Interactie tussen AnyConnect en de OpenDNS-roamingclient

Inhoud

Inleiding

Dit document beschrijft een aantal van de huidige beperkingen en beschikbare werkronden om AnyConnect en de OpenDNS-roamingclient samen te maken. Cisco-klanten vertrouwen op de AnyConnect VPN-client voor beveiligde en versleutelde communicatie met hun bedrijfsnetwerken. Op dezelfde manier biedt de OpenDNS-roamingclient gebruikers de mogelijkheid om met behulp van OpenDNS-openbare servers op veilige wijze gebruik te maken van DNS-services. Beide klanten voegen een rijke reeks beveiligingskenmerken toe op het eindpunt, en daarom is het belangrijk voor hen om met elkaar samen te werken.

Voorwaarden

Werken met kennis van de AnyConnect- en OpenDNS-roamingclient.

Bekendheid met ASA of IOS/IOS-XE head-end configuratie (tunnelgroep/groep-beleid) voor AnyConnect VPN.

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- ASA for IOS/IOS-XE head-end
- Endpoint met ondersteuning van de AnyConnect VPN-client en OpenDNS-roaming client

Gebruikte componenten

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

- ASA head-end systeemrelease 9.4
- Windows 7
- AnyConnect-client 4.2.0096
- OpenDNS-roaming-client 2.0.15.4

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 de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

OpenDNS ontwikkelt een AnyConnect-stekker met het Cisco AnyConnect-team dat in de toekomst beschikbaar zal zijn. Hoewel er geen datums zijn ingesteld, kan de roaming-client met de AnyConnect-client werken zonder dat de aangebrachte werkpunten worden gewijzigd. Hierdoor kan AnyConnect ook een leveringsmechanisme voor de roaming-client worden.

Functionaliteit

AnyConnect DNS-verwerking

Het VPN-head-end kan op een paar verschillende manieren worden ingesteld om verkeer vanaf de AnyConnect-client af te handelen.

1. Volledige tunnelconfiguratie (tunnel-all): Dit dwingt al verkeer van het eindpunt om over de VPN tunnel gecodeerd te worden verzonden en daarom verlaat het verkeer nooit de openbare interfaceadapter in duidelijke tekst
2. Taalconfiguratie splitsen:
   a. Split-Inclusief tunneling: Het verkeer is alleen bestemd voor specifieke subnetten of hosts

die op het VPN-head-end zijn gedefinieerd, wordt over de tunnel verzonden, al het andere verkeer wordt buiten de tunnel in duidelijke tekst verzonden

b. tunneling splitter-uitsluiten: Het verkeer dat alleen bestemd is voor specifieke subnetten of hosts die op het VPN-head-end zijn gedefinieerd, is uitgesloten van encryptie en laat de openbare interface in duidelijke tekst achter, al het andere verkeer is versleuteld en alleen verzonden over de tunnel

Elk van deze configuraties bepaalt hoe DNS-resolutie door de AnyConnect-client wordt verwerkt, afhankelijk van het besturingssysteem op het endpointgebeurtenissen. Er is een gedragsverandering in het DNS-verwerkingsmechanisme opgetreden bij AnyConnect voor Windows, in release 4.2 na de tijdelijke oplossing voor CSCuf07885.

Windows 7+

Tunnel-alle configuratie (en gesplitste tunneling met tunnelalle DNS-enabled)

Vooraf AnyConnect 4.2:

Alleen DNS-verzoeken om DNS-servers die zijn geconfigureerd onder het groepsbeleid (DNS-tunnelservers) zijn toegestaan. De AnyConnect-stuurprogramma reageert op alle andere verzoeken met een antwoord op deze naam. Als resultaat hiervan kan DNS-resolutie alleen worden uitgevoerd met behulp van de DNS-tunnelservers.

AnyConnect 4.2 +

DNS-verzoeken aan om het even welke DNS-servers zijn toegestaan, zolang ze afkomstig zijn van de VPN-adapter en verzonden worden over de tunnel. Alle andere verzoeken worden beantwoord met de reactie van 'geen dergelijke naam' en DNS-resolutie kan alleen worden uitgevoerd via de VPN-tunnel

Voorafgaand aan CSCuf0785 fix beperkt AC de DNS-doelservers, maar met de oplossing voor CSCuf07885 beperkt het de netwerkadapters die DNS-verzoeken kunnen initiëren.

