Configureer AnyConnect Dynamic Split Tunnel op FTD die door FMC wordt beheerd

Inhoud

Inleiding

In dit document wordt beschreven hoe u AnyConnect Dynamic Split Tunnel kunt configureren bij Firepower Threat Defence (FTD), beheerd door Firepower Management Center (FMC).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco AnyConnect
- Basiskennis van het VCC

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende softwareversies:

- FMC versie 7.0
- FTD versie 7.0

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.

Achtergrondinformatie

AnyConnect Dynamic Split Tunnel configuratie op FTD beheerd door FMC is volledig beschikbaar op FMC versie 7.0 en nieuwer. Als u een oudere versie uitvoert, moet u deze via FlexConfig configureren zoals beschreven in de geavanceerde AnyConnect VPN-implementaties voor Firepower Threat Defence met FMC.

Met Dynamic Split Tunnel configuratie, kunt u gesplitste tunnelconfiguratie verfijnen op basis van DNS domeinnamen. Omdat de IP-adressen die gekoppeld zijn aan FQDN-domeinnamen (full-qualified domain) kunnen worden gewijzigd, biedt de gesplitste tunnelconfiguratie op basis van DNS-namen een dynamischer definitie van het verkeer dat al dan niet is opgenomen in de VPN-tunnel (Virtual Private Network) voor externe toegang. Als er adressen worden teruggegeven voor uitgesloten domeinnamen binnen de adrespool die in de VPN is opgenomen, worden die adressen dan uitgesloten. Uitgesloten domeinen worden niet geblokkeerd. In plaats daarvan wordt het verkeer naar die domeinen buiten de VPN-tunnel gehouden.

Merk op dat u ook Dynamic Split Tunnel kunt configureren om domeinen te definiëren die in de tunnel moeten worden opgenomen en die anders op basis van IP-adres zouden worden uitgesloten.

Beperkingen

Op dit moment worden deze functies nog niet ondersteund:

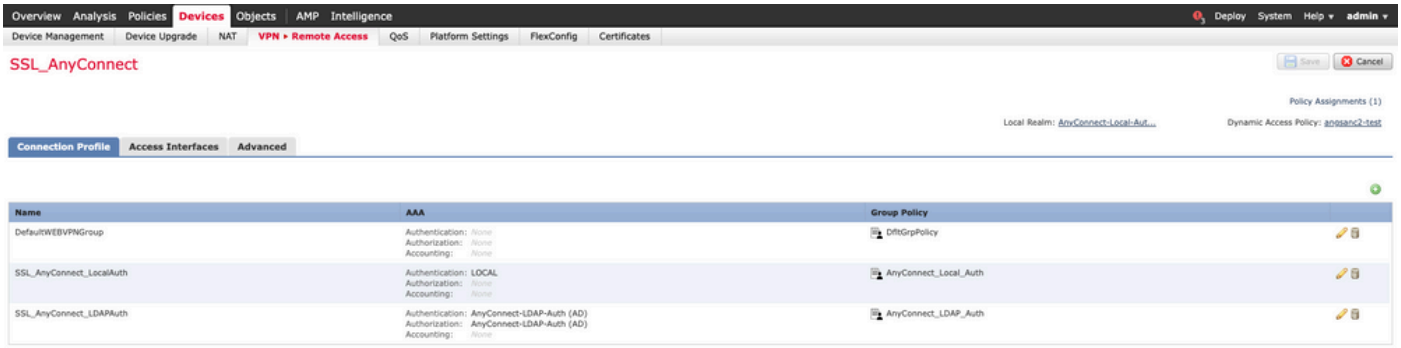
- Dynamic Split Tunnel wordt niet ondersteund op iOS (Apple)-apparaten. Zie Cisco bug-id CSCvr54798
- Dynamic Split Tunnel wordt niet ondersteund op AnyConnect Linux-clients. Zie Cisco-bug IDCSCvt64988

