Firepower Threat DefenseでのNetFlowセキュアイベントロギングの設定

内容

[概要](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[背景説明](#)
[設定](#)
[確認](#)
[関連情報](#)

概要

このドキュメントでは、Firepower Management Center(FMC)を介してFirepower Threat Defense(FTD)でNetFlowセキュアイベントロギング(NSEL)を設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- FMCの知識
- FTDの知識
- FlexConfigポリシーの知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- FTDバージョン6.6.1
- FMCバージョン6.6.1

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

このドキュメントでは、Firepower Management Center(FMC)を介してFirepower Threat Defense(FTD)でNetFlowセキュアイベントロギング(NSEL)を設定する方法について説明します。

FlexConfigテキストオブジェクトは、定義済みのFlexConfigオブジェクトで使用される変数に関連

付けられます。NSELを設定するために、定義済みのFlexConfigオブジェクトおよび関連するテキストオブジェクトがFMCに用意されています。FMC内には4つの定義済みFlexConfigオブジェクトと3つの定義済みテキストオブジェクトがあります。定義済みのFlexConfigオブジェクトは読み取り専用であり、変更できません。NetFlowのパラメータを変更するために、オブジェクトをコピーできます。

次の表に、4つの定義済みオブジェクトを示します。

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

定義済みの3つの文字オブジェクトを表に示します。

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.

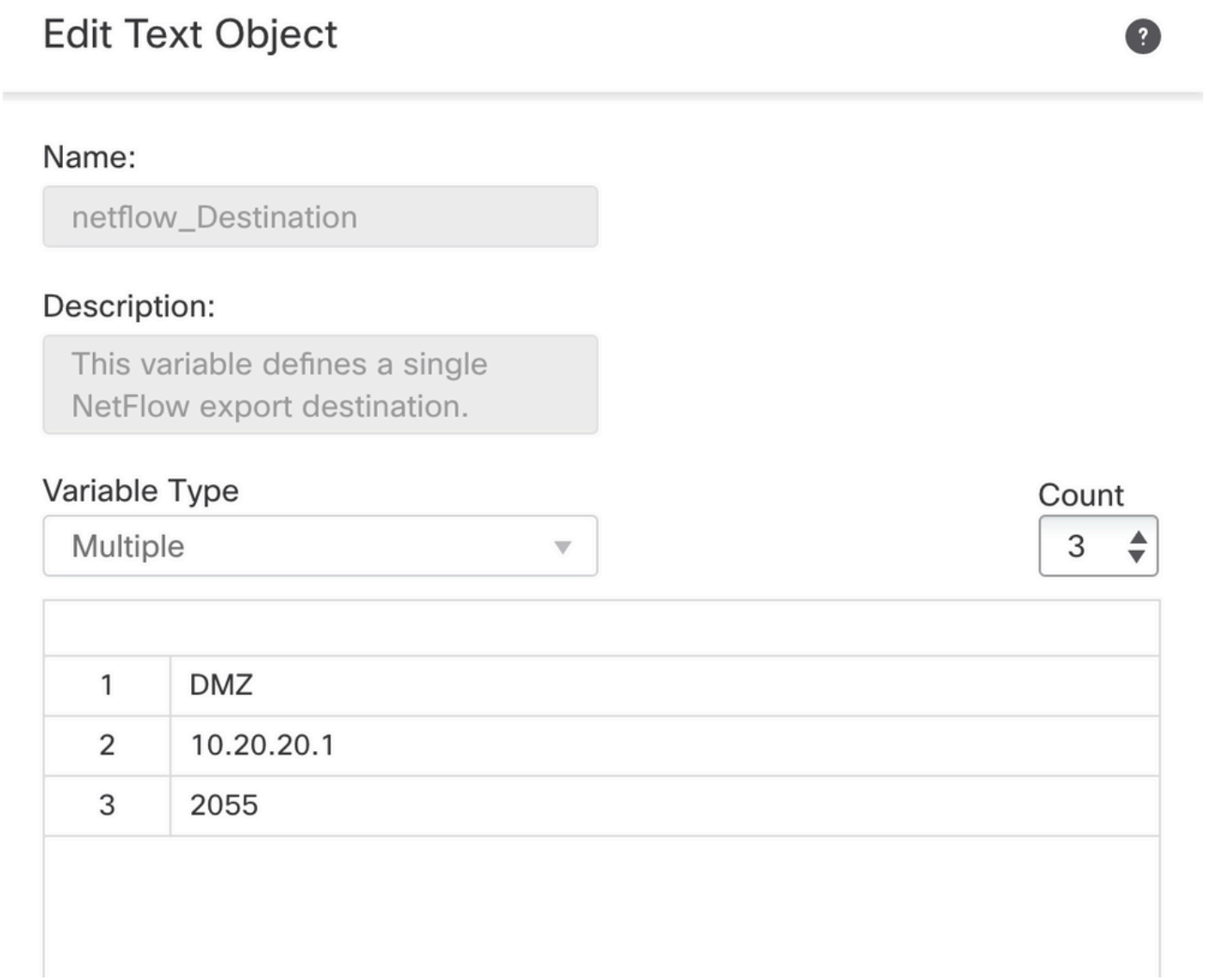
設定

このセクションでは、FlexConfigポリシーを使用してFMCでNSELを設定する方法について説明します。

ステップ 1：Netflowのテキストオブジェクトのパラメータを設定します。

変数パラメータを設定するには、[Objects] > [FlexConfig] > [Text Objects] に移動します。netflow_Destinationオブジェクトを編集します。複数の変数のタイプとカウントを3に設定します。インターフェイス名、宛先IPアドレス、およびポートを設定します。

