在Firepower威脅防禦上配置NetFlow安全事件記錄

目錄

簡介

本檔案介紹如何透過Firepower管理中心(FMC)對Firepower威脅防禦(FTD)設定NetFlow安全事件記錄(NSEL)。

必要條件

需求

思科建議您瞭解以下主題：

- FMC知識
- FTD知識
- FlexConfig策略知識

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- FTD版本6.6.1
- FMC版本6.6.1

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

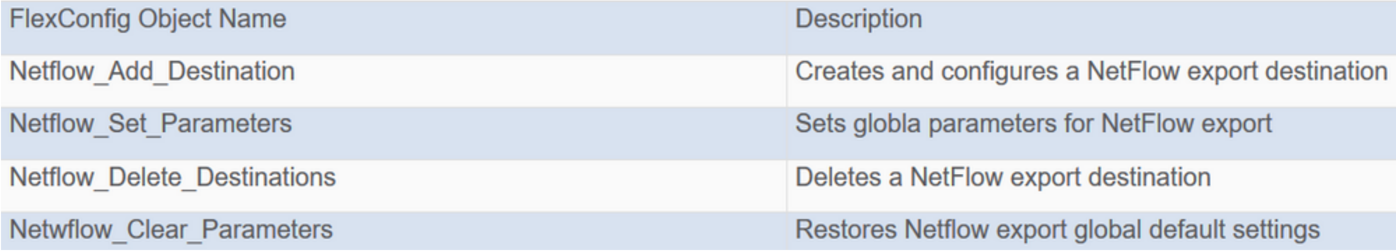
背景資訊

本檔案介紹如何透過Firepower管理中心(FMC)對Firepower威脅防禦(FTD)設定NetFlow安全事件記錄(NSEL)。

FlexConfig文本對象與預定義FlexConfig對象中使用的變數相關聯。預定義的FlexConfig對象和相關文本對象可在FMC中找到，用於配置NSEL。FMC中有四個預定義的FlexConfig對象和三個預定義的文本對象。預定義的FlexConfig對象是只讀的，無法修改。為了修改NetFlow的引數，可以複製對

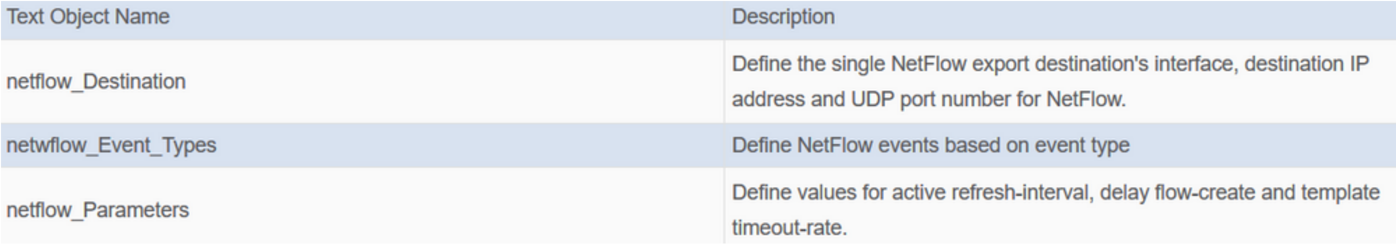
象。

表中列出了四個預定義對象：



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

表格中列出了三個預定義的文本對象：



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.

