为FTD上的RAVPN配置自定义端口，由FMC管理

目录

简介

本文档介绍在FMC管理的Firepower威胁防御(FTD)上为SSL和IKEv2 AnyConnect配置自定义端口的过程。

先决条件

要求

Cisco 建议您了解以下主题：

- 基本了解远程访问VPN(RAVPN)
- 具有Firepower管理中心(FMC)的经验

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科FTD - 7.6
- 思科FMC - 7.6
- Windows 10

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

AnyConnect的SSL/DTLS端口更改

1.导航到设备> VPN >远程访问，并编辑现有的远程访问策略。

2.导航到Access Interfaces部分，将SSL设置下的Web Access Port Number和DTLS Port Number更改为您选择的端口。

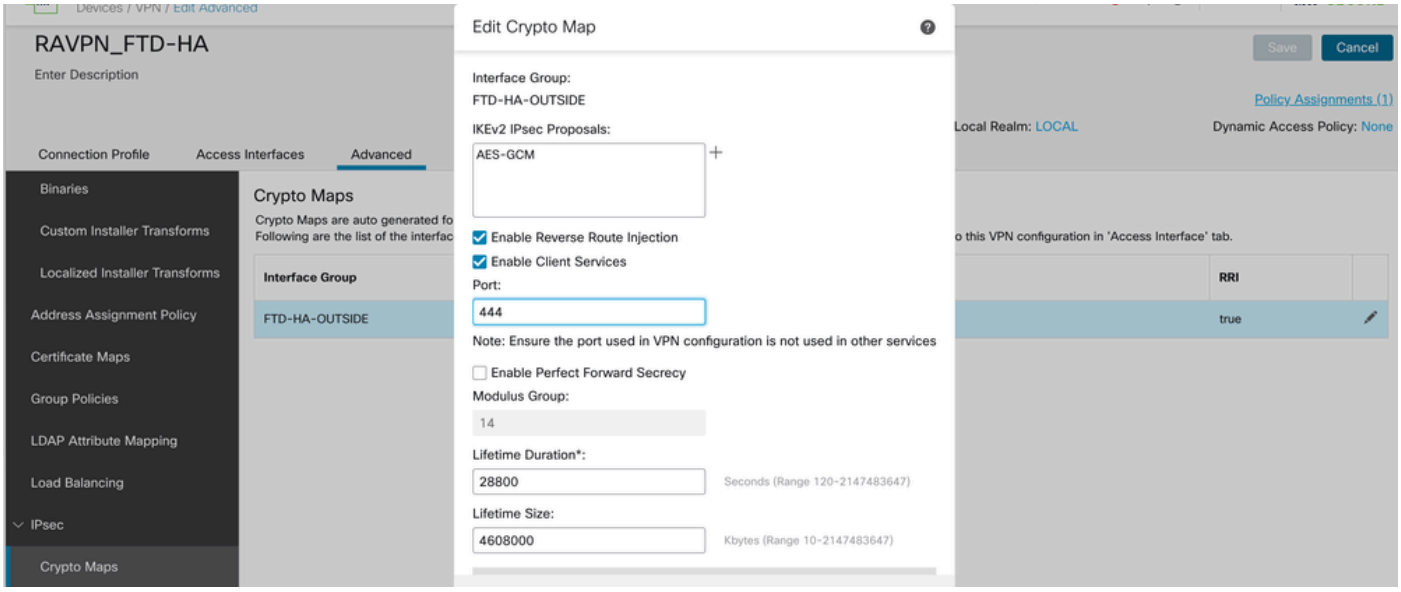
AnyConnect的SSL和DTLS端口更改

3.保存配置。

AnyConnect的IKEv2端口更改

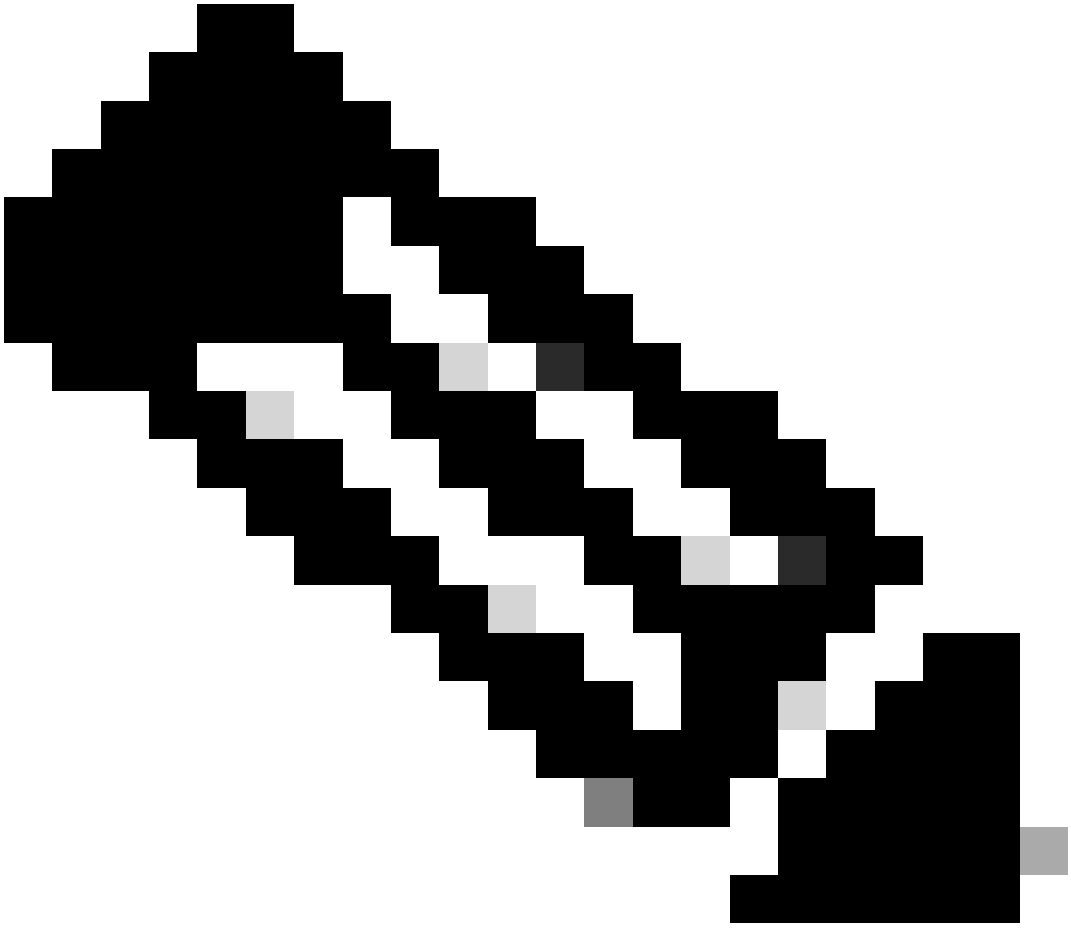
1.导航到设备> VPN >远程访问，并编辑现有的远程访问策略。

