AnyConnect OpenDNS-roamingbeveiligingsmodule - implementatiegids

Inhoud

Inleiding

Dit document beschrijft de installatie, configuratie en probleemoplossing van de stappen voor de OpenDNS (Umbrella)-roamingmodule. In AnyConnect 4.3.X en hoger is de OpenDNS-roamingclient nu beschikbaar als een geïntegreerde module. Het staat ook bekend als de Cloud Security module en kan vooraf worden geïnstalleerd op het eindpunt met de AnyConnect-installateur of het kan via webimplementatie worden gedownload van de adaptieve security applicatie (ASA).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco AnyConnect beveiligde mobiliteit
- OpenDNS/Umbrella-routermodule
- Cisco ASA

Gebruikte componenten

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

- Cisco ASA versie 9.3(3)7
- Cisco AnyConnect beveiligde mobiliteit-client 4.3.1095
- OpenDNS-roamingmodule 4.3.01095
- Cisco Adaptieve Security Devices Manager (ASDM) 7.6.2 of hoger
- Microsoft Windows 8.1
- Opmerking: De minimale vereisten voor de implementatie van OpenDNS Umbrella-module zijn:
  - AnyConnect VPN-clientversie 4.3.010/95 of hoger
  - Cisco ASDM 7.6.2 of hoger
  OpenDNS-roamingmodule wordt momenteel niet ondersteund op het Linux-platform.

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 levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdrachten of configuratie begrijpt.

Achtergrondinformatie

OrgInfo.json

Om de OpenDNS-roamingmodule goed te laten functioneren, moet er een bestand OrgInfo.json worden gedownload van het OpenDNS-dashboard of van de ASA worden geduwd voordat de module wordt gebruikt. Wanneer het bestand voor het eerst wordt gedownload, wordt het opgeslagen op een specifiek pad dat afhankelijk is van het besturingssysteem.

Voor Mac OS X wordt OrgInfo.json gedownload naar /opt/cisco/anyconnect/Umbrella.
Voor Microsoft Windows wordt OrgInfo.json gedownload naar C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Umbrella.

```
{
"organizationId" : "XXXXXXX",
"fingerprint" : "XXXXXXXXXXXXXXXXXXXXXXXXXXXX",
"userId" : "XXXXXXX"
}
```

Zoals aangegeven gebruikt het bestand UTF-8-codering en bevat het een organisatie-ID, vingerafdruk en gebruiker-ID. De organisatie-ID vertegenwoordigt de organisatieinformatie voor de gebruiker die op dit moment aangemeld is in het OpenDNS-dashboard. De organisatie-ID is statisch, uniek en automatisch gegenereerd door OpenDNS voor elke organisatie. De vingerafdruk wordt gebruikt om het bestand OrgInfo.json tijdens de registratie van het apparaat te valideren en de gebruiker-ID vertegenwoordigt een unieke ID voor de ingelogde gebruiker.

Wanneer de Roaming module op Windows begint, wordt het OrgInfo.json bestand gekopieerd

naar de gegevensmap onder de Umbrella-map en gebruikt als de werkende kopie. Op MAC OS X wordt de informatie uit dit bestand opgeslagen in update.plist in de gegevensmap onder de Umbrella-map. Nadat de module met succes informatie uit het bestand OrgInfo.json heeft gelezen, probeert het om met OpenDNS met een cloud API te registreren. Deze registratie resulteert in OpenDNS bij het toewijzen van een uniek apparaat-ID aan de machine die registratie heeft geprobeerd. Als een apparaat-ID uit voorafgaande registratie al beschikbaar is, slaat het apparaat de registratie over.

Nadat de registratie is voltooid, voert de Roaming module een sync-handeling uit om beleidsinformatie voor het eindpunt op te halen. Een apparaat-ID is nodig om de sync-handeling te kunnen laten werken. Sync gegevens omvatten syncInterval, interne bypass-domeinen en IP-adressen onder andere. Het sync-interval is het aantal minuten waarna de module moet proberen te resync.

DNS-provisioninggedrag

Na succesvolle registratie en sync, stuurt de roaming-module DNS-problemen (Domain Name System) naar de lokale resoluties. Deze DNS-verzoeken bevatten TXT-vragen voor debug.opendns.com. Op basis van de respons kan de client bepalen of er een OpenDNS virtuele applicatie (VA) op locatie is in het netwerk.

