# Configuración del túnel dividido dinámico de AnyConnect en FTD administrado por FMC

# Contenido

Introducción **Prerequisites** Requirements **Componentes Utilizados Antecedentes** Limitaciones Configurar Paso 1. Edite la directiva de grupo para utilizar el túnel dividido dinámico Paso 2. Configuración del atributo personalizado de AnyConnect Paso 3. Verificar la configuración, guardar e implementar Verificación Troubleshoot Problema Solución Información Relacionada Introducción

Este documento describe cómo configurar el túnel dividido dinámico de AnyConnect en Firepower Threat Defense (FTD) administrado por Firepower Management Center (FMC).

# Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco AnyConnect
- Conocimientos básicos de FMC

### **Componentes Utilizados**

La información que contiene este documento se basa en estas versiones de software:

- FMC versión 7.0
- FTD versión 7.0

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

# Antecedentes

La configuración del túnel dividido dinámico de AnyConnect en FTD administrado por FMC está totalmente disponible en FMC versión 7.0 y posteriores. Si ejecuta una versión anterior, debe configurarla mediante FlexConfig como se indica en <u>Advanced AnyConnect VPN Deployments for Firepower Threat Defense with FMC</u>.

Con la configuración de túnel dividido dinámico, puede ajustar la configuración de túnel dividido en función de los nombres de dominio DNS. Dado que las direcciones IP asociadas con los nombres de dominio completos (FQDN) pueden cambiar, la configuración de túnel dividido basada en nombres DNS proporciona una definición más dinámica del tráfico que se incluye o no en el túnel de acceso remoto de la red privada virtual (VPN). Si alguna de las direcciones devueltas para los nombres de dominio excluidos se encuentra dentro del conjunto de direcciones incluido en la VPN, esas direcciones se excluyen. Los dominios excluidos no están bloqueados. En su lugar, el tráfico a esos dominios se mantiene fuera del túnel VPN.

Observe que también puede configurar el túnel dividido dinámico para definir los dominios que se incluirán en el túnel y que, de lo contrario, se excluirían en función de la dirección IP.

### Limitaciones

Actualmente, estas funciones aún no son compatibles:

- El túnel dividido dinámico no es compatible con dispositivos iOS (Apple). Consulte Cisco bug ID <u>CSCvr54798</u>
- El túnel dividido dinámico no es compatible con los clientes Linux de Anyconnect. Consulte Cisco bug <u>IDCSCvt64988</u>

# Configurar

En esta sección se describe cómo configurar el túnel dividido dinámico de AnyConnect en FTD gestionado por FMC.

### Paso 1. Edite la directiva de grupo para utilizar el túnel dividido dinámico

1. En el FMC, navegue hasta **Devices > VPN > Remote Access**, luego seleccione el **perfil de conexión** al que desea aplicar la configuración.

Overview Analysis Policies Devices Objects AMP Intelligence		Opplay Sy	stem Help <b>v admin v</b>
Device Management Device Upgrade NAT VPN > Remote Access C	oS Platform Settings FlexConfig Certificates		
SSL_AnyConnect			Save Cancel
		Local Realm: AnyConnect-Local-Aut Dynamic	Policy Assignments (1) Access Policy: anosanc2-test
Connection Profile Access Interfaces Advanced			
			0
Name	AAA	Group Policy	
DefaultWEBVPNGroup	Authentication: None Authorization: None Accounting: None	DittorpPolicy	/ 8
SSL_AnyConnect_LocalAuth	Authorization: LOCAL Authorization: Vicine Accounting: None	AnyConnect_Local_Auth	/ 8
SSL_AnyConnect_LDAPAuth	Authentication: AnyConnect-LDAP-Auth (AD) Authorization: AnyConnect-LDAP-Auth (AD) Accounting: None	■ AnyConnect_LDAP_Auth	/8

2. Seleccione Editar Política de Grupo para modificar una de las políticas de grupo ya creadas.

Overview Analysis Policies Devices Objects AMP Intelligence	0.05	Morm Settings	Confin Cartificates			🍳 Deploy System Help 🛛 admin
SSL_AnyConnect	(03 PA	norm actungs Pres	coning certificates			Save Cance
Connection Profile Access Interfaces Advanced					Local Realm: <u>Am/Conr</u>	Policy Assignments (1) ect-Local-Aut Dynamic Access Policy: angsanc2-test
						0
Name	AAA	Edit Connection P	rofile	7.2	×	
DefaultWEBVPNGroup	Authent Authoriz Account	Connection Profile:*	SSL_AnyConnect_LocalAuth			/8
SSL_AnyConnect_LocalAuth	Authent Authoriz Account	Group Policy:*	Edit Group Policy		Auth	Ø 8
SSL_AnyConnect_LDAPAuth	Authent Authoriz Account	Client Address Ass	ignment AAA Aliases		Auth	/8
		IP Address for the re Configure the 'Client	mote clients can be assigned from local IP Address Address Assignment Policy' in the Advanced tab to	define the assignment criteria.		
		Address Pools:		0.		
		Name	IP Address Range			
		ftdv-dperezve-pool	172.16.13.1-172.16.13.254	/8		
		DHCP Servers:		0		
		Name	DHCP Server IP Address			
		Configure device ov	errides in the address pool object to avoid IP address co	nflicts in case of object is shared across		

