ASDM en WebVPN ingeschakeld op dezelfde interface van de ASA

Inhoud

[Inleiding](#)
[Voorwaarden](#)
[Vereisten](#)
[Gebruikte componenten](#)
[Conventies](#)
[Probleem](#)
[Oplossing](#)
[Gebruik de juiste URL](#)
[Verander de poort waarop elke servicelijst staat](#)
[Verander de poort voor de HTTPS Server-service wereldwijd](#)
[Verander de poort voor de WebVPN-service wereldwijd](#)
[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u toegang hebt tot Cisco Adaptieve Security Devices Manager (ASDM) en het WebVPN-portaal wanneer ze allebei geactiveerd zijn op dezelfde interface van Cisco 5500 Series adaptieve security applicatie (ASA).

> **Opmerking:** Dit document is niet van toepassing op Cisco 500 Series PIX-firewall, omdat WebVPN niet wordt ondersteund.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- De configuratie van WebVPN verwijst naar de Clientless SSL VPN (WebVPN) in ASA Configuration Voorbeeld voor meer informatie.
- Basisconfiguratie vereist voor het lanceren van ASDM ß- Raadpleeg het gedeelte ASDM van de Cisco ASA Series ASDM Configuration Guide, 7.0 voor meer informatie.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco 5500 Series 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.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Probleem

In ASA versies eerder dan versie 8.0(2) kunnen ASDM en WebVPN niet worden ingeschakeld op dezelfde interface van de ASA, omdat beide standaard op dezelfde poort (443) luisteren. In versies 8.0(2) en later ondersteunt de ASA zowel clientloze Secure Socket Layer (SSL) VPN-sessies (WebVPN) en ASDM administratieve sessies tegelijkertijd op Port 443 van de externe interface. Wanneer beide services echter tegelijkertijd zijn ingeschakeld, wordt de standaard-URL voor een bepaalde interface in de ASA altijd standaard ingeschakeld voor de WebVPN-service. Denk bijvoorbeeld aan deze ASA configuratie data:

```
rtpvpnoutbound6# show run ip
!
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
interface Vlan2
 nameif outside
 security-level 0
 ip address 10.150.172.46 255.255.252.0
!
interface Vlan3
 nameif dmz
 security-level 50
 ip address dhcp
!
interface Vlan5
 nameif test
 security-level 0
 ip address 1.1.1.1 255.255.255.255 pppoe setroute
!
rtpvpnoutbound6# show run web
webvpn
 enable outside
 enable dmz
 anyconnect image disk0:/anyconnect-win-3.1.06078-k9.pkg 1
 anyconnect image disk0:/anyconnect-macosx-i386-3.1.06079-k9.pkg 2
 anyconnect enable
```

```
 tunnel-group-list enable
 tunnel-group-preference group-url

rtpvpnoutbound6#  show run http
http server enable
http 192.168.1.0 255.255.255.0 inside
http 0.0.0.0 0.0.0.0 dmz
http 0.0.0.0 0.0.0.0 outside

rtpvpnoutbound6# show run tun
tunnel-group DefaultWEBVPNGroup general-attributes
 address-pool ap_fw-policy
 authentication-server-group ldap2
tunnel-group DefaultWEBVPNGroup webvpn-attributes
 group-url https://rtpvpnoutbound6.cisco.com/admin enable
 without-csd
```

Oplossing

Om dit probleem op te lossen kunt u de juiste URL gebruiken om toegang te krijgen tot de respectievelijke service of de poort waarop de services worden benaderd wijzigen.

> **Opmerking:** Een nadeel van deze laatste oplossing is dat de haven wereldwijd wordt veranderd, zodat elke interface door de verandering wordt beïnvloed.

Gebruik de juiste URL

In de voorbeeldconfiguratiegegevens in het gedeelte Probleem kunnen de externe interface van de ASA door HTTPS worden bereikt via deze twee URL's:

```
https://<ip-address> <=> https://10.150.172.46
https://<domain-name> <=> https://rtpvpnoutbound6.cisco.com
```

Als u echter probeert om toegang te krijgen tot deze URL's terwijl WebVPN-service is ingeschakeld, stuurt de ASA u terug naar het WebVPN-portaal:

```
https://rtpvpnoutbound6.cisco.com/+CSCOE+/logon.html
```

U kunt ASDM als volgt benaderen:

```
https://rtpvpnoutbound6.cisco.com/admin
```

> **Opmerking:** Zoals wordt getoond in de gegevens van de voorbeeldconfiguratie, heeft de standaard tunnelgroep een **groep-url** bepaald met gebruik van de **groep-url https://rtpvpnoutbound6.cisco.com/admin** opdracht **toelaten**, wat met de ASDM toegang zou moeten in conflict brengen. Maar de URL *https://<ip-adres/domein>/admin* is gereserveerd voor ASDM-toegang en als u deze instelt onder de tunnelgroep, is er geen effect. U wordt altijd terugverwezen naar *https://<ip-adres/domein>/admin/public/index.html*.

Verander de poort waarop elke servicelijst staat

In deze sectie wordt beschreven hoe u de poort voor zowel de ASDM- als WebeVPN-services kunt wijzigen.

Verander de poort voor de HTTPS Server-service wereldwijd

Voltooi deze stappen om de poort voor de ASDM-service te wijzigen:

1. Schakel de HTTPS-server in om op een andere poort te luisteren om de configuratie te veranderen die betrekking heeft op de ASDM-service in de ASA ASA, zoals hier wordt getoond:

   ```
   ASA(config)#http server enable <1-65535>

   configure mode commands/options:
   <1-65535> The management server's SSL listening port. TCP port 443 is the
   default.
   ```

   Hierna volgt een voorbeeld:

   ```
   ASA(config)#http server enable 65000
   ```

2. Nadat u de standaardpoortconfiguratie hebt gewijzigd, gebruikt u deze indeling om de ASDM te starten vanaf een ondersteunde webbrowser op het netwerk van het beveiligingsapparaat:

   ```
   https://interface_ip_address:
   ```

   Hierna volgt een voorbeeld:

   ```
   https://192.168.1.1:65000
   ```

Verander de poort voor de WebVPN-service wereldwijd

Voltooi deze stappen om de poort voor de WebVPN-service te wijzigen:

1. Laat WebexVPN op een andere poort luisteren om de configuratie te veranderen die gerelateerd is aan de WebVPN-service in de ASA:

   Schakel de functie WebexVPN in op de ASA:

   ```
   ASA(config)#webvpn
   ```

   Schakel de WebVPN-service voor de externe interface van de ASA in:

   ```
   ASA(config-webvpn)#enable outside
   ```

   Laat ASA naar het WebVPN verkeer op het aangepaste havenaantal luisteren:

   ```
   ASA(config-webvpn)#port <1-65535>

   webvpn mode commands/options:
   <1-65535> The WebVPN server's SSL listening port. TCP port 443 is the
   default.
   ```

Hierna volgt een voorbeeld:

```
ASA(config)#webvpn
ASA(config-webvpn)#enable outside
ASA(config-webvpn)#port 65010
```

2. Nadat u de standaardpoortconfiguratie hebt gewijzigd, opent u een ondersteunde webbrowser en gebruikt u deze indeling om verbinding te maken met de WebVPN server:

   https://interface_ip_address:

   Hierna volgt een voorbeeld:

   https://192.168.1.1:65010

Gerelateerde informatie

- Cisco Adapter Security apparaat Manager - ondersteuningspagina
- Cisco ASA 5500-X Series Next-generation firewalls
- Technische ondersteuning en documentatie – Cisco Systems