Configure ASA and AnyConnect Dynamic Split Tunneling

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background Information

Configuration

- Network Diagram
- Step 1. Create AnyConnect Custom Attributes
- Step 2. Create AnyConnect Custom Name and Configure Values
- Step 3. Add Type and Name to the Group Policy

CLI Configuration Example

Limitations

Verify

Troubleshoot

- If a Wildcard is Used in the Values Field
- If Non-Secured Routes is not seen in the Route Details Tab
- General Troubleshooting

Related Information

Introduction

This document describes how to configure AnyConnect Secure Mobility Client for Dynamic Split Exclude Tunneling via ASDM.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Basic knowledge of ASA.
- Basic knowledge of Cisco AnyConnect Security Mobility Client.

Components Used

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

- ASA 9.12(3)9
- Adaptive Security Device Manager (ASDM) 7.13(1)
- AnyConnect 4.7.0

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, ensure that you understand the potential impact of any command.

Background Information

AnyConnect Split tunneling allows Cisco AnyConnect Secure Mobility Client secure access to corporate resources via IKEV2 or Secure Sockets Layer (SSL). Prior to AnyConnect version 4.5, based on the policy configured on Adaptive Security Appliance (ASA), Split tunnel behavior can be Tunnel Specified, Tunnel All, or Exclude Specified.

With the advent of cloud-hosted computer resources, services sometimes resolve to a different IP address based on the location of the user or based on the load of the cloud-hosted resources.

Since AnyConnect Secure Mobility Client provides split-tunneling to static subnet range, host or a pool of IPV4 or IPV6, it becomes difficult for Network Administrators to exclude domains/FQDNs while they configure AnyConnect. For example, a Network Administrator wants to exclude the Cisco.com domain from Split tunnel configuration but the DNS mapping for Cisco.com changes since it is cloud-hosted.

By using Dynamic Split Exclude tunneling, AnyConnect dynamically resolves the IPv4/IPv6 address of the hosted application and ensures necessary changes in the routing table and filters to allow the connection to be made outside the tunnel.

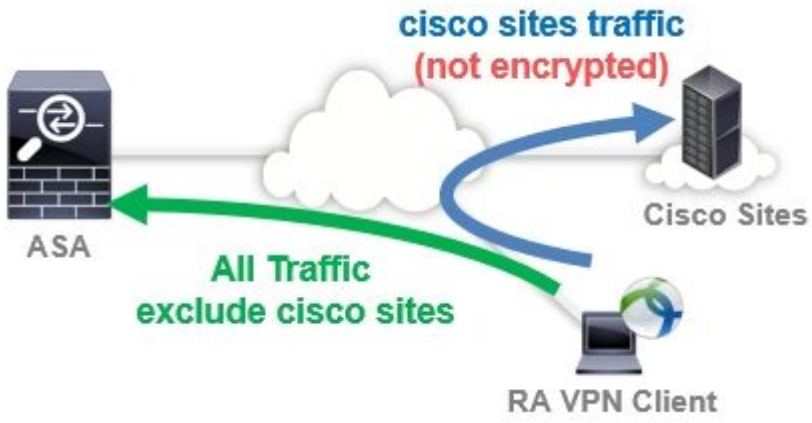
Starting with AnyConnect 4.5, Dynamic Spit Tunnelling can be used wherein AnyConnect dynamically resolves the IPv4/IPv6 address of the hosted application and makes necessary changes in the routing table and filters to allow the connection to be made outside the tunnel

Configuration

This section describes how to configure the Cisco AnyConnect Secure Mobility Client on the ASA.

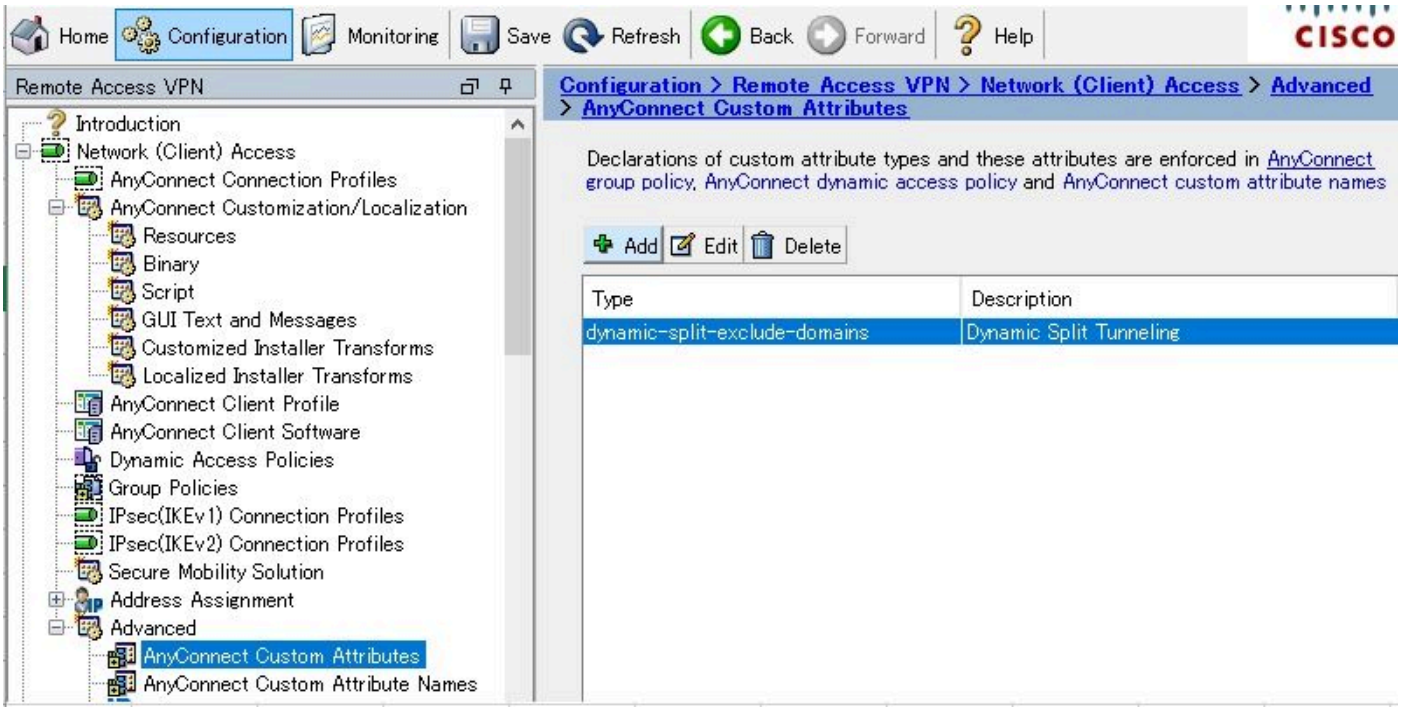
Network Diagram

This image shows the topology used for the examples in this document.



Step 1. Create AnyConnect Custom Attributes

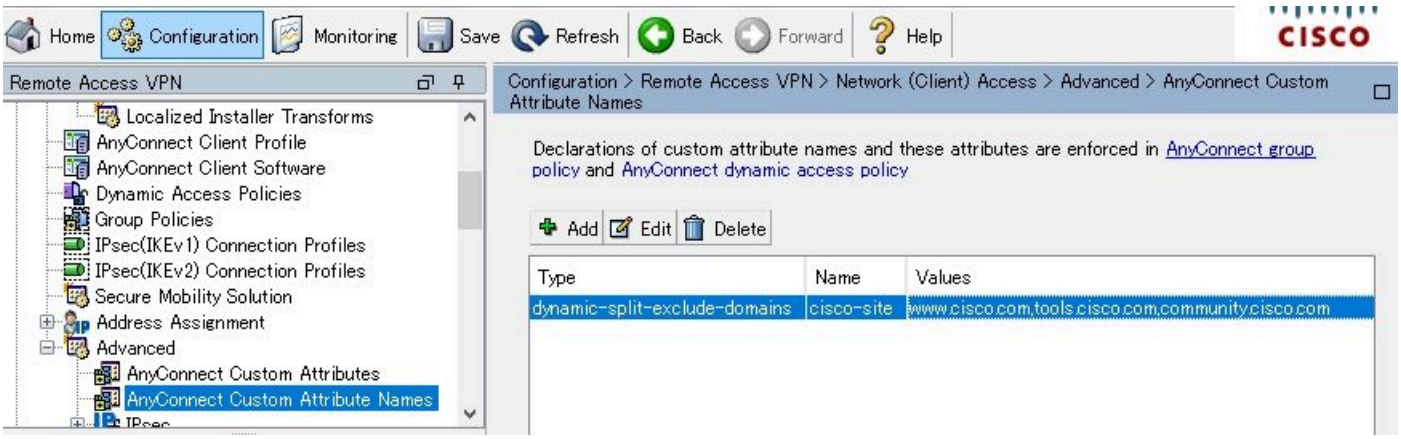
Navigate to Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attributes. Click the **Add** button, and set the **dynamic-split-exclude-domains** attribute and optional description.



Step 2. Create AnyConnect Custom Name and Configure Values

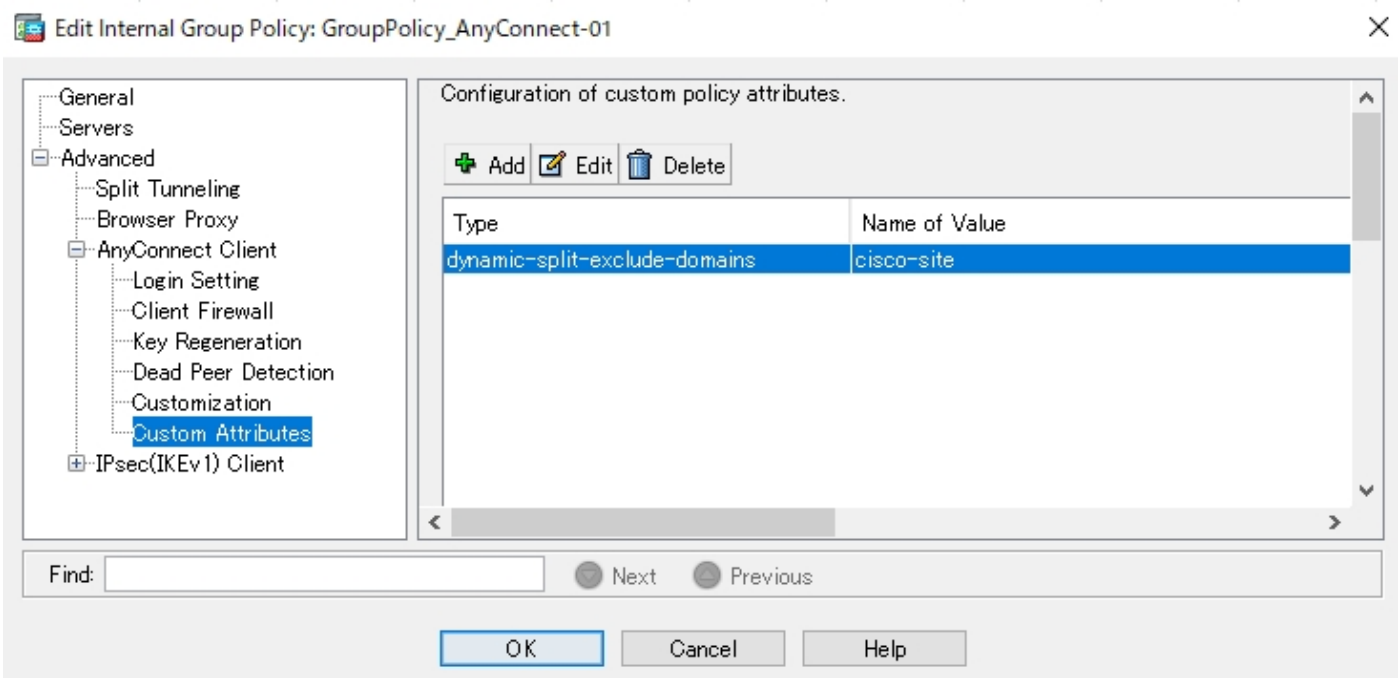
Navigate to **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Advanced** > **AnyConnect Custom Attribute Names**. Click the **Add** button, and set the **dynamic-split-exclude-domains** attribute created earlier from Type, an arbitrary name, and Values.

Be careful not to enter a space in Name (for example, it is possible to use cisco-site, however, it is impossible cisco site). When multiple domains or FQDNs in Values are registered, separate with a comma (,).



Step 3. Add Type and Name to the Group Policy

Navigate to **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Group Policies** and select a Group Policy. Then, navigate to **Advanced** > **AnyConnect Client** > **Custom Attributes** and add the configured **Type** and **Name**.



CLI Configuration Example

This section provides the CLI configuration of Dynamic Split Tunneling for reference purposes.

<#root>

```
ASAv10# show run
  --- snip ---

webvpn


 enable outside

 AnyConnect-custom-attr dynamic-split-exclude-domains description Dynamic Split Tunneling


 hsts
  enable
  max-age 31536000
  include-sub-domains
  no preload
 AnyConnect image disk0:/AnyConnect-win-4.7.04056-webdeploy-k9.pkg 1
 AnyConnect enable
 tunnel-group-list enable
 cache
  disable
 error-recovery disable

AnyConnect-custom-data dynamic-split-exclude-domains cisco-site www.cisco.com,tools.cisco.com,community.


group-policy GroupPolicy_AnyConnect-01 internal

group-policy GroupPolicy_AnyConnect-01 attributes


 wins-server none
 dns-server value 10.0.0.0
 vpn-tunnel-protocol ssl-client
 split-tunnel-policy tunnelall
 split-tunnel-network-list value SplitACL
 default-domain value cisco.com

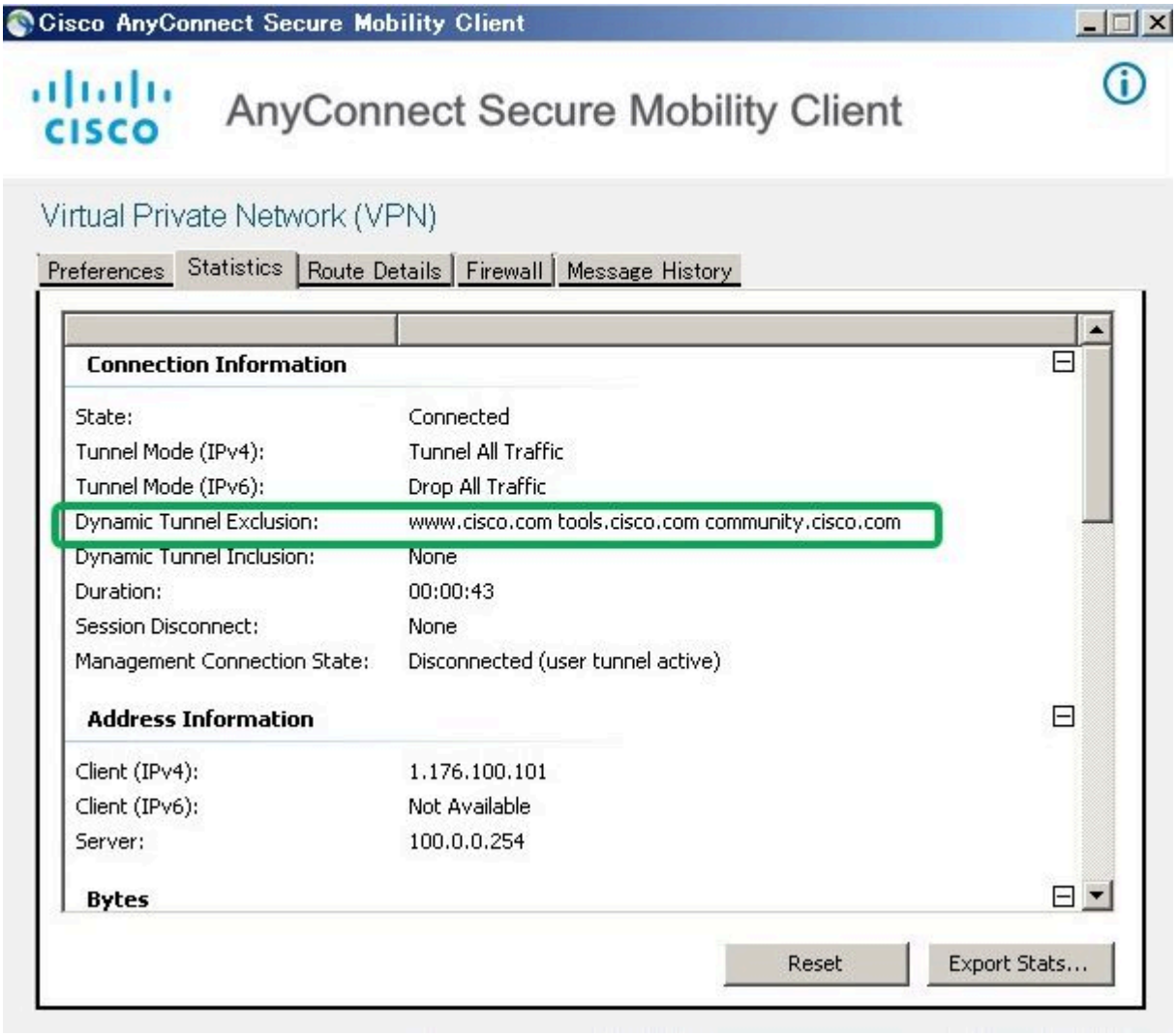
 AnyConnect-custom dynamic-split-exclude-domains value cisco-site
```

Limitations

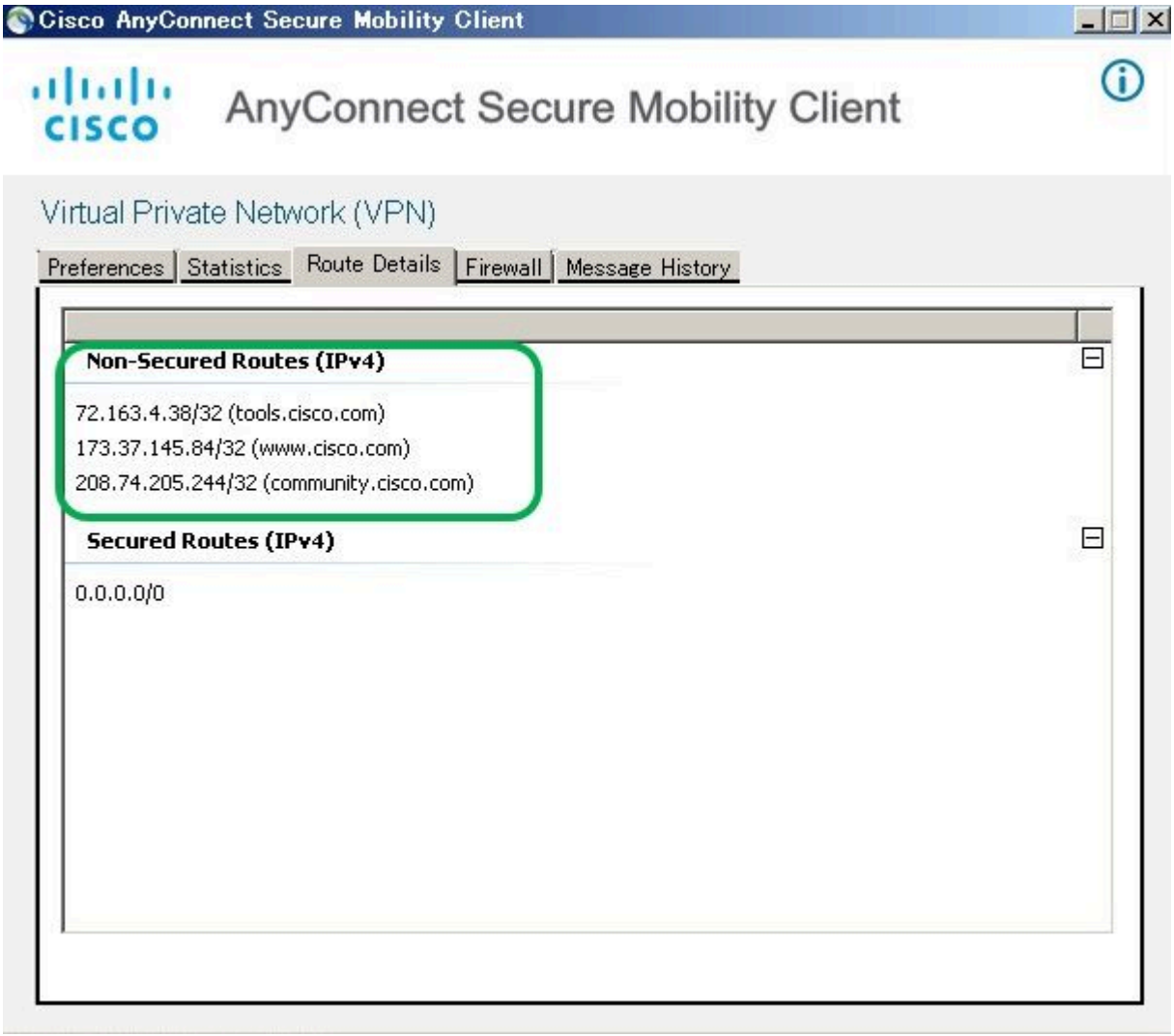
- ASA version 9.0 or later is required to use Dynamic Split Tunneling custom attributes.
- A wildcard in the Values field is not supported.
- Dynamic Split Tunneling is not supported on Cisco