Guida alla distribuzione del modulo di sicurezza roaming AnyConnect OpenDNS

Sommario

Introduzione

In questo documento vengono descritte l'installazione, la configurazione e le procedure di risoluzione dei problemi per il modulo Roaming OpenDNS (Umbrella). In AnyConnect 4.3.X e versioni successive, il client OpenDNS Roaming è ora disponibile come modulo integrato. È noto anche come modulo Cloud Security e può essere pre-implementato sull'endpoint con il programma di installazione di AnyConnect, oppure può essere scaricato da Adaptive Security Appliance (ASA) tramite distribuzione sul Web.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco AnyConnect Secure Mobility

- OpenDNS/Umbrella Roaming Module
- Cisco ASA

Componenti usati

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

- Cisco ASA versione 9.3(3)7
- Cisco AnyConnect Secure Mobility Client 4.3.01095
- OpenDNS Roaming Module 4.3.01095
- Cisco Adaptive Security Device Manager (ASDM) 7.6.2 o versioni successive
- Microsoft Windows 8.1
- **Nota:** I requisiti minimi per distribuire il modulo Ombrella OpenDNS sono:
  - AnyConnect VPN Client versione 4.3.01095 o successive
  - Cisco ASDM 7.6.2 o versioni successive
  Il modulo Roaming OpenDNS non è attualmente supportato sulla piattaforma Linux.

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 o della configurazione.

Premesse

OrgInfo.json

Per il corretto funzionamento del modulo Roaming OpenDNS, è necessario scaricare un file OrgInfo.json dal dashboard OpenDNS o eseguirne il push dall'appliance ASA prima di utilizzare il modulo. Quando il file viene scaricato per la prima volta, viene salvato in un percorso specifico che dipende dal sistema operativo.

Per Mac OS X, OrgInfo.json viene scaricato in /opt/cisco/anyconnect/Umbrella.
Per Microsoft Windows, il file OrgInfo.json viene scaricato in C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Umbrella.

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

Come illustrato, il file utilizza la codifica UTF-8 e contiene un ID organizzazione, un'impronta digitale e un ID utente. L'ID organizzazione rappresenta le informazioni sull'organizzazione per l'utente attualmente connesso al dashboard OpenDNS. L'ID organizzazione è statico, univoco e generato automaticamente da OpenDNS per ogni organizzazione. L'impronta digitale viene utilizzata per convalidare il file OrgInfo.json durante la registrazione del dispositivo e l'ID utente rappresenta un ID univoco per l'utente connesso.

Quando il modulo Roaming viene avviato in Windows, il file OrgInfo.json viene copiato nella directory dei dati all'interno della directory Umbrella e utilizzato come copia di lavoro. In MAC OS

X, le informazioni di questo file vengono salvate in updater.plist nella directory data sotto la directory Umbrella. Una volta che il modulo ha letto correttamente le informazioni dal file OrgInfo.json, tenta di registrarsi con OpenDNS con un'API cloud. In seguito a questa registrazione OpenDNS assegna un ID di dispositivo univoco al computer che ha tentato la registrazione. Se è già disponibile un ID di periferica della precedente registrazione, la periferica ignora la registrazione.

Al termine della registrazione, il modulo Roaming esegue un'operazione di sincronizzazione per recuperare le informazioni sui criteri per l'endpoint. Per il corretto funzionamento dell'operazione di sincronizzazione è necessario un ID dispositivo. I dati di sincronizzazione includono, tra gli altri, syncInterval, domini di bypass interni e indirizzi IP. L'intervallo di sincronizzazione è il numero di minuti trascorso il quale il modulo deve tentare di eseguire nuovamente la sincronizzazione.

Comportamento del probe DNS

Una volta completata la registrazione e la sincronizzazione, il modulo Roaming invia sonde DNS (Domain Name System) ai propri resolver locali. Queste richieste DNS includono query TXT per debug.opendns.com. In base alla risposta, il client è in grado di determinare se nella rete è presente un'appliance virtuale OpenDNS (VA) locale.

Se è presente un'appliance virtuale (VA), il client passa alla modalità 'behind-VA' e l'imposizione DNS non viene eseguita sull'endpoint. Il client si basa sul VA per l'imposizione DNS a livello di rete.

Se non è presente un VA, il client invia una richiesta DNS ai resolver pubblici OpenDNS (208.67.222.222) utilizzando UDP/443.

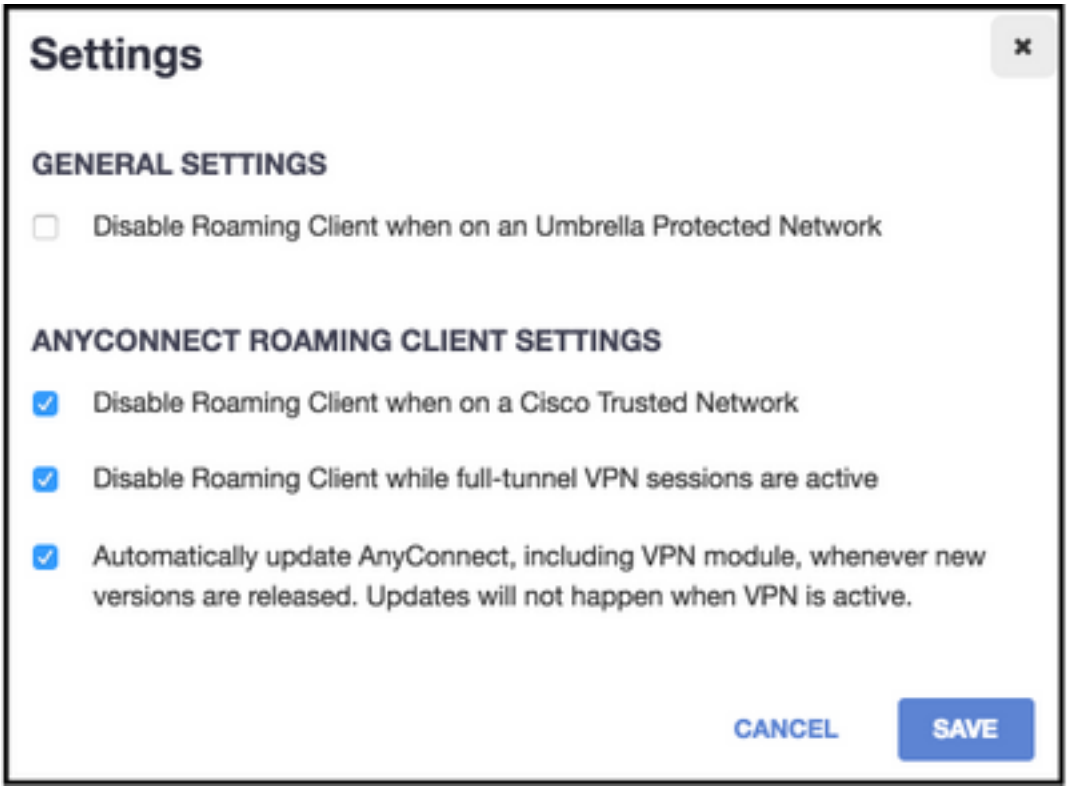
Una risposta positiva indica che è possibile eseguire la crittografia DNS. Se viene ricevuta una risposta negativa, il client invia una richiesta DNS ai resolver pubblici OpenDNS utilizzando UDP/53.

Una risposta positiva a questa query indica che è possibile proteggere il DNS. Se viene ricevuta una risposta negativa, il client ritenterà la query tra qualche secondo.

Dopo aver ricevuto un numero impostato di risposte negative, il client passa allo stato di apertura dopo un errore. Uno stato fail-open indica che la crittografia e/o la protezione DNS non sono possibili. Una volta che il modulo Roaming è passato correttamente a uno stato protetto e/o crittografato, tutte le query DNS per i domini di ricerca al di fuori dei domini di ricerca locali e dei domini di bypass interni vengono inviate ai resolver OpenDNS per la risoluzione dei nomi. Se lo stato è crittografato, tutte le transazioni DNS vengono crittografate dal processo dnscrypt.

Comportamento DNS con modalità di tunneling AnyConnect

1. Tunnel-All (o tunnel-all-DNS abilitato)



Nota: Come mostrato, per impostazione predefinita il modulo Roaming disabilita la protezione DNS mentre è attivo un tunnel VPN con configurazione tunnel all. Affinché il modulo sia attivo durante una configurazione tunnel AnyConnect all, è necessario deselezionare l'opzione **Disabilita client mobile durante le sessioni VPN full-tunnel attive** sul portale OpenDNS. Per abilitare questa funzionalità è necessario un livello di sottoscrizione avanzato con OpenDNS. Le informazioni riportate di seguito presuppongono che la protezione DNS tramite il modulo Roaming sia abilitata.

Parte del dominio sottoposta a query nell'elenco di esclusione interno

Le richieste DNS provenienti dalla scheda del tunnel vengono consentite e inviate ai server DNS del tunnel attraverso il tunnel VPN. La query rimarrà non risolta se non può essere risolta dai server DNS del tunnel.

Dominio sottoposto a query non incluso nell'elenco di esclusione interno

Le richieste DNS provenienti dalla scheda del tunnel sono consentite e verranno inoltrate ai resolver pubblici OpenDNS tramite il modulo Roaming e inviate attraverso il tunnel VPN. Per il client DNS apparirà come se la risoluzione dei nomi fosse stata eseguita tramite il server DNS VPN. Se la risoluzione dei nomi tramite i resolver OpenDNS non riesce, il modulo Roaming esegue il failover sui server DNS configurati localmente, a partire dalla scheda VPN (che è la scheda preferita quando il tunnel è attivo).

2. DNS diviso (DNS tunnel tutto disabilitato)

Nota: Tutti i domini DNS divisi vengono automaticamente aggiunti all'elenco di esclusione interno del modulo Roaming al momento della creazione del tunnel. Questa operazione viene effettuata per fornire un meccanismo di gestione DNS coerente tra AnyConnect e il modulo Roaming. Verificare che in una configurazione split-DNS (con tunneling split-include) i resolver pubblici OpenDNS non siano inclusi nelle reti split-include.

Nota: In Mac OS X, se split-DNS 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, true split-DNS simile a Windows viene imposto.
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. Ciò significa che AnyConnect 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 sui server DNS pubblici), ma non può imporre che le richieste che corrispondono ai domini DNS divisi non vengano inviate in chiaro tramite la scheda pubblica.

Parte del dominio sottoposta a query nell'elenco di esclusione interno e anche parte dei domini DNS divisi

Le richieste DNS provenienti dalla scheda del tunnel vengono consentite e inviate ai server DNS del tunnel attraverso il tunnel VPN. A tutte le altre richieste di domini corrispondenti da altre schede di rete, il driver AnyConnect risponderà con la parola "no this name" (nessun nome di questo tipo) per ottenere un DNS separato vero (impedire il fallback del DNS). Pertanto, solo il traffico DNS non tunnel è protetto dal modulo Roaming.

Parte del dominio sottoposta a query nell'elenco di esclusione interno, ma non appartenente ai domini DNS divisi

Le richieste DNS provenienti dalla scheda fisica sono consentite e inviate ai server DNS pubblici, all'esterno del tunnel VPN. A tutte le altre richieste di domini corrispondenti provenienti dalla scheda del tunnel, il driver AnyConnect risponderà con la parola "no that name" (nessun nome) per impedire l'invio della query attraverso il tunnel VPN.

Dominio sottoposto a query non incluso nell'elenco di esclusione interno o nei domini DNS divisi

Le richieste DNS provenienti dalla scheda fisica vengono consentite e inoltrate ai resolver pubblici OpenDNS e inviate all'esterno del tunnel VPN. Per il client DNS apparirà come se la risoluzione dei nomi fosse stata eseguita tramite il server DNS pubblico. Se la risoluzione dei nomi tramite i resolver OpenDNS ha esito negativo, il modulo Roaming esegue il failover sui server DNS configurati localmente, esclusi quelli configurati sulla scheda VPN. A tutte le altre richieste di domini corrispondenti inviate dalla scheda del tunnel, il driver AnyConnect non avrà questo nome per impedire l'invio della query attraverso il tunnel VPN.

3. Tunneling Split-Include o Split-Exclude (senza split-DNS e tunnel-all-DNS disabilitati)

Parte del dominio sottoposta a query nell'elenco di esclusione interno

Il resolver del sistema operativo nativo esegue la risoluzione DNS in base all'ordine delle schede di rete e AnyConnect è la scheda preferita quando la VPN è attiva. Le richieste DNS avranno origine dalla scheda del tunnel e verranno inviate ai server DNS del tunnel attraverso il tunnel VPN. Se la query non può essere risolta dai server DNS del tunnel, il resolver del sistema operativo tenterà di risolverla tramite i server DNS pubblici.

Dominio sottoposto a query non incluso nell'elenco di esclusione interno

Il resolver del sistema operativo nativo esegue la risoluzione DNS in base all'ordine delle schede di rete e AnyConnect è la scheda preferita quando la VPN è attiva. Le richieste DNS avranno

origine dalla scheda del tunnel e verranno inviate ai server DNS del tunnel attraverso il tunnel VPN. Se la query non può essere risolta dai server DNS del tunnel, il resolver del sistema operativo tenterà di risolverla tramite i server DNS pubblici.

Se i resolver pubblici OpenDNS fanno parte dell'elenco di split-include o non fanno parte dell'elenco di split-exclude, la richiesta proxy viene inviata tramite il tunnel VPN.

Se i resolver pubblici OpenDNS non fanno parte dell'elenco di split-include o dell'elenco di split-exclude, la richiesta proxy viene inviata all'esterno del tunnel VPN.

Se la risoluzione dei nomi tramite i resolver OpenDNS non riesce, il modulo Roaming esegue il failover sui server DNS configurati localmente, a partire dalla scheda VPN (che è la scheda preferita quando il tunnel è attivo). Se la risposta finale restituita dal modulo Roaming (e inoltrata al client DNS nativo) non riesce, il client nativo tenterà altri server DNS, se disponibili.

Installazione e configurazione del modulo Umbrella Roaming

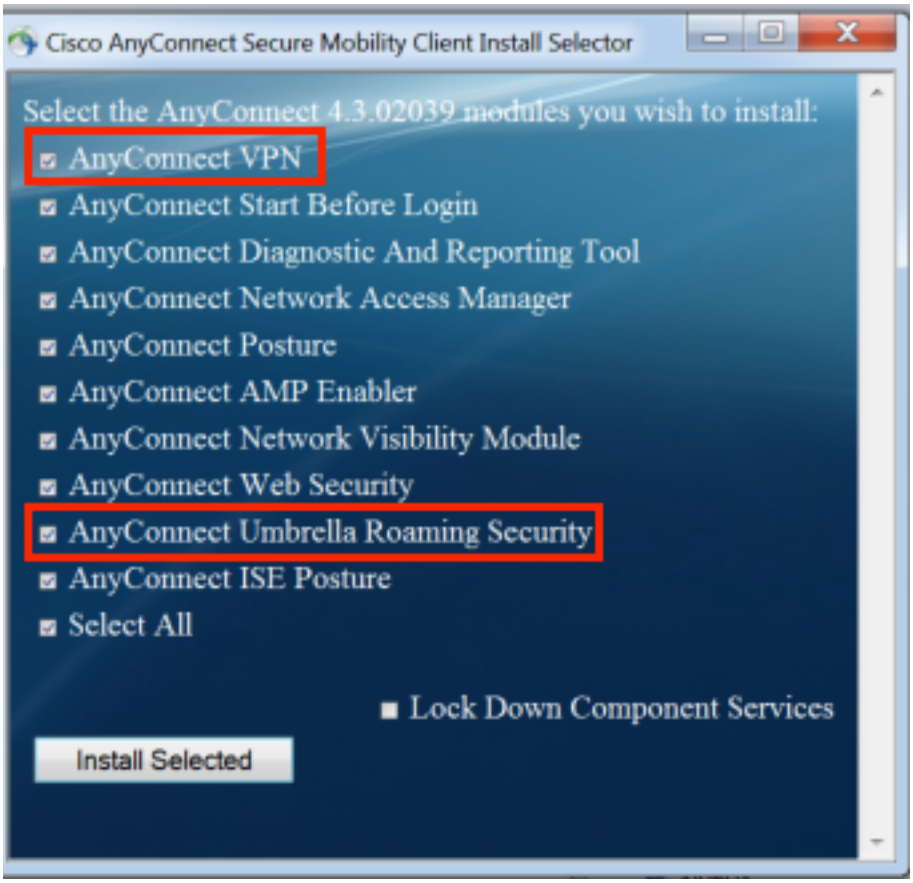
Per integrare il modulo OpenDNS Roaming con il client VPN AnyConnect, il modulo deve essere installato tramite la predistribuzione o il metodo di distribuzione Web:

Metodo di pre-distribuzione (manuale)

La predistribuzione richiede l'installazione manuale del modulo Roaming OpenDNS e la copia del file OrgInfo.json sul computer dell'utente. Le installazioni su larga scala vengono in genere eseguite con i sistemi di gestione software (SMS, Software Management System) aziendali.

Distribuisci modulo roaming OpenDNS

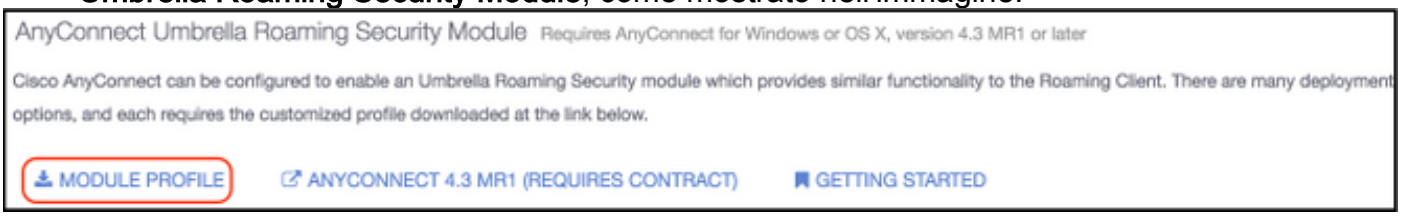
Durante l'installazione del pacchetto AnyConnect, scegliere i moduli **AnyConnect VPN** e **AnyConnect Umbrella Roaming Security**:



Distribuisci OrgInfo.json

Per scaricare il file OrgInfo.json, attenersi alla seguente procedura:

1. Accedere al dashboard OpenDNS.
2. Scegliere **Configurazione > Identità > Computer mobili.**
3. Fare clic sul segno **+**.
4. Scorrere verso il basso e scegliere **Module Profile** (Profilo modulo) nella sezione **Anyconnect Umbrella Roaming Security Module**, come mostrato nell'immagine:



Una volta scaricato, il file deve essere salvato in uno di questi percorsi, che dipende dal sistema operativo.

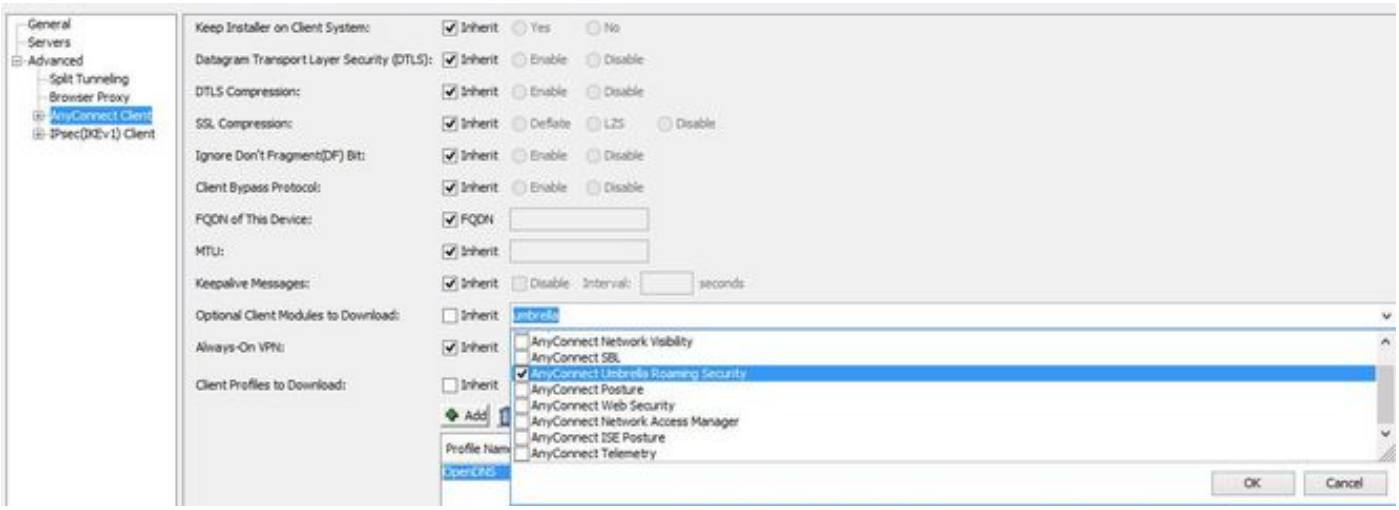
Per Mac OS X: /opt/cisco/anyconnect/Umbrella
Per Windows: C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Umbrella

Metodo di distribuzione Web

Distribuisci modulo roaming OpenDNS

Scaricare il pacchetto Anyconnect Security Mobility Client (ossia anyconnect-win-4.3.02039-k9.pkg) dal sito Web Cisco e caricarlo nella memoria flash dell'ASA. Una volta caricato, in ASDM,

scegliere **Criteri di gruppo > Avanzate > AnyConnect Client > Moduli client facoltativi da scaricare** e quindi **Umbrella Roaming Security.**

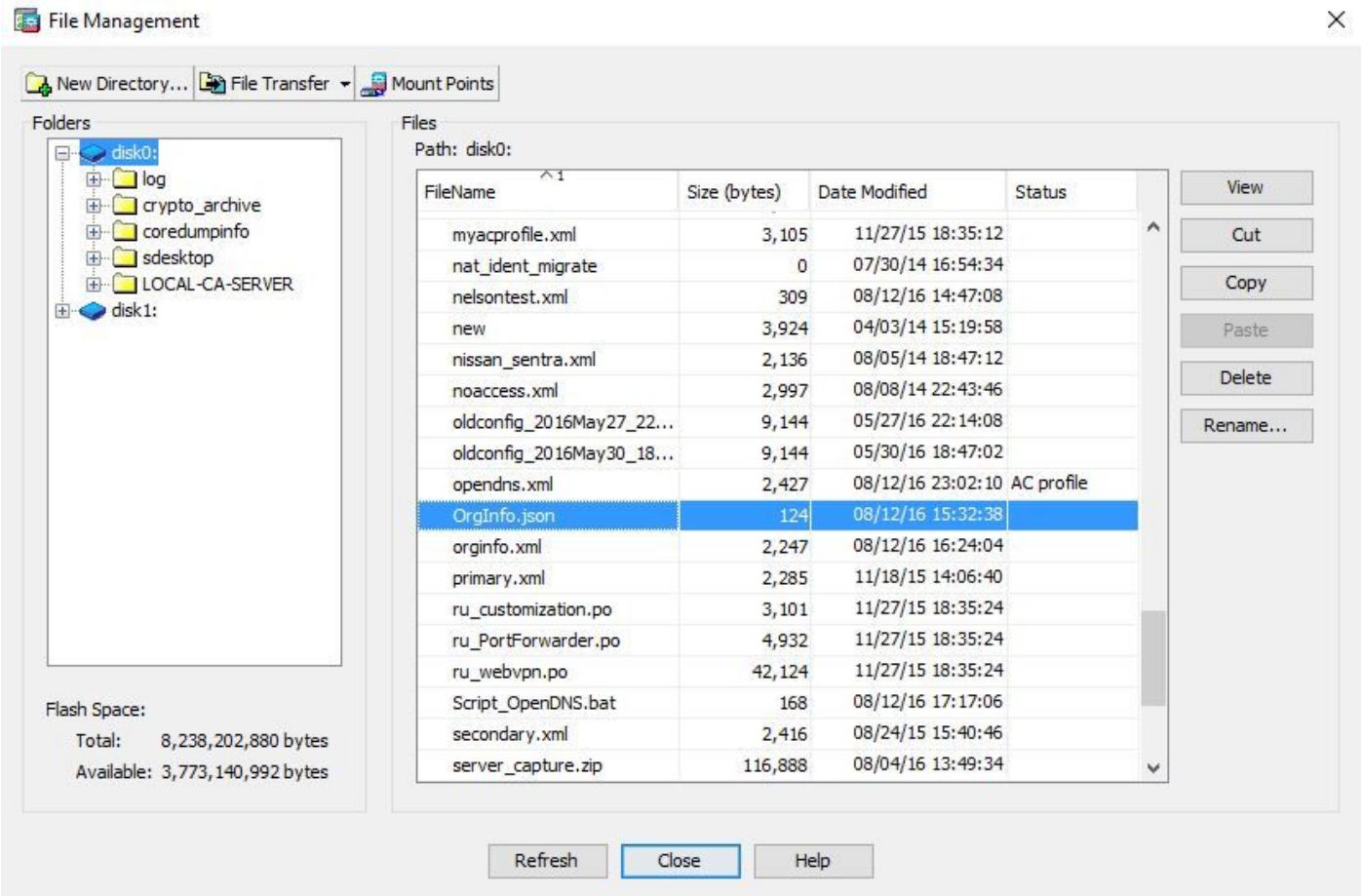


Equivalente alla CLI

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

Distribuisci OrgInfo.json

1. Scaricare il file OrgInfo.json dal dashboard OpenDNS e caricarlo nella memoria flash dell'ASA.



2. Configurare l'ASA in modo che trasferisca il file OrgInfo.json sugli endpoint remoti.

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

> **Nota:** questa configurazione può essere eseguita solo dalla CLI. Per utilizzare ASDM per questo task, è necessario installare ASDM versione 7.6.2 o successive sull'appliance ASA.

Dopo essere stato installato con uno dei metodi descritti, il client Umbrella Roaming deve essere visualizzato come modulo integrato nell'interfaccia utente di AnyConnect, come mostrato nella seguente immagine:

Finché OrgInfo.json non viene distribuito nell'endpoint nella posizione corretta, il modulo Umbrella Roaming non verrà inizializzato.

Configurazione

La sezione mostra alcuni snippet di configurazione CLI di esempio necessari per far funzionare il modulo Roaming DNS Open con le diverse modalità di tunneling di AnyConnect.

```
!--- 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
```

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Per risolvere i problemi relativi a AnyConnect OpenDNS, procedere come segue:

1. Verificare che il modulo Umbrella Roaming Security sia installato insieme al client Anyconnect Secure Mobility.
2. Assicurarsi che OrgInfo.json sia presente sull'endpoint nel percorso corretto basato sul sistema operativo e nel formato specificato in questo documento.
3. Se le query DNS sui resolver OpenDNS devono passare attraverso il tunnel VPN di AnyConnect, verificare che l'appliance ASA sia configurata in modo da consentire la raggiungibilità dei resolver OpenDNS.
4. Raccogliere le acquisizioni dei pacchetti (senza alcun filtro) sulla scheda virtuale e sulla scheda fisica AnyConnect contemporaneamente e individuare i domini che non sono stati risolti.
5. Se il modulo Roaming funziona in stato crittografato, raccogliere le clip dei pacchetti dopo aver bloccato localmente UDP 443, solo per la risoluzione dei problemi. In questo modo si ottiene visibilità sulle transazioni DNS.
6. Eseguire il programma di diagnostica AnyConnect DART, Umbrella e annotare il tempo in cui si è verificato un errore DNS. Per ulteriori informazioni, vedere Come raccogliere il pacchetto DART per Anyconnect.
7. Raccogliere i log di diagnostica Umbrella e inviare l'URL risultante all'amministratore OpenDNS. Solo l'utente corrente e l'amministratore OpenDNS possono accedere a queste informazioni. Per Windows: File C:\Program (x86)\Cisco\Cisco AnyConnect Secure Mobility Client\UmbrellaDiagnostic.exe
   Per Mac OSX: /opt/cisco/anyconnect/bin/UmbrellaDiagnostic

Informazioni correlate

- **ID bug Cisco CSCvb34863: Latenza nella risoluzione del DNS quando AnyConnect è configurato per il tunneling split-include**
- **Documentazione e supporto tecnico – Cisco Systems**