Als er een virtueel apparaat (VA) aanwezig is, gaat de client over naar een 'achter-VA'-modus en wordt DNS-handhaving niet op het eindpunt uitgevoerd. De client is afhankelijk van de VA voor DNS-handhaving op netwerkniveau.

Als er geen VA aanwezig is, stuurt de client een DNS-verzoek naar de OpenDNS-publieke resolutie (208.67.222.222) met UDP/443.

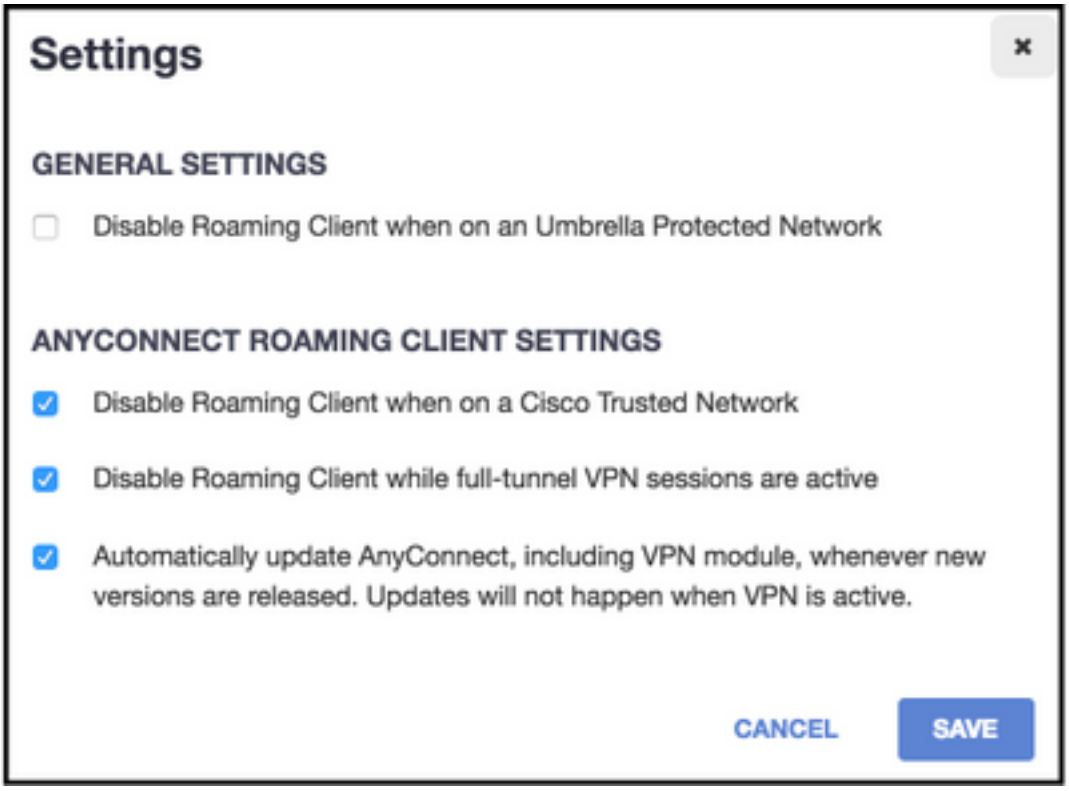
Een positieve reactie geeft aan dat DNS-encryptie mogelijk is. Als een negatieve reactie wordt ontvangen, stuurt de client een DNS-verzoek naar de OpenDNS-publieke resolutie met UDP/53.

Een positief antwoord op deze vraag geeft aan dat DNS-bescherming mogelijk is. Als een negatieve reactie wordt ontvangen, probeert de client de query in een paar seconden opnieuw uit.

Na ontvangst van een bepaald aantal negatieve reacties, gaat de client over naar de open status. Een niet-open toestand betekent dat DNS-encryptie en/of bescherming niet mogelijk is. Nadat de Roaming module met succes is overgestapt naar een beschermde en/of gecodeerde staat, worden alle DNS vragen voor zoekdomeinen buiten de lokale zoekdomeinen en interne omzeilingdomeinen naar de OpenDNS resoluties voor naamresolutie verzonden. Met versleutelde status worden alle DNS-transacties versleuteld met het decrypt-proces.

