Supprimer ou modifier la configuration NetFlow à l'aide de Flexconfig

Table des matières

Introduction	
Conditions préalables	
Exigences	
Composants utilisés	
Configuration initiale	
Supprimer les configurations NetFlow	
Modifier les configurations NetFlow existantes	
Documents associés	

Introduction

Ce document décrit comment supprimer ou modifier la configuration NetFlow sur Firepower Threat Defense (FTD) via Firepower Centre de gestion (FMC).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissance du FMC
- Connaissance du DFT
- Connaissance de la politique FlexConfig

Composants utilisés

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

- Version FTD antérieure à 7.4
- Version FMC antérieure à 7.4

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.



Remarque : Remarque importante pour Firepower versions 7.2.x : lors de la configuration de NetFlow, un bogue Cisco connu portant l'ID <u>CSCwh29167</u> est réorganisé dans l'objet Flex, ce qui entraîne l'échec du déploiement en raison de l'absence de configuration de la carte de classe. Pour résoudre ce problème, mettez en oeuvre la solution de contournement documentée sous l'ID de bogue Cisco <u>CSCwh29167</u> (doublon de l'ID de bogue Cisco <u>CSCwh29167</u>).

Configuration initiale

```
access-list flow_export_acl extended permit ip any any
!
class-map flow_export_class
match access-list flow_export_acl
!
policy-map global_policy
class flow_export_class
flow-export event-type flow-create destination 192.168.1.5
```

```
flow-export event-type flow-denied destination 192.168.1.5
flow-export event-type flow-teardown destination 192.168.1.5
flow-export event-type flow-update destination 192.168.1.5
!
```

```
flow-export destination Inside 192.168.1.5 2055
```

Pour configurer ces configurations initiales, les objets flex config utilisés sont les suivants : 1. Objet texte de destination Netflow

Chief Content	Center Overview Analysis	Policies Devices	Objects	Integration		
> AAA Server	Text Object					
> Access List		Edit Text Object			0	
> Address Pools	Text objects define free-form text strings the				•	or be a list of multiple v
Application Filters		Name:				
AS Path	Name	netflow_Destination				
Cipher Suite List		Description:				e
> Community List	netflow_Destination	This variable defines a	single			168.1.5 ;
> Distinguished Name		NetFlow export destination	ition.			
DNS Server Group	netflow_Event_Types	Variable Type			Count	-create -denied
> External Attributes		Multiple		Ŧ	з 🜲	-teardown -update
File List	netflow Parameters					
✓ FlexConfig	netters	1 inside				
FlexConfig Object		2 192.168.1.5				
Text Object		3 2055				
Geolocation						
Interface						
Key Chain						
Network		Allow Overrides				
> ркі						
Policy List		 Override (0) 				
Port						
> Prefix List				Cancel	Save	
Route Map						
> Security Intelligence						

Objet texte de destination Netflow

2. Liste de contrôle d'accès étendue nommée : flow_export_acl

Firewall Managemen	nt Center	Overvie	w Analysis Polic	ties Devices Obj	ects Integration			Deploy	۹ (9
> AAA Server ~ Access List Extended	Extende Edit Exter	e d nded Acc	ess List Object				Add Extende	ed Access	List	
Standard > Address Pools Application Filters AS Path	Name <u>flow_expo</u> Entries (1)	nt_acl								
Cipher Suite List Community List Distinguished Name DNS server Common	Sequence	Action	Source	Source Port Any	Destination Any	Destination Port	Application Any		Add	
DNS Server Group > External Attributes File List ~ FlexConfig		-							-	
FlexConfig Object Text Object Geolocation	Allow O	verrides								
Interface Key Chain Network		_					Can	cel	Save	
> PKI Policy List Port							c	Displaying 1	1 - 2 of :	2 rov

ACL d'exportation de flux

3. Carte de classe et stratégie de service utilisées pour appliquer cette carte de classe avec la destination d'exportation de flux

