Esaminare il comportamento delle query DNS e della risoluzione dei nomi di dominio

Sommario

- Introduzione
- Prerequisiti
  - Requisiti
  - Componenti usati
- DNS diviso e standard
- DNS suddiviso tra True e Best Effort
- DNS "tunnel-all" e "tunnel-all"
- Problema di prestazioni DNS risolto in AnyConnect versione 3.0(4235)
- DNS con tunneling ripartito su un sistema operativo Cisco diverso
  - Microsoft Windows
    - Windows 7+
    - Configurazione split-include (DNS tunnel tutto disabilitato e nessun split-DNS)
    - Configurazione split-exclude (DNS tunnel tutto disabilitato e no split-DNS)
    - Split-DNS (DNS tunnel tutto disabilitato, split-include configurato)
  - Mac OSx
    - Configurazione tunnel-tutto (e tunneling suddiviso con DNS tunnel-tutto abilitato)
    - Configurazione split-include (DNS tunnel tutto disabilitato e nessun split-DNS)
    - Configurazione split-exclude (DNS tunnel tutto disabilitato e no split-DNS)
    - Split-DNS (DNS tunnel tutto disabilitato, split-include configurato)
  - Linux
    - Configurazione tunnel-tutto (e tunneling suddiviso con DNS tunnel-tutto abilitato)
    - Configurazione split-include (DNS tunnel tutto disabilitato e nessun split-DNS)
    - Configurazione split-exclude (DNS tunnel tutto disabilitato e no split-DNS)
    - Split-DNS (DNS tunnel tutto disabilitato, split-include configurato)
  - iPhone
  - Informazioni correlate ai bug
- Informazioni correlate

Introduzione

In questo documento viene descritto come Cisco OS® gestisce le query DNS e gli effetti sulla risoluzione dei nomi di dominio con Cisco AnyConnect e il tunneling split o completo.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

DNS diviso e standard

Quando si utilizza il tunneling split-include, per il DNS (Domain Name System) sono disponibili le tre opzioni seguenti:

1. DNS diviso: le query DNS che corrispondono ai nomi di dominio vengono configurate in Cisco Adaptive Security Appliance (ASA). a differenza di altri, vengono spostati nel tunnel (ad esempio sui server DNS definiti sull'appliance ASA).

2. Tunnel-all-DNS: è consentito solo il traffico DNS diretto ai server DNS definiti dall'ASA. Questa impostazione è configurata nei Criteri di gruppo.

3. DNS standard - Tutte le query DNS vengono spostate nei server DNS definiti dall'appliance ASA. In caso di risposta negativa, le query DNS possono anche passare ai server DNS configurati sulla scheda fisica.

Nota: Il comando split-tunnel-all-dns è stato implementato per la prima volta in ASA versione 8.2(5). Prima di questa versione, era possibile eseguire solo la divisione del DNS o del DNS standard.

In tutti i casi, le query DNS definite per lo spostamento nel tunnel vengono inviate a qualsiasi server DNS definito da ASA. Se non sono presenti server DNS definiti dall'ASA, le impostazioni DNS per il tunnel sono vuote.

Se non è stato definito il DNS diviso, tutte le query DNS vengono inviate ai server DNS definiti dall'appliance ASA.

Tuttavia, i comportamenti descritti in questo documento possono essere diversi a seconda del sistema operativo.

Nota: Evitare di utilizzare NSLookup quando si esegue il test della risoluzione dei nomi sul client. Usare al suo posto il browser o il comando ping. NSLookup non si basa sul sistema di risoluzione DNS del sistema operativo. AnyConnect non forza la richiesta DNS tramite una determinata interfaccia, ma la consente o la rifiuta a seconda della configurazione DNS divisa. Per forzare il resolver DNS a provare un server DNS accettabile per una richiesta, è

---

importante che i test del DNS diviso vengano eseguiti solo con applicazioni che si basano sul resolver DNS nativo per la risoluzione dei nomi di dominio (ad esempio, tutte le applicazioni ad eccezione di NSLookup, Dig e applicazioni simili che gestiscono la risoluzione DNS autonomamente).

DNS suddiviso tra True e Best Effort

AnyConnect release 2.4 supporta il Fallback DNS suddiviso (DNS suddiviso al massimo sforzo), che non è il DNS suddiviso vero e proprio e si trova nel client IPsec legacy.

Se la richiesta corrisponde a un dominio DNS suddiviso, AnyConnect consente di eseguire il tunneling della richiesta nell'appliance ASA.

Se il server non è in grado di risolvere il nome host, il resolver DNS continua e invia la stessa query al server DNS mappato all'interfaccia fisica.

D'altra parte, se la richiesta non corrisponde a nessuno dei domini DNS suddivisi, AnyConnect non lo tunnel nell'appliance ASA.

Viene invece generata una risposta DNS in modo che il resolver DNS esegua il fallback e invii la query al server DNS mappato all'interfaccia fisica.

Per questo motivo questa funzionalità non è denominata split DNS, ma fallback DNS per il tunneling suddiviso.

AnyConnect non solo assicura che solo le richieste che riguardano domini DNS divisi di destinazione vengano tunneling, ma si basa anche sul comportamento del resolver DNS del sistema operativo del client per la risoluzione dei nomi host.

