AnyConnect OpenDNS 로밍 보안 모듈 구축 설명서

목차

소개

이 문서에서는 OpenDNS(Umbrella) 로밍 모듈의 설치, 구성 및 문제 해결 단계에 대해 설명합니다 .AnyConnect 4.3.X 이상에서 OpenDNS 로밍 클라이언트를 통합 모듈로 사용할 수 있습니다.Cloud Security 모듈이라고도 하며 AnyConnect 설치 프로그램을 사용하여 엔드포인트에 사전 구축하거나 웹 구축을 통해 ASA(Adaptive Security Appliance)에서 다운로드할 수 있습니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco AnyConnect Secure Mobility
- OpenDNS/Umbrella Roaming Module
- Cisco ASA

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ASA 버전 9.3(3)7
- Cisco AnyConnect Secure Mobility Client 4.3.01095
- OpenDNS 로밍 모듈 4.3.01095
- Cisco ASDM(Adaptive Security Device Manager) 7.6.2 이상
- Microsoft Windows 8.1
- **참고:**OpenDNS Umbrella 모듈을 구축하는 최소 요구 사항은 다음과 같습니다.
  - AnyConnect VPN 클라이언트 버전 4.3.01095 이상
  - Cisco ASDM 7.6.2 이상
  OpenDNS 로밍 모듈은 현재 Linux 플랫폼에서 지원되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.네트워크가 작동 중인 경우 모든 명령 또는 컨피그레이션의 잠재적인 영향을 이해해야 합니다.

배경 정보

OrgInfo.json

OpenDNS 로밍 모듈이 제대로 작동하려면 모듈을 사용하기 전에 OpenDNS 대시보드에서 OrgInfo.json 파일을 다운로드하거나 ASA에서 푸시해야 합니다.파일을 처음 다운로드하면 운영 체제에 따라 특정 경로에 저장됩니다.

Mac OS X의 경우 OrgInfo.json이 /opt/cisco/anyconnect/Umbrella에 다운로드됩니다.
Microsoft Windows의 경우 OrgInfo.json이 C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Umbrella으로 다운로드됩니다.

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

표시된 대로 파일은 UTF-8 인코딩을 사용하며 organizationId, fingerprint 및 userId를 포함합니다.조직 ID는 현재 OpenDNS 대시보드에 로그인한 사용자의 조직 정보를 나타냅니다.조직 ID는 OpenDNS에서 각 조직에 대해 정적이고 고유하며 자동으로 생성됩니다.핑거프린트는 디바이스 등록 중에 OrgInfo.json 파일의 유효성을 검사하는 데 사용되며 사용자 ID는 로그인한 사용자의 고유 ID를 나타냅니다.

Windows에서 로밍 모듈을 시작하면 OrgInfo.json 파일이 Umbrella 디렉터리 아래의 데이터 디렉터리에 복사되고 작업 복사본으로 사용됩니다.MAC OS X에서 이 파일의 정보는 Umbrella 디렉토리 아래의 데이터 디렉토리에 updater.plist에 저장됩니다.모듈은 OrgInfo.json 파일에서 정보를 성공적으로 읽으면 클라우드 API를 사용하여 OpenDNS에 등록하려고 시도합니다.이 등록을 수행하면 OpenDNS가 등록을 시도한 시스템에 고유한 디바이스 ID를 할당합니다.이전 등록의 디바이스 ID를 이미 사용할 수 있는 경우 디바이스에서 등록을 건너뜁니다.

등록이 완료되면 로밍 모듈은 엔드포인트에 대한 정책 정보를 검색하기 위해 동기화 작업을 수행합니다.동기화 작업이 작동하려면 장치 ID가 필요합니다.동기화 데이터에는 syncInterval, 내부 바이

패스 도메인, IP 주소가 포함됩니다.동기화 간격은 모듈이 재동기화를 시도해야 하는 시간(분)입니다.

DNS 탐색 동작

등록 및 동기화가 완료되면 로밍 모듈은 DNS(Domain Name System) 프로브를 로컬 리졸버로 전송합니다.이러한 DNS 요청에는 debug.opendns.com에 대한 TXT 쿼리가 포함됩니다.응답에 따라 클라이언트는 온프레미스 OpenDNS VA(Virtual Appliance)가 네트워크에 존재하는지 확인할 수 있습니다.