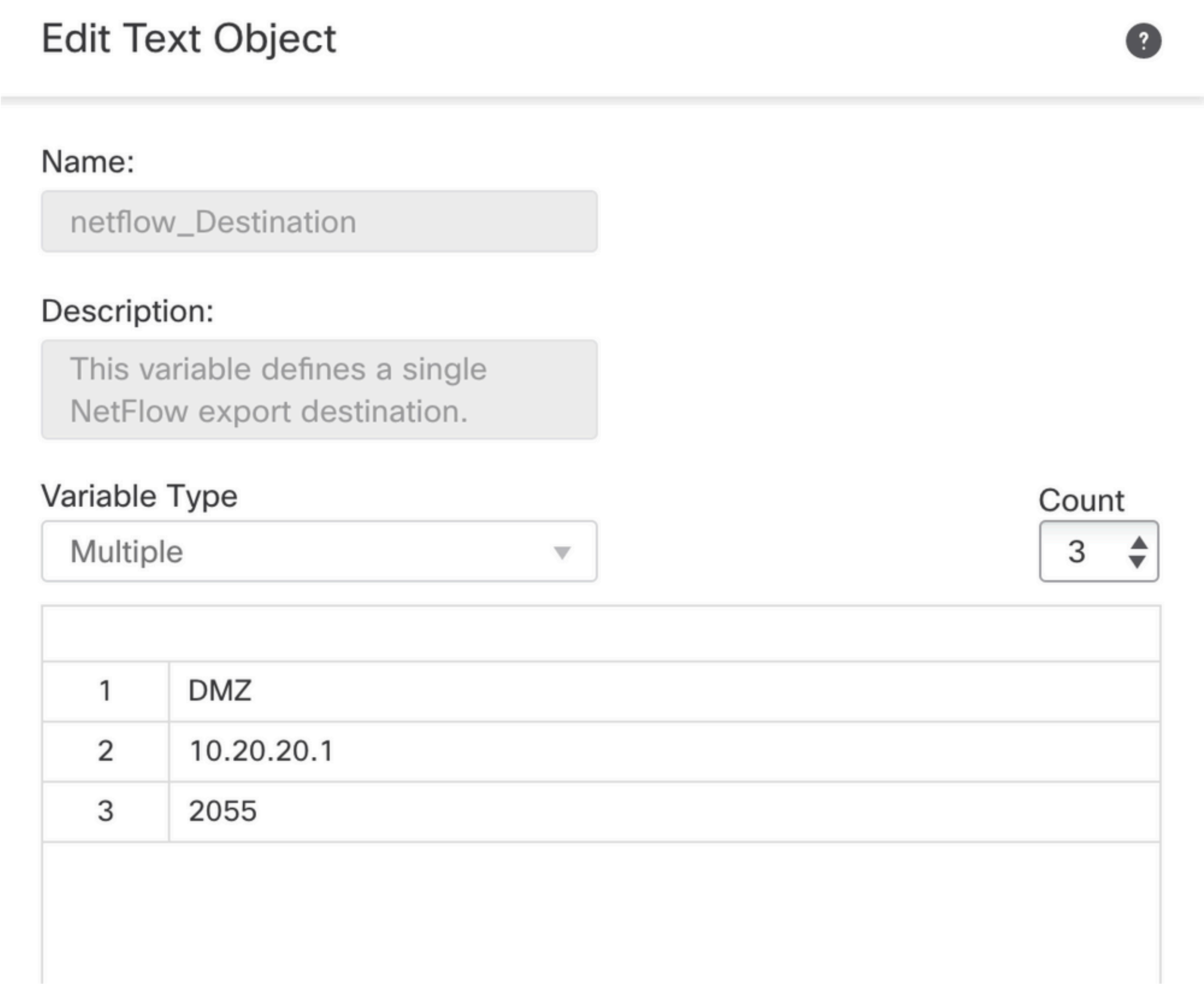
設定

本節介紹如何通過FlexConfig策略在FMC上配置NSEL。

步驟1.設定Netflow文本對象的引數。

若要設定變數引數，請導航到**對象> FlexConfig >文本對象**。編輯netflow_Destination對象。定義多變數型別和計數設定為3。設定介面名稱、目標IP地址和埠。

在此配置示例中，介面為DMZ，NetFlow收集器IP地址為10.20.20.1,UDP埠為2055。



Edit Text Object

Name:

netflow_Destination

Description:

This variable defines a single NetFlow export destination.

Variable Type: Multiple

Count: 3

1	DMZ
2	10.20.20.1
3	2055

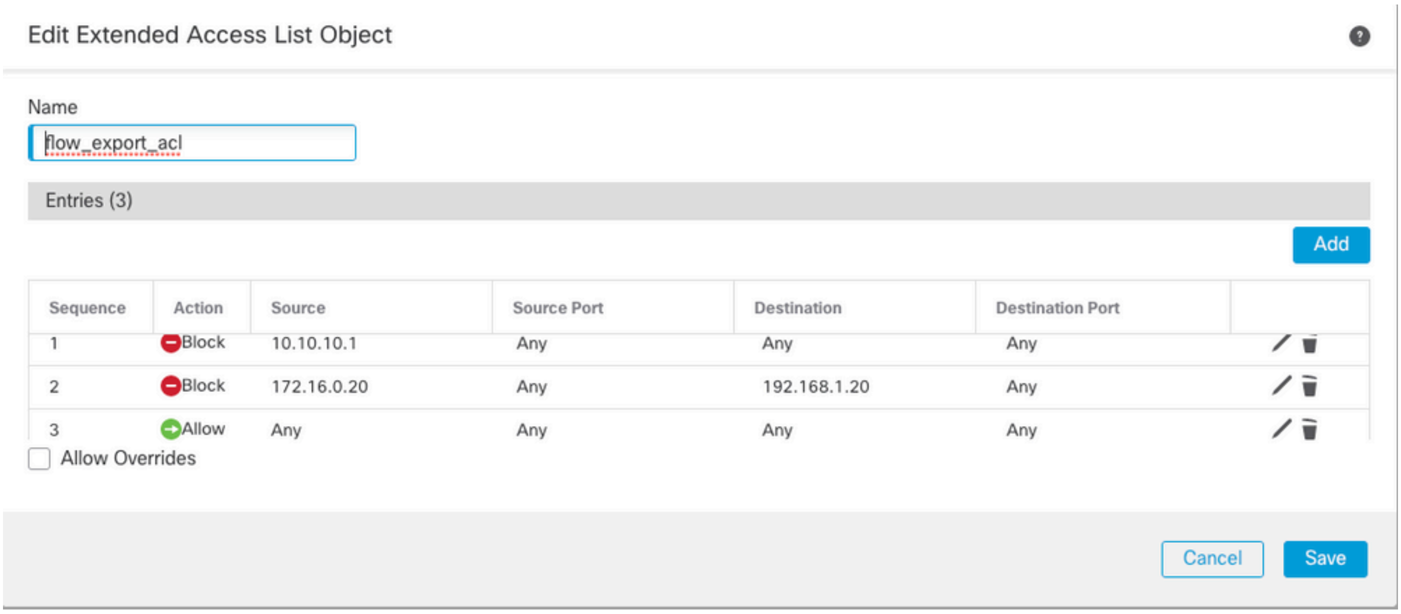
註：使用netflow_Event_Types和netflow_Parameters的預設值。

步驟2.配置擴展訪問清單對象以匹配特定流量。

要在FMC上建立擴展訪問清單，請導航至 **「對象」(Object)>「對象管理」(Object Management)** 在左邊的選單下 **存取清單** 選擇 **延伸。**按一下 **新增擴展訪問清單。**

填寫「名**稱」**欄位。在本例中，名稱為flow_export_acl。按一下**Add**按鈕。配置訪**問控制**條目以匹配特定流量。

在本範例中，從主機10.10.10.1到任何目的地的流量以及主機172.16.0.20和192.168.1.20之間的流量都排除在外。包括任何其他流量。



Name: flow_export_acl

Entries (3)

