Configure AnyConnect Dynamic Split Tunnel on FTD Managed by FMC

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background Information

- Limitations

Configure

- Step 1. Edit the Group Policy to use Dynamic Split Tunnel
- Step 2. Configure the AnyConnect Custom Attribute
- Step 3. Verify the Configuration, Save and Deploy

Verify

Troubleshoot

- Problem
- Solution

Related Information

Introduction

This document describes how to configure AnyConnect Dynamic Split Tunnel on Firepower Threat Defense (FTD) managed by Firepower Management Center.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco AnyConnect
- Basic knowledge of Firepower Management Center (FMC)

Components Used

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

- FMC version 7.0
- FTD version 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 Dynamic Split Tunnel configuration on FTD managed by FMC is fully available on FMC version 7.0 and newer. If you run an older version, you need to configure it via FlexConfig as instructed in the Advanced AnyConnect VPN Deployments for Firepower Threat Defense with FMC.

With Dynamic Split Tunnel configuration, you can fine-tune split tunnel configuration based on DNS domain names. Because the IP addresses associated with full-qualified domain names (FQDN) can change, split tunnel configuration based on DNS names provides a more dynamic definition of which traffic is, or is not, included in the remote access Virtual Private Network (VPN) tunnel. If any addresses returned for excluded domain names are within the address pool included in the VPN, those addresses are then excluded. Excluded domains are not blocked. Instead, traffic to those domains is kept outside the VPN tunnel.

Note: You can also configure Dynamic Split Tunnel to define domains to include in the tunnel that would otherwise be excluded based on IP address.

Limitations

Currently, these features are still unsupported:

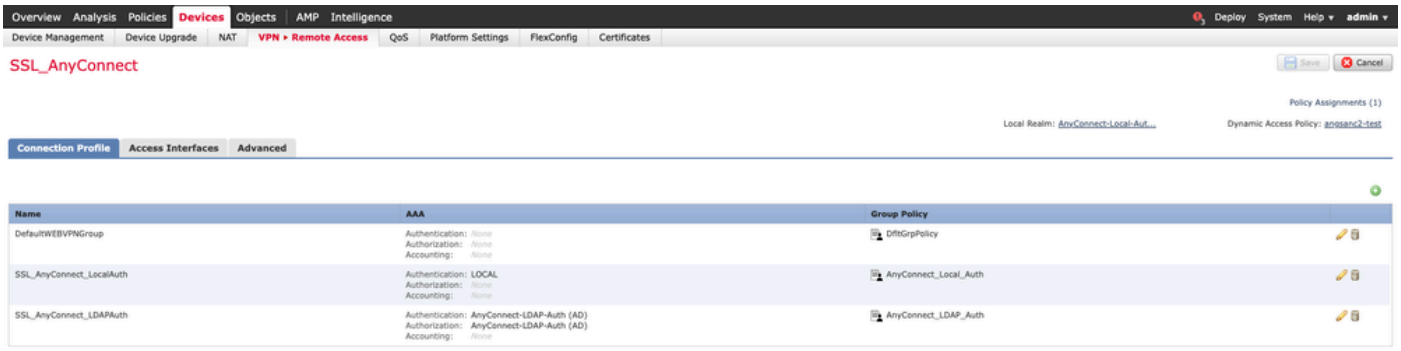
- Dynamic Split Tunnel is not supported on Cisco iOS devices. See Cisco bug ID CSCvr54798
- Dynamic Split Tunnel is not supported on AnyConnect Linux Clients. See Cisco bug ID CSCvt64988

Configure

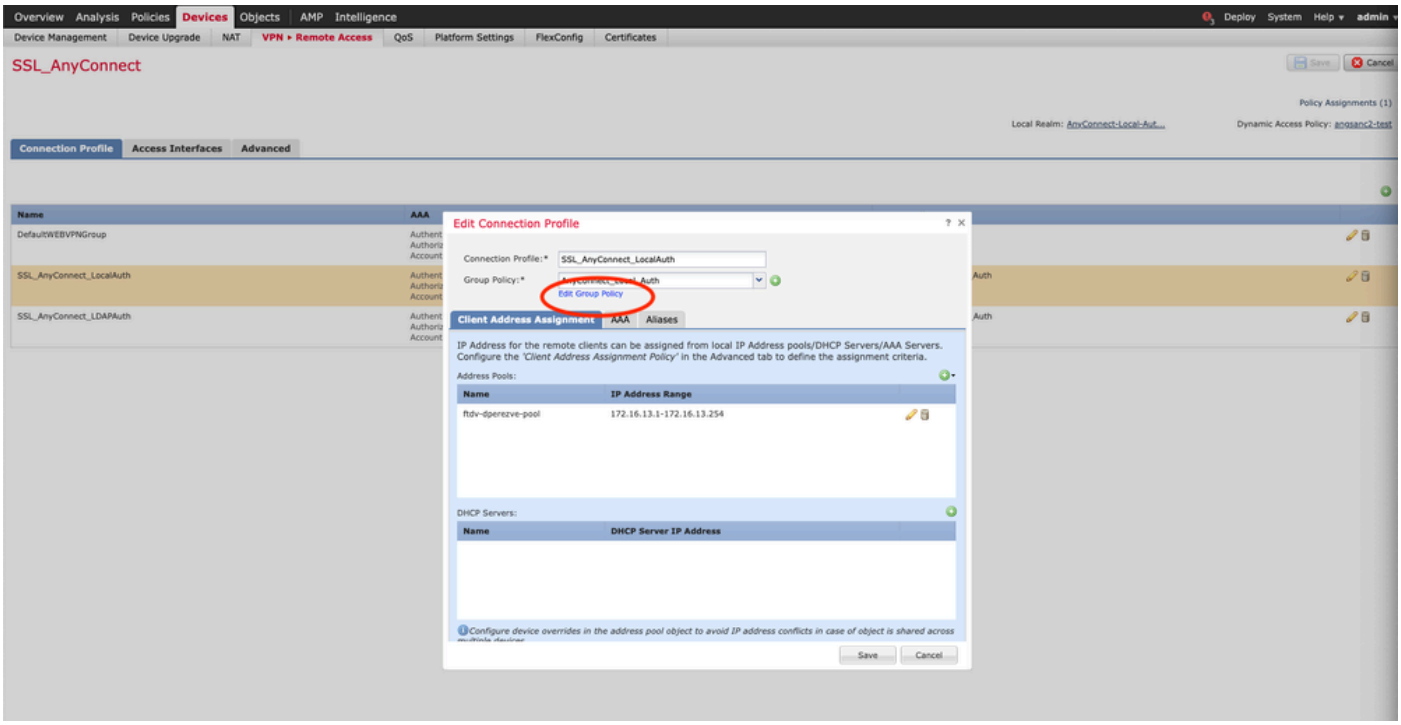
This section describes how to configure AnyConnect Dynamic Split Tunnel on FTD managed by FMC.

Step 1. Edit the Group Policy to use Dynamic Split Tunnel

1. On the FMC, navigate to **Devices > VPN > Remote Access**, then select the **Connection Profile** you desire to apply the configuration:

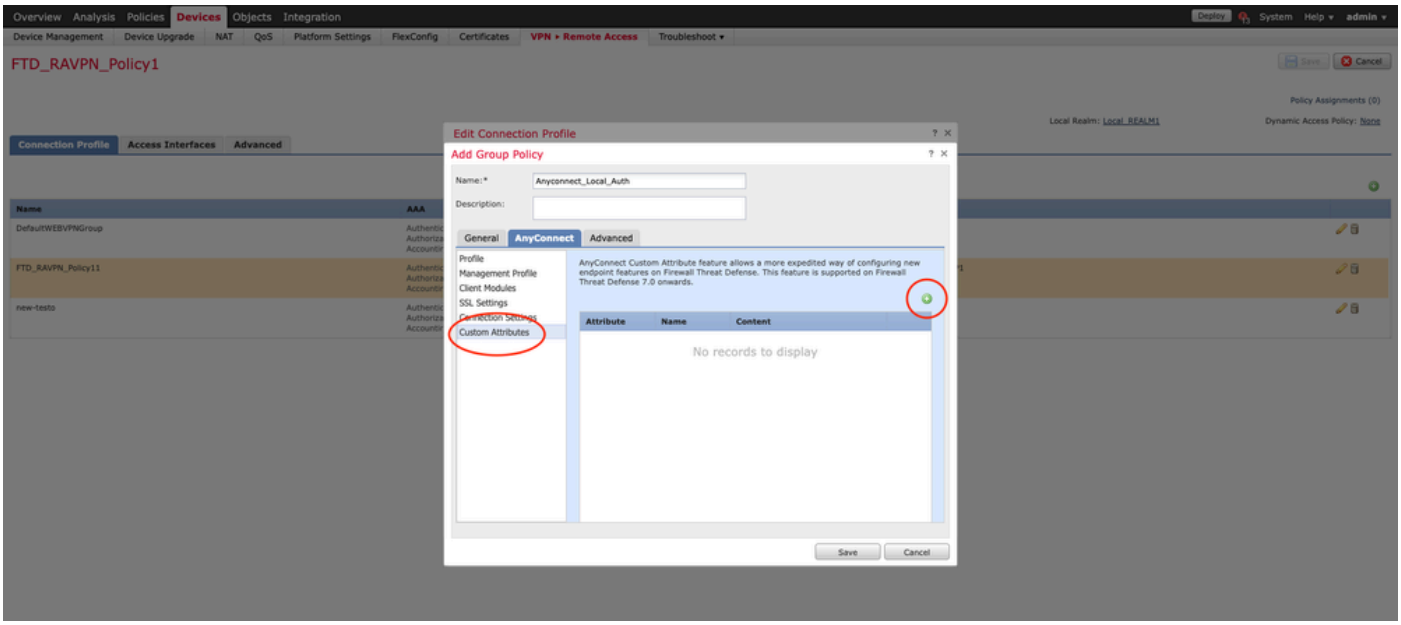


2. Select **Edit Group Policy** to modify one of the group policies already created.

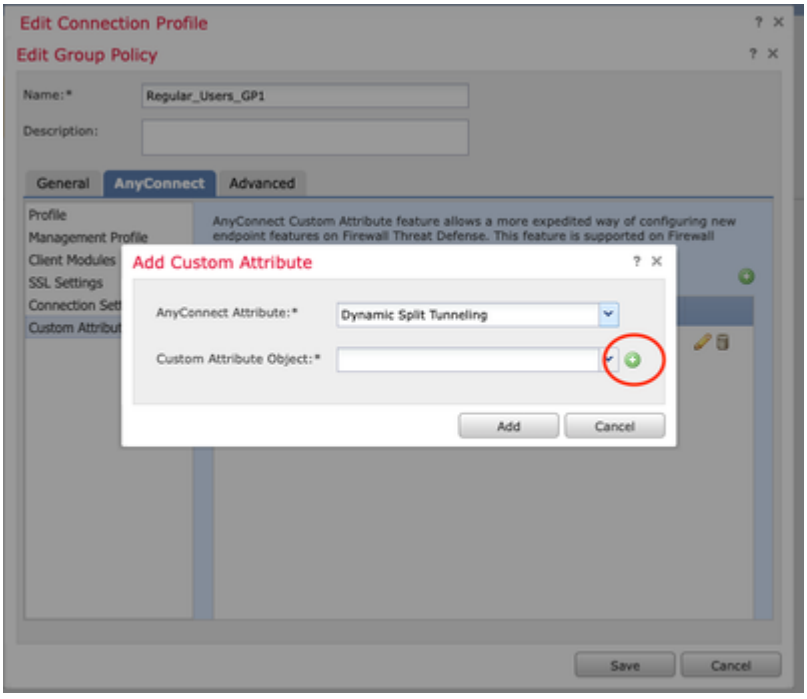


Step 2. Configure the AnyConnect Custom Attribute

1. Under the Group Policy configuration, navigate