Configureren

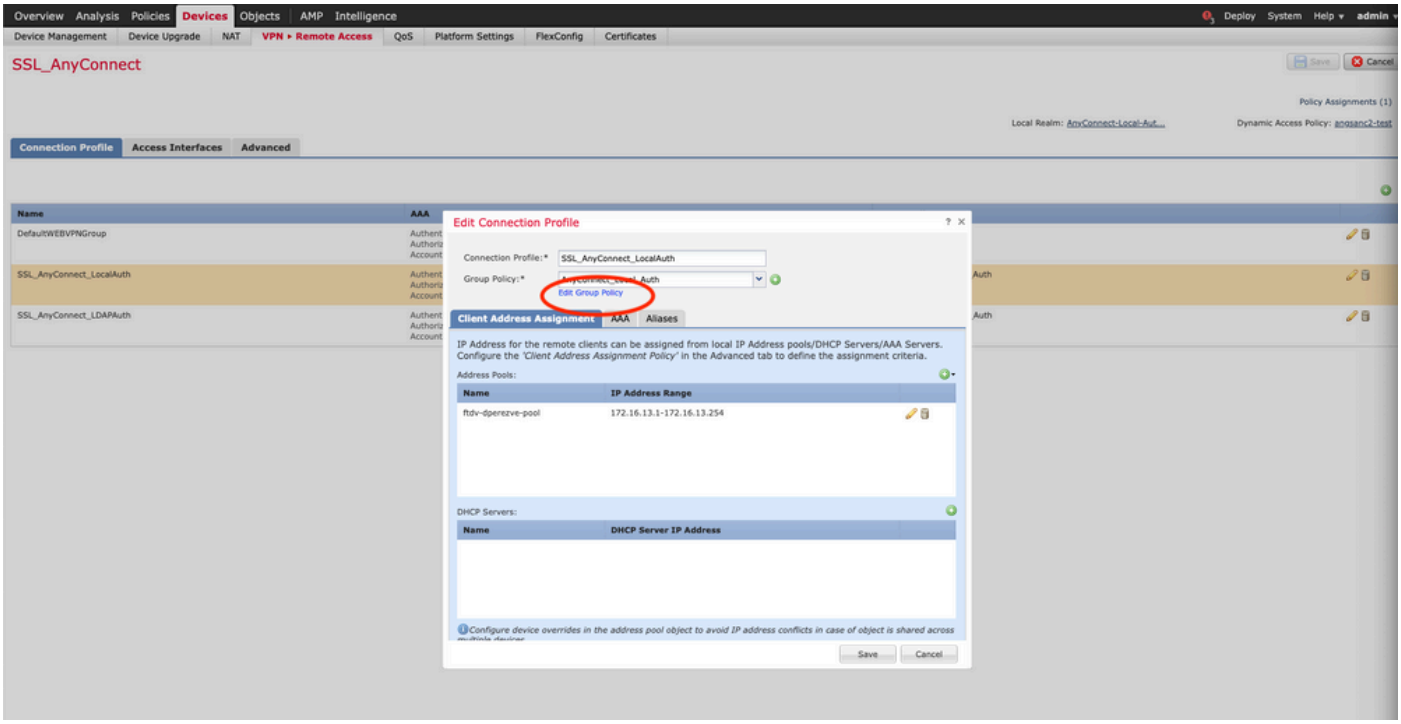
In dit deel wordt beschreven hoe u AnyConnect Dynamic Split Tunnel kunt configureren op een FTD die wordt beheerd door FMC.

Stap 1. Het groepsbeleid bewerken voor gebruik van de dynamische splitstunnel

1. Navigeer in het VCC naar **Apparaten > VPN > Externe toegang** en selecteer vervolgens het **verbindingsprofiel** waarop u de configuratie wilt toepassen.

