FMCによって管理されるFTDでのRAVPNのカスタムポートの設定

内容

はじめに

このドキュメントでは、FMCによって管理されるFirepower Threat Defense(FTD)でSSLおよびIKEv2 AnyConnect用のカスタムポートを設定する手順について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- リモートアクセスVPN(RAVPN)の基本的な知識
- Firepower Management Center(FMC)の使用経験

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco FTD - 7.6
- Cisco FMC:7.6
- Windows 10

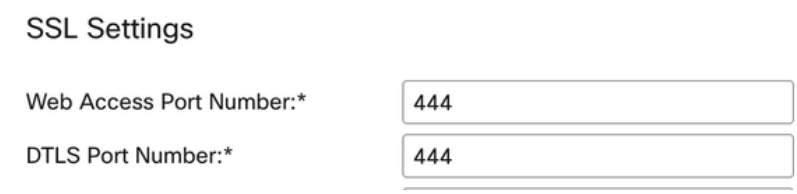
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

コンフィギュレーション

AnyConnectのSSL/DTLSポートの変更

1. Devices > VPN > Remote Accessの順に移動し、既存のリモートアクセスポリシーを編集します。

2. 「アクセスインターフェイス」セクションに移動し、SSL設定でWebアクセスポート番号とDTLSポート番号を任意のポートに変更します。



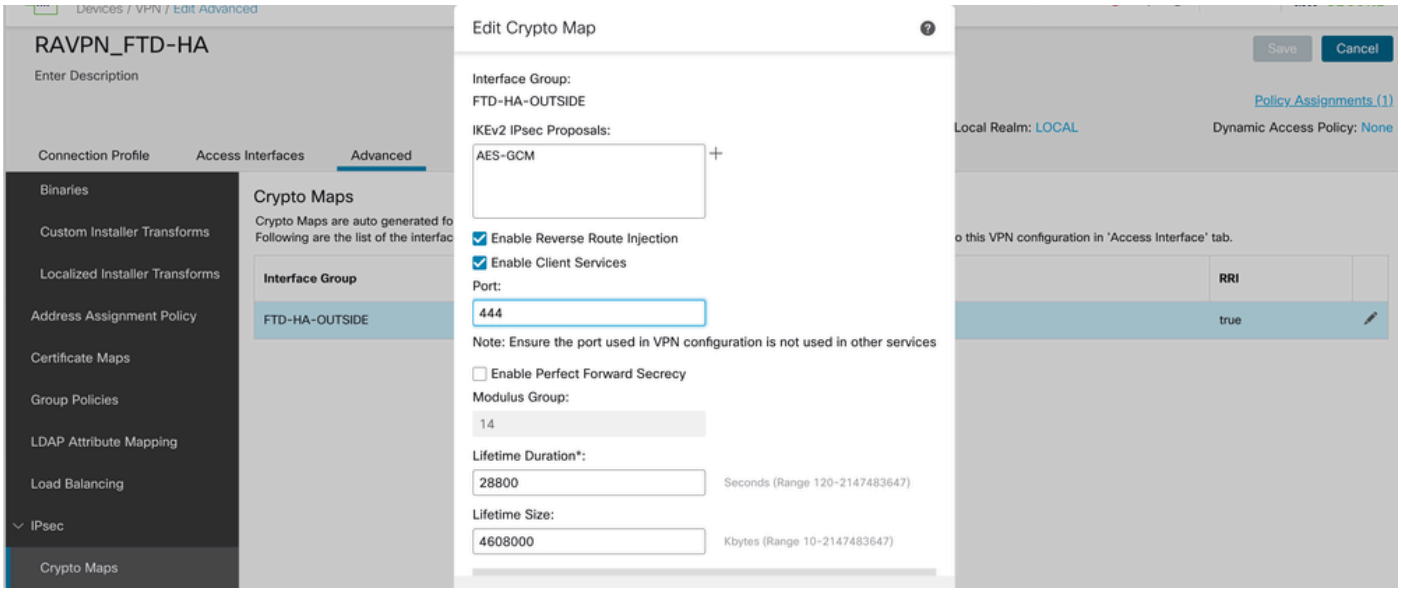
AnyConnectのSSLおよびDTLSポートの変更

3. 設定を保存します。

AnyConnectのIKEv2ポート変更

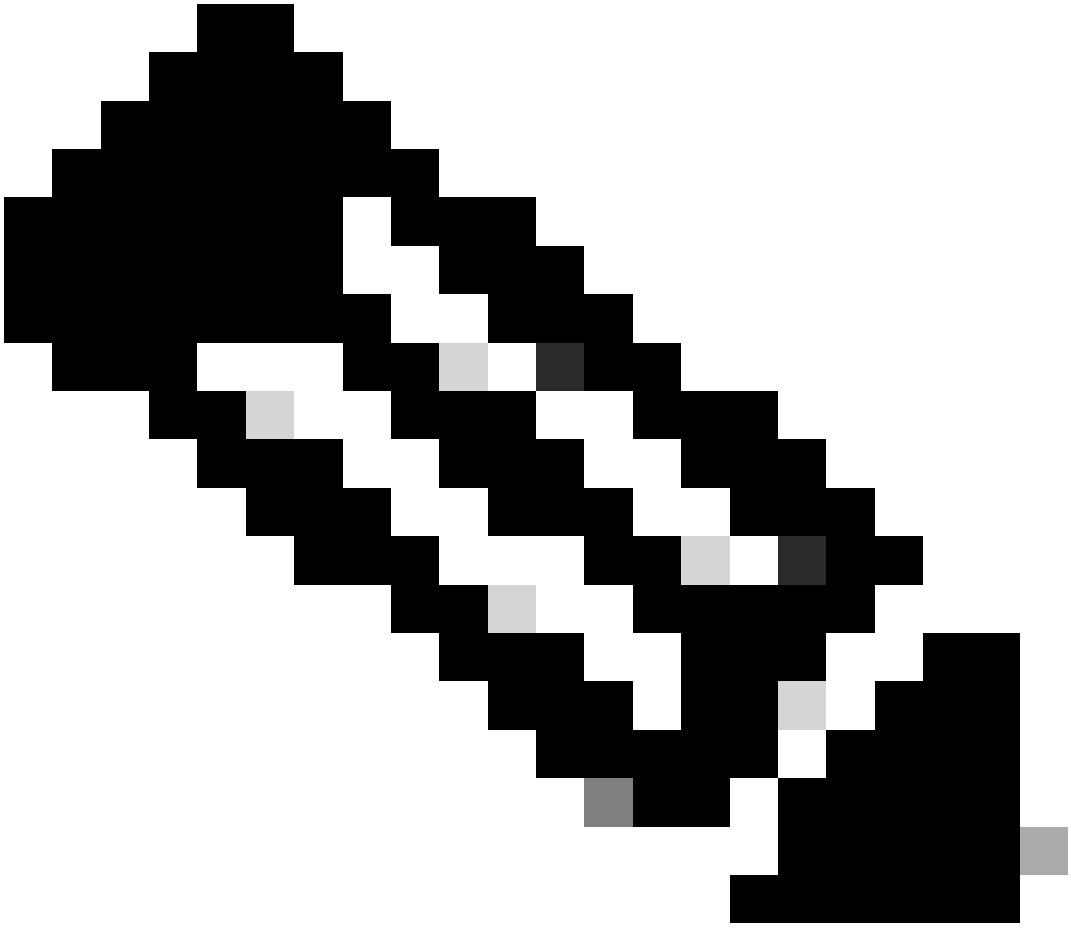