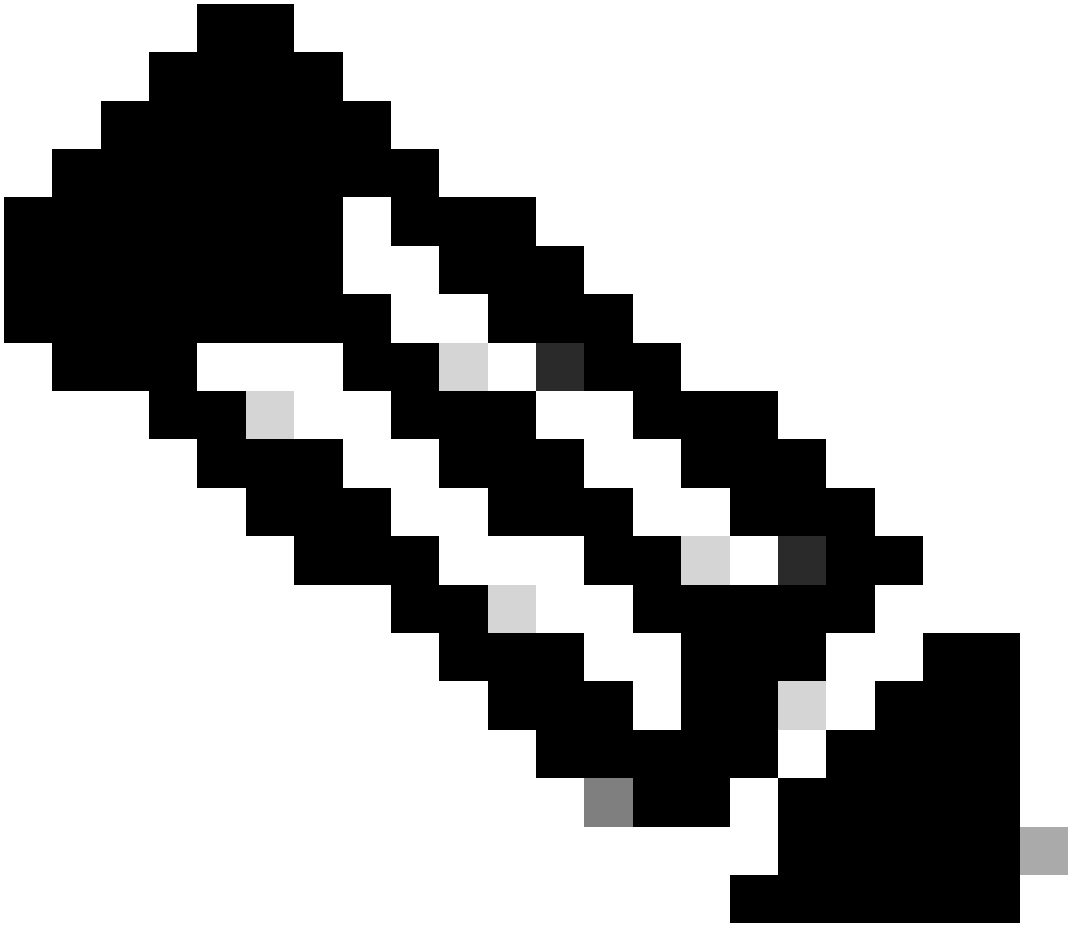
Ciò solleva problemi di sicurezza a causa di una potenziale perdita di informazioni sul nome di dominio privato.

Ad esempio, il client DNS nativo può inviare una query per un nome di dominio privato a un server DNS pubblico in modo specifico quando il server dei nomi DNS VPN non è in grado di risolvere la query DNS.

Fare riferimento all'ID bug Cisco CSCtn14578, attualmente risolto solo in Microsoft Windows, nella versione 3.0(4235).

La soluzione implementa il DNS vero e proprio suddiviso, esegue una query sui nomi di dominio configurati che corrispondono e sono consentiti ai server DNS VPN.

Tutte le altre query sono consentite solo ad altri server DNS, ad esempio quelli configurati sulle schede fisiche.



Nota: Solo gli utenti Cisco registrati possono accedere agli strumenti e alle informazioni interne di Cisco.

DNS "tunnel-all" e "tunnel-all"

Quando il tunneling suddiviso è disabilitato (configurazione Tunnel-all), il traffico DNS è strettamente consentito tramite tunnel.

La configurazione DNS "tutto il tunnel" (configurata nei Criteri di gruppo) invia tutte le ricerche DNS attraverso il tunnel, insieme a un tipo di tunneling suddiviso. Il traffico DNS è consentito esclusivamente attraverso il tunnel.

Ciò è coerente tra le piattaforme con un'avvertenza su Microsoft Windows: quando si configura un DNS tunnel tutto o tunnel tutto, AnyConnect consente il traffico DNS solo verso i server DNS configurati sul gateway sicuro (applicato alla scheda VPN). Si tratta di un miglioramento della sicurezza implementato insieme alla soluzione DNS "true split" precedentemente indicata.

