為FMC管理的FTD上的RAVPN配置自定義埠

目錄

簡介

本檔案介紹在FMC管理的Firepower威脅防禦(FTD)上為SSL和IKEv2 AnyConnect配置自定義埠的過程。

必要條件

需求

思科建議您瞭解以下主題：

- 對遠端訪問VPN(RAVPN)的基本瞭解
- 使用Firepower管理中心(FMC)的經驗

採用元件

本文中的資訊係根據以下軟體和硬體版本：

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

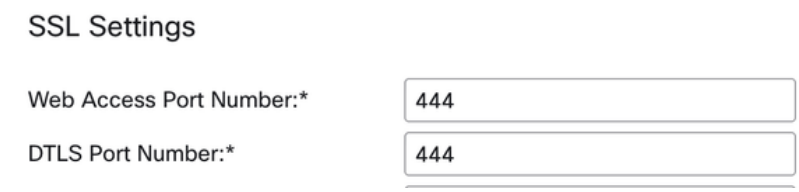
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

組態

AnyConnect的SSL/DTLS埠更改

1.導航到Devices > VPN > Remote Access，然後編輯現有遠端訪問策略。

2.定位至「訪問介面」部分，然後在SSL設定下將Web訪問埠號和DTLS埠號更改為您選擇的埠。



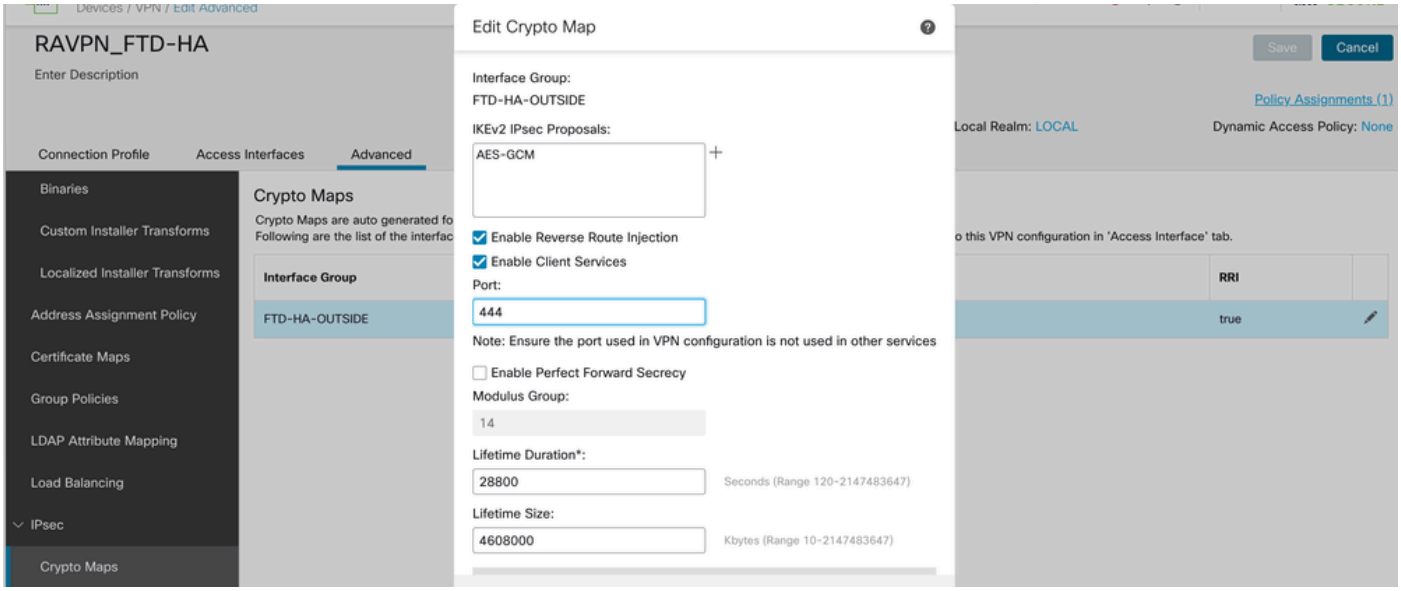
AnyConnect的SSL和DTLS埠更改

3. 儲存組態。

AnyConnect的IKEv2埠更改

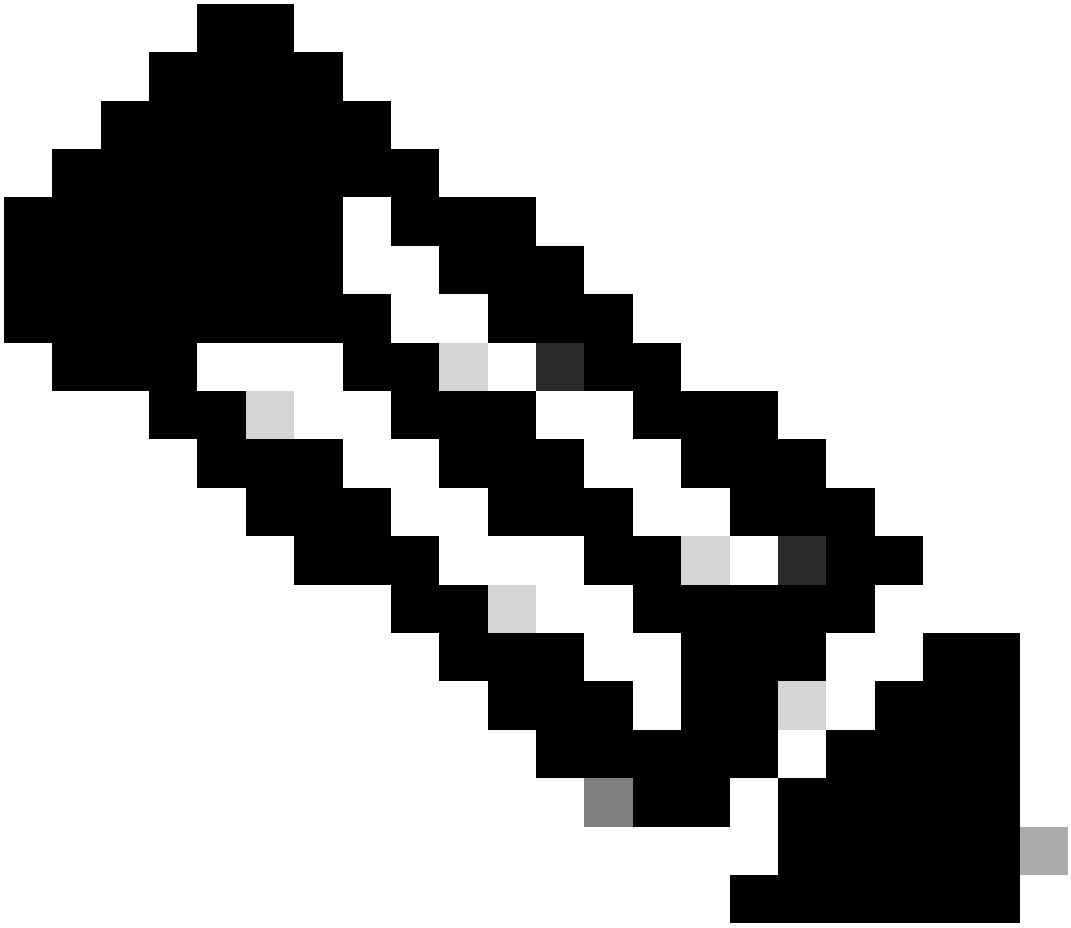
1.導航到Devices > VPN > Remote Access，然後編輯現有遠端訪問策略。

