在ASA的同一接口上启用ASDM和WebVPN

目录

简介

本文档介绍在思科5500系列自适应安全设备(ASA)的同一接口上同时启用思科自适应安全设备管理器(ASDM)和WebVPN门户时，如何访问它们。

> **注意：**本文对Cisco 500系列PIX防火墙是不适用的，因为它不支持WebVPN。

先决条件

要求

Cisco 建议您了解以下主题：

- WebVPN配置有关详细信息，请参阅ASA上的无客户端SSL VPN(WebVPN)配置示例。
- 要启动ASDM，需要基本配置。有关详细信息，请参阅Cisco ASA系列ASDM配置指南7.0的使用ASDM部分。

使用的组件

本文档中的信息基于Cisco 5500系列ASA。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原

始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

问题

在早于8.0(2)版本的ASA中，ASDM和WebVPN无法在ASA的同一接口上启用，因为默认情况下，两者都侦听同一端口(443)。在版本8.0(2)及更高版本中，ASA在外部接口的端口443上同时支持无客户端安全套接字层(SSL)VPN(WebVPN)会话和ASDM管理会话。但是，当两个服务同时启用时，ASA上特定接口的默认URL始终默认为WebVPN服务。例如，请考虑此ASA配置数据（&冒号）；

```
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
```

解决方案

要解决此问题，您可以使用适当的URL来访问各自的服务，也可以更改访问服务的端口。

> **注意**：后一种解决方案的一个缺点是端口全局更改，因此每个接口都受更改的影响。

使用适当的URL

在“问题”部分提供的示例配置数据中，ASA的外部接口可通过以下两个URL通过HTTPS访问：

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

但是，如果在启用WebVPN服务时尝试访问这些URL，ASA会将您重定向到WebVPN门户：

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

要访问ASDM，可以使用此URL:

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

> **注意**：如示例配置数据所示，默认隧道组使用**group-url https://rtpvpnoutbound6.cisco.com/admin enable**命令定义了**group-url**，该命令应与ASDM访问冲突。但是，URL *https://<ip-address/domain>/admin*保留用于ASDM访问，如果在隧道组下设置，则不会产生任何影响。您始终被重定向*到https://<ip-address/domain>/admin/public/index.html*。

更改每个服务侦听的端口

本节介绍如何更改ASDM和WebVPN服务的端口。

全局更改HTTPS服务器服务的端口

要更改ASDM服务的端口，请完成以下步骤：

1. 启用HTTPS服务器以侦听不同端口，以更改与ASA上的ASDM服务相关的配置，如下所示：

   ```
   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.
   ```

   示例如下：

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

2. 更改默认端口配置后，请使用此格式从安全设备网络上支持的Web浏览器启动ASDM:

   https://interface_ip_address:

   示例如下：

   https://192.168.1.1:65000

全局更改WebVPN服务的端口

要更改WebVPN服务的端口，请完成以下步骤：

1. 允许WebVPN侦听不同端口，以更改与ASA上的WebVPN服务相关的配置：

   在ASA上启用WebVPN功能：

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

   为ASA的外部接口启用WebVPN服务：

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

   允许ASA侦听自定义端口号上的WebVPN流量：

   ```
   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.
   ```

   示例如下：

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

2. 更改默认端口配置后，打开支持的Web浏览器并使用此格式以连接到WebVPN服务器：

   https://interface_ip_address:

   示例如下：

   https://192.168.1.1:65010

相关信息

- [思科自适应安全设备管理器 — 支持页]

- Cisco ASA 5500-X系列下一代防火墙
- 技术支持和文档 - Cisco Systems