Aangepaste poort voor RAVPN configureren op FTD beheerd door FMC

Inhoud

Inleiding

In dit document wordt de procedure beschreven om Aangepaste poort voor SSL en IKEv2 AnyConnect op Firepower Threat Defence (FTD) te configureren die wordt beheerd door FMC.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis van Remote Access VPN (RAVPN)
- Ervaring met Firepower Management Center (FMC)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

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

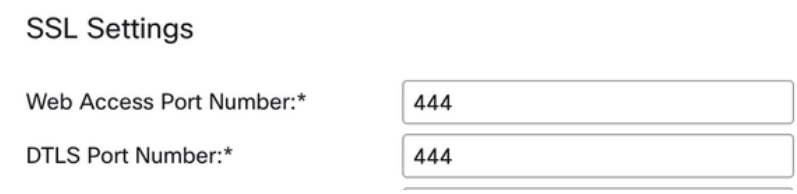
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configuraties

SSL/DTLS-poortwijziging voor AnyConnect

1. Navigeer naar Apparaten > VPN > Externe toegang en bewerk het bestaande beleid voor externe toegang.

2. Navigeer naar het gedeelte Access Interfaces en verander het webtoegangspoortnummer en het DTLS-poortnummer onder SSL-instellingen naar een poort naar keuze.



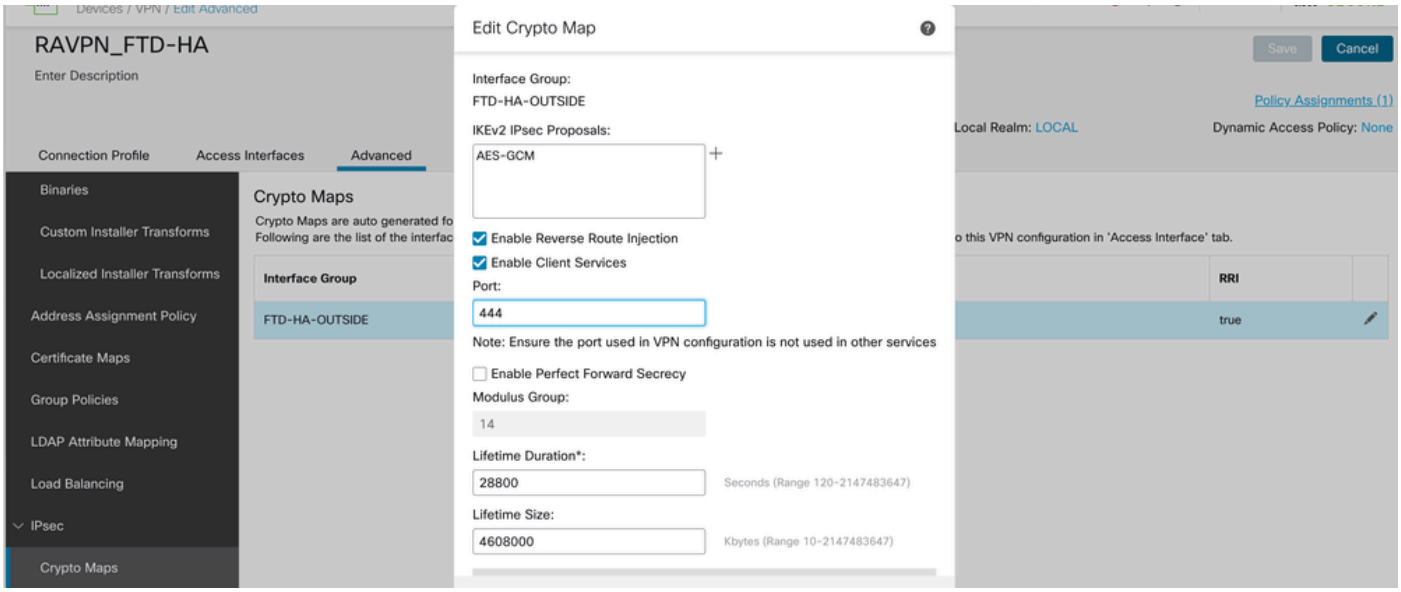
SSL- en DTLS-poortwijziging voor AnyConnect