2.导航到高级部分，然后导航到IPsec >加密映射。编辑策略并将端口更改为所需的端口。



AnyConnect的IKEv2端口更改

3.保存配置并进行部署。



注意：将自定义端口与AnyConnect客户端配置文件一起使用时，请注意服务器列表中的主机地址字段必须具有X.X.X.X:port(192.168.50.5:444)才能进行连接。

验证

1.部署后，可使用show run webvpn和show run crypto ikev2命令验证配置：

```
<#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>

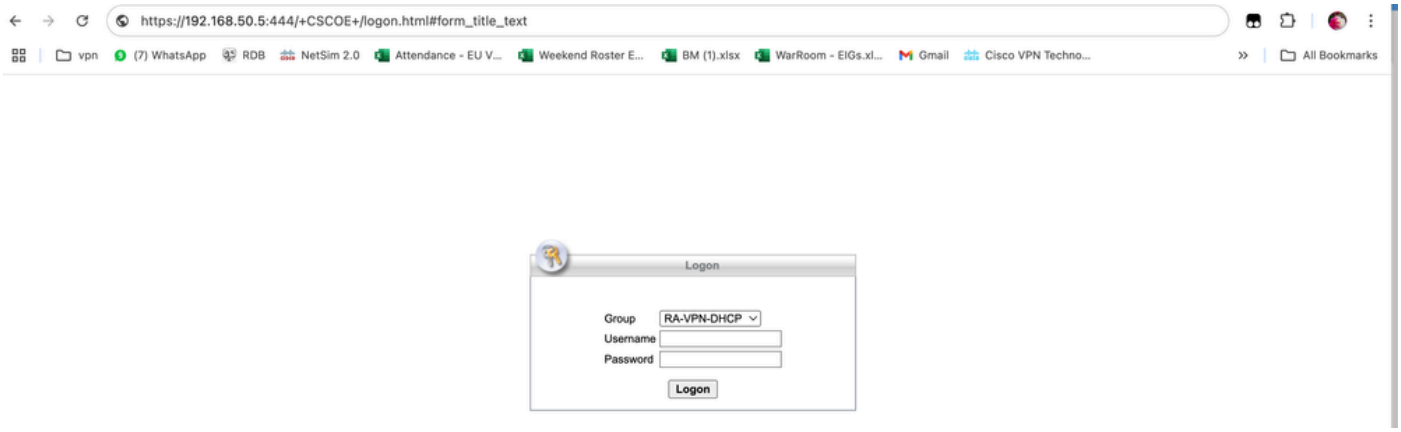
>

```
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.通过自定义端口从浏览器/AnyConnect应用访问远程访问进行验证：



通过自定义端口访问AnyConnect进行验证

故障排除

- 确保远程访问配置中使用的端口不在其他服务中使用。
- 确保ISP或任何中间设备未阻塞端口。
- FTD上的捕获可用于验证数据包是否到达防火墙以及是否发送了响应。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。