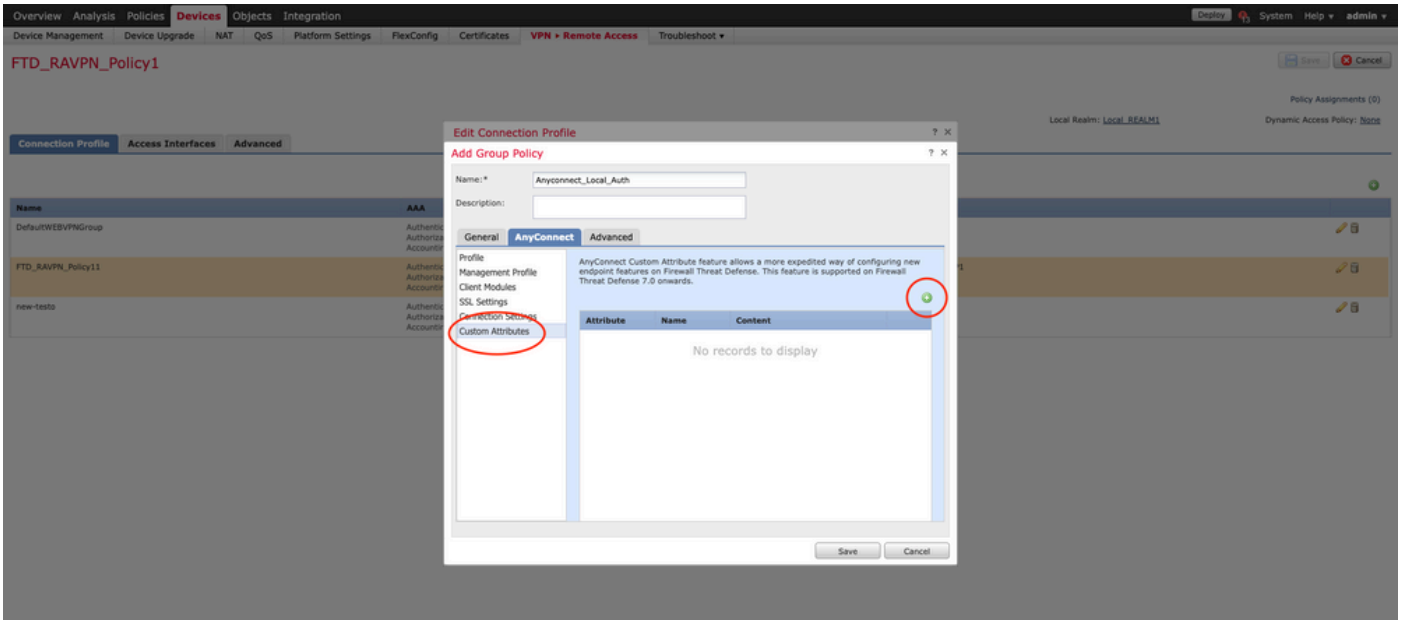


2. Selecteer **Groepsbeleid bewerken** om een van de groepsbeleid te wijzigen dat al is gemaakt.

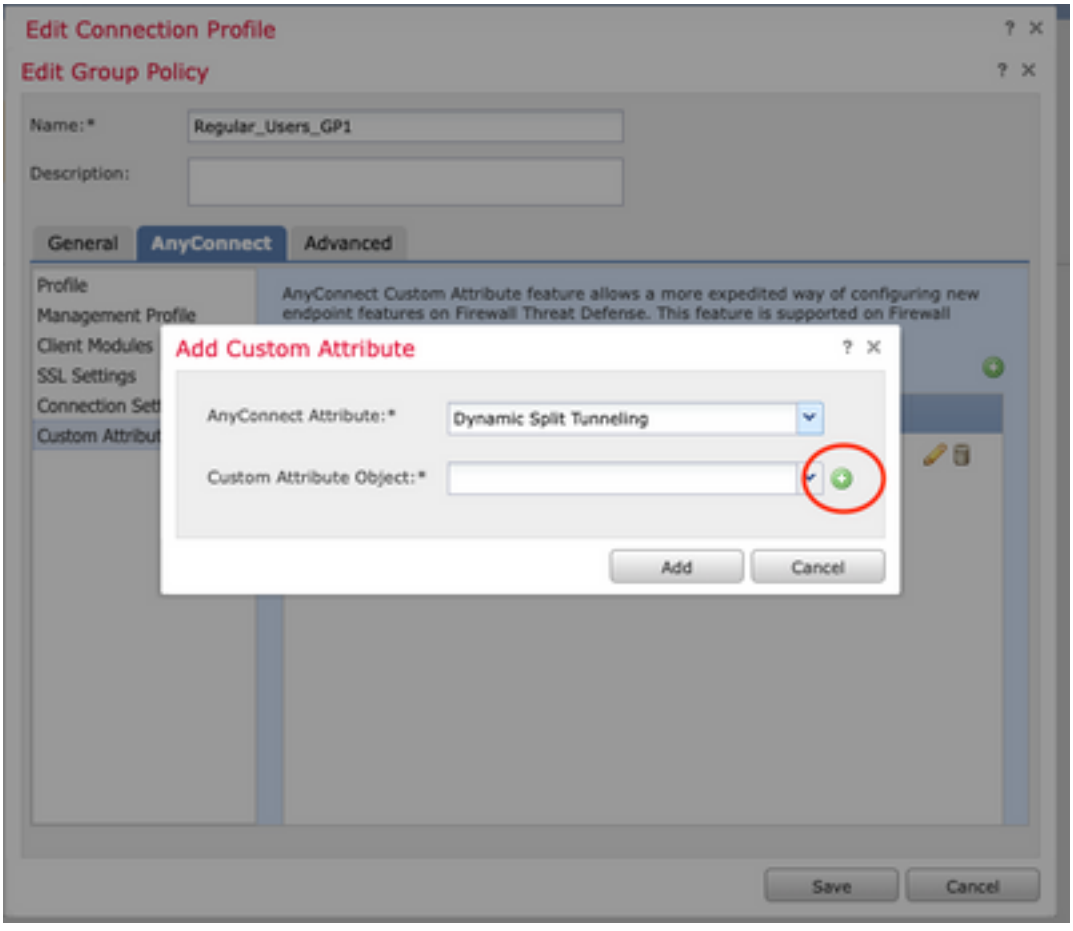


Stap 2. De aangepaste AnyConnect-kenmerken configureren

1. Ga onder de configuratie Groepsbeleid naar **AnyConnect > Aangepaste kenmerken** en klik op de knop **Toevoegen (+)**:

