Configurar Porta Personalizada para RAVPN no FTD Gerenciado pelo FMC

Contents

Introdução

Este documento descreve o procedimento para configurar a Porta personalizada para SSL e IKEv2 AnyConnect no Firepower Threat Defense (FTD) gerenciado pelo FMC.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Entendimento básico de VPN de acesso remoto (RAVPN)
- Experiência com o Firepower Management Center (FMC)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- FTD da Cisco - 7,6
- FMC da Cisco - 7.6
- Windows 10

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurações

Alteração de porta SSL/DTLS para AnyConnect

1. Navegue até Devices > VPN > Remote Access e edite a política de acesso remoto existente.

2. Navegue até a seção Interfaces de Acesso e altere o Número da Porta de Acesso à Web e o Número da Porta DTLS em configurações de SSL para uma porta de sua escolha.

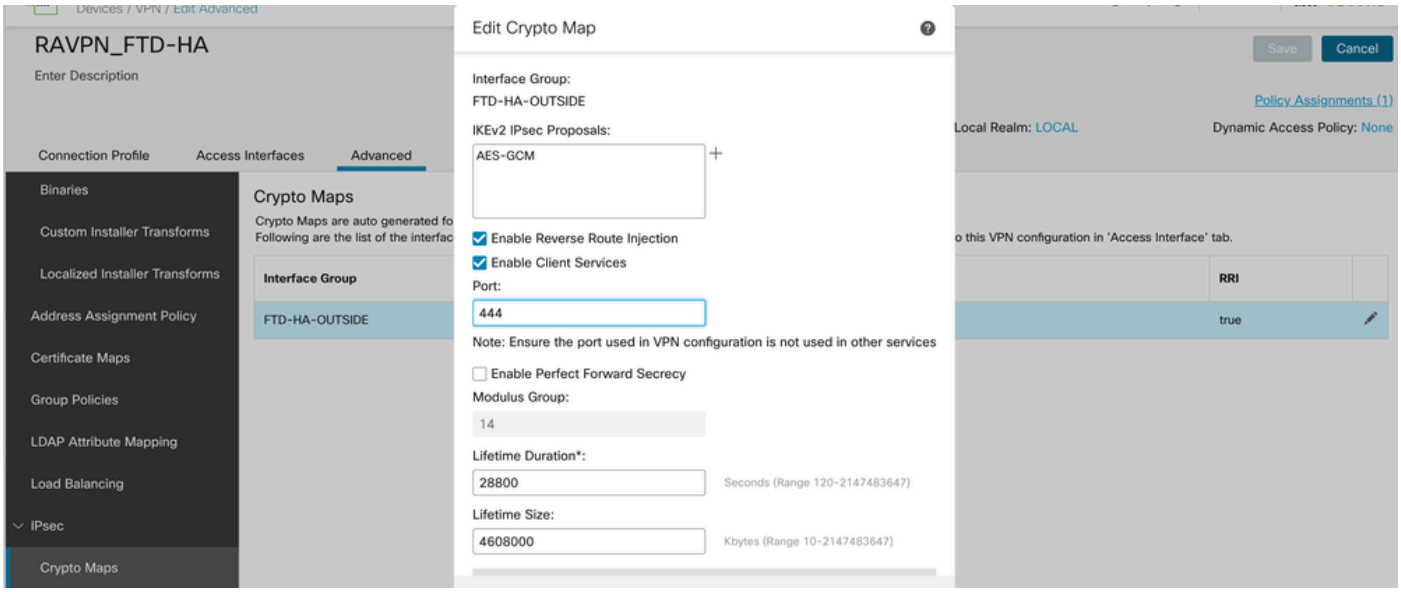
Alteração de portas SSL e DTLS para AnyConnect

3. Salve a configuração.

Alteração de porta IKEv2 para AnyConnect

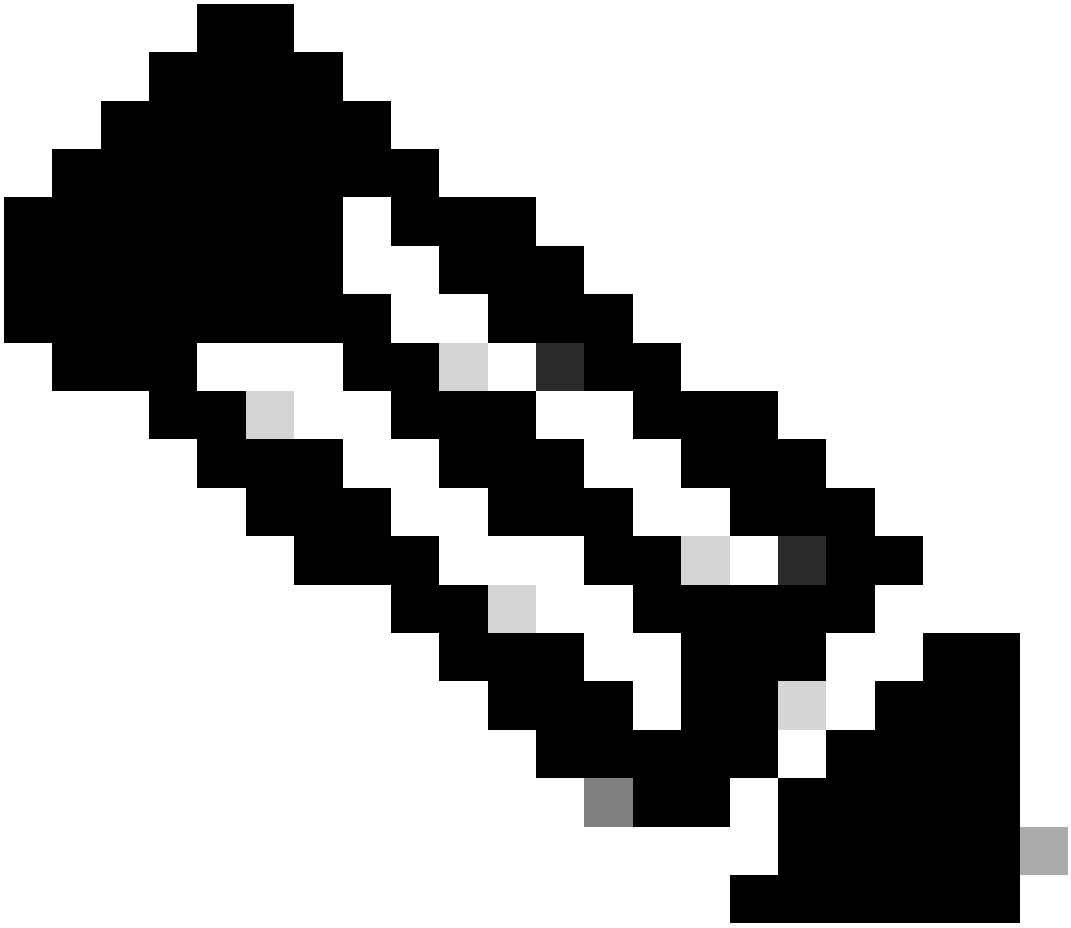
1. Navegue até Devices > VPN > Remote Access e edite a política de acesso remoto existente.

