# Configuración del puerto personalizado para RAVPN en FTD administrado por FMC

## Contenido



## Introducción

Este documento describe el procedimiento para configurar el puerto personalizado para SSL e IKEv2 AnyConnect en Firepower Threat Defense (FTD) administrado por FMC.

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimientos básicos de VPN de acceso remoto (RAVPN)
- Experiencia con Firepower Management Center (FMC)

### Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- FTD de Cisco - 7,6
- Cisco FMC - 7,6
- Windows 10

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

# Configuraciones

## Cambio de puerto SSL/DTLS para AnyConnect

1. Navegue hasta Devices > VPN > Remote Access y edite la política de acceso remoto existente.

2. Vaya a la sección Interfaces de acceso y cambie el Número de puerto de acceso web y el Número de puerto DTLS en Configuración SSL y cambie el puerto que desee.

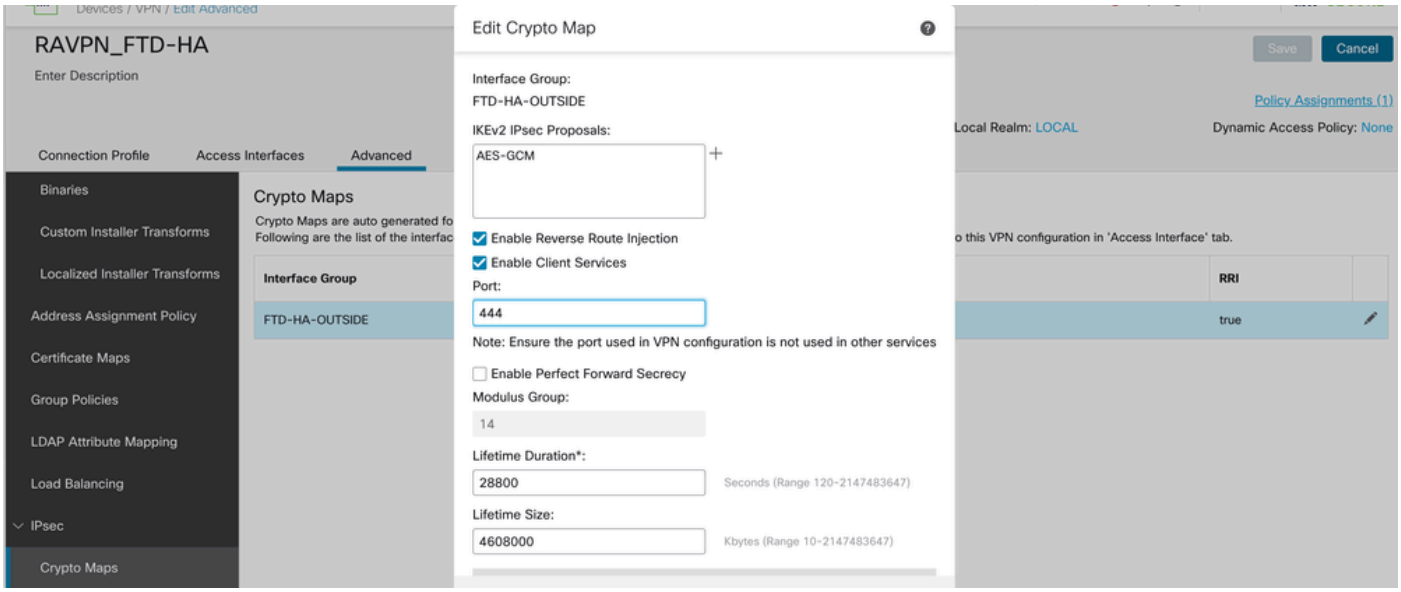

Cambio de puerto SSL y DTLS para AnyConnect

3. Guarde la configuración.

## Cambio de puerto IKEv2 para AnyConnect

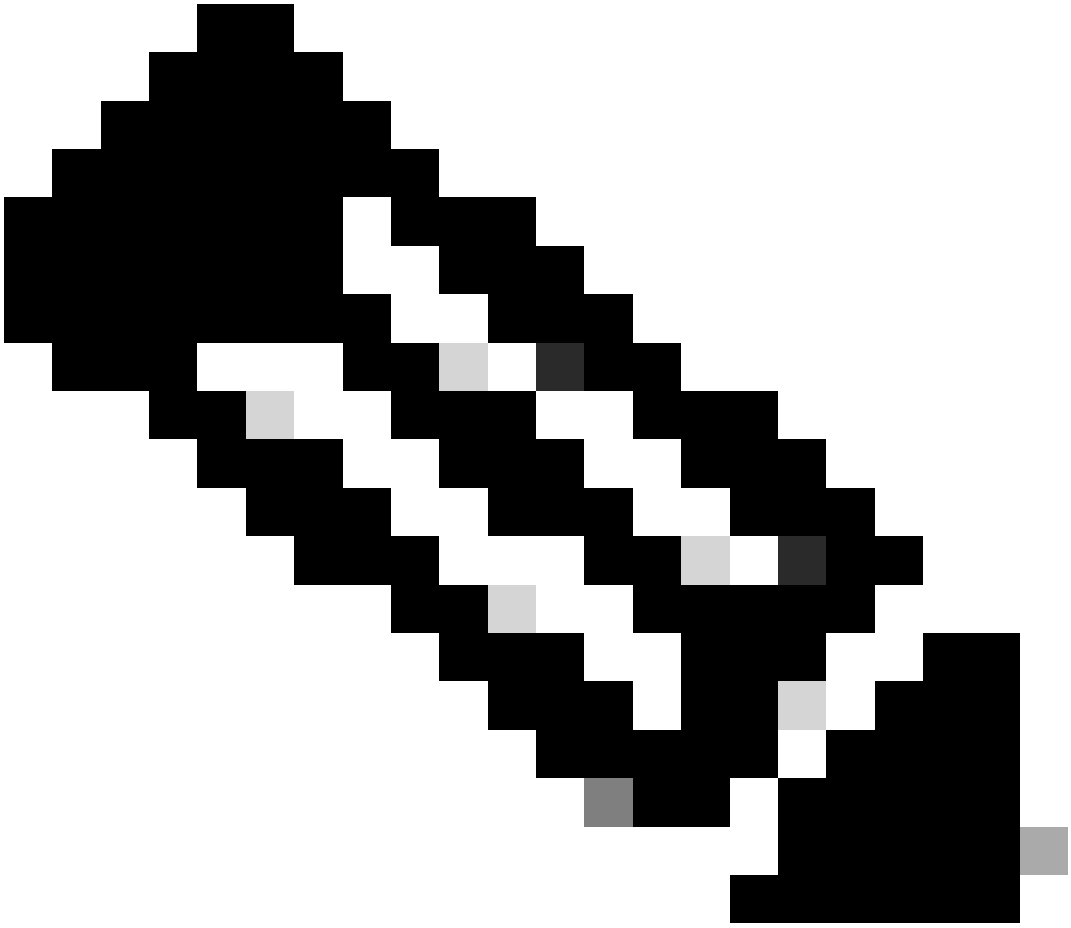
1. Navegue hasta Devices > VPN > Remote Access y edite la política de acceso remoto existente.