### Paso 2. Configuración del atributo personalizado de AnyConnect

1. En la configuración de Directiva de grupo, navegue hasta **Anyconnect > Atributos personalizados**, haga clic en el **botón Agregar (+)**:

Overview Analysis Policies Devices Objects Integration		Deploy 🤷 System Help 👻 admin 👻
Device Management Device Upgrade NAT QoS Platform Settings FlexConfig	Certificates VPN + Remote Access Troubleshoot +	
FTD_RAVPN_Policy1		🖂 Save 🖉 Carcol
		Policy Assignments (0) Local Realm: Local REALM1 Dynamic Access Policy: Ngoe
Connection Profile Access Interfaces Advanced	Edit Connection Profile ? ×	
	Add Group Policy ? ×	
	Name:* Anyconnect_Local_Auth	0
Name AAA	Description:	
DefaultWEBVPWGroup Authentia Authentia Accountin	General AnyConnect Advanced	/8
PTD_RAVPN_Policy11 Authents Authents Accounts	Profile AnryConect Couton Attribute feature allows a more expedited way of configuring new Management Profile endpoint features on Firewall Threat Defense. This feature is supported on Firewall Clerit Modules Threat Defense 7.8 onwards.	<i>2</i> 6
new-teato Authen/i Authen/i Authen/i	SSL Settings Custom Stribute Attribute Name Content	<b>J</b> 8
	No records to display	

2. Seleccione el atributo **Dynamic Split Tunneling** AnyConnect y haga clic en el botón **Agregar (+)** para crear un nuevo objeto de atributo personalizado:

Edit Connection Profile	? ×
Edit Group Policy	? ×
Name:* Regular_Users_GP1	
Description:	
General AnyConnect Advanced	
Profile AnyConnect Custom Attribute feature allows a more expedited way of configure endpoint features on Firewall Threat Defense. This feature is supported on Fi	uring new rewall
Client Modules Add Custom Attribute ? ×	0
Connection Sett Custom Attribute:* Dynamic Split Tunneling	48
Custom Attribute Object:*	
Add Cancel	
Save	Cancel

3. Introduzca el **nombre** del **atributo personalizado de AnyConnect** y configure los dominios que se incluirán o excluirán dinámicamente.

Nota: Solo puede configurar Incluir dominios o Excluir dominios.

	Overview Analysis Policies Devices Objects AMP Intelligence						₿ <sub>3</sub> De	sloy System Help <del>v</del> admin v
	Device Management Device Upgrade NAT VPN > Remote Access Q	os Pl	atform Settings FlexCo	Config Certificates				
	SSL_AnyConnect							Save Cancel
Name       Add         Default/REXVING/rup       Add         SSL, Any:Connect, Local-Auth       Add         SSL, Any:Connect, Local-Auth       Add         Management Horle       Addresse         Forter       Advacement         Default/REXVING/rup       Addresse         SSL, Any:Connect, Local-Auth       Addresse         Management Horle       Advacement         Partie       Advacement         Add Custom Attributes       Operante: Split Turneling         Concetton Stitl       Casem Attributes         Conceton Stitl       Ca	Connection Profile Access Interfaces Advanced					u	cal Realm: <u>AnvConnect-Local-Aut</u>	Policy Assignments (1) Synamic Access Policy: angsans2-test
Name     Add       Dordurd UNERPARTICIPUP     Add       SSL, Any Connect, LIXARACIN     Add       SSL, Any Connect, LIXARACIN     Add       SSL, Any Connect, LIXARACIN     Add       Add     Any Connect, Advanced       Profile     Any Connect, Advanced or PTD 2 Symmits       Profile     Any Connect, Advanced or PTD 2 Symmits       Profile     Any Connect, Attribute       SSL, Serting Connect in Attribute     ? x       SSL, Serting Connect in Attribute     ? x       Add     Connect in Attribute       Connection Stef     Connect in Attribute       Connection Stef     Connect in Attribute       Connect in Stef     Connect in Attribute       Add     Connect in the Rennect Access VPE Tunnell       Add     Connect in the Rennect Access VPE Tunnell								0
DebularREEWINGroup Authors   SSL, Any Connect, Local Author   SSL, Any Connect, Local Author   Authors   SSL, Any Connect, Local Author Authors Solution Authors fabre fabres a nore segretorial segret and in autobrain fabres a local a any connect Custom Attribute fabre fabres a soported in TB 2.58 attributes: Outer Moder Add Custom Attribute: Outer Moder Outer Moder Outer Moder Add Custom Attribute: Outer Moder Outer Moder Outer Moder Outer Moder Outer Moder Outer Moder O	Name	AAA	Edit Connection Pro	ofile		2 ×		
SSL, AnyConnect, LDAMuth SSL, AnyConnect, LDAMuth Access SSL, AnyConnect, Attribute SSL, An	DefaultWEBVPNGroup	Authent Authoria Account	Edit Group Policy	sine .		? ×		/ 5
SSLAN/Connect_LDAMAUN       Autom       Autom       Add AnyConnect Custom Attribute       ? ×         Phale       Automatic Automatic Relative Release a more expedided way of control       Name:*       Description:         Content Modale       Add Custom Attribute Digect.*       •       Add AnyConnect Attribute.*       •         Custom Attribute Digect.*       •       •       •       •       •       •         Add       •	SSL_AnyConnect_LocalAuth	Authent Authoria Account	Name:* AnyCo Description:	onnect_Local_Auth		Auth		28
Profile       AnyConnect Custom Attribute       7 ×         SS. Settings       Add Custom Attribute       7 ×         Custom Attribute       0 ynamic Split Tunneling         AnyConnect Attribute       0 ynamic Split Tunneling         Custom Attribute       0 ynamic Split Tunneling         Exclude domains:       0 ynamic Split Tunneling         Exclude domains:       0 ynamic Split Tunneling         De excluded from the Remote Access VPH Tunnel       0 ynamic Split Tunneling         De exclude domains:       0 ynamic Split Tunneling         De exclude domains:       0 ynamic Split T	SSL_AnyConnect_LDAPAuch	Authent Authoria	General AnyConn	nect Advanced		Auth Add AnyConnect Cus	tom Attribute	2 S
Save and the second s		Account	Profile Management Profile Clarit Modules SG, Settings Connection Sett Custom Attribut Custom Attribut	AnyConnect Custom Attribute feature a endpoint features on FTD. This feature Connect Attribute Connect Attribute: Dynamic Solit Ture tom Attribute Object:*	lovs a more expedited way of configs supported on FTD 7.0 ensets. ? × elling v o Add Cancel Save	Name:* Description: AnyConnect.Attribute: Include domains: Exclude domains: Allow Overrides	Dynamic Split Tunneling     Configure comma separated domain names the     included in the Remote Access VHs Tunnel     Configure comma separated domain names the     be excluded from the Remote Access VHs Tunnel	