DNS-gedrag met AnyConnect-tunneling

1. Tunnel-All (of tunnelal-DNS ingeschakeld)



> Opmerking: Zoals getoond, is het standaardgedrag voor de Roaming module om DNS bescherming uit te schakelen terwijl een VPN-tunnel met tunnel-all configuratie actief is. Om de module actief te laten zijn tijdens een AnyConnect-tunnelconfiguratie, **moet** de **roaming-client uitschakelen terwijl de volledige-tunnel VPN-sessies actief zijn**, op het OpenDNS-portaal niet worden gecontroleerd. De mogelijkheid om deze optie te activeren vereist een geavanceerd abonnementsniveau met OpenDNS. De onderstaande informatie gaat ervan uit dat DNS-beveiliging via de roaming-module is ingeschakeld.

Gebied binnen beperkt domein deel van interne omzeilingslijst

DNS-verzoeken die afkomstig zijn van de tunneladapter zijn toegestaan en worden naar de DNS-tunnelservers in de VPN-tunnel verzonden. De query zal onopgelost blijven als deze niet kan worden opgelost door de DNS-tunnelservers.

Gekoppeld domein dat geen deel uitmaakt van de interne omzeilingelijst

DNS-verzoeken die afkomstig zijn van de tunneladapter zijn toegestaan en worden uitgebreid naar de OpenDNS-publieke resoluties via de Roaming module en verzonden via de VPN-tunnel. Aan de DNS-client wordt het weergegeven alsof de naamresolutie is opgetreden via de VPN-DNS-server. Als de naamresolutie via OpenDNS-resoluties niet succesvol is, wordt de Roaming-module niet uitgevoerd naar de lokaal geconfigureerde DNS-servers, te beginnen met de VPN-adapter (die de voorkeursadapter is terwijl de tunnel omhoog is).

2. Split-DNS (tunnelalle-DNS-uitgeschakeld)

> Opmerking: Alle split-DNS domeinen worden automatisch toegevoegd aan de Roaming module interne bypass list bij tunnelinstelling. Dit gebeurt om een consistent DNS-verwerkingsmechanisme te bieden tussen AnyConnect en de Roaming module. Verzeker u ervan dat in een gesplitste-DNS-configuratie (met gesplitste-inclusieve tunneling) de openbare OpenDNS-resoluties niet in de gesplitste-inclusieve netwerken zijn opgenomen.

Opmerking: Op Mac OS X, als split-DNS ingeschakeld is voor zowel IP-protocollen (IPv4 en IPv6) of als deze alleen ingeschakeld is voor één protocol en er geen adrepool is ingesteld voor het andere protocol, wordt echte split-DNS zoals Windows wordt uitgevoerd.
Als split-DNS is ingeschakeld voor slechts één protocol en er een clientadres is toegewezen voor het andere protocol, wordt alleen DNS-back-up voor split-tunneling gehandhaafd. Dit betekent dat AnyConnect alleen DNS-verzoeken toestaat die overeenkomen met de gesplitste-DNS-domeinen via tunnel (andere verzoeken worden door AC geantwoord met een afgewezen reactie op force-failover naar openbare DNS-servers), maar kan niet afdwingen dat verzoeken die overeenkomen met gesplitste-DNS-domeinen niet in de duidelijke volgorde worden verzonden via de openbare adapter.

Geavanceerd domein deel van interne omzeilingslijst en ook onderdeel van Split-DNS-domein

DNS-verzoeken die afkomstig zijn van de tunneladapter zijn toegestaan en worden naar de DNS-tunnelservers in de VPN-tunnel verzonden. Alle andere aanvragen om overeenkomende domeinen van andere adapters worden door de AnyConnect-stuurprogramma beantwoord met 'geen dergelijke naam' om een echte gesplitste-DNS te bereiken (voorkoming van DNS-back). Daarom wordt alleen niet-tunnelDNS-verkeer beschermd door de Roaming module.

Geavanceerd domein deel van interne omzeilingslijst, maar geen onderdeel van Split-DNS-domein

DNS-verzoeken die afkomstig zijn van de fysieke adapter worden toegestaan en naar de openbare DNS-servers verzonden, buiten de VPN-tunnel. Alle andere verzoeken om overeenkomende domeinen van de tunneladapter zullen worden beantwoord door de AnyConnect-stuurprogramma met 'geen dergelijke naam' om te voorkomen dat de query over de VPN-tunnel wordt verzonden.