Se il problema si verifica in determinati scenari (ad esempio, le richieste di registrazione/aggiornamento DNS devono essere inviate a server DNS non VPN), completare i seguenti passaggi:

1. Se la configurazione corrente è Tunnel-all, abilitare il tunneling split-exclude. È possibile utilizzare qualsiasi rete a host singolo con funzionalità split-exclude, ad esempio un indirizzo locale del collegamento.

2. Verificare che il DNS completo del tunnel non sia configurato nei Criteri di gruppo.

Problema di prestazioni DNS risolto in AnyConnect versione 3.0(4235)

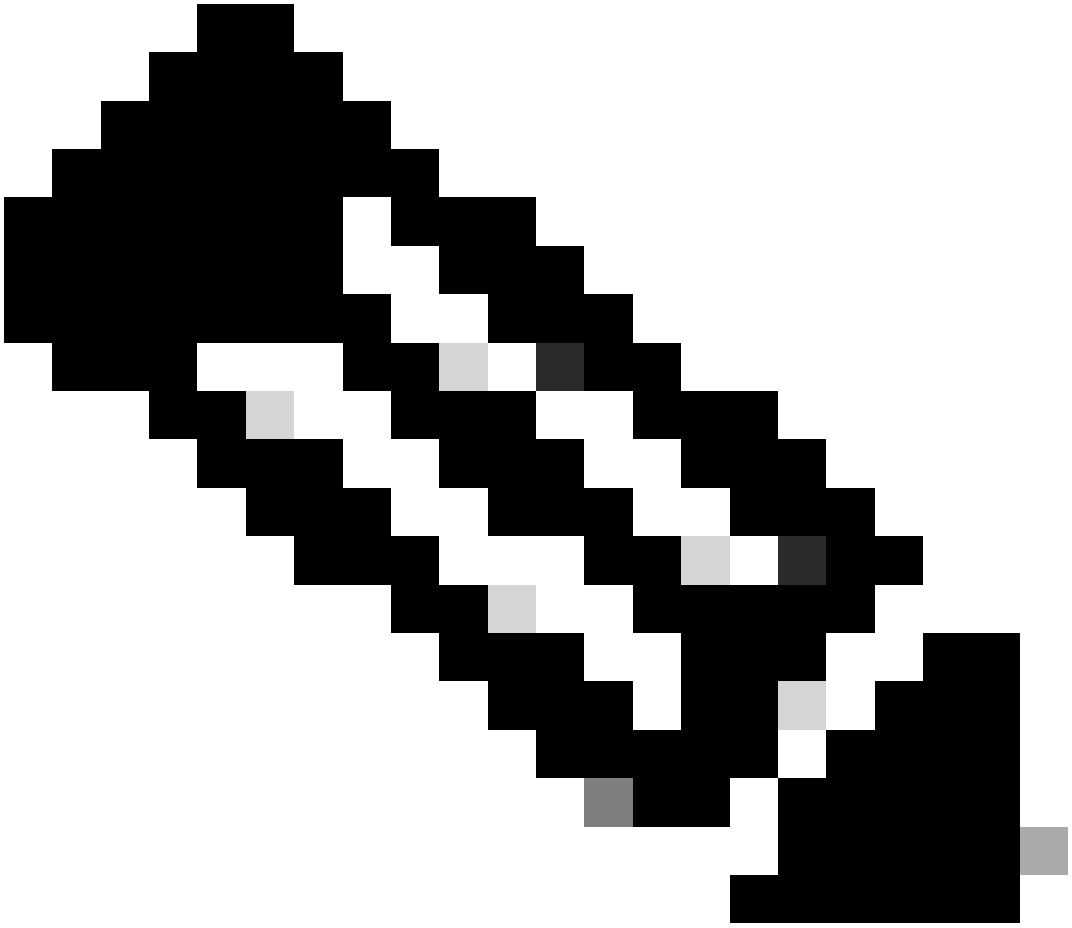
Questo problema relativo a Microsoft Windows è prevalente nelle seguenti condizioni:

- Con la configurazione del router principale, ai server DNS e DHCP viene assegnato lo stesso indirizzo IP (AnyConnect crea una route necessaria al server DHCP).
- Nei Criteri di gruppo sono inclusi numerosi domini DNS.
- Viene utilizzata una configurazione completa di tunnel.
- La risoluzione dei nomi viene eseguita da un nome host non qualificato, il che implica che il resolver deve provare un numero di suffissi DNS in tutti i server DNS disponibili fino a quando non viene tentato quello relativo al nome host richiesto.
- Questo problema è causato dal client DNS nativo che tenta di inviare query DNS tramite la scheda fisica, che viene bloccata da AnyConnect (data la configurazione Tunnel-All).

Ciò comporta un ritardo nella risoluzione dei nomi che può essere significativo, soprattutto se l'headend esegue il push di un numero elevato di suffissi DNS.

Il client DNS deve eseguire tutte le query e i server DNS disponibili fino a quando non riceve una risposta positiva.

Il problema è stato risolto in AnyConnect versione 3.0(4235). Per ulteriori informazioni, fare riferimento agli ID bug Cisco CSCtq02141 e all'ID bug Cisco CSCtn14578, insieme all'introduzione alla soluzione true split DNS precedentemente menzionata.



