# Desactivar el tiempo de espera de inactividad de VPN de sitio a sitio de FTD con las políticas de FlexConfig

# Contenido

Introducción Prerequisites Requirements Componentes Utilizados Antecedentes Configurar Configurar la política FlexConfig y el objeto FlexConfig Verificación Troubleshoot Información Relacionada

## Introducción

Este documento describe cómo modificar el atributo **vpn-idle-timeout** de una VPN con políticas FlexConfig en Cisco Firepower Management Center (FMC) para evitar el tiempo de inactividad del túnel debido a la inactividad o el tiempo de espera inactivo.

## Prerequisites

#### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Firepower Threat Defense (FTD)
- FMC
- Políticas de FlexConfig
- Topologías VPN de sitio a sitio

#### **Componentes Utilizados**

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

- FMCv 6.5.0.4 (compilación 57)
- FTDv 6.4.0.10 (compilación 95)

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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Antecedentes

Tanto las VPN basadas en políticas (mapa criptográfico) basadas en el intercambio de claves de Internet versión 1 (IKEv1) como las de la versión 2 del intercambio de claves de Internet (IKEv2) son túneles a demanda. De forma predeterminada, el FTD finaliza la conexión VPN si no hay actividad de comunicación sobre el túnel en un período determinado llamado **vpn-idle-timeout**. Este temporizador se establece en 30 minutos de forma predeterminada.

# Configurar

#### Configurar la política FlexConfig y el objeto FlexConfig

Paso 1. En **Devices > FlexConfig**, cree una nueva política FlexConfig (si aún no existe) y adáptela al FTD donde se configura la VPN de sitio a sitio.

cisco Firepower Manag	gement C × +		-	- 🗆 ×
$\leftarrow \rightarrow$ C $\textcircled{O}$ O	https://10.31.124.31:6005/	ddd/#Flexc 90% 🏠	☆ 🛛 🖬	\$** @ ≡
Getting Started 💮 New Tab	🖉 BEMS 🏾 🎯 Identity Services Er	gine 號 Next Generation W	/eb >>> []	Other Bookmarks
Overview Analysis Policie	es Devices Objects AMP	Intelligence Deploy	/ 🔍 System I	Help 🔻 admin 🔻
Device Management NAT	VPN   QoS Platform Setti	ngs FlexConfig Cer	rtificates	
				💿 New Policy
FlexConfig Policy	Status	Last Mod	lified	
New Policy			ŕ	
Description:	:xconiig_FTD_B			
Targeted Devices				<b>D</b> 0
Available Devices	· value Add to Policy	Selected Devices	Cancel	
Last login on Monday, 2021-07-05 at 16	5:03:21 PM from 10.24.67.117 How	То		uluulu cisco

$\operatorname{cisco}^{\operatorname{slub}}$ Cisco Firepower Management C X –	F		- 🗆 ×
$\leftarrow$ $\rightarrow$ C $\textcircled{a}$ $\bigcirc$ $\textcircled{b}$ https://10	0.31.124.31:6005/ddd/#Flex 90%	6 ☆ ☆ ⊘	4+- 💿 =
💮 Getting Started 💮 New Tab 🥖 BEMS 🧐	Identity Services Engine 🜼 Next Ge	eneration Web >>>	C Other Bookmarks
Overview Analysis Policies Devices	Objects AMP Intelligence	Deploy 🔒 System	Help 🔻 admin 🔻
Device Management NAT VPN ▼ QoS	Platform Settings FlexCont	fig Certificates	
			📀 New Policy
FlexConfig Policy	Status	Last Modified	
FlexConfig_FTD_B	Targeting 1 devices Up-to-date on all targeted devices	2021-06-15 17:21:38 Modified by "admin"	la 🖉 🔂

Paso 2. Dentro de esa política, cree un objeto FlexConfig de la siguiente manera:

Nombre: S2S\_Idle\_TimeOut Implementación: En cualquier momento Tipo: Anexar

atributos de política de grupo .DefaultS2SGroupPolicy vpn-idle-timeout none



	cisco Fire	power Mana	agement C	× dada	Cisco Firep	oower Man	agement⊂×	+							-	- 1		×
$\leftarrow$	$\rightarrow$ C	6	0 8	https://	/10.31.12	<b>4.31</b> :6005	/ddd/#Flexc	onfigPolicy	/Editor;uuid=0	00C2988-	90%	☆	岔	$\bigtriangledown$		4900	<b>m</b> 9	≡
⊕ Ge	etting Started	🕀 New Tab	b 🖉 BEN	IS 🍥 Ide	entity Servi	ices Engine	e 🗰 Next Ge	eneration We	eb 🔐 Rege	Tester and	d Deb	\delta Mi vacur	na		C	] Other	Bookn	narks
Over	view Analy	sis Polici	es Devi	ices Ob	bjects	AMP I	ntelligence					Deploy	0	System	Help	o≢ a	dmin	<b>^</b>
Devic	Add Flexe	Config Obj	ject													? >	× scel	
Enter I	Name:	S25	_Idle_Time	Dut													ice.	
	Description	1:															nts	(1)
Ava	31																	
	Copy	/-pasting any	y rich text m	ight introd	luce line bre	eaks while	generating CLI	. Please verif	y the CLI before	deployment								а.
1	O Inse	nt •	∎¥ •×								Deploymen	t: Everyti	me 🗸	Type:	Apper	nd v		
	group vpn-	-policy idle-tim	.Defau	ltS2SG1 one	roupPol	licy at	tributes											
1	C.																	
	Variables				Dimen	sion	Default Val	ue	Property (Typ	e Over	ride	Descrit	ption					
							No rec	orde to c	display									
							No rec	lorus to t	лэріау									
Last lo	gin on Monady, 20							How To					Sa	ive	C	ancel		
<																		>

y **guárdelo**.

Paso 3. En el panel izquierdo, busque y arrástrelo al panel derecho con el botón >.

	cisco Firepower Manag	gement C ×	+											-		×
~	→ C ŵ	O 🔓 http	s://10	).31.124.31:	6005/dd	d/#Flexconf	igPolicyEdi	tor;uuid=000	C2988-	90%	숪	岔			. 💿	=
0	Setting Started A New Tab		Ident	ity Services F	ngine 🐙	Next Gener	ation Web	Regev Te	ester and I	Deb	A Mi v	acupa			ther Bor	kmarks
		Q DEMO			ingine un	a riext ocher		neger i	coter and t			acuna				-
Ove	erview Analysis Policie	es Devices	Obje	ects   AMP	P Intell	igence					D	eploy	1 Syst	tem Help	v ad	min ▼
Dev	ice Management NAT	VPN VQ05	; P	latform Sett	tings	FlexConfig	Certifica	tes								
Fle	xConfig_FTD_B							Y	ou have ur	nsaved	changes	Preview C	onfig	😑 Save	8	Cancel
Ente	Description															
													1	🖳 Policy A:	signmen	ts (1)
A	vailable FlexConfig 🕏	FlexConfig Ol	oject		Selected	d Prepend F	lexConfigs									
			×	#			Name				[	Description				
	4 🥩 User Defined		^													
	aaa-server-map															
	disable-am															
	EEM_script_PeriodicLo	gOffAnyconnect														
	Idap-attribute-map															
	Management-access															
	MAT-T-Dicable	igarciam														
l Ir	S25 idle timeout															
				>	Selected	d Append F	exConfias									
	VPN-filter															
	4 🧔 System Defined			*			Name				I.	Description				
	Default_DNS_Configur	e														
	Default_Inspection_Pr	otocol_Disable														
	Default_Inspection_Provide the section_Provide the section_Provide the section_Provide the section of the se	otocol_Enable														
	DHCPv6_Prefix_Delega	ation_Configure														
	DHCPv6_Prefix_Delega	ation_UnConfigure														
	DNS_Configure															
	DNS_UnConfigure															
	Eigrp_Configure															
	Eigrp_Interface_Config	jure														
	📄 Eigrp_UnConfigure		~													
						_	_									
Last	login on Monday, 2021-07-05 at 16	5:03:21 PM from 10	.24.67.	117			low To								1	isco

	cisco Firepower Managemen	t C × +							-		$\times$
~	$\rightarrow$ C $\textcircled{o}$ O	A https://10.	31.124.31:6005/d	ddd/#FlexconfigPolicyEd	itor;uuid=000C2988-	90% 값	岔		41+	6	≡
A	Setting Started A New Tab	REMS 🧐 Identit	v Services Engine	the Next Generation Web	Regex Tester and	Deb. 🛞 Mi	vacuna		C Othe	r Bookr	marks
Ove	erview Analysis Policies D	evices Object	ts   AMP Int	elligence			Deploy	System	Help 🔻	adm	in ▼
Dev	ice Management NAT VPN	<ul> <li>QoS Pla</li> </ul>	atform Settings	FlexConfig Certifica	ates			_	_		
Fle	xConfig_FTD_B				You have u	nsaved changes	Preview Con	fig 📄	Save	🙁 Ca	ncel
Ente	r Description										
								🖳 Pc	olicy Assig	Inments	(1)
A	vailable FlexConfig 🖒 🚺 😡	exConfig Object	T Selec	ted Prepend FlexConfig	5						
		×		Name			Description				
4											٦.
	⊿ 🣁 User Defined	^									
	aaa-server-map										
	disable-am										
	EEM_script_PeriodicLogOffAn	yconnect									
	Idap-attribute-map										
	management-access										
	NAT-T-Disable										
	S2S_idle_timeout										
11	test		Selec	ted Append FlexConfigs							
	VPN-filter			Name			Description				
	4 🣁 System Defined		1	525 idle timeout							
	Default_DNS_Configure		-	525_Idle_diffeout							
	Default_Inspection_Protocol_	Disable									
	Default_Inspection_Protocol_	Enable									
	DHCPv6_Prefix_Delegation_C	Configure									
	DHCPv6_Prefix_Delegation_U	InConfigure									
	DNS_Configure										
	DNS_UnConfigure										
	Eigrp_Configure										
	Eigrp_Interrace_Configure										
	Eigrp_onconfigure	Ŧ									
_											
Last	login on Monday, 2021-07-05 at 16-02-21	PM from 10 24-67-1	17	How To						սև	
cast	login on Honday, 2021-07-05 at 16:03:21	111 1011 10.24.67.1	**	now to						cis	co

Guarde los cambios y implemente.