Split-Inclusie configuratie (tunnelalle DNS uitgeschakeld en geen gesplitste-DNS)

AnyConnect-stuurprogramma interfereert niet met de native DNS-resolutie. Daarom wordt de DNS-resolutie uitgevoerd in de volgorde van de netwerkadapters en AnyConnect is altijd de gewenste adapter wanneer VPN wordt aangesloten. Dus zal een DNS vraag eerst via de tunnel worden verzonden en als deze niet wordt opgelost zal de resoluut proberen om het via de openbare interface op te lossen. De scheidingslijn-bevat access-list moet het subnetwerk omvatten dat de DNS-server(s) van de Tunnel bestrijkt. Om te beginnen met AnyConnect 4.2 worden de host-routes voor de DNS-server(s) van de Tunnel automatisch toegevoegd als gesplitste netwerken (beveiligde routes) door de AnyConnect-client en vereist de gesplitste toegangslijst niet langer een expliciete toevoeging van de DNS-tunnelsubster.

Configuratie splitter-uitsluiten (tunnelalle DNS uitgeschakeld en geen gesplitste-DNS)

AnyConnect-stuurprogramma interfereert niet met de native DNS-resolutie. Daarom wordt de DNS-resolutie uitgevoerd in de volgorde van de netwerkadapters en AnyConnect is altijd de gewenste adapter wanneer VPN wordt aangesloten. Dus zal een DNS vraag eerst via de tunnel worden verzonden en als deze niet wordt opgelost zal de resoluut proberen om het via de openbare interface op te lossen. De toegangslijst dient niet te bevatten dat het subnetwerk van de DNS-server(s) van de Tunnel dekt. Om te beginnen met AnyConnect 4.2 worden de hostroutes voor de DNS-server(s) van de Tunnel automatisch toegevoegd als gesplitste netwerken (beveiligde routes) door de AnyConnect-client en daarom voorkomt u verkeerde configuratie in de toegangslijst met splitsingen-uitsluitingen.

Split-DNS (tunnelalle DNS uitgeschakeld, gesplitst-inclusief)

Pre AnyConnect 4.2

DNS-verzoeken die de gesplitste DNS-domeinen met elkaar overeenkomen, mogen DNS-servers tunnelbestanden hebben, maar mogen niet op andere DNS-servers worden geplaatst. Om te voorkomen dat dergelijke interne DNS-vragen de tunnel uit lekken, reageert het AnyConnect-stuurprogramma met 'geen dergelijke naam' als de query naar andere DNS-servers wordt verzonden. Dus kunnen gesplitste-dns domeinen alleen worden opgelost via de DNS-tunnelservers.

DNS-verzoeken die de gesplitste-dns-domeinen niet op elkaar afstemmen, zijn toegestaan aan andere DNS-servers, maar er is geen toestemming voor om DNS-servers te tunnelnen. Zelfs in dit geval reageert de AnyConnect-stuurprogramma met 'geen dergelijke naam' als een zoekopdracht voor niet-gesplitste DNS-domeinen via de tunnel wordt uitgevoerd. Dus kunnen niet-gesplitste-dns domeinen alleen worden opgelost via openbare DNS-servers buiten de tunnel.

AnyConnect 4.2 +

DNS-verzoeken om de gesplitste-dns-gebieden aan te passen zijn toegestaan op elke DNS-server, zolang deze afkomstig zijn van de VPN-adapter. Als de query afkomstig is van de openbare interface, reageert AnyConnect-stuurprogramma met een 'dergelijke naam' om de resolutie te dwingen altijd de tunnel te gebruiken voor naamresolutie. Dus gesplitste-dns domeinen kunnen alleen opgelost worden via de tunnel.

DNS-verzoeken die de gesplitste-dns-domeinen niet met elkaar overeenkomen, mogen alleen DNS-servers hebben als ze van de fysieke adapter afkomstig zijn. Als de query gegenereerd wordt door de VPN-adapter, reageert AnyConnect met 'geen dergelijke naam' om de resolutie te dwingen altijd een naam-resolutie te proberen via de openbare interface. Niet-gesplitste gebieden kunnen dus alleen via de openbare interface worden opgelost.

Mac OS X

Tunnel-alle configuratie (en gesplitste tunneling met tunnelalle DNS-enabled)

Wanneer AnyConnect is aangesloten, worden alleen DNS-tunnelservers onderhouden in de DNS-configuratie van het systeem en kunnen DNS-verzoeken alleen naar de DNS-server(s) van de Tunnel worden verzonden.