Nota: Solo gli utenti Cisco registrati possono accedere agli strumenti e alle informazioni interne di Cisco.

Se non è possibile implementare un aggiornamento, sono disponibili le soluzioni seguenti:

- Abilitare il tunneling split-exclude per un indirizzo IP, che consente alle richieste DNS locali di passare attraverso la scheda fisica.

È possibile utilizzare un indirizzo dalla subnet locale del collegamento 169.254.0.0/16 perché è improbabile che un dispositivo invii traffico a uno di questi indirizzi IP tramite la VPN.

Dopo aver abilitato il tunneling split-exclude, abilitare l'accesso LAN locale sul profilo del client o sul client stesso e disabilitare il DNS completo del tunnel.

Sull'appliance ASA, apportare le seguenti modifiche alla configurazione:

```
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
```

Nel profilo client è necessario aggiungere la riga seguente:

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

Inoltre, è possibile abilitare questa funzionalità sui singoli client nell'interfaccia utente del client AnyConnect. Passare al menu Preferenze AnyConnect e selezionare la casella di controllo Abilita accesso LAN locale.

- Utilizzare i nomi di dominio completi (FQDN) anziché i nomi host non qualificati per le risoluzioni dei nomi.
- Utilizzare un indirizzo IP diverso per il server DNS sull'interfaccia fisica.

DNS con tunneling ripartito su un sistema operativo Cisco diverso

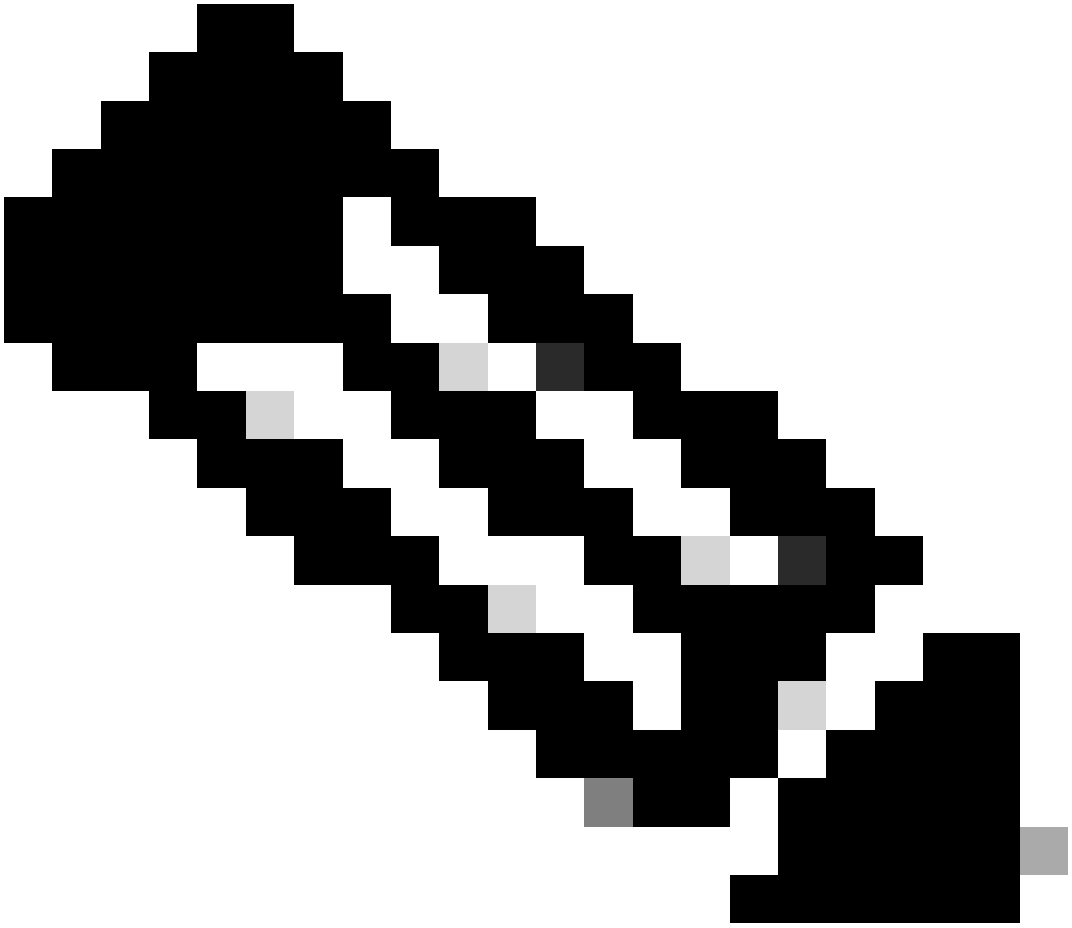
I diversi sistemi operativi Cisco gestiscono le ricerche DNS in modi diversi quando vengono utilizzate con il tunneling suddiviso (senza DNS suddiviso) per AnyConnect. In questa sezione vengono descritte tali differenze.

Microsoft Windows

Nei sistemi Microsoft Windows, le impostazioni DNS sono per interfaccia. Se si utilizza il tunneling suddiviso, le query DNS possono eseguire il fallback ai server DNS della scheda fisica dopo che si sono verificati errori nella scheda tunnel VPN.