2. Navegue hasta la sección Avanzada y luego navegue hasta IPSec > Mapas criptográficos. Edite la política y cambie el puerto al puerto deseado.




Cambio de puerto IKEv2 para AnyConnect

3. Guarde la configuración e implemente.



Nota: Al utilizar el puerto personalizado junto con los perfiles de cliente de AnyConnect, tenga en cuenta que el campo de dirección de host de la lista de servidores debe tener X.X.X.X:port (192.168.50.5:444) para la conectividad.

## Verificación

1. Después de la implementación, la configuración se puede verificar con los comandos show run webvpn y 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>

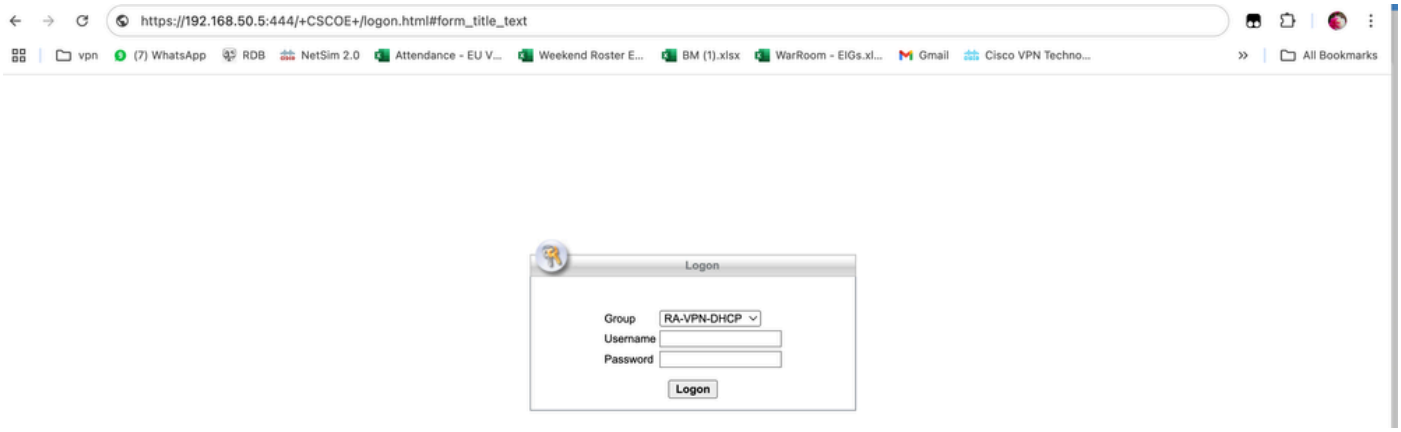
>

**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. Para verificarlo, acceda al acceso remoto desde el navegador o la aplicación AnyConnect con puerto personalizado:




Verificar accediendo a AnyConnect con puerto personalizado

# Troubleshoot

- Asegúrese de que el puerto utilizado en la configuración de acceso remoto no se utiliza en otros servicios.
- Asegúrese de que el puerto no esté bloqueado por el ISP ni por ningún dispositivo intermedio.
- Las capturas en FTD se pueden tomar para verificar si los paquetes están llegando al firewall y si la respuesta se está enviando o no.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).