この設定例では、インターフェイスはDMZ、NetFlow CollectorのIPアドレスは10.20.20.1、UDPポートは2055です。



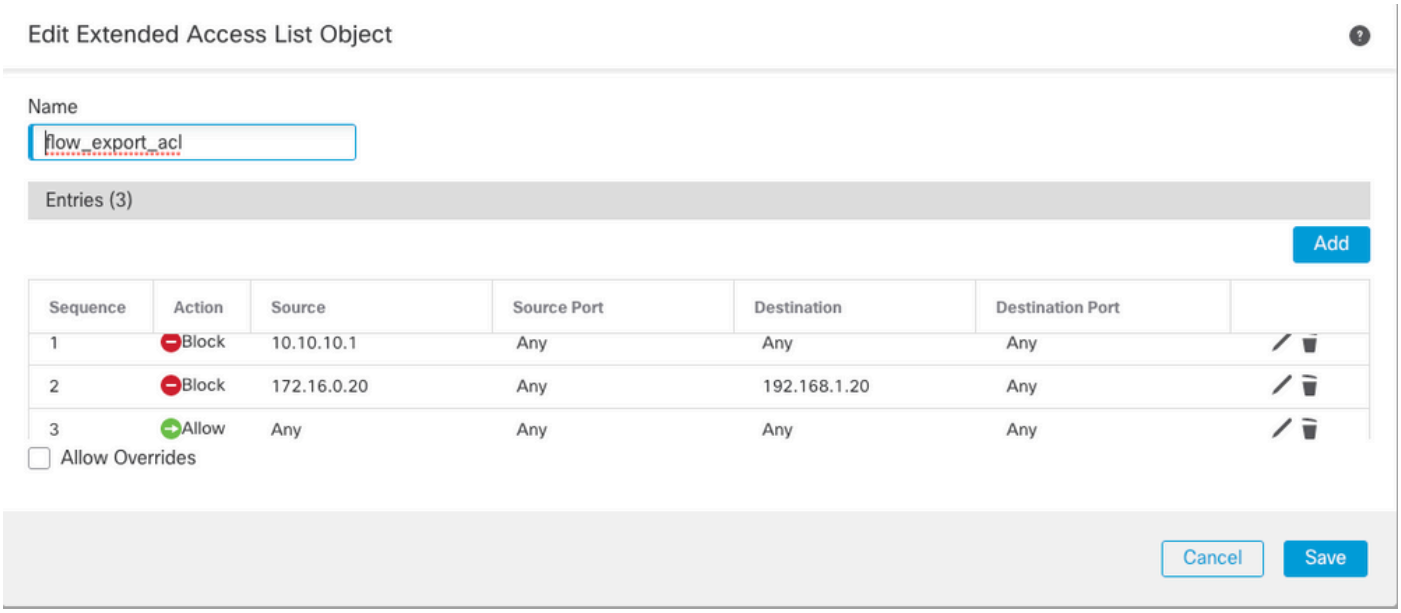
注:netflow_Event_Typesおよびnetflow_Parametersのデフォルト値が使用されます。

ステップ 2：特定のトラフィックに一致するように拡張アクセスリストオブジェクト(ACL)を設定します。

FMCで拡張アクセスリストを作成するには、 **Objects > Object Management** 左側のメニューの **Access List** 選択 **Extended.**クリック **拡張アクセスリストを追加します。**

[Name] フィールドに入力します。この例では、名前はflow_export_aclです。[Add] ボタンをクリックします。特定のトラフィック**に一致する**アクセスコントロールエントリを設定します。

この例では、ホスト10.10.10.1から任意の宛先へのトラフィックと、ホスト172.16.0.20と192.168.1.20の間のトラフィックが除外されます。その他のトラフィックも含まれます。