Se si definisce il tunneling suddiviso senza DNS suddiviso, la risoluzione DNS sia interna che esterna funziona perché ritorna ai server DNS esterni.

Il meccanismo DNS per la gestione di questo problema su AnyConnect per Windows è stato modificato nella versione 4.2 dopo la correzione dell'ID bug Cisco CSCuf07885.



Nota: Solo gli utenti Cisco registrati possono accedere agli strumenti e alle informazioni interne di Cisco.

Windows 7+

Configurazione tunnel-tutto (e tunneling suddiviso con DNS tunnel-tutto abilitato)

Pre AnyConnect 4.2:

Sono consentite solo le richieste DNS ai server DNS configurati in Criteri di gruppo (server DNS tunnel).

Il driver AnyConnect risponde a tutte le altre richieste con una risposta "senza nome".

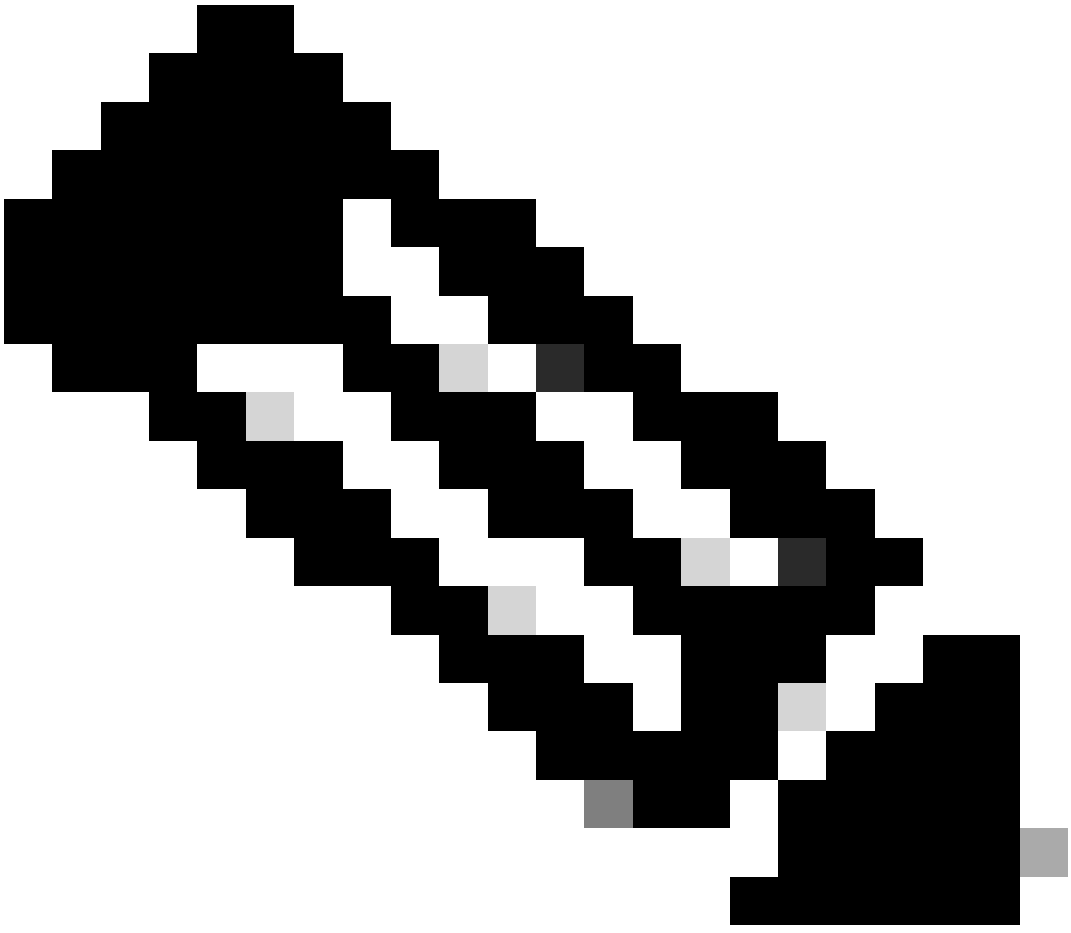
La risoluzione DNS può pertanto essere eseguita solo con i server DNS del tunnel.

AnyConnect 4.2 +

Le richieste DNS a qualsiasi server DNS sono consentite, a condizione che abbiano origine dalla scheda VPN e siano inviate attraverso il tunnel.

A tutte le altre richieste viene risposto senza nome e la risoluzione DNS può essere eseguita solo tramite il tunnel VPN.

Prima della correzione dell'ID bug Cisco CSCuf07885, l'applicazione di una licenza ha limitato i server DNS di destinazione. Tuttavia, con la correzione per il bug, ora vengono limitate le schede di rete che possono avviare richieste DNS.



Nota: Solo gli utenti Cisco registrati possono accedere agli strumenti e alle informazioni interne di Cisco.

Configurazione split-include (DNS tunnel tutto disabilitato e nessun split-DNS)

Il driver AnyConnect non interferisce con il resolver DNS nativo. Pertanto, la risoluzione DNS viene eseguita in base all'ordine delle schede di rete in cui AnyConnect è sempre la scheda preferita quando si connette una VPN.

Inoltre, una query DNS viene prima inviata tramite il tunnel e, se non viene risolta, il resolver tenta di risolverla tramite l'interfaccia pubblica. L'elenco degli accessi con inclusione separata include la subnet che copre i server DNS del tunnel.

Per iniziare con AnyConnect 4.2, il client AnyConnect aggiunge automaticamente le route host per i server DNS del tunnel come reti a inclusione divisa (route sicure) e quindi l'elenco degli accessi a inclusione divisa non richiede più l'aggiunta esplicita della subnet del server DNS del tunnel.

Configurazione split-exclude (DNS tunnel tutto disabilitato e no split-DNS)

Il driver AnyConnect non interferisce con il resolver DNS nativo. Pertanto, la risoluzione DNS viene eseguita in base all'ordine delle schede di rete in cui AnyConnect è sempre la scheda preferita quando si connette una VPN.

Inoltre, una query DNS viene prima inviata tramite il tunnel e, se non viene risolta, il resolver tenta di risolverla tramite l'interfaccia pubblica. L'elenco degli accessi separato-escluso non deve includere la subnet che copre i server DNS del tunnel.

Per iniziare con AnyConnect 4.2, il client AnyConnect aggiunge automaticamente le route host per i server DNS del tunnel come reti con inclusione divisa (route sicure) e impedisce la configurazione errata nell'elenco degli accessi con esclusione divisa.

Split-DNS (DNS tunnel tutto disabilitato, split-include configurato)

Pre AnyConnect 4.2

Le richieste DNS, che corrispondono ai domini split-dns, possono eseguire il tunnel dei server DNS, ma non di altri server DNS.

Per evitare che queste query DNS interne fuoriescano dal tunnel, il driver AnyConnect risponde con "nessun nome" se la query viene inviata ad altri server DNS.

Pertanto, i domini split-dns possono essere risolti solo tramite server DNS del tunnel.

Le richieste DNS, che non corrispondono ai domini split-dns, sono consentite ad altri server DNS, ma non ai server DNS.

Anche in questo caso, il driver AnyConnect risponde con la parola "senza nome" se si tenta di eseguire una query su domini non suddivisi in DNS tramite un tunnel.

Pertanto, i domini DNS non suddivisi possono essere risolti solo tramite server DNS pubblici esterni al tunnel.

AnyConnect 4.2 +

Le richieste DNS, che corrispondono ai domini split-dns, sono consentite a qualsiasi server DNS, purché provengano dalla scheda VPN.

Se la query ha origine nell'interfaccia pubblica, il driver AnyConnect risponde con il messaggio "no that name" (Nessun nome) per forzare il sistema di risoluzione dei nomi a utilizzare sempre il tunnel.

Pertanto, i domini split-dns possono essere risolti solo tramite tunnel.

Le richieste DNS, che non corrispondono ai domini split-dns, sono consentite a qualsiasi server DNS purché provengano dalla scheda fisica.

Se la query è stata creata dalla scheda VPN, AnyConnect risponde con la parola "senza nome" per forzare il resolver a tentare sempre la risoluzione dei nomi tramite l'interfaccia pubblica.

Pertanto, i domini non split-dns possono essere risolti solo tramite l'interfaccia pubblica.

Mac OSx

Nei sistemi Macintosh le impostazioni DNS sono globali. Se si utilizza il tunneling suddiviso, ma non il DNS suddiviso, le query DNS non potranno raggiungere i server DNS all'esterno del tunnel. È possibile risolvere solo internamente, non esternamente.

Questa condizione è documentata nell'ID bug Cisco CSCtf20226 e nell'ID bug Cisco CSCtz86314. In entrambi i casi, la soluzione deve risolvere il problema:

- Specificare l'indirizzo IP di un server DNS esterno in Criteri di gruppo e utilizzare un nome di dominio completo (FQDN) per le query DNS interne.

- Se i nomi esterni possono essere risolti tramite il tunnel, passare a Avanzate > Tunneling ripartito e disabilitare il DNS ripartito tramite la rimozione dei nomi DNS configurati nei Criteri di gruppo. È quindi necessario utilizzare un FQDN per le query DNS interne.

Il caso DNS suddiviso è risolto in AnyConnect versione 3.1. Tuttavia, è necessario verificare che sia soddisfatta una delle seguenti condizioni:

- Il DNS diviso deve essere abilitato per entrambi i protocolli IP, il che richiede Cisco ASA versione 9.0 o successive.

- Il DNS diviso deve essere abilitato per un protocollo IP. Se si esegue Cisco ASA versione 9.0 o successive, usare il protocollo client bypass per l'altro protocollo IP. Verificare, ad esempio, che non vi sia alcun pool di indirizzi e che il protocollo Client Bypass Protocol sia abilitato nei Criteri di gruppo. In alternativa, se si esegue un'appliance ASA versione

precedente alla 9.0, verificare che non vi sia alcun pool di indirizzi configurato per l'altro protocollo IP. Ciò implica che l'altro protocollo IP è IPv6.

Nota: AnyConnect non modifica il file resolv.conf in Macintosh OS X, ma modifica le impostazioni DNS specifiche di OS X. Macintosh OS X mantiene il file resolv.conf aggiornato per motivi di compatibilità. Usare il comando scutil —dns per visualizzare le impostazioni DNS in Macintosh OS X.

Configurazione tunnel-tutto (e tunneling suddiviso con DNS tunnel-tutto abilitato)

Quando AnyConnect è connesso, nella configurazione DNS del sistema vengono gestiti solo i server DNS di tunnel, quindi le richieste DNS possono essere inviate solo ai server DNS di tunnel.

Configurazione split-include (DNS tunnel tutto disabilitato e nessun split-DNS)

AnyConnect non interferisce con il resolver DNS nativo. I server DNS del tunnel sono configurati come resolver preferiti, che hanno la precedenza sui server DNS pubblici, in modo da garantire che la richiesta DNS iniziale per una risoluzione dei nomi venga inviata tramite il tunnel.

Poiché le impostazioni DNS sono globali in Mac OS X, non è possibile per le query DNS utilizzare server DNS pubblici all'esterno del tunnel come documentato nell'ID bug Cisco CSCtf20226 .

Per iniziare con AnyConnect 4.2, il client AnyConnect aggiunge automaticamente le route host per i server DNS del tunnel come reti a inclusione divisa (route sicure) e quindi l'elenco degli accessi a inclusione divisa non richiede più l'aggiunta esplicita della subnet del server DNS del tunnel.

Configurazione split-exclude (DNS tunnel tutto disabilitato e no split-DNS)

AnyConnect non interferisce con il resolver DNS nativo.

I server DNS del tunnel sono configurati come resolver preferiti e hanno la precedenza sui server DNS pubblici, pertanto la richiesta DNS iniziale per la risoluzione dei nomi viene inviata tramite il tunnel.

Poiché le impostazioni DNS sono globali in Mac OS X, non è possibile per le query DNS utilizzare server DNS pubblici all'esterno del tunnel come documentato nell'ID bug Cisco CSCtf20226 .

Per iniziare con AnyConnect 4.2, il client AnyConnect aggiunge automaticamente le route host per i server DNS del tunnel come reti a inclusione divisa (route sicure) e quindi l'elenco degli accessi a inclusione divisa non richiede più l'aggiunta esplicita della subnet del server DNS del tunnel.

Split-DNS (DNS tunnel tutto disabilitato, split-include configurato)

Se il DNS diviso è abilitato per entrambi i protocolli IP (IPv4 e IPv6) o è abilitato solo per un protocollo e non è configurato alcun pool di indirizzi per l'altro protocollo:
Viene applicato True split-DNS, simile a Windows. Se ha valore True, split-DNS indica che le richieste che corrispondono ai domini split-DNS vengono risolte solo tramite il tunnel e non vengono inviate ai server DNS esterni al tunnel.

Se split-DNS è abilitato solo per un protocollo e un indirizzo client è assegnato per l'altro protocollo, viene applicato solo il fallback DNS per lo split-tunneling.

Questo significa che la CA consente solo le richieste DNS che corrispondono ai domini DNS divisi tramite tunnel (altre richieste vengono risposte da CA con risposta "rifiutata" per forzare il failover ai server DNS pubblici), ma non può imporre la richiesta che corrisponde ai domini DNS divisi che non vengono inviati in chiaro tramite la scheda pubblica.

Linux

Configurazione tunnel-tutto (e tunneling suddiviso con DNS tunnel-tutto abilitato)

Quando AnyConnect è connesso, nella configurazione DNS del sistema vengono gestiti solo i server DNS di tunnel, quindi le richieste DNS possono essere inviate solo ai server DNS di tunnel.

Configurazione split-include (DNS tunnel tutto disabilitato e nessun split-DNS)

AnyConnect non interferisce con il resolver DNS nativo. I server DNS del tunnel sono configurati come resolver preferiti, che hanno la precedenza sui server DNS pubblici, in modo da garantire che la richiesta DNS iniziale per una risoluzione dei nomi venga inviata tramite il tunnel.

Configurazione split-exclude (DNS tunnel tutto disabilitato e no split-DNS)

AnyConnect non interferisce con il resolver DNS nativo. I server DNS del tunnel sono configurati come resolver preferiti, che hanno la precedenza sui server DNS pubblici, in modo da garantire che la richiesta DNS iniziale per una risoluzione dei nomi venga inviata tramite il tunnel.

Split-DNS (DNS tunnel tutto disabilitato, split-include configurato)

Se split-DNS è abilitato, viene applicato solo il fallback DNS per lo split-tunneling. Questo significa che AC consente solo le richieste DNS che corrispondono ai domini DNS divisi tramite tunnel (altre richieste vengono risposte da AC con risposta "rifiutata" per forzare il failover ai server DNS pubblici), ma non può applicare tale richiesta che corrisponde ai domini DNS divisi che non vengono inviati in chiaro tramite la scheda pubblica.

