Firepower Threat Defense에서 NetFlow 보안 이벤트 로깅 구성

목차

소개

이 문서에서는 FMC(Firepower Management Center)를 통해 FTD(Firepower Threat Defense)에서 NetFlow NSEL(Secure Event Logging)을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- FMC 지식
- FTD 지식
- FlexConfig 정책에 대한 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- FTD 버전 6.6.1
- FMC 버전 6.6.1

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

이 문서에서는 FMC(Firepower Management Center)를 통해 FTD(Firepower Threat Defense)에서 NetFlow NSEL(Secure Event Logging)을 구성하는 방법에 대해 설명합니다.

FlexConfig 텍스트 객체는 미리 정의된 FlexConfig 객체에 사용되는 변수와 연결됩니다. NSEL을 구성하기 위해 미리 정의된 FlexConfig 개체 및 관련 텍스트 개체가 FMC에 있습니다. FMC 내에는

4개의 사전 정의된 FlexConfig 객체와 3개의 사전 정의된 텍스트 객체가 있습니다. 미리 정의된 FlexConfig 개체는 읽기 전용이므로 수정할 수 없습니다. NetFlow의 매개변수를 수정하기 위해 객체를 복사할 수 있습니다.

미리 정의된 4개의 객체가 테이블에 나열됩니다.

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

다음 세 가지 사전 정의 텍스트 객체가 테이블에 나열됩니다.

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.

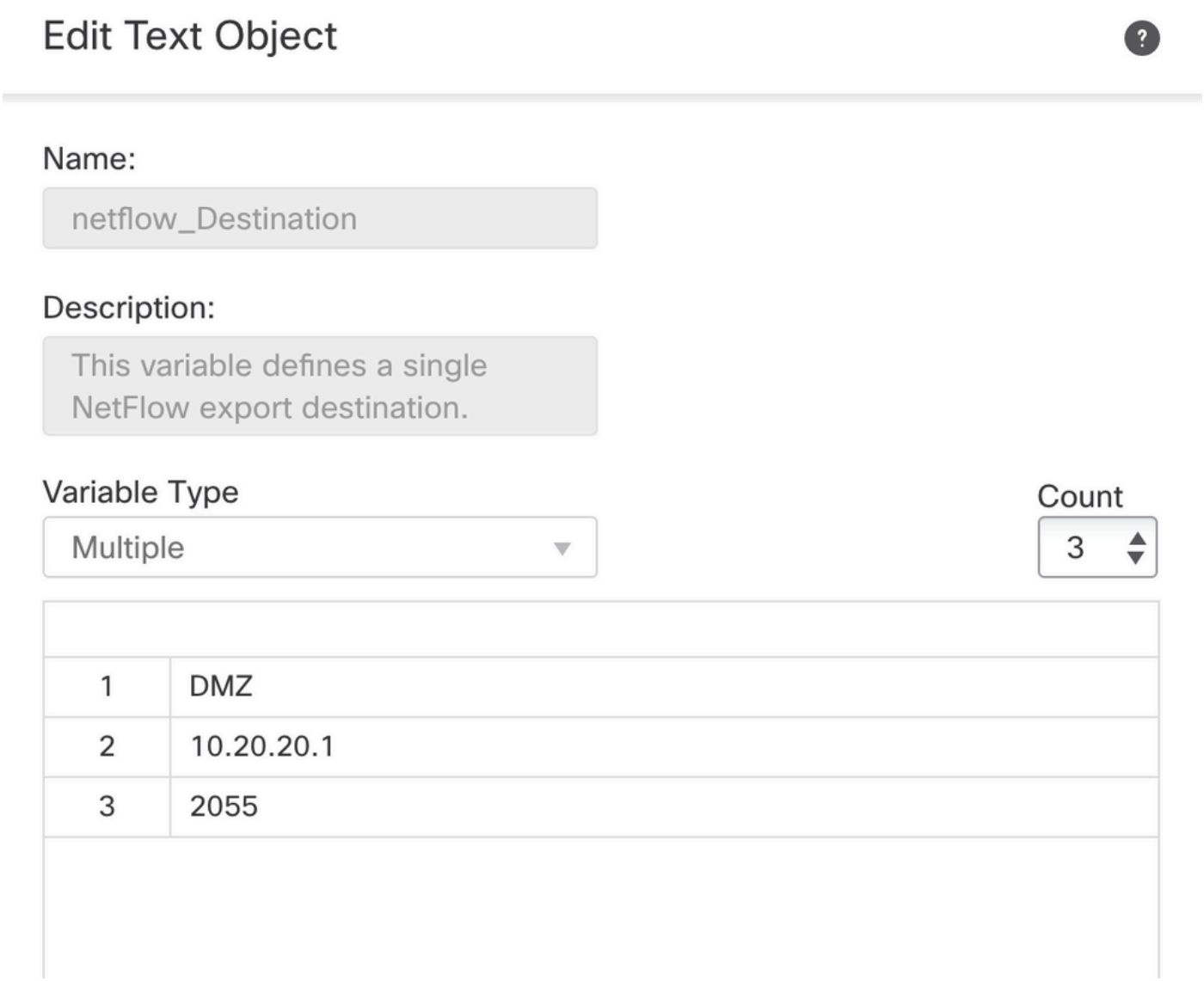
구성

이 섹션에서는 FlexConfig 정책을 통해 FMC에서 NSEL을 구성하는 방법에 대해 설명합니다.