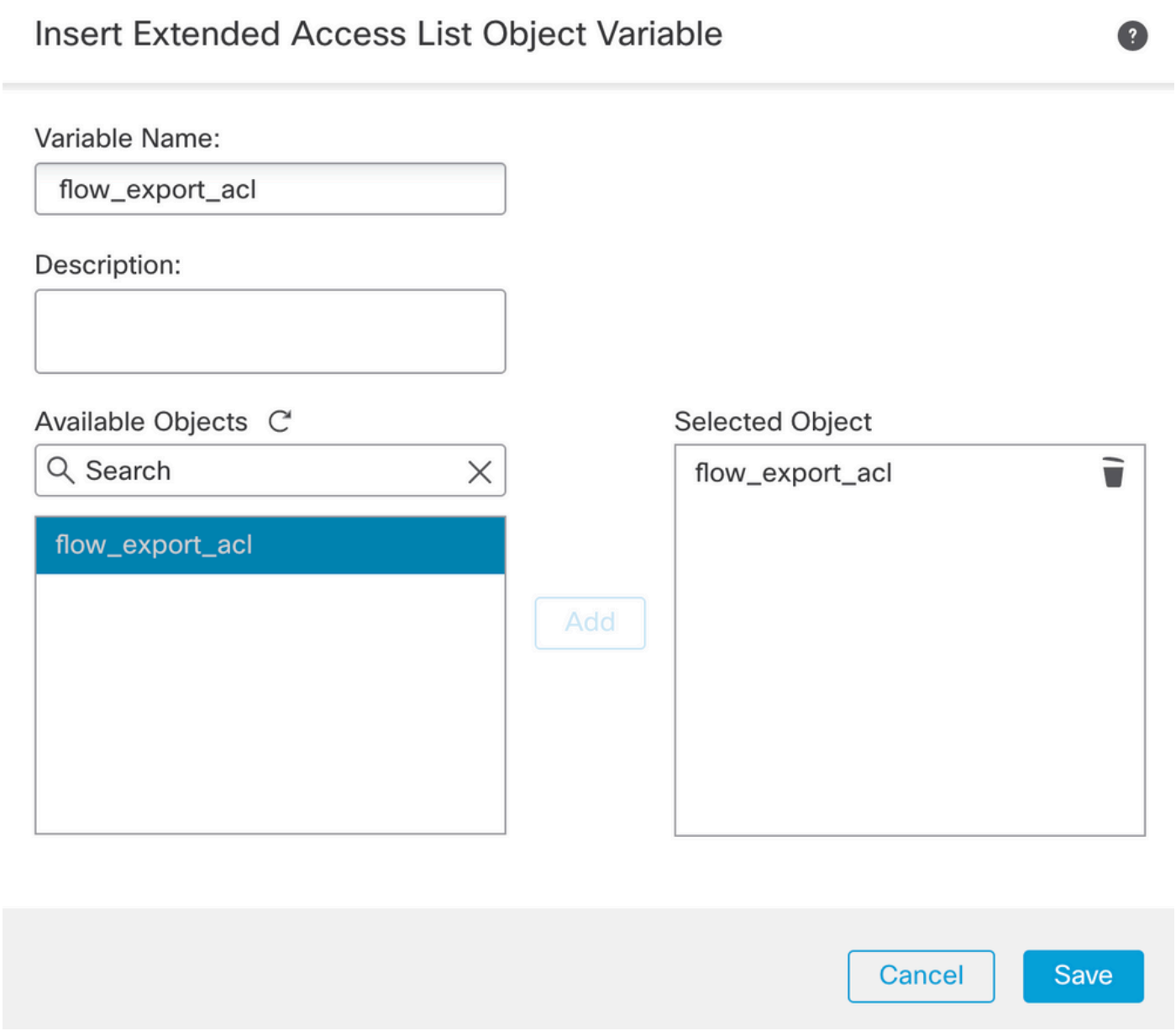


ステップ 3：FlexConfigオブジェクトを設定します。

FlexConfigオブジェクトを設定するには、[Objects] > [FlexConfig] > [FlexConfig] オブジェクトに移動し、[Add FlexConfig Object] ボタンをクリックします。

NetFlowイベントをエクスポートする必要があるトラフィックを識別するクラスマップを定義します。 この例では、オブジェクトの名前はflow_export_classです。

手順2で作成したアクセスリストを選択します。[Insert] > [Insert Policy Object] > [Extended ACL Object] をクリックし、名前を割り当てます。次に、**Add**ボタンをクリックします。この例では、変数の名前はflow_export_aclです。[Save] をクリックします。

