid van het ASDM-bestand:

```
ciscoasa# show flash --#--  --length--  -----date/time------  path

249 76267 Feb 28 2013 19:58:18 startup-config.cfg
250 4096 May 12 2013 20:26:12 sdesktop
251 15243264 May 08 2013 21:59:10 asa823-k8.bin
252 25196544 Mar 11 2013 22:43:40 asa845-k8.bin
253 17738924 Mar 28 2013 00:12:12 asdm-702.bin ---- ASDM Image
```

Om verder te controleren of het beeld dat op de flitser aanwezig is geldig en niet corrupt is, kunt u de verify-opdracht gebruiken om de opgeslagen MD5-hash in het softwarepakket en de MD5-hash van het huidige bestand te vergelijken:

```
ciscoasa# verify flash:/asdm-702.bin
Verifying file integrity of disk0:/asdm-702.bin
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Done!
Embedded Hash MD5: e441a5723505b8753624243c03a40980
Computed Hash MD5: e441a5723505b8753624243c03a40980
CCO Hash      MD5: c305760ec1b7f19d910c4ea5fa7d1cf1
Signature Verified
Verified disk0:/asdm-702.bin
```

Deze stap zou u moeten helpen om te verifiëren of het beeld en zijn integriteit op de ASA aanwezig zijn.

ASDM-afbeelding in gebruik

Dit proces wordt gedefinieerd onder de ASDM-configuratie op de ASA. Een voorbeeldconfiguratie definitie van het huidige beeld dat wordt gebruikt ziet er zo uit:

ASDM-beeldschijf0:/asdm-702.bin

U kunt de opdracht **asdm-afbeelding** ook gebruiken voor meer verificatie:

```
ciscoasa# show asdm image
Device Manager image file, disk0:/asdm-702.bin
```

HTTP-serverbeperkingen

Deze stap is essentieel in de ASDM configuratie, omdat het definieert welke netwerken toegang hebben tot de ASA. Een voorbeeldconfiguratie ziet er zo uit:

```
http server enable
http 192.168.1.0 255.255.255.0 inside

http 64.0.0.0 255.0.0.0 outside
```

Controleer of de gewenste netwerken in de vorige configuratie zijn gedefinieerd. Het ontbreken van deze definities zorgt ervoor dat de ASDM-lanceerinrichting de tijd verliest terwijl zij zich verbindt en deze fout veroorzaakt:

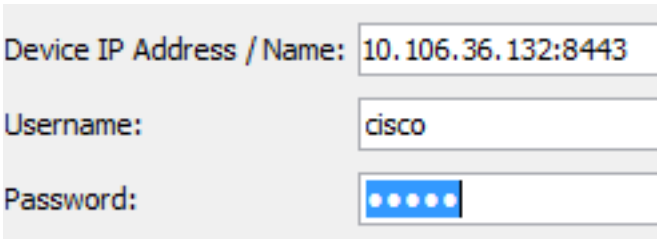
De ASDM-lanceerpagina (**https://<ASA IP-adres>/admin**) veroorzaakt het verzoek om uit te gaan en er wordt geen pagina weergegeven.

Controleer verder dat de HTTP server een niet-standaard poort gebruikt voor ASDM-verbinding, zoals 8443. Dit wordt in de configuratie gemarkeerd:

ciscoasa (configuratie)# **show run http**

http server Enable 8443

Als het een niet-standaard poort gebruikt, moet u de poort specificeren wanneer u in de ASDM-draagster verbinding maakt met de ASA als:



Dit is ook van toepassing bij toegang tot de ASDM-startpagina: **https://10.106.36.132:8443/admin**

Andere mogelijke configuratieproblemen

Nadat u de vorige stappen hebt voltooid, dient ASDM te openen als alles functioneel is aan de clientkant. Als u echter problemen hebt, opent u de ASDM-modus van een andere machine. Als je slaagt is het probleem waarschijnlijk op het toepassingsniveau en is de ASA configuratie prima. Als het echter nog niet start, dient u deze stappen te voltooien om de ASA-zijconfiguraties verder te controleren:

1. Controleer de Secure Socket Layer (SSL)-configuratie op de ASA. ASDM gebruikt SSL terwijl het met de ASA communiceert. Gebaseerd op de manier waarop ASDM wordt gelanceerd, kan de nieuwere OS software het gebruik van zwakkere ciphers niet toestaan wanneer het over SSL sessies onderhandelt.

