ASDM und WebVPN auf derselben Schnittstelle der ASA aktiviert

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie auf den Cisco Adaptive Security Device Manager (ASDM) und das WebVPN-Portal zugreifen, wenn beide auf derselben Schnittstelle der Cisco Adaptive Security Appliance (ASA) der Serie 5500 aktiviert sind.

> **Hinweis**: Dieses Dokument gilt nicht für die Cisco PIX Firewall der Serie 500, da es WebVPN nicht unterstützt.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- WebVPN-Konfiguration - Weitere Informationen finden Sie im Clientless SSL VPN (WebVPN) auf ASA-Konfigurationsbeispiel.
- Eine grundlegende Konfiguration zum Starten des ASDM- ist erforderlich. Weitere Informationen finden Sie im Abschnitt Using ASDM im ASDM Configuration Guide der Cisco ASA-Serie, 7.0.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der Cisco Serie ASA 5500.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Problem

In ASA-Versionen vor Version 8.0(2) können ASDM und WebVPN nicht auf derselben Schnittstelle der ASA aktiviert werden, da beide standardmäßig auf demselben Port (443) lauschen. In Version 8.0(2) und höher unterstützt die ASA sowohl clientlose SSL VPN (SSL)-VPN (WebVPN)-Sitzungen (Secure Sockets Layer) als auch ASDM-Verwaltungssitzungen gleichzeitig auf Port 443 der externen Schnittstelle. Wenn jedoch beide Services zusammen aktiviert sind, wird der WebVPN-Dienst standardmäßig für die Standard-URL einer bestimmten Schnittstelle auf der ASA aktiviert. Nehmen wir zum Beispiel die folgenden ASA-Konfigurationsdaten und -Doppelpunkte:

```
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
```

Lösung

Um dieses Problem zu beheben, können Sie entweder die entsprechende URL verwenden, um auf den entsprechenden Service zuzugreifen, oder den Port ändern, auf den die Services zugegriffen werden.

> **Hinweis**: Ein Nachteil dieser Lösung besteht darin, dass der Port global geändert wird, sodass jede Schnittstelle von der Änderung betroffen ist.

Die entsprechende URL verwenden

In den im Problem Abschnitt bereitgestellten Konfigurationsdaten kann die externe Schnittstelle der ASA über HTTPS über die folgenden beiden URLs erreicht werden:

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

Wenn Sie jedoch versuchen, auf diese URLs zuzugreifen, während der WebVPN-Dienst aktiviert ist, leitet die ASA Sie zum WebVPN-Portal um:

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

Um auf ASDM zuzugreifen, können Sie die folgende URL verwenden:

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

> **Hinweis**: Wie in den Beispielkonfigurationsdaten gezeigt, wird für die Standard-Tunnelgruppe eine **group-url** definiert, die mit dem Befehl **group-url https://rtpvpnoutbound6.cisco.com/admin enable** definiert wird, der in Konflikt mit dem ASDM-Zugriff stehen sollte. Die URL *https://<ip-address/domain>/admin* ist für den ASDM-Zugriff reserviert. Wenn Sie sie in der Tunnelgruppe festlegen, hat dies keine Auswirkungen. Sie werden immer an *https://<ip-address/domain>/admin/public/index.html* weitergeleitet.

Ändern des Ports, an dem die einzelnen Dienstlisten aufgeführt sind

In diesem Abschnitt wird beschrieben, wie Sie den Port für ASDM- und WebVPN-Services ändern.

Globale Änderung des Ports für den HTTPS-Serverdienst

Gehen Sie wie folgt vor, um den Port für den ASDM-Service zu ändern:

1. Aktivieren Sie den HTTPS-Server, um auf einem anderen Port zuzuhören und die Konfiguration zu ändern, die sich auf den ASDM-Service auf der ASA bezieht, wie hier gezeigt:

   ```
   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.
   ```

   Hier ein Beispiel:

   ```
   ASA(config)#http server enable 65000
   ```
2. Nachdem Sie die Standard-Port-Konfiguration geändert haben, verwenden Sie dieses Format, um das ASDM über einen unterstützten Webbrowser im Netzwerk der Security Appliance zu starten:

   https://interface_ip_address:

   Hier ein Beispiel:

   https://192.168.1.1:65000

Globale Änderung des Ports für den WebVPN-Dienst

Gehen Sie wie folgt vor, um den Port für den WebVPN-Dienst zu ändern:

1. Lassen Sie zu, dass WebVPN auf einem anderen Port abhört, um die Konfiguration zu ändern, die sich auf den WebVPN-Dienst auf der ASA bezieht:

   Aktivieren Sie die WebVPN-Funktion auf der ASA:

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

   Aktivieren Sie den WebVPN-Service für die externe Schnittstelle der ASA:

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

   Lassen Sie zu, dass die ASA den WebVPN-Datenverkehr auf der benutzerdefinierten Portnummer überwacht:

   ```
   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.
```

Hier ein Beispiel:

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

2. Nachdem Sie die Standardport-Konfiguration geändert haben, öffnen Sie einen unterstützten Webbrowser, und verwenden Sie dieses Format, um eine Verbindung zum WebVPN-Server herzustellen:

https://interface_ip_address:

Hier ein Beispiel:

https://192.168.1.1:65010

Zugehörige Informationen

- Cisco Adaptive Security Device Manager - Support-Seite
- Cisco Firewalls der nächsten Generation der Serie ASA 5500-X
- Technischer Support und Dokumentation - Cisco Systems