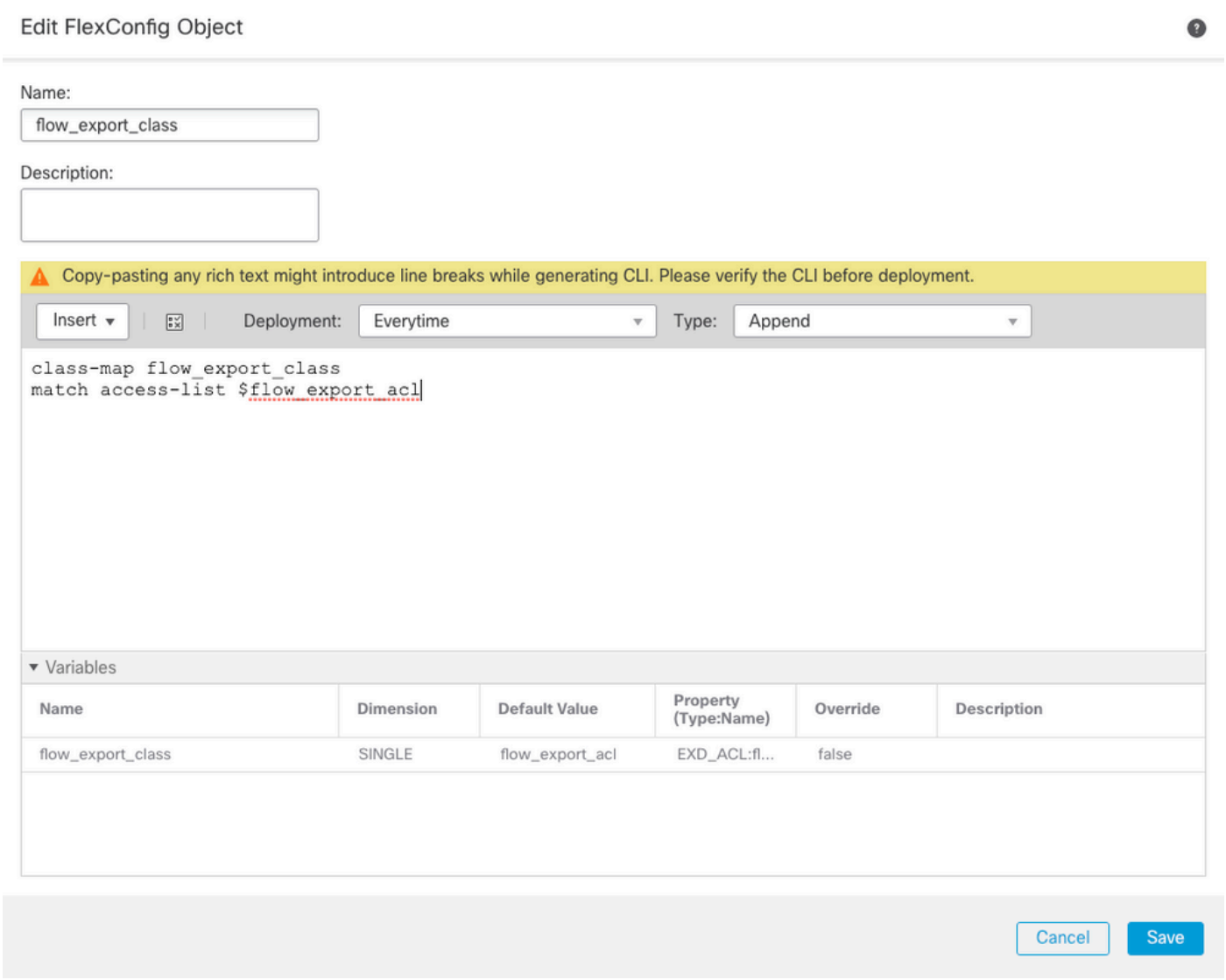


ブランクのフィールド右側に次の設定行を追加し、match access-list設定行に以前に定義した変数(**$flow_export_acl.**)を含めます。

次の点に注意してください。 $ symbolは変数名を開始します。これは、変数がその後に来ることを定義するのに役立ちます。

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

終了したら、[Save] をクリックします。



ステップ 4：Netflowの宛先の設定

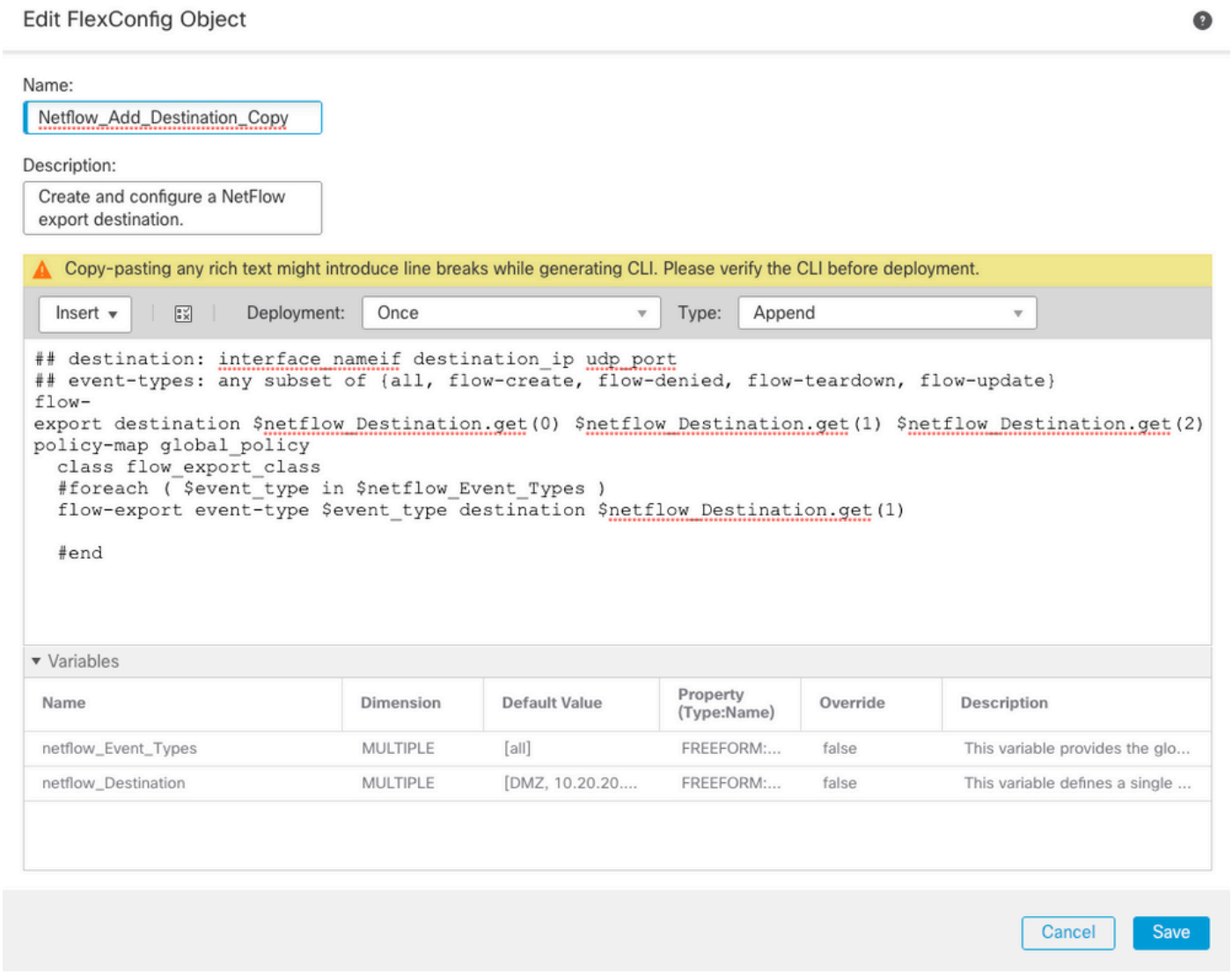
Netflowの宛先を設定するには、[Objects] > [FlexConfig] > [FlexConfig] オブジェクトに移動し、Netflowでフィルタリングします。**オブジェクトNetflow_Add_Destinationをコピーします。**Netflow_Add_Destination_Copyが作成されます。