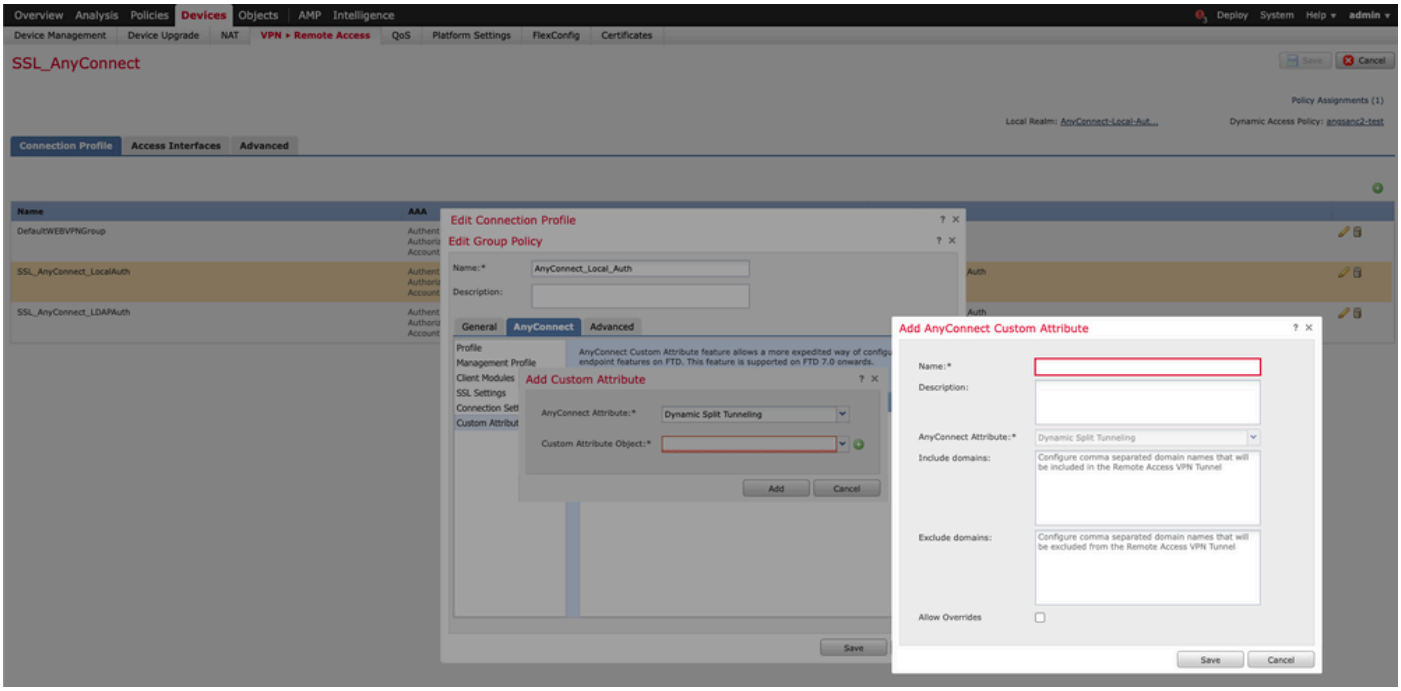


2. Selecteer de **Dynamic Split Tunneling** AnyConnect Attribute en klik op de knop **Add (+)** om een nieuw aangepast Attribute-object te maken:

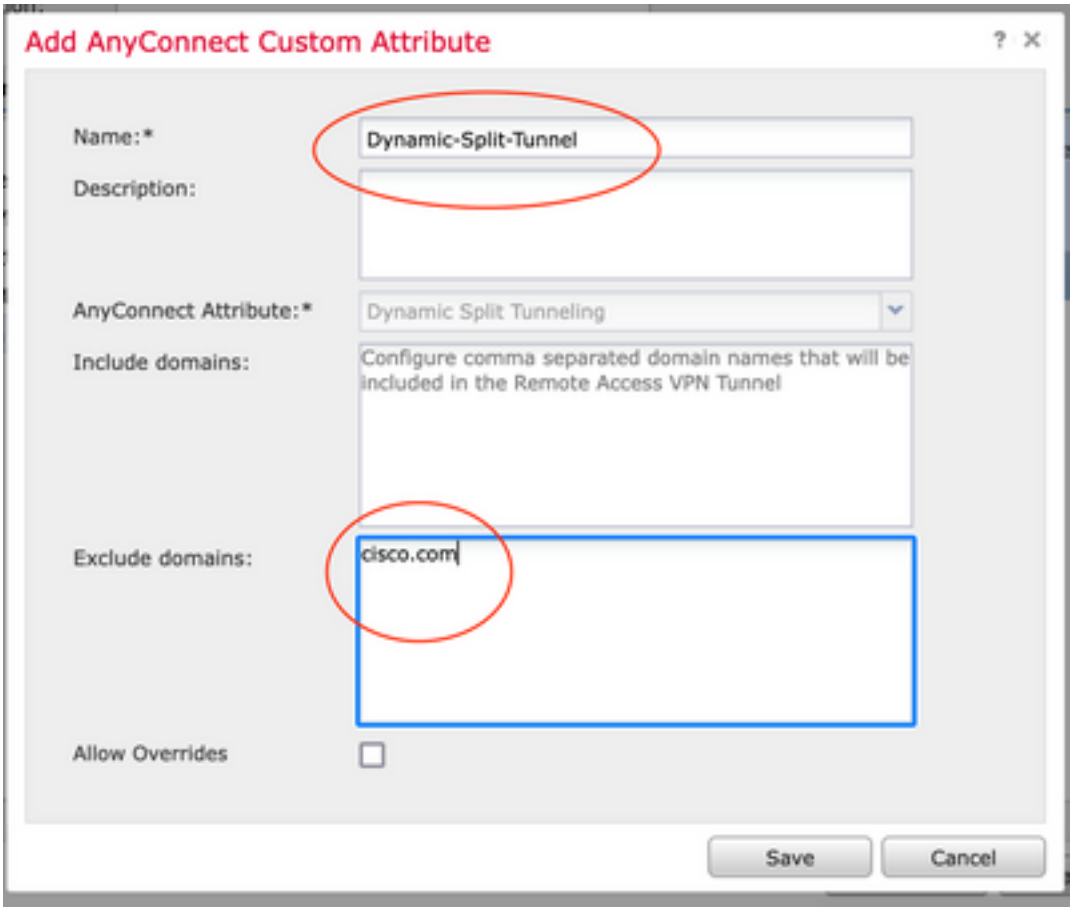


3. Voer de **naam** van het **aangepaste AnyConnect-kenmerk in** en configureer de domeinen die dynamisch moeten worden opgenomen of uitgesloten.

Opmerking: u kunt alleen configureren of **domeinen opnemen** of **domeinen uitsluiten**.

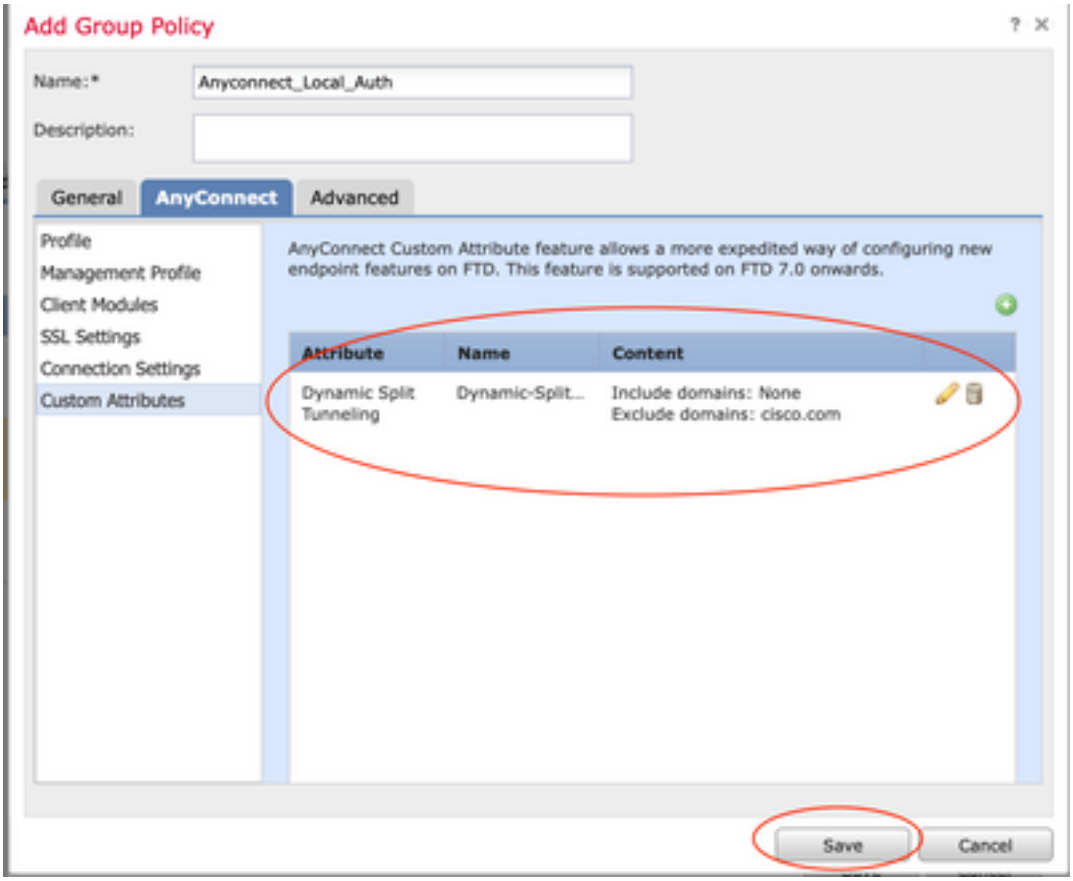


In dit voorbeeld hebben we **cisco.com** geconfigureerd als het uit te sluiten domein en de aangepaste kenmerken **Dynamic-Split-Tunnel** genoemd, zoals in de afbeelding:



Stap 3. Controleer de configuratie, opslaan en implementeren

Controleer of het ingestelde aangepaste kenmerk juist is, sla de configuratie op en implementeer de wijzigingen in het betreffende FTD.



Verifiëren

U kunt deze opdrachten op de FTD uitvoeren via Command Line interface (CLI) om de configuratie van de Dynamic Split Tunnel te bevestigen:

- tonen in werking stellen-configuratiewebvpn
- toon in werking stelt -in werking stellen-configureren om het even welke verbinding-douane-gegevens
- tonen het in werking stellen-Config groep-beleid **<Naam van het groep-beleid>**

In dit voorbeeld is de configuratie de volgende:

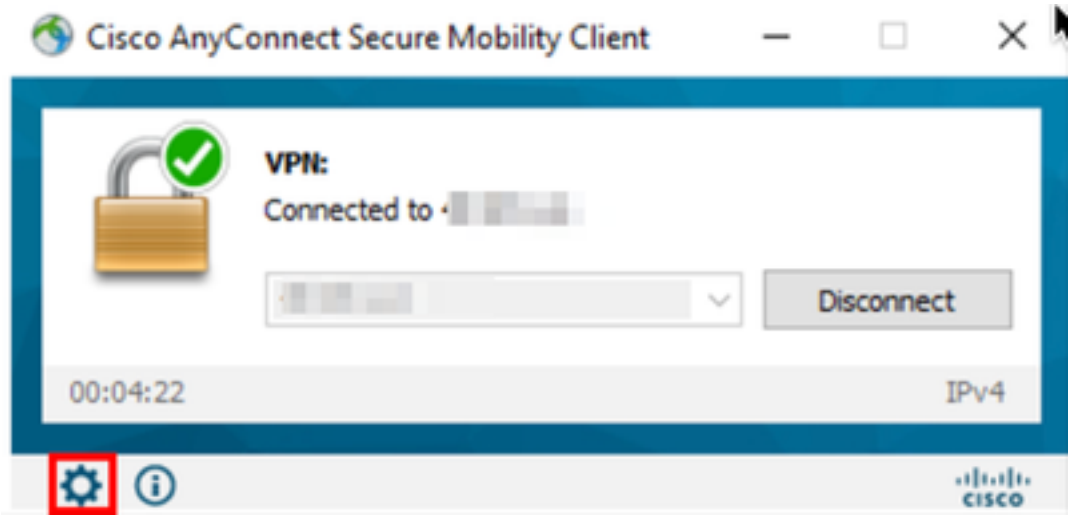
```
ftd# show run group-policy Anyconnect_Local_Auth
group-policy Anyconnect_Local_Auth attributes
vpn-idle-timeout 30
vpn-simultaneous-logins 3
vpn-session-timeout none
vpn-filter none
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelspecified
ipv6-split-tunnel-policy-tunnelall
split-tunnel-network-list value AC_networks
Default-domain none
split-dns none
address-pools value AC_pool
anyconnect-custom dynamic-split-exclude-domains value cisco.com
anyconnect-custom dynamic-split-include-domains none

ftd# show run webvpn
webvpn
enable outside
```

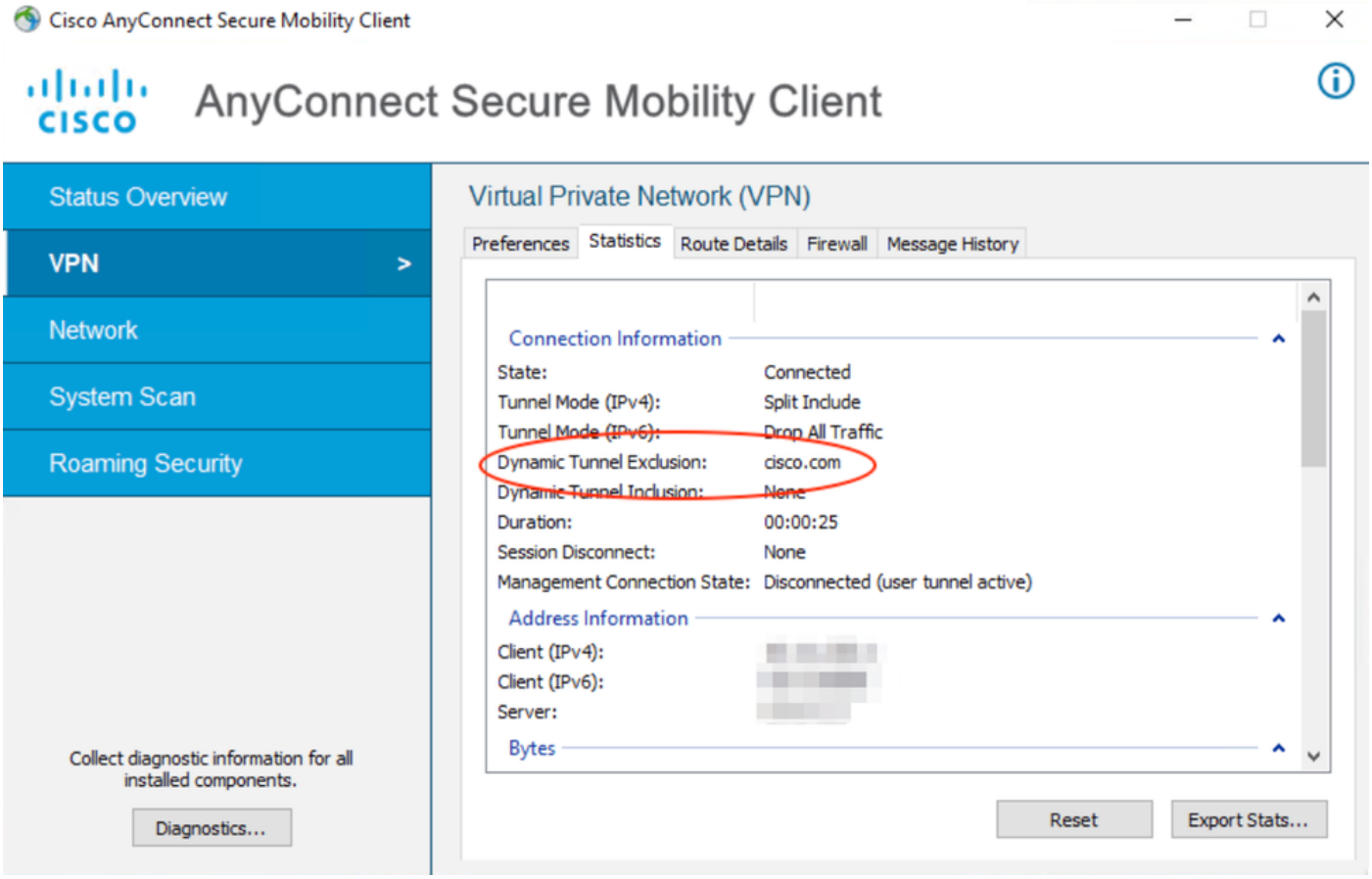
```
anyconnect-custom-attr dynamic-split-exclude-domains
anyconnect-custom-attr dynamic-split-include-domains
http-headers
hsts-server
enable
max-age 31536000
include-sub-domains
no preload
hsts-client
enable
content-security-policy
anyconnect image disk0:/csm/anyconnect-win-4.1005111-webdeploy-k9.pkg regex "Windows"
anyconnect profiles xmltest disk0:/csm/xmltest.xml
anyconnect enable
tunnel-group-list enable
cache
disable
certificate-group-map cert_map_test 10 cert_auth
error-recovery disable
```

Zo controleert u de geconfigureerde uitsluitingen van dynamische tunnels op de client:

1. Start de AnyConnect-software en klik op het pictogram van de versnelling, zoals in de afbeelding wordt weergegeven:



2. Navigeer naar **VPN > Statistieken** en bevestig de domeinen die worden weergegeven onder **Dynamic Split Exclusion/Inclusion**:



Problemen oplossen

U kunt de AnyConnect Diagnostics and Reporting Tool (DART) gebruiken om de gegevens te verzamelen die nuttig zijn voor het oplossen van installatie- en verbindingsproblemen met AnyConnect.

DART verzamelt de logboeken, status en diagnostische informatie voor analyse door de Cisco Technical Assistance Center (TAC) en heeft geen beheerdersbevoegdheden nodig om op het clientapparaat te werken.

Probleem

Als een jokerteken is geconfigureerd in de AnyConnect-aangepaste kenmerken, bijvoorbeeld ***.cisco.com**, wordt de AnyConnect-sessie losgekoppeld.

Oplossing

U kunt de domeinwaarde van **cisco.com** gebruiken om de vervanging van de wildcard toe te staan. Met deze wijziging kunt u domeinen zoals **www, cisco.com** en **tools.cisco.com** opnemen of uitsluiten.

Gerelateerde informatie

- Voor extra assistentie kunt u contact opnemen met het Technical Assistance Center (TAC). Een geldig ondersteuningscontract is vereist: Cisco's wereldwijde contactgegevens voor ondersteuning.

- U kunt ook de Cisco VPN-community bezoeken hier.

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.