Configurer un port personnalisé pour RAVPN sur FTD géré par FMC

Table des matières

Introduction

Ce document décrit la procédure pour configurer le port personnalisé pour SSL et IKEv2 AnyConnect sur Firepower Threat Defense (FTD) géré par FMC.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Compréhension de base du VPN d'accès à distance (RAVPN)
- Expérience avec Firepower Management Center (FMC)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

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

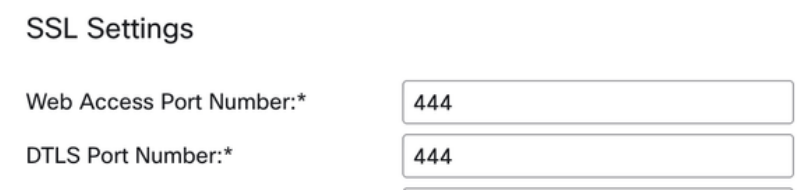
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Configurations

Changement de port SSL/DTLS pour AnyConnect

1. Accédez à Devices > VPN > Remote Access et modifiez la stratégie d'accès à distance existante.

2. Accédez à la section Interfaces d'accès et changez le numéro de port d'accès Web et le numéro de port DTLS sous les paramètres SSL pour un port de votre choix.



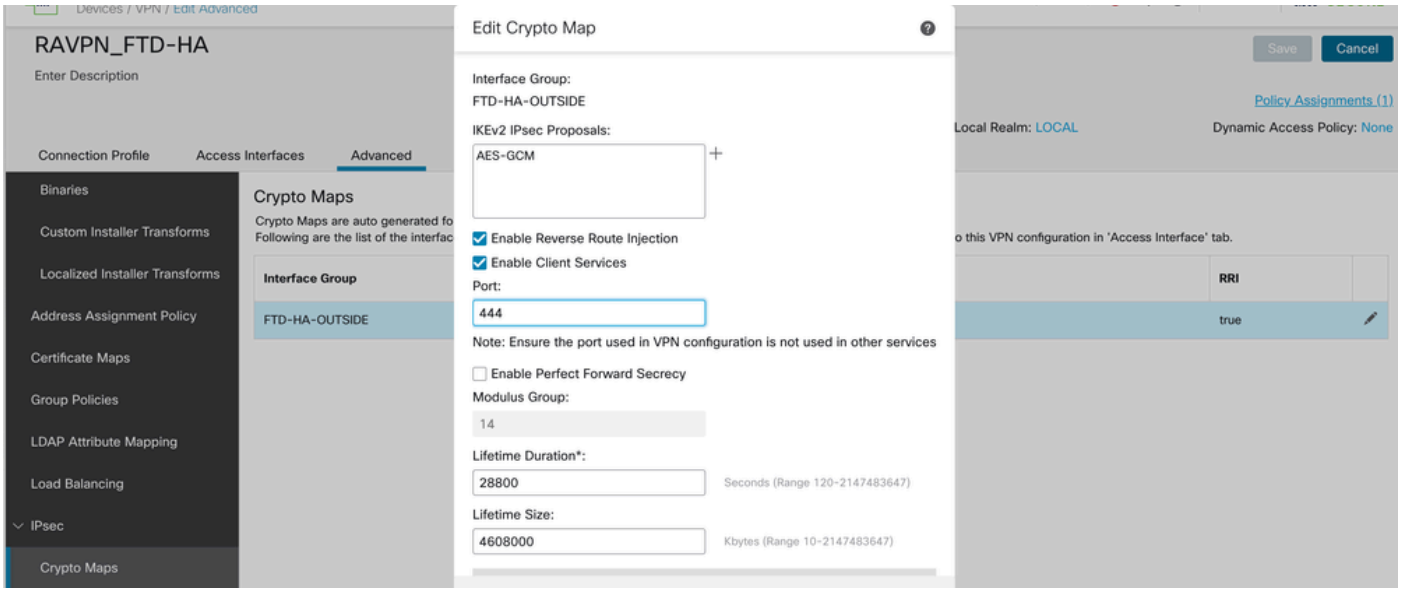
Changement de port SSL et DTLS pour AnyConnect

