# Vastlegging NetFlow Secure Event configureren bij Firepower Threat Defence

# Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Achtergrondinformatie Configureren Verifiëren Gerelateerde informatie

# Inleiding

Dit document beschrijft hoe u NetFlow Secure Event Logging (NSEL) kunt configureren op Firepower Threat Defence (FTD) via Firepower Management Center (FMC).

# Voorwaarden

## Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Kennis van het VCC
- Kennis van het FTD
- Kennis van het FlexConfig-beleid

## Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- FTD versie 6.6.1
- FMC versie 6.6.1

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

## Achtergrondinformatie

Dit document beschrijft hoe u NetFlow Secure Event Logging (NSEL) kunt configureren op Firepower Threat Defence (FTD) via Firepower Management Center (FMC).

De FlexConfig-tekstobjecten zijn gekoppeld aan variabelen die worden gebruikt in de vooraf

gedefinieerde FlexConfig-objecten. Vooraf gedefinieerde FlexConfig-objecten en bijbehorende tekstobjecten worden gevonden in FMC om NSEL te configureren. Er zijn vier vooraf gedefinieerde FlexConfig-objecten in het VCC en drie vooraf gedefinieerde tekstobjecten. Voorgedefinieerde FlexConfig-objecten worden alleen-lezen en kunnen niet worden aangepast. Om de parameters van NetFlow aan te passen, kunnen de objecten worden gekopieerd.

De vier vooraf gedefinieerde objecten worden in de tabel weergegeven:

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

### De drie vooraf gedefinieerde tekstobjecten worden in de tabel weergegeven:

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.

# Configureren

In dit deel wordt beschreven hoe u NSEL op FMC kunt configureren via een FlexConfig-beleid.

Stap 1. Stel de parameters van de Tekstobjecten in voor NetFlow.

Als u de variabele parameters wilt instellen, navigeer dan naar **Objecten > FlexConfig > Tekstobjecten**. Bewerk het object netflow\_Destination. Definieer het meerdere variabele type en telling ingesteld op 3. Stel de interfacenaam, het IP-adres en de poort van de bestemming in.

In dit configuratievoorbeeld is de interface DMZ, is het IP-adres van NetFlow Collector 10.20.20.1 en is de UDP-poort 2055.

# Edit Text Object

### Name:

netflow\_Destination

### Description:

This variable defines a single NetFlow export destination.

### Variable Type

Multiple	$\mathbf{\nabla}$



1	DMZ
2	10.20.20.1
3	2055

**Opmerking**: standaardwaarden voor netflow\_Event\_Types en netflow\_Parameters worden gebruikt.

Stap 2. Configureer een object uitgebreide toegangslijst om specifiek verkeer aan te passen.

Om een uitgebreide toegangslijst op het VCC te maken, navigeer naar **Objecten > Objectbeheer** en in het linker menu, onder **Toegangslijst** uitkiezen **Uitgebreid**.Klik **Uitgebreide toegangslijst toevoegen**.

Vul het veld **Naam** in. In dit voorbeeld is de naam flow\_export\_acl. Klik op de knop **Toevoegen**. Configureer de vermeldingen **toegangscontrole** om specifiek verkeer aan te passen.

In dit voorbeeld is verkeer van host 10.10.10.1 naar elke bestemming en verkeer tussen host 172.16.0.20 en 192.168.1.20 uitgesloten. Al het andere verkeer is inbegrepen.



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	/ •
2	Block	172.16.0.20	Any	192.168.1.20	Any	/ 🖬
3 Allow Ove	Allow	Any	Any	Any	Any	/1
						Cancel Save

Stap 3. Configureer een FlexConfig-object.

Om de FlexConfig-objecten te configureren navigeert u naar **Objecten > FlexConfig > FlexConfig-** objecten en klikt u op de knop **Add FlexConfig Object**.

Definieer de klassekaart die verkeer identificeert waarvoor NetFlow-gebeurtenissen moeten worden geëxporteerd. In dit voorbeeld is de naam van het object flow\_export\_class.

