# Problemen met ASA Connection Problemen oplossen op ASDM

## Inhoud



## Inleiding

Dit document beschrijft de methodologie voor probleemoplossing die nodig is om problemen te onderzoeken wanneer u Cisco ASA opent/configureert met Cisco ASDM.

## Voorwaarden

### Vereisten

De scenario's, symptomen en stappen die in dit document worden vermeld, worden geschreven voor problemen met de probleemoplossing nadat de eerste configuratie is ingesteld op de adaptieve security applicatie (ASA). Raadpleeg voor de eerste configuratie het gedeelte ASDM Access for Appliances configureren van de configuratiehandleiding voor Cisco ASA Series General Operations Adaptive Security Device Manager (ASDM), 7.1.

Dit document gebruikt de ASA CLI voor probleemoplossing, waarvoor toegang tot de ASA is vereist voor Secure Shell (SSH)/Telnet/Console.

### Gebruikte componenten

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

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 zorgen dat u de potentiële impact van elke opdracht begrijpt.

## Achtergrondinformatie

ASDM levert security management en monitoring services voor security applicaties via een grafische beheerinterface.

# Methodologie voor probleemoplossing

Er zijn drie belangrijke mislukkingspunten waarop dit document van het oplossen van problemen zich concentreert. Als u het algemene probleemoplossingsproces in deze volgorde volgt, kan dit document u helpen om het exacte probleem met het gebruik/de toegang tot ASDM te bepalen.

- ASA-configuratie
- Netwerkverbinding
- Toepassingssoftware

## ASA-configuratie

Er zijn drie belangrijke configuraties op de ASA die nodig zijn om met succes toegang te krijgen tot de ASDM:

- ASDM-afbeelding in Flash
- ASDM-afbeelding in gebruik
- HTTP-serverbeperkingen

### ASDM-afbeelding in Flash

Zorg ervoor dat de vereiste versie van de ASDM naar de flitser is geüpload. Het kan worden geüpload met de momenteel gebruikte versie van de ASDM of met andere conventionele methoden voor bestandsoverdracht naar de ASA, zoals TFTP.

Voer **flitser** op de ASA CLI in om u te helpen de bestanden op het ASA flitsgeheugen weer te geven. Controleer of het ASDM-bestand aanwezig is:

<#root>

```
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 verifiëren of het beeld dat op de flitser aanwezig is geldig en niet beschadigd is, kunt u de **verify**-opdracht gebruiken om de opgeslagen MD5-hash in het softwarepakket te vergelijken met de MD5-hash van het huidige bestand:

<#root>

```
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
```

Met deze stap kunt u controleren of het beeld en de integriteit ervan op de ASA aanwezig zijn.

**ASDM-afbeelding in gebruik**

Dit proces wordt gedefinieerd onder de ASDM-configuratie op de ASA. Een definitie van de steekproefconfiguratie van het huidige beeld dat wordt gebruikt kijkt als dit:

ASDM-image disk0:/asdm-702.bin

Om verder te verifiëren, kunt u ook de opdracht **asdm image tonen** gebruiken:

