ASA/AnyConnect dynamische splitter-tunneling configureren

Inhoud

Inleiding

Dit document beschrijft hoe u AnyConnect Secure Mobility Client voor Dynamic Split Exclude Tunneling via ASDM moet configureren.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis van ASA.
- Basiskennis van Cisco AnyConnect Security Mobility Client.

Gebruikte componenten

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

- ASA 9.12(3)9
- Adaptieve security apparaatbeheer (ASDM) 7.13(1)
- AnyConnect 4.7.0

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 Split-tunneling biedt Cisco AnyConnect Secure Mobility Client beveiligde toegang tot bedrijfsresources via IKEV2 of Secure Sockets Layer (SSL).

Voorafgaand aan AnyConnect versie 4.5, gebaseerd op het beleid dat op adaptieve security applicatie (ASA) is geconfigureerd, kan het gedrag van de splitstunnel worden gespecificeerd, tunnelalles of gespecificeerd uitsluiten.

Met de komst van cloud-gehoste computerbronnen, lossen services soms op naar een ander IP-adres op basis van de locatie van de gebruiker of op basis van de belasting van de cloud-gehoste resources.

Aangezien AnyConnect Secure Mobility Client voorziet in split-tunneling naar statische subnetbereik, host of pool van IPV4 of IPV6, wordt het voor netwerkbeheerders moeilijk om domeinen/FQDNâ€™s uit te sluiten terwijl ze AnyConnect configureren.

Een netwerkbeheerder wil bijvoorbeeld het Cisco.com domein uitsluiten van de Split-tunnelconfiguratie, maar de DNS-toewijzing voor Cisco.com verandert omdat het cloudgehost wordt.

Met Dynamic Split Exclude tunneling lost AnyConnect dynamisch het IPv4/IPv6-adres van de gehoste toepassing op en brengt noodzakelijke wijzigingen aan in de routeringstabel en filters om de verbinding buiten de tunnel te kunnen maken.

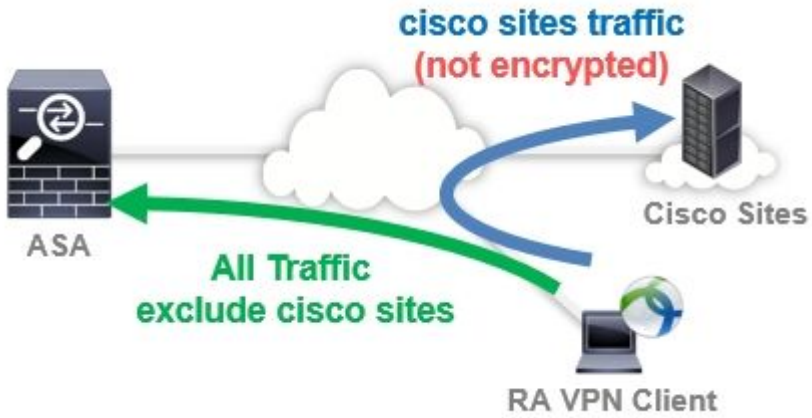
Vanaf AnyConnect 4.5 kan Dynamic Spit Tunneling worden gebruikt, waarbij AnyConnect het IPv4/IPv6-adres van de gehoste toepassing dynamisch oplost en noodzakelijke wijzigingen in de routeringstabel en filters aanbrengt om de verbinding buiten de tunnel mogelijk te maken

Configuratie

In dit gedeelte wordt beschreven hoe u de Cisco AnyConnect Secure Mobility Client op de ASA kunt configureren.

