Onderzoek het gedrag van DNS-vragen en de resolutie van de domeinnaam

Inhoud

Inleiding

Dit document beschrijft hoe Cisco OS® DNS-vragen en de effecten op de resolutie van domeinnamen verwerkt met Cisco AnyConnect en splitter of volledige tunneling.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

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.

Splitsen op standaardDNS

Wanneer u gesplitste tunneling gebruikt, zijn dit de drie opties die u hebt voor het Domain Name System (DNS):

1. Split DNS - De DNS-vragen die overeenkomen met de domeinnamen, worden ingesteld op de Cisco adaptieve security applicatie (ASA). Zij bewegen zich door de tunnel (naar de DNS servers die zijn gedefinieerd op de ASA, bijvoorbeeld) terwijl anderen dat niet doen.

2. Tunnel-all-DNS - alleen DNS-verkeer naar de DNS-servers die door de ASA zijn gedefinieerd, is toegestaan. Deze instelling wordt ingesteld in het groepsbeleid.

3. Standaard DNS - Alle DNS-query's worden door de DNS-servers die door de ASA worden gedefinieerd. In het geval van een negatieve reactie, kunnen de DNS vragen ook naar de DNS servers gaan die op de fysieke adapter worden gevormd.

Opmerking: De opdracht gesplitste tunnels-all-dns werd voor het eerst geïmplementeerd in ASA versie 8.2(5). Voor deze versie kon je alleen gesplitste DNS of standaard DNS doen.

In alle gevallen, de DNS vragen die worden bepaald om zich door de tunnel te bewegen, gaan naar om het even welke DNS servers die door ASA worden bepaald. Als er geen DNS-servers zijn gedefinieerd door de ASA, zijn de DNS-instellingen leeg voor de tunnel. Als u geen gesplitste DNS hebt gedefinieerd, worden alle DNS-vragen naar de DNS-servers verzonden die door de ASA worden gedefinieerd. De gedragingen die in dit document worden beschreven, kunnen echter afwijken, op basis van het besturingssysteem.

Opmerking: Vermijd het gebruik van de NSLookup wanneer u de naamresolutie op de client test. Vertrouw in plaats daarvan op een browser of gebruik de ping-opdracht. Dit komt doordat NSLookup niet afhankelijk is van de OS DNS-resolutie. AnyConnect dwingt het DNS-verzoek niet via een bepaalde interface maar staat het toe of verwerpt het afhankelijk van de gesplitste DNS-configuratie. Om DNS resolver te dwingen om een acceptabele DNS-server voor een verzoek te proberen, is het belangrijk dat gesplitste DNS-testen alleen wordt uitgevoerd met toepassingen die vertrouwen op de native DNS-resolver voor domeinnaamresolutie (alle toepassingen behalve NSLookup, Dig en soortgelijke toepassingen die DNS-resolutie zelf behandelen, bijvoorbeeld).

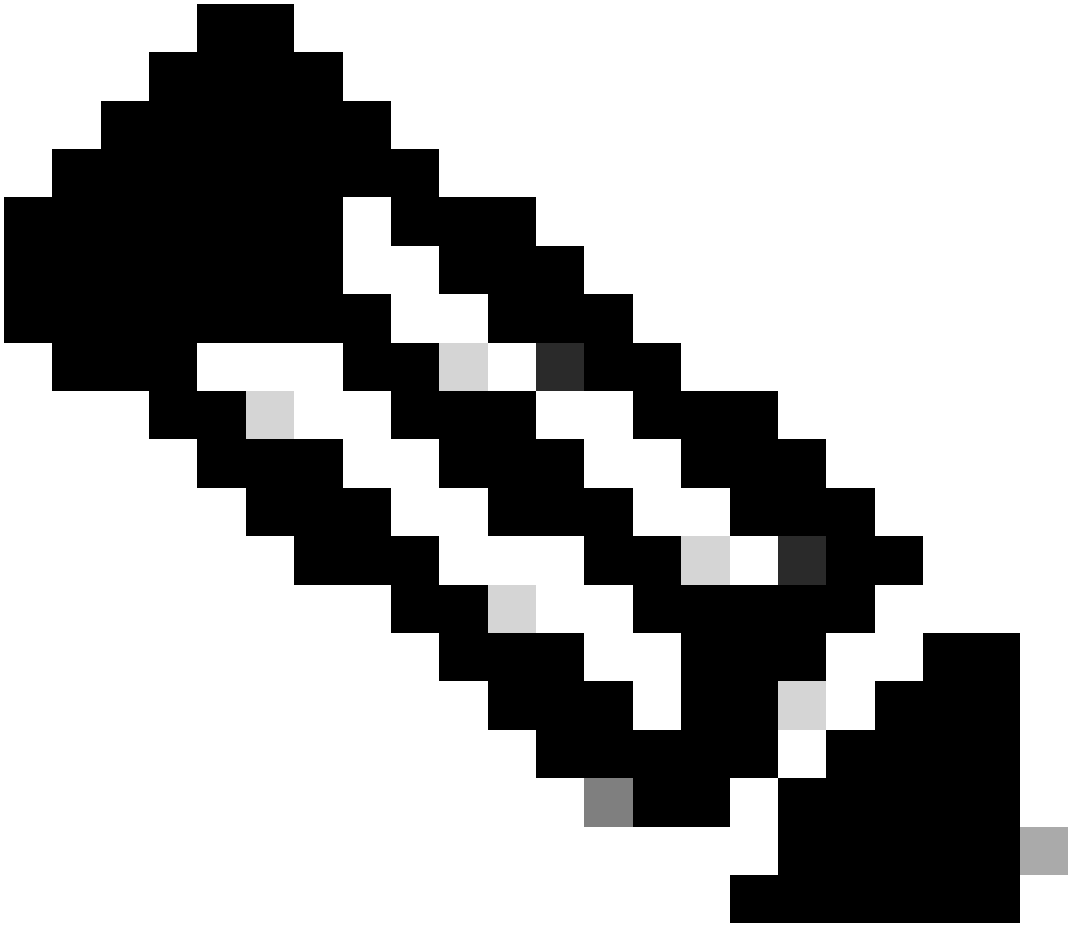
Waar versus beste inspanning splitter DNS