```
<#root>

ciscoasa# s

how asdm image


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

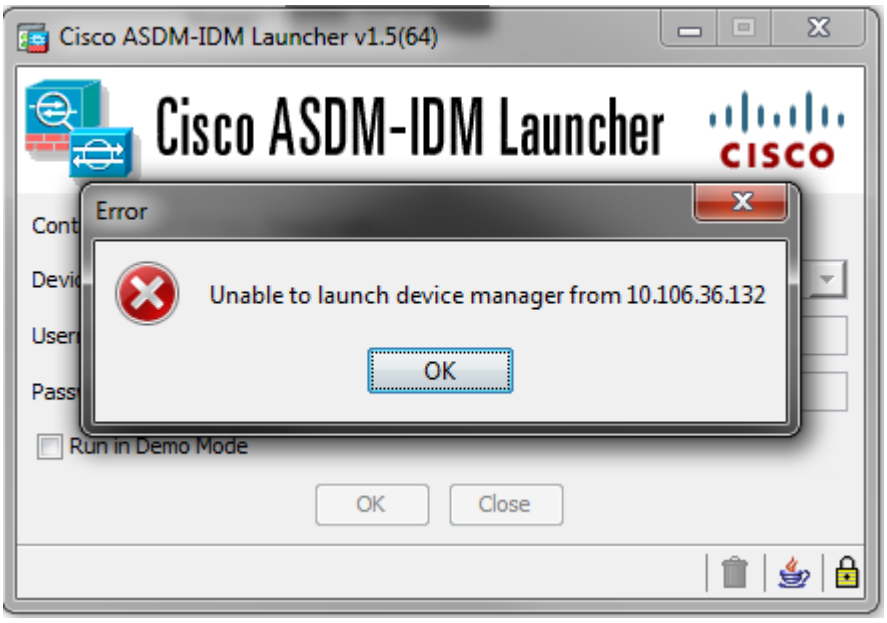
**HTTP-serverbeperkingen**

Deze stap is essentieel in de ASDM-configuratie omdat deze bepaalt 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 10.0.0.1 255.0.0.0 outside
```

Controleer of u de benodigde netwerken hebt die in de vorige configuratie zijn gedefinieerd. De afwezigheid van die definities zorgt ervoor dat de ASDM lanceerinrichting uitvalt tijdens het verbinden en geeft deze fout:

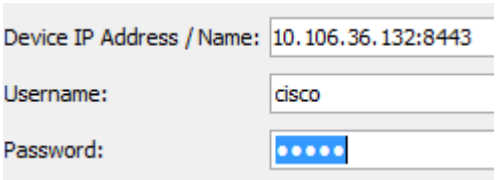



De startpagina van ASDM (https://<ASA IP-adres>/admin) veroorzaakt een time-out van het verzoek en er wordt geen pagina weergegeven.

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

ciscoasa (config)# **show run http**
http server inschakelen 8443

Als het een niet-standaard poort gebruikt, moet u de poort opgeven wanneer u verbinding maakt met de ASA in de ASDM-startkabel zoals:




Dit geldt ook wanneer u de ASDM-startpagina bezoekt: https://10.106.36.132:8443/admin

**Andere mogelijke configuratieproblemen**

Nadat u de vorige stappen hebt voltooid, kan de ASDM worden geopend als alles functioneel is aan de clientzijde. Als u echter nog steeds problemen ondervindt, opent u de ASDM vanaf een andere machine. Als u slaagt, is de kwestie waarschijnlijk op het toepassingsniveau, en de ASA configuratie is fijn. Als de applicatie echter nog steeds niet is gestart, moet u deze stappen voltooien om de configuraties op de ASA-zijde verder te verifiëren:

1. Controleer de SSL-configuratie (Secure Sockets Layer) op de ASA. ASDM maakt gebruik van SSL terwijl het communiceert met de ASA. Gebaseerd op de manier waarop ASDM wordt gelanceerd, kan nieuwere OS software geen gebruik van zwakkere algoritmen toestaan wanneer het SSL sessies bespreekt. Controleer welke algoritmen op de ASA zijn toegestaan en of er specifieke SSL-versies in de configuratie met de **show** zijn opgegeven **en voer alle ssl**-opdracht uit:

   <#root>

   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 tijdens de start van de ASDM fouten optreden in de onderhandeling van SSL-algoritmen, worden deze in de ASA-logboeken 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:10.103.236.189/52501 to
identity:10.106.36.132/443 duration 0:00:00 bytes 7 TCP Reset by appliance
```

Als u specifieke instellingen ziet, gaat u terug naar de standaardinstellingen. Bericht dat de VPN-3DES-AES-licentie op de ASA moet worden ingeschakeld voor de 3DES- en AES-algoritmen die door de ASA in de configuratie moeten worden gebruikt. Dit kan met het bevel van de **showversie** op CLI worden geverifieerd. Het uitvoersignaal wordt als volgt weergegeven:

