Configuración del registro de eventos seguro de NetFlow en Firepower Threat Defence

Contenido

Introducción Prerequisites Requirements Componentes Utilizados Antecedentes Configurar Verificación Información Relacionada

Introducción

Este documento describe cómo configurar NetFlow Secure Event Logging (NSEL) en Firepower Threat Defense (FTD) a través de Firepower Management Center (FMC).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento del CSP
- Conocimiento de FTD
- Conocimiento de la política FlexConfig

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- FTD versión 6.6.1
- FMC versión 6.6.1

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Este documento describe cómo configurar NetFlow Secure Event Logging (NSEL) en Firepower Threat Defense (FTD) a través de Firepower Management Center (FMC).

Los objetos de texto FlexConfig están asociados a variables utilizadas en los objetos FlexConfig predefinidos. Los objetos FlexConfig predefinidos y los objetos de texto asociados se encuentran en FMC para configurar NSEL. Hay cuatro objetos FlexConfig predefinidos en el FMC y tres objetos de texto predefinidos. Los objetos FlexConfig predefinidos son de solo lectura y no se pueden modificar. Para modificar los parámetros de NetFlow, se pueden copiar los objetos.

En la tabla se enumeran los cuatro objetos predefinidos:

FlexConfig Object Name	Description
Netflow_Add_Destination	Creates and configures a NetFlow export destination
Netflow_Set_Parameters	Sets globla parameters for NetFlow export
Netflow_Delete_Destinations	Deletes a NetFlow export destination
Netwflow_Clear_Parameters	Restores Netflow export global default settings

En la tabla se enumeran los tres objetos de texto predefinidos:

Text Object Name	Description
netflow_Destination	Define the single NetFlow export destination's interface, destination IP address and UDP port number for NetFlow.
netwflow_Event_Types	Define NetFlow events based on event type
netflow_Parameters	Define values for active refresh-interval, delay flow-create and template timeout-rate.

Configurar

En esta sección se describe cómo configurar NSEL en FMC mediante una política FlexConfig.

Paso 1. Establezca los parámetros de los objetos de texto para Netflow.

Para establecer los parámetros de variable, navegue hasta **Objetos > FlexConfig > Objetos de texto**. Edite el objeto netflow_Destination. Defina el tipo de variable múltiple y el recuento establecido en 3. Establezca el nombre de la interfaz, la dirección IP de destino y el puerto.

En este ejemplo de configuración, la interfaz es DMZ, la dirección IP del colector de NetFlow es 10.20.20.1 y el puerto UDP es 2055.

Edit Text Object

Name:

netflow_Destination

Description:

This variable defines a single NetFlow export destination.

Variable Type

Multiple	•
----------	---



10.20.20.1
2055
1

Nota: Se utilizan los valores predeterminados para netflow_Event_Types y netflow_Parameters.

Paso 2. Configure un objeto de lista de acceso ampliado para que coincida con el tráfico específico.

Para crear una lista de acceso ampliada en FMC, navegue hasta **Objetos > Gestión de objetos** y en el menú de la izquierda, debajo de **Lista de acceso** seleccionar **Ampliado.**Haga clic en **Agregar lista de acceso ampliada.**

Rellene el campo **Nombre**. En este ejemplo, el nombre es flow_export_acl. 'Haga clic en el botón Add (Agregar).' Configure las entradas **de control de acceso** para que coincidan con el tráfico específico.

En este ejemplo, se excluye el tráfico del host 10.10.10.1 a cualquier destino y el tráfico entre el host 172.16.0.20 y 192.168.1.20. Se incluye cualquier otro tráfico.

?

Name flow_export	t_acl					
Entries (3)						
						Add
Sequence	Action	Source	Source Port	Destination	Destination Port	
1	Block	10.10.10.1	Any	Any	Any	/ 1
2	Block	172.16.0.20	Any	192.168.1.20	Any	/ 1
3 Allow Ove	Allow	Any	Any	Any	Any	/ 🗑
						Cancel Save

Paso 3. Configure un objeto FlexConfig.

Para configurar los objetos de FlexConfig, navegue hasta **Objetos > FlexConfig > Objetos de FlexConfig** y haga clic en el botón **Agregar objeto de FlexConfig**.

Defina el mapa de clase que identifica el tráfico para el que se deben exportar los eventos de NetFlow. En este ejemplo, el nombre del objeto es flow_export_class.

Seleccione la lista de acceso creada en el paso 2. Haga clic en Insert > Insert Policy Object > Extended ACL Object y asigne un nombre. A continuación, haga clic en el botón Add. En este ejemplo, el nombre de la variable es flow_export_acl. Click Save.

Variable Name:				
flow_export_acl				
Description:				
Available Objects C			Selected Object	
Q Search	\times		flow_export_acl	Ì
flow_export_acl				
	[Add		

Cancel Save	Cancel

Agregue las siguientes líneas de configuración en el campo en blanco a la derecha e incluya la variable previamente definida (**\$flow_export_acl.**) en la línea de configuración de match access-list.

Observe que un **\$** símbolo comienza el nombre de la variable. Esto ayuda a definir que una variable viene después de ella.

class-map flow_export_class match access-list **\$flow_export_acl** Haga clic en **Guardar** cuando haya terminado. 2

Edit FlexConfig Object

Name:							
flow_export_class							
Description:							
A Copy-pasting any rich	text might intro	duce line break	s while generating Cl	.I. Please ve	rify the	CLI before deploy	ment.
Insert 🗸 🔣	Deployment:	Everytime		Type:	Apper	nd	v
class-map flow_exp match access-list	port_class \$flow expo	rt acl					
- Variables							
Name		Dimension	Default Value	Propert (Type:N	y ame)	Override	Description
flow_export_class		SINGLE	flow_export_acl	EXD_A	CL:fl	false	
							Cancel
							Cancer Save

Paso 4. Configuración del destino de Netflow

Para configurar el destino de Netflow, navegue hasta **Objetos > FlexConfig > Objetos de FlexConfig** y filtre por Netflow. **Copie** el objeto Netflow_Add_Destination. Se crea Netflow_Add_Destination_Copy.

Asigne la clase creada en el paso 3. Puede crear un nuevo policy map para aplicar las acciones de exportación de flujo a las clases definidas.

En este ejemplo, la clase se inserta en la directiva actual (directiva global).

```
## destination: interface_nameif destination_ip udp_port
## event-types: any subset of {all, flow-create, flow-denied, flow-teardown, flow-update}
flow-
export destination $netflow_Destination.get(0) $netflow_Destination.get(1) $netflow_Destination.
get(2)
policy-map global_policy
    class flow_export_class
    #foreach ( $event_type in $netflow_Event_Types )
    flow-export event-type $event_type destination $netflow_Destination.get(1)
    #end
```

Haga clic en Guardar cuando haya terminado.

Name:					
Netflow_Add_Destination_Copy]				
Description: Create and configure a NetFlow export destination.]				
	J A ladar dura i Bara Jaarah	la schille annandiae Old	Discourse		
Copy-pasting any rich text migh	t introduce line brea	ks while generating CLI	Please verify the	e CLI before depi	oyment.
Insert 🔻 🔣 Deploym	ent: Once	Ŧ	Type: App	end	*
<pre>flow- export destination \$netf policy-map global_policy class flow_export_clas. #foreach (\$event_type flow-export event-type #end</pre>	low Destination s in \$netflow_E \$event_type do	n.get(0) \$netflo vent_Types) estination \$netf	w Destinatio	on.get(1) \$n	etflow Destination.get(2)
▼ Variables					
Name	Dimension	Default Value	Property (Type:Name)	Override	Description
netflow_Event_Types	MULTIPLE	[all]	FREEFORM:	false	This variable provides the glo
netflow_Destination	MULTIPLE	[DMZ, 10.20.20	FREEFORM:	false	This variable defines a single
					Cancel Save

Paso 5. Asignar la política FlexConfig al FTD

Navegue hasta **Devices > FlexConfig** y cree una nueva política (a menos que ya haya una creada para otro propósito y asignada al mismo FTD). En este ejemplo, ya se ha creado FlexConfig. Edite la política FlexConfig y **seleccione** los objetos FlexConfig creados en los pasos anteriores.

En este ejemplo, se utilizan los parámetros de exportación de Netflow predeterminados, por lo tanto, se selecciona Netflow_Set_Parameters. **Guarde los cambios e impleméntelo.**

FlexConfigPolicy			You have unsaved chang	ges Preview Config	Save Cancel
Enter Description				l.	Policy Assignments (1)
	"à S	elected Prepend FlexConfigs			
Available FlexConfig C FlexConfig Object		Name	Description		
V User Defined					
Netflow_Add_Destination_Copy					
"Netflow_Delete_Destination_Copy					
"I Netflow_export_Copy					
✓ System Defined					
Netflow_Add_Destination	. S	elected Append FlexConfigs			
Netflow_Clear_Parameters	#	Name	Description		
Netflow_Set_Parameters	1	flow_export_class			Q 🖬
	2	Netflow_Add_Destination_Copy	Create and configure a NetFlow export destination.		٩.
	3	Netflow_Set_Parameters	Set global parameters for NetFlow export.		2
			How To		

Nota: Para hacer coincidir todo el tráfico sin necesidad de hacer coincidir tráfico específico, puede saltar de los pasos 2 a 4 y utilizar los objetos NetFlow predefinidos.

FlexConfigPolicy			You have unsaved changes Preview Confi	g Save	Cancel
	"à (Selected Prepend FlexConfigs		Policy Ass	ignments (1)
Available FlexConfig C FlexConfig Object netflow X		Name	Description		
User Defined "a Netflow_Add_Destination_Copy		Selected Append FlexConfigs			
" Netflow_Clear_Parameters		Name	Description		
Netflow_Delete_Destination Netflow Set Parameters	1	Netflow_Set_Parameters	Set global parameters for NetFlow export.		2
	2	Netflow_Add_Destination	Create and configure a NetFlow export destination.		۹.

Nota: Para agregar un segundo colector NSEL al que se envían los paquetes de NetFlow. En el paso 1, agregue 4 variables para agregar la segunda dirección IP del recopilador de Netflow.

Edit Text Object

Name:

netflow_Destination

Description:

This variable defines a single NetFlow export destination.

Variable Type

Multiple		
	Multiple	



1	DMZ
2	10.20.20.1
3	2055
4	10.20.20.1

En el paso 4, agregue la línea de configuración: flow-export destination \$netflow_Destination.get(0) \$netflow_Destination.get(1) \$netflow_Destination.get(2)

Edite la variable \$netflow_Destination.get para la variable de correspondencia. En este ejemplo, el valor de la variable es 3. Por ejemplo:

flowexport destination \$netflow_Destination.get(0) \$netflow_Destination.get(1) \$netflow_Destination.
get(2)
flowexport destination \$netflow_Destination.get(0) \$netflow_Destination.get(3) \$netflow_Destination.
get(2)

Además, agregue la segunda variable \$netflow_Destination.get en la línea de configuración: flowexport event-type \$event_type destination \$netflow_Destination.get(1). Por ejemplo:

Edit FlexConfig Object

Name:					
Netflow_Add_Destination_Copy					
Description:					
Create and configure a NetFlow export destination.					
▲ Copy-pasting any rich text might int	roduce line break	s while generating CLI	Please verify the	e CLI before deplo	oyment.
Insert 🔻 🛛 🔣 🔹 Deployment	Once	v	Туре: Арр	end	v
<pre>## destination: interface n ## event-types: any subset flow- export destination \$netflow flow- export destination \$netflow policy-map global_policy class flow_export_class #foreach (\$event_type in flow-export event- type \$event_type destination #end</pre>	ameif destin of {all, flo Destination Destination \$netflow_Ev n \$netflow D	<pre>ation_ip_udp_po w-create, flow- get(0) \$netflo get(0) \$netflo rent_Types) estination.get(</pre>	rt denied, flow w Destinatio w Destinatio 1)\$ <u>netflow </u>	w-teardown, : on.get(1) \$nd on.get(3) \$nd Destination.d	<pre>flow-update} stflow Destination.get(2) stflow Destination.get(2) get(3)</pre>
▼ Variables					
Name	Dimension	Default Value	Property (Type:Name)	Override	Description
netflow_Event_Types	MULTIPLE	[all]	FREEFORM:	false	This variable provides the glo
netflow_Destination	MULTIPLE	[DMZ, 10.20.20	FREEFORM:	false	This variable defines a single
					Cancel