AnyConnect release 2.4 ondersteunt gesplitste DNS-reserve (best practice split DNS), wat niet de echte gesplitste DNS is en wordt gevonden in de legacy IPsec-client. Als het verzoek overeenkomt met een gesplitste DNS-domein, laat AnyConnect het verzoek toe om in de ASA te worden getunneld. Als de server de hostnaam niet kan oplossen, gaat de DNS-resoluver verder en verstuurt dezelfde query naar de DNS-server die wordt toegewezen aan de fysieke interface.

Aan de andere kant, als het verzoek niet overeenkomt met een van de gesplitste DNS-domeinen, AnyConnect tunnelt het niet in de ASA. In plaats daarvan, bouwt het een DNS reactie zodat DNS resolver terugvalt en de vraag naar de DNS server verzendt die aan de fysieke interface in kaart wordt gebracht. Dat is de reden waarom deze functie niet gesplitste DNS wordt genoemd, maar DNS-fall-back voor gesplitste tunneling. Niet alleen zorgt AnyConnect ervoor dat alleen verzoeken dat doel gesplitste DNS-domeinen worden ingetunneld, het is ook afhankelijk van het client-OS DNS-oplossingsgedrag voor de resolutie van de hostnaam.

Dit leidt tot beveiligingsproblemen als gevolg van een mogelijk lek van een particuliere domeinnaam. De native DNS-client kan bijvoorbeeld een query voor een private domeinnaam naar een openbare DNS-server sturen, specifiek wanneer de VPN DNS-naamserver de DNS-query niet kan oplossen.

Raadpleeg Cisco-bug-id CSCtn14578, momenteel alleen opgelost op Microsoft Windows, vanaf versie 3.0(4235). De oplossing implementeert ware gesplitste DNS, het strikt de gevormde domeinnamen die overeenkomen en toegestaan aan de VPN DNS servers. Alle andere vragen zijn alleen toegestaan aan andere DNS-servers, zoals de vragen die zijn geconfigureerd op de fysieke adapter(s).



Opmerking: alleen geregistreerde Cisco-gebruikers hebben toegang tot interne Cisco-tools en -informatie.

Tunnel-alle en Tunnel-alle DNS

Wanneer gesplitste tunneling is uitgeschakeld (de configuratie van tunnels), is DNS-verkeer alleen via tunnels toegestaan. De Tunnel-alle DNS configuratie (die in het groepsbeleid wordt gevormd) verzendt alle DNS raadplegingen door de tunnel, samen met één of ander type van gespleten tunneling, en DNS het verkeer wordt strikt via tunnel toegestaan.

Dit is consistent voor alle platforms met één waarschuwing op Microsoft Windows: wanneer een tunnelall of tunnelall DNS is geconfigureerd, staat AnyConnect alleen DNS-verkeer toe naar de DNS-servers die zijn geconfigureerd op de beveiligde gateway (toegepast op de VPN-adapter). Dit is een beveiligingsverbetering die samen met de eerder vermelde ware gesplitste DNS-oplossing wordt geïmplementeerd.

Als dit in bepaalde scenario's problematisch blijkt (er moeten bijvoorbeeld DNS-update-

/registratieaanvragen naar niet-VPN DNS-servers worden verzonden), moet u deze stappen uitvoeren:

1. Als de huidige configuratie tunnel-allen is, dan laat spleet-exclusief het een tunnel graven toe . Om het even welk enig-gastheer, spleet-sluit netwerk uit is aanvaardbaar voor gebruik, zoals een verbinding-lokaal adres.

