ASDM et WebVPN activés sur la même interface de l'ASA

Contenu

Introduction

Ce document décrit comment accéder au Cisco Adaptive Security Device Manager (ASDM) et au portail WebVPN lorsqu'ils sont tous deux activés sur la même interface de l'appliance de sécurité adaptatif (ASA) de la gamme Cisco 5500.

> **Note**: Ce document ne s'applique pas au pare-feu PIX de la gamme Cisco 500, car il ne prend pas en charge WebVPN.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration de WebVPN - consultez l'exemple de configuration de VPN SSL sans client (WebVPN) sur ASA pour plus d'informations.
- Configuration de base requise pour lancer l'ASDM - Reportez-vous à la section Utilisation de l'ASDM du Guide de configuration ASDM de la gamme Cisco ASA, 7.0 pour plus d'informations.

Components Used

Les informations de ce document sont basées sur la gamme Cisco 5500 ASA.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Problème

Dans les versions ASA antérieures à la version 8.0(2), ASDM et WebVPN ne peuvent pas être activés sur la même interface de l'ASA, car les deux écoutent sur le même port (443) par défaut. Dans les versions 8.0(2) et ultérieures, l'ASA prend en charge simultanément les sessions VPN SSL (WebVPN) sans client et les sessions d'administration ASDM sur le port 443 de l'interface externe. Cependant, lorsque les deux services sont activés ensemble, l'URL par défaut d'une interface particulière sur l'ASA est toujours définie par défaut sur le service WebVPN. Par exemple, considérez les données de configuration ASA&deux-points ;

```
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
```

Solution

Afin de résoudre ce problème, vous pouvez soit utiliser l'URL appropriée afin d'accéder au service concerné, soit modifier le port sur lequel les services sont accessibles.

> **Note**: Un inconvénient de cette dernière solution est que le port est modifié globalement, de sorte que chaque interface est affectée par le changement.

Utiliser l'URL appropriée

Dans l'exemple de données de configuration fourni dans la section Problème, l'interface externe de l'ASA peut être atteinte par HTTPS via ces deux URL :

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

Cependant, si vous tentez d'accéder à ces URL lorsque le service WebVPN est activé, l'ASA vous redirige vers le portail WebVPN :

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

Pour accéder à ASDM, vous pouvez utiliser cette URL :

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

> **Note**: Comme indiqué dans l'exemple de données de configuration, le groupe de tunnels par défaut a une **url-groupe** définie avec l'utilisation de la commande **group-url https://rtpvpnoutbound6.cisco.com/admin enable**, qui devrait entrer en conflit avec l'accès ASDM. Cependant, l'URL *https://<adresse-ip/domaine>/admin* est réservée à l'accès ASDM et si vous la définissez sous le groupe de tunnels, il n'y a aucun effet. Vous êtes toujours redirigé vers *https://<adresse-ip/domaine>/admin/public/index.html*.

Modifier le port sur lequel chaque service écoute

Cette section décrit comment modifier le port pour les services ASDM et WebVPN.

Modifier globalement le port du service de serveur HTTPS

Complétez ces étapes afin de modifier le port pour le service ASDM :

1. Activez le serveur HTTPS à écouter sur un autre port afin de modifier la configuration associée au service ASDM sur l'ASA, comme indiqué ici :

   ```
   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.
   ```

   Voici un exemple :

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

2. Après avoir modifié la configuration de port par défaut, utilisez ce format afin de lancer l'ASDM à partir d'un navigateur Web pris en charge sur le réseau de l'appliance de sécurité :

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

   Voici un exemple :

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

Modifier le port du service WebVPN à l'échelle mondiale

Complétez ces étapes afin de modifier le port du service WebVPN :

1. Autoriser WebVPN à écouter sur un autre port afin de modifier la configuration associée au service WebVPN sur l'ASA :

   Activez la fonctionnalité WebVPN sur l'ASA :

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

   Activez le service WebVPN pour l'interface externe de l'ASA :

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

   Autoriser l'ASA à écouter le trafic WebVPN sur le numéro de port personnalisé :

   ```
   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.
   ```

   Voici un exemple :

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

2. Après avoir modifié la configuration de port par défaut, ouvrez un navigateur Web pris en charge et utilisez ce format afin de vous connecter au serveur WebVPN :

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

   Voici un exemple :

   ```
   https://192.168.1.1:65010
   ```

Informations connexes

- Page d'assistance de Cisco Adaptive Security Device Manager
- Pare-feu de nouvelle génération Cisco ASA 5500-X
- Support et documentation techniques - Cisco Systems