

ASDM e WebVPN ativadas na mesma interface do ASA

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Conventions](#)

[Problema](#)

[Solução](#)

[Use o URL apropriado](#)

[Altere a porta na qual cada serviço ouve](#)

[Alterar globalmente a porta do serviço de servidor HTTPS](#)

[Alterar globalmente a porta do serviço WebVPN](#)

[Informações Relacionadas](#)

Introduction

Este documento descreve como acessar o Cisco Adaptive Security Device Manager (ASDM) e o portal WebVPN quando ambos estão ativados na mesma interface do Cisco 5500 Series Adaptive Security Appliance (ASA).

Note: Este documento não se aplica ao Cisco 500 Series PIX Firewall, porque não oferece suporte a WebVPN.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração de WebVPN. Consulte o [Exemplo de Configuração de VPN SSL Sem Clientes \(WebVPN\) no ASA](#) para obter mais informações.
- Configuração básica necessária para iniciar o ASDM. Consulte a seção [Uso do ASDM](#) do [Guia de Configuração do ASDM da Cisco ASA Series, 7.0](#) para obter mais informações.

Componentes Utilizados

As informações neste documento são baseadas no Cisco 5500 Series ASA.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Consulte as [Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos](#).

Problema

Em versões do ASA anteriores à versão 8.0(2), o ASDM e o WebVPN não podem ser habilitados na mesma interface do ASA, pois ambos ouvem na mesma porta (443) por padrão. Nas versões 8.0(2) e posterior, o ASA oferece suporte a sessões VPN SSL (WebVPN) sem cliente e sessões administrativas ASDM simultaneamente na porta 443 da interface externa. No entanto, quando ambos os serviços são ativados juntos, o URL padrão para uma interface específica no ASA sempre assume como padrão o serviço WebVPN. Por exemplo, considere estes dados de configuração do 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
```

Solução

Para resolver esse problema, você pode usar o URL apropriado para acessar o respectivo serviço ou alterar a porta na qual os serviços são acessados.

Note: Uma desvantagem da última solução é que a porta é alterada globalmente, portanto, cada interface é afetada pela alteração.

Use o URL apropriado

No exemplo de dados de configuração fornecidos na seção [Problema](#), a interface externa do ASA pode ser acessada por HTTPS através destes dois URLs:

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

No entanto, se você tentar acessar esses URLs enquanto o serviço WebVPN estiver habilitado, o ASA o redirecionará para o portal WebVPN:

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

Para acessar o ASDM, você pode usar este URL:

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

Note: Como mostrado no exemplo de dados de configuração, o grupo de túnel padrão tem um **group-url** definido com o uso do comando **group-url https://rtpvpnoutbound6.cisco.com/admin enable**, que deve entrar em conflito com o acesso ASDM. No entanto, o URL *https://<ip-address/domain>/admin* é reservado para acesso ASDM e, se você o definir no grupo de túneis, não haverá efeito. Você sempre é redirecionado para *https://<ip-address/domain>/admin/public/index.html*.

Altere a porta na qual cada serviço ouve

Esta seção descreve como alterar a porta para os serviços ASDM e WebVPN.

Alterar globalmente a porta do serviço de servidor HTTPS

Conclua estes passos para alterar a porta do serviço ASDM:

1. Ative o servidor HTTPS para ouvir em uma porta diferente para alterar a configuração relacionada ao serviço ASDM no ASA, como mostrado aqui:

```
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.
```

Aqui está um exemplo:

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

2. Depois de alterar a configuração de porta padrão, use este formato para iniciar o ASDM a partir de um navegador da Web suportado na rede do Security Appliance:

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

Aqui está um exemplo:

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

Alterar globalmente a porta do serviço WebVPN

Conclua estes passos para alterar a porta do serviço WebVPN:

1. Permitir que a WebVPN ouça em uma porta diferente para alterar a configuração relacionada ao serviço WebVPN no ASA:

Ative o recurso WebVPN no ASA:

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

Ative o serviço WebVPN para a interface externa do ASA:

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

Permitir que o ASA ouça o tráfego WebVPN no número de porta personalizada:

```
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.
```

Aqui está um exemplo:

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

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

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

2. Depois de alterar a configuração de porta padrão, abra um navegador da Web suportado e use este formato para se conectar ao servidor WebVPN:

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

Aqui está um exemplo:

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

Informações Relacionadas

- [Cisco Adaptive Security Device Manager - Página de suporte](#)
- [Firewalls de próxima geração Cisco ASA 5500-X Series](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)