가상 어플라이언스(VA)가 있는 경우 클라이언트는 'behind-VA' 모드로 전환되며 엔드포인트에서 DNS 시행이 수행되지 않습니다.클라이언트는 네트워크 레벨에서 DNS 시행을 위해 VA를 사용합니다.

VA가 없는 경우 클라이언트는 UDP/443을 사용하여 OpenDNS 공용 리졸버(208.67.222.222)에 DNS 요청을 보냅니다.

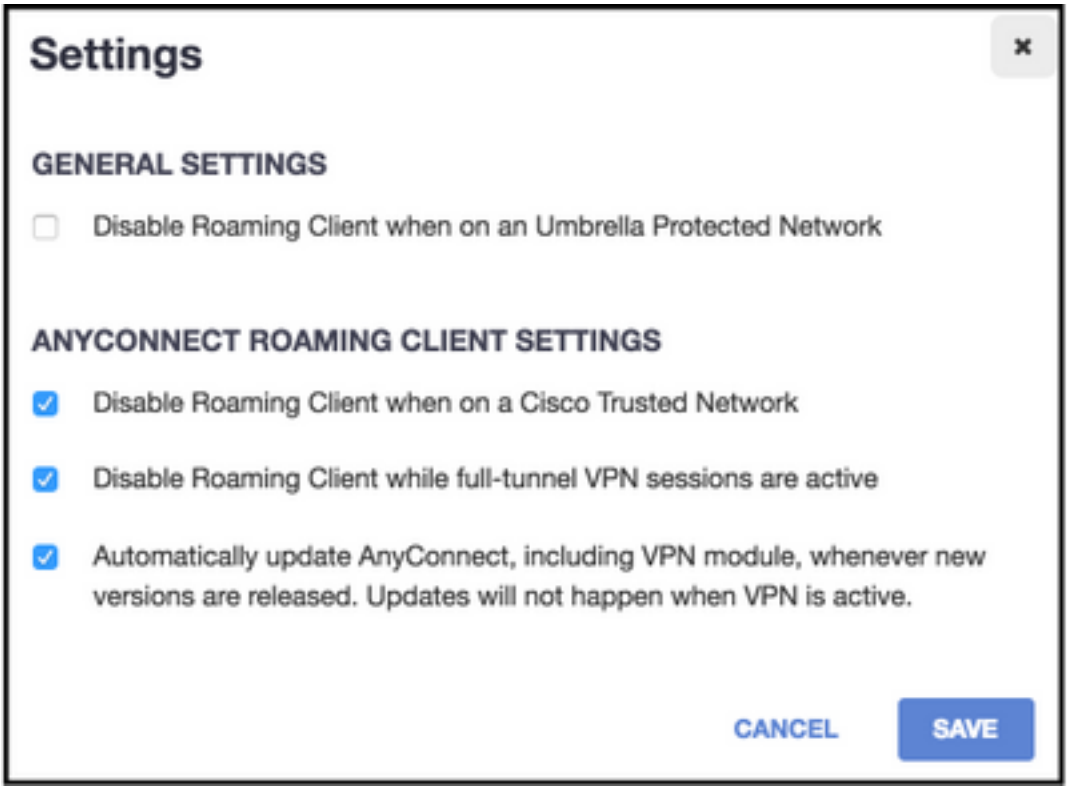
긍정적인 응답은 DNS 암호화가 가능함을 나타냅니다.부정적인 응답이 수신되면 클라이언트는 UDP/53을 사용하여 OpenDNS 공용 확인자에게 DNS 요청을 보냅니다.

이 쿼리에 대한 긍정적인 응답은 DNS 보호가 가능함을 나타냅니다.부정적인 응답이 수신되면 클라이언트는 몇 초 내에 쿼리를 다시 시도합니다.

설정된 수의 음수 응답을 수신하면 클라이언트는 실패 열기 상태로 전환됩니다.fail-open 상태는 DNS 암호화 및/또는 보호가 불가능함을 의미합니다.로밍 모듈이 보호 및/또는 암호화 상태로 전환되면 로컬 검색 도메인 및 내부 바이패스 도메인 외부의 검색 도메인에 대한 모든 DNS 쿼리가 이름 확인을 위해 OpenDNS 확인기로 전송됩니다.암호화된 상태가 활성화된 경우 모든 DNS 트랜잭션은 dnscrypt 프로세스에 의해 암호화됩니다.