En este ejemplo, configuramos **cisco.com** como el dominio que se excluirá y denominamos el atributo personalizado **Dynamic-Split-Tunnel**, como se muestra en la imagen:

,		
Name:*	Dynamic-Split-Tunnel	
Description:		
AnyConnect Attribute:*	Dynamic Split Tunneling	~
Include domains:	Configure comma separated domain names that will included in the Remote Access VPN Tunnel	be
Exclude domains:	cisco.com	
Allow Overrides		

### Paso 3. Verificar la configuración, guardar e implementar

Verifique que el atributo personalizado configurado sea correcto, guarde la configuración e implemente los cambios en el FTD en cuestión.



### Verificación

Puede ejecutar estos comandos en el FTD mediante la interfaz de línea de comandos (CLI) para confirmar la configuración del túnel dividido dinámico:

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

En este ejemplo, la configuración es la siguiente:

```
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

Para verificar las exclusiones de túnel dinámico configuradas en el cliente:

1. Inicie el software AnyConnect y haga clic en el icono del engranaje, como se muestra en la imagen:

Sisco AnyConnect Secure Mobility Client			- 🗆	×	Ņ
	VPN: Connected to 4	V [	Disconne	ct	
00:04:22				IPv4	
<b>‡</b>				cisco	

2. Navegue hasta VPN > Statistics y confirme los dominios mostrados en Dynamic Split Exclusion/Inclusion:

cisco	AnyConnect Secure Mobility Client				t	
Status Ove	rview	Virtual Pri	ivate Ne	twork (VPN	I)	
		Preferences	Statistics	Route Details	Firewall	Message

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
	Duration: 00:00:25 Session Disconnect: None Management Connection State: Disconnected (user tunnel active) Address Information
Collect diagnostic information for all	Client (IPv4): Client (IPv6): Server: Bytes
Diagnostics	Reset Export Stats

# Troubleshoot

Puede utilizar la herramienta de diagnóstico e informes (DART) de AnyConnect para recopilar los datos que son útiles para solucionar los problemas de instalación y conexión de AnyConnect.

La DART reúne los registros, el estado y la información de diagnóstico para el análisis de Cisco Technical Assistance Center (TAC) y no requiere privilegios de administrador para ejecutarse en la máquina del cliente.

### Problema

Si se configura un comodín en los atributos personalizados de AnyConnect, por ejemplo, **\*.cisco.com**, la sesión de AnyConnect se desconecta.

### Solución

Puede utilizar el valor del dominio **cisco.com** para permitir el reemplazo del comodín. Este cambio le permite incluir o excluir dominios como **www,cisco.com** y **tools.cisco.com**.

# Información Relacionada

- Para obtener asistencia adicional, póngase en contacto con el centro de asistencia técnica (TAC). Se necesita un contrato de soporte válido: <u>Contactos de soporte a nivel mundial de</u> <u>Cisco.</u>
- También puede visitar Cisco VPN Community aquí.

×

#### Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).