# Konfigurieren der sicheren NetFlow-Ereignisprotokollierung in Firepower Threat Defense

## Inhalt

Einleitung Voraussetzungen Anforderungen Verwendete Komponenten Hintergrundinformationen Konfigurieren Überprüfung Zugehörige Informationen

## Einleitung

Dieses Dokument beschreibt die Konfiguration von NetFlow Secure Event Logging (NSEL) auf Firepower Threat Defense (FTD) über Firepower Management Center (FMC).

## Voraussetzungen

## Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Kenntnisse von FMC
- FTD-Kenntnisse
- Kenntnis der FlexConfig-Richtlinie

## Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- FTD-Version 6.6.1
- FMC Version 6.6.1

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

## Hintergrundinformationen

Dieses Dokument beschreibt die Konfiguration von NetFlow Secure Event Logging (NSEL) auf

Firepower Threat Defense (FTD) über Firepower Management Center (FMC).

Die FlexConfig-Textobjekte sind Variablen zugeordnet, die in den vordefinierten FlexConfig-Objekten verwendet werden. Vordefinierte FlexConfig-Objekte und zugehörige Textobjekte befinden sich in FMC, um NSEL zu konfigurieren. Das FMC verfügt über vier vordefinierte FlexConfig-Objekte und drei vordefinierte Textobjekte. Vordefinierte FlexConfig-Objekte sind schreibgeschützt und können nicht geändert werden. Um die Parameter von NetFlow zu ändern, können die Objekte kopiert werden.

Die vier vordefinierten Objekte sind in der Tabelle aufgelistet:

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

### Die drei vordefinierten Textobjekte sind in der Tabelle aufgelistet:

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.

## Konfigurieren

In diesem Abschnitt wird beschrieben, wie Sie NSEL auf FMC über eine FlexConfig-Richtlinie konfigurieren.

Schritt 1: Legen Sie die Parameter der Textobjekte für NetFlow fest.

Um die Variablenparameter festzulegen, navigieren Sie zu **Objects > FlexConfig > Text Objects**. Bearbeiten Sie das Objekt netflow\_Destination. Definieren Sie den Typ und den Zählersatz für mehrere Variablen auf 3. Legen Sie den Schnittstellennamen, die Ziel-IP-Adresse und den Port fest.

In diesem Konfigurationsbeispiel lautet die Schnittstelle DMZ, die IP-Adresse von NetFlow Collector 10.20.20.1 und der UDP-Port 2055.

## Edit Text Object

### Name:

netflow\_Destination

### Description:

This variable defines a single NetFlow export destination.

### Variable Type

Multiple	•
----------	---



0.20.20.1
)55
)

**Hinweis**: Es werden Standardwerte für netflow\_Event\_Types und netflow\_Parameters verwendet.

Schritt 2: Konfigurieren eines erweiterten Zugriffslistenobjekts für bestimmten Datenverkehr

Um eine erweiterte Zugriffsliste für FMC zu erstellen, navigieren Sie zu **Objekte > Objektverwaltung** und im Menü links unter **Zugriffsliste** auswählen **Erweitert.**Klicken Sie auf **Erweiterte Zugriffsliste hinzufügen.** 

Füllen Sie das Feld **Name** aus. In diesem Beispiel lautet der Name flow\_export\_acl. Klicken Sie auf die Schaltfläche **Hinzufügen**. Konfigurieren der **Zugriffssteuerungseinträge** entsprechend dem jeweiligen Datenverkehr

In diesem Beispiel wird Datenverkehr von Host 10.10.10.1 zu einem beliebigen Ziel und Datenverkehr zwischen Host 172.16.0.20 und 192.168.1.20 ausgeschlossen. Der restliche Datenverkehr ist enthalten.

?

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	/1
						Cancel Save

Schritt 3: Konfigurieren eines FlexConfig-Objekts

Um die FlexConfig-Objekte zu konfigurieren, navigieren Sie zu **Objects > FlexConfig > FlexConfig**-Objekte, und klicken Sie auf die Schaltfläche **Add FlexConfig Object (FlexConfig-Objekt** hinzufügen).

Definieren Sie die Klassenzuordnung, die den Datenverkehr identifiziert, für den NetFlow-Ereignisse exportiert werden müssen. In diesem Beispiel lautet der Name des Objekts flow\_export\_class.

Wählen Sie die in Schritt 2 erstellte Zugriffsliste aus. Klicken Sie auf Einfügen > Richtlinienobjekt einfügen > Erweitertes ACL-Objekt, und weisen Sie einen Namen zu. Klicken Sie dann auf die Schaltfläche Hinzufügen. In diesem Beispiel lautet der Name der Variablen flow\_export\_acl. Klicken Sie auf Speichern.

Variable Name:		
flow_export_acl	]	
Description:		
Available Objects C		Selected Object
Q Search X	]	flow_export_acl
flow_export_acl		
	Add	

Cancel	Save	

Fügen Sie die nächsten Konfigurationsposten in das leere Feld rechts ein, und fügen Sie die zuvor definierte Variable (**\$flow\_export\_acl.**) in die Konfigurationsposition der Übereinstimmungszugriffsliste ein.

Beachten Sie, dass **USD** -Symbol beginnt der Variablenname. Dies hilft, zu definieren, dass eine Variable danach kommt.

class-map flow\_export\_class match access-list **\$flow\_export\_acl** Klicken Sie abschließend auf **Speichern**. 2

#### 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	ovment.
Insert 🔻   🐹	Deployment:	Everytime	•	Type:	Apper	nd	· · · · · ·
class-map flow_exp match access-list	port_class \$flow_expo	rt acl					
▼ Variables							
Name		Dimension	Default Value	Propert (Type:N	y lame)	Override	Description
flow_export_class		SINGLE	flow_export_acl	EXD_A	CL:fl	false	
							Cancel Save

Schritt 4: Konfigurieren des NetFlow-Ziels

Um das NetFlow-Ziel zu konfigurieren, navigieren Sie zu **Objects > FlexConfig > FlexConfig-**Objekten, und filtern Sie nach NetFlow. **Kopieren Sie** das Objekt NetFlow\_Add\_Destination. Die NetFlow\_Add\_Destination\_Copy wird erstellt.

Zuweisen der in Schritt 3 erstellten Klasse Sie können eine neue Richtlinienzuordnung erstellen, um die Flow-Export-Aktionen auf die definierten Klassen anzuwenden.

In diesem Beispiel wird die Klasse in die aktuelle Richtlinie (globale Richtlinie) eingefügt.

```
## 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
```

Klicken Sie abschließend auf Speichern.

Name:					
Netflow_Add_Destination_Copy					
Description: Create and configure a NetFlow					
export destination.					
Copy-pasting any rich text might in	roduce line break	s while generating CLI.	Please verify the	e CLI before deple	oyment.
Insert 🗸 🛛 🐹 🔹 Deployment	Once	Ψ	Туре: Арр	end	<b>V</b>
<pre>## destination: interface_n ## event-types: any subset flow- export destination \$netflow policy-map global_policy     class flow_export_class     #foreach ( \$event_type in     flow-export event-type \$e     #end</pre>	ameif destir of {all, flo Destination \$netflow_Ev vent_type de	<pre>hation_ip_udp_po bw-create, flow- h.get(0) \$netflow yent_Types ) estination \$netf</pre>	rt denied, flow w Destinatio low Destinat	w-teardown, on.get(1) \$n	flow-update} 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

#### Schritt 5: Zuweisung der FlexConfig-Richtlinie zum FTD

Navigieren Sie zu **Devices > FlexConfig**, und erstellen Sie eine neue Richtlinie (es sei denn, es wurde bereits eine Richtlinie für einen anderen Zweck erstellt und demselben FTD zugewiesen). In diesem Beispiel ist die FlexConfig bereits erstellt. Bearbeiten Sie die FlexConfig-Richtlinie, und wählen Sie die FlexConfig-Objekte aus, die in den vorherigen Schritten erstellt wurden.

In diesem Beispiel werden die standardmäßigen NetFlow-Exportparameter verwendet. Daher ist NetFlow\_Set\_Parameters ausgewählt. Speichern Sie die Änderungen, und stellen Sie sie bereit.

FlexConfigPolicy			You have unsaved chang	ges Preview Config Save	Cancel
Enter Description				Policy Assignment	ents (1)
Eleverte Oblast	"à S	elected Prepend FlexConfigs			
Available FlexConfig C Prexcoming Object		Name	Description		
✓ User Defined					
Netflow_Add_Destination_Copy					
"Netflow_Delete_Destination_Copy					
"i Netflow_Set_Parameters_Copy					
✓ System Defined					
Netflow_Add_Destination	. <b>9</b> S	elected Append FlexConfigs			
-9 Netflow_Clear_Parameters	#	Name	Description		
Netflow_Set_Parameters	1	flow_export_class			2
	2	Netflow_Add_Destination_Copy	Create and configure a NetFlow export destination.		9
	3	Netflow_Set_Parameters	Set global parameters for NetFlow export.		2
			How To		

**Hinweis**: Sie können die Schritte 2 bis 4 überspringen und die vordefinierten NetFlow-Objekte verwenden, um den gesamten Datenverkehr abzugleichen, ohne dass ein bestimmter Datenverkehr abgeglichen werden muss.

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.

**Hinweis**: Einen zweiten NSEL-Collector hinzufügen, an den NetFlow-Pakete gesendet werden. Fügen Sie in Schritt 1 vier Variablen hinzu, um die zweite Netflow Collector-IP-Adresse hinzuzufügen.

## Edit Text Object

### Name:

netflow\_Destination

## Description:

This variable defines a single NetFlow export destination.

## Variable Type

Multiple	



1	DMZ
2	10.20.20.1
3	2055
4	10.20.20.1

Fügen Sie in Schritt 4 die Konfigurationsposition hinzu: flow-export destination \$netflow\_Destination.get(0) \$netflow\_Destination.get(1) \$netflow\_Destination.get(2)

# Bearbeiten Sie die Variable \$netflow\_Destination.get für die Korrespondenzvariable. In diesem Beispiel ist der Variablenwert 3. Beispiele:

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)

Fügen Sie außerdem die zweite Variable \$netflow\_Destination.get in der Konfigurationszeile hinzu: flow-export event-type \$event\_type destination \$netflow\_Destination.get(1). Beispiele:

#### Edit FlexConfig Object

Name:					
Netflow_Add_Destination_Copy					
Description:					
Create and configure a NetFlow export destination.					
▲ Copy-pasting any rich text might int	troduce line break	s while generating CLI	Please verify the	CLI before deple	oyment.
Insert 🔻 🛛 🐹 🔹 Deployment	Once	v	Type: Appe	nd	v
<pre>## destination: interface i ## 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>	of (all, flo pestination pestination \$netflow_Ev \$n \$netflow D	<pre>w-create, flow- get(0) \$netflo get(0) \$netflo rent_Types ) estination.get(</pre>	denied, flow w Destinatio w Destinatio 1)\$ <u>netflow D</u>	-teardown, n.get(1) \$n n.get(3) \$n estination.	flow-update) etflow Destination.get(2) etflow Destination.get(2) get(3)
▼ 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

## Überprüfung

Die NetFlow-Konfiguration kann in der FlexConfig-Richtlinie überprüft werden. Um eine Vorschau der Konfiguration anzuzeigen, klicken Sie auf **Preview Config (Konfigurationsvorschau)**. Wählen Sie den FTD aus, und überprüfen Sie die Konfiguration.

FTD-b T	
exit	
!INTERFACE_END	
###Flex-config Appended CLI ###	
class-map flow export class	
match access-list flow_export_acl	
flow-export destination DMZ 10.20.20.1 2055	
policy-map global_policy	
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	
flow-export template timeout-rate 30	

### Greifen Sie über Secure Shell (SSH) auf die FTD zu, und verwenden Sie die Befehlsunterstützungs-CLI des Befehlssystems, und führen Sie die folgenden Befehle aus:

```
> 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
1
policy-map type inspect dns preset_dns_map
parameters
message-length maximum client auto
message-length maximum 512
no tcp-inspection
```

8

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

## Zugehörige Informationen

Technischer Support und Downloads von Cisco

### Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.