3. Enregistrez la configuration.

Changement de port IKEv2 pour AnyConnect

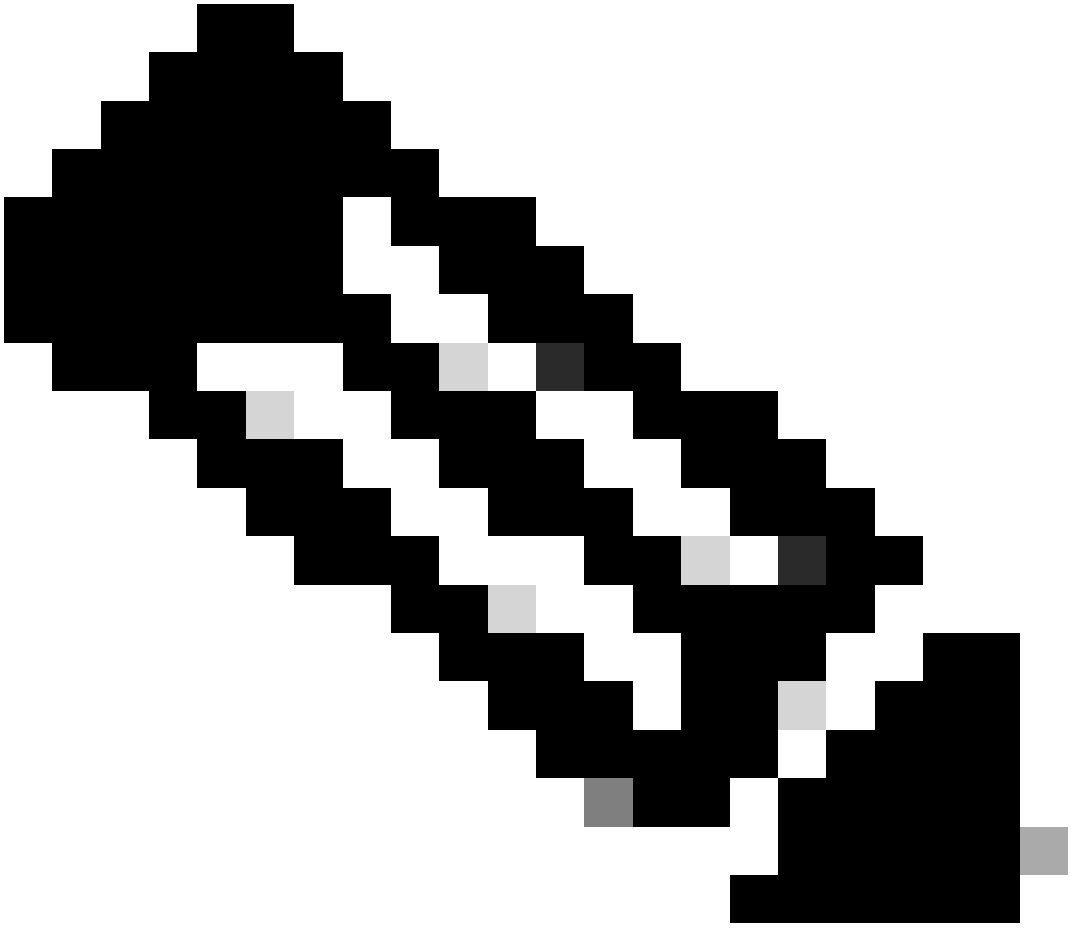
1. Accédez à Devices > VPN > Remote Access et modifiez la stratégie d'accès à distance existante.

2. Accédez à la section Advanced, puis à IPsec > Crypto Maps. Modifiez la stratégie et remplacez le port par le port souhaité.



Changement de port IKEv2 pour AnyConnect

3. Enregistrez la configuration et déployez.



Remarque : Lorsque vous utilisez un port personnalisé avec des profils client AnyConnect, notez que le champ d'adresse d'hôte dans la liste des serveurs doit avoir X.X.X.X : port (192.168.50.5:444) pour la connectivité.

Vérifier

1. Après le déploiement, la configuration peut être vérifiée avec les commandes show run webvpn et 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>

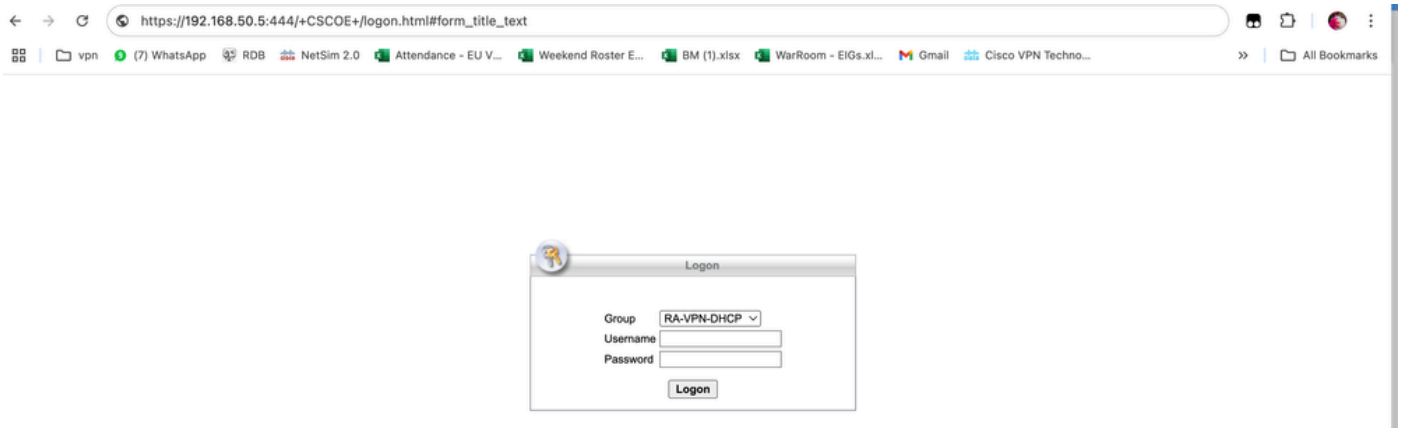
>

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. Vérifiez en accédant à l'accès à distance à partir du navigateur/de l'application AnyConnect avec un port personnalisé :



Vérifiez en accédant à AnyConnect avec un port personnalisé

Dépannage

- Assurez-vous que le port utilisé dans la configuration de l'accès à distance n'est pas utilisé dans d'autres services.
- Assurez-vous que le port n'est pas bloqué par le FAI ou tout périphérique intermédiaire.
- Les captures sur FTD peuvent être effectuées pour vérifier si les paquets atteignent le pare-feu et si la réponse est envoyée ou non.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.