<#root>

```
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 extra kosten worden verkregen van de Cisco-licentiewebsite. Klik op **Security producten** en kies vervolgens **Cisco ASA 3DES/AES-licentie**.

---

> **Opmerking**: in de nieuwe ASA 5500-X-platforms die met 8.6/9.x-code worden verzonden, worden de SSL-algoritme instellingen standaard op de Dasha1 ingesteld, waardoor de ASDM-sessies niet werken. Raadpleeg de ASA 5500-x: ASDM en andere SSL-functie werken niet uit het artikel in de box voor meer informatie.

---

2. Controleer of Web VPN op de ASA is ingeschakeld. Als deze URL is ingeschakeld, moet u deze gebruiken (https://10.106.36.132/admin) om er toegang toe te krijgen wanneer u de startpagina van het ASDM-web bezoekt.
3. Controleer of er een NAT-configuratie (Network Address Translation) op de ASA voor poort 443 is. Dit zorgt ervoor dat de ASA de aanvragen voor ASDM niet verwerkt, maar naar het netwerk/de interface stuurt waarvoor de NAT is geconfigureerd.
4. Als alles wordt geverifieerd en de ASDM nog steeds uitvalt, controleer dan of de ASA is ingesteld om te luisteren op de poort die is gedefinieerd voor ASDM met de opdracht **asp-tabelsocket** op de ASA

CLI. De output kan aantonen dat de ASA luistert op de ASDM-poort:

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

Als deze uitvoer de HTTP-serverconfiguratie niet op de ASA weergeeft, verwijdert en opnieuw toepast om de socket op de ASA-software te resetten.

5. Als u problemen ondervindt bij het inloggen/verifiëren op de ASDM, moet u controleren of de verificatieopties voor HTTP correct zijn ingesteld. Als er geen verificatieopdrachten zijn ingesteld, kunt u de ASA Enable password (Wachtwoord inschakelen) gebruiken om in te loggen op de ASDM. Als u gebruikersnaam/op 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:

<#root>

**aaa authentication http console LOCAL**

Vergeet niet een gebruikersnaam/wachtwoord aan te maken wanneer u de vorige opdracht inschakelt:

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

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

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

## Netwerkverbinding

Als u de vorige sectie hebt voltooid en nog steeds geen toegang hebt tot de ASDM, is de volgende stap om de netwerkverbinding met uw ASA te verifiëren vanaf de machine van waaruit u toegang wilt tot de ASDM. Er zijn een paar basisstappen voor probleemoplossing om te verifiëren dat de ASA het verzoek van de clientmachine ontvangt:

1. Test met Internet Control Message Protocol (ICMP).
   Ping de ASA interface van waaruit u toegang wilt tot de ASDM. Pingel kan succesvol zijn als ICMP wordt toegestaan om uw netwerk over te steken en er zijn geen beperkingen op het ASA interfaceniveau. Als pingelen mislukt, is dit waarschijnlijk omdat er een communicatieprobleem is tussen de ASA en de clientmachine. Dit is echter geen beslissende stap om vast te stellen of er sprake is van dat soort communicatiekwesties.
2. Bevestig met pakketopname.
   Plaats een pakketopname op de interface vanwaar u toegang tot de ASDM wilt hebben. De opname kan aantonen dat TCP-pakketten die bestemd zijn voor het IP-adres van de interface, aankomen met bestemmingspoortnummer 443 (standaard).

Om een opname te configureren gebruikt u deze opdracht:

<#root>

**capture asdm_test interface**

**match tcp host**

**eq 443 host**

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

Dit neemt elk TCP-verkeer op dat voor poort 443 op de ASA-interface komt van waaruit u verbinding maakt met de ASDM. Maak op dit punt verbinding via ASDM of open de startpagina van de ASDM-website. Gebruik vervolgens de opdracht **show capture asdm_test** om het resultaat van de opgenomen pakketten te bekijken:

<#root>

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 toont een synchroon (SYN) verzoek van de clientmachine aan de ASA, maar de ASA stuurt geen antwoord. Als u een opname ziet die vergelijkbaar is met de vorige, betekent dit dat de pakketten de ASA bereiken, maar de ASA reageert niet op die verzoeken, waardoor de kwestie wordt geïsoleerd voor de ASA zelf. Raadpleeg het eerste gedeelte van dit document voor meer informatie over de probleemoplossing.

Als u echter geen uitvoer ziet die vergelijkbaar is met de vorige en er geen pakketten worden opgenomen, betekent dit dat er een connectiviteitsprobleem is tussen de ASA en de ASDM-clientmachine. Controleer of er geen intermediaire apparaten zijn die TCP-poort 443 verkeer kunnen blokkeren en dat er geen browserinstellingen zijn, zoals Proxy-instellingen, die kunnen voorkomen dat het verkeer de ASA bereikt.

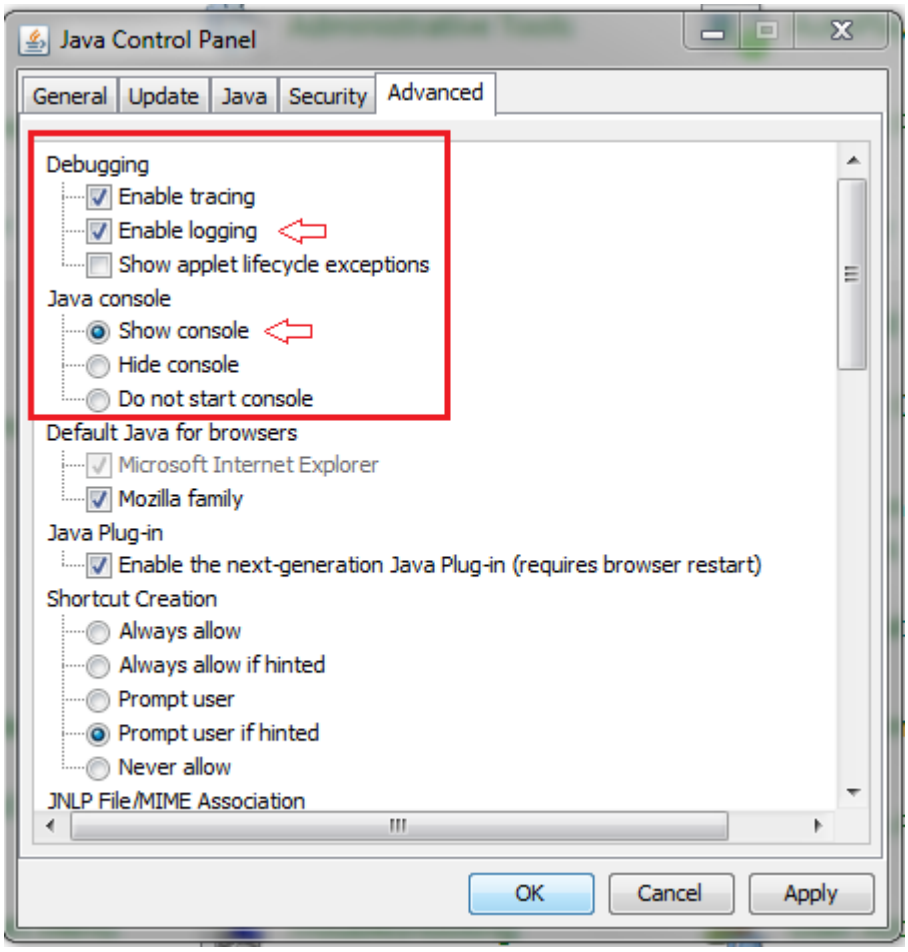
Packet Capture is doorgaans een goede manier om te bepalen of het pad naar de ASA duidelijk is en of er geen verdere diagnostiek nodig is om problemen met netwerkverbindingen uit te sluiten.

## Toepassingssoftware

In dit gedeelte wordt beschreven hoe u problemen kunt oplossen met de ASDM-startprogramma's die op de clientmachine zijn geïnstalleerd wanneer deze niet kan worden gestart/geladen. De ASDM startcher is het onderdeel dat zich op de clientmachine bevindt en met de ASA verbindt om het ASDM-beeld op te halen. Nadat de ASDM-afbeelding is opgehaald, wordt deze meestal in het cache opgeslagen en vervolgens naar de ASA-kant gebracht totdat veranderingen worden opgemerkt, zoals een ASDM-image update.

Voltooi de volgende basisstappen voor probleemoplossing om problemen op de clientmachine uit te sluiten:

1. Open de ASDM-startpagina vanaf een andere machine. Als het start, betekent dit dat het probleem met de betreffende client-machine is. Als dit niet lukt, gebruikt u de handleiding voor probleemoplossing vanaf het begin om de betrokken onderdelen in volgorde te isoleren.
2. Open de ASDM via web launch en start de software direct vanaf daar. Als het lukt, is het waarschijnlijk dat er problemen zijn met de ASDM lanceerinrichting installatie. Verwijder de ASDM-startkabel van de clientmachine en installeer deze opnieuw vanaf de ASA web launch zelf.