AnyConnect 터널링 모드의 DNS 동작

1. Tunnel-All(또는 tunnel-all-DNS 사용)



참고:표시된 대로 기본 동작은 터널-모두 컨피그레이션이 있는 VPN 터널이 활성 상태일 때 로밍 모듈에서 DNS 보호를 비활성화하는 것입니다.AnyConnect tunnel-all 컨피그레이션 중에 모듈을 활성화하려면 OpenDNS 포털**에서 Disable roaming client while full-tunnel VPN sessions are active** 옵션을 선택 취소해야 합니다.이 기능을 사용하려면 OpenDNS의 고급 서브스크립션 레벨이 필요합니다.아래 정보에서는 로밍 모듈을 통한 DNS 보호가 활성화된 것으로 가정합니다.

내부 바이패스 목록의 쿼리된 도메인 부분

터널 어댑터에서 시작된 DNS 요청은 VPN 터널을 통해 터널 DNS 서버로 허용되고 전송됩니다.터널 DNS 서버에서 쿼리를 확인할 수 없는 경우 쿼리는 확인되지 않습니다.

쿼리한 도메인이 내부 바이패스 목록에 포함되지 않음

터널 어댑터에서 시작되는 DNS 요청은 허용되며, 로밍 모듈을 통해 OpenDNS 공용 확인기로 프록시되고 VPN 터널을 통해 전송됩니다.DNS 클라이언트에는 VPN DNS 서버를 통해 이름 확인이 발생한 것처럼 표시됩니다.OpenDNS 리졸버를 통한 이름 확인에 성공하지 못하면 로밍 모듈은 VPN 어댑터(터널이 작동 중인 동안 기본 설정 어댑터)부터 시작하여 로컬로 구성된 DNS 서버로 장애 조치됩니다.

2. 스플릿-DNS(tunnel-all-DNS 사용 안 함)

참고:모든 스플릿 DNS 도메인이 터널 설정 시 로밍 모듈 내부 바이패스 목록에 자동으로 추가됩니다.이는 AnyConnect와 로밍 모듈 간에 일관된 DNS 처리 메커니즘을 제공하기 위해 수행됩니다.스플릿-DNS 컨피그레이션(스플릿-포함 터널링 사용)에서 OpenDNS 공용 리졸버가 스플릿-포함 네트워크에 포함되지 않았는지 확인합니다.

참고: Mac OS X에서 IP 프로토콜(IPv4 및 IPv6)에 대해 split-DNS가 활성화되었거나 한 프로토콜에 대해서만 활성화되고 다른 프로토콜에 대해 구성된 주소 풀이 없는 경우 Windows와

유사한 true split-DNS가 적용됩니다.
스플릿-DNS가 한 프로토콜에 대해서만 활성화되고 다른 프로토콜에 대해 클라이언트 주소가 할당된 경우 스플릿 터널링에 대한 DNS 폴백만 적용됩니다.즉, AnyConnect는 터널을 통해 스플릿-DNS 도메인과 일치하는 DNS 요청만 허용합니다(다른 요청은 AC에서 퍼블릭 DNS 서버로 장애 조치를 강제하기 위해 거부된 응답으로 응답함). 그러나 스플릿-DNS 도메인과 일치하는 요청은 공용 어댑터를 통해 암호화되지 않습니다.

내부 바이패스 목록의 쿼리 도메인 부분 및 스플릿-DNS 도메인의 일부

터널 어댑터에서 시작된 DNS 요청은 VPN 터널을 통해 터널 DNS 서버로 허용되고 전송됩니다.다른 어댑터에서 일치하는 도메인에 대한 다른 모든 요청은 진정한 스플릿 DNS를 얻기 위해 'no such name'을 가진 AnyConnect 드라이버에서 응답합니다(DNS 폴백 방지). 따라서 터널이 아닌 DNS 트래픽만 로밍 모듈에 의해 보호됩니다.

내부 바이패스 목록의 쿼리된 도메인 부분이지만 스플릿-DNS 도메인에 속하지 않음

물리적 어댑터에서 시작된 DNS 요청은 VPN 터널 외부의 공용 DNS 서버로 허용되고 전송됩니다.터널 어댑터에서 일치하는 도메인에 대한 다른 모든 요청은 VPN 터널을 통해 쿼리가 전송되지 않도록 AnyConnect 드라이버가 'no such name'으로 응답합니다.

