Disable FTD Site-to-Site VPN Idle Timeout with FlexConfig Policies

Contents

Introduction Prerequisites Requirements Components Used Background Information Configure Configure FlexConfig Policy and FlexConfig Object Verify Troubleshoot Related Information

Introduction

This document describes how to modify the **vpn-idle-timeout** attribute of a VPN with FlexConfig Policies in Cisco Firepower Management Center (FMC) in order to prevent tunnel downtime due to Inactivity or Idle Timeout.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Firepower Threat Defense (FTD)
- FMC
- FlexConfig Policies
- Site-to-Site VPN topologies

Components Used

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

- FMCv 6.5.0.4 (build 57)
- FTDv 6.4.0.10 (build 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. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Both Internet Key Exchange version 1 (IKEv1) and Internet Key Exchange version 2 (IKEv2) Policy Based (Crypto map) Site-to-Site VPNs are on-demand tunnels. By default, the FTD terminates the VPN connection if there is no communication activity over the tunnel in a certain period of time called **vpn-idle-timeout**. This timer is set to 30 minutes by default.

Configure

Configure FlexConfig Policy and FlexConfig Object

Step 1. Under **Devices > FlexConfig** create a new FlexConfig Policy (if one does not already exist) and attach it to the FTD where the Site-to-Site VPN is configured.

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				D 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

cisco Firepower Management	+		_	□ ×
\leftarrow \rightarrow C \textcircled{a} \bigcirc \textcircled{a} ht	ttps://10.31.124.31:6005/ddd/#	#Flex 90% ☆ ☆	♥	
🕀 Getting Started 🕀 New Tab 🥖 BE	MS 🛯 🗐 Identity Services Engine	Next Generation Web	≫ 🗅 Otł	ner Bookmarks
Overview Analysis Policies Dev	vices Objects AMP Inte	elligence Deploy 🧕	System Help	🔹 admin 💌
Device Management NAT VPN •	QoS Platform Settings	FlexConfig Certificate	s	
			💽 N	ew Policy
FlexConfig Policy	Status	Last Modified		
FlexConfig_FTD_B	Targeting 1 devices Up-to-date on all target	2021-06-15 17:2 ed devices Modified by "adm	1:38 in"	Fi 🥒 🗊

Step 2. Inside that policy create a FlexConfig object as follows:

Name: S2S_Idle_TimeOut Deployment: Everytime Type: Append

group-policy .DefaultS2SGroupPolicy attributes 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	4.31 :6005	/ddd/#Flexc	onfigPolicy	/Editor;uuid=0	00C2988-	90%	☆	岔	\bigtriangledown		4900	m 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	^
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		
<																		>

and **Save** it.

Step 3. In the left pane search for it and drag it to the right pane with the button >.

	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 VQoS	; 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 lr	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

	the Cisco Firepower Management C X	+					-		×
←	\rightarrow C \bigcirc \bigcirc A http://www.end/aligned.com/aligned.co	.ps://10.31.124.31	:6005/ddd/#Flexconf	iaPolicvEditor:uuid=000	C2988- 90% 5	☆ <u>호</u>	☑ 🖬 🗰	me	=
A	Setting Started A New Tab REMS	ldentity Services (Engine 🗯 Next Gener	ration Web Regev Te	ester and Deb	Mi vacuna		er Bookm	narks
								. Doolar	lano
Ove	rview Analysis Policies Devices	Objects AM	P Intelligence			Deploy 🔒	System Help 🔻	admi	in v
Dev	ce Management NAT VPN VQ0	S Platform Set	ttings FlexConfig	Certificates					
Fle				Yi	ou have unsaved cha	anges Preview Confi	ig 🔚 Save	🙁 Can	ncel
	o comption						🖳 Policy Assig	gnments	(1)
A	vailable FlexConfig C 🛛 🔾 FlexConfig C	Object 📑	Selected Prepend F	lexConfigs					
		×	•	Name		Description			
	 aaa-server-map disable-am EEM_script_PeriodicLogOffAnyconnect LDAP Idap-attribute-map Management-access management-access-agarciam NAT-T-Disable S25_idle_timeout test 		Selected Append F	lexConfigs					
	UPN-filter		,	Name		Description			
	Default_DNS_Configure	1	s25_i	dle_timeout				۹,	
	 Default_Inspection_Protocol_Disable Default_Inspection_Protocol_Enable DHCPv6_Prefix_Delegation_Configure DHCPv6_Prefix_Delegation_UnConfigure DNS_Configure DNS_UnConfigure Eigrp_Configure Eigrp_Interface_Configure Eigrp_UnConfigure 	re							
Last	ogin on Monday, 2021-07-05 at 16:03:21 PM from 1	0.24.67.117		łow To				،رار، cise	ılı. co

Save the changes and Deploy.

Step 3.1 (Optional) As an intermediate step, after configuration changes have been saved, you could choose **Preview Config** in order to ensure the FlexConfig commands are ready to be pushed at the end of the configuration.

the Cisco Firepower Management C × the Cisco Firepower Management C × +	- 🗆 X
$\leftarrow \rightarrow \mathbb{C} \textcircled{a} \qquad \bigcirc \textcircled{b} \qquad \textcircled{b} \qquad$	
🕀 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 Q Syst	tem Help 🔻 admin 🔻
Device Management NAT VPN VQOS Platform Settings FlexConfig Certificates	
FlexConfig_FTD_B Preview Config	Save 🔀 Cancel
Enter Description Preview FlexConfig ? X	E Bolicy Assignments (1)
Select Device: FTDv_B	Policy Assignments (1)
Available FlexConfig	
Image: State Stat	
Last login on Monday, 2021-07-05 at 16:03:21 PM from 10.24.67.117 How To	սիսիս

Verify

Once deployment is complete, you can run this command in LINA (> system support diagnosticcli) in order to confirm the new configuration is there:

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

Caution: Keep in mind that this change affects all of the S2S VPNs on the FTD. It is NOT a per-tunnel setting but a global one.

Even though the configuration is there, the active tunnel needs to be bounced (**clear crypto ipsec sa peer** <*Remote_Peer_IP_Address>*) so the change takes effect when the tunnel gets established back again. You can confirm that the change is in effect with this command:

```
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
```

Idle Time Out counter must be set to 0 Minutes instead of 30 minutes and the VPN must remain active regardless of the activity/traffic running over it.

Note: At the time of writing, there exists an Enhancement Bug to integrate the ability to modify this setting directly on FMC without the need of Flexconfig. See Cisco bug ID <u>CSCvr82274</u> - ENH: make the vpn-idle-timeout configurable

Troubleshoot

There is currently no specific information to troubleshoot available.

Related Information

- Firepower Management Center Configuration Guide, Version 7.0 Chapter: FlexConfig Policies for Firepower Threat Defense
- Firepower Management Center Configuration Guide, Version 7.0 Chapter: Site-to-Site VPNs for Firepower Threat Defense
- <u>Technical Support & Documentation Cisco Systems</u>