Verificación

La configuración de NetFlow se puede verificar dentro de la política FlexConfig. Para obtener una vista previa de la configuración, haga clic en **Preview Config**. **Seleccione** el FTD y verifique la configuración.

FTD-b 🔻	
exit	
!INTERFACE_END	
###Flex-config Appended CLI ###	
class-map flow_export_class	
match access-list flow_export_acl	
flow expert destination DMZ 10 20 20 1 2055	
now-export destination DMZ 10.20.20.1 2055	
class flow export class	
flow-export event-type all destination 10.20.20.1	
flow-export active refresh-interval 1	
no flow-export delay flow-create 1	
tiow-export template timeout-rate 30	

Acceda al FTD a través de Secure Shell (SSH) y utilice el comando system support diagnostic-cli y ejecute estos comandos:

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
firepower# show access-list flow_export_acl
access-list flow_export_acl; 3 elements; name hash: 0xe30fladf
access-list flow_export_acl line 1 extended deny object-group ProxySG_ExtendedACL_34359742097
object 10.10.10.1 any (hitcnt=0) 0x8edff419
access-list flow_export_acl line 1 extended deny ip host 10.10.10.1 any (hitcnt=0) 0x3d4f23a4
access-list flow_export_acl line 2 extended deny object-group ProxySG_ExtendedACL_34359742101
object 172.16.0.20 object 192.168.1.20 (hitcnt=0) 0x0ec22ecf
access-list flow_export_acl line 2 extended deny ip host 172.16.0.20 host 192.168.1.20
(hitcnt=0) 0x134aaeea
access-list flow_export_acl line 3 extended permit object-group ProxySG_ExtendedACL_30064776111
any any (hitcnt=0) 0x3726277e
access-list flow_export_acl line 3 extended permit ip any any (hitcnt=0) 0x759f5ecf
firepower# sh running-config class-map flow_export_class
class-map flow_export_class
match access-list flow_export_acl
firepower# show running-config policy-map
1
policy-map type inspect dns preset_dns_map
parameters
message-length maximum client auto
message-length maximum 512
no tcp-inspection
```

?

policy-map type inspect ip-options UM_STATIC_IP_OPTIONS_MAP parameters eool action allow nop action allow router-alert action allow policy-map global_policy class inspection_default inspect dns preset_dns_map inspect ftp inspect h323 h225 inspect h323 ras inspect rsh inspect rtsp inspect sqlnet inspect skinny inspect sunrpc inspect xdmcp inspect sip inspect netbios inspect tftp inspect icmp inspect icmp error inspect ip-options UM_STATIC_IP_OPTIONS_MAP inspect snmp class flow_export_class flow-export event-type all destination 10.20.20.1 class class-default set connection advanced-options UM_STATIC_TCP_MAP firepower# show running-config | include flow access-list flow_export_acl extended deny object-group ProxySG_ExtendedACL_34359742097 object 10.10.10.1 any access-list flow_export_acl extended deny object-group ProxySG_ExtendedACL_34359742101 object 172.16.0.20 object 192.168.1.20 access-list flow_export_acl extended permit object-group ProxySG_ExtendedACL_30064776111 any any flow-export destination DMZ 10.20.20.1 2055 class-map flow_export_class match access-list flow_export_acl class flow_export_class flow-export event-type all destination 10.20.20.1

Información Relacionada

Asistencia técnica y descargas de Cisco

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).