# **Configure AnyConnect Dynamic Split Tunnel on FTD Managed by FMC**

### Contents

Introduction
Prerequisites
Requirements
Components Used
Background Information
Limitations
<u>Configure</u>
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
<u>Verify</u>
<u>Troubleshoot</u>
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 <u>Advanced AnyConnect VPN Deployments for Firepower Threat Defense with FMC</u>.

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 iOS (Apple) devices. See Cisco bug ID <u>CSCvr54798</u>
- Dynamic Split Tunnel is not supported on AnyConnect Linux Clients. See Cisco bug IDCSCvt64988

### 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 to.

Overview Analysis Policies Devices Objects AMP Intelligence			0 <sub>3</sub> Deploy System Help <b>v admin v</b>
Device Management Device Upgrade NAT VPN • Remote Access Q	oS Platform Settings FlexConfig Certificates		
SSL_AnyConnect			Save Save
			Policy Assignments (1)
		Local Realm: AmConnect-Local-Aut	Dynamic Access Policy: angsanc2-test
Connection Profile Access Interfaces Advanced			
			0
Name	AAA	Group Policy	
DefaultWE8VPNGroup	Authentication: None Authorization: None Accounting: None	DfttGrpPolicy	/ 8
SSL_AnyConnect_LocalAuth	Authentication: LOCAL Authorization: None Accounting: None	AnyConnect_Local_Auth	/ 6
SSL_AnyConnect_LDAPAuth	Authentication: AnyConnect-LDAP-Auth (AD) Authorization: AnyConnect-LDAP-Auth (AD) Accounting: None	AnyConnect_LDAP_Auth	/ 8

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

Overview Analysis Policies Devices Objects AMP Intelligence	ce					🔍 Deploy System Help <del>v</del> admin v
Device Management Device Upgrade NAT VPN > Remote Access	QoS PI	atform Settings Flex	Config Certificates			
SSL AnyConnect						Save Save
						Policy Assignments (1)
					Local Realm: Am/Connect-Lo	cal-Aut Dynamic Access Policy: angsanc2-test
Connection Profile Access Interfaces Advanced						
						0
Name	AAA	Edit Consection D				
DefaultWEBVPNGroup	Authent	Edit Connection P	rome		^	/ 8
	Authoriz	Connection Profile:*	SSL_AnyConnect_LocalAuth			
SSL_AnyConnect_LocalAuth	Authent	Group Policy:*	Auth	0	Auth	Ø 6
	Account	( ( )	Edit Group Policy			
SSL_AnyConnect_LDAPAuth	Authent	Client Address Ass	Ignment AAA Aliases		Auth	/ 8
	Account	IP Address for the re	mote clients can be assigned from local IP Add	ress pools/DHCP Servers/AAA Servers.		
		Configure the 'Client	Address Assignment Policy' in the Advanced ta	b to define the assignment criteria.		
		Address Pools:		0.		
		Name	IP Address Range			
		ftdv-dperezve-pool	172.16.13.1-172.16.13.254	2 B		
		DHCP Security		0		
		Name	DHCP Server IP Address			
		Configure device ov	errides in the address pool object to avoid IP addre	ss conflicts in case of object is shared across		
		muttinia deulnar		Save Cancel		

Step 2. Configure the AnyConnect Custom Attribute

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

Overview Analysis Policies Devices Objects Integration Device Management Device Upgrade NAT QoS Platform Settings FlexCor	fig Certificates VPN	Remote Access     Troubleshoot +	Desloy) 🧌 System Help v admin v
FTD_RAVPN_Policy1			E Save
			Policy Assignments (0) Local Realm: Local REALM1 Dynamic Access Policy: Boog
Connection Profile Access Interfaces Advanced	Edit Connection Pr	rofile ? ×	
	Add Group Policy	? ×	
	Name:* Any	vconnect_Local_Auth	0
Name AAA	Description:		
DefaultWEBVPNGroup Aut Aut	ritiza General AnyCon	nnect Advanced	/8
FTD_RAVPN_Policy11 Auth Auth Acct	Management Profile	AnyConnect Custom Attribute feature allows a more expedited way of configuring new endpoint features on Firewall Threat Defense. This feature is supported on Firewall Threat Defense 7.0 onwards.	28
new-testo Auto Auto	SSL Settings	Attribute Name Content	/8
		No records to display	
		Save Cancel	