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	Any	Any	Any	Any

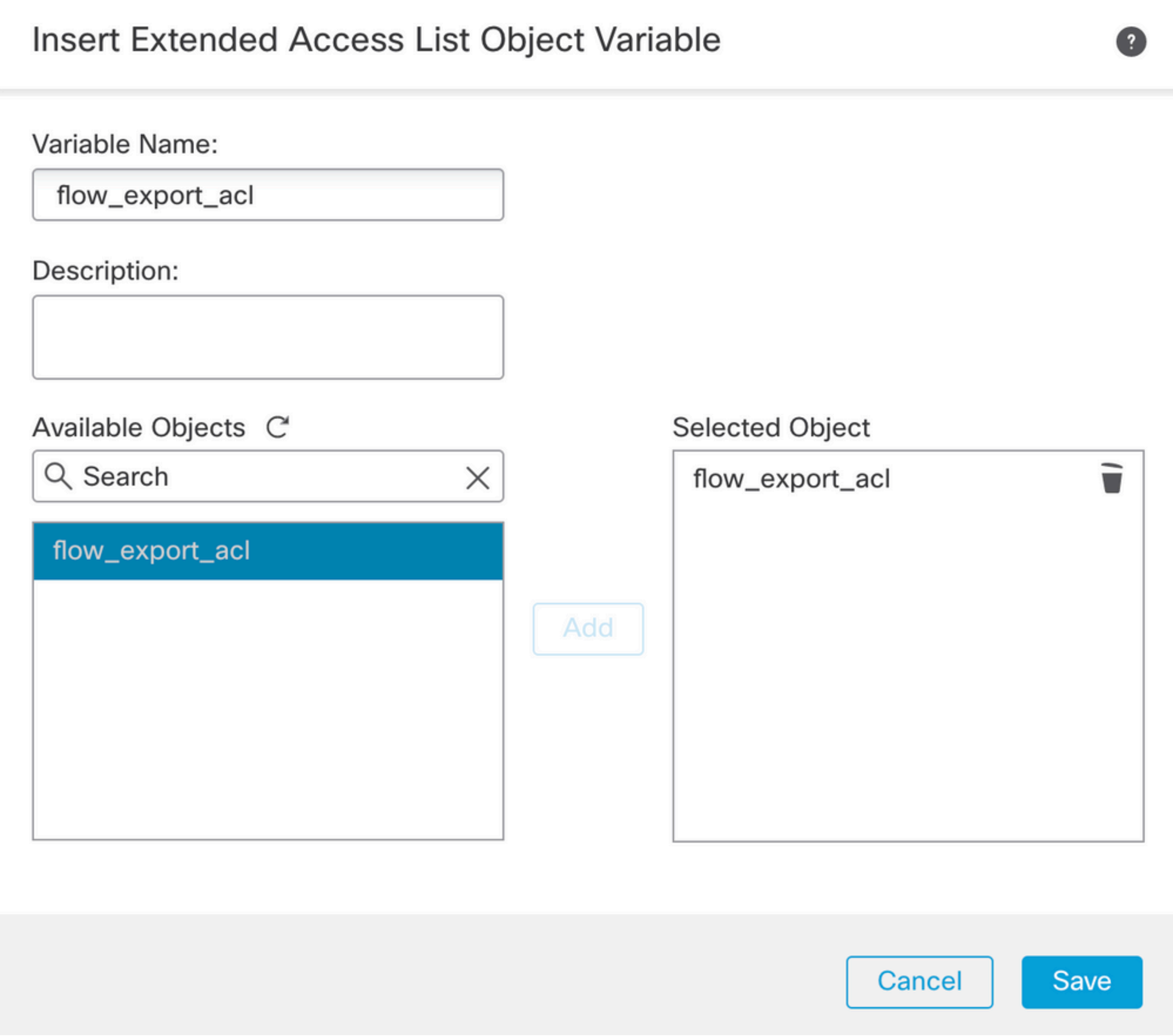
☐ Allow Overrides

步驟3.配置FlexConfig對象。

若要設定FlexConfig物件，請導覽至**物件** > **FlexConfig** > **FlexConfig**物件，然後按一下**Add FlexConfig Object**按鈕。

定義標識需要為其匯出NetFlow事件的流量的類對映。 在本示例中，對象的名稱為flow_export_class。

選擇步驟2中建立的訪問清單。按一下**Insert** > **Insert Policy Object** > **Extended ACL Object**，然後分配名稱。然後，按一下**Add**按鈕。在本例中，變數的名稱為flow_export_acl。按一下「**Save**」。


Insert Extended Access List Object Variable

Variable Name: flow_export_acl

Description:

Available Objects

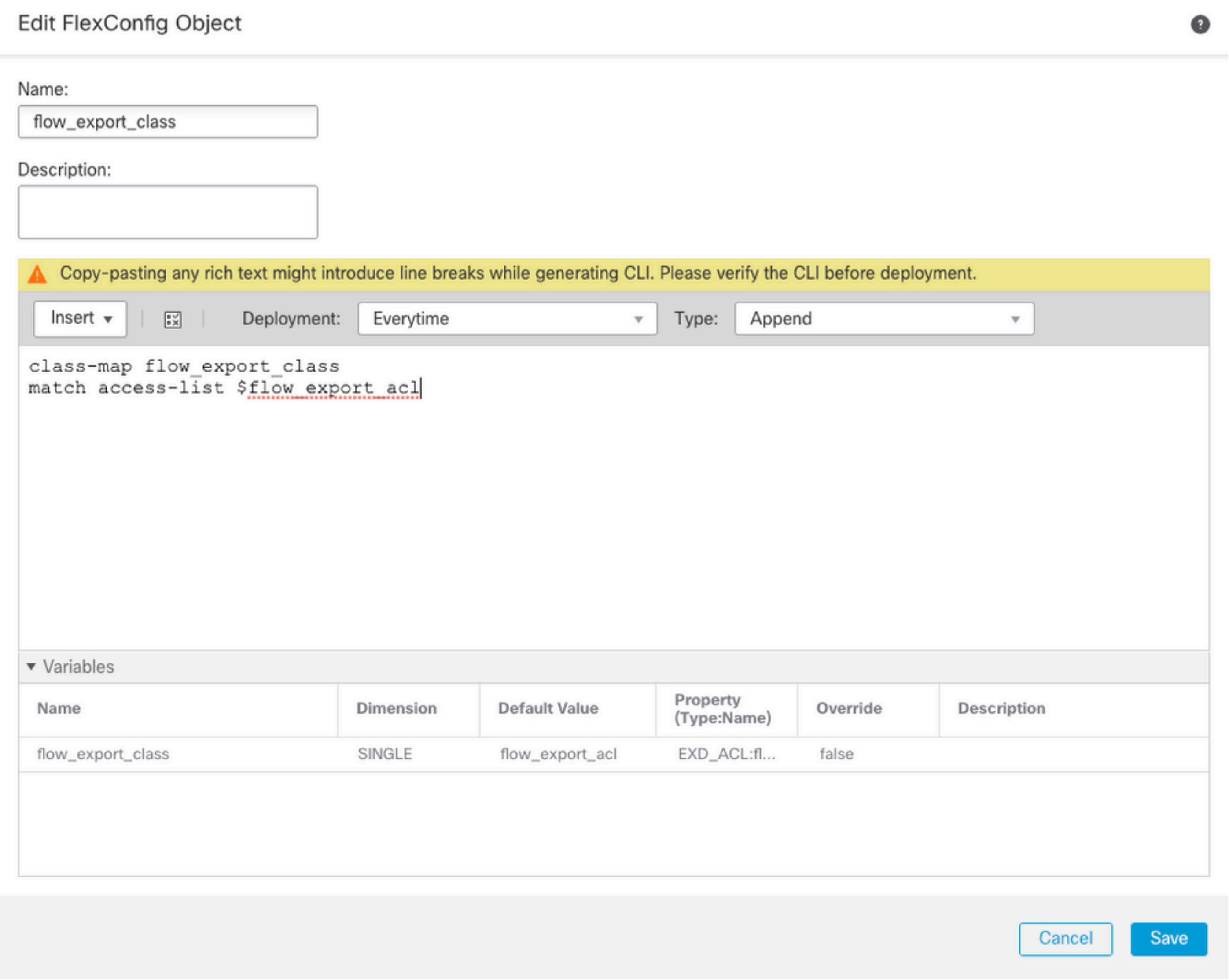
Selected Object: flow_export_acl

在右側空白欄位中新增後續配置行，並將先前定義的變量($**flow_export_acl.**)包括在match access-list配置行中。

請注意， **美元** 符號以變數名稱開頭。這有助於定義變數緊跟在它之後。

```
class-map flow_export_class
match access-list $flow_export_acl
```

完成後按一下**Save**。



Name: flow_export_class

Description:

Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.

Deployment: Everytime

Type: Append

```
class-map flow_export_class
match access-list $flow_export_acl
```

▾ Variables

Name	Dimension	Default Value	Property (Type:Name)	Override	Description
flow_export_class	SINGLE	flow_export_acl	EXD_ACL:fl...	false	

步驟4.配置Netflow目標

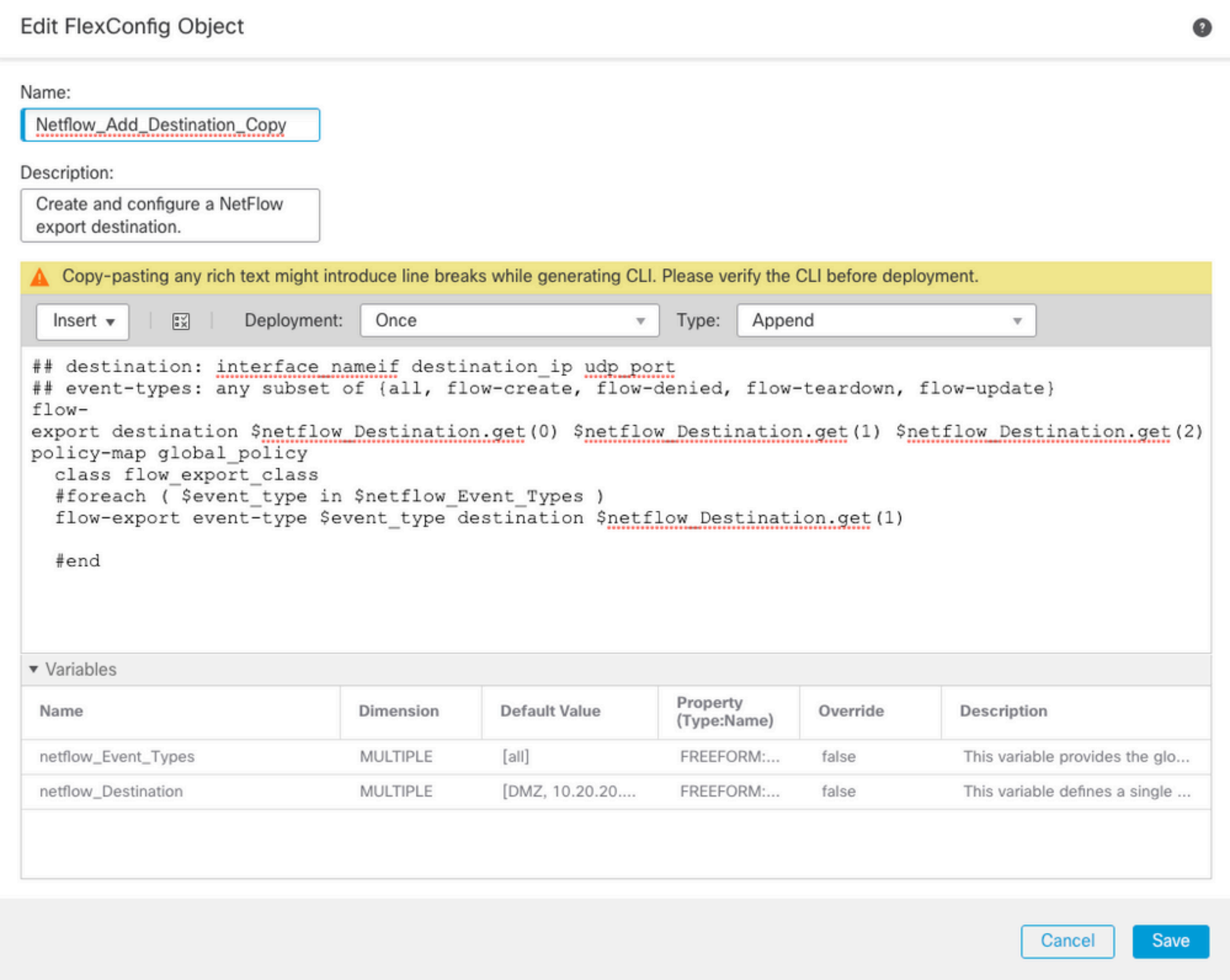
若要設定Netflow目的地，請導覽至**對象** > **FlexConfig** > **FlexConfig**對象，然後由Netflow進行過濾。**復制對象Netflow_Add_Destination。**系統將建立Netflow_Add_Destination_Copy。

分配在步驟3中建立的類。可以建立新的策略對映以將流匯出操作應用於已定義的類。

在本示例中，類插入到當前策略（全域性策略）中。

```
## 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
```

完成後按一下**Save**。



Edit FlexConfig Object

Name: Netflow_Add_Destination_Copy

Description: Create and configure a NetFlow export destination.

⚠ Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.

Deployment: Once

Type: Append

```
## 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
```

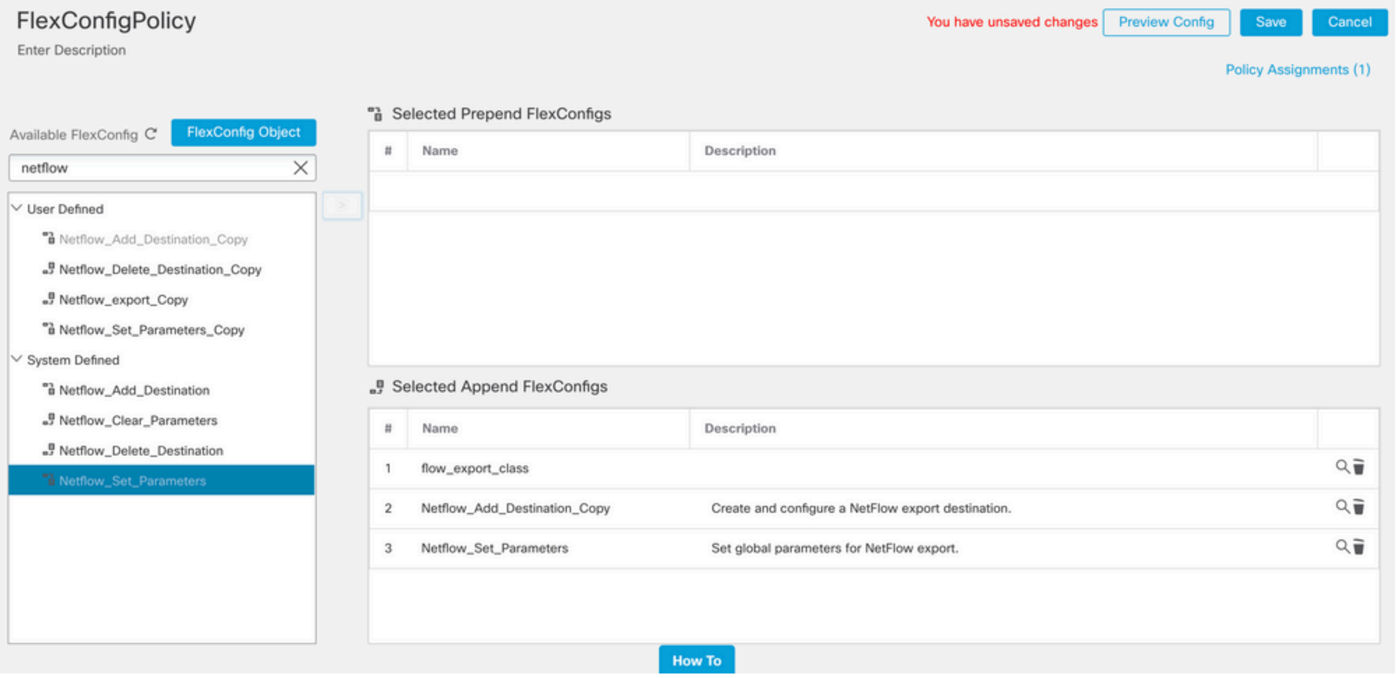
▾ Variables

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 ...

步驟5.將FlexConfig原則分配到FTD

導覽至**Devices > FlexConfig**，然後建立一個新原則（除非已經有一個原則是為其他用途建立並已指定給同一個FTD）。在本示例中，已建立FlexConfig。編輯FlexConfig策略並**選擇**在以上步驟中建立的FlexConfig對象。

在此示例中，使用預設的Netflow匯出引數，因此選擇了Netflow_Set_Parameters。 **儲存更改並部署。**



FlexConfigPolicy

Enter Description

You have unsaved changes

Policy Assignments (1)

Available FlexConfig: netflow

- User Defined
  - Netflow_Add_Destination_Copy
  - Netflow_Delete_Destination_Copy
  - Netflow_export_Copy
  - Netflow_Set_Parameters_Copy
- System Defined
  - Netflow_Add_Destination
  - Netflow_Clear_Parameters
  - Netflow_Delete_Destination
  - Netflow_Set_Parameters

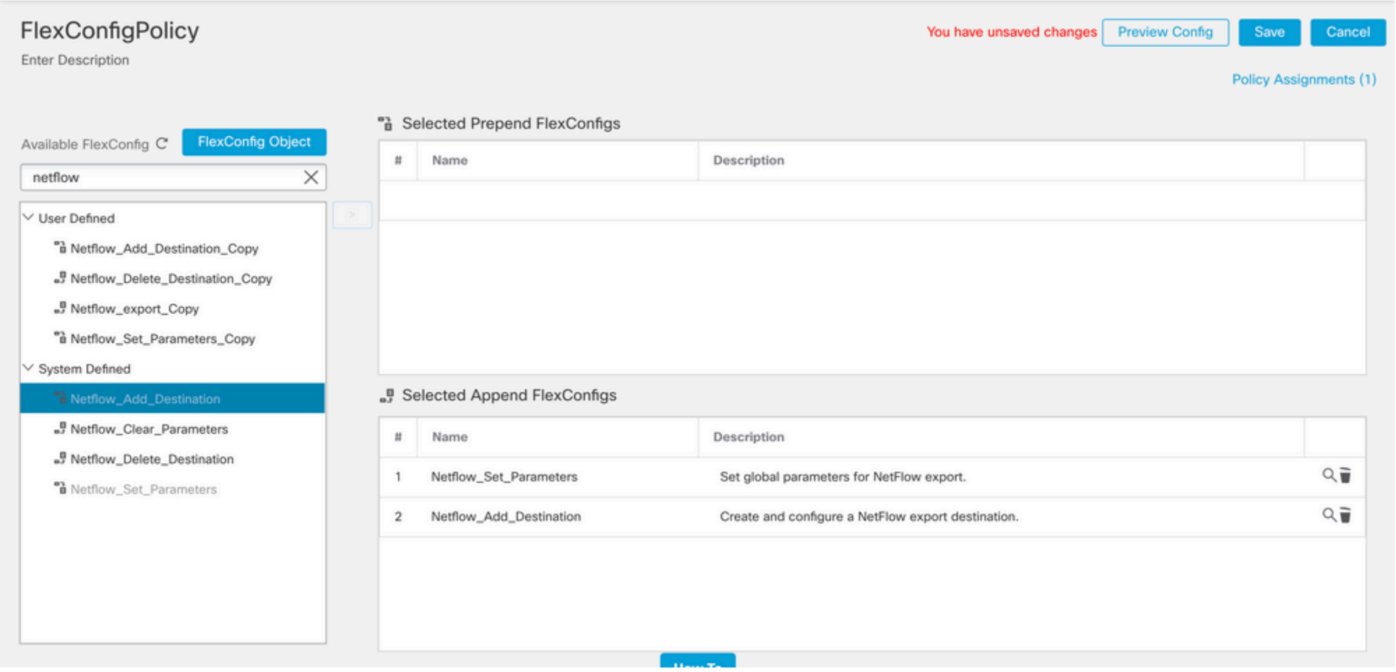
Selected Prepend FlexConfigs

#	Name	Description

Selected Append FlexConfigs

#	Name	Description
1	flow_export_class	
2	Netflow_Add_Destination_Copy	Create and configure a NetFlow export destination.
3	Netflow_Set_Parameters	Set global parameters for NetFlow export.

注意：為了匹配所有流量而不需要匹配特定流量，您可以從步驟2跳到步驟4，並使用預定義的NetFlow對象。



FlexConfigPolicy

Enter Description

You have unsaved changes

Policy Assignments (1)

Available FlexConfig: netflow

- User Defined
  - Netflow_Add_Destination_Copy
  - Netflow_Delete_Destination_Copy
  - Netflow_export_Copy
  - Netflow_Set_Parameters_Copy
- System Defined
  - Netflow_Add_Destination
  - Netflow_Clear_Parameters
  - Netflow_Delete_Destination
  - Netflow_Set_Parameters