Geëvenaard domein dat geen deel uitmaakt van interne omzeilingslijst of splitter-DNS-velden

DNS-verzoeken die afkomstig zijn van de fysieke adapter zijn toegestaan en worden uitgebreid naar de OpenDNS-openbare resolutie en worden verzonden vanuit de VPN-tunnel. Aan de DNS-client wordt het weergegeven alsof de naamresolutie is opgetreden via de openbare DNS-server. Als de naamresolutie via OpenDNS-resoluties niet werkt, heeft de roaming-module geen invloed op de lokaal geconfigureerde DNS-servers, met uitzondering van de servers die op de VPN-adapter zijn ingesteld. Alle andere verzoeken om overeenkomende domeinen van de tunneladapter zullen worden beantwoord door de AnyConnect-stuurprogramma met een dergelijke naam om te voorkomen dat de query over de VPN-tunnel wordt verzonden.

3. Split-Inclusief of Split-Embedded Tunneling (geen gesplitste DNS en tunnelall-DNS uitgeschakeld)

Gebied binnen beperkt domein deel van interne omzeilingslijst

Een native OS-resolutie voert een DNS-resolutie uit op basis van de volgorde van netwerkadapters en AnyConnect is de gewenste adapter wanneer VPN actief is. DNS-verzoeken komen eerst uit de tunneladapter en worden naar de DNS-tunnelservers in de VPN-tunnel verzonden. Als de query niet kan worden opgelost door de DNS-tunnelservers, zal de OS-resolutie proberen deze op te lossen via de openbare DNS-servers.

Gekoppeld domein dat geen deel uitmaakt van de interne omzeilingelijst

Een native OS-resolutie voert een DNS-resolutie uit op basis van de volgorde van netwerkadapters en AnyConnect is de gewenste adapter wanneer VPN actief is. DNS-verzoeken komen eerst uit de tunneladapter en worden naar de DNS-tunnelservers in de VPN-tunnel verzonden. Als de query niet kan worden opgelost door de DNS-tunnelservers, zal de OS-resolutie proberen deze op te lossen via de openbare DNS-servers.

Als de openbare resoluties van OpenDNS deel uitmaken van de gesplitste-inclusieve lijst of geen deel uitmaken van de lijst met gesplitste-uitsluitingen, wordt het geproxiseerde verzoek verzonden over de VPN-tunnel.

Als de openbare resoluties van OpenDNS geen deel uitmaken van de gesplitste-inclusieve lijst of een deel van de gesplitste-uitsluitingslijst, wordt het geproxiseerde verzoek verzonden buiten de VPN-tunnel.

Als de naamresolutie via OpenDNS-resoluties niet succesvol is, wordt de Roaming-module niet uitgevoerd naar de lokaal geconfigureerde DNS-servers, te beginnen met de VPN-adapter (die de voorkeursadapter is terwijl de tunnel omhoog is). Als de definitieve reactie die door de Roaming module is teruggegeven (en teruggeleid is naar de oorspronkelijke DNS-client) niet succesvol is, zal de oorspronkelijke client andere DNS-servers proberen, indien beschikbaar.