쿼리한 도메인이 내부 바이패스 목록 또는 스플릿-DNS 도메인에 속하지 않음

물리적 어댑터에서 시작된 DNS 요청은 OpenDNS 공용 확인기로 허용 및 프록시되고 VPN 터널 외부로 전송됩니다.DNS 클라이언트에는 공용 DNS 서버를 통해 이름 확인이 발생한 것처럼 표시됩니다.OpenDNS 리졸버를 통한 이름 확인에 실패하면 로밍 모듈은 VPN 어댑터에 구성된 DNS 서버를 제외하고 로컬로 구성된 DNS 서버로 장애 조치됩니다.터널 어댑터에서 일치하는 도메인에 대한 다른 모든 요청은 해당 이름이 없는 AnyConnect 드라이버에 의해 응답되어 쿼리가 VPN 터널을 통해 전송되는 것을 방지합니다.

3. 스플릿-포함 또는 스플릿-제외 터널링(스플릿-DNS 및 tunnel-all-DNS가 비활성화되지 않음)

내부 바이패스 목록의 쿼리된 도메인 부분

네이티브 OS 확인자는 네트워크 어댑터의 순서를 기반으로 DNS 확인을 수행하고, VPN이 활성 상태일 때 AnyConnect가 기본 어댑터입니다.DNS 요청은 먼저 터널 어댑터에서 시작되어 VPN 터널을 통해 터널 DNS 서버로 전송됩니다.터널 DNS 서버에서 쿼리를 확인할 수 없는 경우 OS 확인자는 공용 DNS 서버를 통해 쿼리를 확인하려고 시도합니다.

쿼리한 도메인이 내부 바이패스 목록에 포함되지 않음

네이티브 OS 확인자는 네트워크 어댑터의 순서를 기반으로 DNS 확인을 수행하고, VPN이 활성 상태일 때 AnyConnect가 기본 어댑터입니다.DNS 요청은 먼저 터널 어댑터에서 시작되어 VPN 터널을 통해 터널 DNS 서버로 전송됩니다.터널 DNS 서버에서 쿼리를 확인할 수 없는 경우 OS 확인자는 공용 DNS 서버를 통해 쿼리를 확인하려고 시도합니다.

OpenDNS 공용 확인자가 split-include 목록의 일부이거나 split-exclude 목록의 일부가 아닌 경우 프록시된 요청이 VPN 터널을 통해 전송됩니다.

OpenDNS 공용 확인자가 split-include 목록 또는 split-exclude 목록의 일부가 아닌 경우 프록시된 요청은 VPN 터널 외부에서 전송됩니다.

OpenDNS 리졸버를 통한 이름 확인에 성공하지 못하면 로밍 모듈은 VPN 어댑터(터널이 작동 중인 동안 기본 설정 어댑터)부터 시작하여 로컬로 구성된 DNS 서버로 장애 조치됩니다. 로밍 모듈에서 반환된 최종 응답(그리고 네이티브 DNS 클라이언트로 다시 프록시됨)이 실패하면 네이티브 클라이언트는 사용 가능한 경우 다른 DNS 서버를 시도합니다.