手順3で作成したクラスを割り当てます。新しいポリシーマップを作成して、定義したクラスにフローエクスポートアクションを適用できます。

この例では、クラスは現在のポリシー（グローバルポリシー）に挿入されます。

```
## 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
```

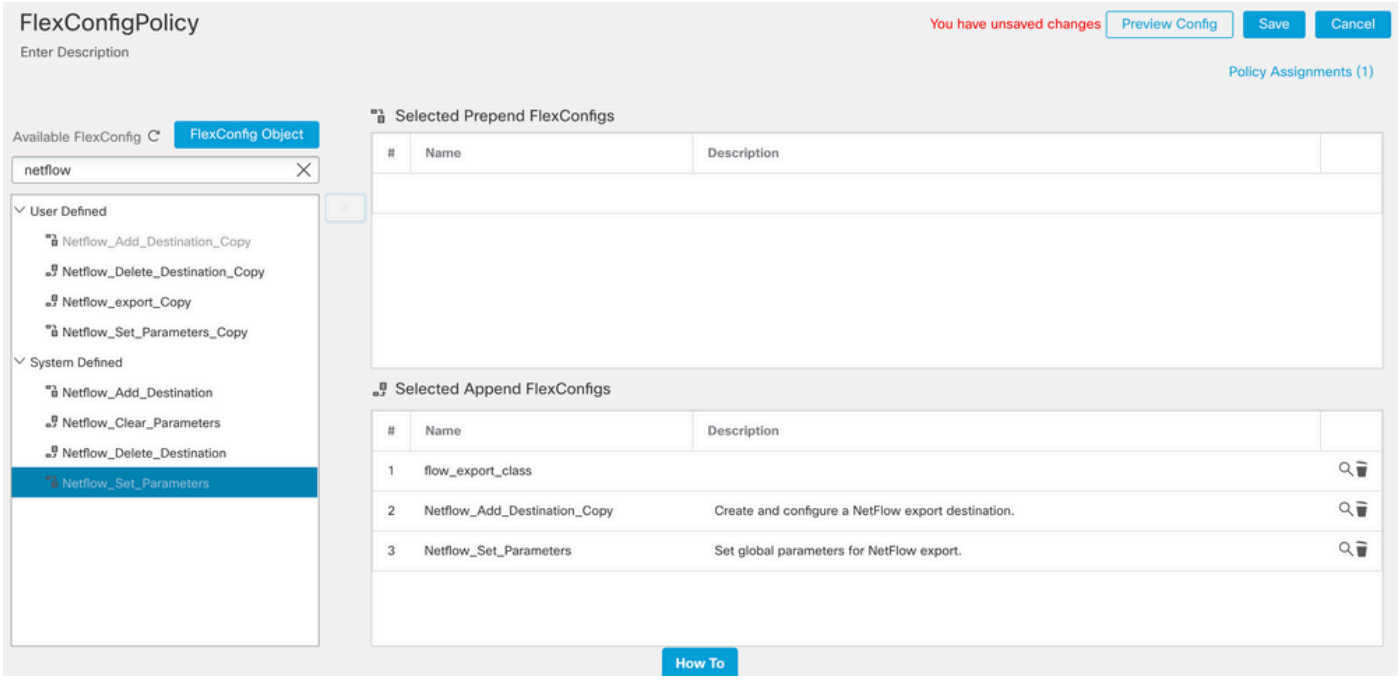
終了したら、[Save] をクリックします。



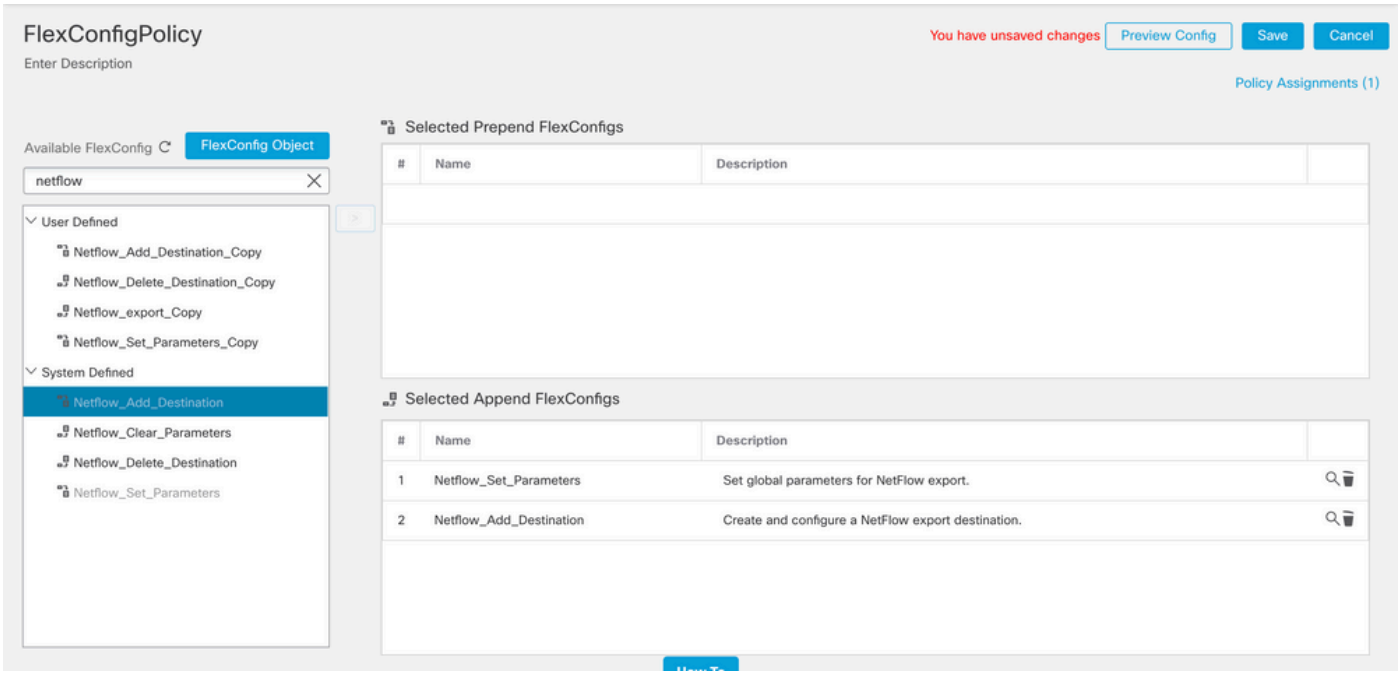
ステップ 5：FTDへのFlexConfigポリシーの割り当て