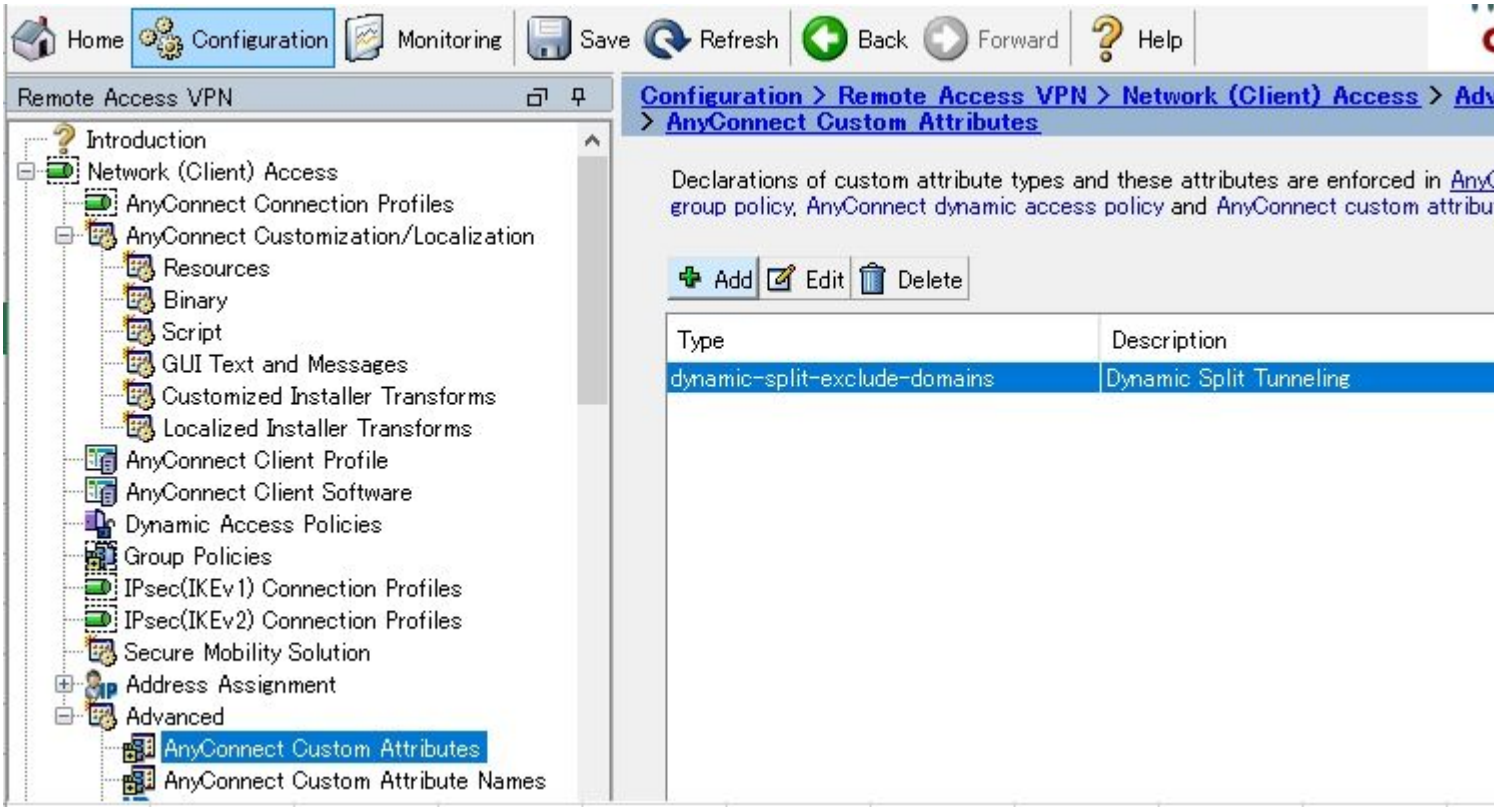
Netwerkdiagram

Dit beeld toont de topologie die voor de voorbeelden van dit document wordt gebruikt.



Stap 1. Aangepaste AnyConnect-kenmerken maken.