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

Edit Connectio	on Profile	? ×
Edit Group Poli	icy	? ×
Name:*	Regular_Users_GP1	
Description:		
General An	yConnect Advanced	
Profile Management Profi	AnyConnect Custom Attribute feature allows a more expedited way of configuring new endpoint features on Firewall Threat Defense. This feature is supported on Firewall	
Client Modules	Add Custom Attribute ? ×	
Connection Set	AnyConnect Attribute:* Dynamic Split Tunneling	
	Custom Attribute Object:"	
	Add Cancel	
	Save Cance	

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.

Overview Analysis Policies Devices Objects AMP Intelligence	2			₿ <sub>3</sub> Deploy	System Heip + admin +
Device Management Device Upgrade NAT VPN > Remote Access	QoS Platfor	orm Settings FlexConfig Certificates			
SSL_AnyConnect					Seve Cancel
Connection Profile Access Interfaces Advanced			L	ocal Realm: <u>AnvConnect-Local-Aut</u> Dynar	Policy Assignments (1) tic Access Policy: <u>angsanc2-test</u>
					0
Name	AAA	Edit Connection Profile	2 X		
DefaultWE8VPNGroup	Authent Authoria Account	idit Group Policy	? ×		/ 8
SSL_AnyConnect_LocalAuth	Authent Authoria Account De	Name:* AnyConnect_Local_Auth Description:	Auth		05
SSL_AnyConnect_LDAPAuth	Authent		Auth		/8
	Authoria Account	General AnyConnect Advanced	Add AnyConnect Cus	stom Attribute	? ×
	P S C C	Profile Profile AnyConnect Custom Attribute feature alsos a more expected way of conte AnyConnect Custom Attribute Add Custom Attribute ? × SSI. Setting: AnyConnect Attribute:  AnyConnect Attribute:  AnyConnect Attribute:  AnyConnect Attribute:  AnyConnect Attribute:  Add Cancel	Name:* Description: AnyConnect Attribute: Enclude domains: Exclude domains:	Dynamic Split Tunneling     Cenfigure comma separated domain names that will be included in the Remote Access VPH Tunnel     Configure comma separated domain names that will	
		Save	Exclude domains:	Connguire control separated domain hames that we be excluded from the Remote Access VMI Turnel	Cancel

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.

Add Group Po	olicy				? X
Name:*	Anycon	nect_Local_Auth			
Description:					
General 🗛	nyConne	ct Advanced			
Profile Management Pro Client Modules	ofile	AnyConnect Custo endpoint features	om Attribute feature on FTD. This featur	allows a more expedited way of confi e is supported on FTD 7.0 onwards.	guring new
SSL Settings		Attribute	Name	Content	
Custom Attribute	11/25	Dynamic Split Tunneling	Dynamic-Split	Include domains: None Exclude domains: cisco.com	-
				Save	Cancel

### 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 the next:

<#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**:



Status Overview	Virtual Private Network (VPN)
VPN >	Preferences Statistics Route Details Firewall Message History
Network	Connection Information
System Scan	State:     Connected       Tunnel Mode (IPv4):     Split Include
Roaming Security	Tunnel Mode (IPv6): Drop All Traffic Dynamic Tunnel Exclusion: cisco.com
	Dynamic variation:       00:00:25         Session Disconnect:       None         Management Connection State:       Disconnected (user tunnel active)         Address Information       ^         Client (IPv4):
Collect diagnostic information for all installed components.	Reset Export Stats

### 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 <u>www.cisco.com and</u> tools.cisco.com.

### **Related Information**

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