Module voor Umbrella installeren en configureren

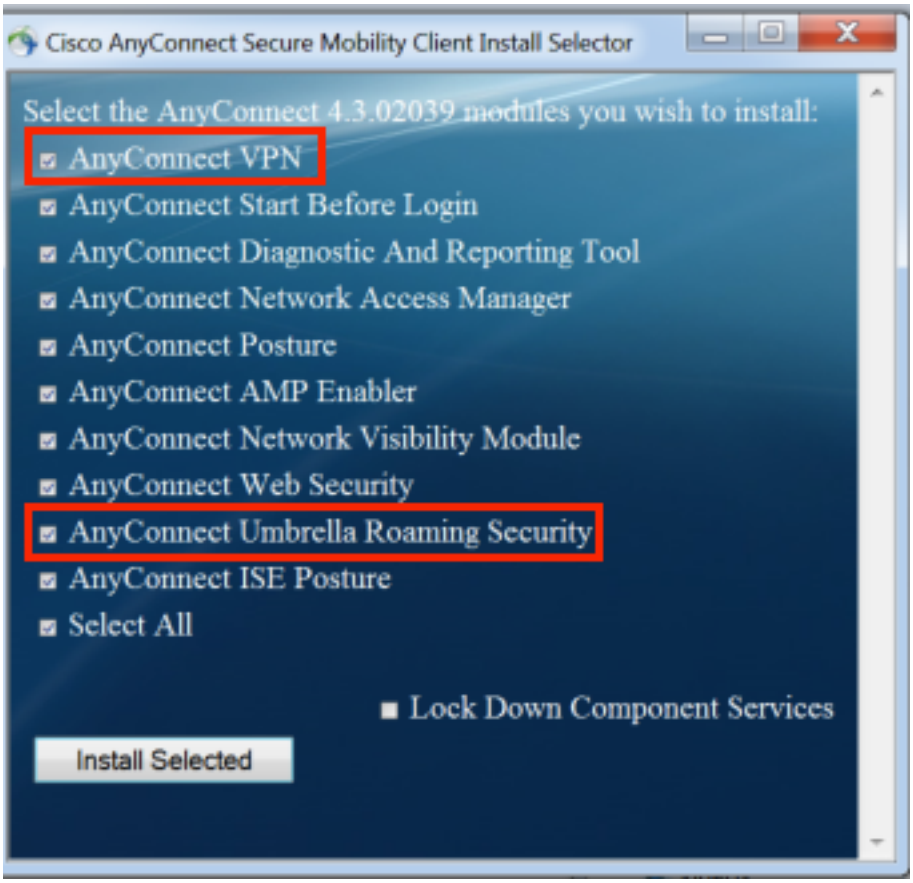
Om de OpenDNS-roamingmodule met de AnyConnect VPN-client te integreren, moet de module worden geïnstalleerd via de pre-implementatiemethode of op het web:

Methode vóór implementatie (handmatig)

Voor het vooraf implementeren moet de OpenDNS-roamingmodule handmatig worden geïnstalleerd en moet het bestand OrgInfo.json op de gebruikersmachine worden gekopieerd. Grote implementaties worden meestal bereikt met bedrijfssoftware-beheersystemen (sms).

OpenDNS-roamingmodule implementeren

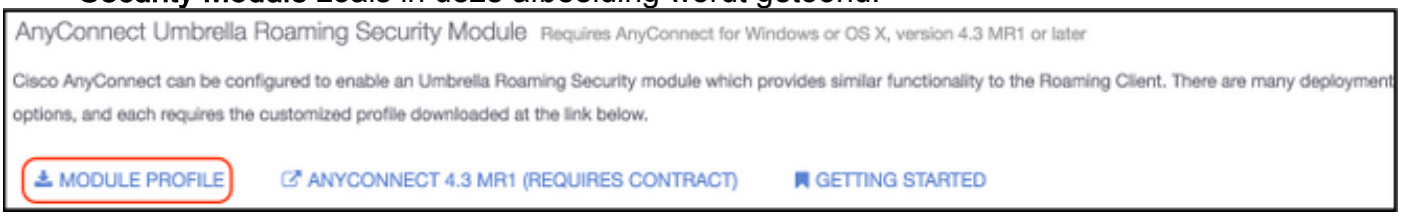
Kies tijdens de installatie van AnyConnect de modules **AnyConnect VPN** en **AnyConnect Umbrella Roaming security** modules:



Deploy OrgInfo.json

Voltooi de volgende stappen om het bestand OrgInfo.json te downloaden:

1. Log in op het OpenDNS-dashboard.
2. Kies **Configuration > Identity Services > Roaming Computers.**
3. Klik op het **+** teken.
4. Scrolt naar beneden en kies **Module profiel** in het gedeelte **AnyConnect Umbrella Roaming Security Module** zoals in deze afbeelding wordt getoond:



Nadat het bestand is gedownload, moet het op een van deze paden worden opgeslagen, wat afhankelijk is van het besturingssysteem.

