Interoperabilità tra AnyConnect e OpenDNS Roaming Client

Sommario

Introduzione
Prerequisiti
Requisiti
Componenti usati
Premesse
Funzionalità
Gestione DNS AnyConnect
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 OS X
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)
OpenDNS Roaming client
Limitazioni
Soluzione alternativa
Configurazioni
Traffico OpenDNS tunnel
Escludi traffico OpenDNS dal tunnel VPN
Verifica

Introduzione

Questo documento descrive alcune delle limitazioni correnti e le soluzioni disponibili per far funzionare AnyConnect e OpenDNS Roaming Client insieme. I clienti Cisco si affidano al client VPN AnyConnect per comunicare in modo sicuro e crittografato con le reti aziendali. Analogamente, il client Roaming OpenDNS offre agli utenti la possibilità di utilizzare in modo sicuro i servizi DNS con l'aiuto dei server pubblici OpenDNS. Entrambi i client aggiungono un insieme completo di funzionalità di sicurezza all'endpoint, pertanto è importante che interagiscano tra loro.

Prerequisiti

Conoscenze operative dei client mobili AnyConnect e OpenDNS.

Familiarità con la configurazione headend ASA o IOS/IOS-XE (tunnel-group/group-policy) per AnyConnect VPN.

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Headend ASA o IOS/IOS-XE
- Endpoint che esegue il client VPN AnyConnect e il client OpenDNS Roaming

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Headend ASA con release 9.4
- Windows 7
- Client AnyConnect 4.2.0096
- OpenDNS Roaming client 2.0.154

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.

Premesse

OpenDNS sta sviluppando un plug-in AnyConnect con il team Cisco AnyConnect che sarà disponibile in futuro. Anche se non è stata impostata alcuna data, questa integrazione permetterà al client in roaming di funzionare con il client AnyConnect senza le soluzioni indicate. Ciò consentirà anche di usare AnyConnect come meccanismo di consegna per il client in roaming.

Funzionalità

Gestione DNS AnyConnect

L'headend VPN può essere configurato in un paio di modi diversi per gestire il traffico proveniente dal client AnyConnect.

1. Configurazione tunnel completa (tunnel-all): In questo modo, tutto il traffico proveniente dall'endpoint viene inviato attraverso il tunnel VPN e crittografato, quindi il traffico non lascia mai la scheda di interfaccia pubblica in testo non crittografato
2. Configurazione tunnel diviso:

r. Tunneling split-include: Il traffico destinato solo a subnet o host specifici definiti sull'headend VPN viene inviato attraverso il tunnel, tutto il resto del traffico viene inviato all'esterno del tunnel in formato testo non crittografato

b. Tunneling split-exclude: Il traffico destinato solo a subnet o host specifici definiti sull'headend VPN viene escluso dalla crittografia e lascia l'interfaccia pubblica in modalità non crittografata, tutto il resto del traffico viene crittografato e inviato solo attraverso il tunnel

Ciascuna di queste configurazioni determina la modalità di gestione della risoluzione DNS da parte del client AnyConnect, a seconda del sistema operativo sull'endpoint. Il meccanismo di gestione DNS di AnyConnect per Windows è stato modificato nella versione 4.2 dopo la correzione di CSCuf07885.

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". Di conseguenza, la risoluzione DNS può essere eseguita solo utilizzando i server DNS del tunnel.

AnyConnect 4.2 e versioni successive

Le richieste DNS a qualsiasi server DNS sono consentite, purché originate dalla scheda VPN e inviate attraverso il tunnel. A tutte le altre richieste viene risposto 'nessun nome di questo tipo' e la risoluzione DNS può essere eseguita solo tramite il tunnel VPN

Prima della correzione di CSCuf07885, AC limita i server DNS di destinazione, tuttavia con la correzione di CSCuf07885 limita le schede di rete che possono avviare richieste DNS.

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 e AnyConnect è sempre la scheda preferita quando si connette una VPN. Pertanto, una query DNS verrà prima inviata tramite il tunnel e, se non viene risolta, il resolver tenterà di risolverla tramite l'interfaccia pubblica. L'elenco degli accessi separato deve includere la subnet che copre i server DNS del tunnel. A partire da AnyConnect 4.2, le route host per i server DNS del tunnel vengono aggiunte automaticamente dal client AnyConnect come reti con inclusione divisa (route sicure). Pertanto, l'elenco degli accessi con 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 e AnyConnect è sempre la scheda preferita quando si connette una VPN. Pertanto, una query DNS verrà prima inviata tramite il tunnel e, se non viene risolta, il resolver tenterà di risolverla tramite l'interfaccia pubblica. L'elenco degli accessi separato-escluso non deve includere la subnet che copre i server DNS del tunnel. A partire da 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 quindi impedisce una 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 corrispondenti 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 'no that name' se la query viene inviata ad altri server DNS. Pertanto, i domini split-dns possono essere risolti solo tramite i server DNS del tunnel.