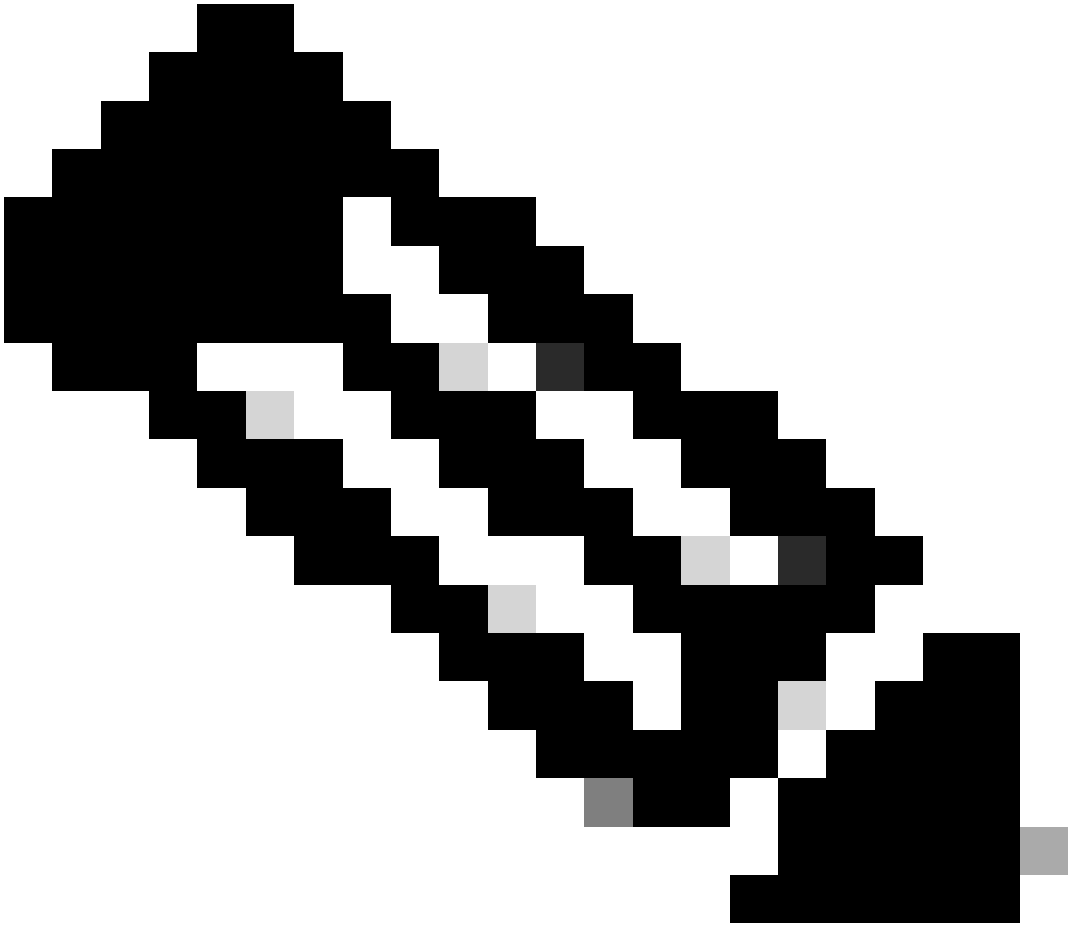
2. Zorg ervoor dat Tunnel-all DNS niet is geconfigureerd in het groepsbeleid.

Problemen met DNS-prestaties opgelost in AnyConnect versie 3.0(4235)

Deze Microsoft Windows-kwestie komt onder deze omstandigheden meestal voor:

- Bij de installatie van de thuisrouter worden de DNS- en DHCP-servers toegewezen aan hetzelfde IP-adres (AnyConnect maakt een noodzakelijke route naar de DHCP-server).
- Een groot aantal DNS-domeinen zit in het groepsbeleid.
- Er wordt een tunnelall-configuratie gebruikt.
- De naamresolutie wordt uitgevoerd door een niet-gekwalificeerde hostnaam, wat impliceert dat de resolver een aantal DNS-achtervoegsels op alle beschikbare DNS-servers moet proberen totdat de voor de gevraagde hostnaam relevante naam wordt geprobeerd. Dit probleem is te wijten aan de native DNS-client die probeert DNS-vragen te verzenden via de fysieke adapter, die AnyConnect blokkeert (gezien de Tunnel-all configuratie). Dit leidt tot een vertraging van de naamresolutie die significant kan zijn, vooral als een groot aantal DNS achtervoegsels door het uiteinde worden geduwd. De DNS-client moet door alle vragen en beschikbare DNS-servers lopen tot het een positieve reactie ontvangt.

Dit probleem wordt opgelost in AnyConnect versie 3.0(4235). Raadpleeg Cisco bug-id's CSCtq02141 en Cisco bug-id CSCtn14578, samen met de inleiding tot de eerder genoemde ware gesplitste DNS-oplossing, voor meer informatie.



Opmerking: alleen geregistreerde Cisco-gebruikers hebben toegang tot interne Cisco-tools en -informatie.

Als een upgrade niet kan worden geïmplementeerd, zijn dit de mogelijke tijdelijke oplossingen:

- Schakel split-exclusion-tunneling in voor een IP-adres, waarmee lokale DNS-verzoeken door de fysieke adapter kunnen stromen. U kunt een adres van linklocal subnetnet 169.254.0.0/16 gebruiken omdat het onwaarschijnlijk is dat een apparaat verkeer naar een van die IP-adressen via VPN verstuurt. Nadat u de tunneling van splitsen en uitsluiten hebt ingeschakeld, schakelt u lokale LAN-toegang in op het clientprofiel of op de client zelf en schakelt u Tunnel-alle dDNS uit.