Selecteer de toegangslijst die in Stap 2 is gemaakt. Klik op Invoegen > Beleidsobject invoegen > Uitgebreid ACL-object en wijs een naam toe. Klik vervolgens op de knop Toevoegen. In dit voorbeeld is de naam van de variabele flow\_export\_acl. Klik op Save (Opslaan).

0

Variable Name:			
flow_export_acl			
Description:			
Available Objects C		Selected Object	
Q Search	×	flow_export_acl	Ì
flow_export_acl			
	Add		

Cancel	Save	

Voeg de volgende configuratielijnen toe in het lege veld rechts en neem de variabele die eerder is gedefinieerd (**\$flow\_export\_acl.**) op in de configuratielijn voor overeenkomende toegangslijsten.

Het is een **\$** Het symbool begint met de variabele naam. Dit helpt te definiëren dat een variabele erna komt.

class-map flow\_export\_class
match access-list \$flow\_export\_acl
Klik op Opslaan als u klaar bent.

8

#### Edit FlexConfig Object

Name:							
flow_export_class							
Description:							
Copy-pasting any rich	text might intro	duce line break	ks while generating Cl	.I. Please ve	erify the (	CLI before deplo	yment.
Insert 🗸 🛛 🔛	Deployment:	Everytime		Type:	Apper	nd	- 
class-map flow_exp match access-list	ort_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 Save

Stap 4. De NetFlow-bestemming configureren

Als u de NetFlow-bestemming wilt configureren, navigeert u naar **Objecten > FlexConfig > FlexConfig**-objecten en filter via NetFlow. **Kopieert** het object NetFlow\_Add\_Destination. De NetFlow\_Add\_Destination\_Copy wordt aangemaakt.

Wijs de klasse toe die in Stap 3 is gemaakt. U kunt een nieuwe beleidskaart maken om de flowexport-acties op de gedefinieerde klassen toe te passen.

In dit voorbeeld wordt de klasse ingevoegd in het huidige beleid (globaal beleid).

```
## 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
```

Name:					
Netflow_Add_Destination_Copy					
Description:					
export destination.					
▲ Copy-pasting any rich text might in	ntroduce line breal	ks while generating CLI.	Please verify th	e CLI before deple	oyment.
Insert 🔻 🛛 🕄 🔹 Deploymen	t: Once	٣	Type: App	pend	•
<pre>## destination: interface ## event-types: any subset</pre>	nameif destin of {all, flo	nation_ip_udp_po: ow-create, flow-c	rt denied, flo	w-teardown,	flow-update}
flow-	w Destinatio	n get(0) Spetflor	. Destinati	on get (1) ŝn	etflow Destination get (2)
policy-map global_policy class flow export class	, peseindero		Desernaer	011.900(1) 41	cerrow pescringer (2)
<pre>#foreach ( \$event_type i flow_evport_event_type i </pre>	n \$netflow_E	vent_Types )	low Doctina	tion got (1)	
liow-export event-type \$	event_type de	estimation sheet.	IOW DESCINA	cion.get(1)	
#end					
▼ 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

Stap 5. Wijs het FlexConfig-beleid toe aan de FTD

Navigeer naar **Apparaten > FlexConfig** en maak een nieuw beleid (tenzij er al een beleid is gemaakt voor een ander doel en toegewezen aan hetzelfde FTD). In dit voorbeeld is FlexConfig al gemaakt. Bewerk het FlexConfig-beleid en **selecteer** de FlexConfig-objecten die in de vorige stappen zijn gemaakt.

In dit voorbeeld worden de standaard NetFlow export parameters gebruikt, daarom wordt de NetFlow\_Set\_Parameters geselecteerd. **Sla de wijzigingen op en implementeer deze.** 

FlexConfigPolicy			You have unsaved ch	anges Preview Config	Save Cancel
Enter Description					Policy Assignments (1)
FlayConfig Object	"à S	elected Prepend FlexConfigs			
Available FlexConing C FlexConing Object		Name	Description		
V User Defined					
Netflow_Add_Destination_Copy					
.9 Netflow_Delete_Destination_Copy					
" Netflow_export_Copy " Netflow_Set_Percenters_Copy					
✓ System Defined					
"∎ Netflow_Add_Destination	. <b>9</b> S	elected Append FlexConfigs			
.9 Netflow_Clear_Parameters	#	Name	Description		
Netflow_Delete_Destination	1	flow_export_class			2
	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		

**Opmerking**: om al het verkeer aan te passen zonder dat u specifiek verkeer hoeft aan te passen, kunt u de stappen 2 tot en met 4 overslaan en de vooraf gedefinieerde NetFlow-objecten gebruiken.

FlexConfigPolicy		You have unsaved changes Preview Config	Save Cancel
Available FlexConfig C FlexConfig Object       netflow     X       VUser Defined     **       ** Netflow_Add_Destination_Copy         Netflow_export_Copy	Selected Prepend FlexConfigs  Name	Description	Policy Assignments (1)
*i Netflow_Set_Parameters_Copy	Selected Append FlexConfigs		
"9 Netflow_Clear_Parameters	# Name	Description	
Netflow_Delete_Destination Netflow_Set_Parameters	1 Netflow_Set_Parameters	Set global parameters for NetFlow export.	٩.
	2 Netflow_Add_Destination	Create and configure a NetFlow export destination.	۹.

**Opmerking**: Om een tweede NSEL-collector toe te voegen waarnaar NetFlow-pakketten worden verzonden. In Stap 1, voeg 4 variabelen toe om het tweede NetFlow Collector IP adres toe te voegen.

# Edit Text Object

### Name:

netflow\_Destination

## Description:

This variable defines a single NetFlow export destination.

### Variable Type

Multiple	r



1	DMZ
2	10.20.20.1
3	2055
4	10.20.20.1

In Stap 4., voeg de configuratie regel toe: flow-export bestemming \$netflow\_Destination.get(0) \$netflow\_Destination.get(1) \$netflow\_Destination.get(2)

# Bewerk de variabele \$netflow\_Destination.get voor de correspondentievariabele. In dit voorbeeld is de variabele waarde 3. Voorbeeld:

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)

Voeg ook de tweede variabele \$netflow\_Destination.get toe in de configuratielijn: flow-export event-type \$event\_type bestemming \$netflow\_Destination.get(1). Voorbeeld:

#### 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 depl	oyment.		
Insert 🔻   🐹   Deployment:	Once	Ŧ	Туре: Арр	end	<b>v</b>		
<pre>## destination: interface n ## event-types: any subset flow-</pre>	ameif destin of {all, flo	ation_ip udp po w-create, flow-	rt denied, flow	v-teardown,	flow-update}		
export destination \$netflow Destination.get(0) \$netflow Destination.get(1) \$netflow Destination.get(2) flow-							
<pre>export destination \$netflow policy-map global_policy class flow_export_class #foreach ( \$event_type in flow-export event- type \$event_type destination</pre>	_Destination \$netflow_Ev n \$netflow_D	rent_Types )	w Destinati 1)\$netflow 1	on.get(3) \$n Destination.	<pre>etflow Destination.get(2) get(3)</pre>		
#end							
<ul> <li>Variables</li> </ul>							
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		

# Verifiëren

De NetFlow-configuratie kan worden geverifieerd binnen het FlexConfig-beleid. Klik om de configuratie te bekijken op **Preview Config. Selecteer** de FTD en controleer de configuratie.

FTD-b	•		
exit			
INTERFACE_END			
###Flex-config Appende	d CLI ###		
class-map flow_export_	class		
match access-list flow_	xport_acl		
flow-export destination	MZ 10.20.20.1 2055		
policy-map global_polic	,		
class flow_export_clas			
flow-export event-typ	e all destination 10.20.20.1		
flow-export active refre	h-interval 1		
no flow-export delay flo	w-create 1		
flow-export template tir	eout-rate 30		
note oxport tomplate th			

# Toegang tot de FTD via Secure Shell (SSH) en gebruik de diagnostische client voor opdrachtsysteem en voer deze opdrachten uit:

> 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: 0xe30f1adf
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
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum client auto
message-length maximum 512
no tcp-inspection

3

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

# Gerelateerde informatie

<u>Cisco technische ondersteuning en downloads</u>

### Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.