# **Configurare NetFlow in FMC**

# Sommario

Introduzione
Prerequisiti
Requisiti
Componenti usati
Premesse
Aggiungi agente di raccolta in NetFlow
Aggiungi classe traffico a NetFlow
Risoluzione dei problemi
Informazioni correlate

## Introduzione

In questo documento viene descritto come configurare Netflow in Cisco Secure Firewall Management Center con versione 7.4 o successive.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Secure Firewall Management Center (FMC)
- Cisco Secure Firewall Threat Defense (FTD)
- Protocollo NetFlow

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Secure Firewall Management Center per VMWare in esecuzione versione 7.4.1
- Secure Firewall Runs v7.4.1

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

### Premesse

I requisiti specifici per questo documento includono:

- Cisco Secure Firewall Threat Defense con versione 7.4 o superiore
- Cisco Secure Firewall Management Center con versione 7.4 o superiore

### Aggiungi agente di raccolta in NetFlow

#### Passaggio 1. Selezionare Devices > Platform Settings:



Accesso alle impostazioni della piattaforma

# Passaggio 2. Modificare il criterio Impostazioni piattaforma assegnato al dispositivo di monitoraggio:

Firewall Management Center Devices / Platform Settings	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy	९ 🍯	<mark>ې</mark> ې	0	admin $\sim$	cisco	SECURE
											Obje	ct Manag Nev	gement v Policy
Platform Settings			Device Type				Status						
Policy for Secure Firewall			Threat Defense	9			Targeting 1 devices Up-to-date on all targete	d devices				¶ <b>∕</b> i	ì

Edizione criterio

### Passaggio 3. Scegliere NetFlow:

Firewall Management	Firewall Management Center Devices / Platform Settings Editor		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							

Accesso alle impostazioni di NetFlow

Passaggio 4. Attiva/disattiva esportazione flusso per abilitare l'esportazione dati NetFlow:

Firewall Managemen Devices / Platform Settings Ec	t Center Overview	Analysis	Policies	Devices	Objects	Integration		
Policy for Secure Firewall								
Enter Description								
ARP Inspection	Enable Flow Export							
Banner	$\sim$							
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 (1-360	0)	_					
NetFlow	30	-	minutes					
SSH Access								
SMTP Server								
SNMP	Traffic Class							
SSL								
Syslog								
Timeouts								
Time Synchronization								
Time Zone								
UCAPL/CC Compliance								
Performance Profile								

Abilitazione di NetFlow

Passaggio 5. Fare clic su Add Collector:

Policy Assignments (1)



Aggiunta agente di raccolta

Passaggio 6. Scegliere l'oggetto IP dell'host del collector per l'agente di raccolta eventi NetFlow, la porta UDP sul collector a cui devono essere inviati i pacchetti NetFlow, scegliere il gruppo di interfacce attraverso cui deve essere raggiunto il collector e fare clic su OK:

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

Impostazioni agente di raccolta

# Aggiungi classe traffico a NetFlow

### Passaggio 1. Fare clic su Add Traffic Class:

	Collector			Add Collector
minutes	Host	Interface Groups	Port	
	Netflow_Collector	Netflow_Export	2055	/ 1
seconds				
minutes				
				Add Traffic Class
	N	io traffic class records.		
	minutes seconds minutes	Collector minutes Host Netflow_Collector seconds minutes	Collector minutes Host Interface Groups Netflow_Collector seconds minutes No traffic class records.	Collector       minutes     Host     Interface Groups     Port       Netflow_Collector     Netflow_Eport     2055

Aggiunta di una classe di traffico

Passaggio 2. Immettere il campo del nome della classe di traffico che deve corrispondere agli eventi NetFlow, l'ACL per specificare la classe di traffico che deve corrispondere al traffico acquisito per gli eventi NetFlow, selezionare le caselle di controllo per i diversi eventi NetFlow che si desidera inviare agli agenti di raccolta e fare clic su OK:

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

0

Impostazioni classe traffico

## Risoluzione dei problemi

Passaggio 1. È possibile verificare la configurazione dalla CLI FTD.

1.1. Dalla CLI FTD, accedere al supporto di sistema diagnostic-cli:

>system support diagnostic-cli

1.2 Controllare la configurazione della mappa dei criteri:

#### <#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
```

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. Controllare la configurazione del flusso di esportazione:

<#root>

firepower#show running-config flow-export

flow-export destination Inside 192.168.31.1 2055



Nota: nell'esempio, "Inside" è il nome dell'interfaccia configurata nel gruppo di interfacce denominato Netflow\_Export

Passaggio 2. Verificare il numero di passaggi per l'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

### Passaggio 3. Verificare i contatori 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

## Informazioni correlate

• Guida alla configurazione dei dispositivi di Cisco Secure Firewall Management Center, 7.4

### Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).