# Configuración de NetFlow en FMC

# Contenido

Introducción
Prerequisites
Requirements
Componentes Utilizados
Antecedentes
Agregar recopilador en NetFlow
Agregar clase de tráfico a NetFlow
Resolución de problemas
Información Relacionada

# Introducción

Este documento describe cómo configurar Netflow en Cisco Secure Firewall Management Center que ejecuta la versión 7.4 o superior.

# Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Secure Firewall Management Center (FMC)
- Cisco Secure Firewall Threat Defence (FTD)
- Protocolo NetFlow

### **Componentes Utilizados**

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

- Secure Firewall Management Center para VMWare ejecuta la versión 7.4.1
- Secure Firewall ejecuta la versión 7.4.1

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

Los requisitos específicos para este documento incluyen:

- · Cisco Secure Firewall Threat Defence con versión 7.4 o superior
- · Cisco Secure Firewall Management Center con versión 7.4 o superior

### Agregar recopilador en NetFlow

### Paso 1. Vaya a Devices > Platform Settings:



Acceso a configuración de plataforma

Paso 2. Edite la política de configuración de la plataforma asignada al dispositivo de supervisión:

Firewall Management Center Devices / Platform Settings	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy	۹	¢	≎	0	admin $\sim$	cisco SECU	RE
												Obje	t Management	
													New Policy	
Platform Settings			Device Type				Status							
Policy for Secure Firewall			Threat Defense	Ð			Targeting 1 devices Up-to-date on all target	ed devic	es				₽ <mark>∕</mark> •	

Edición de políticas

Paso 3. Elija Netflow:

Firewall Management	Center tor	Overview	Analysis	Policies	Devices	Objects	Integration
Policy for Secure Fire	wall						
Enter Description							
ARP Inspection							
Banner	Interface						Inspect Enabled
DNS							
External Authentication							
Fragment Settings							
HTTP Access							
ICMP Access							
NetFlow							
SSH Access							
SMTP Server							
SNMP							
SSL							
Syslog							
Timeouts							
Time Synchronization							
Time Zone							
UCAPL/CC Compliance							
Performance Profile							

Acceso a la configuración de NetFlow

Paso 4. Active la opción Exportar Flujo para activar la exportación de datos de NetFlow:

Firewall Managemen Devices / Platform Settings Ed	t Center Overview Analysis <sup>ditor</sup>	Policies	Devices	Objects	Integration				
Policy for Secure Firewall									
Enter Description									
ARP Inspection	Enable Flow Export								
Banner				o					
DNS	Active Refresh Interval (1-60)			Collector					
External Authentication	1	minutes							
Fragment Settings	Delay Flow Create (1-180)								
HTTP Access		seconds							
ICMP Access	Template Timeout Rate (1-3600)								
NetFlow	30	minutes							
SSH Access									
SMTP Server									
SNMP	Traffic Class								
SSL									
Syslog									
Timeouts									
Time Synchronization									
Time Zone									
UCAPL/CC Compliance									
Performance Profile									

Habilitación de NetFlow

Paso 5. Haga clic en Agregar recopilador:

Policy Assignments (1)



Paso 6. Elija el objeto IP de host del colector del colector de eventos de NetFlow, el puerto UDP en el colector al que se deben enviar los paquetes de NetFlow, elija el grupo de interfaz a través del cual se debe alcanzar el colector y haga clic en Aceptar:

Add Collector			0
Host Netflow_Collector	~ +		
Port (1-65535) 2055			
Available Interface Groups (1) C	+	Selected Interface Group	s (0)
	Add		
Select at least one interface group.			
			Cancel OK

Configuración del recopilador

# Agregar clase de tráfico a NetFlow

### Paso 1. Haga clic en Add Traffic Class:

C Enable Flow Export					
Active Refresh Interval (1-60)		Collector			Add Collector
1	minutes	Host	Interface Groups	Port	
Delay Flow Create (1-180)		Netflow_Collector	Netflow_Export	2055	/ 1
	seconds				
Template Timeout Rate (1-3600)					
30	minutes				
Traffic Class					Add Traffic Class
		N	lo traffic class records.		

Adición de clase de tráfico

Paso 2. Ingrese el campo de nombre de la clase de tráfico que debe coincidir con los eventos de NetFlow, la ACL para especificar la clase de tráfico que debe coincidir con el tráfico capturado para los eventos de NetFlow, seleccione las casillas de verificación para los diferentes eventos de

NetFlow que desea enviar a los recopiladores y haga clic en Aceptar:

Add Traffic Class

Name Netflow_class					
Type ● Access List ⊚ Default					
Access List Object Netflow_ACL	~ +				
Event Types					
Collector	All	Created	Denied	Updated	Torn Down
Netflow_Collector					
				Cancel	ОК

Configuración de clase de tráfico

# Resolución de problemas

Paso 1. Puede verificar la configuración desde la CLI de FTD.

1.1. Desde FTD CLI, ingrese a system support diagnostic-cli:

>system support diagnostic-cli

1.2 Comprobar la configuración de policy-map:

#### <#root>

```
firepower#show running-config policy-map
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum client auto
message-length maximum 512
no tcp-inspection
```

0

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 sip inspect netbios inspect tftp inspect icmp inspect icmp error inspect ip-options UM\_STATIC\_IP\_OPTIONS\_MAP class class\_snmp inspect snmp class Netflow\_class\_Netflow\_ACL

flow-export event-type all destination 192.168.31.1

```
class class-default
set connection advanced-options UM_STATIC_TCP_MAP
!
```

1.3. Comprobar la configuración de exportación de flujo:

<#root>

firepower#show running-config flow-export

flow-export destination Inside 192.168.31.1 2055



Nota: En este ejemplo, "Inside" es el nombre de la interfaz configurada en el grupo de interfaces denominado Netflow\_Export

Paso 2. Verifique el conteo de aciertos para la ACL:

<#root>

firepower#show access-list Netflow\_ACL access-list Netflow\_ACL; 1 elements; name hash: 0xbad5d4bf access-list Netflow\_ACL line 1 extended permit ip object Inside\_Network any ( hitcnt=44 ) 0xb704fc5b access-list Netflow\_ACL line 1 extended permit ip 10.1.2.0 255.255.255.0 any ( hitcnt=44 ) 0xb704fc5b

### Paso 3. Verificar contadores de Netflow:

#### <#root>

firepower#show flow-export counters

destination: Inside 192.168.31.1 2055 Statistics:

packets sent	101
Errors:	
block allocation failure	0
invalid interface	0
template send failure	0
no route to collector	0
failed to get lock on block	0
source port allocation failure	0

## Información Relacionada

• Guía de configuración de dispositivos de Cisco Secure Firewall Management Center, 7.4

### 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).