1단계. Netflow에 대한 Text Objects의 매개변수를 설정합니다.

변수 매개 변수를 설정하려면 Objects > FlexConfig **> Text Objects로 이동합니다**.
netflow_Destination 객체를 편집합니다. 여러 변수 유형을 정의하고 count를 3으로 설정합니다. 인터페이스 이름, 대상 IP 주소 및 포트를 설정합니다.

이 컨피그레이션 예에서는 인터페이스가 DMZ이고, NetFlow 컬렉터 IP 주소가 10.20.20.1이며, UDP 포트가 2055입니다.



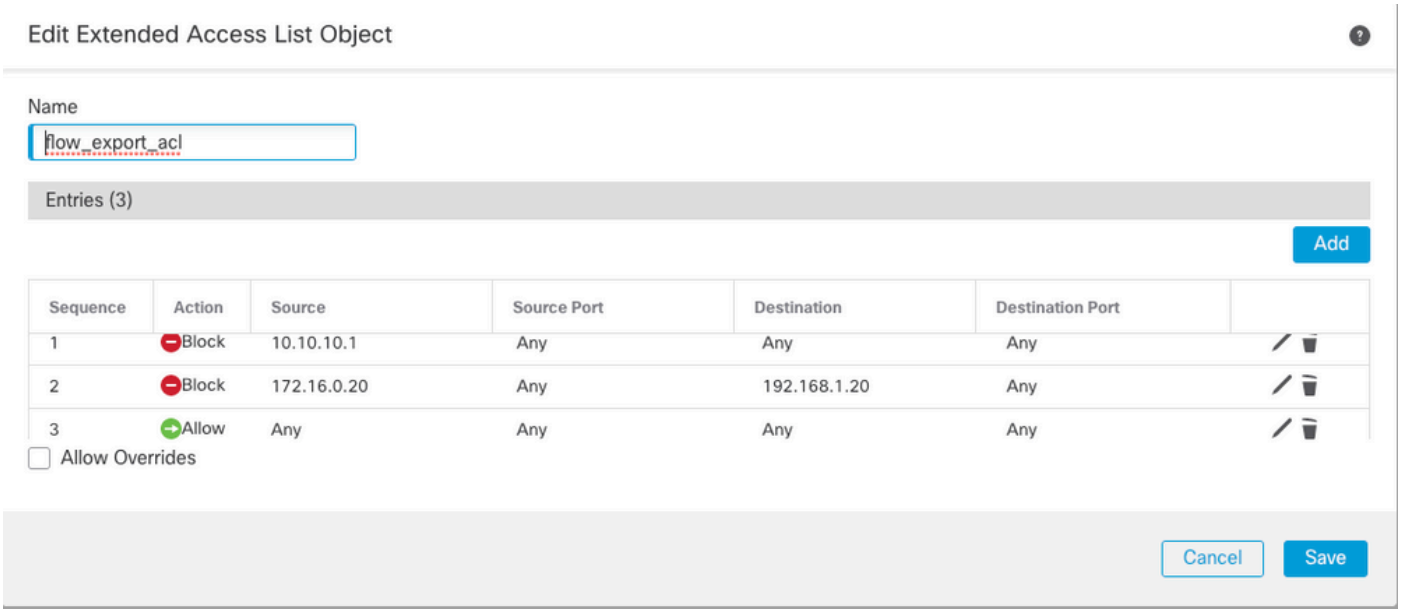
참고: netflow_Event_Types 및 netflow_Parameters의 기본값이 사용됩니다.

2단계. 특정 트래픽과 일치하도록 확장 액세스 목록 객체를 구성합니다.

FMC에서 확장 액세스 목록을 생성하려면 **객체 > 객체 관리** 왼쪽 메뉴에서 **액세스 목록** 선택 **확장** .클릭 **확장 액세스 목록을 추가합니다.**

Name(이름) 필드를 입력합니다. 이 예에서 이름은 flow_export_acl입니다. Add(추가) **버튼**을 클릭합니다. 특정 트래픽과 **일치하도록 액세스 제어** 항목을 구성합니다.

이 예에서는 호스트 10.10.10.1에서 임의의 목적지로 가는 트래픽과 호스트 172.16.0.20과 192.168.1.20 간의 트래픽은 제외됩니다. 기타 모든 트래픽이 포함됩니다.

