Désactiver le délai d'inactivité du VPN site à site FTD avec les stratégies FlexConfig

Contenu

Introduction Conditions préalables Conditions requises Components Used Informations générales Configuration Configurer la stratégie FlexConfig et l'objet FlexConfig Vérification Dépannage Informations connexes

Introduction

Ce document décrit comment modifier l'attribut **vpn-idle-timeout** d'un VPN avec des stratégies FlexConfig dans Cisco Firepower Management Center (FMC) afin d'empêcher les temps d'arrêt du tunnel dus à l'inactivité ou au délai d'inactivité.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Firepower Threat Defense (FTD)
- FMC
- Stratégies FlexConfig
- Topologies VPN site à site

Components Used

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Les VPN de site à site basés sur une stratégie (Crypto map) d'échange de clés Internet version 1 (IKEv1) et de clé Internet version 2 (IKEv2) sont tous deux des tunnels à la demande. Par défaut, le FTD met fin à la connexion VPN s'il n'y a aucune activité de communication sur le tunnel dans une certaine période appelée **vpn-idle-timeout**. Ce compteur est défini sur 30 minutes par défaut.

Configuration

Configurer la stratégie FlexConfig et l'objet FlexConfig

Étape 1. Sous **Devices > FlexConfig**, créez une nouvelle stratégie FlexConfig (si elle n'existe pas déjà) et associez-la au FTD où le VPN site à site est configuré.

	cisco Fire	epower M	anagem	ent C ×	+						-		\times
\leftarrow	\rightarrow C	6	0 8	https://	/10.31.124.31	:6005/ddd/	#Flexc 90	» ۲	2	\bigtriangledown	. 4	ta (100	\equiv
G	etting Started	() New	Tab 🤞	BEMS	ldentity Sen	vices Engine	diste Next O	Generati	on Web		» 🗅 o	ther Book	marks
Over	view Anal	ysis Po	licies	Devices	Objects	AMP In	telligence	De	eploy 🌔	Syst	em Help	🔹 adr	nin 🔻
Devic	e Managemer	nt NAT	T VP	N▼ Q	oS Platforr	m Settings	FlexCor	nfig	Certificat	es			
												New Polic	Y
	Now Dolicy	cy			Status			Last	t Modified		2 X		
	Name:	, 	FlexCo	nfia FTD B	3							40 6/	
	Description:												2 8
	Targeted De	evices			- I - this the							D	8
	Availab Sea P	le Devices arch by nan TDv_B TDv_C	s ne or val	ue	Add	to Policy	elected Dev	rices	Save	Can	cel		
Last lo	ogin on Monday.	2021-07-05	at 16:03:	21 PM from	10.24.67.117	How To						al	ուլը
												CI	sco

Cisco Cisco Firepower Management C X	F		- 🗆 X
\leftarrow \rightarrow C \textcircled{a} \bigcirc \textcircled{b} https://10	0.31.124.31:6005/ddd/#Flex 90%	6 ☆ 塗 ♡	
💮 Getting Started 💮 New Tab 🖉 BEMS 🥘	Identity Services Engine 🜼 Next Ge	eneration Web >>>	C Other Bookmarks
Overview Analysis Policies Devices	Objects AMP Intelligence	Deploy 🔒 System	n 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"	Th 🥒 🖬

Étape 2. Dans cette stratégie, créez un objet FlexConfig comme suit :

Name : S2S_Délai_InactifSortant Déploiement : Partout type : Ajouter

group-policy .DefaultS2SGroupPolicy attributs vpn-idle-timeout none



	cisco (Cisco Firepowe	r Manage	ment C>	< data	Cisco Fir	epower Mar	nagement	CX	+									_		\times
\leftarrow	\rightarrow	C ŵ		0 🔒	https://	/10.31.1	24.31 :600	5/ddd/#I	Flexcon	nfigPolicy	yEditor;	uuid=0000	22988-	90%	ŝ	公	\bigtriangledown		41+++	m 3	≡
€G	etting	Started 🕀 N	lew Tab	@ BEM	S 🍥 Ide	entity Se	rvices Engin	e 👬 Ne	ext Gene	eration W	'eb 🚦	Regex Te	ster and	Deb 🤇) Mi vac	una		C] Othe	r Bool	cmarks
Ove	rview	Analysis	Policies	Devi	ces Ol	bjects	AMP I	ntelliger	nce						Deploy	0 1	System	Hel	p ₹ a	admin	· ^
Devi	e Ad	dd FlexConf	ig Obje	ct															?	×	
FIE: Enter		lame:	S2S_Id	lle_TimeC	out															ic	
Av	D	escription:																		nt	s (1)
		Copy-past	ting any rid	ch text mi	ght introd	luce line t	oreaks while	generatin	ig CLI. Pl	lease veri	fy the CL	I before dep	loyment.							J.	8.
		 Insert • 											D	eployment	: Every	time 🗸	Type:	Appe	end 🗸)	
	• •	group-pol vpn-idls	licy .1	Defaul	tS2SG: ne	roupPo	blicy at	ttribut	tes												
		Variables Name				Dime	ension	Defau	ilt Value	L.	Prope	rty (Type	Overri	ide	Descr	iption					
								No) recor	rds to (display	/									
1	nir									How To						S	ave		Cancel		1.
<	sgin on	Honddy, 2021 07	ob at ron							10										CISC	° _ ~

et enregistrez-le.

Étape 3. Dans le volet gauche, recherchez-le et faites-le glisser vers le volet droit à l'aide du bouton *>*.

	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 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

tisse Cisco Firepower Management C × +	- 🗆	\times
$\leftarrow \rightarrow \mathbb{C}$ \bigtriangleup https://10.31.124.31:6005/ddd/#FlexconfigPolicyEditor;uuid=000C2988-90% \Leftrightarrow $\diamondsuit \mathbb{C}$.	=
🕀 Getting Started 💮 New Tab 🥖 BEMS 🧐 Identity Services Engine 🗰 Next Generation Web 🧮 Regex Tester and Deb 🍥 Mi vacuna	C Other Bookn	narks
Quantieur Applicies Devises Chiesta AMD Intelligence	a Holo = adm	in -
Device Management NAT VIIN - OoC Platform Settings FlavConfin Cartificates	i neip v aun i	
Device Management WAT VPN V QOS Plationin settings Plexcoming Certificates		
FlexConfig_FTD_B	🚽 Save 🛛 🔀 Car	ncel
Enter Description		
	Policy Assignments	(1)
Available FlexConfig C FlexConfig Object Selected Prepend FlexConfigs		
× # Name Description		
		٦.
▲ 🗇 User Defined		
aaa-server-map		
i usdue-an		
Management-arcess		
annangement-access-agarciam		
NAT-T-Disable		
S25_idle_timeout		
Lest Selected Append FlexConfigs		
VPN-filter # Name Description		
▲ 💋 System Defined		
Default_DNS_Configure	<u> </u>	4.
Default_Inspection_Protocol_Disable		
Default_Inspection_Protocol_Enable		
DHCPv6_Prefix_Delegation_Configure		
DHCPv6_Pretx_Delegation_UnConfigure		
Eigrp_conligure		
cyp_oncomyore •		

Enregistrez les modifications et Déployez.

Étape 3.1 (Facultatif) En tant qu'étape intermédiaire, après avoir enregistré les modifications de configuration, vous pouvez choisir **Preview Config** afin de vous assurer que les commandes FlexConfig sont prêtes à être poussées à la fin de la configuration.

the Cisco Firepower Management C × the Cisco Firepower Management C × +	- 🗆 ×
$\leftarrow \rightarrow \mathbb{C}$ \bigtriangleup https://10.31.124.31:6005/ddd/#FlexconfigPolicyEditor;uuid=000C2988- 90% \overleftrightarrow \pounds \heartsuit	
🕀 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 System	em Help 🔻 admin 🔻
Device Management NAT VPN V QoS Platform Settings FlexConfig Certificates	
FlexConfig_FTD_B	Save Save
Enter Description Preview FlexConfig ? X	Policy Assignments (1)
Select Device: FTDv_B	
Available FlexConfig	
<pre> Wuser Defined Goging IIST MANAGER_VPN_EVENT_LIST level debugging dass weebon logging IIST MANAGER_VPN_EVENT_LIST level debugging dass weebon logging IIST MANAGER_VPN_EVENT_LIST level debugging dass usa logging IIST MANAGER_VPN_EVENT_LIST logging IIST MANAG</pre>	4.8
Last login on Monday, 2021-07-05 at 16:03:21 PM from 10.24.67.117 How To	որոր

Vérification

Une fois le déploiement terminé, vous pouvez exécuter cette commande dans LINA (> system support diagnostic-cli) afin de confirmer la nouvelle configuration :

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

Attention : Gardez à l'esprit que cette modification affecte tous les VPN S2S sur le FTD. Il ne s'agit PAS d'un paramètre par tunnel mais d'un paramètre global.

Même si la configuration est présente, le tunnel actif doit être renvoyé (**clear crypto ipsec sa peer** *<Remote_Peer_IP_Address>*) afin que la modification prenne effet lorsque le tunnel est rétabli. Vous pouvez confirmer que la modification est en vigueur avec cette commande :

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
```

Le compteur de temps d'inactivité doit être défini sur 0 minute au lieu de 30 minutes et le VPN doit rester actif indépendamment de l'activité/trafic qui le traverse.

Note: Au moment de l'écriture, il existe un bogue d'amélioration pour intégrer la possibilité de modifier ce paramètre directement sur FMC sans avoir besoin de Flexconfig. Voir l'ID de bogue Cisco <u>CSCvr82274</u> - ENH : rendre le vpn-idle-timeout configurable

Dépannage

Aucune information spécifique n'est actuellement disponible pour le dépannage.

Informations connexes

- Guide de configuration de Firepower Management Center, version 7.0 Chapitre : Stratégies
 FlexConfig pour la défense contre les menaces Firepower
- Guide de configuration de Firepower Management Center, version 7.0 Chapitre : VPN site à site pour la défense contre les menaces Firepower
- Support et documentation techniques Cisco Systems