2. Navegue até a seção Advanced e navegue até IPsec > Crypto Maps. Edite a diretiva e altere a Porta para a porta desejada.



Alteração de porta IKEv2 para AnyConnect

3. Salvar a Configuração e Implantar.



Note: Ao usar a Porta personalizada junto com os Perfis do cliente AnyConnect, observe que o campo de endereço do host na lista de servidores deve ter X.X.X.X:porta (192.168.50.5:444) para a conectividade.

Verificar

1. Após a implantação, a configuração pode ser verificada com os comandos show run webvpn e show run crypto ikev2:

```
<#root>

>

show run webvpn

webvpn

port 444  <----- Custom Port that has been configured for SSL
```

```
enable outside
```

dtls port 444 <----- Custom Port that has been configured for DTLS

```
http-headers
  hsts-server
   enable
   max-age 31536000
   include-sub-domains
   no preload
  hsts-client
   enable
  x-content-type-options
  x-xss-protection
  content-security-policy
anyconnect image disk0:/csm/cisco-secure-client-win-X.X.X.X-webdeploy-k9.pkg 1 regex "Windows"
anyconnect enable
tunnel-group-list enable
cache
  disable
error-recovery disable
```

<#root>

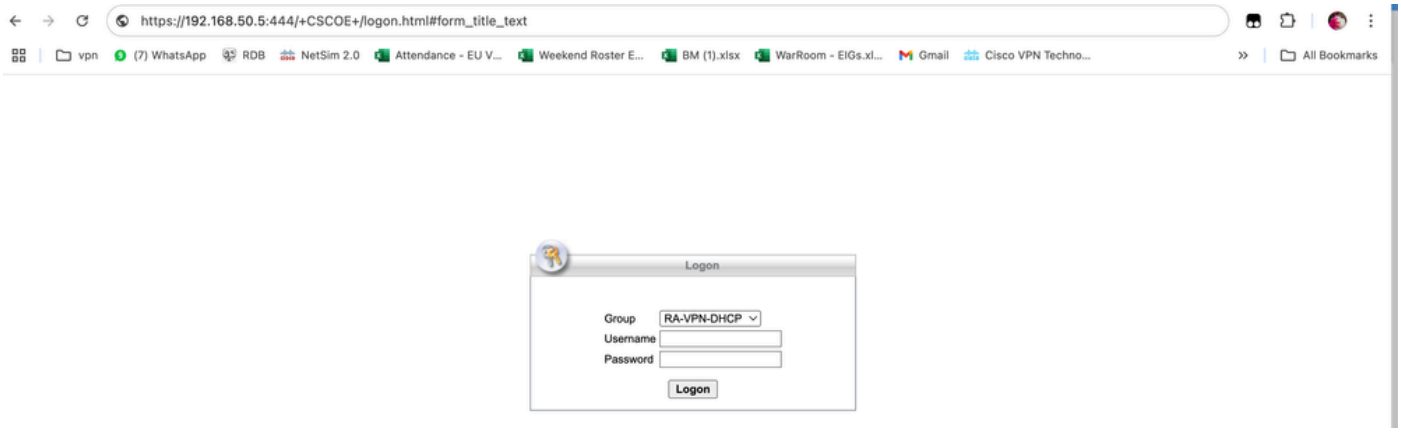
>

show run crypto ikev2

```
crypto ikev2 policy 10
 encryption aes-gcm-256 aes-gcm-192 aes-gcm
 integrity null
 group 21 20 19 16 15 14
 prf sha512 sha384 sha256 sha
 lifetime seconds 86400
```

crypto ikev2 enable outside client-services port 444 <----- Custom Port configured for IKEv2 Client Serv

2. Verifique acessando o Acesso Remoto a partir do navegador/Aplicativo AnyConnect com Porta Personalizada:



Verificar acessando o AnyConnect com porta personalizada

Troubleshooting

- Certifique-se de que a porta usada na configuração de Acesso Remoto não seja usada em outros serviços.
- Verifique se a porta não está bloqueada pelo ISP ou por qualquer dispositivo intermediário.
- As capturas no FTD podem ser feitas para verificar se os pacotes estão chegando ao firewall e se a resposta está sendo enviada ou não.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.