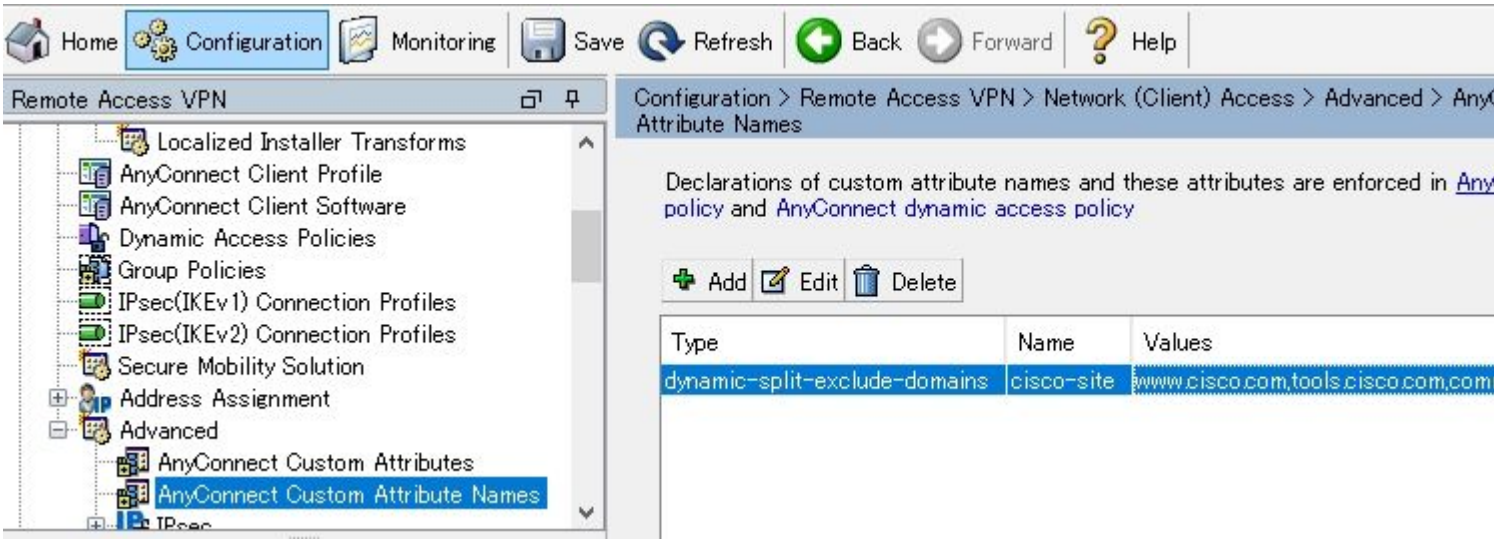
Naar navigeren **Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attributes.**klik op de knop **Add** toets te drukken en in te stellen **dynamic-split-exclude-domains** attribuut en optionele beschrijving, zoals in de afbeelding:



Stap 2. Aangepaste AnyConnect-naam maken en waarden configureren.