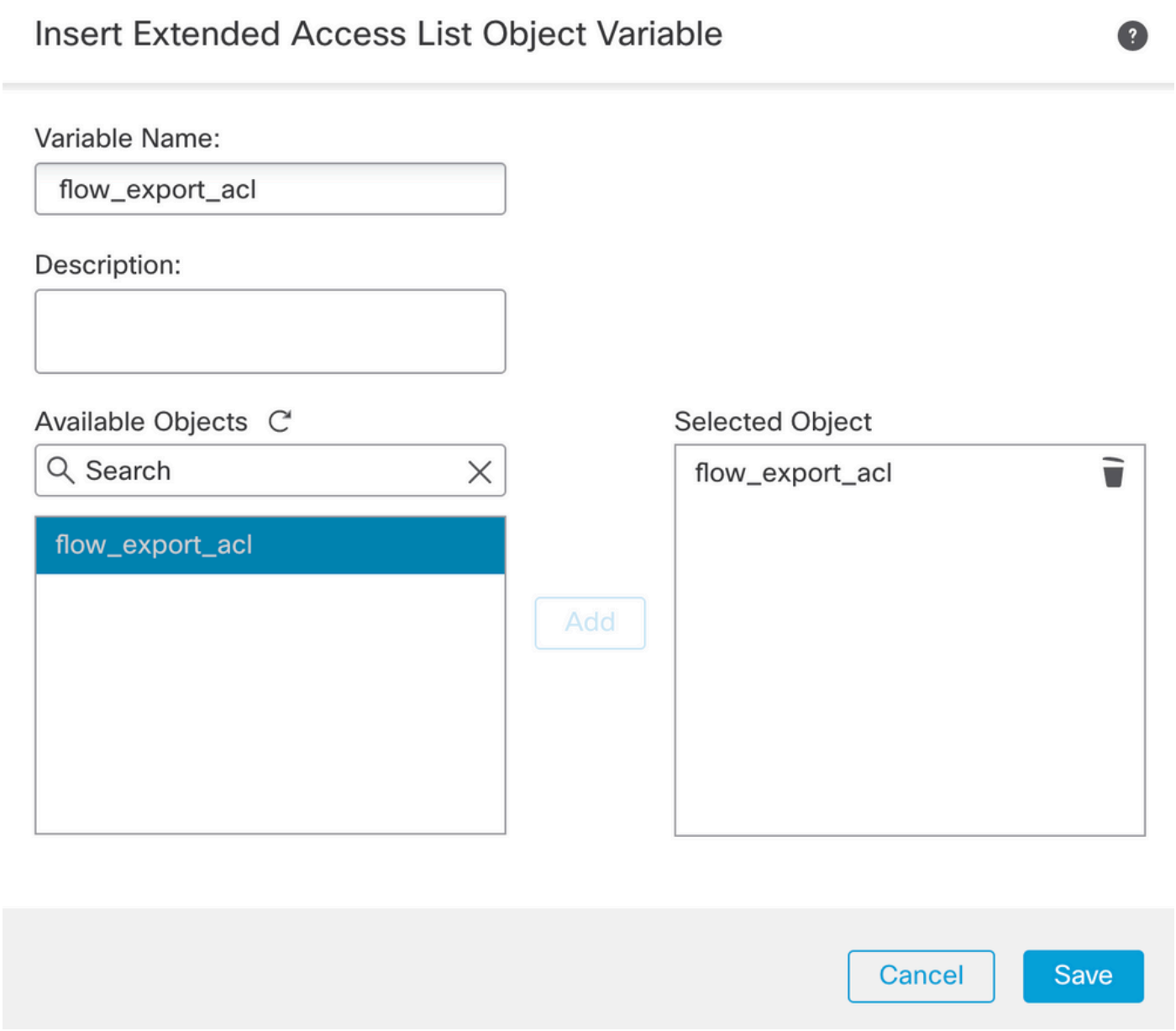


3단계. FlexConfig 개체를 구성합니다.

FlexConfig Objects(FlexConfig 개체)를 구성하려면 **Objects(개체) > FlexConfig** > FlexConfig Objects(**FlexConfig 개체)로** 이동하고 **Add FlexConfig Object(FlexConfig 개체 추가) 버튼을** 클릭합니다.

NetFlow 이벤트를 내보내야 하는 트래픽을 식별하는 클래스 맵을 정의합니다. 이 예에서 객체의 이름은 flow_export_class입니다.

2단계에서 생성한 액세스 목록을 **선택합니다**. Insert(**삽입) > Insert Policy Object(정책 개체 삽입) > Extended ACL Object(확장 ACL 개체)**를 클릭하고 이름을 할당합니다. 그런 다음 Add(추가) **버튼**을 클릭합니다. 이 예에서 변수의 이름은 flow_export_acl입니다. 저장을 **클릭합니다**.