   Controleer welke ciphers op de ASA zijn toegestaan en als om het even welke specifieke SSL versies in de configuratie worden gespecificeerd met de **show open alle ssl** opdracht:

   ```
   ciscoasa# show run all ssl
   ssl server-version any <--- Check SSL Version restriction configured on the ASA
   ssl client-version any
   ssl encryption rc4-sha1 aes128-sha1 aes256-sha1 3des-sha1 <--- Check SSL ciphers
   permitted on the ASA
   ```

   Als er onderhandelingsfouten zijn met een SSL-algoritme terwijl de ASDM start, worden deze in de ASA-logbestanden weergegeven:

   ```
   %ASA-7-725014: SSL lib error. Function: SSL3_GET_CLIENT_HELLO Reason:
   no shared cipher
   %ASA-6-302014: Teardown TCP connection 3 for mgmt:64.103.236.189/52501 to
   identity:10.106.36.132/443 duration 0:00:00 bytes 7 TCP Reset by appliance
   ```

   Als u specifieke instellingen ziet, keert u deze terug naar de standaard.

   Merk op dat de VPN-3DES-AES licentie op de ASA moet worden ingeschakeld voor de 3DES en AES-telefoons die door de ASA in de configuratie gebruikt worden. Dit kan worden geverifieerd met de opdracht **show version** op de CLI. De uitvoer wordt als volgt weergegeven:

   ```
   ciscoasa#show version

   Hardware: ASA5510, 256 MB RAM, CPU Pentium 4 Celeron 1600 MHz
   Internal ATA Compact Flash, 64MB
   Slot 1: ATA Compact Flash, 32MB
   BIOS Flash M50FW080 @ 0xffe00000, 1024KB
   <snip>
   Failover            : Active/Active
   VPN-DES             : Enabled
   VPN-3DES-AES        : Enabled
   <snip>
   ```

   Een VPN-3DES-AES-licentie kan zonder kosten worden aangeschaft op de Cisco-licentiewebsite. Klik op **Security Producten** en kies vervolgens **Cisco ASA 3DES/AES-licentie**.

   Opmerking: In de nieuwe ASA 5500-X platforms die verzenden met 8.6/9.x code, worden de SSL algoritme instellingen standaard ingesteld op **des-sha1** waardoor de ASDM sessies niet werken. Raadpleeg de ASA 5500-x: ASDM en andere SSL functies werken niet vanuit het artikel van het vakje voor meer informatie.
2. Controleer dat WebVPN op de ASA is ingeschakeld. Als deze functie is ingeschakeld, moet u deze URL (**https://10.106.36.132/admin**) gebruiken om er toegang toe te hebben wanneer u toegang krijgt tot de ASDM webstartpagina.
3.
4. Controleer voor een NAT-configuratie (Network Address Translation) op de ASA voor poort 443. Dit zorgt ervoor dat de ASA de verzoeken om ASDM niet verwerkt, maar ze eerder naar het netwerk/de interface stuurt waarvoor de NAT is geconfigureerd.
5.