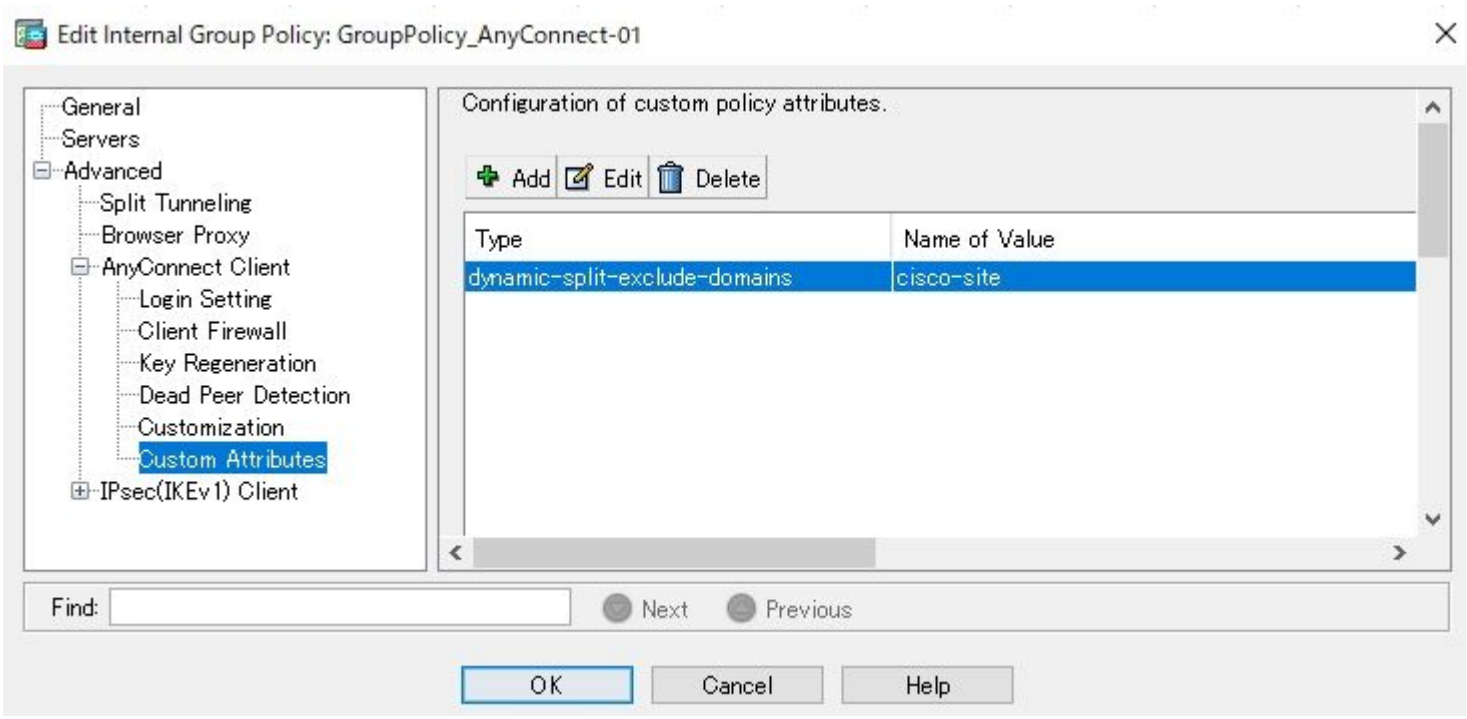
Naar navigeren **Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attribute Names.**klik op de knop **Add** toets te drukken en de **dynamic-split-exclude-domains** attribuut dat eerder is gemaakt van Type, een willekeurige naam en waarden, zoals in de afbeelding:

Let erop dat u geen spatie in Naam invoert. (Voorbeeld: Mogelijk "cisco-site" Onmogelijke "cisco site") Wanneer meerdere domeinen of FQDN's in Waarden zijn geregistreerd, scheidt u deze met een komma (,).



Stap 3. Voeg Type en Naam toe aan het Groepsbeleid.

Naar navigeren **Configuration> Remote Access VPN> Network (Client) Access> Group Policies** en Selecteer een groepsbeleid. Navigeer daarna naar **Advanced> AnyConnect Client> Custom Attributes** en het ingestelde bestand toevoegen **Type** en **Name,** zoals aangegeven op de afbeelding:



Voorbeeld van CLI-configuratie

Deze sectie biedt de CLI-configuratie van Dynamic Split Tunneling voor referentiedoeleinden.

