# ASA の同じインターフェイスで有効になっている ASDM および WebVPN

## 内容



## 概要

このドキュメントでは、Cisco 5500 シリーズ適応型セキュリティ アプライアンスの同一インターフェイスで同時に有効化されている Cisco Adaptive Security Device Manager（ASDM）と WebVPN ポータルにアクセスする方法について説明します。

> **注**：このドキュメントは Cisco 500 シリーズ PIX ファイアウォールには適用されません（Cisco 500 シリーズ PIX ファイアウォールは WebVPN をサポートしていないため）。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- WebVPNの設定の詳細は、『ASAでのクライアントレスSSL VPN(WebVPN)の設定例』を参照してください。
- ASDMを起動するために必要な基本設定詳細については、『Cisco ASAシリーズASDMコンフィギュレーションガイド7.0』の「ASDMの使用」セクションを参照してください。

## 使用するコンポーネント

このドキュメントの情報は、Cisco 5500 シリーズ ASA に基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

## 表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

# 問題

バージョン8.0(2)より前のASAバージョンでは、ASDMとWebVPNはデフォルトで同じポート(443)でリッスンするため、ASAの同じインターフェイスでは有効にできません。バージョン8.0(2)以降では、ASAはクライアントレスSecure Sockets Layer(SSL)VPN(WebVPN)セッションとASDM管理セッションの両方を外部インターフェイスのポート443で同時にサポートします。ただし、両方のサービスを同時に有効にすると、ASAの特定のインターフェイスのデフォルトURLは常にWebVPNサービスにデフォルト設定されます。たとえば、次のASA設定データとコロンについて考えてみましょう。

```
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
```

# 解決方法

この問題を解決するには、適切なURLを使用してそれぞれのサービスにアクセスするか、サービスにアクセスするポートを変更します。

> **注**：後者のソリューションの1つの欠点は、ポートがグローバルに変更されることです。そのため、すべてのインターフェイスが変更の影響を受けます。

## 適切なURLの使用

「問題」セクションで提供されている設定データの例では、次の2つのURLを介してASAの外部インターフェイスにHTTPSで到達できます。

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

ただし、WebVPNサービスが有効になっている間にこれらのURLにアクセスしようとすると、ASAによってWebVPNポータルにリダイレクトされます。

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

ASDMにアクセスするには、次のURLを使用できます。

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

> **注**：設定例の設定データに示すように、デフォルトのトンネルグループには**group-url https://rtpvpnoutbound6.cisco.com/admin enableコマンドを使用して定義されたgroup-urlが**あり、ASDMアクセスと競合する必要があります。ただし、URL *https://<ip-address/domain>/admin*はASDMアクセス用に予約されており、トンネルグループで設定しても効果はありません。*https://<ip-address/domain>/admin/public/index.html*にリダイレクトされます。

## 各サービスがリッスンするポートの変更

このセクションでは、ASDMサービスとWebVPNサービスの両方のポートを変更する方法につい

て説明します。

### HTTPSサーバサービスのポートをグローバルに変更する

ASDMサービスのポートを変更するには、次の手順を実行します。

1. 次に示すように、ASAのASDMサービスに関連する設定を変更するために、HTTPSサーバが別のポートでリッスンできるようにします。

   ```
   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.
   ```

   以下が一例です。

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

2. デフォルトのポート設定を変更した後、セキュリティアプライアンスネットワークでサポートされているWebブラウザからASDMを起動するには、次の形式を使用します。

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

   以下が一例です。

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

### WebVPNサービスのポートをグローバルに変更する

WebVPNサービスのポートを変更するには、次の手順を実行します。

1. ASAのWebVPNサービスに関連する設定を変更するために、WebVPNが別のポートでリッスンすることを許可します。

   ASAでWebVPN機能を有効にします。

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

   ASAの外部インターフェイスに対してWebVPNサービスを有効にします。

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

   ASAがカスタマイズされたポート番号でWebVPNトラフィックをリッスンできるようにします。

   ```
   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.
   ```

   以下が一例です。

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

2. デフォルトのポート設定を変更したら、サポートされているWebブラウザを開き、次の形式を使用してWebVPNサーバに接続します。

   **https://interface_ip_address:**

   以下が一例です。

   **https://192.168.1.1:65010**

# 関連情報

- Cisco Adaptive Security Device Manager に関するサポート ページ
- Cisco ASA 5500-X シリーズ次世代ファイアウォール
- テクニカル サポートとドキュメント – Cisco Systems