Umbrella Roaming 모듈 설치 및 구성

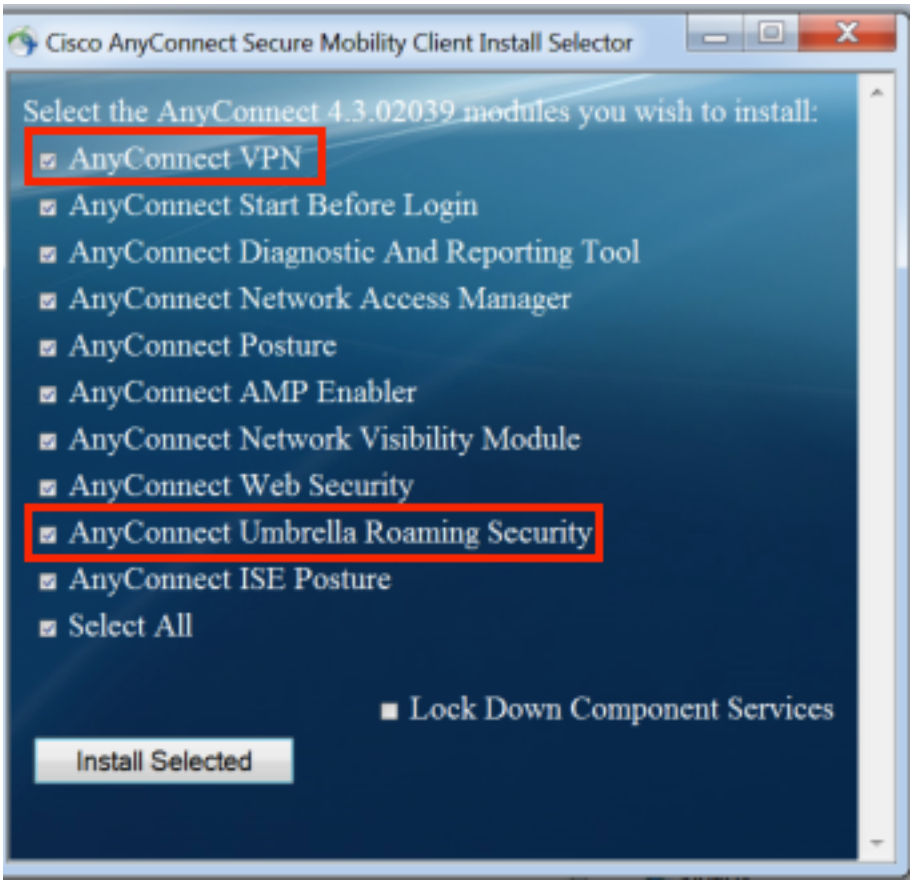
OpenDNS 로밍 모듈을 AnyConnect VPN 클라이언트와 통합하려면 사전 구축 또는 웹 구축 방법을 통해 모듈을 설치해야 합니다.

사전 구축(수동) 방법

사전 구축에는 OpenDNS 로밍 모듈을 수동으로 설치하고 사용자 컴퓨터에 OrgInfo.json 파일을 복사해야 합니다.대규모 구축은 일반적으로 엔터프라이즈 SMS(Software Management System)를 통해 이루어집니다.

OpenDNS 로밍 모듈 구축

AnyConnect 패키지를 설치하는 동안 AnyConnect **VPN** 및 **AnyConnect Umbrella Roaming Security** 모듈을 선택합니다.



OrgInfo.json 구축

OrgInfo.json 파일을 다운로드하려면 다음 단계를 완료하십시오.

1. OpenDNS 대시보드에 로그인합니다.

2. Configuration(**컨피그레이션) > Identities(ID) > Roaming Computers(로밍 컴퓨터)를 선택합니다.**
3. **+**기호를 클릭합니다.
4. 아래로 스크롤하여 다음 이미지에 표시된 대로 Anyconnect **Umbrella Roaming Security Module** 섹션에서 **Module Profile**을 선택합니다.

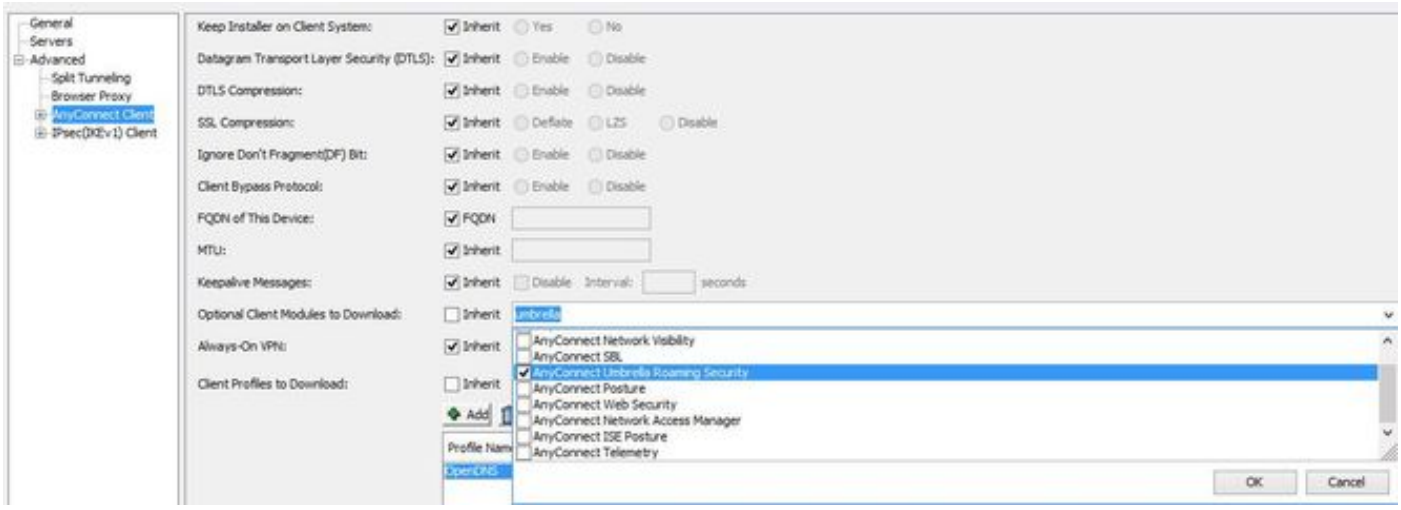
파일을 다운로드한 후에는 운영 체제에 따라 이러한 경로 중 하나에 저장해야 합니다.