<#root>

```
ASAv10# show run
  --- snip ---
webvpn


 enable outside
 anyconnect-custom-attr dynamic-split-exclude-domains description Dynamic Split Tunneling


 hsts
  enable
  max-age 31536000
  include-sub-domains
  no preload
 anyconnect image disk0:/anyconnect-win-4.7.04056-webdeploy-k9.pkg 1
 anyconnect enable
 tunnel-group-list enable
 cache
  disable
 error-recovery disable
anyconnect-custom-data dynamic-split-exclude-domains cisco-site www.cisco.com,tools.cisco.com,community.


group-policy GroupPolicy_AnyConnect-01 internal
```

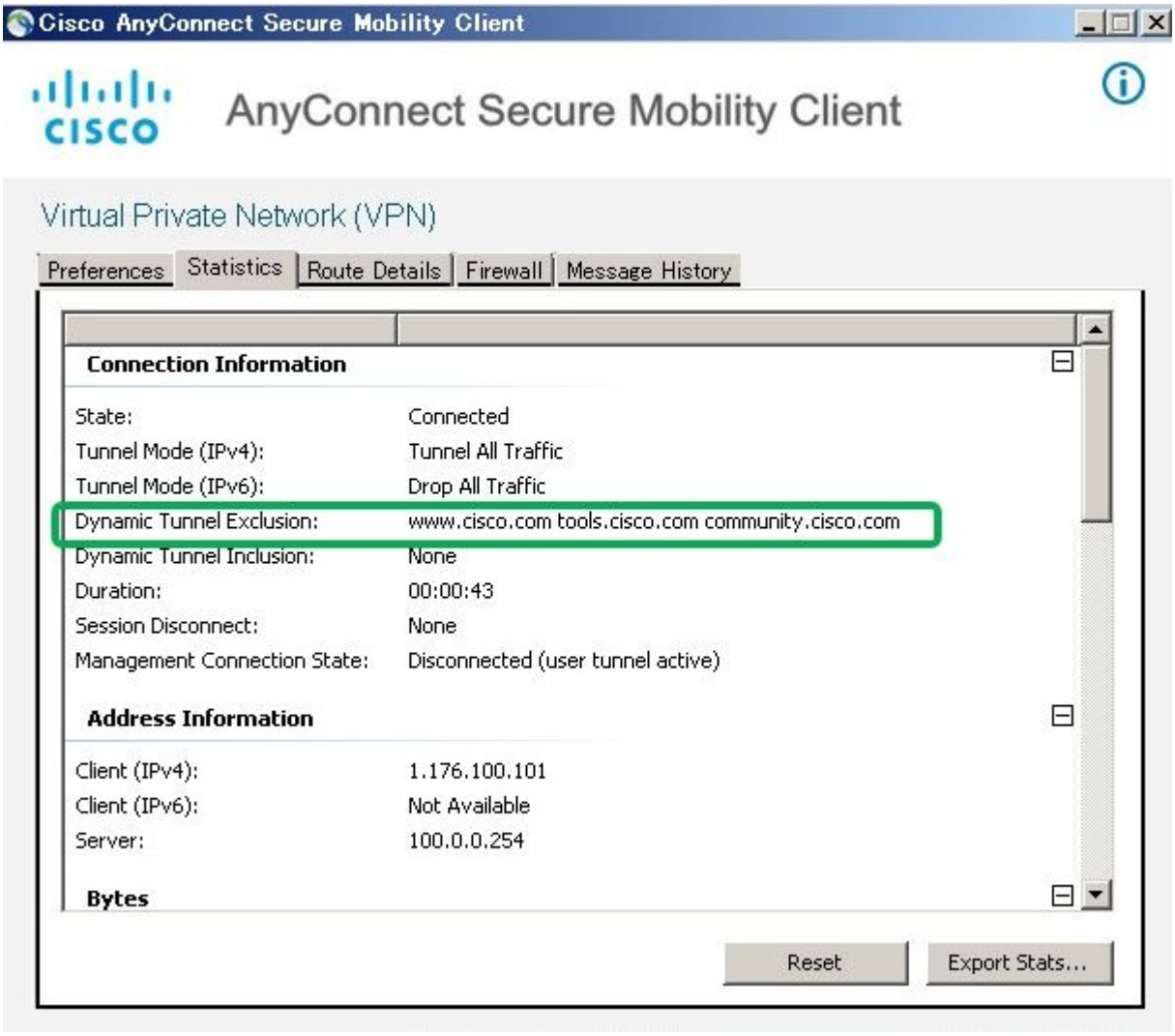
```
group-policy GroupPolicy_AnyConnect-01 attributes


 wins-server none
 dns-server value 10.0.0.0
 vpn-tunnel-protocol ssl-client
 split-tunnel-policy tunnelall
 split-tunnel-network-list value SplitACL
 default-domain value cisco.com

 anyconnect-custom dynamic-split-exclude-domains value cisco-site
```

