Remover ou modificar a configuração do NetFlow usando o Flexconfig

Contents

Introdução	
Pré-requisitos	
Requisitos	
Componentes Utilizados	
Configuração inicial	
Remover configurações do NetFlow	
Modificar as configurações do NetFlow existentes	
Documentos relacionados	

Introdução

Este documento descreve como remover ou modificar a configuração do NetFlow no Firepower Threat Defense (FTD) através do Firepower Centro de Gestão do Tráfego Aéreo (CVP).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento do CVP
- Conhecimento de FTD
- Conhecimento da política FlexConfig

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Versão do FTD anterior à 7.4
- Versão do CVP inferior a 7.4

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.



Observação: observação importante para o Firepower versões 7.2.x: ao configurar o NetFlow, há um bug da Cisco ID <u>CSCwh29167</u> em que o objeto Flex é reorganizado, fazendo com que a implantação falhe devido à não configuração do mapa de classes. Para resolver esse problema, implemente a solução documentada sob o bug da Cisco ID <u>CSCwf9848</u> (duplicata do bug da Cisco ID <u>CSCwh29167</u>).

Configuração inicial

```
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
```

Para configurar essas configurações iniciais, os objetos flex config usados são: 1. Objeto de texto de destino do Netflow



Objeto de Texto de Destino do Netflow

2. ACL estendida chamada: flow_export_acl

Firewall Managemer	nt Center	Overvie	w Analysis Polic	ies Devices Obj	ects Integration		Ľ	Deploy Q 🕑	
> AAA Server Access List Extended 	Extende Edit Exter	ed nded Acc	ess List Object				Add Extende	d Access List	a
Standard > Address Pools Application Filters AS Path	Name flow_expo Entries (1)	nt_acl							
Cipher Suite List > Community List > Distinguished Name DNS Server Group	Sequence	Action	Source Any	Source Port Any	Destination Any	Destination Port	Application Any	Add	
 External Attributes File List FlexConfig FlexConfig Object Text Object Geolocation 	Allow O	verrides							
Interface Kay Chain Network > PKI Policy List Port							Cano	splaying 1 - 2 of 2 r	TOW

ACL de exportação de fluxo

3. Mapeamento de classe e política de serviço usados para aplicar esse mapa de classe com destino de exportação de fluxo

Cipects / Object Managem	ent Cente	Edit FlexConfig Object						0	. 0	• •	🕽 admin 🕶	ciaco SECU	R
AAA Server Access List Address Pools Application Filters To put	Flex	Name: Netflow_Event_FlexQbject Description: Create and configure a NetFlow export destination.							ict C	t netflo	w	×	x
As Path Cipher Suite List	Nam	Copy-pasting any rich text might in Insert E Deployment	troduce line break	ks while generating CL	. Please verify the Type:	CLI before deplo	yment.		NetFlow	export o	destination.	™ ⊂ †	
> Distinguished Name	Netflo	class-map flow export class							NetFlow	export o	destination.	后人家	
DNS Server Group	Netflo	match access-list \$flow_export_ac	:1						bal settin	gs back	to default va		
External Attributes File List	Netfio	<pre>## event-types: any subset of (al policy-map global_policy class flow event class</pre>	1, flow-create,	, flow-denied, flow	-teardown, flow-	-update)			t clestina	tion.		1 ∎ Q ₹	
✓ FlexConfig	Netfio	<pre>#foreach (Sevent_type in Snets flow-export event-type Sevent_t #end</pre>	low_Event_Type ype destination	s) n \$netflow_Destinat	ion.get(1)				t destina	tion.		5/1	i
FlexConfig Object	Netflo								NetFlow	export o	destination.	5/1	
Text Object Geolocation	Netflo								or NetFlo	w expor	ıt.	¶∎ Q ()	
Interface Key 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						
Port		flow_export_acl	SINGLE	flow_export_acl	EXD_ACL:fl	false							
> Prefix List													
Route Map								_	7 of 7 ro	ws K	< Page 1	of 1 > > (c

Mapa de classe e política de serviço

4. Destino da exportação do fluxo

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.	19/10 19 0 0
File List Netto								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

Destino da exportação de fluxo

5. Em seguida, adicionou estes dois objetos na política de configuração flexível e implantou:

Firewall Management Center	c	Jverview	Analysis	Policies	Devices	Objects	Integration		Deploy	۹ 🕯	°	🛛 admin •	aludo cisco	SECUR
FTD01-FP Enter Description											Preview	Config	iave	Cance
												POIIC	y Assign	iments (1
		6 Selecter	d Prepend F	lexConfigs										
Available FlexConfig C FlexConfig Object		# Nam	10			Description								
V User Defined														
a EEM-Script								Sale	acted Prepend	lesConfic	16			
								- Cont	octed i repene	Taxoonni,				
"à flow_export_class														
Netflow_Add_Destination_Copy														
" Plete_Destination_Copy														
" Netflow_Event_FlexObject		" Selected	d Append H	lexConfigs										
✓ System Defined		# Nam	0			Description								
"à Default_DNS_Configure		1 Netfl	ow_Add_Desti	ination_Copy		Create and con	figure a NetFlow export destination.	L.						۹. 🗑
" ³ Default_Inspection_Protocol_Disable ³ Default_Inspection_Protocol_Enable		2 Netfi	cw_Event_Flex	cObject		Create and con	figure a NetFlow export destination.	h.						۹.2
** DHCPuS Prefy Delegation Configure														
- DHCPv6 Prefx Delegation UnConfigure														
"à DNS Configure														
- 7 DNS UnConfigure														



Remover configurações do NetFlow

Etapa 1: Exclua os objetos flex da política flex.

Firewall Management Center Devices / Flexconfig Policy Editor	Overview Analy	is Policies	Devices	Objects	Integration		Deploy	Q	େ 🍄	🕲 admin 🔻	ence SECUR
FTD01-FP									Preview	Config	eve Cance
										Policy	y Assignments (1
	"à Selected Prepe	nd FlexConfigs									
Available FlexConfig C FlexConfig Object	# Name		D	Description							
V User Defined											
JE AAAdummy											
"à EEM-Script											
"9 EEM-Script-Removal											
"à flow_export_class											
"a Netflow_Add_Destination_Copy											
" Netflow_Delete_Destination_Copy	R Coloriad Arms	d FlauCaafaa									
"à Netflow_Event_FlexObject	"7 Selected Appe	id PlexConfigs									
✓ System Defined	# Name		D	Description							
"à Default_DNS_Configure											
5 Default_Inspection_Protocol_Disable											
"å Default_Inspection_Protocol_Enable											
** DHCPv6_Prefx_Delegation_Configure											
7 DHCPv6_Prefx_Delegation_UnConfigure						Related toward Electronics					
"à DNS_Configure						Selected Append FlexConfigs					
"9 DNS_UnConfigure											

Excluir flexconfig existente

Etapa 2: Implante a política. Na linha de comando, veríamos que as configurações removidas são:

```
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
```

Considerando que a configuração que não é removida é:

flow-export destination Inside 192.168.1.5 2055

Etapa 3: Para remover isso, precisamos criar um objeto flex com o Tipo 'prepend' e adicionar a configuração:

Chievell Management	t Cente	Edit FlexConfig Object	9
> AAA Server > Access List	Flex	Name: AAAdummy	
> Address Pools	FlexCc	Description:	
Application Filters			
AS Path	Name	Consumption any rich text might introduce line breaks while generation CLL Diages varify the CLL before devicement	
Cipher Suite List	AAAd	Copy pasting any nen text might included into breaks while generating dear mease very the dear before deproyment.	
> Community List		Insert v E Deployment: Once v Type: Prepend v	
> Distinguished Name	Defau	no flow-export destination Inside 192.168.1.5 2055	
DNS Server Group	Defau		
> External Attributes	Defeu		
File List	Derau		
✓ FlexConfig	DHCP		
FlexConfig Object	DHCP		
Text Object			
Geolocation	DNS_		

Excluir destino de configuração flexível

Etapa 4: em política flex, chame o objeto prefixo recém-criado na Etapa 3 e implante a política.

Firewall Management Center Devices / Flexconfig Policy Editor	С	Verview	Analysis	Policies	Devices	Objects	Integration		Deploy	a 🕜	¢ (admin 🔹	altalta cisco	SECURE
FTD01-FP Enter Description										Pr	eview C	onfig S	ove y Assign	Cancel ments (1)
		i Selecte	d Prepend F	lexConfigs										
Available FlexConfig C FlexConfig Object		# Nam	ve			Description								
^		1 AAA	dummy											۹.
- User Denned														
"à EEM-Script														
₀∄ EEM-Script-Removal														
"å flow_export_class														
"à Netflow_Add_Destination_Copy														
Netflow_Delete_Destination_Copy Netflow_Except Electronic		Selecte	d Append Fl	exConfigs										
System Defined		# Narr	ie.			Description								
a Default_DNS_Configure														
□ □ □ □ □ □ □ □ □ □ □ □														
*à Default_Inspection_Protocol_Enable														

Adicione isso na política de configuração flexível

Etapa 5: Exclua esse objeto de prefixo da política flex e implante novamente.

Firewall Management Center Devices / Flexconing Policy Editor		Overview	Analysis	Policies	Devices	Objects	Integration		Deploy	۹ (¢ 💡	🔕 admir	• alual cisco	SECURE
FTD01-FP Enter Description											Preview	Config	Save	Cancel
Available FlexConfig 😋 🛛 FlexConfig Object	Į	°i Selecti # Nat	ad Prepend F	lexConfigs		Description								
V User Defined														
្លាវ AAAdummy ារ EEM-Script ្ទា EEM-Script-Removal														
"à flow_export_class "à Netflow_Add_Destination_Copy														
-9 Netflow_Delete_Destination_Copy To Netflow_Event_FlexObject			ed Append F	lexConfigs										
 System Defined Bafault, DNS, Configure 		# Nar	me			Description								
"Default_Inspection_Protocol_Disable								Selected Append	FlexConfigs					

Excluir o objeto precedente

Toda a configuração relacionada à exportação de fluxo é removida agora.

Modificar as configurações do NetFlow existentes

Etapa 1: edite o objeto Texto criado para o destino do Netflow. Altere os parâmetros necessários: IP, nome da interface ou Porta.

Exemplo: alteramos o IP e a porta de (192.168.1.5, 2055) para (192.168.1.78, 2056)

Firewall Management	nt Center Overview Analysis	Policies Devices Objects	Integration	
> AAA Server	Text Object			
> Access List	Text objects define free-form text strings the	Edit Text Object	0	or be a list of multiple v
> Address Pools	rext objects denne nee-torri text sungs un			or be a nation multiple v
Application Filters		Name:		
AS Path	Name	netflow_Destination		
Cipher Suite List	notflow Doctination	Description:		e 169 1 70
> Community List	hellow_besthaton	This variable defines a single		3
> Distinguished Name		NetFlow export destination.		create
DNS Server Group	netflow_Event_Types	Variable Type	Count	-denied
> External Attributes		Multiple	▼ 3 ♣	-update
File List	netflow. Parameters			
✓ FlexConfig		1 inside		
FlexConfig Object		2 192.168.1.78		
Text Object		3 2056		
Geolocation				
Interface				
Key Chain				
Network				
> ркі		Allow Overrides		
Policy List		 Override (0) 		
Port				
> Prefix List			Cancel Save	
Route Map				
> Security Intelligence				