  Wijzig de configuratie van de ASA als volgt:

```
access-list acl_linklocal_169.254.1.1 standard permit host 169.254.1.1
 group-policy gp_access-14 attributes
```

```
 split-tunnel-policy excludespecified
 split-tunnel-network-list value acl_linklocal_169.254.1.1
 split- Tunnel-all-dns disable
exit
```

In het clientprofiel moet u deze regel toevoegen:

```
<LocalLanAccess UserControllable="true">true</LocalLanAccess>
```

U kunt dit ook per client inschakelen in de AnyConnect-client GUI. Navigeer naar het menu Voorkeuren AnyConnect en controleer het vakje Lokale LAN-toegang inschakelen.

- Gebruik de volledig gekwalificeerde domeinnamen (FQDN's) in plaats van de ongekwalificeerde hostnamen voor de naamresoluties.
- Gebruik een ander IP-adres voor de DNS-server op de fysieke interface.

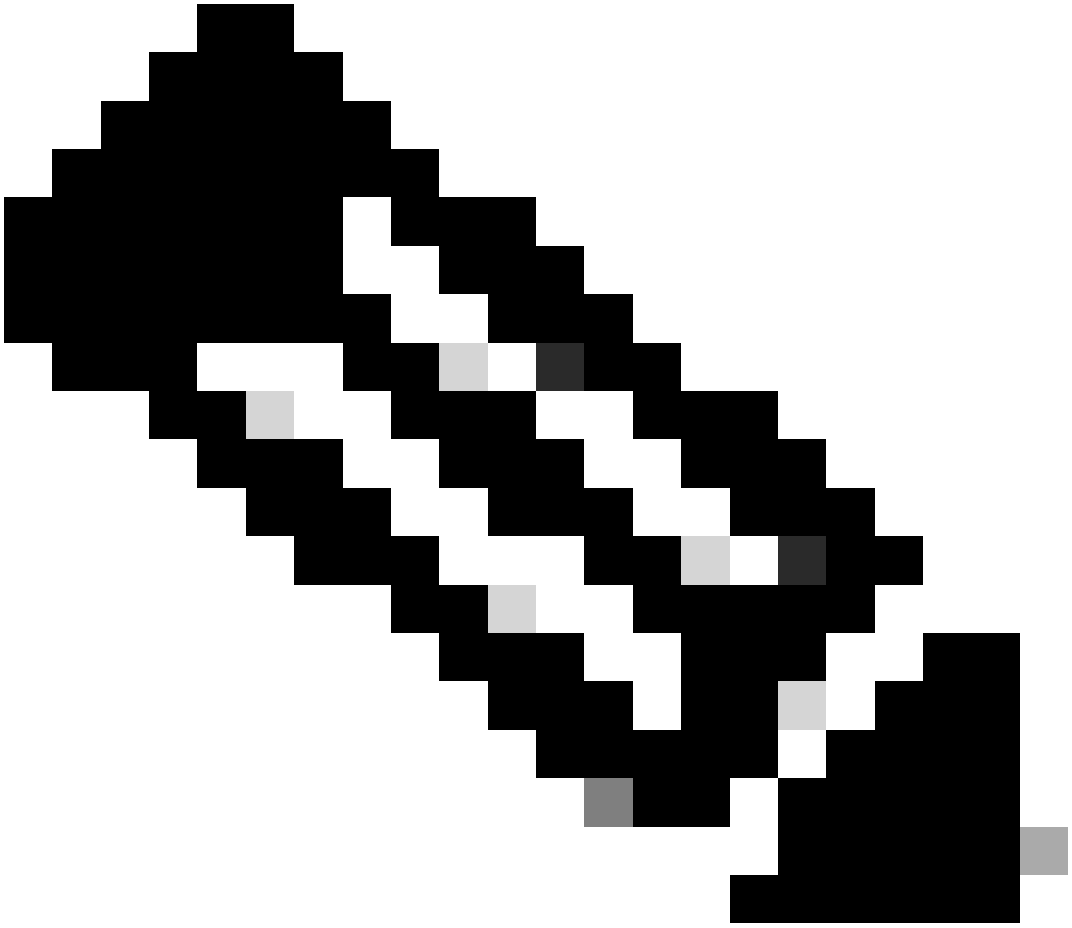
DNS met Split-tunneling op verschillende Cisco-besturingssystemen

De verschillende Cisco OS-handleidingen voor DNS-zoekopdrachten op verschillende manieren bij gebruik van gesplitste tunneling (zonder gesplitste DNS) voor AnyConnect. In dit deel worden deze verschillen beschreven.

Microsoft Windows

Op Microsoft Windows-systemen zijn DNS-instellingen per interface. Als gesplitste tunneling wordt gebruikt, kunnen DNS-vragen terugvallen op de fysieke adaptor DNS-servers nadat ze zijn mislukt op de VPN-tunneladapter. Als gesplitste tunneling zonder gesplitste DNS is gedefinieerd, werkt zowel interne als externe DNS-resolutie omdat deze terugvalt naar de externe DNS-servers.

Er is een verandering in gedrag in het DNS mechanisme dat dit op AnyConnect voor Windows, in versie 4.2 na de moeilijke situatie voor Cisco bug-id CSCuf07885 behandelt.



Opmerking: alleen geregistreerde Cisco-gebruikers hebben toegang tot interne Cisco-tools en -informatie.