6. Als alles wordt geverifieerd en de ASDM nog steeds tijden uit, controleer of de ASA is ingesteld om te luisteren op de poort die voor ASDM is gedefinieerd met de opdracht **asp-**stopcontact op de ASA CLI. De uitvoer moet aantonen dat de ASA op de ASDM-poort luistert:

```
Protocol  Socket    Local Address               Foreign Address         State
SSL       0001b91f  10.106.36.132:443           0.0.0.0:*               LISTEN
```

   Als deze uitvoer niet wordt weergegeven, verwijdert en past u de HTTP-serverconfiguratie op de ASA-software opnieuw toe om de socket op de ASA-software te resetten.
7.
8. Als u problemen ervaart wanneer u inlogt/voor de ASDM authenticeert, controleer dan of de authenticatieopties voor **HTTP** correct zijn ingesteld. Als er geen verificatieopdrachten zijn ingesteld, kunt u met behulp van de ASA het wachtwoord inschakelen om in te loggen op de ASDM. Als u op gebruikersnaam/wachtwoord gebaseerde verificatie wilt inschakelen, moet u deze configuratie invoeren om ASDM/HTTP-sessies naar de ASA te authenticeren vanuit de gebruikersnaam/wachtwoorddatabase van de ASA:

   ```
   aaa authentication http console LOCAL
   ```

   Denk eraan om een gebruikersnaam/wachtwoord te maken wanneer u de vorige opdracht activeert:

   ```
   username <username> password <password> priv <Priv level>
   ```

   Als geen van deze stappen helpt, zijn deze debug-opties beschikbaar in de ASA voor verder onderzoek:

   ```
   debug http 255
   debug asdm history 255
   ```

Netwerkconnectiviteit

Als u de vorige sectie hebt voltooid en nog steeds niet in staat bent om toegang te krijgen tot de ASDM, is de volgende stap om de netwerkconnectiviteit naar uw ASA te verifiëren van de machine waarvandaan u toegang wilt hebben tot de ASDM. Er zijn een paar basisstappen voor het oplossen van problemen om te verifiëren dat de ASA het verzoek van de clientmachine ontvangt:

1. **Test met Internet Control Message Protocol (ICMP)**.
   Ping de ASA interface waarvan u tot ASDM toegang wilt hebben. ping moet succesvol zijn als ICMP wordt toegestaan om uw netwerk te verplaatsen en er geen beperkingen op het ASA interface niveau zijn. Als ping mislukt, is het waarschijnlijk omdat er een communicatieprobleem is tussen de ASA en de client machine. Dit is echter geen beslissende stap om vast te stellen of er sprake is van een dergelijk soort communicatie.
2.
3. **Bevestig met de pakketvastlegging**.
   Plaats een pakketvastlegging op de interface waartoe u toegang wilt hebben tot de ASDM. De opname moet laten zien dat TCP-pakketten bestemd voor het IP-adres van de interface aankomen met bestemmingshaven 443 (standaard).

   Gebruik deze opdracht om een opname te configureren:

```
capture asdm_test interface
```

```
For example, cap asdm_test interface mgmt match tcp host 10.106.36.132
eq 443 host 10.106.36.13
```

Dit vangt elk TCP-verkeer op dat voor poort 443 komt op de ASA-interface waarvan u verbinding maakt met de ASDM. Connect via ASDM op dit punt of open de ASDM webstartpagina. Gebruik vervolgens de opdracht **show Capture asdm_test** om het resultaat van de opgenomen pakketten te bekijken:

```
ciscoasa# show capture asdm_test

Three packets captured

   1: 21:38:11.658855 10.106.36.13.54604 > 10.106.36.132.443:
      S 807913260:807913260(0) win 8192 <mss 1260,nop,wscale 2,nop,nop,sackOK>

   2: 21:38:14.659252 10.106.36.13.54604 > 10.106.36.132.443:
      S 807913260:807913260(0) win 8192 <mss 1260,nop,wscale 2,nop,nop,sackOK>

   3: 21:38:20.662166 10.106.36.13.54604 > 10.106.36.132.443:
      S 807913260:807913260(0) win 8192 <mss 1260,nop,nop,sackOK>
```

Deze opname laat een synchroon (SYN) verzoek van de client naar de ASA zien, maar de ASA stuurt geen antwoord. Als je een opname ziet die lijkt op de vorige, betekent dit dat de pakketten de ASA bereiken maar de ASA niet reageert op deze verzoeken, wat de ASA zelf isoleert. Raadpleeg het eerste gedeelte van dit document om de oplossing verder te verbeteren.