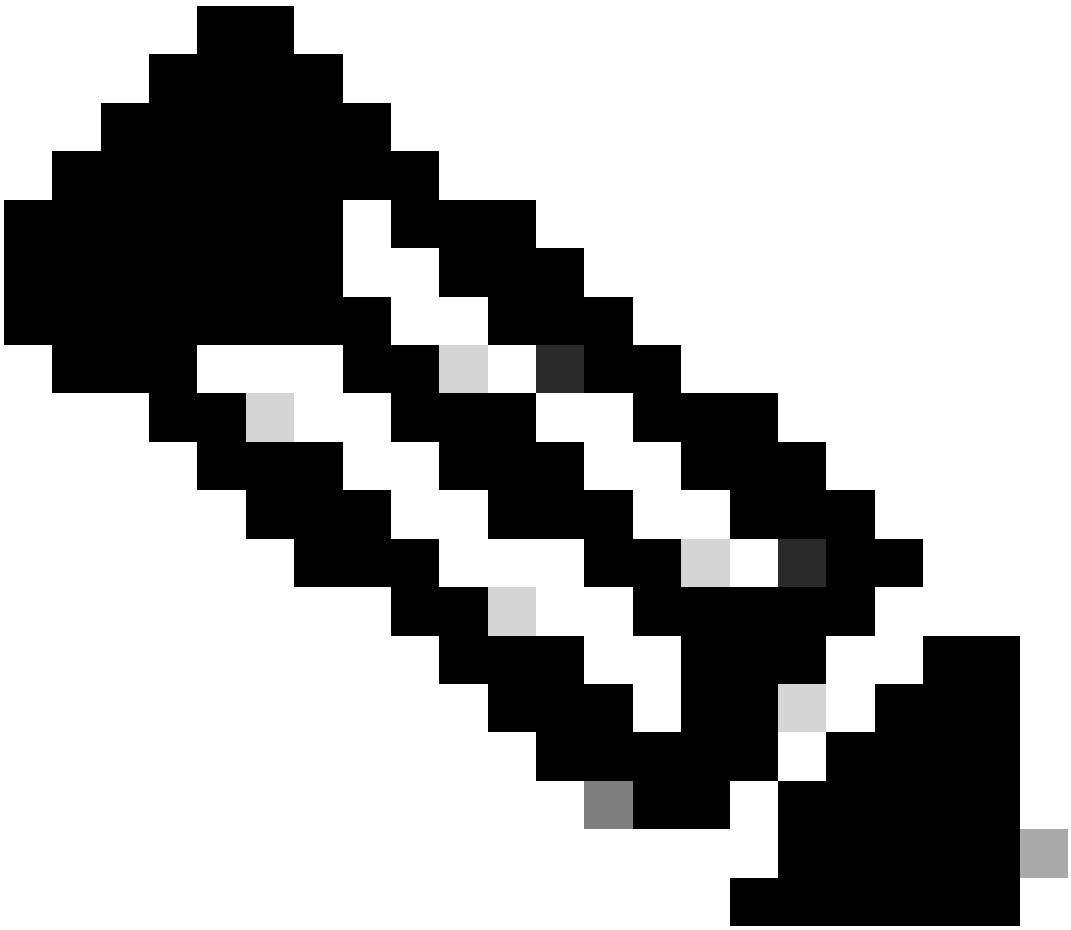
iPhone

L'iPhone è l'esatto opposto del sistema Macintosh e non è simile a Microsoft Windows. Se il tunneling suddiviso è definito ma il DNS suddiviso non è definito, le query DNS verranno eseguite nel server DNS globale definito.

Ad esempio, le voci di dominio DNS suddivise sono obbligatorie per la risoluzione interna. Questo comportamento è documentato nell'ID bug Cisco CSCtq09624 e viene risolto nella versione 2.5.4038 per il client Apple iOS AnyConnect.

Nota: Tenere presente che le query DNS iPhone ignorano i domini .local. Questa condizione è documentata nell'ID bug Cisco CSCts89292. I tecnici di Apple confermano che il problema è causato dalla funzionalità del sistema operativo. Questo è il comportamento progettato e Apple conferma che non c'è alcun cambiamento.

Informazioni correlate ai bug



Nota: Solo gli utenti Cisco registrati possono accedere agli strumenti e alle informazioni interne di Cisco.

- Cisco ID bug CSCsv34395 - Aggiungere il supporto in AnyConnect per inviare il FQDN al server DHCP
- Cisco ID bug CSCtn14578 - AnyConnect per supportare DNS true split; non fallback
- Cisco ID bug CSCtq02141 - Problema DNS di AnyConnect quando il DNS dell'ISP si trova sulla stessa subnet dell'IP pubblico
- Cisco ID bug CSCtf20226 - Rendere AnyConnect DNS con comportamento tunnel suddiviso per Mac uguale a Windows
- ID bug Cisco CSCtz86314 - Mac: Query DNS non inviate correttamente tramite il tunnel con DNS suddiviso
- Cisco ID bug CSCtq09624 - Rendere AnyConnect iPhone DNS con tunneling suddiviso uguale a Windows
- Cisco ID bug CSCts89292 - AC per le query DNS iPhone che ignorano i domini .local

Informazioni correlate

- Cisco IOS® Firewall
- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).