Cipects / Object Managem	ient Cente	Edit FlexConfig Object						0	େ ୍	🕜 admin 🕶	cinco SECUR
AAA Server Access List Address Paols	FlexCo	Name: Netflow_Event_FlexObject							t Q na	tflow	×
Application Filters AS Path Cipher Suite List	Nam	Create and compute a NetHow export destination.	ntroduce line break	ks while generating CL	. Please verify the	CLI before dapla	ment.	J			
> Community List	Netflo	Insert 🔻 🗄 Deploymen	t: Everytime		• Type:	Append			etFlow expo	ort clestination.	¶∎ Q 🗑
> Distinguished Name	Netflo	class-map flow_export_class						N	etFlow expr	art destination.	· ◎/ ●
DNS Server Group	Netflo	match access-list \$flow_export_a	cl					bi	al settings b	ack to default val	F aq 🗑
External Attributes Cite List	Netflo	<pre>## event-types: any subset of {a policy-map global_policy class flow export class</pre>	11, flow-create	, flow-denied, flow	-teardown, flow	-update)			destination.		R Q 🗑
✓ FlexConfig	Netflo	#foreach (Sevent_type in Snet. flow-export event-type Sevent_ Hend	flow_Event_Type type_destination	s) n \$netflow_Destinat	ion.get(1)				destination.		5×1
FlexConfig Object	Netflo	1000						N	etFlow expt	prt cleatination.	后之来
Text Object Geolocation	Netflo							0	r NetFlow ea	iport.	n <u>a</u> Q ≣
Intertace Kau Chain		▼ Variables									
Network		Name	Dimension	Default Value	Property (Type:Name)	Override	Description				
> ркі		netflow_Event_Types	MULTIPLE	[all, flow-create,	FREEFORM:	false	This variable provides the glo				
Policy List		netflow_Destination	MULTIPLE	[inside, 192.168	FREEFORM:	false	This variable defines a single	. 1			
Port		flow_export_acl	SINGLE	flow_export_aci	EXD_ACL:fl	false					
> Prefix List											
Route Map									of 7 rows	I< < Page 1	of 1 > > C

Carte de classe et politique de service

4. Destination d'exportation de flux

Firewall Management Center	Edit FlexConfig Object						0	ኢ 💕 🔅 🔞 admin 🔹 🗧	SECUR
AAA Server Flex Access List Address Pools Application Filters Access	Name: Netflow_Add_Destination_Copy Description: Create and configure a NetFlow export destination.							ict 🔍 netflaw	×
AS Path Nam Cipher Suite List Netfic Community List	Copy-pasting any rich text might int Insert Deployment	roduce line break	s while generating CLI.	Please verify the Type:	CLI before deploy Append	ment.		NetFlow export destination.	¶a Q. ⊕
Distinguished Name Netfic DNS Server Group Netfic External Attributes	₩ destination: interface_nameif flow-export destination Snetflow_	destination_ip Destination.get	udp_port (0) Spetflow_Destin	ation.get(1) 5	netflow_Destinat	tion.get(2)		NetFlow export destination.	19/1 19 Q ()
File List Nettor V FlexConfig Netfor ElexConfig Object Direct								n destination.	
Text Object Netfic Geolocation								NetFlow export destination.	% × ¥ ¶a Q ⊕
Interface Key Chain Network	♥ Variables Name	Dimension	Default Value	Property (Type:Name)	Override	Description			
> PKI Policy List	netflow_Destination	MULTIPLE	[inside, 192.168	FREEFORM:	false	This variable defines a single .			
Port > Prefix List Route Map									
							-	7 of 7 rows < < Page 1	of 1 > > C

Destination d'exportation de flux

5. Ensuite, ces deux objets ont été ajoutés à la stratégie de configuration flexible et déployés :

Firewall Management Center Devices / Flexconfig Policy Editor	(Overview	Analysis	Policies	Devices	Objects	Integration		Deploy	۹ (°	🕜 admin 🕶	aludu cisco	SECUR
FTD01-FP Enter Description											Preview	v Config	eve	Cance
												Polic	y Assign	ments (1
		"à Selecte	d Prepend F	lexConfigs										
Available FlexConfig C FlexConfig Object		# Nam	ne			Description								
V User Defined														
"P AAAdummy														
"à EEM-Script								Salact	ted Prepard	HacConfig	16			
" EEM-Script-Removal								00100	ted repend	- Hakoonini,				
"à flow_export_class														
" Netflow_Add_Destination_Copy														
		B. Calcate	d American II	les Confere										
" Netflow_Event_FlexObject		"à Pelecte	a Appena F	lexconfigs										
✓ System Defined		# Nam	ne			Description								
"à Default_DNS_Configure		1 Netf	low_Add_Dest	ination_Copy		Create and con	figure a NetFlow export destination.							۹. 🗑
" Default_Inspection_Protocol_Disable		2 Netf	low_Event_Flex	xObject		Create and con	figure a NetFlow export destination.							् 🗑
"- DHCRid Resty Delegation Contains														
- DHCP/6 Prefx Delegation UnConfigure														
"à DNS Configure														
.9 DNS_UnConfigure														

Politique FlexConfig

Supprimer les configurations NetFlow

Étape 1 : Supprimez les objets Flex de la stratégie Flex.