Windows 7+

Tunnel-alle configuratie (en split-tunneling met tunnel-alle DNS ingeschakeld)

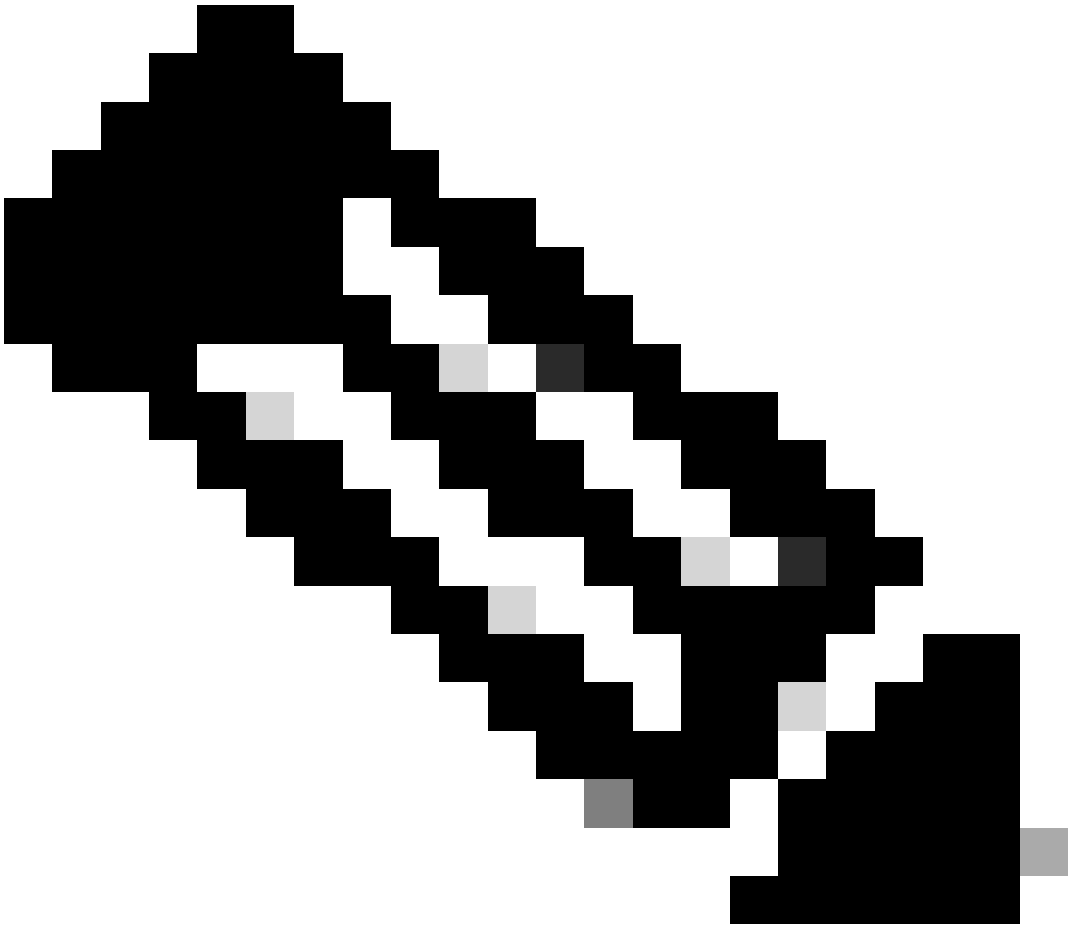
Pre AnyConnect 4.2:

Alleen DNS-verzoeken naar DNS-servers die zijn geconfigureerd onder het groepsbeleid (tunnelDNS-servers) zijn toegestaan. Het AnyConnect-stuurprogramma reageert op alle andere verzoeken met een antwoord van "geen dergelijke naam". Hierdoor kan DNS-resolutie alleen worden uitgevoerd met de DNS-tunnelservers.

AnyConnect 4.2 +

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

Voorafgaand aan Cisco bug ID CSCuf07885 fix, AC beperkt de doel DNS servers, maar met de fix voor deze bug, het nu beperkt welke netwerkadapters DNS verzoeken kunnen initiëren.



> Opmerking: alleen geregistreerde Cisco-gebruikers hebben toegang tot interne Cisco-tools en -informatie.

Splitsen-inclusief configuratie (tunnel-alle DNS uitgeschakeld en geen splitsen-DNS)

AnyConnect-stuurprogramma interfereert niet met de native DNS-oplosser. Daarom wordt DNS-resolutie uitgevoerd op basis van de volgorde van netwerkadapters, waarbij AnyConnect altijd de

voorkeursadapter is wanneer VPN is verbonden. Bovendien wordt eerst een DNS-query verzonden via de tunnel en als deze niet wordt opgelost, probeert de resolver dit via de openbare interface op te lossen. De opgesplitste toegangslijst omvat het subnet dat de tunnelDNS-server(s) omvat. Om met AnyConnect 4.2 te beginnen, worden hostroutes voor de Tunnel DNS-server(s) automatisch toegevoegd als split-include-netwerken (beveiligde routes) door de AnyConnect-client. Daarom vereist de split-include-toegangslijst geen expliciete toevoeging van de tunnel-DNS-serversubnet.

