Anyconnect OpenDNS Roaming Security Module Deployment Guide

Contents

Introduction

This document describes the installation, configuration and troubleshooting steps for the OpenDNS (Umbrella) Roaming module.Starting from AnyConnect 4.3.X, the OpenDNS Roaming client is now available as an integrated module. It is also known as the Cloud Security module and it can pre-deployed to the endpoint using the AnyConnect installer, or can be downloaded from the ASA via web-deploy.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco AnyConnect Secure Mobility Client
- OpenDNS/Umbrella Roaming module
- Cisco Adaptive Security Appliance

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Adaptive Security Appliance (ASA) Version 9.3(3)7
- Cisco AnyConnect Secure Mobility Client 4.3.01095
- OpenDNS Roaming module 4.3.01095
- Cisco Adaptive Security Device Manager 7.6.2 or later
- Windows 8.1

- **Note**: Minimum requirement to deploy OpenDNS Umbrella module:
  - AnyConnect VPN Client version 4.3.01095 or later
  - Cisco Adaptive Security Device Manager 7.6.2 or later
  OpenDNS Roaming module is currently not supported on Linux platform.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any commands or configuration.

Background Information

Orginfo.json

For proper functioning of the OpenDNS Roaming module, an **Orginfo.json** file must be downloaded from the OpenDNS dashboard or pushed from the ASA prior to using the module. When the file is first downloaded, it is saved at a specific path depending on the operating system.

For Mac OS X, **Orginfo.json** is downloaded to **/opt/cisco/anyconnect/Umbrella**
For Windows, **Orginfo.json** is downloaded to ' **C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Umbrella**

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

As shown, the file uses UTF-8 encoding and contains an organizationId, fingerprint and userId. The Organization ID represents the organization information for the user that is currently logged into the OpenDNS dashboard. The Organization ID is static, unique and auto-generated by OpenDNS for each organization. The fingerprint is used to validate the **Orginfo.json** file during device registration and the User ID represents a unique ID for the logged in user.

When the Roaming module starts, on Windows, the **Orginfo.json** file is copied to the data directory under the Umbrella directory and used as the working copy. On MAC OS X, information from this file is saved to updater.plist in the data directory under the Umbrella directory. Once the module has successfully read information from the **Orginfo.json** file, it attempts to register with OpenDNS using a cloud API. This registration results in OpenDNS assigning a unique device ID to the machine that attempted registration. If a device ID from prior registration is already available, the device skips registration.

After registration is complete, the Roaming module performs a sync operation to retrieve policy information for the endpoint. A device ID is necessary for the sync operation to work. Sync data

includes syncInterval, whitelisted domains and IP addresses among other things. The sync interval is the number of minutes after which the module should attempt to resync.

DNS probing behavior

Upon successful registration and sync, the Roaming module sends DNS probes to its local resolvers. These DNS requests include TXT queries for debug.opendns.com. Based on the response, the client is able to determine if an on-premise OpenDNS Virtual Appliance (VA) exists in the network.

If a VA is present, the client transitions to a 'behind-VA' mode, and DNS enforcement is not performed on the endpoint. The client relies on the VA for DNS enforcement at the network level.

If a VA is not present, the client sends a DNS request to the OpenDNS public resolvers (208.67.222.222) using UDP/443.

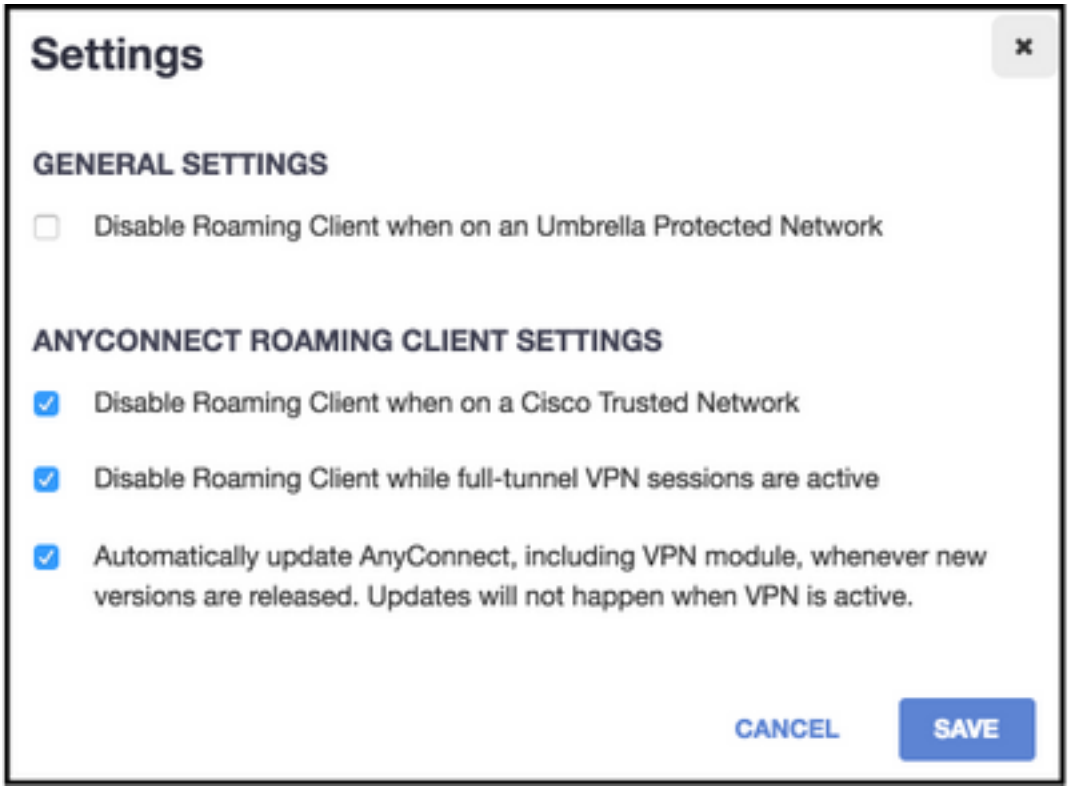
A positive response indicates that DNS encryption is possible. If a negative response is received, the client sends a DNS request to the OpenDNS public resolvers using UDP/53.

A positive response to this query indicates that DNS protection is possible. If a negative response is received, the client retries the query in a few seconds.

Upon receiving a set number of negative responses, the client transitions to fail-open state. A fail-open state means that DNS encryption and/or protection is not possible. Once the Roaming module has successfully transitioned to a protected and/or encrypted state, all DNS queries for search domains outside of the local search domains and whitelist domains are sent to the OpenDNS resolvers for name resolution. With encrypted state enabled, all DNS transactions are encrypted by the dnscrypt process.

DNS behavior with AnyConnect tunneling modes

1. Tunnel-All (or tunnel-all-DNS enabled)



Note: As shown, the default behavior is for Roaming module to disable DNS protection while a VPN tunnel with tunnel-all configuration is active. For the module to be active during an AnyConnect tunnel-all configuration, the **Disable roaming client while full-tunnel VPN sessions are active** option must be unchecked on the OpenDNS portal. The ability to enable this feature requires an advanced subscription level with OpenDNS. The information below assumes that DNS protection via Roaming module is enabled.

Queried domain part of whitelist:

DNS requests that originate from the tunnel adapter are allowed and sent to the tunnel DNS servers, across the VPN tunnel. The query will remain unresolved if it cannot be resolved by the tunnel DNS servers.

Queried domain not part of whitelist:

DNS requests that originate from the tunnel adapter are allowed, and will be proxied to the OpenDNS public resolvers via the Roaming module and sent across the VPN tunnel. To the DNS client it will appear as if name resolution had occurred via the VPN DNS server. If name resolution via OpenDNS resolvers is not successful, Roaming module fails over to the locally configured DNS servers, starting with the VPN adapter (which is the preferred adapter while the tunnel is up).

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

Note: All split-DNS domains are automatically added to Roaming module whitelist upon tunnel establishment. This is done to provide consistent DNS handling mechanism between AnyConnect and Roaming module. Ensure that in a split-DNS configuration (with split-include tunneling) the OpenDNS public resolvers are not included in the split-include

networks.

Note: On Mac OS X, If split-DNS is enabled for both IP protocols (IPv4 and IPv6) or it's only enabled for one protocol and there is no address pool configured for the other protocol: True split-DNS, similar to Windows, is enforced.
If split-DNS is enabled for only one protocol and a client address is assigned for the other protocol, only DNS fallback for split-tunneling is enforced. This means AnyConnect only allows DNS requests matching the split-DNS domains via tunnel (other requests are replied by AC with refused response to force failover to public DNS servers), but cannot enforce that requests matching split-DNS domains are not sent in the clear, via the public adapter.

Queried domain part of whitelist and also part of split-DNS domains:

DNS requests that originate from the tunnel adapter are allowed and sent to the tunnel DNS servers, across the VPN tunnel. All other requests for matching domains from other adapters will be responded by AnyConnect driver with 'no such name' to achieve true split-DNS (prevent DNS fallback). Therefore, only non-tunnel DNS traffic is protected by the Roaming module.

Queried domain part of whitelist but not part of split-DNS domains:

DNS requests that originate from the physical adapter are allowed and sent to the public DNS servers, outside the VPN tunnel. All other requests for matching domains from the tunnel adapter will be responded by AnyConnect driver with 'no such name' to prevent the query from being sent across the VPN tunnel.

Queried domain not part of whitelist or split-DNS domains:

DNS requests that originate from the physical adapter are allowed and proxied to the OpenDNS public resolvers, and sent outside the VPN tunnel. To the DNS client it will appear as if name resolution had occurred via the public DNS server. If name resolution via OpenDNS resolvers is unsuccessful, Roaming module fails over to the locally configured DNS servers, excluding the ones configured on the VPN adapter. All other requests for matching domains from the tunnel adapter will be responded by AnyConnect driver with no such name to prevent the query from being sent across the VPN tunnel.

3. Split-include or Split-exclude tunneling (no split-DNS and tunnel-all-DNS disabled)

Queried domain part of whitelist:

Native OS resolver performs DNS resolution based on the order of network adapters, and AnyConnect is the preferred adapter when VPN is active. DNS requests will first originate from the tunnel adapter and be sent to the tunnel DNS servers, across the VPN tunnel. If the query cannot be resolved by the tunnel DNS servers, the OS resolver will attempt to resolve it via the public DNS servers.

Queried domain not part of whitelist:

Native OS resolver performs DNS resolution based on the order of network adapters, and AnyConnect is the preferred adapter when VPN is active. DNS requests will first originate from the tunnel adapter and be sent to the tunnel DNS servers, across the VPN tunnel. If the query cannot be resolved by the tunnel DNS servers, the OS resolver will attempt to resolve it via the public DNS servers.

If the OpenDNS public resolvers are part of the split-include list or not part of the split-exclude list, the proxied request is sent across the VPN tunnel
If the OpenDNS public resolvers are not part of the split-include list or part of the split-exclude list, the proxied request is sent outside the VPN tunnel

If name resolution via OpenDNS resolvers is not successful, Roaming module fails over to the locally configured DNS servers, starting with the VPN adapter (which is the preferred adapter while the tunnel is up). If the final response returned by Roaming module (and proxied back to the native DNS client) is not successful, the native client will attempt other DNS servers, if available.

Install and Configure Umbrella Roaming Module

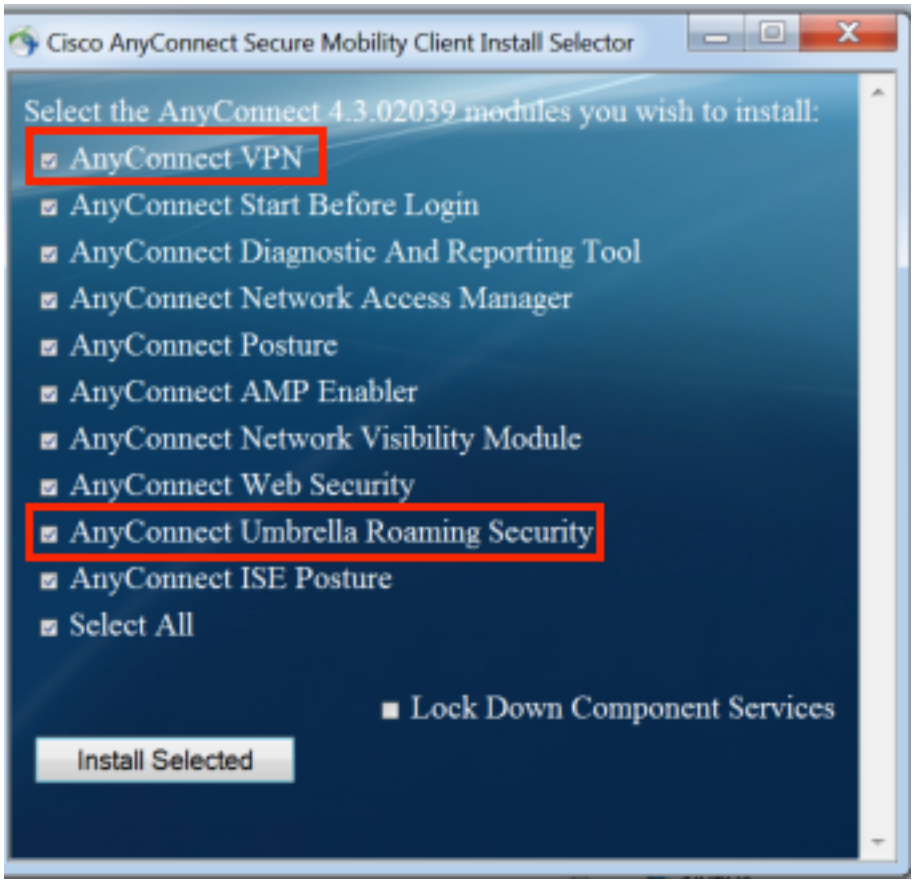
In order to integrate OpenDNS Roaming module with the AnyConnect VPN client, the module needs to be installed either via pre-deplomen or web deployment method:

Pre-Deployment (Manual) Method

Pre-deployment requires manual installation of OpenDNS Roaming module and copying of OrgInfo.json file on the user machine. Large scale deployments are typically achieved using enterprise software management systems (SMS).

Deploy OpenDNS Roaming Module

During AnyConnect package installation choose the Anyconnect VPN and Anyconnect Umbrella Roaming Security modules:



Deploying OrgInfo.json

Download OrgInfo.json file by logging into OpenDNS dashboard and navigating to **Configuration > Identities > Roaming Computers** and Click on the **+** sign. Scroll down and select **Module Profile** under **Anyconnect Umbrella Roaming Security Module** section as shown in this image:

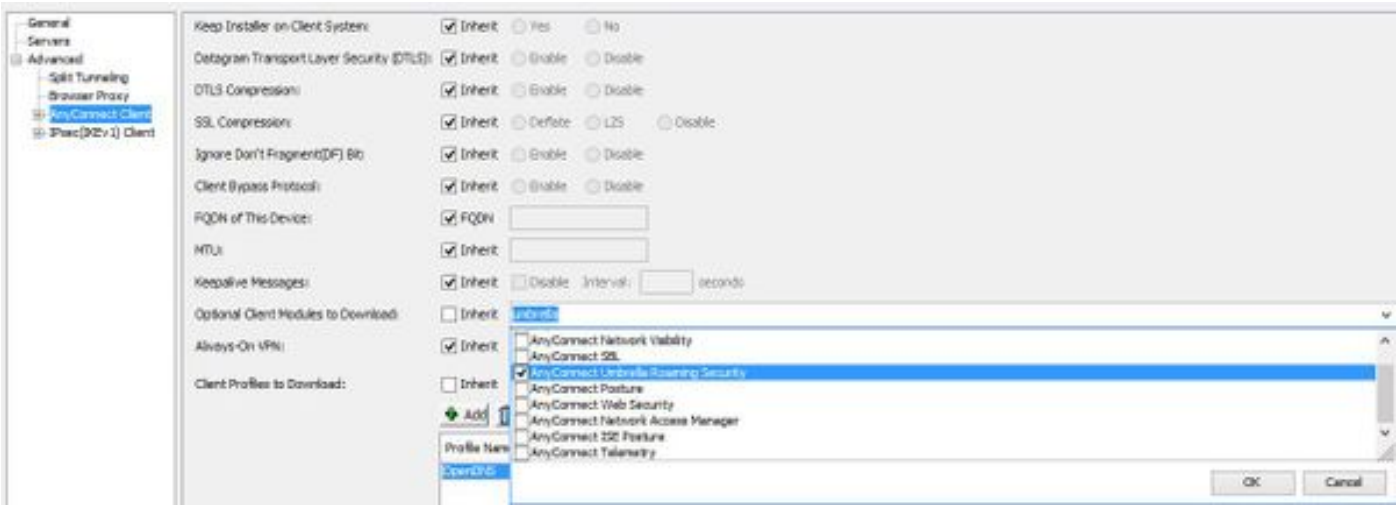
Once the file is downloaded, it must be saved at these paths depending on the operating system.

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

Web-Deployment Method

Deploy OpenDNS Roaming Module

Download the Anyconnect Security Mobility Client (e.g. anyconnect-win-4.3.02039-k9.pkg) package from the Cisco website and upload it to ASA's flash. Once uploaded, on ASDM go to **Group Policy > Advanced > AnyConnect Client > Optional Client Modules to Download** and select **Umbrella Roaming Security.**

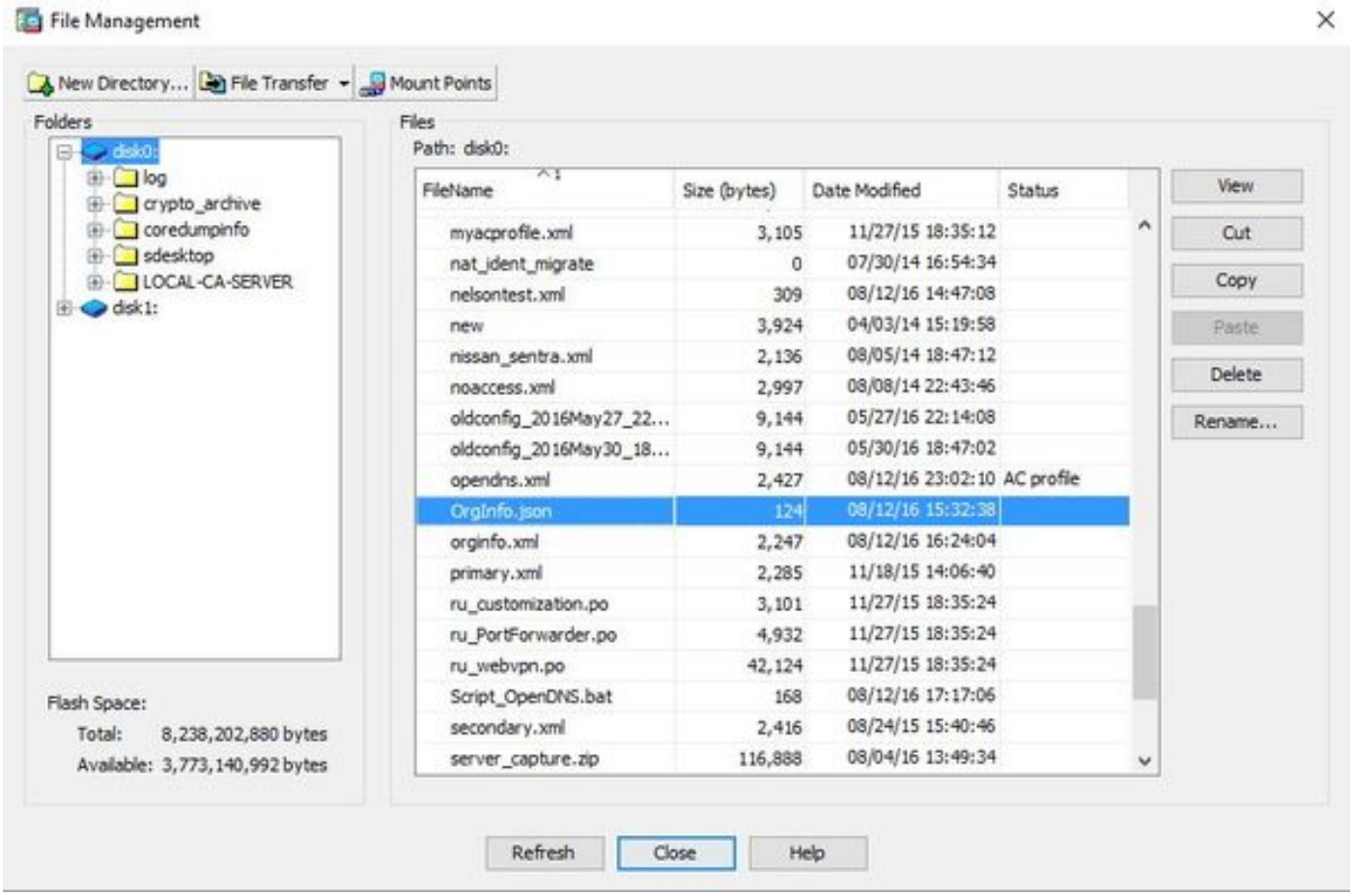


CLI equivalent:

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

Deploy Orginfo.json

1. Download Orginfo.json file from OpenDNS dashboard and upload it to ASA's flash.



2. Configure the ASA to push the **OrgInfo.json** file to remote endpoints.

```
webvpn
anyconnect profiles OpenDNS disk0:/orginfo.json
!
!
group-policy <Group_Policy_Name> attribute
```

```
webvpn
anyconnect profiles value OpenDNS type umbrella
```

> **Note**: This configuration can only be performed through CLI. In order to use ASDM for this task, ASDM version 7.6.2 or later needs to be installed on the ASA.

Once the Umbrella Roaming client is installed via one of the methods discussed, it should appear as an integrated module within the AnyConnect GUI as shown in this image

Until the **Orginfo.json** is deployed on the endpoint at the correct location, the Umbrella Roaming module will not be initialized.

Configure

The section shows sample CLI configuration snippets necessary to operate the OpenDNS Roaming module with the various AnyConnect tunneling modes.

```
!--- 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 <internal domains> (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
```

Troubleshoot

Steps to troubleshoot AnyConnect OpenDNS related issues:

1. Ensure that the Umbrella Roaming Security module is installed along with Anyconnect Secure Mobility Client
2. Ensure OrgInfo.json is present on the endpoint at the correct path based on the operating system and is in the format specified in this document
3. If DNS queries to OpenDNS resolvers are intended to go over the AnyConnect VPN tunnel, ensure that hairpin is configured on ASA to allow reachability to OpenDNS resolvers
4. Collect packet captures (without any filters) on the AnyConnect virtual adapter and physical adapter simultaneously and note down the domains which are failing to resolve
5. If the Roaming module is operating in an encrypted state, collect packet captures after blocking UDP 443 locally, for troubleshooting purposes only. That way there is visibility into the DNS transactions
6. Run the Anyconnect DART, Umbrella diagnostics and note down the time of DNS failure:

Collecting DART: https://supportforums.cisco.com/document/12747756/how-collect-dart-bundle-anyconnect

7. Collect Umbrella diagnostic logs and send the resulting URL to your OpenDNS administrator. Only you and OpenDNS administrator have access to this information.

For Windows: 'C:\Program Files (x86)\Cisco\Cisco AnyConnect Secure Mobility Client\UmbrellaDiagnostic.exe

For Mac OSX: /opt/cisco/anyconnect/bin/UmbrellaDiagnostic

Related Defects

CSCvb34863 : Latency in resolving DNS when AnyConnect configured for split-include tunneling