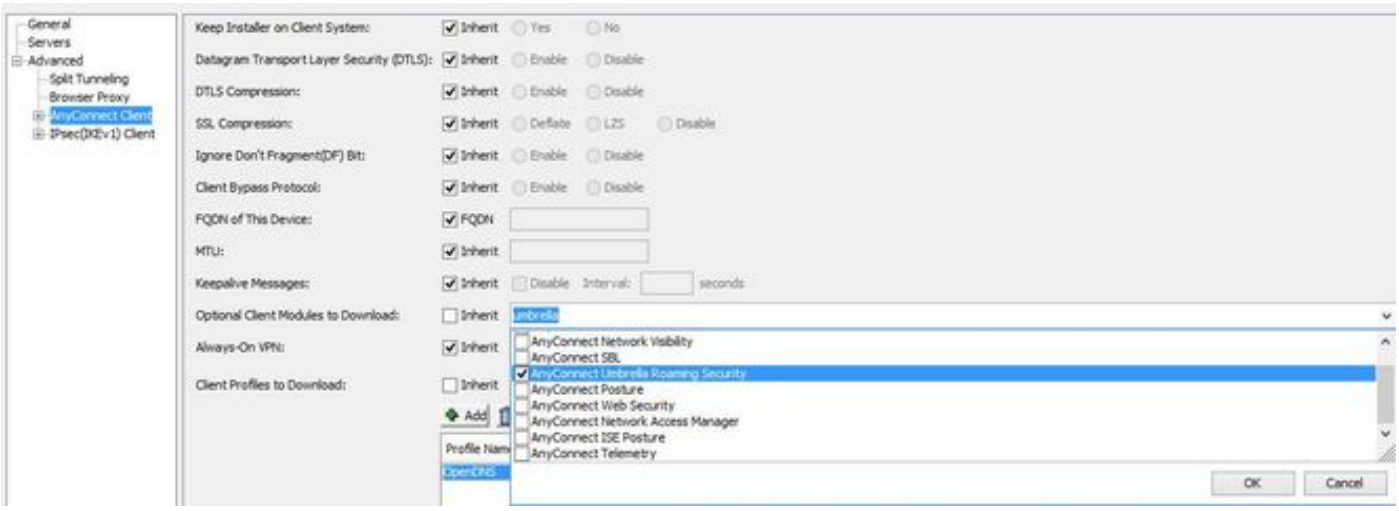
Voor Mac OS X: /opt/cisco/anyconnect/Umbrella
Voor Windows: C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Umbrella

Web-implementatiemethode

OpenDNS-roamingmodule implementeren

Download het AnyConnect Security Mobility Client-pakket (dwz, AnyConnect-win-4.3.02039-k9.pkg) van de Cisco website en uploaden het naar ASA's flitser. Kies **na** het uploaden in de

ASDM **groepsbeleid > Geavanceerd > AnyConnect-client > optionele clientmodules voor downloads** en kies vervolgens **Umbrella-roamingbeveiliging.**