Mac OS X의 경우:/opt/cisco/anyconnect/Umbrella
Windows의 경우: C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Umbrella

웹 구축 방법

OpenDNS 로밍 모듈 구축

Cisco 웹 사이트에서 Anyconnect Security Mobility Client 패키지(즉, anyconnect-win-4.3.02039-k9.pkg)를 다운로드하여 ASA의 플래시에 업로드합니다.업로드한 후 ASDM에서 **Group Policy(그룹 정책) > Advanced(고급) > AnyConnect Client(AnyConnect 클라이언트) > Optional Client Modules to Download(다운로드할 선택적 클라이언트 모듈)를** 선택하고 **Umbrella Roaming Security(Umbrella 로밍 보안)를** 선택합니다.

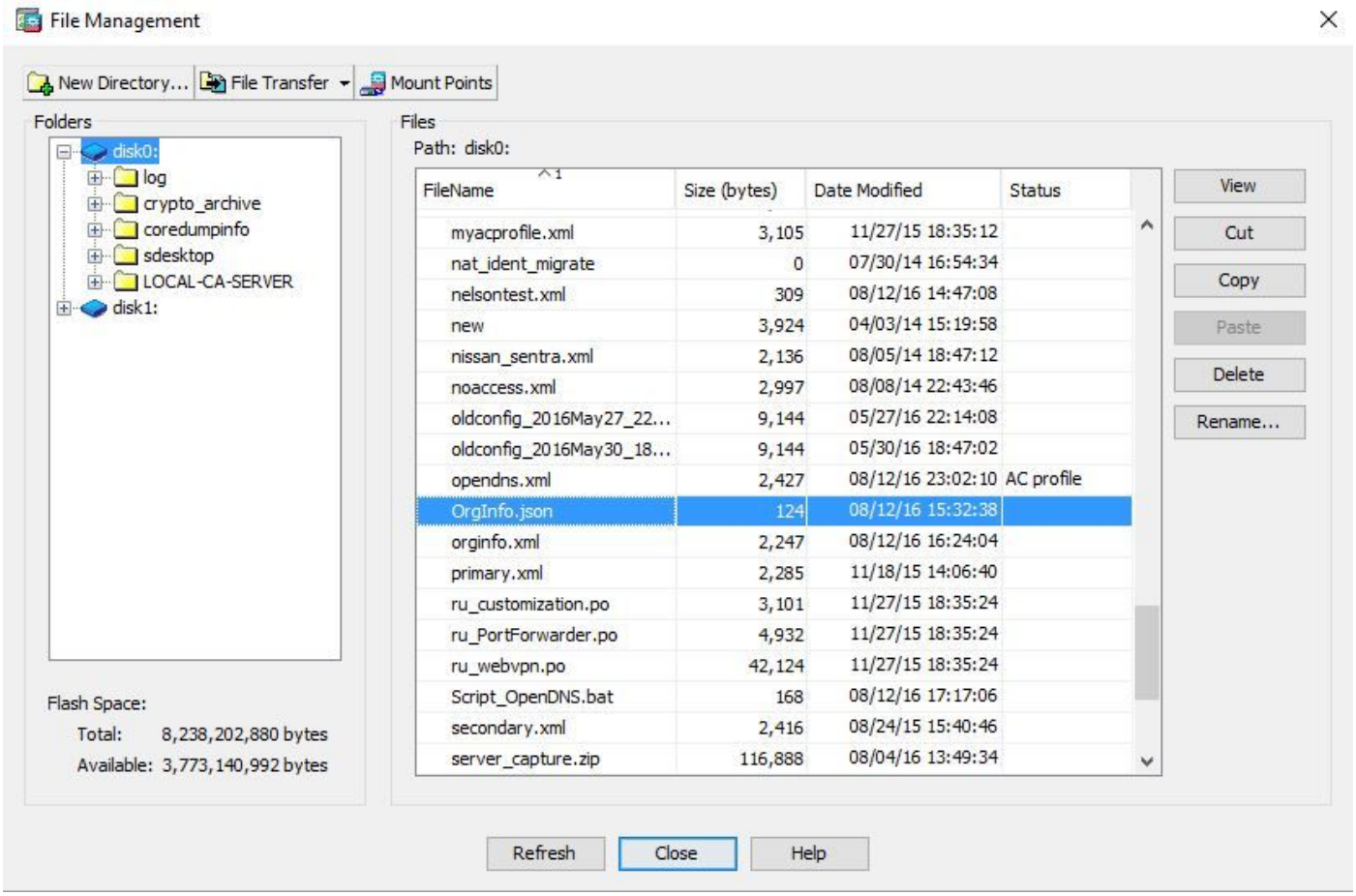


CLI 등가

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

OrgInfo.json 구축

1. OpenDNS 대시보드에서 OrgInfo.json 파일을 다운로드하여 ASA의 플래시에 업로드합니다.



2. OrgInfo.json 파일을 원격 엔드포인트로 푸시하도록 ASA를 구성합니다.

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

> **참고:**이 컨피그레이션은 CLI를 통해서만 수행할 수 있습니다.이 작업에 ASDM을 사용하려면 ASA에 ASDM 버전 7.6.2 이상을 설치해야 합니다.

설명한 방법 중 하나를 통해 Umbrella Roaming 클라이언트가 설치되면 다음 이미지에 표시된 대로 AnyConnect GUI에 통합 모듈로 나타나야 합니다.

OrgInfo.json이 올바른 위치의 엔드포인트에 배포될 때까지 Umbrella Roaming 모듈이 초기화되지 않습니다.

구성

이 섹션에서는 OpenDNS 로밍 모듈을 다양한 AnyConnect 터널링 모드로 작동하는 데 필요한 샘플 CLI 컨피그레이션 조각을 보여줍니다.

```
!--- 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
```

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

AnyConnect OpenDNS 관련 문제를 해결하기 위한 단계는 다음과 같습니다.

1. AnyConnect Secure Mobility Client와 함께 Umbrella Roaming Security 모듈이 설치되어 있는지 확인합니다.
2. OrgInfo.json이 운영 체제를 기반으로 올바른 경로의 엔드포인트에 있고 이 문서에 지정된 형식인지 확인합니다.
3. OpenDNS 확인자에 대한 DNS 쿼리가 AnyConnect VPN 터널을 통과하도록 의도된 경우, OpenDNS 확인자에 연결할 수 있도록 ASA에 헤어핀이 구성되어 있는지 확인하십시오.
4. AnyConnect 가상 어댑터와 물리적 어댑터에서 필터 없이 패킷 캡처를 동시에 수집하고, 확인에 실패한 도메인을 기록합니다.
5. 로밍 모듈이 암호화된 상태로 작동하는 경우 문제 해결을 위해서만 UDP 443을 로컬로 차단 후 패킷 캡처를 수집합니다.이렇게 하면 DNS 트랜잭션에 대한 가시성이 제공됩니다.
6. AnyConnect DART, Umbrella 진단 프로그램을 실행하고 DNS 장애 시간을 기록합니다.자세한 내용은 Anyconnect용 DART 번들을 수집하는 방법을 참조하십시오.
7. Umbrella 진단 로그를 수집하고 결과 URL을 OpenDNS 관리자에게 보냅니다.사용자와 OpenDNS 관리자만 이 정보에 액세스할 수 있습니다. Windows의 경우:C:\Program Files (x86)\Cisco\Cisco AnyConnect Secure Mobility Client\UmbrellaDiagnostic.exe
Mac OSX의 경우:/opt/cisco/anyconnect/bin/UmbrellaDiagnostic

관련 정보

- **Cisco 버그 ID CSCvb34863:스플릿-포함 터널링에 대해 AnyConnect가 구성된 경우 DNS 확인 대기 시간**
- **기술 지원 및 문서 – Cisco Systems**