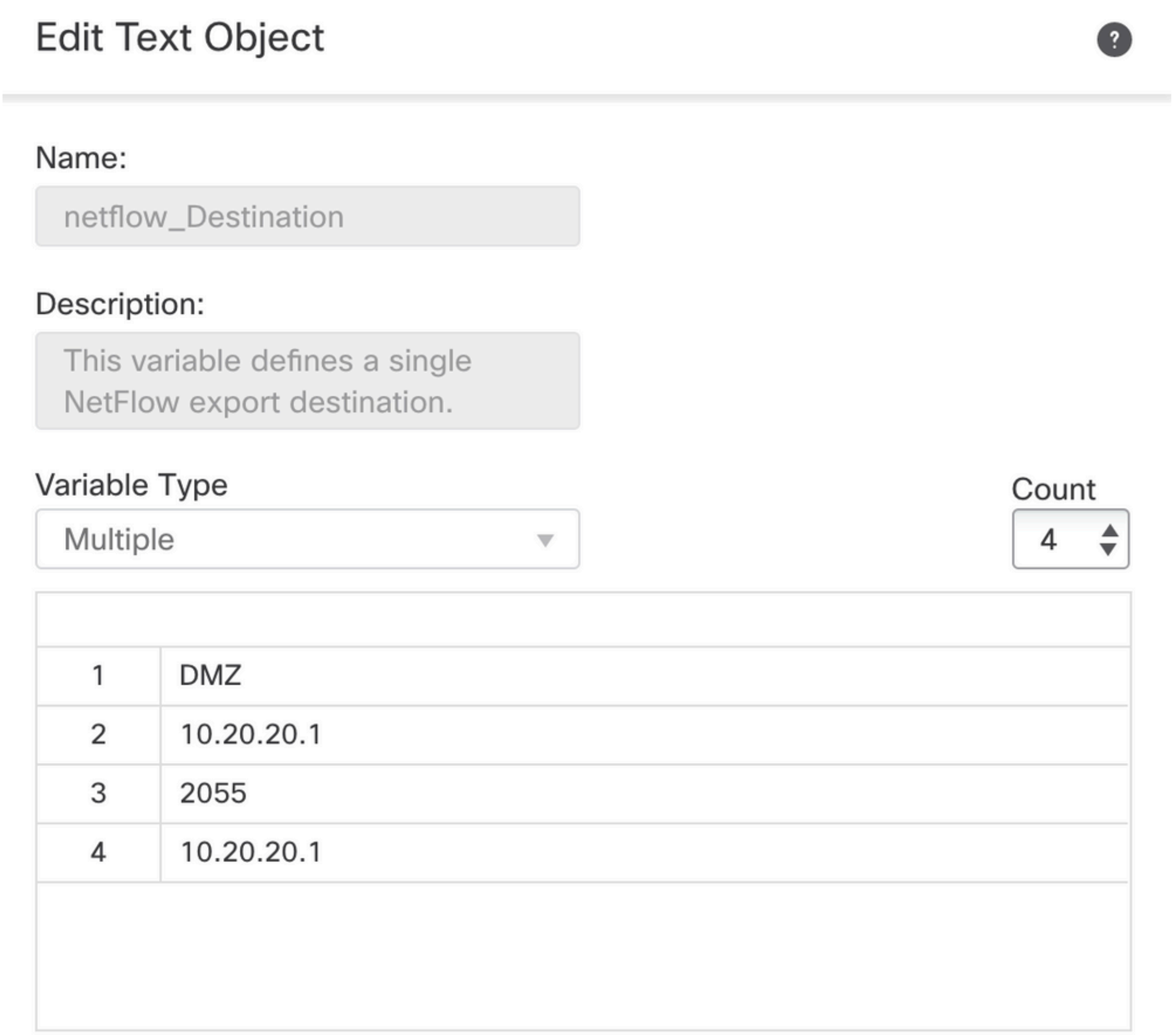
Selected Prepend FlexConfigs

#	Name	Description

Selected Append FlexConfigs

#	Name	Description
1	Netflow_Set_Parameters	Set global parameters for NetFlow export.
2	Netflow_Add_Destination	Create and configure a NetFlow export destination.

注意：新增第二個NSEL收集器，將NetFlow資料包傳送到該收集器。在步驟1中，新增4個變數以新增第二個Netflow收集器IP地址。



Edit Text Object

Name:

netflow_Destination

Description:

This variable defines a single NetFlow export destination.

Variable Type

Multiple

Count

4

1	DMZ
2	10.20.20.1
3	2055
4	10.20.20.1

在第4步中，新增配置行：flow-export destination $netflow_Destination.get(0)$netflow_Destination.get(1)$netflow_Destination.get(2)

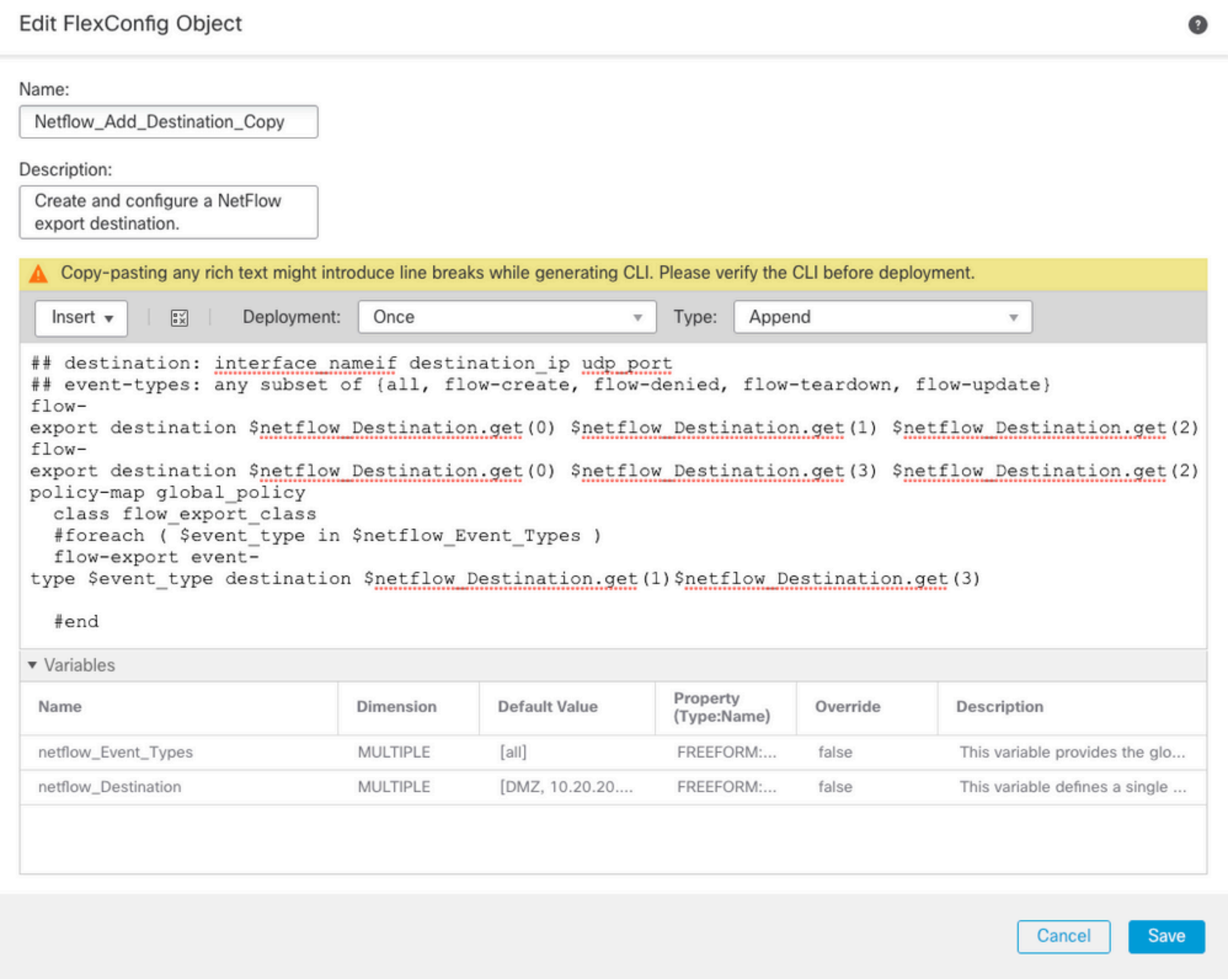
編輯對應變數的變數$netflow_Destination.get。在此示例中，變數值為3。例如：

```
flow-export destination $netflow_Destination.get(0) $netflow_Destination.get(1) $netflow_Destination.get(2)
flow-export destination $netflow_Destination.get(0) $netflow_Destination.get(3) $netflow_Destination.get(2)
```