to **AnyConnect > Custom Attributes**, click the **Add (+)** button:

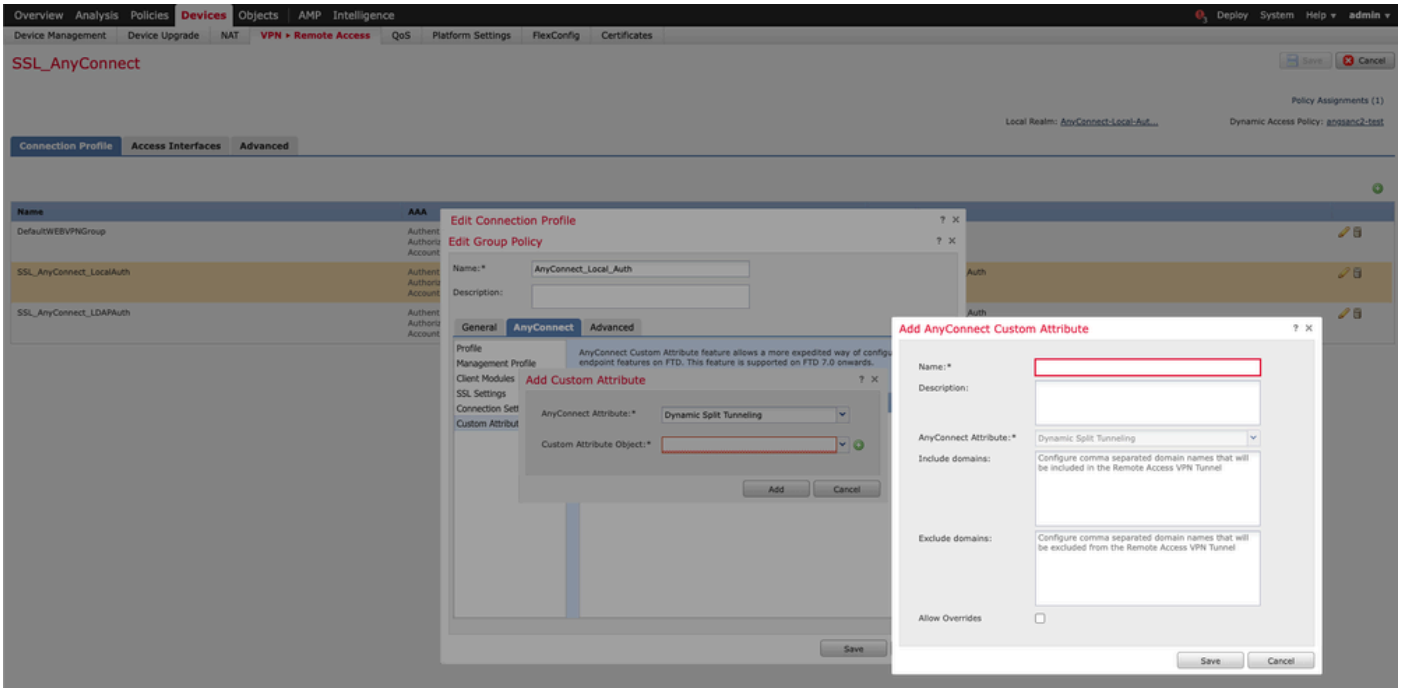


2. Select the **Dynamic Split Tunneling** AnyConnect Attribute, and click the **Add (+)** button to create a new Custom Attribute Object:

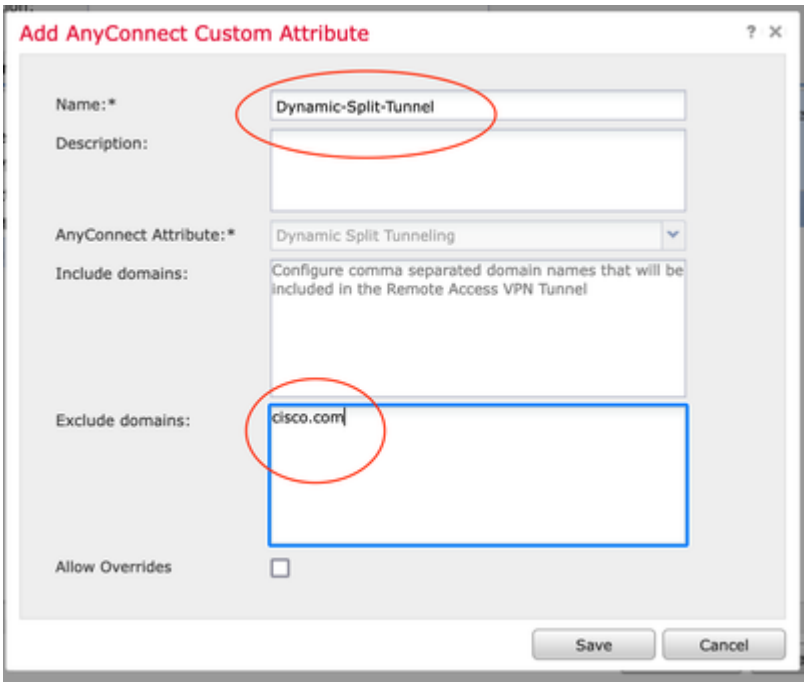


3. Enter the **Name** of the **AnyConnect Custom Attribute** and configure the domains to be dynamically included or excluded.

Note: You can only configure either Include domains or Exclude domains.

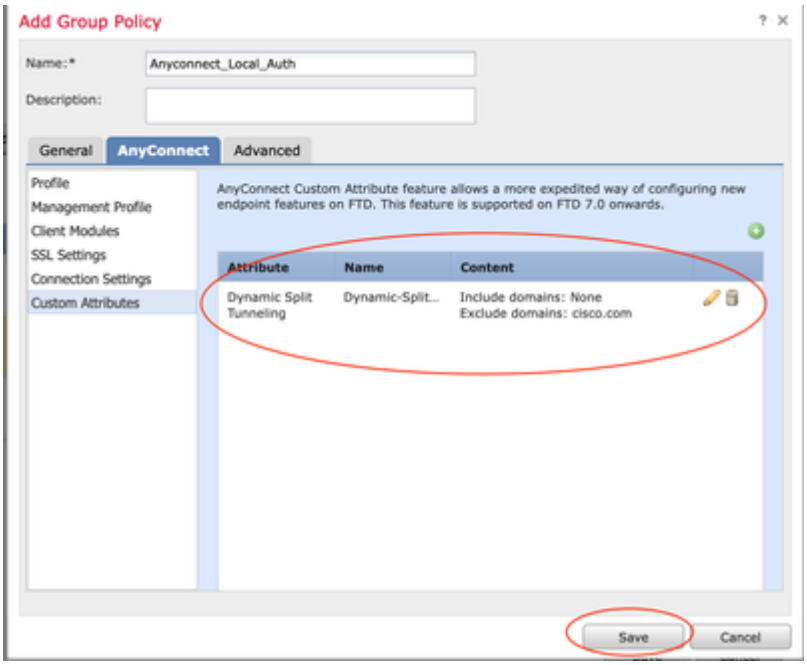


In this example, you configured cisco.com as the domain to be excluded, and named the custom attribute **Dynamic-Split-Tunnel**, as shown in the image:



Step 3. Verify the Configuration, Save and Deploy

Verify that the **configured custom attribute** is correct, **save** the configuration and **deploy** the changes to the FTD in question.



Verify

You can run these commands on the FTD via Command Line interface (CLI) to confirm the Dynamic Split Tunnel configuration:

- **show running-config webvpn**
- **show running-config anyconnect-custom-data**
- **show running-config group-policy <Name of the group-policy>**

In this example, the configuration is:

<#root>

ftd# show run group-policy AnyConnect_Local_Auth

```
group-policy AnyConnect_Local_Auth attributes
vpn-idle-timeout 30
vpn-simultaneous-logins 3
vpn-session-timeout none
vpn-filter none
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelspecified
ipv6-split-tunnel-policy-tunnelall
split-tunnel-network-list value AC_networks
Default-domain none
split-dns none
address-pools value AC_pool
```

anyconnect-custom dynamic-split-exclude-domains value cisco.com

```
anyconnect-custom dynamic-split-include-domains none
```

ftd# show run webvpn

```
webvpn
enable outside
```

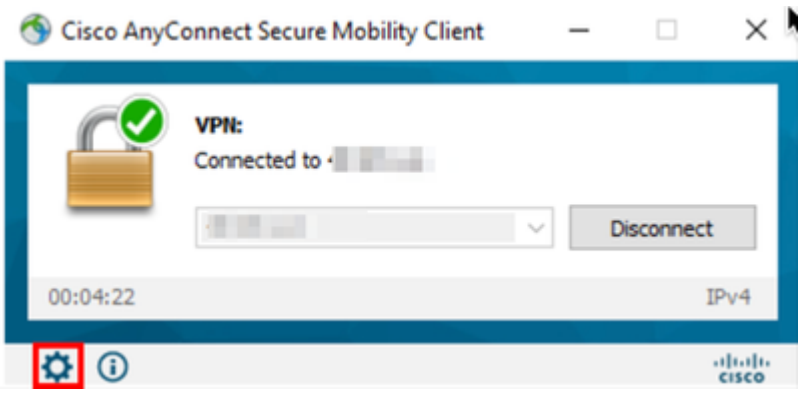
anyconnect-custom-attr dynamic-split-exclude-domains

```
anyconnect-custom-attr dynamic-split-include-domains
http-headers
hsts-server
enable
max-age 31536000
```

