ASDM y WebVPN habilitados en la misma interfaz del ASA

Contenido

Introducción

Este documento describe cómo acceder al Cisco Adaptive Security Device Manager (ASDM) y al portal WebVPN cuando ambos están habilitados en la misma interfaz del Cisco 5500 Series Adaptive Security Appliance (ASA).

> **Nota:** Este documento no es aplicable para Cisco 500 Series PIX Firewall, porque no soporta WebVPN.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Configuración WebVPN â Consulte el Ejemplo de Configuración de Clientless SSL VPN (WebVPN) en ASA para obtener más información.
- Configuración básica requerida para iniciar el ASDM â Consulte la sección Uso de ASDM de la Guía de Configuración de Cisco ASA Series ASDM, 7.0 para obtener más información.

Componentes Utilizados

La información de este documento se basa en el Cisco 5500 Series 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.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Problema

En las versiones de ASA anteriores a la versión 8.0(2), el ASDM y el WebVPN no se pueden habilitar en la misma interfaz del ASA, ya que ambos escuchan en el mismo puerto (443) de forma predeterminada. En las versiones 8.0(2) y posteriores, ASA admite sesiones VPN (WebVPN) sin cliente de capa de sockets seguros (SSL) y sesiones administrativas ASDM simultáneamente en el puerto 443 de la interfaz exterior. Sin embargo, cuando ambos servicios se habilitan juntos, la dirección URL predeterminada para una interfaz determinada en el ASA siempre adopta de forma predeterminada el servicio WebVPN. Por ejemplo, considere estos datos y puntos de configuración de ASA;

```
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
```

Solución

Para resolver este problema, puede utilizar la URL apropiada para acceder al servicio respectivo o cambiar el puerto en el que se accede a los servicios.

> **Nota:** Una desventaja con esta última solución es que el puerto se cambia globalmente, por lo que cada interfaz se ve afectada por el cambio.

Utilice la URL adecuada

En el ejemplo de datos de configuración proporcionados en la sección Problema, HTTPS puede alcanzar la interfaz externa del ASA a través de estas dos URL:

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

Sin embargo, si intenta acceder a estas URL mientras el servicio WebVPN está habilitado, el ASA le redirige al portal WebVPN:

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

Para acceder a ASDM, puede utilizar esta URL:

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

> **Nota:** Como se muestra en los datos de configuración de ejemplo, el grupo de túnel predeterminado tiene un **group-url** definido con el uso del comando **group-url https://rtpvpnoutbound6.cisco.com/admin enable**, que debería entrar en conflicto con el acceso ASDM. Sin embargo, la URL *https://<ip-address/domain>/admin* está reservada para el acceso ASDM, y si lo configura en el grupo de túnel, no hay ningún efecto. Siempre se le redirige a *https://<ip-address/domain>/admin/public/index.html*.

Cambiar el puerto en el que escucha cada servicio

Esta sección describe cómo cambiar el puerto para los servicios ASDM y WebVPN.

Cambiar globalmente el puerto del servicio de servidor HTTPS

Complete estos pasos para cambiar el puerto para el servicio ASDM:

1. Habilite el servidor HTTPS para escuchar en un puerto diferente para cambiar la configuración relacionada con el servicio ASDM en el ASA, como se muestra aquí:

   ```
   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.
   ```

   Aquí tiene un ejemplo:

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

2. Después de cambiar la configuración de puerto predeterminada, utilice este formato para iniciar el ASDM desde un navegador web soportado en la red del dispositivo de seguridad:

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

   Aquí tiene un ejemplo:

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

Cambiar globalmente el puerto del servicio WebVPN

Complete estos pasos para cambiar el puerto para el servicio WebVPN:

1. Permita que WebVPN escuche en un puerto diferente para cambiar la configuración relacionada con el servicio WebVPN en el ASA:

   Habilite la función WebVPN en el ASA:

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

   Habilite el servicio WebVPN para la interfaz exterior del ASA:

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

   Permita que ASA escuche el tráfico WebVPN en el número de puerto personalizado:

   ```
   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.
   ```

   Aquí tiene un ejemplo:

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

2. Después de cambiar la configuración predeterminada del puerto, abra un navegador web admitido y utilice este formato para conectarse al servidor WebVPN:

   https://interface_ip_address:

   Aquí tiene un ejemplo:

   https://192.168.1.1:65010

Información Relacionada

- Página de soporte de Cisco Adaptive Security Device Manager
- Firewalls de próxima generación Cisco ASA Serie 5500-X
- Soporte Técnico y Documentación - Cisco Systems