[Devices] > [FlexConfig] に移動し、新しいポリシーを作成します（別の目的で作成され、同じFTDに割り当てられたポリシーがすでに存在する場合を除く）。この例では、FlexConfigはすでに作成されています。FlexConfigポリシーを編集し、前の手順で作成したFlexConfigオブジェクトを**選択**します。

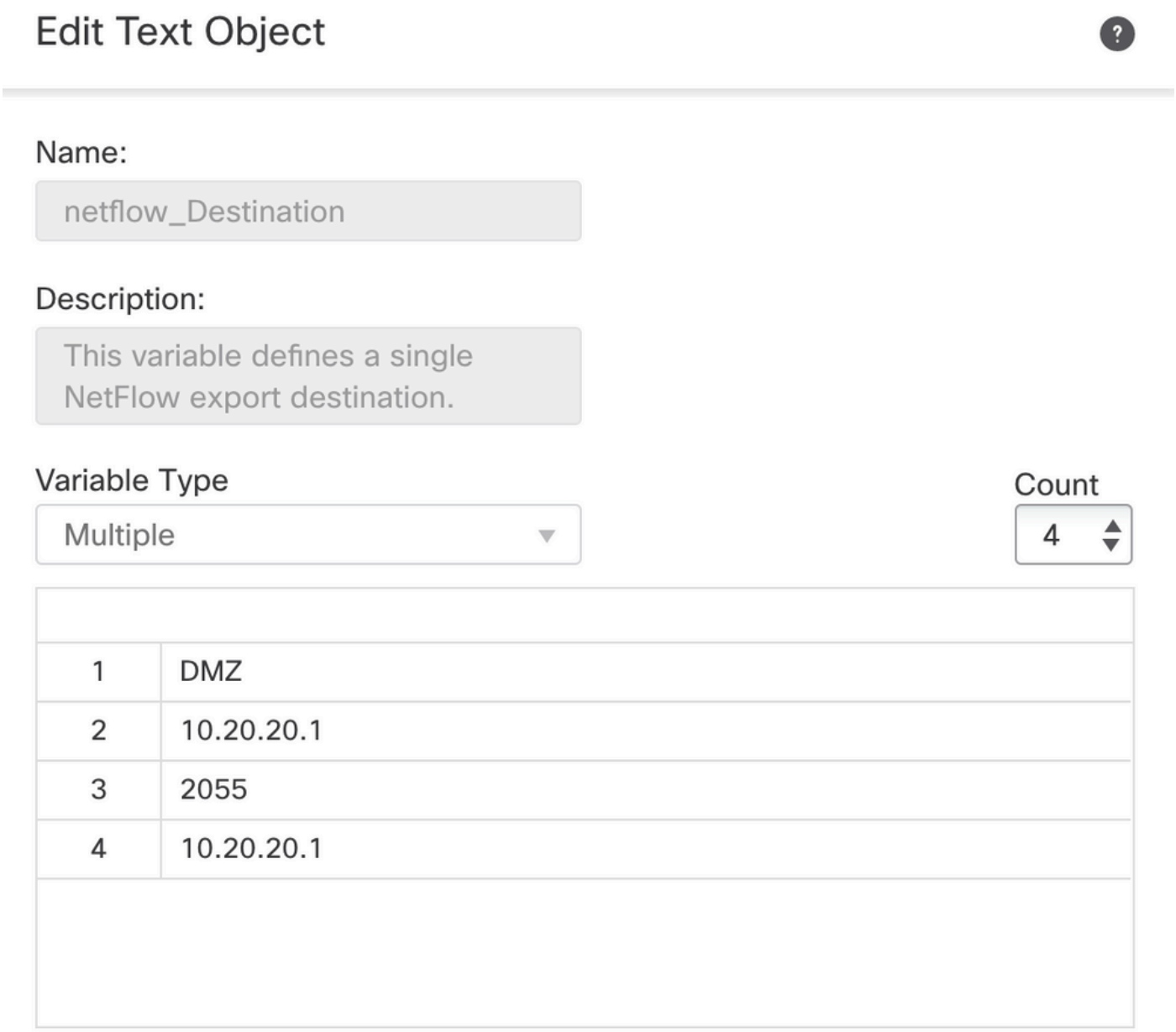
この例では、デフォルトのNetflowエクスポートパラメータが使用されるため、Netflow_Set_Parametersが選択されます。 **変更したファイルを保存し、展開します。**