Split-Inclusie configuratie (tunnelalle DNS uitgeschakeld en geen gesplitste-DNS)

AnyConnect interfereert niet met de native DNS-resolutie. De DNS-tunnelservers zijn ingesteld als voorkeursresoluties, waarbij voorrang wordt gegeven boven openbare DNS-servers, zodat het oorspronkelijke DNS-verzoek om een naamresolutie via de tunnel wordt verzonden. Aangezien DNS-instellingen mondiaal zijn op Mac OS X, is het niet mogelijk voor DNS-vragen om openbare DNS-servers buiten de tunnel te gebruiken zoals gedocumenteerd in CSCtf20226. Om te beginnen met AnyConnect 4.2 worden de host-routes voor de DNS-server(s) van de Tunnel automatisch toegevoegd als gesplitste netwerken (beveiligde routes) door de AnyConnect-client en vereist de gesplitste toegangslijst niet langer een expliciete toevoeging van de DNS-tunnelsubster.

Configuratie splitter-uitsluiten (tunnelalle DNS uitgeschakeld en geen gesplitste-DNS)

AnyConnect interfereert niet met de native DNS-resolutie. De DNS-tunnelservers zijn ingesteld als voorkeursresoluties, waarbij voorrang wordt gegeven boven openbare DNS-servers, zodat het oorspronkelijke DNS-verzoek om een naamresolutie via de tunnel wordt verzonden. Aangezien DNS-instellingen mondiaal zijn op Mac OS X, is het niet mogelijk voor DNS-vragen om openbare DNS-servers buiten de tunnel te gebruiken zoals gedocumenteerd in CSCtf20226. Om te beginnen met AnyConnect 4.2 worden de host-routes voor de DNS-server(s) van de Tunnel automatisch toegevoegd als gesplitste netwerken (beveiligde routes) door de AnyConnect-client en vereist de gesplitste toegangslijst niet langer een expliciete toevoeging van de DNS-tunnelsubster.

Split-DNS (tunnelalle DNS uitgeschakeld, gesplitst-inclusief)

Als split-DNS is ingeschakeld voor zowel IP-protocollen (IPv4 en IPv6) of het is alleen ingeschakeld voor één protocol en er is geen adrepool ingesteld voor het andere protocol:
True split-DNS, vergelijkbaar met Windows, wordt gehandhaafd. True split-DNS betekent dat verzoeken om de gesplitste-DNS-domeinen alleen via de tunnel worden opgelost, maar niet op DNS-servers buiten de tunnel worden gelekt.

Als split-DNS beschikbaar is voor slechts één protocol en er een clientadres is toegewezen voor het andere protocol, wordt alleen "DNS fallback for split-tunneling" uitgevoerd. Dit betekent dat alleen AC DNS-verzoeken die de gesplitste-DNS-domeinen via tunnels aanpassen (andere verzoeken worden door AC geantwoord met "geweigerd" reactie op force failover naar openbare DNS-servers), maar kunnen niet afdwingen dat verzoeken om gesplitste-DNS-domeinen niet duidelijk worden verstuurd via de openbare adapter.

Linux

Tunnel-alle configuratie (en gesplitste tunneling met tunnelalle DNS-enabled)

Wanneer AnyConnect is aangesloten, worden alleen DNS-tunnelservers onderhouden in de DNS-configuratie van het systeem en kunnen DNS-verzoeken alleen naar de DNS-server(s) van de Tunnel worden verzonden.

Split-Inclusie configuratie (tunnelalle DNS uitgeschakeld en geen gesplitste-DNS)

AnyConnect interfereert niet met de native DNS-resolutie. De DNS-tunnelservers zijn ingesteld als voorkeursresoluties, waarbij voorrang wordt gegeven boven openbare DNS-servers, zodat het oorspronkelijke DNS-verzoek om een naamresolutie via de tunnel wordt verzonden.

Configuratie splitter-uitsluiten (tunnelalle DNS uitgeschakeld en geen gesplitste-DNS)

AnyConnect interfereert niet met de native DNS-resolutie. De DNS-tunnelservers zijn ingesteld als voorkeursresoluties, waarbij voorrang wordt gegeven boven openbare DNS-servers, zodat het oorspronkelijke DNS-verzoek om een naamresolutie via de tunnel wordt verzonden.

