Implementierungsleitfaden für AnyConnect OpenDNS Roaming Security Module

Inhalt

Einführung

Dieses Dokument beschreibt die Schritte zur Installation, Konfiguration und Fehlerbehebung für das OpenDNS (Umbrella) Roaming-Modul. In AnyConnect 4.3.X und höher ist der OpenDNS-Roaming-Client jetzt als integriertes Modul verfügbar. Das Cloud Security-Modul wird auch als Cloud Security-Modul bezeichnet und kann mit dem AnyConnect-Installationsprogramm auf dem Endgerät bereitgestellt oder über das Internet von der Adaptive Security Appliance (ASA) heruntergeladen werden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Cisco AnyConnect Secure Mobility

- OpenDNS/Umbrella Roaming Module
- Cisco ASA

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco ASA Version 9.3(3) 7
- Cisco AnyConnect Secure Mobility Client 4.3.01095
- OpenDNS-Roaming-Modul 4.3.01095
- Cisco Adaptive Security Device Manager (ASDM) 7.6.2 oder höher
- Microsoft Windows 8.1
- **Hinweis**: Die Mindestvoraussetzungen für die Bereitstellung des OpenDNS Umbrella-Moduls sind:
  - AnyConnect VPN Client Version 4.3.01095 oder höher
  - Cisco ASDM 7.6.2 oder höher
  Das OpenDNS-Roaming-Modul wird derzeit auf der Linux-Plattform nicht unterstützt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen von Befehlen oder Konfigurationen verstehen.

Hintergrundinformationen

OrgInfo.json

Damit das OpenDNS-Roaming-Modul ordnungsgemäß funktioniert, muss eine Datei OrgInfo.json aus dem OpenDNS-Dashboard heruntergeladen oder von der ASA gedrängt werden, bevor das Modul verwendet wird. Wenn die Datei zum ersten Mal heruntergeladen wird, wird sie in einem bestimmten Pfad gespeichert, der vom Betriebssystem abhängig ist.

Für Mac OS X wird OrgInfo.json unter /opt/cisco/anyconnect/Umbrella heruntergeladen.
Für Microsoft Windows wird OrgInfo.json unter C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Umbrella heruntergeladen.

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

Wie gezeigt, verwendet die Datei UTF-8-Codierung und enthält eine OrganisationID, einen Fingerabdruck und eine BenutzerID. Die Organisation-ID stellt die Organisationsinformationen für den Benutzer dar, der derzeit im OpenDNS-Dashboard angemeldet ist. Die Organisations-ID ist statisch, eindeutig und wird von OpenDNS für jede Organisation automatisch erstellt. Der Fingerabdruck wird bei der Geräteregistrierung zur Validierung der Datei OrgInfo.json verwendet, und die Benutzer-ID stellt eine eindeutige ID für den angemeldeten Benutzer dar.

Wenn das Roaming-Modul unter Windows startet, wird die Datei OrgInfo.json unter dem Umbrella-

Verzeichnis in das Datenverzeichnis kopiert und als Arbeitskopie verwendet. Auf MAC OS X werden Informationen aus dieser Datei im Datenverzeichnis unter Umbrella auf updater.plist gespeichert. Sobald das Modul erfolgreich Informationen aus der Datei OrgInfo.json gelesen hat, versucht es, sich bei OpenDNS mit einer Cloud-API zu registrieren. Diese Registrierung führt dazu, dass OpenDNS dem Computer, der die Registrierung versucht hat, eine eindeutige Geräte-ID zuweist. Wenn bereits eine Geräte-ID aus der vorherigen Registrierung verfügbar ist, überspringt das Gerät die Registrierung.

Nach Abschluss der Registrierung führt das Roaming-Modul einen Synchronisierungsvorgang durch, um Richtlinieninformationen für den Endpunkt abzurufen. Damit der Synchronisierungsvorgang funktioniert, ist eine Geräte-ID erforderlich. Synchronisierungsdaten umfassen u. a. SyncInterval, interne Bypass-Domänen und IP-Adressen. Das Synchronisierungsintervall ist die Anzahl der Minuten, nach denen das Modul versuchen soll, eine Neusynchronisierung durchzuführen.

DNS-Testverhalten

Nach erfolgreicher Registrierung und Synchronisierung sendet das Roaming-Modul DNS-Abfragen (Domain Name System) an seine lokalen Resolver. Diese DNS-Anfragen umfassen TXT-Abfragen für debug.opendns.com. Basierend auf der Antwort kann der Client bestimmen, ob eine lokale OpenDNS Virtual Appliance (VA) im Netzwerk vorhanden ist.

Wenn eine virtuelle Appliance (VA) vorhanden ist, wechselt der Client in den "Behind-VA"-Modus, und die DNS-Durchsetzung wird auf dem Endpunkt nicht durchgeführt. Der Client verlässt sich bei der DNS-Durchsetzung auf Netzwerkebene auf die VA.

Wenn keine VA vorhanden ist, sendet der Client mithilfe von UDP/443 eine DNS-Anforderung an die öffentlichen OpenDNS-Resolver (208.67.222.222).

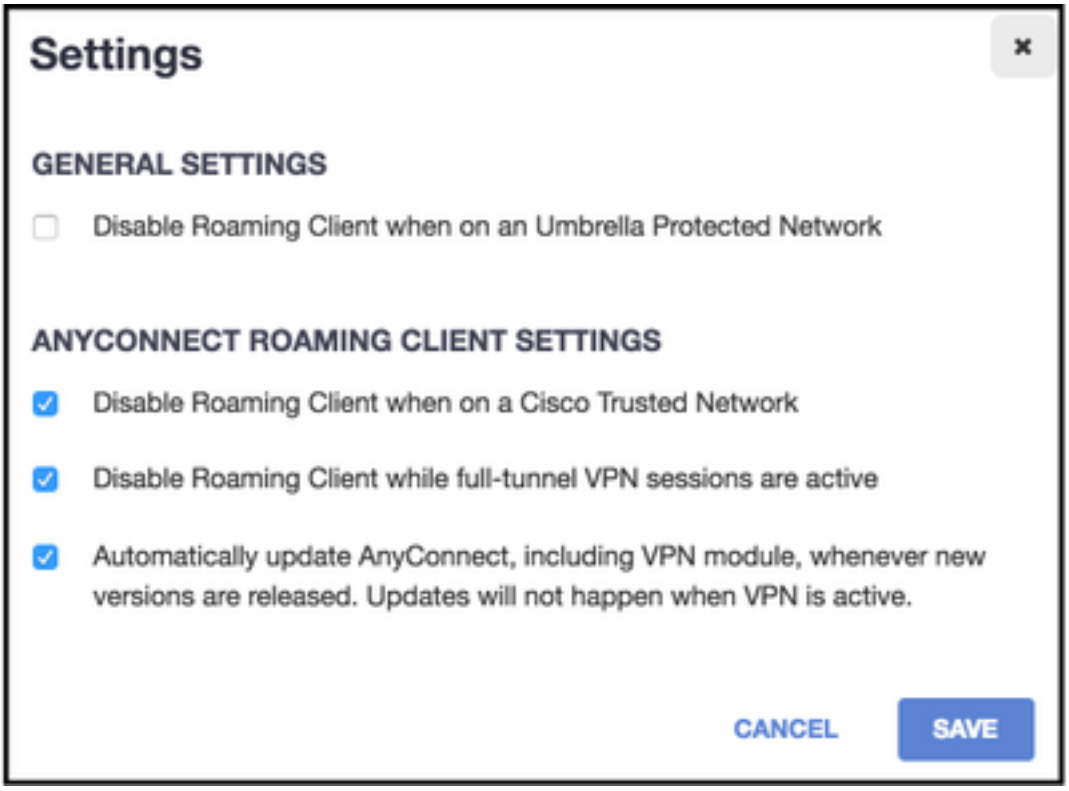
Eine positive Antwort weist darauf hin, dass eine DNS-Verschlüsselung möglich ist. Wenn eine negative Antwort empfangen wird, sendet der Client mithilfe von UDP/53 eine DNS-Anforderung an die öffentlichen OpenDNS-Resolver.

Eine positive Antwort auf diese Abfrage weist darauf hin, dass DNS-Schutz möglich ist. Wenn eine negative Antwort empfangen wird, versucht der Client die Abfrage innerhalb weniger Sekunden erneut.

Nach Erhalt einer festgelegten Anzahl negativer Antworten wechselt der Client in den Fail-Open-Zustand. Ein Fail-Open-Zustand bedeutet, dass eine DNS-Verschlüsselung und/oder ein Schutz nicht möglich ist. Sobald das Roaming-Modul erfolgreich in einen geschützten und/oder verschlüsselten Zustand übergegangen ist, werden alle DNS-Abfragen für Suchdomänen außerhalb der lokalen Suchdomänen und internen Umgehungsdomänen zur Namensauflösung an die OpenDNS-Resolver gesendet. Wenn der verschlüsselte Zustand aktiviert ist, werden alle DNS-Transaktionen durch den Entschlüsselungsprozess verschlüsselt.

DNS-Verhalten mit AnyConnect Tunneling-Modi

1. Tunnel-All (oder tunnel-all-DNS aktiviert)



Hinweis: Wie gezeigt, deaktiviert das Roaming-Modul standardmäßig den DNS-Schutz, während ein VPN-Tunnel mit der Konfiguration des gesamten Tunnels aktiv ist. Damit das Modul während einer Konfiguration für den AnyConnect-Tunnel aktiv ist, muss die Option **Roaming-Client deaktivieren**, **während Full-Tunnel-VPN-Sitzungen aktiv sind,** im OpenDNS-Portal deaktiviert sein. Um diese Funktion aktivieren zu können, ist ein erweitertes Abonnement mit OpenDNS erforderlich. Die folgenden Informationen setzen voraus, dass der DNS-Schutz über das Roaming-Modul aktiviert ist.

Abfragter Domänenteil der internen Umgehungsliste

DNS-Anfragen vom Tunnel-Adapter sind zulässig und werden über den VPN-Tunnel an die Tunnel-DNS-Server gesendet. Die Abfrage bleibt ungelöst, wenn sie nicht durch die Tunnel-DNS-Server aufgelöst werden kann.

Die abgefragte Domäne gehört nicht zur internen Umgehungsliste.

DNS-Anfragen vom Tunnel-Adapter sind zulässig, werden über das Roaming-Modul an die öffentlichen OpenDNS-Resolver weitergeleitet und über den VPN-Tunnel gesendet. Dem DNS-Client erscheint es so, als ob die Namensauflösung über den VPN DNS-Server erfolgt wäre. Wenn die Namensauflösung über OpenDNS-Resolver nicht erfolgreich ist, wird das Roaming-Modul auf die lokal konfigurierten DNS-Server umgeschaltet, beginnend mit dem VPN-Adapter (dem bevorzugten Adapter bei aktiviertem Tunnel).

2. Split-DNS (tunnel-all-DNS deaktiviert)

Hinweis: Alle Split-DNS-Domänen werden bei der Tunneleinrichtung automatisch zur internen Umgehungsliste des Roaming-Moduls hinzugefügt. Dies geschieht, um einen konsistenten DNS-Verarbeitungsmechanismus zwischen AnyConnect und dem Roaming-Modul bereitzustellen. Stellen Sie sicher, dass in einer Split-DNS-Konfiguration (mit Split-Include-Tunneling) die öffentlichen OpenDNS-Resolver nicht in Split-Include-Netzwerke

enthalten sind.

Hinweis: Wenn unter Mac OS X Split-DNS für beide IP-Protokolle (IPv4 und IPv6) aktiviert ist oder nur für ein Protokoll aktiviert ist und es keinen Adresspool für das andere Protokoll gibt, wird echter Split-DNS, ähnlich wie Windows, erzwungen.
Wenn Split-DNS nur für ein Protokoll aktiviert ist und dem anderen Protokoll eine Client-Adresse zugewiesen ist, wird nur der DNS-Fallback für Split-Tunneling erzwungen. Dies bedeutet, dass AnyConnect nur DNS-Anfragen zulässt, die über Tunnel mit den Split-DNS-Domänen übereinstimmen (andere Anfragen werden von der AC beantwortet, wobei die Antwort verweigert wird, um Failover auf öffentliche DNS-Server zu erzwingen), jedoch nicht durchsetzen kann, dass Anfragen, die Split-DNS-Domänen entsprechen, nicht über den öffentlichen Adapter in Klarform gesendet werden.

Abfragter Domänenteil der internen Umgehungsliste und Teil von Split-DNS-Domänen

DNS-Anfragen vom Tunnel-Adapter sind zulässig und werden über den VPN-Tunnel an die Tunnel-DNS-Server gesendet. Alle anderen Anfragen nach passenden Domänen von anderen Adaptern werden vom AnyConnect-Treiber mit "no such name" beantwortet, um eine echte Split-DNS-Abfrage (Vermeidung von DNS-Fallback) zu erreichen. Daher ist nur DNS-Verkehr ohne Tunnel durch das Roaming-Modul geschützt.

Abfragter Domänenteil der internen Umgehungsliste, aber nicht Teil von Split-DNS-Domänen

DNS-Anfragen vom physischen Adapter sind zulässig und werden außerhalb des VPN-Tunnels an die öffentlichen DNS-Server gesendet. Alle anderen Anfragen nach passenden Domänen vom Tunnel-Adapter werden vom AnyConnect-Treiber mit "no such name" beantwortet, um zu verhindern, dass die Abfrage über den VPN-Tunnel gesendet wird.

Die abgefragte Domäne gehört nicht zur internen Umgehungsliste oder zu Split-DNS-Domänen.

DNS-Anfragen vom physischen Adapter werden zugelassen, an die öffentlichen OpenDNS-Resolver weitergeleitet und außerhalb des VPN-Tunnels gesendet. Dem DNS-Client erscheint es so, als ob die Namensauflösung über den öffentlichen DNS-Server erfolgt wäre. Wenn die Namensauflösung über OpenDNS-Resolver nicht erfolgreich ist, wird das Roaming-Modul auf die lokal konfigurierten DNS-Server umgeschaltet, mit Ausnahme der auf dem VPN-Adapter konfigurierten Server. Alle anderen Anfragen nach passenden Domänen vom Tunnel-Adapter werden vom AnyConnect-Treiber ohne diesen Namen beantwortet, um zu verhindern, dass die Abfrage über den VPN-Tunnel gesendet wird.

3. Split-Include oder Split-Exclude Tunneling (kein Split-DNS und Tunnel-all-DNS deaktiviert)

Abfragter Domänenteil der internen Umgehungsliste

Der native Betriebssystemresolver führt die DNS-Auflösung auf der Grundlage der Reihenfolge der Netzwerkadapter aus, und AnyConnect ist der bevorzugte Adapter, wenn VPN aktiv ist. DNS-Anfragen stammen zunächst vom Tunnel-Adapter und werden über den VPN-Tunnel an die Tunnel-DNS-Server gesendet. Wenn die Abfrage nicht durch die Tunnel-DNS-Server aufgelöst werden kann, versucht der OS-Resolver, sie über die öffentlichen DNS-Server aufzulösen.

Die abgefragte Domäne gehört nicht zur internen Umgehungsliste.

Der native Betriebssystemresolver führt die DNS-Auflösung auf der Grundlage der Reihenfolge der Netzwerkadapter aus, und AnyConnect ist der bevorzugte Adapter, wenn VPN aktiv ist. DNS-Anfragen stammen zunächst vom Tunnel-Adapter und werden über den VPN-Tunnel an die Tunnel-DNS-Server gesendet. Wenn die Abfrage nicht durch die Tunnel-DNS-Server aufgelöst werden kann, versucht der OS-Resolver, sie über die öffentlichen DNS-Server aufzulösen.

Wenn die öffentlichen OpenDNS-Resolver Teil der Split-Include-Liste sind oder nicht Teil der Split-Exclude-Liste sind, wird die proxiierte Anforderung über den VPN-Tunnel gesendet.