此外，在配置行中新增第二個變數$netflow_Destination.get: flow-export event-type $event_type destination $netflow_Destination.get(1)。例如：

```
flow-export event-type $event_type destination $netflow_Destination.get(1) $netflow_Destination.get(3)
```

驗證此組態，如下圖所示：



Name: Netflow_Add_Destination_Copy

Description: Create and configure a NetFlow export destination.

⚠ Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.

Deployment: Once ▾ Type: Append ▾

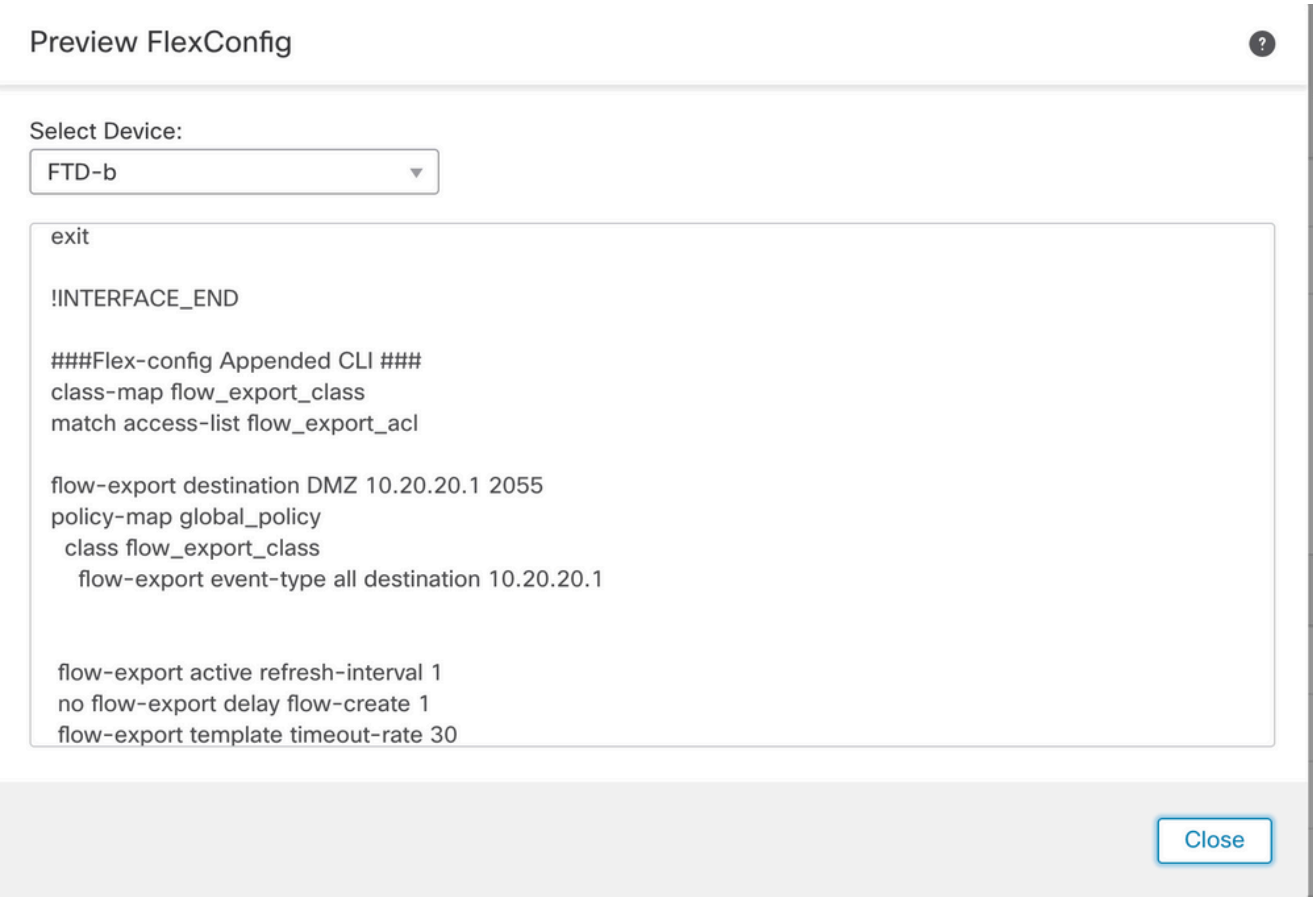
```
## destination: interface_nameif destination_ip udp_port
## event-types: any subset of {all, flow-create, flow-denied, flow-teardown, flow-update}
flow-
export destination $netflow_Destination.get(0) $netflow_Destination.get(1) $netflow_Destination.get(2)
flow-
export destination $netflow_Destination.get(0) $netflow_Destination.get(3) $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 $netflow_Destination.get(1)$netflow_Destination.get(3)

  #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 ...

驗證

可以在FlexConfig策略中驗證NetFlow配置。若要預覽配置，請按一下**Preview Config**。**選擇**FTD並驗證設定。



FTD-b

```
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
```

透過安全殼層(SSH)存取FTD，並使用system support diagnostic-cli指令來運行以下指令：

```
> 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
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
```

相關資訊

- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。