Configurar o túnel de divisão dinâmica do AnyConnect no FTD gerenciado pelo FMC

Contents

Introduction **Prerequisites** Requirements **Componentes Utilizados** Informações de Apoio Limitações Configurar Etapa 1. Edite a Política de Grupo para usar o Túnel Dividido Dinâmico Etapa 2. Configurar o atributo personalizado do AnyConnect Etapa 3. Verificar a configuração, Salvar e Implantar Verificar Troubleshoot Problema Solução Informações Relacionadas Introduction

Este documento descreve como configurar o AnyConnect Dynamic Split Tunnel no Firepower Threat Defense (FTD) gerenciado pelo Firepower Management Center (FMC).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco AnyConnect
- Conhecimentos básicos de CVP

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- FMC versão 7.0
- FTD versão 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

A configuração do túnel dividido dinâmico AnyConnect no FTD gerenciado pelo FMC está totalmente disponível no FMC versão 7.0 e mais recente. Se você executar uma versão mais antiga, precisará configurá-la via FlexConfig, conforme instruído em <u>Advanced AnyConnect VPN</u> <u>Deployments for Firepower Threat Defense with FMC</u>.

Com a configuração de túnel dividido dinâmico, você pode ajustar a configuração de túnel dividido com base nos nomes de domínio DNS. Como os endereços IP associados a nomes de domínio totalmente qualificados (FQDN) podem mudar, a configuração de túnel dividido com base em nomes DNS fornece uma definição mais dinâmica de qual tráfego está ou não incluído no túnel VPN de acesso remoto. Se algum endereço retornado para nomes de domínio excluídos estiver dentro do pool de endereços incluído na VPN, esses endereços serão excluídos. Os domínios excluídos não são bloqueados. Em vez disso, o tráfego para esses domínios é mantido fora do túnel VPN.

Observe que você também pode configurar o túnel de divisão dinâmica para definir domínios a serem incluídos no túnel que seriam excluídos de outra forma com base no endereço IP.

Limitações

No momento, esses recursos ainda não são suportados:

- O Dynamic Split Tunnel não é suportado em dispositivos iOS (Apple). Consulte o bug da Cisco ID <u>CSCvr54798</u>
- O Dynamic Split Tunnel não é suportado em clientes Anyconnect Linux. Consulte o bug da Cisco IDCSCvt64988

Configurar

Esta seção descreve como configurar o túnel de divisão dinâmica do AnyConnect no FTD gerenciado pelo FMC.

Etapa 1. Edite a Política de Grupo para usar o Túnel Dividido Dinâmico

1. No FMC, navegue até **Devices > VPN > Remote Access** e selecione o **Perfil de Conexão** ao qual deseja aplicar a configuração.

Overview Analysis Policies Devices Objects AMP Intelligence		Opplay Sy	stem Help v admin v
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. Selecione Editar Política de Grupo para modificar uma das políticas de grupo já criadas.

Overview Analysis Policies Devices Objects AMP Intelligence	:e					0, Deploy System Help v admin v
Device Management Device Upgrade NAT VPN + Remote Access	QoS Pl	atform Settings Flex	Config Certificates			
SSL_AnyConnect						Save Cancel
						Policy Assignments (1)
					Local Realm: AnyConnect-Local-Aut	Dynamic Access Policy: angsanc2-test
					Color Property Colorado Antonio	optimiting reaction force (). Burnanting, Aug
Connection Profile Access Interfaces Advanced						
						0
Name	AAA	Edit Connection Pr	ofile	7 >		
DefaultWEBVPNGroup	Authent					/ 8
	Account	Connection Profile:*	SSL_AnyConnect_LocalAuth			
SSL_AnyConnect_LocalAuth	Authent	Group Policy:*	Any consider and Auth		Auth	Ø 8
	Account	C	Edit Group Policy			
SSL_AnyConnect_LDAPAuth	Authent	Client Address Assi	gnmenc AAA Aliases		Auth	/ 8
	Account	IP Address for the ren	note clients can be assigned from local IP Addre	is pools/DHCP Servers/AAA Servers.		
		Configure the 'Client'	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	2 G		
		Name	DHCP Server IP Address			
		Name	Unce server 17 Address			
			rrides in the address paul object to avoid IP address	conflicts in case of object is shared across		
		multinla dassinar	These in the sources providely to show in sources			
				Save Cancel		

Etapa 2. Configurar o atributo personalizado do AnyConnect

1. Na configuração de Diretiva de Grupo, navegue até **Anyconnect** > Custom Attributes, clique no botão **Add (+)**:

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	J 8
	No records to display	

2. Selecione o atributo **Dynamic Split Tunneling** AnyConnect e clique no botão **Add (+)** para criar um novo objeto de atributo personalizado:

Edit Connection Profile	? ×
Edit Group Policy	? ×
Name:* Regular_Users_GP1	
Description:	
General AnyConnect Advanced	
Profile AnyConnect Custom Attrib Management Profile endpoint features on Firew	ute feature allows a more expedited way of configuring new all Threat Defense. This feature is supported on Firewall
Client Modules Add Custom Attribute	? × 0
Connection Set: AnyConnect Attribute:* Dyna Custom Attribut	mic Split Tunneling
Custom Attribute Object:*	
	Add Cancel
	Save Cancel

3. Insira o **Nome** do **Atributo personalizado do AnyConnect** e configure os domínios para serem dinamicamente incluídos ou excluídos.

Observação: você só pode configurar Incluir domínios ou Excluir domínios.

	Overview Analysis Policies Devices Objects AMP Intelligence						₿ ₃ De	sloy System Help v 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 Operante: Split Turneling Concetton Stitl Casem Attributes Operante: Split Turneling Exclude demains: Careful Hittlintes Careful Hittlintes Add Custom Attributes Casem Attributes Careful Hittlintes Casem Attributes Operante: Split Turneling Exclude demains: Confugure comma separated duratin names But will Exclude demains: Confugure comma separated duratin names But will <td< th=""><th>Connection Profile Access Interfaces Advanced</th><th></th><th></th><th></th><th></th><th>u</th><th>cal Realm: <u>AnvConnect-Local-Aut</u></th><th>Policy Assignments (1) Synamic Access Policy: anssans2-test</th></td<>	Connection Profile Access Interfaces Advanced					u	cal Realm: <u>AnvConnect-Local-Aut</u>	Policy Assignments (1) Synamic Access Policy: anssans2-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 Connection Set Any Connect Attribute Connection Set Any Connect Attribute Connection Set Connection Methode Status								0
DebularREEWINGroup Authors SSL, Any Connect, Local Author SSL, Any Connect, Local Author Authors SSL, Any Connect, Local Author Authors Solution Authors fabric fabrics a more segretated and in names that will Custom Attribute: Output and Top Link Educe is Split Tunnelling Add Custom Attribute: Output and Top Link Educe is Split Tunnelling Add Custom Attribute: Output and Top Link Educe is Split Tunnelling Solution Attribute: Output and Top Link Educe is Split Tunnelling Solution Attribute: Output and Top Link Educe is Split Tunnelling Solution Attribute: Output and Top Link Educe is Split Tunnelling Solution Attribute: Output and Top Link Educe is Split Tunnelling Solution Attribute: Output and Top Link Educe is Split Tunnelling Solution Attribute: Output and Top Link Educe is Split Tunnelling Solution Attribute: Output and Top Link Educe is Split Tunnelling Solution Attribute: Output and Top Link Educe is Split Tunnelling Solution Attribute: Output and Top Link Educe is Split Tunnelling Solution Attribute: Output and Top Link Educe in the Remote Access Vint Tunnelling Exclude domains: Configure genma separated domain names that will Exclude domains: Configure genma separated domain names that will Addition top Configure genma separ	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 v 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	

Neste exemplo, configuramos **cisco.com** como o domínio a ser excluído e nomeamos o atributo personalizado **Dynamic-Split-Tunnel**, como mostrado na imagem:

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	٦
```````````````````````````````````````		

### Etapa 3. Verificar a configuração, Salvar e Implantar

Verifique se o atributo personalizado configurado está correto, salve a configuração e implante as alterações no FTD em questão.



### Verificar

Você pode executar estes comandos no FTD através da interface de linha de comando (CLI) para confirmar a configuração do túnel dividido dinâmico:

- show running-config webvpn
- show running-config anyconnect-custom-data
- show running-config group-policy <Nome da diretiva de grupo>

Neste exemplo, a configuração é a seguinte:

```
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 as exclusões de túnel dinâmico configuradas no cliente:

1. Inicie o software AnyConnect e clique no ícone da engrenagem, como mostrado na imagem:

🕙 Cisco AnyO	Connect Secure Mobility Client	-	- 🗆	×	Ņ
	VPN: Connected to •	V [	Disconne	ect	
00:04:22				IPv4	
<b>‡</b> (i)				cisco	

2. Navegue até VPN > Statistics e confirme os domínios exibidos em Dynamic Split Exclusion/Inclusion:

cisco	AnyConnect	t Secure	e Mo	bility C	lien	t
Status Ove	rview	Virtual Pr	ivate Ne	twork (VPN	1)	
		Preferences	Statistics	Route Details	Firewall	Message

VPN >	Preferences Statistics Route Details Firewall Message History	
Network	Connection Information	<b>^</b>
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	
	Client (IPv4): Client (IPv6): Server:	
Collect diagnostic information for all installed components.	Bytes Reset Export Sta	• •

# Troubleshoot

Você pode usar o AnyConnect Diagnostics and Reporting Tool (DART) para coletar os dados que são úteis para solucionar problemas de instalação e conexão do AnyConnect.

O DART reúne os registros, o status e as informações de diagnóstico para a análise do Cisco Technical Assistance Center (TAC) e não exige os privilégios de administrador para ser executado no computador cliente.

#### Problema

Se um curinga for configurado nos atributos personalizados do AnyConnect, por exemplo, ***.cisco.com**, a sessão do AnyConnect será desconectada.

### Solução

Você pode usar o valor de domínio **cisco.com** para permitir o substituto do curinga. Essa alteração permite incluir ou excluir domínios como **www.cisco.com** e **tools.cisco.com**.

## Informações Relacionadas

- Para obter assistência adicional, entre em contato com o Centro de Assistência Técnica (TAC). É necessário um contrato de suporte válido: <u>Contatos de suporte da Cisco no mundo</u> <u>inteiro.</u>
- Você também pode visitar a Comunidade Cisco VPN aqui.

×

**()** 

#### Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.