Le richieste DNS non corrispondenti ai domini split-dns sono consentite ad altri server DNS, ma non ai server DNS. Anche in questo caso, il driver AnyConnect risponde con "no this name" (Nessun nome di questo tipo) se si tenta di eseguire una query su domini non suddivisi in DNS tramite il tunnel. Pertanto, i domini DNS non suddivisi possono essere risolti solo tramite server DNS pubblici esterni al tunnel.

AnyConnect 4.2 e versioni successive

Le richieste DNS corrispondenti 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 'nome inesistente' per forzare il sistema di risoluzione dei nomi a utilizzare sempre il tunnel. Pertanto, i domini split-dns possono essere risolti solo tramite il 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, la risposta di AnyConnect sarà 'no that name' per forzare il sistema di risoluzione dei nomi a tentare sempre la risoluzione tramite l'interfaccia pubblica. Pertanto, i domini non split-dns possono essere risolti solo tramite l'interfaccia pubblica.

Mac 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, garantendo in tal modo che la richiesta DNS iniziale per la 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 in CSCtf20226 . A partire da AnyConnect 4.2, le route host per i server DNS del tunnel vengono aggiunte automaticamente dal client AnyConnect come reti con inclusione divisa (route sicure). Pertanto, l'elenco degli accessi con 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, che hanno la precedenza sui server DNS pubblici, garantendo in tal modo che la richiesta DNS iniziale per la 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 in CSCtf20226 . A partire da AnyConnect 4.2, le route host per i server DNS del tunnel vengono aggiunte automaticamente dal client AnyConnect come reti con inclusione divisa (route sicure). Pertanto, l'elenco degli accessi con 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 per un solo 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, le richieste corrispondenti ai domini DNS divisi vengono risolte solo tramite il tunnel e non vengono inviate a 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 split-tunneling. Questo significa che la connessione CA consente solo le richieste DNS corrispondenti 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 che le richieste corrispondenti ai domini DNS divisi non vengano inviate 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, garantendo in tal modo che la richiesta DNS iniziale per la 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, garantendo in tal modo che la richiesta DNS iniziale per la 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 la connessione CA consente solo le richieste DNS corrispondenti 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 che le richieste corrispondenti ai domini DNS divisi non vengano inviate in chiaro, tramite la scheda pubblica.

OpenDNS Roaming client

Il client Roaming è un componente software che gestisce i servizi DNS sull'endpoint e utilizza i server DNS pubblici OpenDNS per proteggere e crittografare il traffico DNS.

In teoria, il client dovrebbe essere in uno stato protetto e crittografato. Tuttavia, se il client non è in grado di stabilire una sessione TLS con il server di risoluzione pubblico OpenDNS (208.67.222.222), tenta di inviare il traffico DNS non crittografato sulla porta UDP da 53 a 208.67.222.222. Il client mobile utilizza esclusivamente l'indirizzo IP 208.67.222.222 del resolver pubblico OpenDNS (ce ne sono alcuni altri, ad esempio 208.67.220.2 20, 208.67.222.220 e 208.67.220.222). Una volta installato, il client mobile imposta 127.0.0.1 (localhost) come server DNS locale e ignora le impostazioni DNS correnti per interfaccia. Le impostazioni DNS correnti vengono archiviate in file resolv.conf locali (anche in Windows) all'interno della cartella di configurazione di client mobili. OpenDNS eseguirà il backup anche dei server DNS acquisiti tramite la scheda AnyConnect. Ad esempio, se 192.168.92.2 è il server DNS nella scheda pubblica, OpenDNS creerà il file resolv.conf nel seguente percorso:

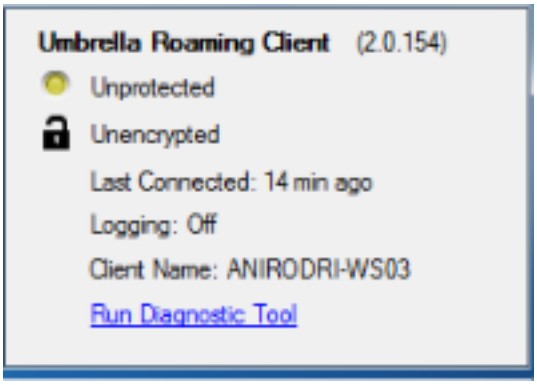
C:\ProgramData\OpenDNS\ERC\Resolver1-LocalAreaConnection-resolv.conf
nameserver 192.168.92.2

