

在ASA的同一介面上啟用ASDM和WebVPN

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[問題](#)

[解決方案](#)

[使用適當的URL](#)

[更改每個服務偵聽的埠](#)

[全域性更改HTTPS伺服器服務的埠](#)

[全域性更改WebVPN服務的埠](#)

[相關資訊](#)

簡介

本檔案介紹如何存取思科調適型安全裝置管理員(ASDM)和WebVPN入口網站(當兩者在思科5500系列調適型安全裝置(ASA)的相同介面上啟用時)。

附註：本文檔不適用於Cisco 500系列PIX防火牆，因為它不支援WebVPN。

必要條件

需求

思科建議您瞭解以下主題：

- WebVPN配置â有關詳細資訊，請參閱[ASA上的無客戶端SSL VPN\(WebVPN\)配置示例](#)。
- 啟動ASDM所需的基本配置â請參閱[Cisco ASA系列ASDM配置指南7.0的使用ASDM](#)一節瞭解更多資訊。

採用元件

本文檔中的資訊基於Cisco 5500系列ASA。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設

)的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱[思科技術提示慣例](#)。

問題

在低於版本8.0(2)的ASA版本中，無法在ASA的同一介面上啟用ASDM和WebVPN，因為預設情況下，兩者都在同一埠(443)上偵聽。在8.0(2)及更高版本中，ASA在外部介面的埠443上同時支援無客戶端安全套接字層(SSL)VPN(WebVPN)會話和ASDM管理會話。但是，當同時啟用這兩個服務時，ASA上特定介面的預設URL始終預設為WebVPN服務。例如，請考慮此ASA配置資料(&C);

```
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
```

解決方案

為了解決此問題，您可以使用適當的URL存取對應的服務，或是變更存取服務的連線埠。

附註：後一種解決方案的缺點是埠全域性更改，因此每個介面都會受到更改的影響。

使用適當的URL

在[問題](#)部分提供的示例配置資料中，HTTPS可通過以下兩個URL訪問ASA的外部介面：

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

但是，如果在啟用WebVPN服務時嘗試訪問這些URL，則ASA會將您重定向到WebVPN門戶：

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

要訪問ASDM，您可以使用以下URL：

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

附註：如示例配置資料所示，預設隧道組具有使用**group-url https://rtpvpnoutbound6.cisco.com/admin enable**命令定義的**group-url**，該命令應與ASDM訪問衝突。但是，*https://<ip-address/domain>/admin*的URL保留用於ASDM訪問，如果您在隧道組下設定它，則不起作用。系統總是將您重新導向到*https://<ip-address/domain>/admin/public/index.html*。

更改每個服務偵聽的埠

本節介紹如何更改ASDM和WebVPN服務的埠。

全域性更改HTTPS伺服器服務的埠

完成以下步驟，以便更改ASDM服務的埠：

1. 啟用HTTPS伺服器以偵聽其他埠，以便更改與ASA上的ASDM服務相關的配置，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.
```

以下是範例：

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

2. 更改預設埠配置後，使用以下格式從安全裝置網路上支援的網路瀏覽器啟動ASDM:

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

以下是範例：

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

全域性更改WebVPN服務的埠

完成以下步驟即可變更WebVPN服務的連線埠：

1. 允許WebVPN偵聽其他埠，以便更改與ASA上的WebVPN服務相關的配置：

在ASA上啟用WebVPN功能：

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

為ASA的外部介面啟用WebVPN服務：

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

允許ASA偵聽自定義埠號上的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.
```

以下是範例：

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

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

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

2. 更改預設埠配置後，開啟支援的Web瀏覽器，然後使用以下格式連線到WebVPN伺服器：

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

以下是範例：

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

相關資訊

- [Cisco Adaptive Security Device Manager — 支援頁](#)
- [Cisco ASA 5500-X系列下一代防火牆](#)

- [技術支援與文件 - Cisco Systems](#)