Beperkingen

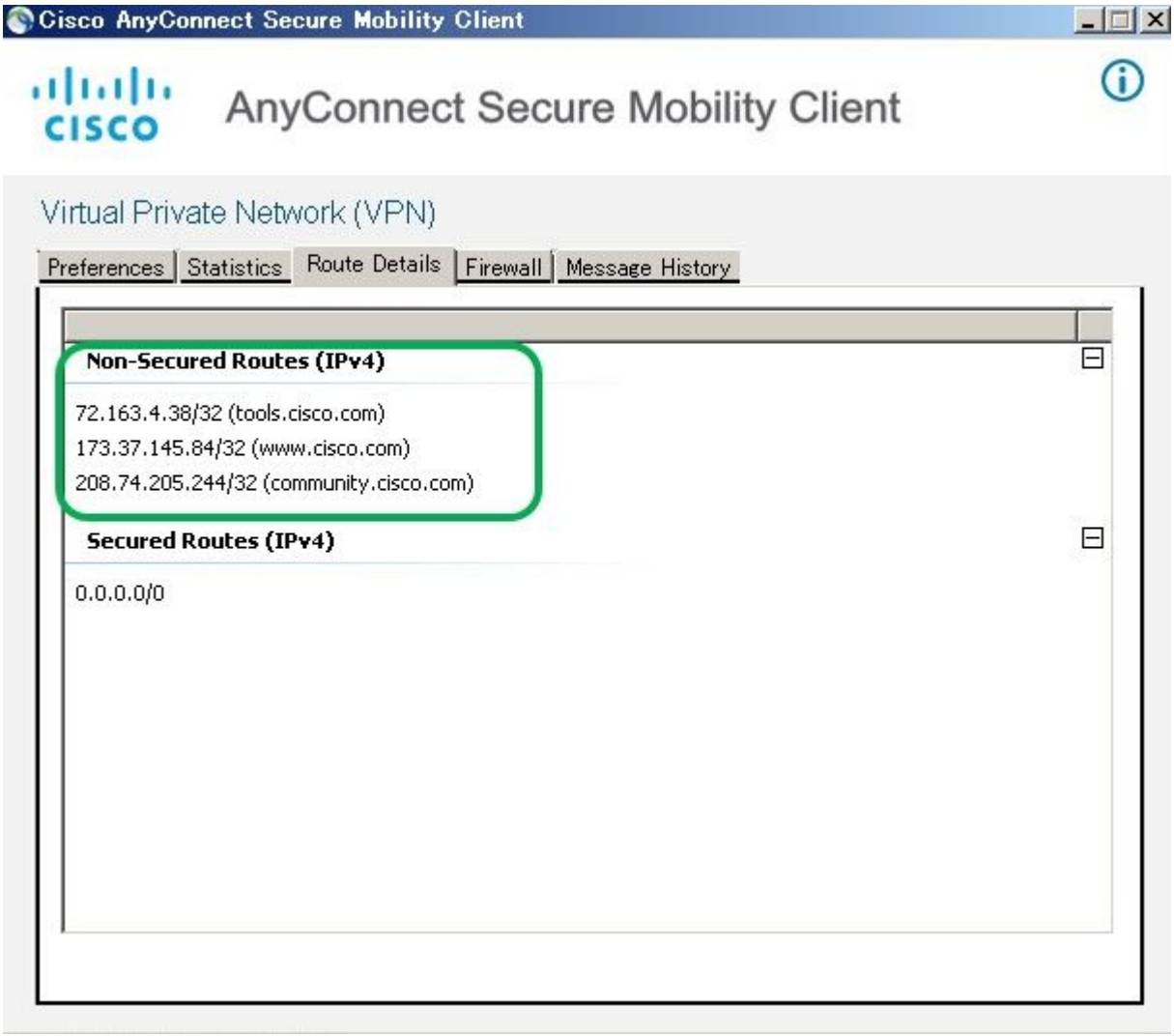
- ASA versie 9.0 of hoger is nodig om aangepaste kenmerken van Dynamic Split Tunneling te gebruiken.
- De jokerteken in het veld Waarden wordt niet ondersteund.
- Dynamic Split Tunneling wordt niet ondersteund op iOS (Apple)-apparaten (Verbeteringsaanvraag: 'Cisco bug-id CSCvr54798').