3. Sla de configuratie op.

IKEv2-poortwijziging voor AnyConnect

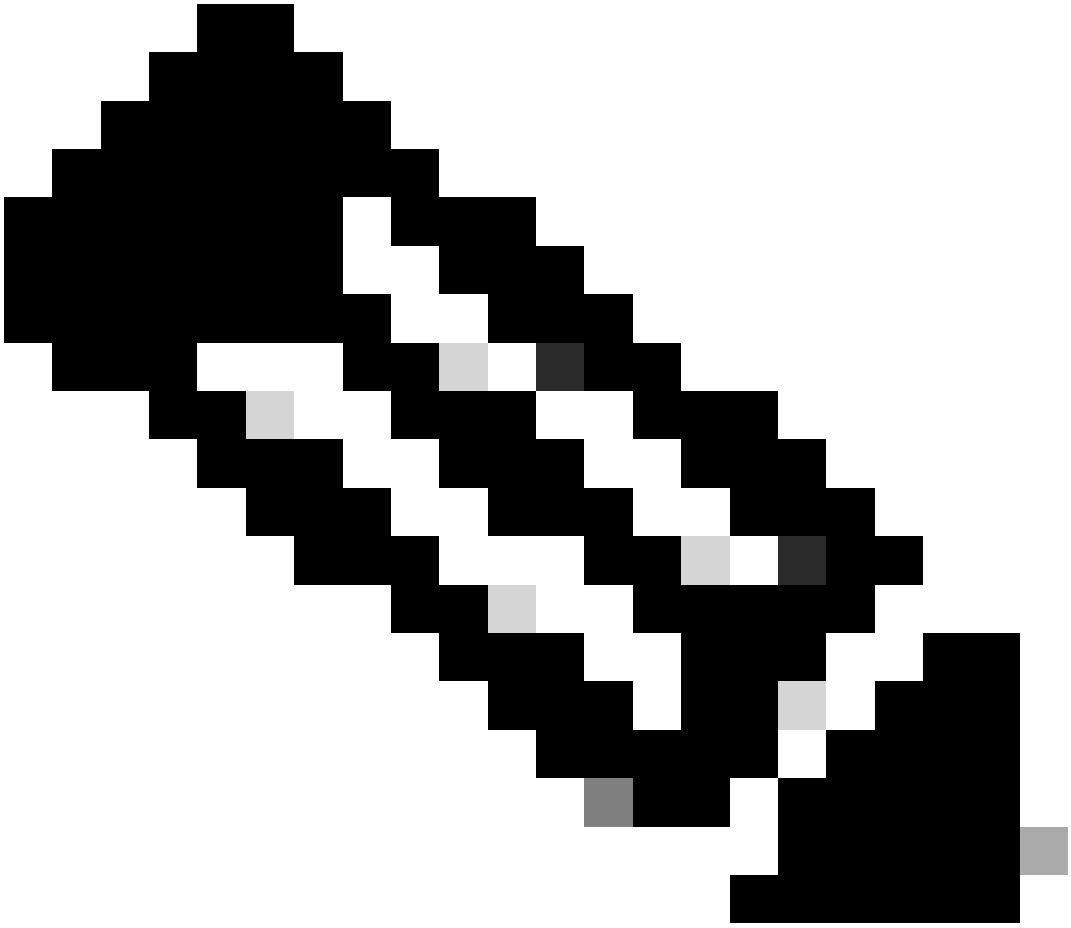
1. Navigeer naar Apparaten > VPN > Externe toegang en bewerk het bestaande beleid voor externe toegang.

2. Ga naar de sectie Advanced en navigeer vervolgens naar IPsec > Crypto Maps. Bewerk het beleid en verander de poort naar de gewenste poort.



IKEv2-poortwijziging voor AnyConnect

3. Sla de configuratie en de implementatie op.



Opmerking: Wanneer u Custom Port gebruikt samen met AnyConnect-clientprofielen, moet u er rekening mee houden dat het veld voor het hostadres in de serverlijst X.X.X.X:poort (192.168.50.5:444) moet hebben voor de connectiviteit.

Verifiëren

1. Na de implementatie kan de configuratie worden geverifieerd met de show run webvpn en toon run crypto ikev2 commando's:

```
<#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>

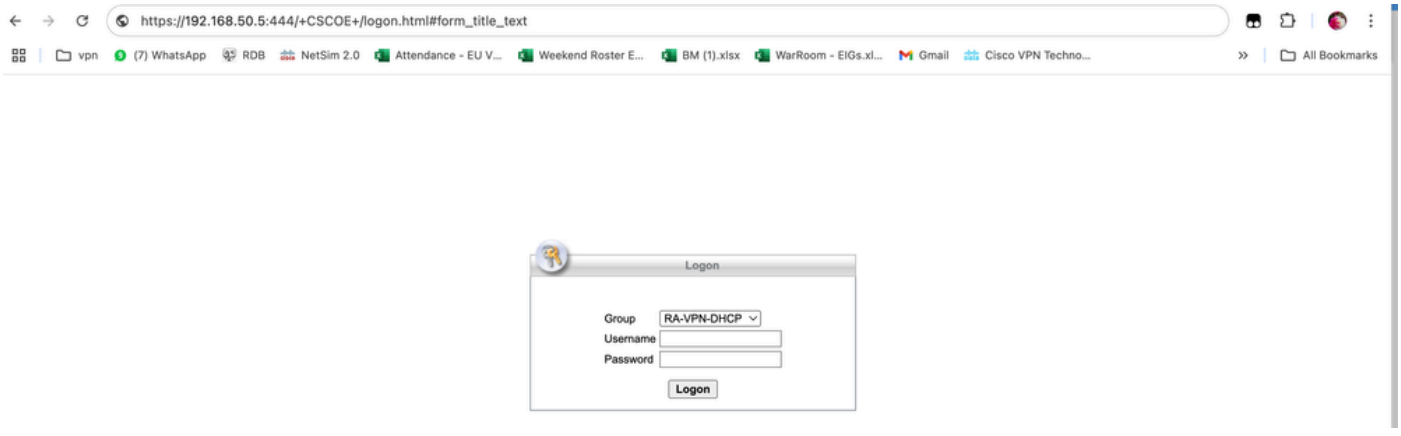
>

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. Controleer door toegang te krijgen tot Remote Access vanuit de browser/AnyConnect-toepassing met aangepaste poort:



Verifiëren door AnyConnect met aangepaste poort te gebruiken

Problemen oplossen

- Zorg ervoor dat de poort die wordt gebruikt in de configuratie van de externe toegang niet wordt gebruikt in andere services.
- Zorg ervoor dat de poort niet wordt geblokkeerd door een ISP of een Intermediate-apparaat.
- Captures op FTD kunnen worden uitgevoerd om te verifiëren of pakketten de firewall bereiken en of er respons wordt verstuurd of niet.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.