1. Devices > VPN > Remote Accessの順に移動し、既存のリモートアクセスポリシーを編集します。

2. Advancedセクションに移動し、次にIPSec > Crypto Mapsに移動します。ポリシーを編集し、ポートを目的のポートに変更します。



AnyConnectのIKEv2ポート変更

3. 設定を保存し、展開します。



注：AnyConnectクライアントプロファイルとともにカスタムポートを使用する場合、サーバリストのホストアドレスフィールドの接続は、X.X.X.X:port(192.168.50.5:444)である必要があります。

確認

1. 導入後、show run webvpnコマンドおよびshow run crypto ikev2コマンドを使用して設定を確認できます。

<#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>

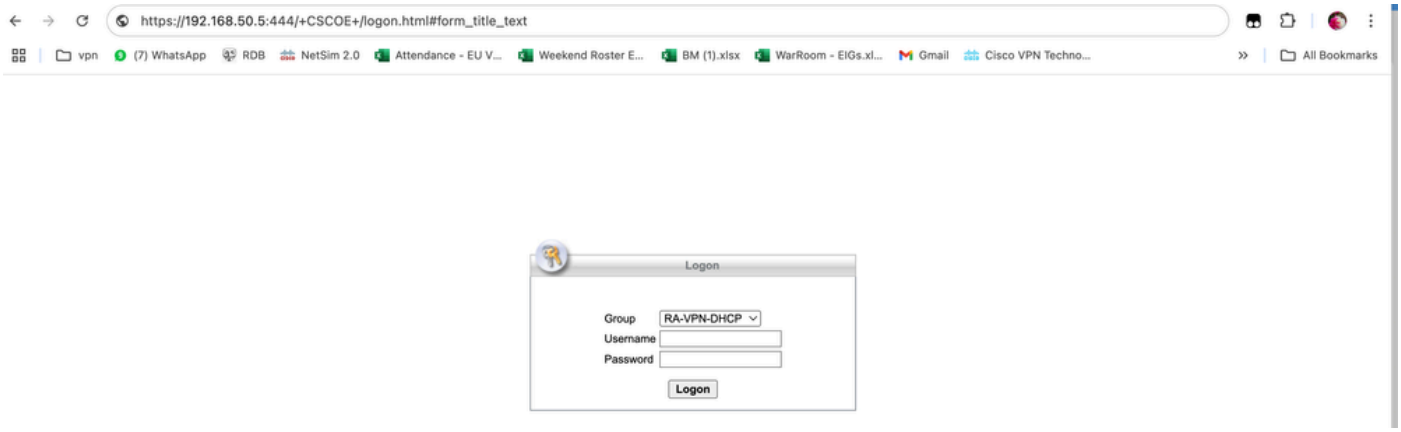
>

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. カスタムポートを使用して、ブラウザ/AnyConnectアプリケーションからリモートアクセスにアクセスして確認します。



カスタムポートを使用したAnyConnectへのアクセスによる検証

トラブルシュート

- リモートアクセス設定で使用されているポートが他のサービスで使用されていないことを確認します。
- ポートがISPまたは中継デバイスによってブロックされていないことを確認します。
- FTDのキャプチャを取得して、パケットがファイアウォールに到達していて、応答が送信されているかどうかを確認できます。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。