Disabilita timeout di inattività VPN da sito a sito FTD con criteri FlexConfig

Sommario

Introduzione Prerequisiti Requisiti Componenti usati Premesse Configurazione Configura criteri FlexConfig e oggetto FlexConfig Verifica Risoluzione dei problemi Informazioni correlate

Introduzione

In questo documento viene descritto come modificare l'attributo **vpn-idle-timeout** di una VPN con criteri FlexConfig in Cisco Firepower Management Center (FMC) per evitare il downtime del tunnel dovuto a inattività o timeout di inattività.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Firepower Threat Defense (FTD)
- CCP
- Criteri FlexConfig
- Topologie VPN da sito a sito

Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni software:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Le VPN da sito a sito basate su policy (mappa crittografica) di Internet Key Exchange versione 1 (IKEv1) e Internet Key Exchange versione 2 (IKEv2) sono entrambe tunnel su richiesta. Per impostazione predefinita, l'FTD termina la connessione VPN se non vi è attività di comunicazione sul tunnel in un determinato periodo di tempo chiamato **vpn-idle-timeout**. Per impostazione predefinita, questo timer è impostato su 30 minuti.

Configurazione

Configura criteri FlexConfig e oggetto FlexConfig

Passaggio 1. In **Dispositivi > FlexConfig** creare un nuovo criterio FlexConfig (se non ne esiste già uno) e collegarlo all'FTD in cui è configurata la VPN da sito a sito.

disco Firepower Manager	nent C × +		-	- 🗆 ×
$\leftarrow \rightarrow$ C \textcircled{a} O \textcircled{a}	https://10.31.124.31:6005/	Idd/#Flexc 90% 🏠	☆ 🛛 🖬	\$** 💿 ≡
Getting Started () New Tab	🖉 BEMS 🛛 🧐 Identity Services En	gine determine Next Generation	Web >> [Other Bookmarks
Overview Analysis Policies	Devices Objects AMP	Intelligence Deplo	oy 🔍 System I	Help 🔻 admin 🔻
Device Management NAT V	PN ▼ QoS Platform Settin	gs FlexConfig Co	ertificates	
ElayConfig Doligy	Statur	Lact Me	udified	Vew Policy
New Policy	Status	Last MU	amea ?	× D 2 B
Name: FlexCo	onfig_FTD_B			
Description:				
Targeted Devices Select devices to which vo	u want to apply this policy.			
Available Devices	lue Add to Policy	Selected Devices	e Cancel	
Last login on Monday, 2021-07-05 at 16:03	:21 PM from 10.24.67.117	То		،،ا،،،ا،، cisco

tisco Firepower Management C × +	-		- 🗆 ×
\leftarrow \rightarrow C \textcircled{a} \bigcirc \textcircled{b} https://10.	31.124.31:6005/ddd/#Flexc 90%	☆ ☆ ♡	. 41++• 💿 =
💮 Getting Started 💮 New Tab 🖉 BEMS 🧐 I	dentity Services Engine 🛯 👹 Next Ge	neration Web >>>	C Other Bookmarks
Overview Analysis Policies Devices (Objects AMP Intelligence	Deploy 🔒 System	Help 🔻 admin 🔻
Device Management NAT VPN ▼ QoS	Platform Settings FlexConf	ig 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"	Th 🥒 🖬

Passaggio 2. All'interno del criterio, creare un oggetto FlexConfig come segue:

Nome: S2S_Idle_TimeOut Implementazione: Sempre Tipo: Aggiungi

attributi .DefaultS2SGroupPolicy di criteri di gruppo vpn-idle-timeout none



	cisco Firepor	wer Manag	ement C ×	cisco Ci	sco Firepov	wer Mana	gement⊂×	+									-		×
\leftarrow	\rightarrow C G)	0 8	https://1	0.31.124.3	31 :6005/	/ddd/#Flexc	onfigPolicy	yEditor;u	uid=0000	2988-	90%	5	岔	\bigtriangledown	•	470	me	≡
G	etting Started	New Tab	@ BEMS	🧐 Iden	tity Service	s Engine	🗰 Next Ge	eneration W	eb	Regex Te	ster and [Deb	\delta Mi vacı	una		0	🗋 Othe	r Boo	kmarks
Over	rview Analysis	5 Policies	s Devic	es Obj	ects A	MP Int	telligence						Deploy	0 1	System	Hel	p▼ a	admir	· •
Devic	e Add FlexCo	nfig Obje	ect														?	×	
Flex Enter	KC Name:	S2S_1	Idle_TimeOu	t														10	e
	Description:																	nt	s (1)
Av	ail																	H	
	🔬 Сору-р	asting any r	rich text mig	ht introduc	e line break	ks while g	enerating CLI.	Please veri	fy the CLI	before depl	loyment.								п.
1	 Insert 	• 55									De	ploymen	t: Every	time 🗸	Type:	Appe	end 🗸		
	group-p vpn-id	olicy . le-time	.Default sout nor	ts2sGro nel	pupPoli	cy att	ributes											н	
																		Ш	
																		Ш	
																		Ш	
																		н	
1	•																	Ш	
																		Ш	
	Variables																	5	
	Name				Dimensio	on	Default Val	ue	Propert	у (Туре	Overric	le	Descr	ription				ч	
							No rec	ords to	display									Ш	
																		Ш	
														S	ave		Cancel		
Last lo	igin on Honduy, 2021	07 05 01 10.						How Io										cisc	°`∨

e salvatelo.

Passaggio 3. Nel riquadro di sinistra, cercarlo e trascinarlo nel riquadro di destra con il pulsante >.

	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

tisso Firepower Management C × +	- 🗆 ×
$\leftarrow \rightarrow C$ \bigtriangleup https://10.31.124.31:6005/ddd/#FlexconfigPolicyEditor;uuid=000C2988-90% \updownarrow	
🛱 Getting Started 🛱 New Tab 🥖 REMS 🧐 Identity Services Engine 🗯 Next Generation Web 🚬 🗮 Regex Tester and Deb 🖉 Mi vacuna	C Other Bookmarks
Overview Analysis Policies Devices Objects AMP Intelligence Deploy	🦺 System Help 🔻 admin 🔻
Device Management NAT VPN V QoS Platform Settings FlexConfig Certificates	
FlexConfig_FTD_B You have unsaved changes Preview C	Config 📄 Save 🔇 Cancel
	Policy Assignments (1)
Available FlexConfig C Selected Prepend FlexConfigs	
× A * Name Description	
<pre>aaa-server-map disable-am EEEM_script_PeriodicLogOffAnyconnect LDAP Idap-attribute-map Anaagement-access Anaagement-access-agarciam ANAT-F-Disable S2S_idle_timeout S2S_idl</pre>	
VPN-filter # Name Description	
Default DNS Configure 1 S25_idle_timeout	۹. 📋
 Default_Inspection_Protocol_Disable Default_Inspection_Protocol_Enable DHCPv6_Prefix_Delegation_Configure DHCPv6_Prefix_Delegation_UnConfigure DNS_Configure Eigrp_Configure Eigrp_Interface_Configure Eigrp_UnConfigure 	
Last login on Monday, 2021-07-05 at 16:03:21 PM from 10.24.67.117 How To	

Salvare le modifiche e distribuire.

Passaggio 3.1 (Facoltativo) Come passo intermedio, dopo aver salvato le modifiche alla configurazione, è possibile scegliere **Preview Config** per assicurarsi che i comandi FlexConfig siano pronti per essere sottoposti a push al termine della configurazione.

cisco Firepower	Management C × +		- 🗆 X
\leftarrow \rightarrow C \textcircled{a}	🛇 🔓 https://10.31.124.31:6005/ddd/#FlexconfigPolicyEditor;uuid=000C2988-1 90% 🖒	☆ ☆ ♡	
⊕ Getting Started ⊕ Ne	w Tab 🖉 BEMS 🧐 Identity Services Engine 🗰 Next Generation Web 🗮 Regex Tester and Deb 🛞	Mi vacuna	C Other Bookmarks
Overview Analysis I	olicies Devices Objects AMP Intelligence	Deploy 0, Sys	item Help 🔻 admin 🔻
Device Management N	AT VPN VQoS Platform Settings FlexConfig Certificates		
FlexConfig_FTD_	В	Preview Config	Save Sancel
Enter Description	Preview FlexConfig	? ×	Policy Assignments (1)
	Select Device: FTDv_B	~	Policy Assignments (1)
Available FlexConfig			
	<pre>mg mg m</pre>	Close	
Last login on Monday, 2021-07-	S at 16:03:21 PM from 10.24.67.117		սիսիս

Verifica

Al termine della distribuzione, è possibile eseguire questo comando in LINA (> system support diagnostic-cli) per verificare che la nuova configurazione sia presente:

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

Attenzione: Tieni presente che questa modifica interessa tutte le VPN da sito a sito sull'FTD. NON si tratta di un'impostazione per tunnel, bensì globale.

Anche se la configurazione è presente, il tunnel attivo deve essere riavviato (**cancellare ipsec sa peer** <*Indirizzo_Peer_IP_Remoto>*) in modo che la modifica abbia effetto quando il tunnel viene ristabilito. Per verificare che la modifica sia effettiva, usare questo comando:

firepower# show vpn-sessiondb detail 121 filter ipaddress

```
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
```

Il contatore del *timeout di inattività* deve essere impostato su 0 minuti anziché su 30 minuti e la VPN deve rimanere attiva indipendentemente dall'attività/traffico che la sovrasta.

Nota: Al momento della stesura di questo documento, esiste un bug di miglioramento che consente di integrare la possibilità di modificare questa impostazione direttamente su FMC senza la necessità di Flexconfig. Vedere l'ID bug Cisco <u>CSCvr82274</u> - ENH: rendere la vpn-idle-timeout configurabile

Risoluzione dei problemi

Non sono attualmente disponibili informazioni specifiche per la risoluzione dei problemi.

Informazioni correlate

- Guida alla configurazione di Firepower Management Center, versione 7.0 Capitolo: Criteri FlexConfig per Firepower Threat Defense
- <u>Guida alla configurazione di Firepower Management Center, versione 7.0 Capitolo: VPN da</u> <u>sito a sito per Firepower Threat Defense</u>
- <u>Documentazione e supporto tecnico Cisco Systems</u>