Als u echter geen uitvoer ziet die vergelijkbaar is met de vorige en er geen pakketten worden opgenomen, betekent dit dat er een aansluitingsprobleem is tussen de ASA en de ASDM-clientmachine. Controleer dat er geen intermediaire apparaten zijn die TCP poort 443 verkeer kunnen blokkeren en dat er geen browser instellingen zijn, zoals Proxy instellingen, die het verkeer kunnen verhinderen om de ASA te bereiken.

Meestal is pakketvastlegging een goede manier om te bepalen of het pad naar de ASA helder is en of verdere diagnostiek niet nodig is om problemen met de netwerkconnectiviteit uit te sluiten.

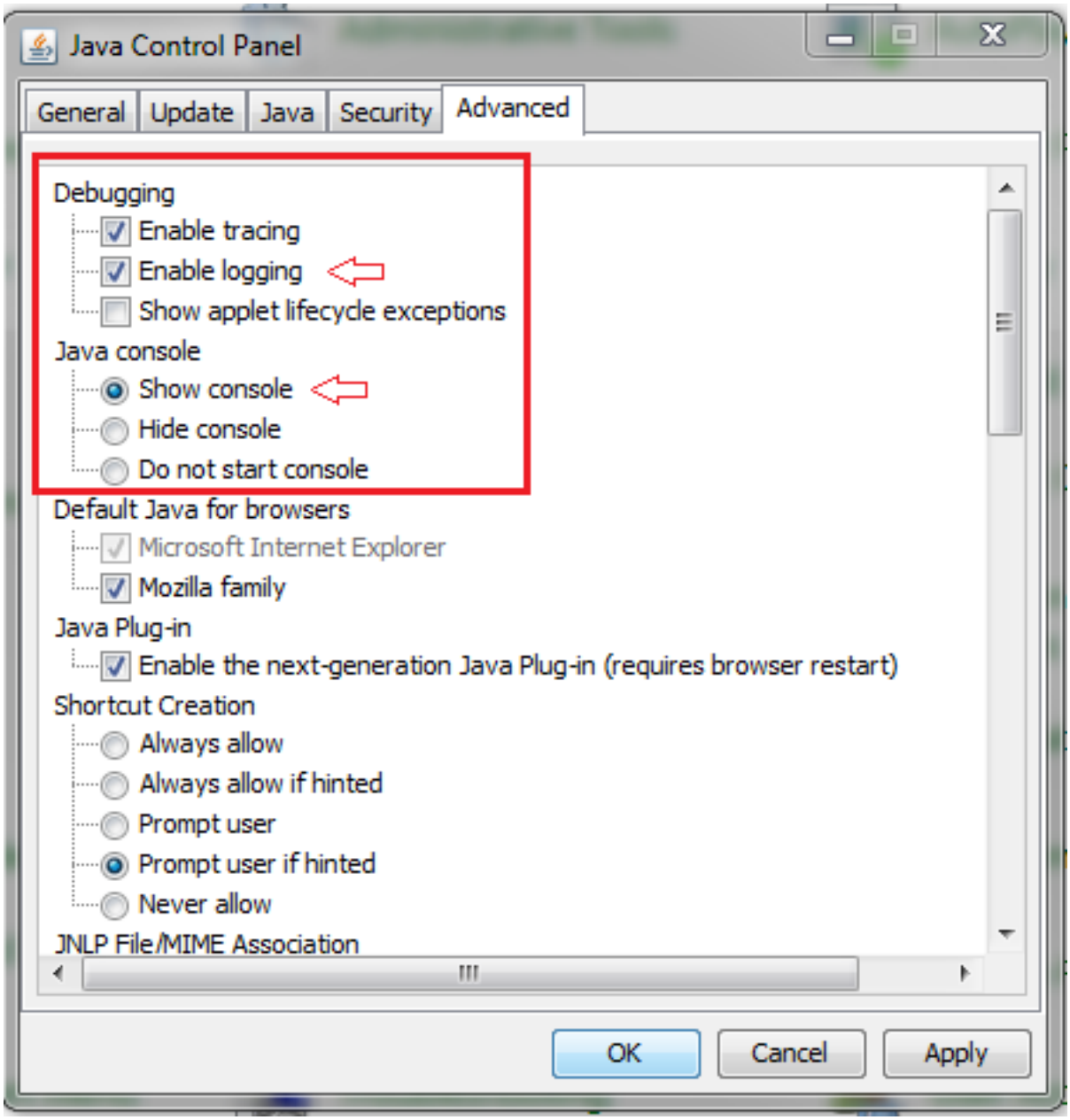
Toepassingssoftware

In dit gedeelte wordt beschreven hoe u de ASDM-lanceersoftware kunt oplossen die op de clientmachine is geïnstalleerd wanneer deze niet start/geladen is. De ASDM-lanceerinrichting is de component die op de client aanwezig is en op de ASA aangesloten is om het ASDM-beeld op te halen. Zodra het is opgehaald, wordt het ASDM-beeld gewoonlijk opgeslagen in cache en wordt het van daaruit meegenomen totdat er enige veranderingen zijn opgemerkt aan de ASA-kant, zoals een ASDM-beeldupdate.

Voltooi deze basisstappen voor het oplossen van problemen om problemen op de clientmachine uit te sluiten:

1. Open de ASDM-startpagina vanuit een andere machine. Indien het van start gaat, betekent dit dat het probleem bij de betrokken cliënt-machine ligt. Als het mislukt, volgt u de handleiding voor probleemoplossing uit het begin om de betrokken onderdelen op volgorde te isoleren.
2.
3. Open de ASDM-toepassing via weblancering en start de software direct vanaf deze website. Als dit succes heeft, is het waarschijnlijk dat er problemen zijn met de installatie van de ASDM-lanceerinrichting. Installeer de ASDM-lanceerinrichting van de clientmachine en herinstalleer deze vanaf de ASA-weblancering zelf.
4.
5. Schakel de ASDM's cache folder in de home folder van de gebruiker uit. In Windows 7 is het bijvoorbeeld hier te vinden: **<gebruikersnaam>\.asdm\cache**. Het cache wordt gewist als u de gehele **cache** folder verwijdert. Als de ASDM met succes start, kunt u de cache ook wissen vanuit het ASDM **File** menu.
6.
7. Controleer of de juiste Java-versie is geïnstalleerd. De Cisco ASDM release Notes bevat de vereisten voor geteste Java-versies.
8.
9. Schakel de Java cache uit. Selecteer in het **Java Control Panel** de optie **Algemeen > Tijdelijk internetbestand**. Klik vervolgens op **Weergave** om een **Java Cache Viewer** te starten. Verwijdert alle items die verwijzen naar of gerelateerd zijn aan ASDM.
10.
11. Als deze stappen falen, verzamel de zuiverende informatie van de klant machine voor verder onderzoek. Schakel foutoplossing voor ASDM in met de URL: **<IP-adres van de ASA>?debug=5 bijv. https://10.0.0.1?debug=5**.

    Met Java versie 6 (ook versie 1.6 genoemd) worden de debugging van Java ingeschakeld vanuit **Java Control Panel > Advanced**. Selecteer vervolgens de vinkjes onder **Afluisteren**. Selecteer geen **console** onder de **Java-console**. De debugging van Java moet ingeschakeld worden voordat ASDM start.



De uitvoer van de Java-console wordt opgenomen in de **.asdm/log** folder van de home folder van de gebruiker. ASDM-logbestanden kunnen ook in dezelfde map worden gevonden. In Windows 7 zijn de logbestanden bijvoorbeeld onder **C:\Users\<gebruikersnaam>/.asdm/log/**.

Opdrachten met HTTPS uitvoeren

Deze procedure helpt om alle Layer 7-problemen voor het HTTP-kanaal te bepalen. Deze informatie blijkt nuttig wanneer u zich in een situatie bevindt waar de ASDM-toepassing zelf niet toegankelijk is en er geen CLI-toegang beschikbaar is om het apparaat te beheren.

De URL die wordt gebruikt om tot de ASDM website te toegang lanceren kan ook worden gebruikt om om het even welke configuratie-vlakke opdrachten op de ASA uit te voeren. Deze URL kan worden gebruikt om configuratie veranderingen op een basisniveau aan de ASA aan te brengen, die een ver apparaat herladen omvat. Gebruik deze syntaxis om een opdracht in te voeren:

https://<IP-adres van de ASA>/admin/exec/<opdracht>

Als er een ruimte in de opdracht staat en de browser geen ruimtetekens in een URL kan parseren,

kunt u het **+** teken of **%20** gebruiken om de ruimte aan te geven.

https://10.106.36.137/admin/exec/show bijvoorbeeld resulteert in een uitvoer van de show versie naar de browser:


```
Cisco Adaptive Security Appliance Software Version 8.4(3)

Compiled on Fri 06-Jan-12 10:24 by builders
System image file is "disk0:/asa843-k8.bin"
Config file at boot was "startup-config"

ciscoasa up 4 mins 41 secs

Hardware:   ASA5505, 512 MB RAM, CPU Geode 500 MHz
Internal ATA Compact Flash, 128MB
BIOS Flash M50FW016 @ 0xfff00000, 2048KB

Encryption hardware device : Cisco ASA-5505 on-board accelerator (revision 0x0)
                             Boot microcode         : CN1000-MC-BOOT-2.00
                             SSL/IKE microcode      : CNLite-MC-SSLm-PLUS-2.03
                             IPSec microcode        : CNlite-MC-IPSECm-MAIN-2.06
                             Number of accelerators: 1

 0: Int: Internal-Data0/0    : address is d0d0.fd0f.902d, irq 11
 1: Ext: Ethernet0/0         : address is d0d0.fd0f.9025, irq 255
 2: Ext: Ethernet0/1         : address is d0d0.fd0f.9026, irq 255
 3: Ext: Ethernet0/2         : address is d0d0.fd0f.9027, irq 255
 4: Ext: Ethernet0/3         : address is d0d0.fd0f.9028, irq 255
 5: Ext: Ethernet0/4         : address is d0d0.fd0f.9029, irq 255
 6: Ext: Ethernet0/5         : address is d0d0.fd0f.902a, irq 255
 7: Ext: Ethernet0/6         : address is d0d0.fd0f.902b, irq 255
 8: Ext: Ethernet0/7         : address is d0d0.fd0f.902c, irq 255
 9: Int: Internal-Data0/1    : address is 0000.0003.0002, irq 255
10: Int: Not used            : irq 255
11: Int: Not used            : irq 255

Licensed features for this platform:
Maximum Physical Interfaces       : 8              perpetual
VLANs                             : 3              DMZ Unrestricted
Dual ISPs                         : Enabled        perpetual
VLAN Trunk Ports                  : 8              perpetual
```

Deze methode van opdrachtuitvoering vereist dat de HTTP-server is ingeschakeld op de ASA en dat de benodigde HTTP-beperkingen actief zijn. Dit vereist echter NIET dat er een ASDM-beeld op de ASA aanwezig is.

Gerelateerde informatie

- ASDM-toegang configureren voor applicaties
- ASA 5500-x: ASDM en andere SSL-functie Werken niet buiten het kader
- Cisco ASDM release-opmerkingen
- Cisco-licentiepagina voor een 3DES/AES-licentie op de ASA
- Technische ondersteuning en documentatie – Cisco Systems