IOS® (Apple) devices (Enhancement Request: Cisco bug ID CSCvr54798).

Verify

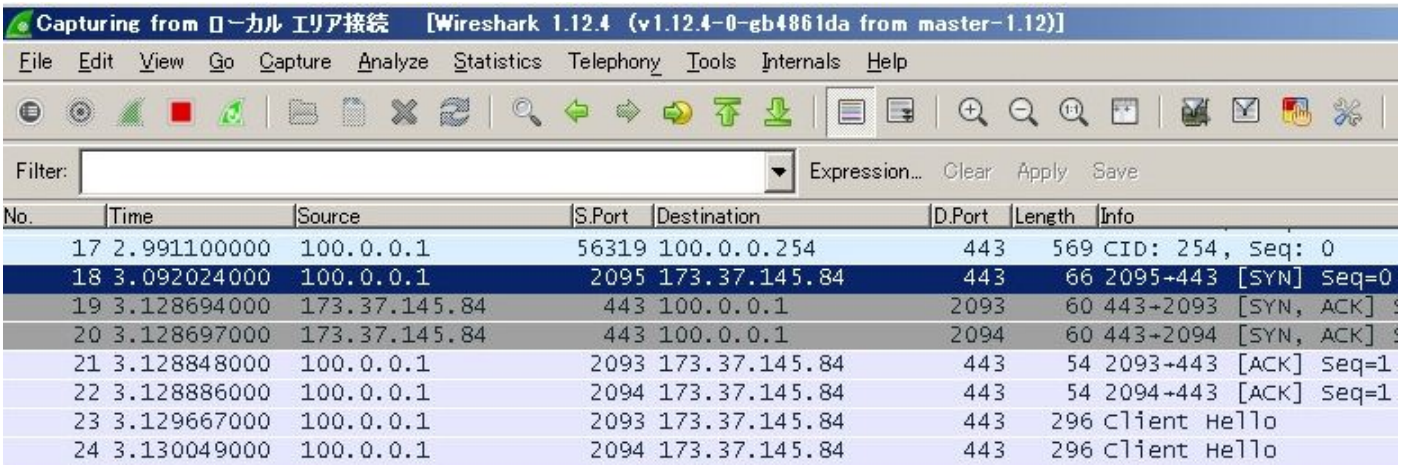
To verify configured **Dynamic Tunnel Exclusions**, launchAnyConnectsoftware on the client, select **Advanced Window** > **Statistics**.