2.導航到Advanced部分，然後導航到IPsec > Crypto Maps。編輯策略並將埠更改為所需的埠。



AnyConnect的IKEv2埠更改

3. 儲存組態並進行部署。



附註：將自定義埠與AnyConnect客戶端配置檔案一起使用時，請注意伺服器清單中的主機地址欄位必須具有X.X.X.X:port(192.168.50.5:444)才能進行連線。

驗證

1.部署後，可以使用show run webvpn和show run crypto ikev2命令驗證配置：

```
<#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>

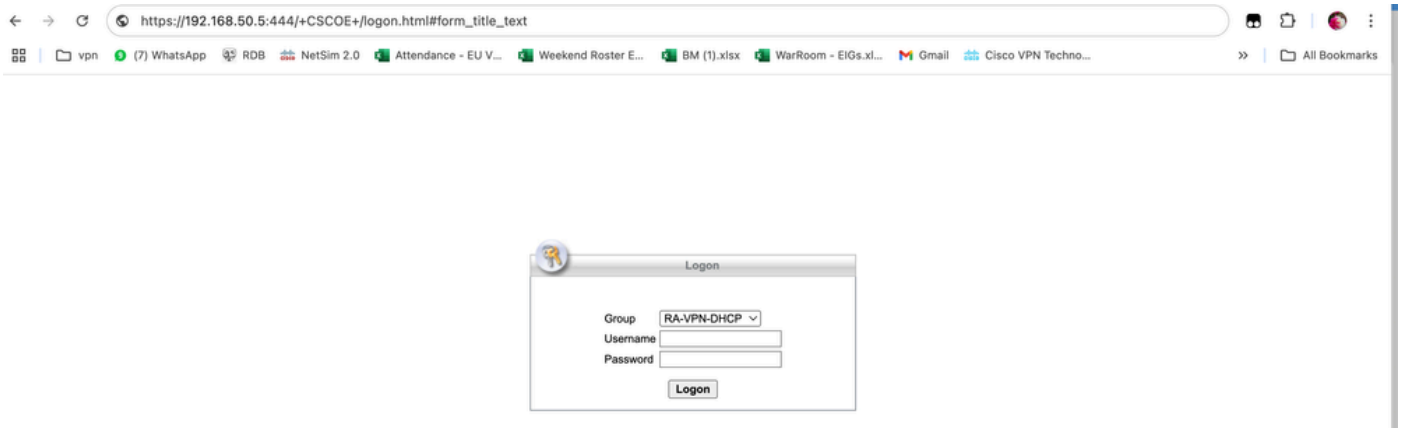
>

```
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.通過自定義埠從瀏覽器/AnyConnect應用程式訪問遠端訪問進行驗證：



通過自定義埠訪問AnyConnect進行驗證

疑難排解

- 請確保遠端訪問配置中使用的埠未在其他服務中使用。
- 確保ISP或任何中間裝置未阻塞埠。
- FTD上的擷取可用於驗證封包是否抵達防火牆以及是否傳送回應。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。