Verifiëren

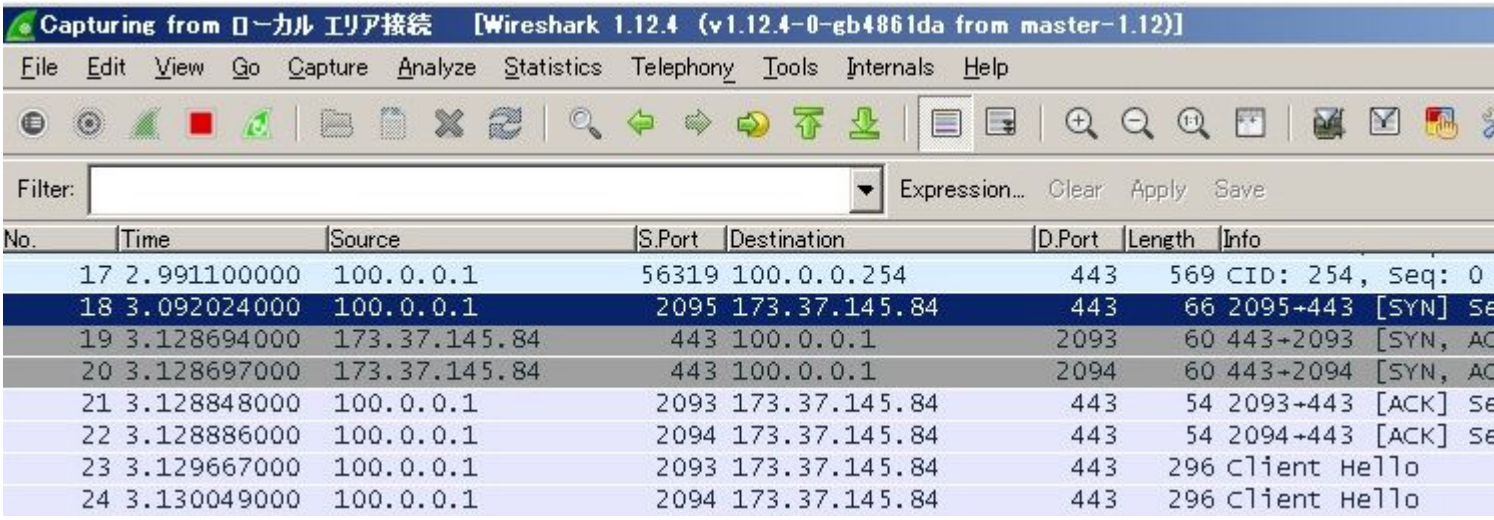
Zo controleert u ingesteld op **Dynamic Tunnel Exclusions,** Start **AnyConnect** op de client, klikt u op **Advanced Window** > **Statistics,** zoals in de afbeelding:



U kunt ook navigeren naar **Advanced Window** > **Route Details** tabblad waarin u kunt verifiëren **Dynamic Tunnel Exclusions** worden vermeld onder **Non-Secured Routes,** zoals in de afbeelding.



In dit voorbeeld hebt u www.cisco.com geconfigureerd onder **Dynamic Tunnel Exclusion list** en de Wireshark Capture die is verzameld op de fysieke interface van de AnyConnect-client bevestigt dat het verkeer naar www.cisco.com (198.51.100.0) niet door DTLS is versleuteld.



Problemen oplossen

Indien de jokerteken wordt gebruikt in het veld Waarden

Als een jokerteken bijvoorbeeld in het veld Waarden is geconfigureerd, wordt ***.cisco.com** in Waarden geconfigureerd en wordt de AnyConnect-sessie verbroken, zoals in de logboeken wordt getoond:

```
Apr 02 2020 10:01:09: %ASA-4-722041: TunnelGroup <AnyConnect-01> GroupPolicy <GroupPolicy_AnyConnect-01>
Apr 02 2020 10:01:09: %ASA-5-722033: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> Firs
Apr 02 2020 10:01:09: %ASA-6-722022: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> TCP
Apr 02 2020 10:01:09: %ASA-6-722055: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> Clie
Apr 02 2020 10:01:09: %ASA-4-722051: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> IPv4
Apr 02 2020 10:01:09: %ASA-6-302013: Built inbound TCP connection 8570 for outside:172.16.0.0/44868 (172
Apr 02 2020 10:01:09: %ASA-4-722037: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> SVC
Apr 02 2020 10:01:09: %ASA-5-722010: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> SVC
Apr 02 2020 10:01:09: %ASA-6-716002: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> WebV
Apr 02 2020 10:01:09: %ASA-4-113019: Group = AnyConnect-01, Username = cisco, IP = 172.16.0.0, Session d
```

> **Opmerking**: Als alternatief kunt u het domein **cisco.com** gebruiken in Waarden om FQDNâ€™s zoals www.cisco.com en tools.cisco.com toe te staan.

In het geval dat niet-beveiligde routers niet worden weergegeven in het tabblad Routedetails

AnyConnect-client leert en voegt automatisch het IP-adres en FQDN toe op het tabblad Routedetails wanneer de client het verkeer voor de uitgesloten bestemmingen start.

Om te verifiëren dat de AnyConnect-gebruikers zijn toegewezen aan het juiste AnyConnect-groepsbeleid, kunt u de opdracht '**show vpn-sessiondb anyconnect filter name**
"

<#root>

```
ASAv10# show vpn-sessiondb anyconnect filter name cisco

Session Type: AnyConnect

Username     : cisco                  Index : 7
Assigned IP  : 172.16.0.0          Public IP : 10.0.0.0
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256
Hashing      : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384
Bytes Tx     : 7795373                Bytes Rx : 390956
```

Group Policy : GroupPolicy_AnyConnect-01

```
Tunnel Group : AnyConnect-01
Login Time   : 13:20:48 UTC Tue Mar 31 2020
Duration     : 20h:19m:47s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN : none
Audt Sess ID : 019600a9000070005e8343b0
Security Grp : none
```

Algemene probleemoplossing

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. De DART Wizard wordt gebruikt op de computer waarop AnyConnect wordt uitgevoerd. 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.

Gerelateerde informatie

- **Cisco AnyConnect Secure Mobility Client-beheerdershandleiding, release 4.7 - Over dynamische splitter-tunneling**
- **ASDM Book 3: Cisco ASA Series VPN ASDM-configuratiehandleiding, 7.13 - Dynamische splitter-tunneling configureren**

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.