You can also navigate to **Advanced Window > Route Details** tab, where you can verify the **Dynamic Tunnel Exclusions** are listed under **Non-Secured Routes**.



In this example, you have configured www.cisco.com under the **Dynamic Tunnel Exclusion** list and the Wireshark capture collected on the AnyConnect client physical interface confirms the traffic to www.cisco.com (198.51.100.0), is not encrypted by DTLS.



Troubleshoot

If a Wildcard is Used in the Values Field

If a wildcard is configured in Values field, for example, ***.cisco.com** is configured in Values, the AnyConnect session is disconnected, as shown in the logs:

```
Apr 02 2020 10:01:09: %ASA-4-722041: TunnelGroup <AnyConnect-01> GroupPolicy <GroupPolicy_AnyConnect-01
Apr 02 2020 10:01:09: %ASA-5-722033: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> Fir
Apr 02 2020 10:01:09: %ASA-6-722022: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> TCP
Apr 02 2020 10:01:09: %ASA-6-722055: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> Cli
Apr 02 2020 10:01:09: %ASA-4-722051: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> IPv
Apr 02 2020 10:01:09: %ASA-6-302013: Built inbound TCP connection 8570 for outside:172.16.0.0/44868 (17
Apr 02 2020 10:01:09: %ASA-4-722037: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> SVC
Apr 02 2020 10:01:09: %ASA-5-722010: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> SVC
Apr 02 2020 10:01:09: %ASA-6-716002: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> Web
Apr 02 2020 10:01:09: %ASA-4-113019: Group = AnyConnect-01, Username = cisco, IP = 172.16.0.0, Session
```

Note: As an alternative, you can use the cisco.com domain in Values, to allow FQDNs such as www.cisco.com and tools.cisco.com.

If Non-Secured Routes is not seen in the Route Details Tab

AnyConnect client automatically learns and adds the IP address and FQDN in the Route Details tab, when the client initiates traffic for the excluded destinations.

To verify AnyConnect users are assigned to the correct Anyconnect group-policy, you can run the command **show vpn-sessiondb anyconnect filter name <username>**.

<#root>

```
ASAv10# show vpn-sessiondb anyconnect filter name cisco

Session Type: AnyConnect

Username     : cisco                 Index : 7
Assigned IP  : 172.16.0.0          Public IP : 10.0.0.0
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256
Hashing      : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384
Bytes Tx     : 7795373               Bytes Rx : 390956

Group Policy : GroupPolicy_AnyConnect-01


Tunnel Group : AnyConnect-01
Login Time   : 13:20:48 UTC Tue Mar 31 2020
Duration     : 20h:19m:47s
```

```
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN : none
Audt Sess ID : 019600a9000070005e8343b0
Security Grp : none
```

General Troubleshooting

You can use the AnyConnect Diagnostics and Reporting Tool (DART) to collect data that is useful to troubleshoot AnyConnect installation and connection problems. The DART Wizard is used on the computer that runs AnyConnect. DART assembles the logs, status, and diagnostic information for the Cisco Technical Assistance Center (TAC) analysis and does not require administrator privileges to run on the client machine.

Related Information

- Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 4.7 - About Dynamic Split Tunneling
- ASDM Book 3: Cisco ASA Series VPN ASDM Configuration Guide, 7.13 - Configure Dynamic Split Tunneling