注：特定のトラフィックを照合する必要なくすべてのトラフィックを照合するには、手順2 ～ 4を省略して、事前定義されたNetFlowオブジェクトを使用できます。



注:NetFlowパケットの送信先となる2番目のNSELコレクタを追加するには、次の手順を実行します。ステップ1では、4つの変数を追加して、2番目のNetflowコレクタのIPアドレスを追加します。



ステップ4:flow-export destination $netflow_Destination.get(0) $netflow_Destination.get(1) $netflow_Destination.get(2)の設定行を追加します。

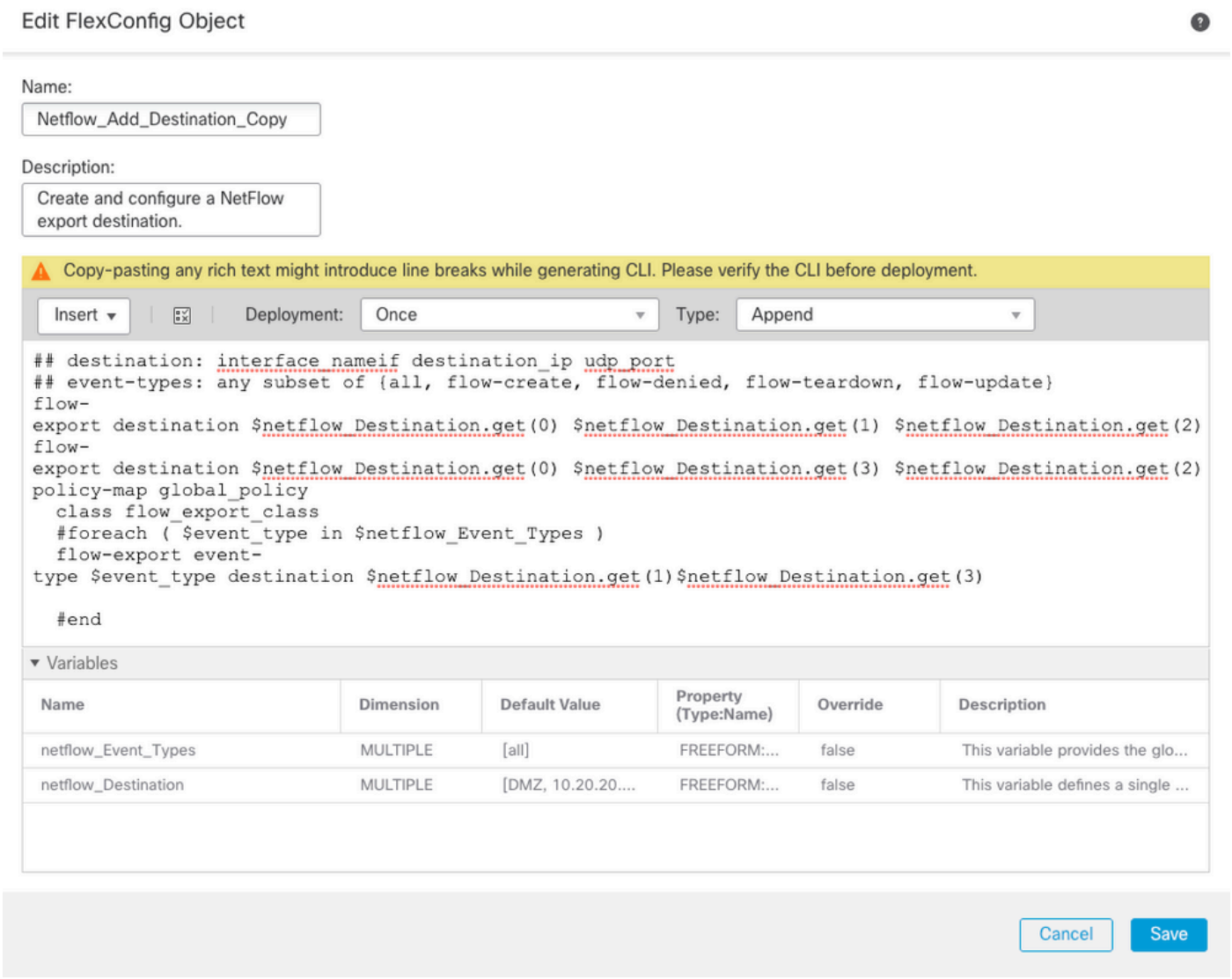
対応変数の変数$netflow_Destination.getを編集します。この例では、変数値は3です。以下に、いくつかの例を示します。

```
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)
```