Firewall Management Center Devices / Flexconflg Policy Editor	Overview Ana	Ilysis Policies	Devices Objects	Integration		Deploy	Q 🔗 (🔅 🞯 admin 🕶	cinco SECUR
FTD01-FP							Prev	iew Config S	ave Cance
Line sourcemparent								Policy	y Assignments (1
	"à Selected Pre	pend FlexConfigs							
Available FlexConfig C FlexConfig Object	# Name		Description						
V User Defined									
JE AAAdummy									
"à EEM-Script									
all EEM-Script-Removal									
"à flow_export_class									
"à Netflow_Add_Destination_Copy									
	E Colomad Ann								
"à Netflow_Event_FlexObject	"y Selected App	bend FlexConfigs							
✓ System Defined	# Name		Description						
"à Default_DNS_Configure									
of Default_Inspection_Protocol_Disable									
" Default_Inspection_Protocol_Enable									
"å DHCPv6_Prefx_Delegation_Configure									
DHCPv6_Prefx_Delegation_UnConfigure									
"à DNS_Configure					Selected Append FlexConfigs				
.9 DNS_UnConfigure									

Supprimer la configuration flexible existante

Étape 2 : Déployez la stratégie. À partir de la ligne de commande, nous constatons que les configurations supprimées sont les suivantes :

```
access-list flow_export_acl extended permit ip any any
!
class-map flow_export_class
match access-list flow_export_acl
!
policy-map global_policy
class flow_export_class
flow-export event-type flow-create destination 192.168.1.5
flow-export event-type flow-denied destination 192.168.1.5
flow-export event-type flow-teardown destination 192.168.1.5
flow-export event-type flow-update destination 192.168.1.5
```

considérant que la configuration qui n'est pas supprimée est :

flow-export destination Inside 192.168.1.5 2055

Étape 3 : Pour supprimer ce, nous devons créer un objet flexible avec le type 'prepend' et l'ajout de la configuration :

Firewall Management Center Objects / Object Management	Edit FlexConfig Object	9
> AAA Server Flex	Name:	
Address Pools Application Filters AS Path		
Cipher Suite List AAAd	Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.	
Distinguished Name DNS Server Group Defau	no flow-export destination Inside 192.168.1.5 2055	
External Attributes Defau File List		
FlexConfig Object DHCP Text Object		
Geolocation DNS_		

Supprimer la destination de configuration flexible

Étape 4 : sous Flex Policy, appelez l'objet prepend nouvellement créé à l'étape 3 et déployez la stratégie.

Firewall Management Center Devices / Flexconing Policy Editor	Overview	Analysis Poli	icies Devices	Objects	Integration		Deploy	Q 💞	🗘 🙆 admi	n • deale SECURE
FTD01-FP Enter Description								Pres	view Config	Sove Cancel
Available FlexConfig	"à Selecte	d Prepend FlexCo	nfigs							
×	# Nam	ю		Description						
	1 AAA	dummy								0,1
User Denned										
*a EEM-Script										
39 EEM-Script-Removal										
"å flow_export_class										
"å Netflow_Add_Destination_Copy										
"Netflow_Delete_Destination_Copy		d Append FlexCor	nfigs							
✓ System Defined	# Nam	e		Description						
a Default_DNS_Configure										
"à Default_Inspection_Protocol_Enable										

Ajoutez ceci sous la politique de configuration flexible

Étape 5 : supprimez cet objet de préfixe de la stratégie Flex et redéployez-le.

Firewall Management Center Devices / Flexconing Policy Editor	Overview A	nalysis Policies	Devices Objects	Integration		Deploy Q 🚱 🛱 (admin • dedb SECURE
FTD01-FP Enter Description						Preview C	Policy Assignments (1)
Available FlexConfig C FlexConfig Object	°∎ Selected Pr # Name	epend FlexConfigs	Description				
V User Defined							
3 EEM-Script 과 EEM-Script-Removal							
*3 flow_export_class *3 Netflow_Add_Destination_Copy							
** Netflow_Deeters_Destination_copy *** Netflow_Event_FlexObject		opend FlexConfigs	Description				
"a Default_DNS_Configure 						Endenford	
"à Default_Inspection_Protocol_Enable					Selected Append	Hexuchigs	

Supprimer l'objet de préfixe

Toute la configuration liée à l'exportation de flux est supprimée maintenant.

Modifier les configurations NetFlow existantes

Étape 1 : Modifiez l'objet Text créé pour la destination Netflow. Modifiez les paramètres requis IP, Interface name ou Port.

Exemple : nous avons modifié l'adresse IP et le port de (192.168.1.5, 2055) à (192.168.1.78, 2056)



Objet texte de destination Netflow

Étape 2 : Déployez la stratégie. Vous verriez que les modifications sont reflétées comme prévu, mais avec l'ancienne configuration de destination Netflow :

```
access-list flow_export_acl extended permit ip any any
!
class-map flow_export_class
match access-list flow_export_acl
!
policy-map global_policy
class flow_export_class
flow-export event-type flow-create destination 192.168.1.78
flow-export event-type flow-denied destination 192.168.1.78
flow-export event-type flow-teardown destination 192.168.1.78
flow-export event-type flow-update destination 192.168.1.78
!
flow-export destination Inside 192.168.1.78 2056
flow-export destination Inside 192.168.1.5 2055
```

Étape 3 : Pour supprimer ce, vous devez créer un objet flexible avec le type 'prepend' et l'ajout de la configuration :

Collects / Objects / Object Management	Edit FlexConfig Object
 > AAA Server > Access List > Address Pools Application Filters AS Path Cipher Suite List > Community List > Distinguished Name 	Name: AAAdummy Description: Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment. Insert Deployment: Once Type: Prepend
DNS Server Group Defa > External Attributes Defa File List Defa FlexConfig DHC 	
Interface	▼ Variables
Key Chain EEM Network EEM	Name Dimension Default Value Property (Type:Name) Override Description
Policy List Eigrp Port Eigrp > Prefix List Eigrp	
Noute Map Security Intelligence	Cancel

Supprimer la destination Netflow

Étape 4 : sous Flex Policy, appelez l'objet prepend nouvellement créé à l'étape 3 et déployez la stratégie.

Firewall Management Center Devices / Flexconfig Policy Editor	Coverview Analysis Policies Devices Objects Integration	Deploy Q 🥝 🔅 🕲 admin 🖲 🖏 SECURE
FTD01-FP		Preview Config Sove Cancel
Enter Description		Policy Assignments (1)
	C Selected Prepend FlexConfigs	
Available FlexConing C FlexConing Object	# Name Description	
V User Defined	1 AAAdummy	٩.
JI AAAdummy		
"à EEM-Script		
.9 EEM-Script-Removal		
"à flow_export_class		
a Netflow_Add_Destination_Copy		
. Netflow_Delete_Destination_Copy		Selected Prepend FlexConfigs
*a Netflow_Event_FlexObject	Es cenered Abbenet rescontige	
✓ System Defined	# Name Description	
"è Default_DNS_Configure	1 Netflow_Add_Destination_Copy Create and configure a NetFlow export destination.	् च
.9 Default_Inspection_Protocol_Disable	2 Netflow_Event_FlexObject Create and configure a NetFlow export destination.	۵. 🖥
Desurt_inspection_Protocol_Enable		
BDHCPv6_Prenx_Delegation_Conngure		
3 DNS Configure		
-T DNS UnConfigure		

Ajouter au début Flex Config

Étape 5 : supprimez cet objet de préfixe de la stratégie Flex et redéployez-le.

Firewall Management Center Devices / Flexconfig Policy Editor	Cverview Analysis Policies Devices Objects Integration Da	sploy 🔍 🥝 🔅 🕲 admin 🖲 🐝 SECURE
FTD01-FP Enter Description		Preview Config Sove Cancel
		Policy Assignments (1)
	Selected Prepend FlexConfigs	
Available FlexConfig C FlexConfig Object	# Name Description	
^		
✓ User Defined		
JI AAAdummy		
"à EEM-Script		Selected Presend FlexConflas
₀9 EEM-Script-Removal		
"à flow_export_class		
Netflow_Add_Destination_Copy		
" Netflow_Delete_Destination_Copy		
*a Netflow_Event_FlexObject	Selected Append FlexConfigs	
✓ System Defined	# Name Description	
"à Default_DNS_Configure	1 Netflow_Add_Destination_Copy Create and configure a NetFlow export destination.	् 🗑
B Default_Inspection_Protocol_Disable	2 Netflow Event FlexObject Create and configure a NetFlow export destination.	9.
"2 Default_Inspection_Protocol_Enable		
The DHCPv6_Prefix_Delegation_Configure		
DHCPv6_Prefix_Delegation_UnConfigure		
"à DNS_Configure		
" DNS_UnConfigure		

Suppression de Prepend FlexConfig

La configuration liée à NetFlow a été modifiée.

access-list flow_export_acl extended permit ip any any
!
flow-export destination Inside 192.168.1.78 2056
!
class-map flow_export_class
match access-list flow_export_acl
!
policy-map global_policy
class flow_export_class
flow-export event-type flow-create destination 192.168.1.78
flow-export event-type flow-denied destination 192.168.1.78
flow-export event-type flow-teardown destination 192.168.1.78
flow-export event-type flow-update destination 192.168.1.78

Documents associés

https://www.cisco.com/c/en/us/support/docs/quality-of-service-qos/netflow/216126-configurenetflow-secure-event-logging-o.html

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.