Configuratie splitsen-uitsluiten (tunnel-alle DNS uitgeschakeld en geen splitsen-DNS)

AnyConnect-stuurprogramma interfereert niet met de native DNS-oplosser. Daarom wordt DNS-resolutie uitgevoerd op basis van de volgorde van netwerkadapters, waarbij AnyConnect altijd de voorkeursadapter is wanneer VPN is verbonden. Bovendien wordt eerst een DNS-query verzonden via de tunnel en als deze niet wordt opgelost, probeert de resolver dit via de openbare interface op te lossen. De gesplitste toegangslijst met uitsluitingen mag niet de sublijst bevatten die de DNS-server(s) van de tunnel bedekt. Om met AnyConnect 4.2 te beginnen, worden hostroutes voor de Tunnel DNS-server(s) automatisch toegevoegd als split-include-netwerken (beveiligde routes) door de AnyConnect-client en voorkomt zo een foutieve configuratie in de split-exclusion-toegangslijst.

Split-DNS (tunnel-alle DNS uitgeschakeld, splitsen-omvatten geconfigureerd)

Pre AnyConnect 4.2

DNS-verzoeken, die overeenkomen met de split-dns-domeinen, mogen DNS-servers tunnelen, maar mogen niet worden gebruikt voor andere DNS-servers. Om te voorkomen dat dergelijke interne DNS-vragen de tunnel uitlekken, reageert het AnyConnect-stuurprogramma met "geen dergelijke naam" als de query naar andere DNS-servers wordt verzonden. Daarom kunnen de split-dns domeinen alleen worden opgelost via tunnelDNS-servers.

DNS-verzoeken, die niet overeenkomen met de split-dns-domeinen, zijn toegestaan aan andere DNS-servers, maar mogen DNS-servers niet tunnelen. Zelfs in dit geval reageert het AnyConnect-stuurprogramma met "geen dergelijke naam" als via de tunnel wordt geprobeerd een zoekopdracht uit te voeren voor niet-splitsdns-domeinen. Daarom kunnen de niet splitsen-dns domeinen alleen worden opgelost via openbare DNS-servers buiten de tunnel.

AnyConnect 4.2 +

DNS-verzoeken, die overeenkomen met de splitsen-dns-domeinen, zijn toegestaan op alle DNS-servers, zolang ze afkomstig zijn van de VPN-adapter. Als de query afkomstig is van de openbare interface, AnyConnect-stuurprogramma reageert met een "geen dergelijke naam" om de oplosser te dwingen altijd de tunnel te gebruiken voor naamresolutie. Daarom kunnen de split-dns domeinen alleen worden opgelost via een tunnel.

DNS-verzoeken, die niet overeenkomen met de split-dns-domeinen, zijn toegestaan aan DNS-servers zolang ze afkomstig zijn van de fysieke adapter. Als de query afkomstig is van de VPN-adapter, reageert AnyConnect met "geen dergelijke naam" om de resolutor te dwingen altijd de naamresolutie te proberen via de openbare interface. Daarom kunnen de niet opgesplitste domeinen alleen worden opgelost via de openbare interface.

Mac OSx

Op Macintosh-systemen zijn de DNS-instellingen wereldwijd. Als gesplitste tunneling wordt gebruikt, maar gesplitste DNS niet wordt gebruikt, is het niet mogelijk voor de DNS-vragen om DNS-servers buiten de tunnel te bereiken. Je kunt dit alleen intern oplossen, niet extern.

Dit is gedocumenteerd in Cisco bug-id CSC2026 en Cisco bug-id CSC86314. In beide gevallen moet deze tijdelijke oplossing het probleem oplossen:

- Specificeer een extern DNS server IP-adres onder het groepsbeleid en gebruik een FQDN voor de interne DNS-vragen.

- Als de externe namen oplosbaar zijn door de tunnel, navigeer dan naar Advanced > Split Tunneling en schakel gesplitste DNS via verwijdering van de DNS namen die in het groepsbeleid zijn geconfigureerd uit. Dit vereist het gebruik van een FQDN voor de interne DNS-vragen.

De gesplitste DNS-case wordt opgelost in AnyConnect versie 3.1. U moet er echter voor zorgen dat aan een van deze voorwaarden wordt voldaan:

- Split-DNS moet zijn ingeschakeld voor beide IP-protocollen, waarvoor Cisco ASA versie 9.0 of hoger is vereist.

- Split DNS moet voor één IP-protocol zijn ingeschakeld. Als u Cisco ASA versie 9.0 of hoger uitvoert, gebruikt u het clientomzeilprotocol voor het andere IP-protocol. Zorg er bijvoorbeeld voor dat er geen adrespool is en dat Client Bypass Protocol is ingeschakeld in het groepsbeleid. Als u echter een ASA-versie uitvoert die eerder is dan Versie 9.0, dient u ervoor te zorgen dat er geen adrespool is geconfigureerd voor het andere IP-protocol. Dit houdt in dat het andere IP-protocol IPv6 is.

Opmerking: AnyConnect verandert het resolv.conf-bestand op Macintosh OS X niet, maar wijzigt eerder de OS X-specifieke DNS-instellingen. Macintosh OS X houdt het resolv.conf bestand actueel om compatibiliteitsredenen. Gebruik de opdracht scutil —dns om de DNS-instellingen te bekijken op Macintosh OS X.

Tunnel-alle configuratie (en split-tunneling met tunnel-alle DNS ingeschakeld)

Wanneer AnyConnect is verbonden, worden alleen tunnelDNS-servers onderhouden in de systeem-DNS-configuratie en kunnen DNS-verzoeken daarom alleen worden verzonden naar de

tunnelDNS-server(s).