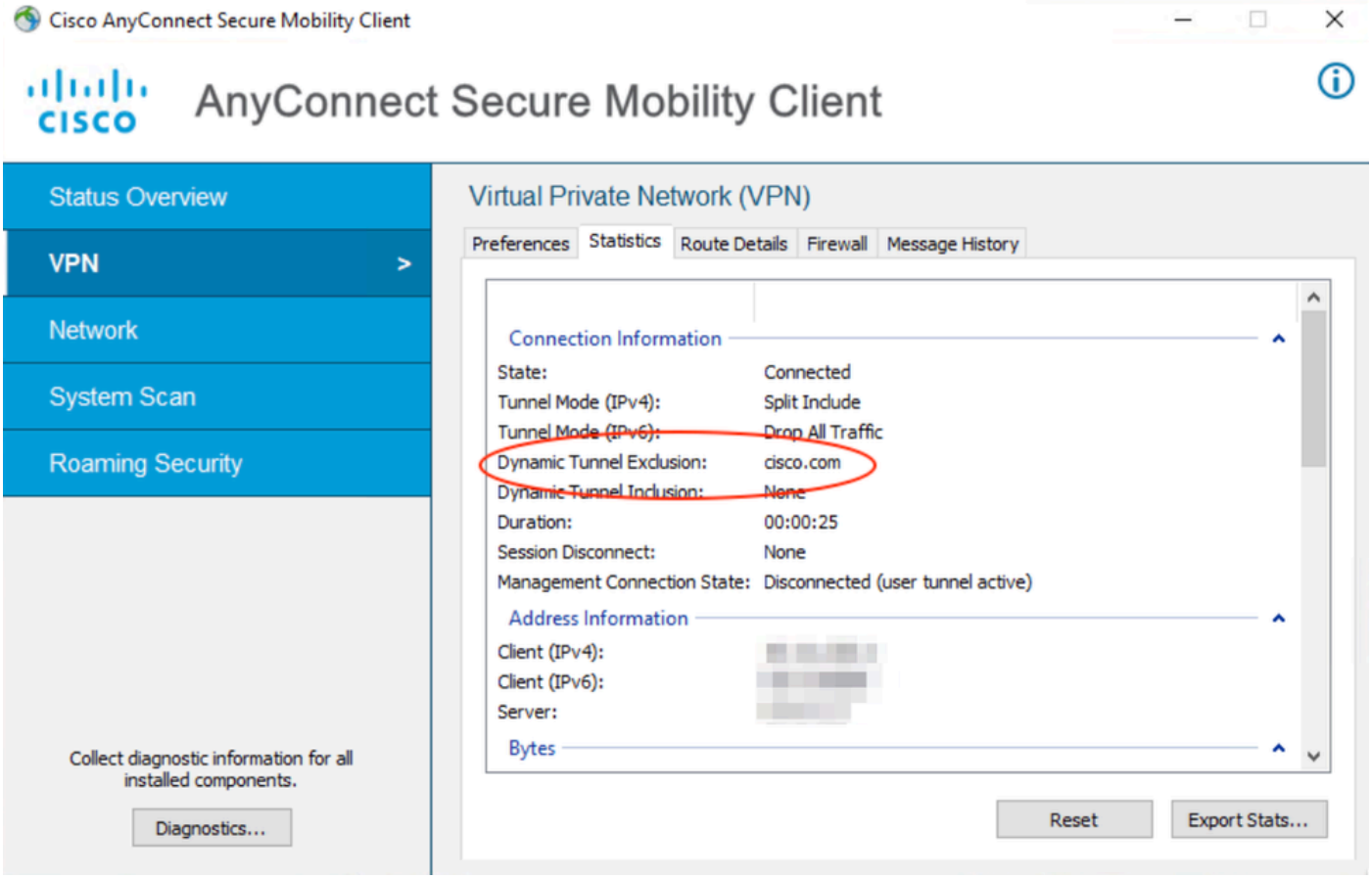
```
include-sub-domains
no preload
hsts-client
enable
content-security-policy
anyconnect image disk0:/csm/anyconnect-win-4.1005111-webdeploy-k9.pkg regex "Windows"
anyconnect profiles xmltest disk0:/csm/xmltest.xml
anyconnect enable
tunnel-group-list enable
cache
disable
certificate-group-map cert_map_test 10 cert_auth
error-recovery disable
```

In order to verify the configured dynamic tunnel exclusions on the client:

1. **Launch** the AnyConnect software and **click** the gear icon, as shown the image:



2. Navigate to **VPN > Statistics**, and confirm the domains displayed under **Dynamic Split Exclusion/Inclusion**:



Troubleshoot

You can use the AnyConnect Diagnostics and Reporting Tool (DART) in order to collect the data that is useful to troubleshoot AnyConnect installation and connection problems.

The 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.

Problem

If a wildcard is configured in the AnyConnect custom attributes, for example, *.cisco.com, the AnyConnect session is disconnected.

Solution

You can use the cisco.com domain value to allow the substitute of the wildcard. This change allows you to either include or exclude domains such as www.cisco.com and tools.cisco.com.

Related Information

- For additional assistance, contact Technical Assistance center (TAC). A valid support contract is required: Cisco Worldwide Support Contacts
- You can also visit the Cisco VPN Community.