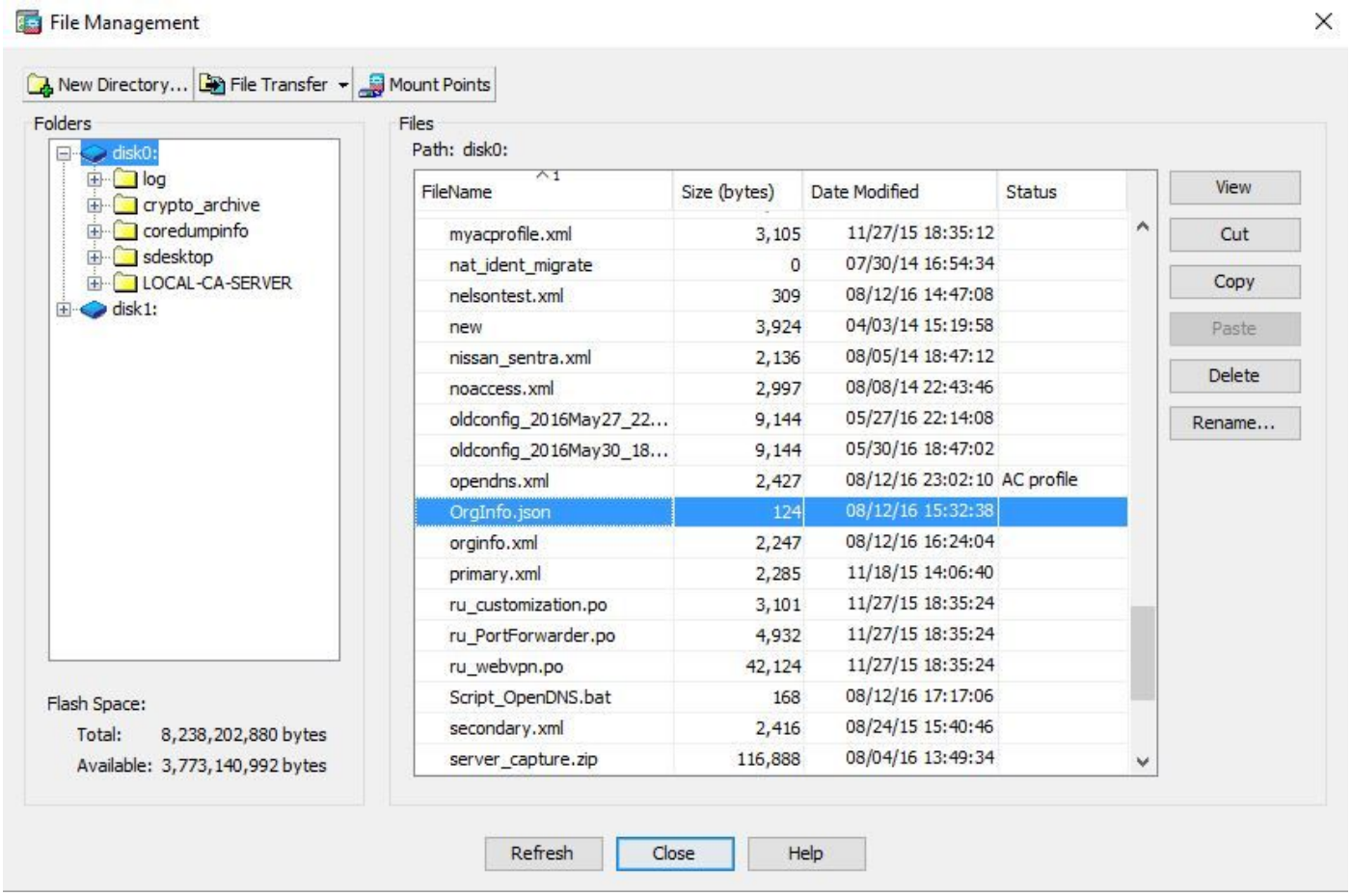


CLI-equivalent

```
group-policy <Group_Policy_Name> attributes
webvpn
anyconnect modules value umbrella
```

Deploy OrgInfo.json

1. Download het bestand OrgInfo.json van het OpenDNS-dashboard en uploaden het naar de ASA-flitser.



2. Configureer de ASA om het bestand OrgInfo.json op externe eindpunten te duwen.

```
webvpn
anyconnect profiles OpenDNS disk0:/OrgInfo.json
!
!
group-policy <Group_Policy_Name> attribute
webvpn
anyconnect profiles value OpenDNS type umbrella
```

> Opmerking: Deze configuratie kan alleen via de CLI worden uitgevoerd. Om ASDM voor deze taak te kunnen gebruiken, moet ASDM versie 7.6.2 of hoger op de ASA zijn geïnstalleerd.

Nadat de Umbrella Roaming client via een van de besproken methoden is geïnstalleerd, moet deze client als een geïntegreerde module in de AnyConnect GUI verschijnen zoals in deze afbeelding:

Totdat de OrgInfo.json op het eindpunt op de juiste plaats wordt opgesteld, zal de Umbrella Roaming module niet worden geïnitialiseerd.

Configureren

In het gedeelte worden voorbeelden van CLI-configuratiehandelingen weergegeven die nodig zijn om de OpenDNS-roamingmodule met de verschillende AnyConnect-tunneling te bedienen.

```
!--- ip local pool for vpn
ip local pool vpn_pool 198.51.100.1-198.51.100.9 mask 255.255.255.224

!--- Optional NAT Hairpin configuration to reach OpenDNS servers through VPN tunnel
object network OpenDNS
```

```
subnet 198.51.100.0 255.255.255.0
nat (outside,outside) source dynamic OpenDNS interface
!
same-security-traffic permit intra-interface

!--- Global Webvpn Configuration
webvpn
enable outside
anyconnect image disk0:/anyconnect-win-4.3.01095-k9.pkg 1
anyconnect profiles Anyconnect disk0:/anyconnect.xml
 anyconnect profiles OpenDNS disk0:/OrgInfo.json
anyconnect enable
tunnel-group-list enable

!--- split-include Configuration
access-list Split_Include standard permit <host/subnet>

group-policy OpenDNS_Split_Include internal
group-policy OpenDNS_Split_Include attributes
wins-server none
dns-server value 198.51.100.11
vpn-tunnel-protocol ssl-client ssl-clientless
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value Split_Include
split-dns value




         (Optional Split-DNS Configuration)
webvpn
anyconnect profiles value AnyConnect type user
 anyconnect profiles value OpenDNS type umbrella
!
tunnel-group OpenDNS_Split_Include type remote-access
tunnel-group OpenDNS_Split_Include general-attributes
address-pool vpn_pool
default-group-policy OpenDNS_Split_Include
tunnel-group OpenDNS_Split_Include webvpn-attributes
group-alias OpenDNS_Split_Include enable


!--- Split-exclude Configuration
access-list Split_Exclude standard permit <host/subnet>

group-policy OpenDNS_Split_Exclude internal
group-policy OpenDNS_Split_Exclude attributes
wins-server none
dns-server value 198.51.100.11
vpn-tunnel-protocol ssl-client ssl-clientless
 split-tunnel-policy excludespecified
 split-tunnel-network-list value Split_Exclude
webvpn
anyconnect profiles value AnyConnect type user
 anyconnect profiles value OpenDNS type umbrella
!
tunnel-group OpenDNS_Split_Exclude type remote-access
tunnel-group OpenDNS_Split_Exclude general-attributes
address-pool vpn_pool
default-group-policy OpenDNS_Split_Exclude
tunnel-group OpenDNS_Split_Exclude webvpn-attributes
group-alias OpenDNS_Split_Exclude enable
```

```
!--- Tunnelall Configuration
group-policy OpenDNS_Tunnel_All internal
group-policy OpenDNS_Tunnel_All attributes
wins-server none
dns-server value 198.51.100.11
vpn-tunnel-protocol ssl-client ssl-clientless
 split-tunnel-policy tunnelall
webvpn
anyconnect profiles value AnyConnect type user
 anyconnect profiles value OpenDNS type umbrella
!
tunnel-group OpenDNS_Tunnel_All type remote-access
tunnel-group OpenDNS_Tunnel_All general-attributes
address-pool vpn_pool
default-group-policy OpenDNS_Tunnel_All
tunnel-group OpenDNS_Tunnel_All webvpn-attributes
group-alias OpenDNS_Tunnel_All enable
```

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Stappen om problemen met AnyConnect OpenDNS op te lossen zijn:

1. Zorg ervoor dat de Umbrella Roaming security module samen met AnyConnect Secure Mobility Client is geïnstalleerd.
2. Zorg ervoor dat OrgInfo.json op het eindpunt in het juiste pad op basis van het besturingssysteem aanwezig is en in het formaat is gespecificeerd in dit document.
3. Als DNS-vragen naar OpenDNS-resoluties bedoeld zijn om over de AnyConnect VPN-tunnel te gaan, zorg er dan voor dat haarspelden op de ASA zijn geconfigureerd om bereikbaarheid te bieden aan OpenDNS-resoluties.
4. Verzamel tegelijkertijd pakketvastlegging (zonder filters) op de AnyConnect virtuele adapter en fysieke adapter en noteer de domeinen die niet zijn opgelost.
5. Als de Roaming module in een versleutelde staat werkt, verzamelt u pakketvastlegging na het blokkeren van UDP 443 lokaal, alleen voor probleemoplossing. Op die manier wordt de DNS-transacties zichtbaar.
6. Start de diagnostische instellingen AnyConnect DART, Umbrella en noteer de tijd van de DNS-fout. Zie De DART-bundel verzamelen voor meer informatie.
7. Verzamel Umbrella-diagnostische logbestanden en verstuur de resulterende URL naar uw OpenDNS-beheerder. Alleen u en OpenDNS-beheerder hebben toegang tot deze informatie.
   Voor Windows: C:\Program Files (x86)\Cisco\Cisco AnyConnect Secure Mobility Client\UmbrellaDiagnostic.exe
   Voor Mac OSX: /opt/cisco/anyconnect/bin/UmbrellaDiagnostic

Gerelateerde informatie

- **Cisco bug-ID CSCvb34863: Latentie bij het oplossen van DNS wanneer AnyConnect geconfigureerd voor gesplitste tunneling**
- **Technische ondersteuning en documentatie – Cisco Systems**