ASDM e WebVPN abilitati sulla stessa interfaccia dell'ASA

Sommario

Introduzione

Questo documento descrive come accedere a Cisco Adaptive Security Device Manager (ASDM) e al portale WebVPN quando entrambi sono abilitati sulla stessa interfaccia di Cisco serie 5500 Adaptive Security Appliance (ASA).

> **Nota:** Questo documento non è applicabile per Cisco serie 500 PIX Firewall, perché non supporta WebVPN.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione di WebVPN â Per ulteriori informazioni, fare riferimento all'esempio di configurazione di WebVPN (WebVPN) SSL senza client sull'appliance ASA.
- Configurazione di base richiesta per avviare ASDM â Per ulteriori informazioni, consultare la sezione Uso di ASDM della guida alla configurazione di ASDM Cisco serie ASA, versione 7.0.

Componenti usati

Per la stesura del documento, è stata usata una appliance Cisco ASA serie 5500.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Problema

Nelle versioni ASA precedenti alla versione 8.0(2), ASDM e WebVPN non possono essere abilitati sulla stessa interfaccia dell'ASA, in quanto per impostazione predefinita entrambi sono in ascolto sulla stessa porta (443). Nelle versioni 8.0(2) e successive, l'ASA supporta sia le sessioni VPN (WebVPN) Secure Sockets Layer (SSL) senza client sia le sessioni amministrative ASDM simultaneamente sulla porta 443 dell'interfaccia esterna. Tuttavia, quando entrambi i servizi sono abilitati insieme, l'URL predefinito di una particolare interfaccia sull'ASA diventa sempre il servizio WebVPN. Ad esempio, considerare i seguenti dati di configurazione dell'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
```

Soluzione

Per risolvere questo problema, è possibile utilizzare l'URL appropriato per accedere al servizio corrispondente o modificare la porta su cui si accede ai servizi.

> **Nota:** Uno svantaggio di quest'ultima soluzione è che la porta viene modificata a livello globale, in modo che ogni interfaccia sia interessata dalla modifica.

Utilizzare l'URL appropriato

Nell'esempio di dati di configurazione fornito nella sezione Problem, l'interfaccia esterna dell'ASA può essere raggiunta da HTTPS tramite i due URL seguenti:

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

Tuttavia, se si tenta di accedere a questi URL mentre il servizio WebVPN è abilitato, l'ASA reindirizza l'utente al portale WebVPN:

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

Per accedere ad ASDM, è possibile usare il seguente URL:

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

> **Nota:** Come mostrato nei dati di configurazione dell'esempio, per il gruppo di tunnel predefinito viene definito un **URL di gruppo** con il comando **group-url https://rtpvpnoutbound6.cisco.com/admin enable**, che deve essere in conflitto con l'accesso ASDM. Tuttavia, l'URL *https://<ip-address/domain>/admin* è riservato per l'accesso ASDM e, se impostato nel gruppo di tunnel, non ha alcun effetto. Viene sempre reindirizzato a *https://<ip-address/domain>/admin/public/index.html*.

Modificare la porta di ascolto di ogni servizio

In questa sezione viene descritto come modificare la porta per i servizi ASDM e WebVPN.

Modifica globale della porta per il servizio server HTTPS

Per modificare la porta del servizio ASDM, completare i seguenti passaggi:

1. Abilitare il server HTTPS per restare in ascolto su una porta diversa e modificare la configurazione correlata al servizio ASDM sull'appliance ASA, come mostrato di seguito:

   ```
   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.
   ```

   Di seguito è riportato un esempio:

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

2. Dopo aver modificato la configurazione predefinita della porta, usare questo formato per avviare ASDM da un browser Web supportato sulla rete dell'appliance di sicurezza:

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

   Di seguito è riportato un esempio:

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

Modifica globale della porta per il servizio WebVPN

Completare questi passaggi per modificare la porta per il servizio WebVPN:

1. Consentire a WebVPN di restare in ascolto su una porta diversa per modificare la configurazione relativa al servizio WebVPN sull'appliance ASA:

   Abilitare la funzione WebVPN sull'appliance ASA:

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

   Abilitare il servizio WebVPN per l'interfaccia esterna dell'ASA:

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

   Consentire all'ASA di ascoltare il traffico WebVPN sul numero di porta personalizzato:

   ```
   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.
   ```

   Di seguito è riportato un esempio:

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

2. Dopo aver modificato la configurazione predefinita della porta, aprire un browser Web supportato e utilizzare questo formato per connettersi al server WebVPN:

   https://interface_ip_address:

   Di seguito è riportato un esempio:

   https://192.168.1.1:65010

Informazioni correlate

- Cisco Adaptive Security Device Manager - Pagina di supporto
- Cisco ASA serie 5500-X Next-Generation Firewall
- Documentazione e supporto tecnico – Cisco Systems