Il client mobile crittografa ogni pacchetto impostato su OpenDNS; tuttavia, non viene avviato né utilizzato un tunnel di crittografia per 208.67.222.222. Il client in roaming non dispone di una funzionalità di imposizione del livello IP opzionale che consente di aprire una connessione IPSec per scopi non DNS per bloccare gli indirizzi IP. Questa funzione viene disabilitata automaticamente in presenza di una connessione AnyConnect attiva. Viene inoltre eseguito il binding a 127.0.0.1:53 per ricevere le query generate localmente nel computer. Quando l'endpoint deve risolvere un nome, le query locali vengono indirizzate a 127.0.0.1 a causa dell'override, quindi il processo dnscrypt-proxy sottostante del client roaming le inoltra ai server pubblici OpenDNS sul canale crittografato.

Se il flusso del DNS non è consentito a 127.0.0.1:53, il client in roaming non sarà in grado di funzionare e si verificherà quanto segue. Se il client non è in grado di raggiungere i server DNS pubblici o l'indirizzo associato a 127.0.0.1:53, passerà a uno stato di apertura con errori e ripristinerà le impostazioni DNS sulle schede locali. In background, continua a inviare richieste a 208.67.222.222 e può passare alla modalità attiva se la connessione sicura viene ristabilita.

Limitazioni

Dopo aver esaminato le funzionalità di alto livello di entrambi i client, è evidente che il client in roaming deve avere la capacità di modificare le impostazioni DNS locali e di eseguire il binding a 127.0.0.1:53 per inoltrare le query attraverso il canale sicuro. Quando la VPN è connessa, le uniche configurazioni in cui AnyConnect non interferisce con il resolver DNS nativo sono split-include e split-exclude (con split-tunnel-all DNS disabilitato). Pertanto, si consiglia di utilizzare una di queste configurazioni quando è in uso anche il client di roaming. Il client in roaming rimarrà in uno stato non protetto/non crittografato se viene utilizzata la configurazione tunnel-all o se è abilitato il DNS split-tunnel-all, come mostrato nell'immagine.



Soluzione alternativa

Se lo scopo è quello di proteggere la comunicazione tra il client in roaming e i server OpenDNS che utilizzano il tunnel VPN, è possibile utilizzare un elenco di accesso fittizio con split-exclude sull'headend VPN. Questa sarà la soluzione più simile a una configurazione completa del tunnel. Se tale requisito non è previsto, è possibile utilizzare la funzione di inclusione divisa se l'elenco degli accessi non include i server pubblici OpenDNS oppure la funzione di esclusione divisa se l'elenco degli accessi include i server pubblici OpenDNS.

Inoltre, quando si utilizza il client in roaming, non è possibile utilizzare le modalità split-DNS in quanto ciò comporterà una perdita della risoluzione DNS locale. Anche il DNS split-tunnel-all deve rimanere disabilitato; tuttavia, è parzialmente supportato e deve consentire al client in roaming di diventare crittografato dopo il failover.

Configurazioni

Traffico OpenDNS tunnel

In questo esempio viene utilizzato un indirizzo IP fittizio nell'elenco degli accessi con diritti di esclusione separati. Con questa configurazione, tutte le comunicazioni con 208.67.222.222 si

verificano attraverso il tunnel VPN e il client in roaming funziona in uno stato crittografato e protetto.

```
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#
```

Escludi traffico OpenDNS dal tunnel VPN

In questo esempio viene utilizzato l'indirizzo del resolver OpenDNS nell'elenco degli accessi split-exclude. Con questa configurazione, tutte le comunicazioni con 208.67.222.222 si verificano all'esterno del tunnel VPN e il client in roaming funziona in uno stato crittografato e protetto.

```
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#
```

Nell'esempio viene mostrata una configurazione con inclusione divisa per una subnet interna 192.168.1.0/24. Con questa configurazione, il client in roaming continuerà a funzionare in uno stato crittografato e protetto poiché il traffico fino a 208.67.222.222 non viene inviato tramite il tunnel.

```
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

Verifica

Quando la VPN è connessa, il client in roaming deve mostrare protetto e crittografato, come mostrato nell'immagine: