ASA의 동일한 인터페이스에서 ASDM 및 WebVPN 활성화

목차

소개

이 문서에서는 Cisco 5500 Series ASA(Adaptive Security Appliance)의 동일한 인터페이스에서 Cisco ASDM(Adaptive Security Device Manager) 및 WebVPN 포털이 모두 활성화된 경우 Cisco ASDM(Adaptive Security Device Manager) 및 WebVPN 포털에 액세스하는 방법에 대해 설명합니다.

> **참고:** 이 문서는 WebVPN을 지원하지 않으므로 Cisco 500 Series PIX 방화벽에 적용할 수 없습니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- WebVPN 컨피그레이션 자세한 내용은 ASA 컨피그레이션의 클라이언트리스 SSL VPN(WebVPN) 예를 참조하십시오.
- ASDM을 시작하는 데 필요한 기본 컨피그레이션은 Cisco ASA Series ASDM 컨피그레이션 가이드 7.0의 ASDM 사용 섹션을 참조하십시오.

사용되는 구성 요소

이 문서의 정보는 Cisco 5500 Series ASA를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

문제

버전 8.0(2) 이전 버전의 ASA에서는 ASA의 동일한 인터페이스에서 ASDM과 WebVPN을 활성화할 수 없습니다. 둘 다 기본적으로 동일한 포트(443)에서 수신됩니다. 버전 8.0(2) 이상에서 ASA는 외부 인터페이스의 포트 443에서 동시에 클라이언트리스 SSL(Secure Sockets Layer) VPN(WebVPN) 세션과 ASDM 관리 세션을 모두 지원합니다. 그러나 두 서비스가 함께 활성화되면 ASA의 특정 인터페이스에 대한 기본 URL은 항상 WebVPN 서비스로 기본 설정됩니다. 예를 들어, 이 ASA 구성 데이터&colon을 고려하십시오.

```
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
```

솔루션

이 문제를 해결하려면 적절한 URL을 사용하여 해당 서비스에 액세스하거나 서비스가 액세스되는 포트를 변경할 수 있습니다.

> **참고:** 후자 솔루션의 한 가지 단점은 포트가 전체적으로 변경되므로 모든 인터페이스가 변경 사항에 영향을 받는다는 것입니다.

적절한 URL 사용

문제 섹션에 제공된 컨피그레이션 데이터의 예에서 ASA의 외부 인터페이스는 다음 두 URL을 통해 HTTPS를 통해 연결할 수 있습니다.

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

그러나 WebVPN 서비스가 활성화된 상태에서 이러한 URL에 액세스하려고 하면 ASA는 WebVPN 포털로 리디렉션합니다.

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

ASDM에 액세스하려면 다음 URL을 사용할 수 있습니다.

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

> **참고:** 예제 컨피그레이션 데이터에서 볼 수 있듯이 기본 터널 그룹에는 **group-url https://rtpvpnoutbound6.cisco.com/admin enable** 명령을 사용하여 정의된 **group-url**이 있으며 , 이는 ASDM 액세스와 충돌해야 합니다. 그러나 URL *https://<ip-address/domain>/admin은* ASDM 액세스를 위해 예약되어 있으며, 터널 그룹 아래에 설정하면 아무 영향도 없습니다. 항상 https://*<ip-address/domain>/admin/public/index.html으로 리디렉션됩니다*.

각 서비스가 수신 대기하는 포트 변경

이 섹션에서는 ASDM 및 WebVPN 서비스의 포트를 변경하는 방법에 대해 설명합니다.

HTTPS 서버 서비스의 포트 전역 변경

ASDM 서비스의 포트를 변경하려면 다음 단계를 완료하십시오.

1. 다음과 같이 ASA의 ASDM 서비스와 관련된 컨피그레이션을 변경하려면 HTTPS 서버가 다른 포트에서 수신하도록 설정합니다.

```
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.
```

   예를 들면 다음과 같습니다.

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

2. 기본 포트 컨피그레이션을 변경한 후 보안 어플라이언스 네트워크에서 지원되는 웹 브라우저에서 ASDM을 시작하려면 다음 형식을 사용합니다.

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

   예를 들면 다음과 같습니다.

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

WebVPN 서비스의 포트 전역 변경

WebVPN 서비스의 포트를 변경하려면 다음 단계를 완료하십시오.

1. ASA의 WebVPN 서비스와 관련된 컨피그레이션을 변경하기 위해 WebVPN이 다른 포트에서 수신 대기하도록 허용:

   ASA에서 WebVPN 기능을 활성화합니다.

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

   ASA의 외부 인터페이스에 대해 WebVPN 서비스를 활성화합니다.

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

   ASA가 사용자 지정된 포트 번호의 WebVPN 트래픽을 수신하도록 허용합니다.

```
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.
```

   예를 들면 다음과 같습니다.

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

2. 기본 포트 컨피그레이션을 변경한 후 지원되는 웹 브라우저를 열고 다음 형식을 사용하여 WebVPN 서버에 연결합니다.

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

예를 들면 다음과 같습니다.

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

관련 정보

- Cisco Adaptive Security Device Manager - 지원 페이지
- Cisco ASA 5500-X Series 차세대 방화벽
- 기술 지원 및 문서 – Cisco Systems