Splitsen-inclusief configuratie (tunnel-alle DNS uitgeschakeld en geen splitsen-DNS)

AnyConnect interfereert niet met de native DNS-oplosser. De tunnelDNS-servers worden geconfigureerd als voorkeursleveranciers, die voorrang hebben op openbare DNS-servers, zodat het initiële DNS-verzoek om een naamresolutie via de tunnel wordt verzonden. Aangezien DNS-instellingen wereldwijd worden gebruikt op Mac OS X, is het niet mogelijk voor DNS-vragen om openbare DNS-servers buiten de tunnel te gebruiken zoals gedocumenteerd in Cisco bug-id CSCtf20226 . Om met AnyConnect 4.2 te beginnen, worden hostroutes voor de Tunnel DNS-server(s) automatisch toegevoegd als split-include-netwerken (beveiligde routes) door de AnyConnect-client. Daarom vereist de split-include-toegangslijst geen expliciete toevoeging van de tunnel-DNS-serversubnet.

Configuratie splitsen-uitsluiten (tunnel-alle DNS uitgeschakeld en geen splitsen-DNS)

AnyConnect interfereert niet met de native DNS-oplosser. De tunnelDNS-servers worden geconfigureerd als voorkeursresolvers, ze hebben voorrang op openbare DNS-servers, zodat het initiële DNS-verzoek om een naamresolutie via de tunnel wordt verzonden. Aangezien DNS-instellingen wereldwijd worden gebruikt op Mac OS X, is het niet mogelijk voor DNS-vragen om openbare DNS-servers buiten de tunnel te gebruiken zoals gedocumenteerd in Cisco bug-id CSCtf20226 . Om met AnyConnect 4.2 te beginnen, worden hostroutes voor de Tunnel DNS-server(s) automatisch toegevoegd als split-include-netwerken (beveiligde routes) door de AnyConnect-client. Daarom vereist de split-include-toegangslijst geen expliciete toevoeging van de tunnel-DNS-serversubnet.

Split-DNS (tunnel-alle DNS uitgeschakeld, splitsen-omvatten geconfigureerd)

Als split-DNS is ingeschakeld voor zowel IP-protocollen (IPv4 als IPv6) of alleen voor één protocol en er is geen adrespool geconfigureerd voor het andere protocol:
Echte split-DNS, vergelijkbaar met Windows, wordt afgedwongen. Ware split-DNS betekent dat verzoeken die overeenkomen met de split-DNS-domeinen alleen worden opgelost via de tunnel, ze worden niet uitgelekt naar DNS-servers buiten de tunnel.

Als split-DNS voor slechts één protocol is ingeschakeld en een clientadres voor het andere protocol is toegewezen, wordt alleen DNS-fallback voor split-tunneling afgedwongen. Dit betekent dat AC alleen DNS-verzoek toestaat dat overeenkomt met de split-DNS-domeinen via de tunnel (andere verzoeken worden door AC beantwoord met "geweigerd" antwoord op force failover naar openbare DNS-servers), maar niet het verzoek kan afdwingen dat overeenkomt met de split-DNS-domeinen die niet in het duidelijke, via de openbare adapter worden verzonden.

Linux

Tunnel-alle configuratie (en split-tunneling met tunnel-alle DNS ingeschakeld)

Wanneer AnyConnect is verbonden, worden alleen tunnelDNS-servers onderhouden in de systeem-DNS-configuratie en kunnen DNS-verzoeken daarom alleen worden verzonden naar de tunnelDNS-server(s).

Splitsen-inclusief configuratie (tunnel-alle DNS uitgeschakeld en geen splitsen-DNS)

AnyConnect interfereert niet met de native DNS-oplosser. De tunnelDNS-servers worden geconfigureerd als voorkeursleveranciers, die voorrang hebben op openbare DNS-servers, zodat het initiële DNS-verzoek om een naamresolutie via de tunnel wordt verzonden.

Configuratie splitsen-uitsluiten (tunnel-alle DNS uitgeschakeld en geen splitsen-DNS)

AnyConnect interfereert niet met de native DNS-oplosser. De tunnelDNS-servers worden geconfigureerd als voorkeursleveranciers, die voorrang hebben op openbare DNS-servers, zodat het initiële DNS-verzoek om een naamresolutie via de tunnel wordt verzonden.

Split-DNS (tunnel-alle DNS uitgeschakeld, splitsen-omvatten geconfigureerd)

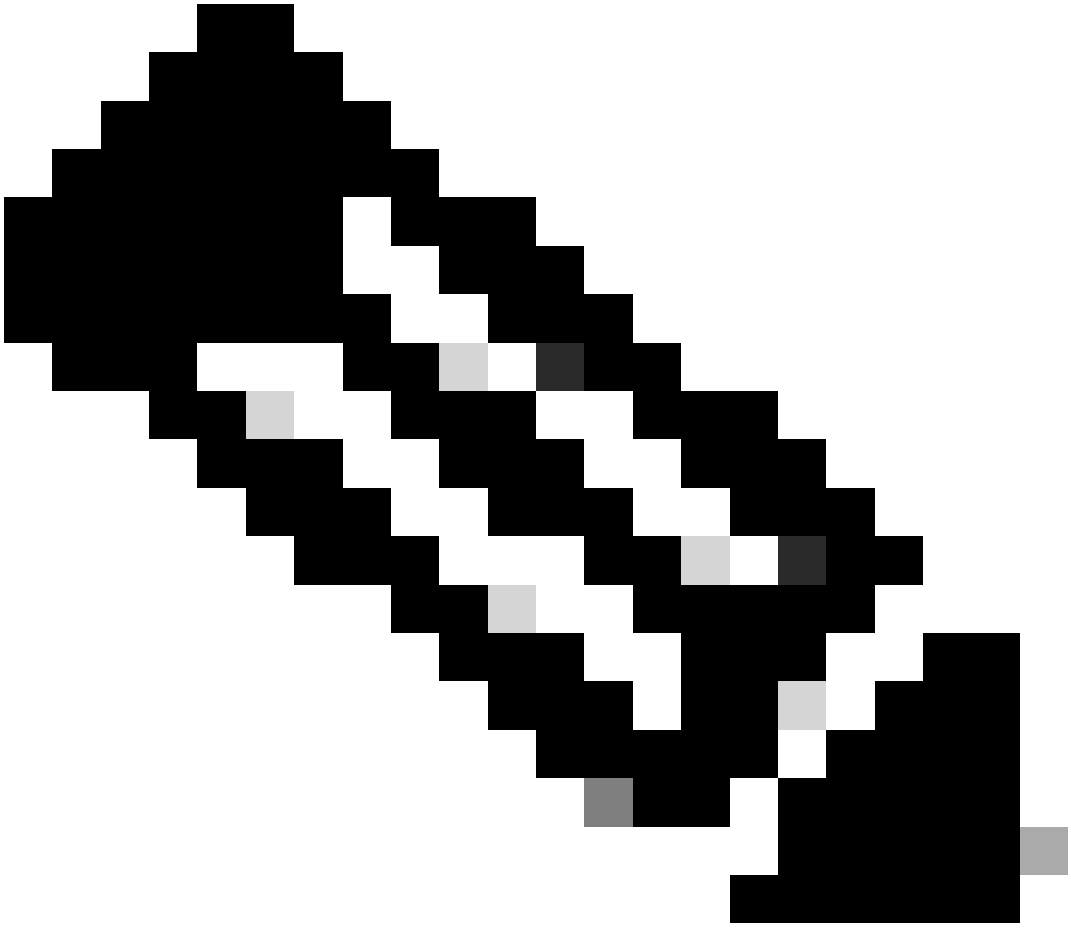
Als split-DNS is ingeschakeld, wordt alleen DNS-fall-back voor split-tunneling afgedwongen. Dit betekent dat AC alleen DNS-verzoek toestaat dat overeenkomt met de split-DNS-domeinen via de tunnel (andere verzoeken worden door AC beantwoord met "geweigerd" antwoord op force failover naar openbare DNS-servers), maar kan dat verzoek niet afdwingen dat overeenkomt met de split-DNS-domeinen die niet in het duidelijke, via de openbare adapter worden verzonden.

iPhone

De iPhone is het volledige tegenovergestelde van het Macintosh-systeem en is niet vergelijkbaar met Microsoft Windows. Als gesplitste tunneling is gedefinieerd maar gesplitste DNS niet is gedefinieerd, worden DNS-vragen afgesloten via de algemene DNS-server die is gedefinieerd. Bijvoorbeeld, gesplitste DNS domeinvermeldingen zijn verplicht voor interne resolutie. Dit gedrag is gedocumenteerd in Cisco bug-id CSCtq09624 en is vastgelegd in versie 2.5.4038 voor de Apple iOS AnyConnect-client.

Opmerking: houd er rekening mee dat de DNS-vragen van de iPhone .local domeinen negeren. Dit is gedocumenteerd in Cisco bug-id CSC89292. Apple engineers bevestigen dat het probleem wordt veroorzaakt door de functionaliteit van het besturingssysteem. Dit is het ontworpen gedrag, en Apple bevestigt dat er geen verandering voor is.

Verwante informatie over bugs



Opmerking: alleen geregistreerde Cisco-gebruikers hebben toegang tot interne Cisco-tools en -informatie.

- Cisco bug-id CSCsv34395 - ondersteuning toevoegen in AnyConnect voor die proxy's de FQDN naar DHCP-server
- Cisco bug-id CSCtn14578 - AnyConnect ter ondersteuning van ware gesplitste DNS; geen back-up
- Cisco bug-id CSCtq02141 - AnyConnect DNS-probleem wanneer ISP DNS op hetzelfde subnetwerkknooppunt staat als openbare IP
- Cisco bug-id CSCtf20226 - AnyConnect DNS met gesplitste tunnelgedrag voor Mac hetzelfde als Windows
- Cisco bug ID CSCtz86314 - Mac: DNS-vragen worden niet via de tunnel met gesplitste DNS verzonden

- Cisco bug-id CSCtq09624 - maakt AnyConnect iPhone-DNS met gesplitst tunnelgedrag hetzelfde als Windows
- Cisco bug-id CSCts89292 - AC voor iPhone DNS-vragen negeren lokale domeinen

Gerelateerde informatie

- Cisco IOS®-firewall
- Cisco Technical Support en downloads

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.