Objeto de texto de destino do Netflow

Etapa 2: Implante a política. Você verá que as alterações são refletidas como esperado, mas junto com a antiga configuração de destino do 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
```

Etapa 3: Para remover isso, você precisa criar um objeto flex com o Tipo 'prepend' e adicionar a configuração:

Firewall Management Cente Objects / Object Management	Edit FlexConfig Object					
> AAA Server Flex	Name: AAAdummy					
Address bat Address Pools Application Filters AS Path	Description:					
Cipher Suite List	Copy-pasting any rich text might int	roduce line breaks	while generating CLI.	Type:	CLI before deployn	nent.
Distinguished Name Defau DNS Secure Crown	no flow-export destination Inside	192.168.1.5 20	55			
External Attributes Defau						
✓ FlexConfig DHCP ElexConfig DHcP						
Text Object DNS_ Geolocation						
Interface DNS_	 Variables 					
Network	Name	Dimension	Default Value	Property (Type:Name)	Override	Description
> PKI Policy List Eigrp.			No records to dis	play		
Port Eigrp_ > Prefix List						
Route Map Security Intelligence						Cancel

Excluir destino do netflow

Etapa 4: em política flex, chame o objeto prefixo recém-criado na Etapa 3 e implante a política.

Firewall Management Center Devices / Flexconfig Policy Editor	Dverview	Analysis	Policies	Devices	Objects	Integration		Deploy	Q 📀	¢	🙆 sdmin 🕶	-di-di- cisco	SECURE
FTD01-FP Enter Description									P	eview	Config	Sove cy Assign	Cancel
	ී Selecte	ed Prepend F	lexConfigs										
Available FlexConfig C FlexConfig Object	# Nan	ne			Description								
V User Defined	1 AAA	Adummy											۹.
_9 AAAdummy													
"a EEM-Script													
.9 EEM-Script-Removal													
"à flow_export_class													
"& Netflow_Add_Destination_Copy													
" Netflow_Delete_Destination_Copy Netflow_Event_FlexObject	. ^g Selecte	d Append Fl	exConfigs								Selecte	d Prepend	d FlexConfigs
✓ System Defined	# Nan	ne			Description								
*** Default_DNS_Configure	1 Netf	Now_Add_Desti	nation_Copy		Create and con	figure a NetFlow export destinat	tion.						۹. 🗑
Default_Inspection_Protocol_Disable Default_Inspection_Protocol_Enable	2 Net	flow_Event_Flex	Object		Create and con	figure a NetFlow export destinat	tion.						۹.
** DHCPv6_Prefix_Delegation_Configure													
"à DNS_Configure													
.9 DNS_UnConfigure													

Etapa 5: Exclua esse objeto de prefixo da política flex e implante novamente.

Firewall Management Center Devices / Flexconfig Policy Editor	31 Overview Analysis Policies Devices Objects Integration Deplo	y Q 🙋 🔅 🞯 admin 🕶 🔤 SECURE
FTD01-FP		Preview Config Seve Cancel
Enter Description		Policy Assignments (1)
	Selected Prepend FlexConfigs	
Available FlexConfig C FlexConfig Object	# Name Description	
×	<	
✓ User Defined		
.ª AAAdummy		
"à EEM-Script		Selected Present ElexConflas
"9 EEM-Script-Removal		
"à flow_export_class		
"a Netflow_Add_Destination_Copy		
" Netflow_Delete_Destination_Copy	8 Selected Annext ElevPontice	
Netflow_Event_FlexObject	as selected Append Flexcollings	
✓ System Defined	# Name Description	
"è Default_DNS_Configure	1 Netflow_Add_Destination_Copy Create and configure a NetFlow expert destination.	् 🗑
	2 Netflow_Event_FlexObject Create and configure a NetFlow export destination.	٩.
"à Default_Inspection_Protocol_Enable		
*a DHCPv6_Prefix_Delegation_Configure		
.9 DHCPv6_Prefix_Delegation_UnConfigure		
"à DNS_Configure		
" DNS_UnConfigure		

Excluir o prefixo FlexConfig

A configuração relacionada ao NetFlow foi modificada com êxito.

```
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
```

Documentos relacionados

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

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.