3. Schakel de cache directory van de ASDM uit in de home directory van de gebruiker. De cache wordt gewist wanneer u de gehele cache directory verwijdert. Als de ASDM met succes start, kunt u de cache ook verwijderen uit het menu ASDM **File**.
4. Controleer of de juiste Java-versie is geïnstalleerd. In de Cisco ASDM release Notes wordt een lijst gemaakt met de vereisten voor geteste Java-versies.
5. Schakel de Java cache uit. Kies **Algemeen > Tijdelijk internetbestand** in het **Java-configuratiescherm**. Klik vervolgens op **Weergeven** om een **Java Cache Viewer** te starten. Verwijder alle items die verwijzen naar of gerelateerd zijn aan ASDM.
6. Als deze stappen niet slagen, verzamel de het zuiveren informatie van de cliëntmachine voor verder onderzoek. Schakel debugging voor ASDM in met de URL: https://<IP-adres van de ASA>?debug=5, bijvoorbeeld https://10.0.0.1?debug=5.
   Met Java Versie 6 (ook wel Versie 1.6 genoemd), zijn Java debugging-berichten ingeschakeld vanuit **Java Control Panel > Advanced**. Selecteer vervolgens de aankruisvakjes onder **Debugging**. Selecteer **Niet starten console** onder de **Java console**. Java-debugging moet zijn ingeschakeld voordat ASDM kan worden gestart.




De Java-consoleuitvoer wordt vastgelegd in de directory .asdm/log van de thuismap van de gebruiker. ASDM-logbestanden kunnen ook in dezelfde map worden gevonden.

# Opdrachten uitvoeren met HTTPS

Deze procedure helpt bij het bepalen van alle Layer 7-problemen voor het HTTP-kanaal. Deze informatie blijkt nuttig wanneer u in een situatie bent 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 voor toegang tot de startpagina van het ASDM-web kan ook worden gebruikt om opdrachten op configuratieniveau op de ASA uit te voeren. Deze URL kan worden gebruikt om configuratie wijzigingen aan te brengen op basisniveau in de ASA, die een externe apparaatherlading omvat. Gebruik de volgende syntaxis om een opdracht in te voeren:

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

Als de opdracht een spatie bevat en de browser geen spatie-tekens in een URL kan parseren, kunt u het +-teken of **%20** gebruiken om de spatie aan te geven.

https://10.106.36.137/admin/exec/show resulteert bijvoorbeeld in een uitvoer van de showversie 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
```

Voor deze opdrachtmethode moet de HTTP-server op de ASA zijn ingeschakeld en moeten de nodige HTTP-beperkingen actief zijn. Dit betekent echter NIET dat er een ASDM-afbeelding op de ASA aanwezig moet zijn.

# Gerelateerde informatie

- **ASDM Access for applicaties configureren**
- **ASA 5500-x: ASDM en andere SSL-functies werken niet buiten het vak**
- **Cisco ASDM Releaseopmerkingen**
- **Cisco-licentiepagina voor het verkrijgen van een 3DES/AES-licentie op de ASA**
- **Technische ondersteuning en documentatie â€“ Cisco Systems**

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.