Wenn die öffentlichen OpenDNS-Resolver nicht Teil der Split-Include-Liste oder Teil der Split-Exclude-Liste sind, wird die proxiierte Anforderung außerhalb des VPN-Tunnels gesendet.

Wenn die Namensauflösung über OpenDNS-Resolver nicht erfolgreich ist, wird das Roaming-Modul auf die lokal konfigurierten DNS-Server umgeschaltet, beginnend mit dem VPN-Adapter (dem bevorzugten Adapter bei aktiviertem Tunnel). Wenn die letzte Antwort, die vom Roaming-Modul zurückgegeben (und zurück an den nativen DNS-Client geleitet) wird, nicht erfolgreich ist, versucht der native Client andere DNS-Server, falls verfügbar.

Installieren und Konfigurieren des Umbrella Roaming Module

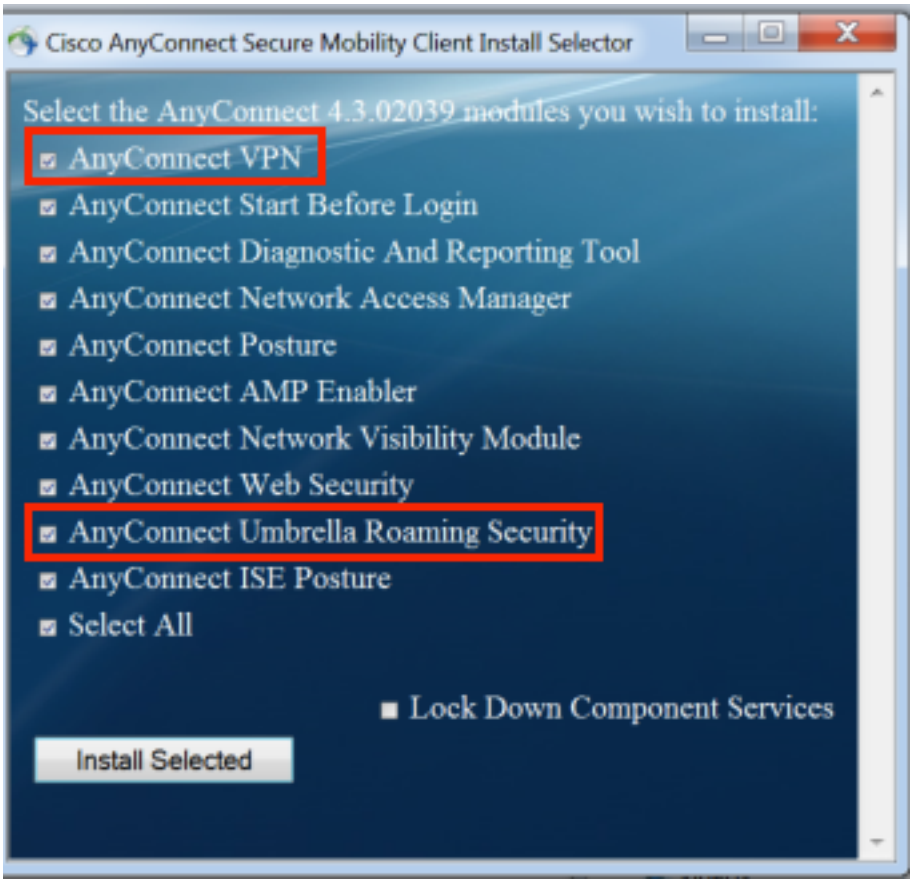
Um das OpenDNS-Roaming-Modul in den AnyConnect VPN-Client zu integrieren, muss das Modul entweder über eine Bereitstellungsmethode oder eine Web-Bereitstellungsmethode installiert werden:

Methode vor der Bereitstellung (manuell)

Vor der Bereitstellung müssen das OpenDNS-Roaming-Modul manuell installiert und die Datei OrgInfo.json auf den Benutzercomputer kopiert werden. Große Bereitstellungen werden in der Regel mit Enterprise Software Management Systemen (SMS) erreicht.

OpenDNS-Roaming-Modul bereitstellen

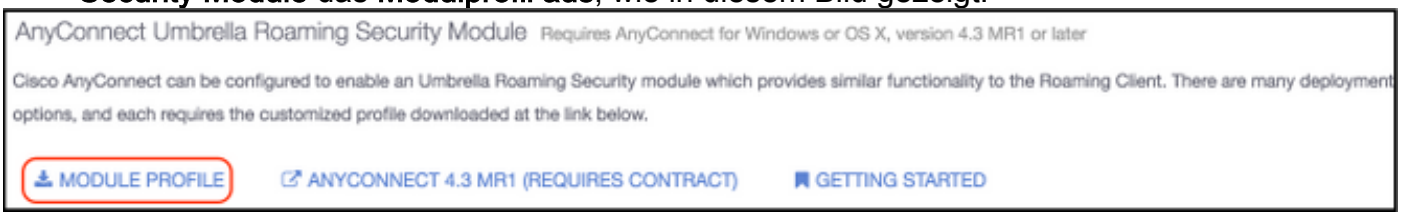
Wählen Sie bei der Installation des AnyConnect-Pakets die Module **AnyConnect VPN** und **AnyConnect Umbrella Roaming Security**:



Bereitstellen von OrgInfo.json

Gehen Sie wie folgt vor, um die Datei OrgInfo.json herunterzuladen:

1. Melden Sie sich beim OpenDNS-Dashboard an.
2. Wählen Sie **Configuration > Identities > Roaming Computers aus.**
3. Klicken Sie auf das **+**-Zeichen.
4. Blättern Sie nach unten, und wählen Sie im Abschnitt des **AnyConnect Umbrella Roaming Security Module** das **Modulprofil aus**, wie in diesem Bild gezeigt:



Sobald die Datei heruntergeladen wurde, muss sie in einem dieser Pfade gespeichert werden, der vom Betriebssystem abhängig ist.

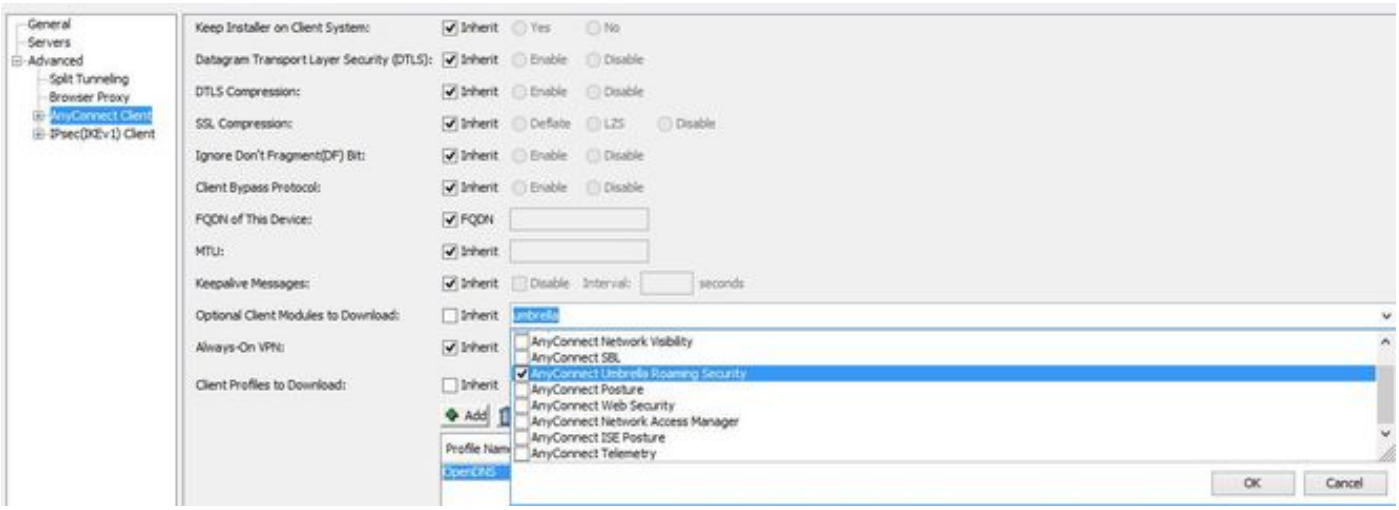
Für Mac OS X: /opt/cisco/anyconnect/Umbrella
Für Windows: C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Umbrella

Webbereitstellungsmethode

OpenDNS-Roaming-Modul bereitstellen

Laden Sie das AnyConnect Security Mobility Client-Paket (d. h. anyconnect-win-4.3.02039-k9.pkg) von der Cisco Website herunter und laden Sie es in den Flash-Speicher der ASA hoch. Wählen

Sie nach dem Hochladen im ASDM **Gruppenrichtlinie > Erweitert > AnyConnect-Client > Optionale Client-Module zum Herunterladen aus,** und wählen Sie dann **Umbrella Roaming Security** aus.

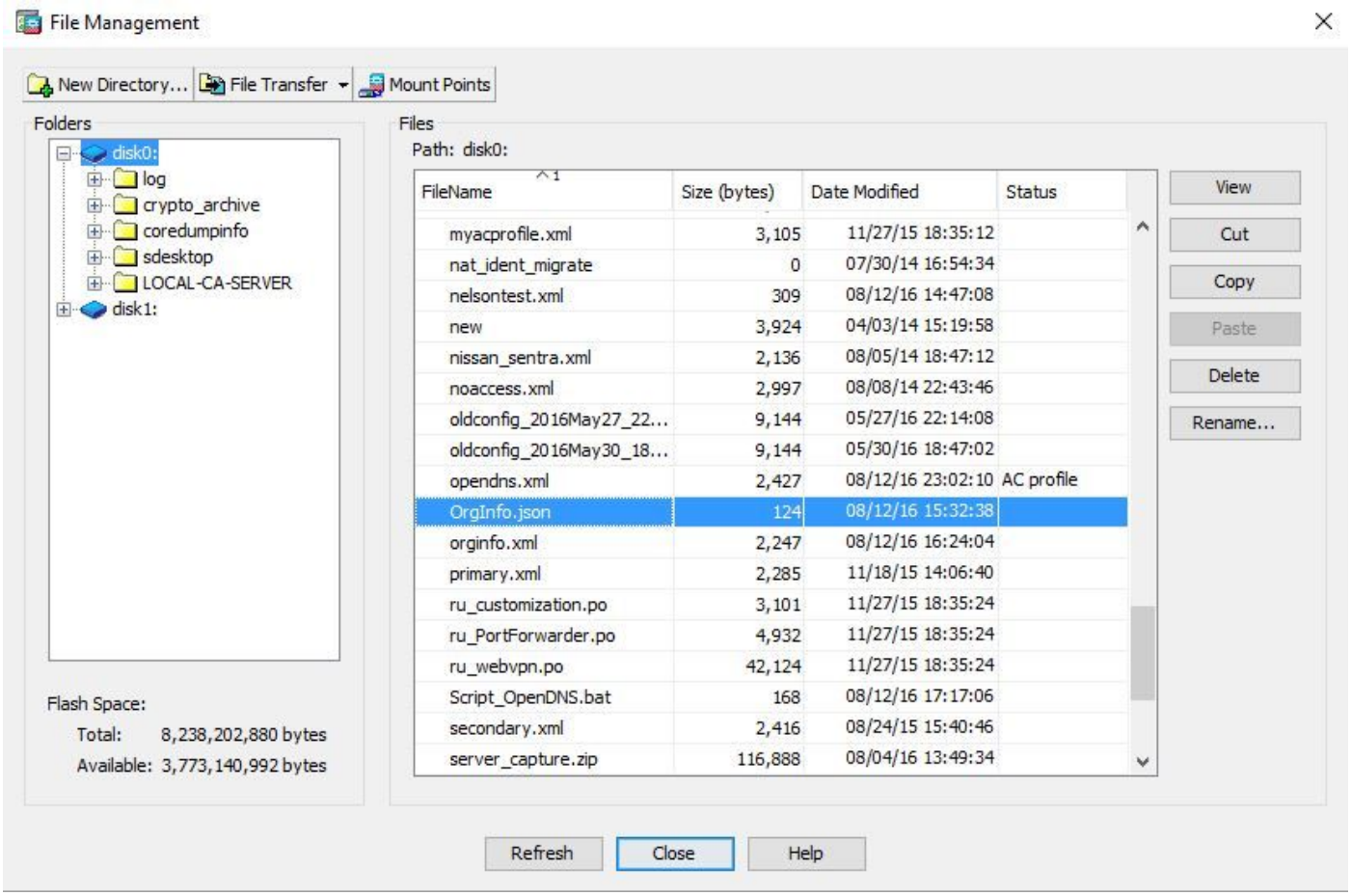


CLI-Äquivalent

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

Bereitstellen von OrgInfo.json

1. Laden Sie die Datei OrgInfo.json vom OpenDNS-Dashboard herunter und laden Sie sie in den Flash-Speicher der ASA hoch.



2. Konfigurieren Sie die ASA so, dass die Datei OrgInfo.json an Remote-Endpunkte gesendet wird.

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

> **Hinweis**: Diese Konfiguration kann nur über die CLI vorgenommen werden. Um ASDM für diese Aufgabe verwenden zu können, muss ASDM Version 7.6.2 oder höher auf der ASA installiert sein.

Sobald der Umbrella Roaming Client über eine der oben beschriebenen Methoden installiert wurde, sollte er als integriertes Modul in der AnyConnect GUI angezeigt werden, wie in diesem Bild gezeigt:

Bis die OrgInfo.json auf dem Endpunkt am richtigen Standort bereitgestellt ist, wird das Umbrella Roaming-Modul nicht initialisiert.

Konfigurieren

Der Abschnitt zeigt Beispiele für CLI-Konfigurationsausschnitte, die für den Betrieb des OpenDNS-Roaming-Moduls mit den verschiedenen AnyConnect-Tunneling-Modi erforderlich sind.

```
!--- 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
```

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Schritte zur Fehlerbehebung bei Problemen im Zusammenhang mit AnyConnect OpenDNS:

1. Stellen Sie sicher, dass das Umbrella Roaming Security-Modul zusammen mit dem AnyConnect Secure Mobility Client installiert ist.
2. Stellen Sie sicher, dass OrgInfo.json auf dem Endpunkt im richtigen Pfad des Betriebssystems im angegebenen Format vorhanden ist.
3. Wenn DNS-Abfragen an OpenDNS-Resolver über den AnyConnect VPN-Tunnel geleitet werden sollen, stellen Sie sicher, dass der Hairpin auf der ASA konfiguriert ist, um die Erreichbarkeit von OpenDNS-Resolvern zu ermöglichen.
4. Sammeln Sie gleichzeitig Paketerfassungen (ohne Filter) auf dem virtuellen AnyConnect-Adapter und dem physischen Adapter, und notieren Sie die Domänen, die nicht aufgelöst werden können.
5. Wenn das Roaming-Modul verschlüsselt betrieben wird, sammeln Sie Paketerfassungen, nachdem Sie UDP 443 lokal blockiert haben, nur zu Fehlerbehebungszwecken. Auf diese Weise werden die DNS-Transaktionen transparent.
6. Führen Sie die AnyConnect DART-, Umbrella-Diagnose aus, und notieren Sie sich die Zeit, zu der der DNS-Fehler auftritt. Weitere Informationen finden Sie unter Sammeln des DART-Pakets für AnyConnect.
7. Sammeln Sie Umbrella-Diagnoseprotokolle und senden Sie die resultierende URL an Ihren OpenDNS-Administrator. Nur Sie und der OpenDNS-Administrator haben Zugriff auf diese Informationen. Für Windows: C:\Program Files (x86)\Cisco\Cisco AnyConnect Secure Mobility Client\UmbrellaDiagnostic.exe
   Für Mac OSX: /opt/cisco/anyconnect/bin/UmbrellaDiagnostic

Zugehörige Informationen

- Cisco Bug-ID CSCvb34863: Latenz bei der Auflösung von DNS, wenn AnyConnect für Split-Include-Tunneling konfiguriert ist
- Technischer Support und Dokumentation - Cisco Systems