Paso 3.1 (Opcional) Como paso intermedio, después de haber guardado los cambios de configuración, puede elegir **Vista previa de configuración** para asegurarse de que los comandos FlexConfig estén listos para ser empujados al final de la configuración.

the Cisco Firepower Management C × +		- 🗆 ×
← → C 🟠 https://10.31.124.31:6005/ddd/#FlexconfigPolicyEditor;uuid=000C2988-  90%	☆ ☆ ♡	<b>.</b> 4+• 💿 =
🕀 Getting Started 🕀 New Tab 🥖 BEMS 🧐 Identity Services Engine 🛲 Next Generation Web 🇮 Regex Tester and Deb 🧃	🌖 Mi vacuna	C Other Bookmarks
Overview Analysis Policies Devices Objects AMP Intelligence	Deploy 0, Sy	stem Help 🔻 admin 🔻
Device Management NAT VPN  VPN  QoS Platform Settings  FlexConfig Certificates		
FlexConfig_FTD_B	Preview Config	Save Cancel
Preview PlexConing	1 ^	Policy Assignments (1)
Available FlexConfig	~	
<pre>Provide the set of the set o</pre>	Close	
Last login on Monday, 2021-07-05 at 16:03:21 PM from 10.24.67.117		aludo

#### Verificación

Una vez que se complete la implementación, puede ejecutar este comando en LINA (> system support diagnostic-cli) para confirmar que la nueva configuración está ahí:

firepower# show running-config group-policy .DefaultS2SGroupPolicy
group-policy .DefaultS2SGroupPolicy internal
group-policy .DefaultS2SGroupPolicy attributes
vpn-idle-timeout none <<<----<omitted output>

**Precaución:** Tenga en cuenta que este cambio afecta a todas las VPN S2S del FTD. NO es una configuración por túnel sino una global.

Aunque la configuración está ahí, el túnel activo necesita ser rebotado (**clear crypto ipsec sa peer** <*Remote\_Peer\_IP\_Address>*) para que el cambio surta efecto cuando el túnel se restablezca nuevamente. Puede confirmar que el cambio está en vigor con este comando:

```
Connection : X.X.X.X
Index : 7 IP Addr : X.X.X.X
Protocol : IKEv1 IPsec
Encryption : IKEv1: (1)AES256 IPsec: (1)AES256
Hashing : IKEv1: (1)SHA1 IPsec: (1)SHA1
Bytes Tx : 400 Bytes Rx : 400
Login Time : 22:06:56 UTC Tue Jun 15 2021
Duration : 0h:18m:00s
Tunnel Zone : 0
IKEv1 Tunnels: 1
IPsec Tunnels: 1
IKEv1:
Tunnel ID : 7.1
UDP Src Port : 500 UDP Dst Port : 500
IKE Neg Mode : Main Auth Mode : preSharedKeys
Encryption : AES256 Hashing : SHA1
Rekey Int (T): 86400 Seconds Rekey Left(T): 85319 Seconds
D/H Group : 5
Filter Name :
IPsec:
Tunnel ID : 7.2
Local Addr : A.A.A.A/255.255.255.255/0/0
Remote Addr : B.B.B.B/255.255.255.128/0/0
Encryption : AES256 Hashing : SHA1
Encapsulation: Tunnel
Rekey Int (T): 28800 Seconds Rekey Left(T): 27719 Seconds
Rekey Int (D): 4608000 K-Bytes Rekey Left(D): 4608000 K-Bytes
Idle Time Out: 0 Minutes Idle TO Left : 0 Minutes <<<<<-----
Bytes Tx : 400 Bytes Rx : 400
Pkts Tx : 4 Pkts Rx : 4
```

El contador *de tiempo de espera inactivo* debe establecerse en 0 Minutos en lugar de 30 minutos y la VPN debe permanecer activa independientemente de la actividad/tráfico que se esté ejecutando sobre ella.

**Nota:** Al momento de escribir este artículo, existe un Bug de mejora para integrar la capacidad de modificar esta configuración directamente en FMC sin la necesidad de Flexconfig. Consulte Cisco bug ID <u>CSCvr82274</u> - ENH: haga configurable vpn-idle-timeout

### Troubleshoot

Actualmente no hay información específica disponible para resolver problemas.

#### Información Relacionada

- Guía de Configuración de Firepower Management Center, Versión 7.0 Capítulo: Políticas FlexConfig para Firepower Threat Defense
- <u>Guía de Configuración de Firepower Management Center, Versión 7.0 Capítulo: VPN de</u> sitio a sitio para Firepower Threat Defense
- Soporte Técnico y Documentación Cisco Systems