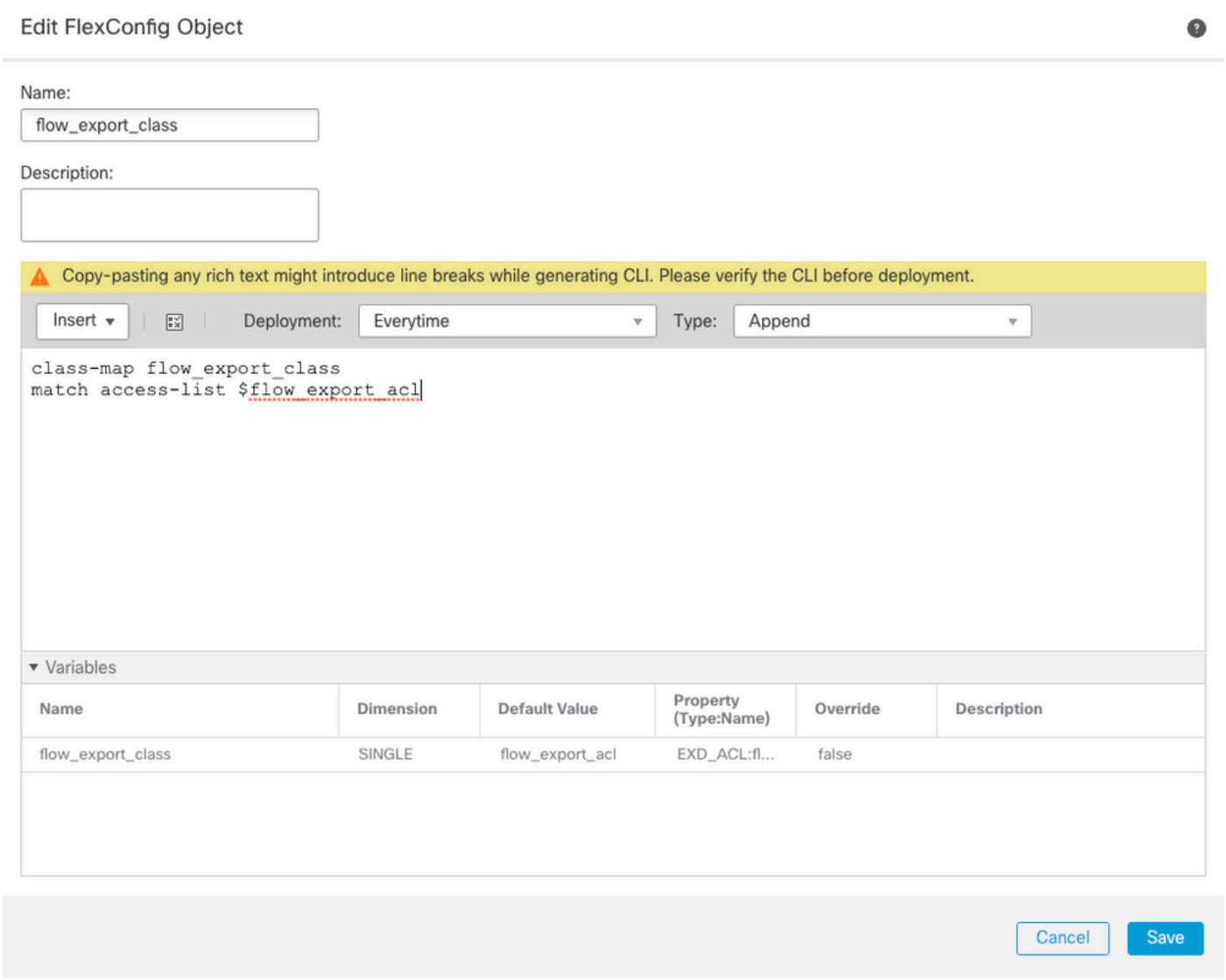


빈 필드 오른쪽에 다음 컨피그레이션 라인을 추가하고 이전에 정의한 변수(**$flow_export_acl.**)를 match access-list 컨피그레이션 라인에 포함합니다.

Cisco의 **$** 기호는 변수 이름을 시작합니다. 이렇게 하면 변수가 뒤에 오는 것을 정의할 수 있습니다 .

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

완료되면 Save(**저장**)를 클릭합니다.



4단계. Netflow 대상 구성

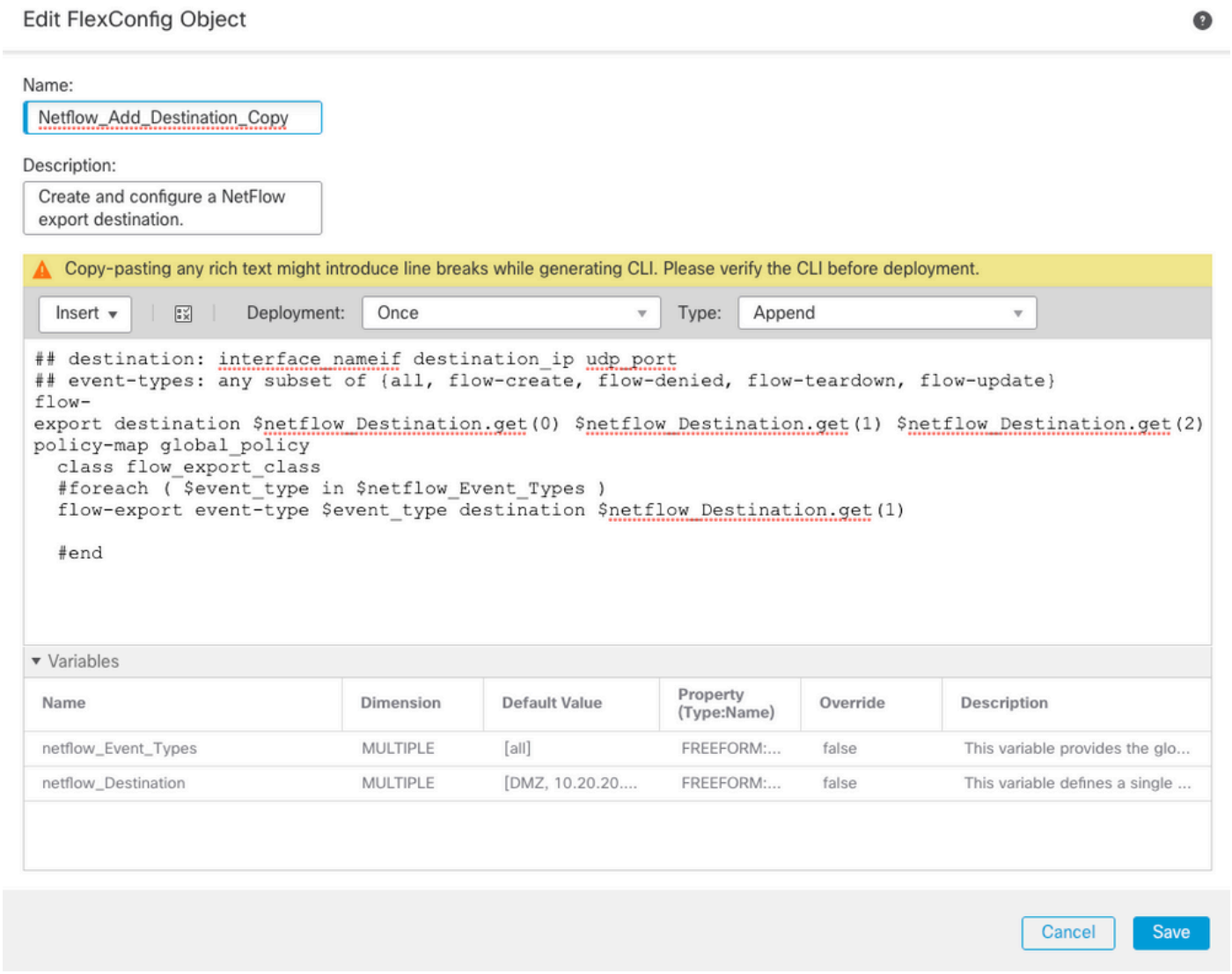
Netflow Destination을 구성하려면 Objects(개체) > FlexConfig > **FlexConfig Objects(FlexConfig 개체)로** 이동하고 Netflow로 필터링합니다. **Netflow**_Add_Destination 객체를 복사합니다. Netflow_Add_Destination_Copy가 생성됩니다.

3단계에서 생성한 클래스를 할당합니다. 정의된 클래스에 flow-export 작업을 적용하기 위해 새 정책 맵을 만들 수 있습니다.

이 예에서는 클래스가 현재 정책(전역 정책)에 삽입됩니다.

```
## 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
```

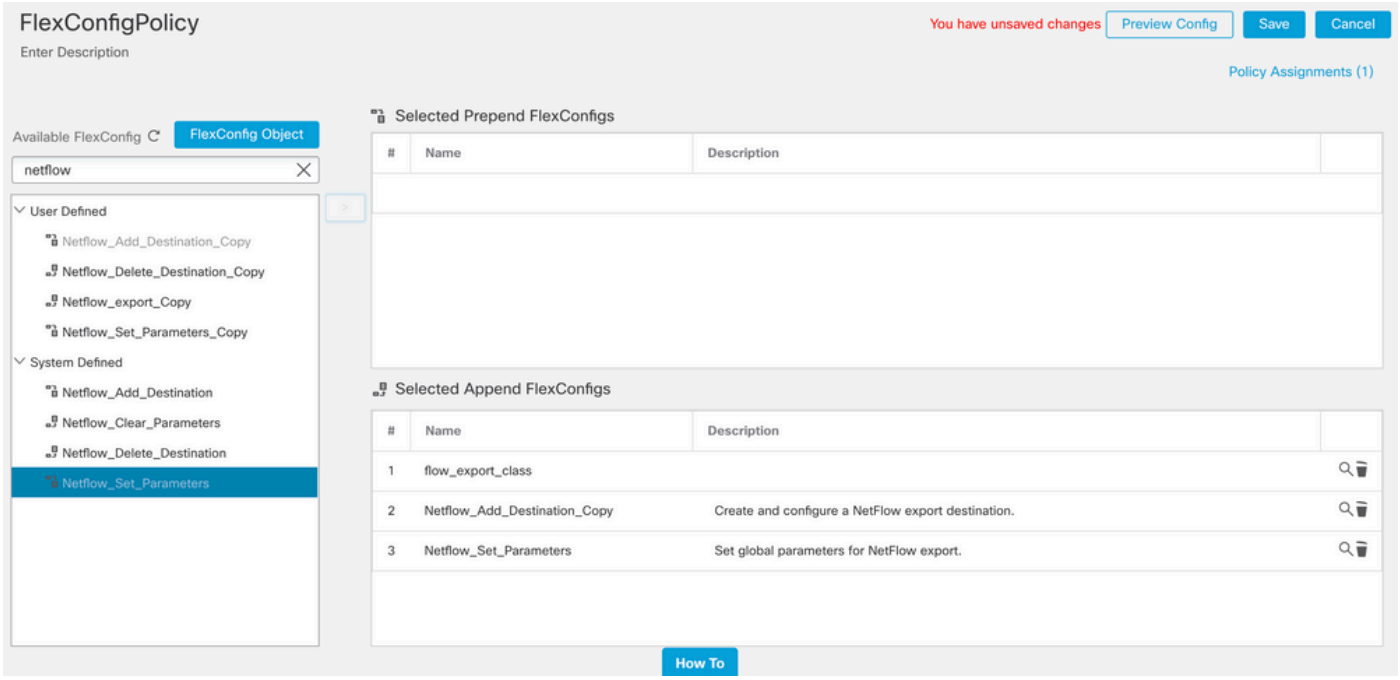
완료되면 Save(**저장**)를 클릭합니다.



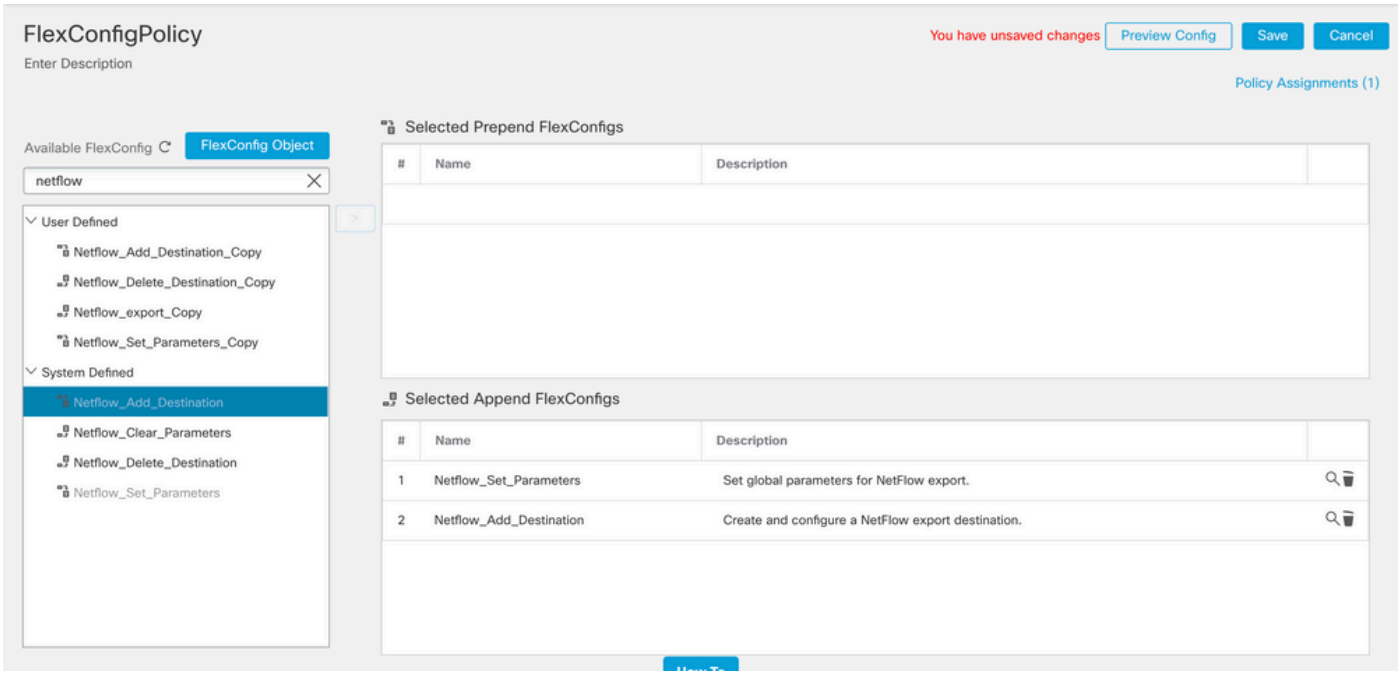
5단계. FTD에 FlexConfig 정책 할당

다른 용도로 생성되어 동일한 **FTD**에 할당된 정책이 아직 없는 경우 Devices(디바이스) > FlexConfig(FlexConfig)로 이동하여 새 정책을 생성합니다. 이 예에서는 FlexConfig가 이미 생성되었습니다. FlexConfig 정책을 수정하고 이전 **단계**에서 생성한 FlexConfig 개체를 선택합니다.

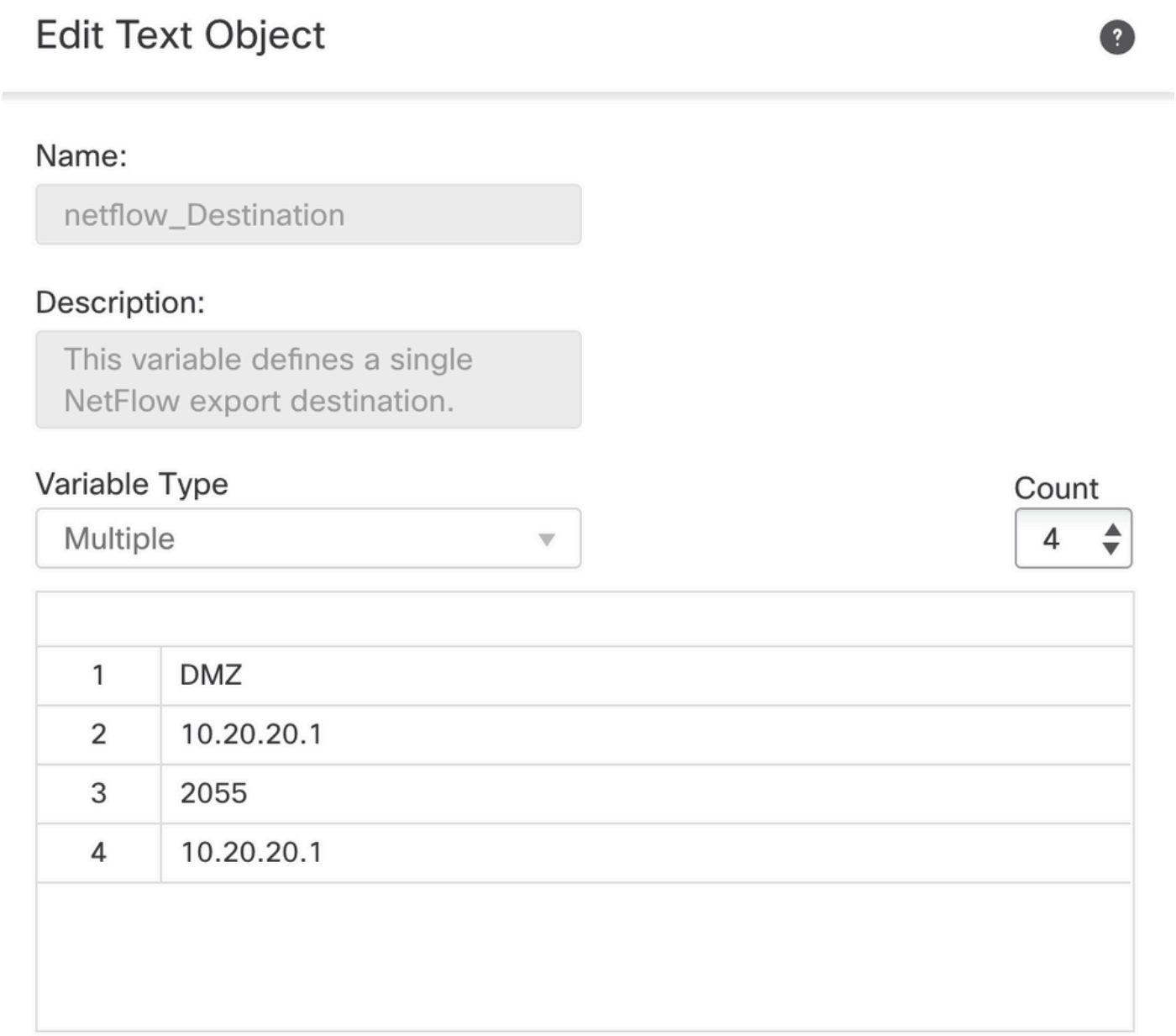
이 예에서는 기본 Netflow 내보내기 매개변수가 사용되므로 Netflow_Set_Parameters가 선택됩니다. 변경된 **내용**을 저장하고 구축합니다.



참고: 특정 트래픽을 확인할 필요 없이 모든 트래픽을 확인하기 위해 2~4단계에서 건너뛰고 사전 정의된 NetFlow 개체를 사용할 수 있습니다.



참고: NetFlow 패킷이 전송되는 두 번째 NSEL 컬렉터를 추가하려면 1단계에서 4개의 변수를 추가하여 두 번째 Netflow 컬렉터 IP 주소를 추가합니다.



4단계에서 flow-export destination $netflow_Destination.get(0) $netflow_Destination.get(1) $netflow_Destination.get(2) 컨피그레이션 라인을 추가합니다.

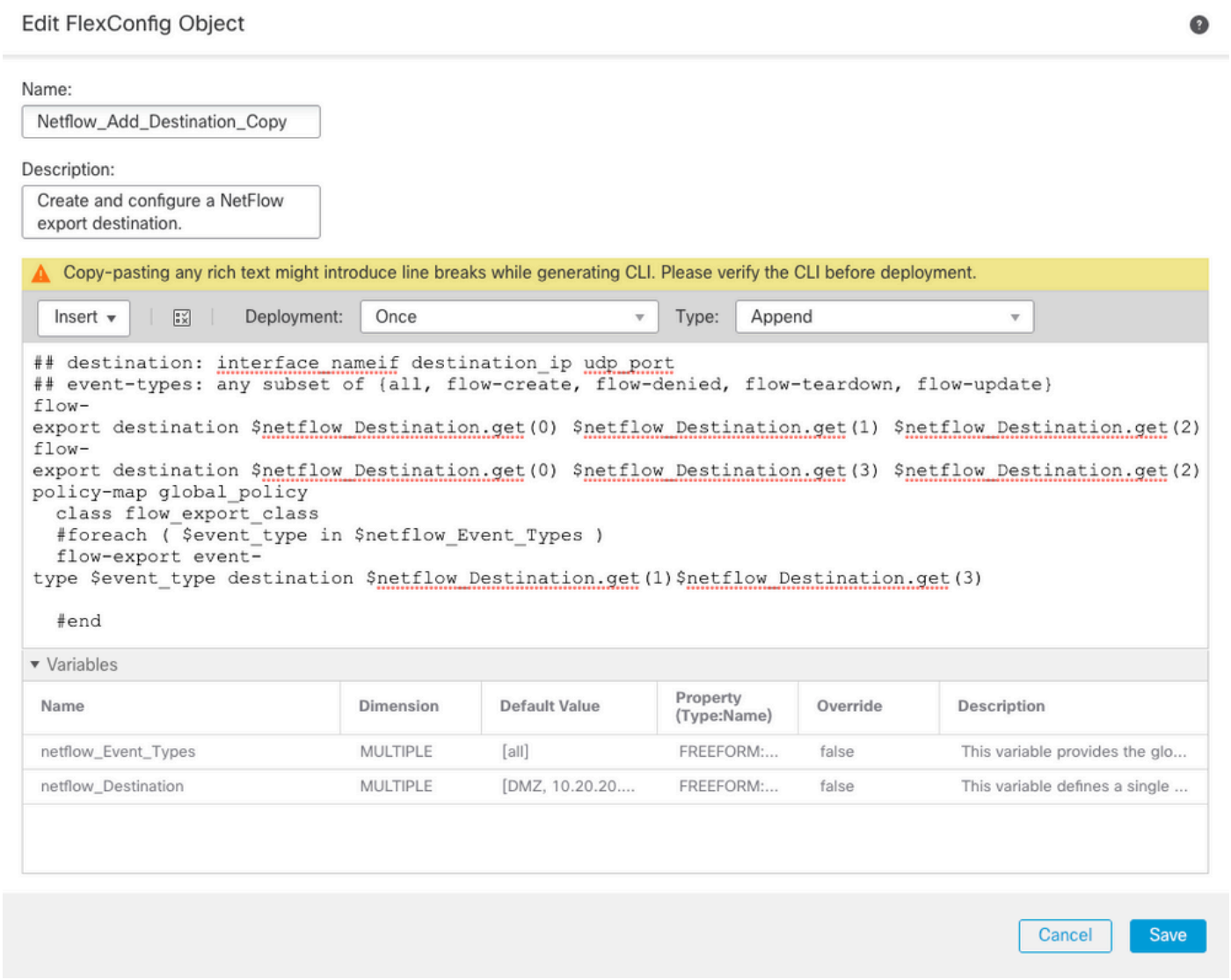
대응 변수에 대한 $netflow_Destination.get 변수를 편집합니다. 이 예에서 변수 값은 3입니다. 예를 들면 다음과 같습니다.

```
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)
```

또한 flow-export event-type $event_type destination $netflow_Destination.get(1) 구성 라인에 두 번째 변수 $netflow_Destination.get을 추가합니다. 예를 들면 다음과 같습니다.

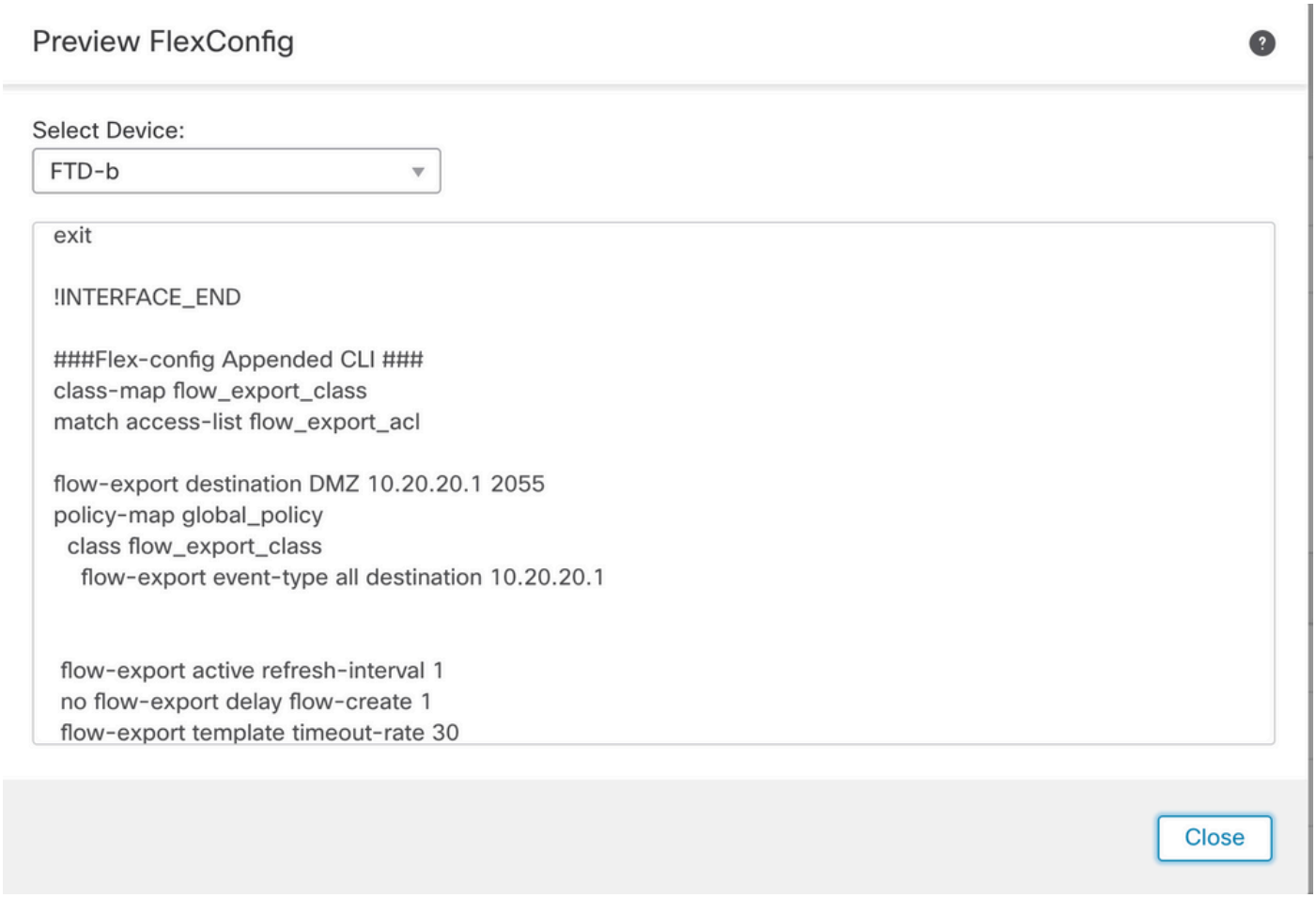
```
flow-export event-
type $event_type destination $netflow_Destination.get(1) $netflow_Destination.get(3)
```

아래 이미지에 표시된 대로 이 컨피그레이션을 검증합니다.



다음을 확인합니다.

NetFlow 컨피그레이션은 FlexConfig 정책 내에서 확인할 수 있습니다. 컨피그레이션을 미리 보려면 Preview Config(컨피그레이션 미리 보기)**를 클릭합니다**. **FTD**를 선택하고 컨피그레이션을 확인합니다.



SSH(Secure Shell)를 통해 FTD에 액세스하고 system support diagnostic-cli 명령을 사용하고 다음 명령을 실행합니다.

```
> 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
```

관련 정보

- Cisco 기술 지원 및 다운로드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.