Split-DNS (tunnelalle DNS uitgeschakeld, gesplitst-inclusief)

Als split-DNS is ingeschakeld, wordt alleen "DNS-back-up voor split-tunneling" gehandhaafd. Dit betekent dat alleen AC DNS-verzoeken die de gesplitste-DNS-domeinen via tunnels aanpassen (andere verzoeken worden door AC geantwoord met "geweigerd" reactie op force failover naar openbare DNS-servers), maar kunnen niet afdwingen dat verzoeken om gesplitste-DNS-domeinen niet duidelijk worden verstuurd via de openbare adapter.

OpenDNS-roaming-client

De roaming-client is een stuk software die de DNS-services op het eindpunt beheert en de OpenDNS-openbare DNS-servers gebruikt om DNS-verkeer te beveiligen en te versleutelen.

Idealiter zou de client in een beschermde en gecodeerde staat moeten zijn. Als de client echter geen TLS-sessie met de OpenDNS-server (208.67.222.222) kan opzetten, probeert deze client DNS-verkeer zonder encryptie op UDP-poort 53 naar 208.67.222.222 te verzenden. De client gebruikt uitsluitend het openbare DNS-adres van OpenDNS 208.67.222.222 (er zijn een paar andere, zoals 208.67.220.220, 208.67.222.220 en 208.67.220.222). De roaming-client nadat deze geïnstalleerd is, stelt 127.0.0.1 (lokale host) in als de lokale DNS-server en voert de huidige DNS-instellingen per interface-over. Huidige DNS-instellingen worden opgeslagen in lokale resoluv.conf-bestanden (zelfs op Windows) in de configuratiemap van de client voor roaming. OpenDNS maakt een back-up van zelfs de DNS-servers die u via de AnyConnect-adapter hebt geleerd. Als 192.168.92.2 bijvoorbeeld de DNS-server op de openbare adapter is, dan maakt OpenDNS op de volgende locatie de resolutie.conf:

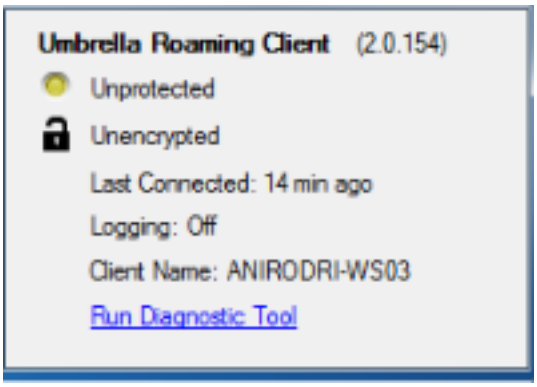
C:\ProgramData\OpenDNS\ERC\Resolver1-LocalAreaConnection-resolv.conf
server 192 168 92.2

De roamende client versleutelt elk pakket dat op OpenDNS is ingesteld. zij start of gebruikt echter geen encryptietunnel tot 208.67.222.222 . De client voor roaming heeft wel een optionele functie voor IP Layer Encapsulation die een IPSec-verbinding opent voor niet-DNS-doeleinden om IP-adressen te blokkeren. Dit schakelt automatisch uit in aanwezigheid van een actieve AnyConnect-verbinding. Het bindt ook aan 127.0.1:53 om vragen te ontvangen die lokaal op de computer gegenereerd worden. Wanneer het eindpunt een naam moet oplossen, worden de lokale vragen naar 127.0.0.1 gericht door de opheffing, en dan het onderliggende decrypt-proxy van de Roaming Client hen naar de OpenDNS openbare servers via het gecodeerde kanaal door te sturen.

Als DNS niet naar 127.0.0.1:53 mag stromen, kan de roaming-client niet werken en gebeurt het volgende. Als de client niet in staat is om de openbare DNS-servers of het 127.0.0.1:53-adres te bereiken, wordt er overgeschakeld naar een openstaande DNS-status en worden de DNS-instellingen op de lokale adapters hersteld. Op de achtergrond blijft het project sondes naar 208.67.222.222 doorsturen en kan het overgaan naar actieve modus indien de beveiligde verbinding wordt hersteld.