また、2番目の変数$netflow_Destination.getを設定行に追加します。flow-export event-type $event_type destination $netflow_Destination.get(1)。以下に、いくつかの例を示します。

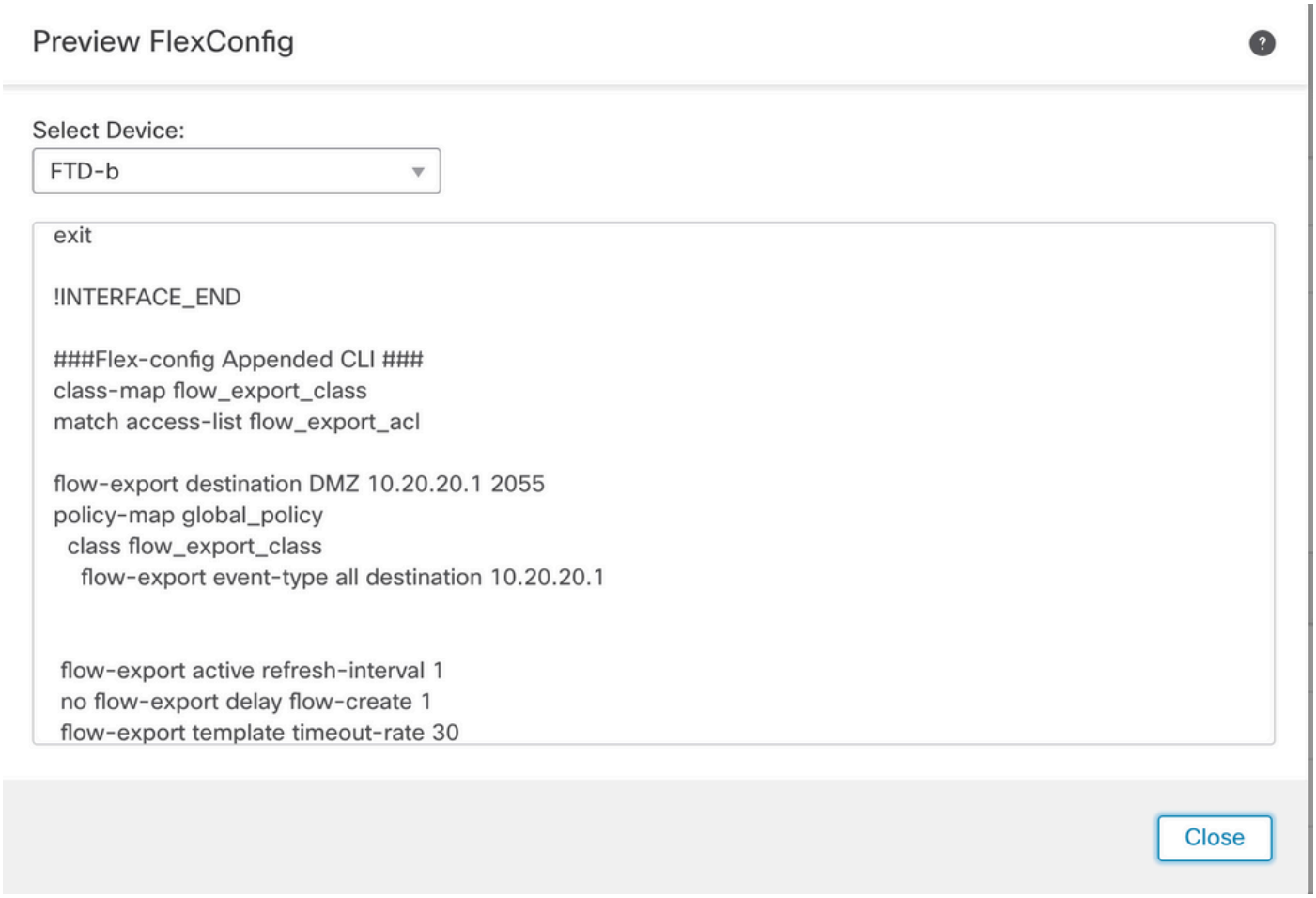
```
flow-export event-
type $event_type destination $netflow_Destination.get(1) $netflow_Destination.get(3)
```

次の図に示すように、**この設定を検証します。**



確認

NetFlowの設定は、FlexConfigポリシー内で確認できます。設定をプレビューするには、[Preview Config] をクリックします。**FTDを選**択し、設定を確認します。



セキュアシェル(SSH)を介してFTDにアクセスし、コマンドsystem support diagnostic-cliを使用して次のコマンドを実行します。

```
> 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
```

関連情報

- [シスコテクニカルサポートおよびダウンロード]

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。