Beperkingen

Gezien de hoge functionaliteit van beide klanten is het duidelijk dat de roamende klant de mogelijkheid moet hebben om de lokale DNS-instellingen te wijzigen en gebonden te zijn aan 127.0.0.1:53 om vragen over het beveiligde kanaal door te sturen. Wanneer VPN is aangesloten, zijn de enige configuraties waar AnyConnect niet interfereert met de native DNS-resolutie de gesplitste-inclusie en gesplitste-uitsluiting (met gesplitste-tunnel-alle DNS-uitgeschakeld). Daarom wordt momenteel aanbevolen één van deze configuraties te gebruiken wanneer de roamende klant ook in gebruik is. De client voor roaming blijft onbeveiligd/niet-versleuteld als de tunnelconfiguratie wordt gebruikt of als alle DNS-tunneltunnel is ingeschakeld, zoals in de afbeelding wordt getoond.



Werken

Als de bedoeling is om communicatie tussen de roaming-client en OpenDNS-servers te beschermen met behulp van de VPN-tunnel, dan kan een dummy split-Expliciete toegangslijst worden gebruikt op het VPN-head-end. Dit is het dichtste bij een volledige tunnelconfiguratie. Als dergelijke vereisten niet bestaan, kan de splitsing-inclusie worden gebruikt wanneer de toegangslijst niet de OpenDNS-openbare servers bevat, of kan de split-exclusion worden gebruikt wanneer de toegangslijst de OpenDNS-openbare servers bevat.

Bovendien kunnen gesplitste-DNS-modi bij gebruik van de client voor roaming niet worden gebruikt, omdat de lokale DNS-resolutie hierdoor verloren gaat. Ook Split-tunnel-alle DNS moet worden uitgeschakeld; het wordt echter gedeeltelijk ondersteund en moet de roaming-client in staat stellen gecodeerde post-failover te worden.

Configuraties

Tunnel OpenDNS-verkeer

Dit voorbeeld gebruikt een dummy IP adres in de gesplitste-uitsluitings toegangslijst. Met deze configuratie gebeurt alle communicatie met 208.67.222.22 in de VPN-tunnel en werkt de roamende klant in een versleutelde en beschermde toestand.

```
ciscoasa# sh run access-li split
access-list split standard permit host 2.2.2.2

ciscoasa# sh run group-policy
group-policy GroupPolicy-OpenDNS internal
group-policy GroupPolicy-OpenDNS attributes
 wins-server none
 dns-server value 1.1.1.1
 vpn-tunnel-protocol ssl-client
 split-tunnel-policy excludespecified
 split-tunnel-network-list value split
 default-domain value cisco.com
 address-pools value acpool
 webvpn
 anyconnect profiles value AnyConnect type user
ciscoasa#
```

OpenDNS-verkeer uitsluiten van VPN-tunnelknooppunt

Dit voorbeeld gebruikt het adres van de OpenDNS oplossing in de gesplitste-uitsluitings access-lijst. Met deze configuratie gebeurt alle communicatie met 208.67.222.222 buiten de VPN-tunnel en werkt de roamende klant in een versleutelde en beschermde toestand.

```
ciscoasa# sh run access-li split
access-list split standard permit host 208.67.222.222

ciscoasa# sh run group-policy
group-policy GroupPolicy-OpenDNS internal
group-policy GroupPolicy-OpenDNS attributes
 wins-server none
 dns-server value 1.1.1.1
 vpn-tunnel-protocol ssl-client
 split-tunnel-policy excludespecified
 split-tunnel-network-list value split
 default-domain value cisco.com
 address-pools value acpool
 webvpn
 anyconnect profiles value AnyConnect type user
ciscoasa#
```

Dit voorbeeld toont een gespleten-omvat configuratie voor intern 192.168.1.0/24 subnet. Met deze configuratie zal de roamende klant nog steeds in een versleutelde en beschermde staat opereren, aangezien het verkeer naar 208.67.222.222 niet via de tunnel wordt verstuurd.

```
ciscoasa# sh run access-li split
access-list split standard permit 192.168.1.0 255.255.255.0

ciscoasa# sh run group-policy
group-policy GroupPolicy-OpenDNS internal
group-policy GroupPolicy-OpenDNS attributes
 wins-server none
 dns-server value 1.1.1.1
 vpn-tunnel-protocol ssl-client
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value split
 default-domain value cisco.com
 address-pools value acpool
 webvpn
 anyconnect profiles value AnyConnect type user
ciscoasa#
```

Note: Split-tunnel-all-dns must be disabled in all of the scenarios

Verifiëren

Wanneer VPN is aangesloten, dient de roaming-client beveiligd en versleuteld te tonen zoals in deze afbeelding: