FTD:如何使用FlexConfig策略啟用TCP狀態旁路配置

目錄

簡介

本檔案介紹如何使用6.3.0之前的版本中的FlexConfig原則，透過Firepower管理中心(FMC)在Firepower威脅防禦(FTD)裝置上實作傳輸控制通訊協定(TCP)狀態略過功能。

必要條件

需求

思科建議您瞭解以下主題：

- 瞭解Firepower管理中心。
- Firepower威脅防禦基礎知識。
- 瞭解TCP狀態略過功能。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Firepower威脅防禦(FTD)版本6.2.3。
- Firepower管理中心(FMC)版本6.2.3。

背景資訊

TCP狀態旁路是從自適應安全裝置(ASA)繼承的一項功能，在排查TCP規範化功能、非對稱路由條件和某些應用檢查可能丟棄的流量時提供幫助。

從版本6.3.0開始，FMC本身支援此功能。建議在升級後刪除Flexconfig對象，並在首次部署前將此配置移動到FMC。有關如何在6.3.0版或更高版本中配置TCP狀態旁路的詳細資訊，請訪問本配置指南。

Firepower威脅防禦使用ASA配置命令實施某些功能，但並非所有功能。沒有唯一的Firepower威脅防禦配置命令。相反，FlexConfig的意義在於允許您配置尚未通過Firepower管理中心策略和設定直接支援的功能。

> **注意**:TCP狀態旁路應僅用於故障排除或無法解析非對稱路由時。使用此功能會禁用多個安全功能，而且如果未正確實施，可能會導致大量連線。

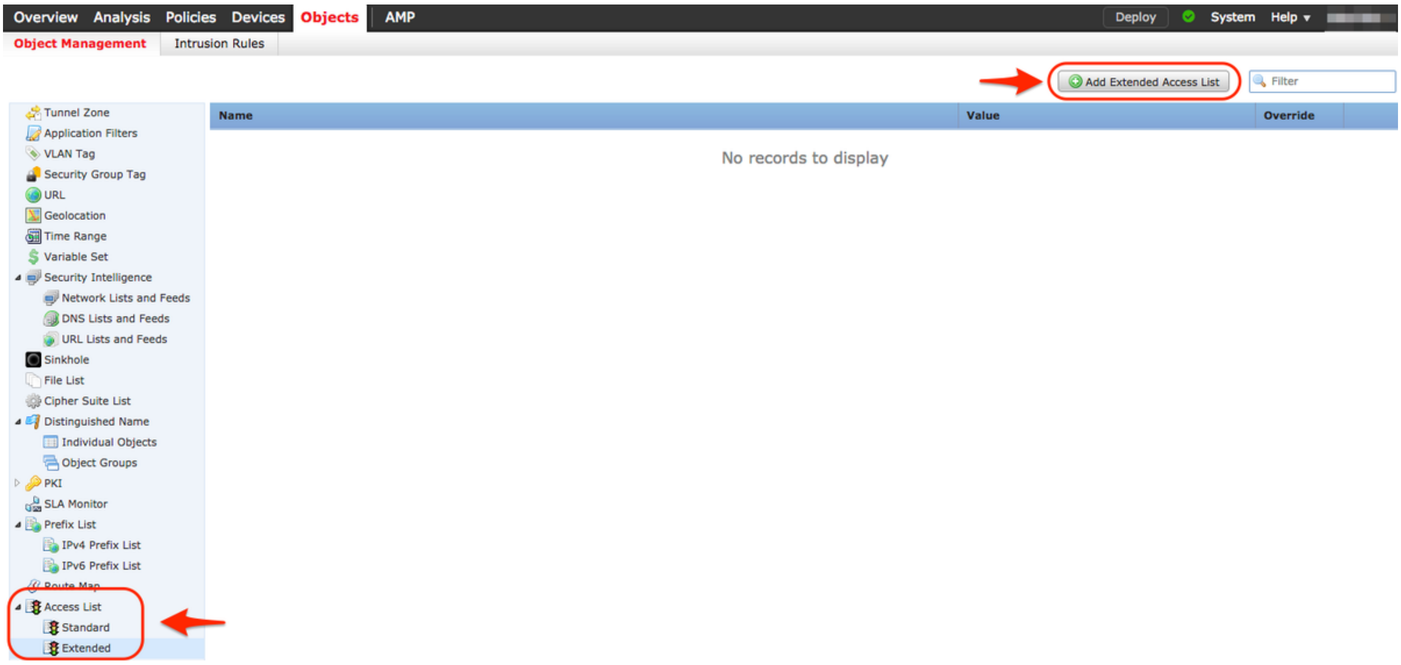
要瞭解有關TCP狀態旁路功能或其在ASA中的實施的詳細資訊，請參閱在ASA 5500系列上配置TCP狀態旁路功能和Cisco ASA 5500系列配置指南。

組態

本節介紹如何透過FlexConfig原則在FMC上設定TCP狀態略過。

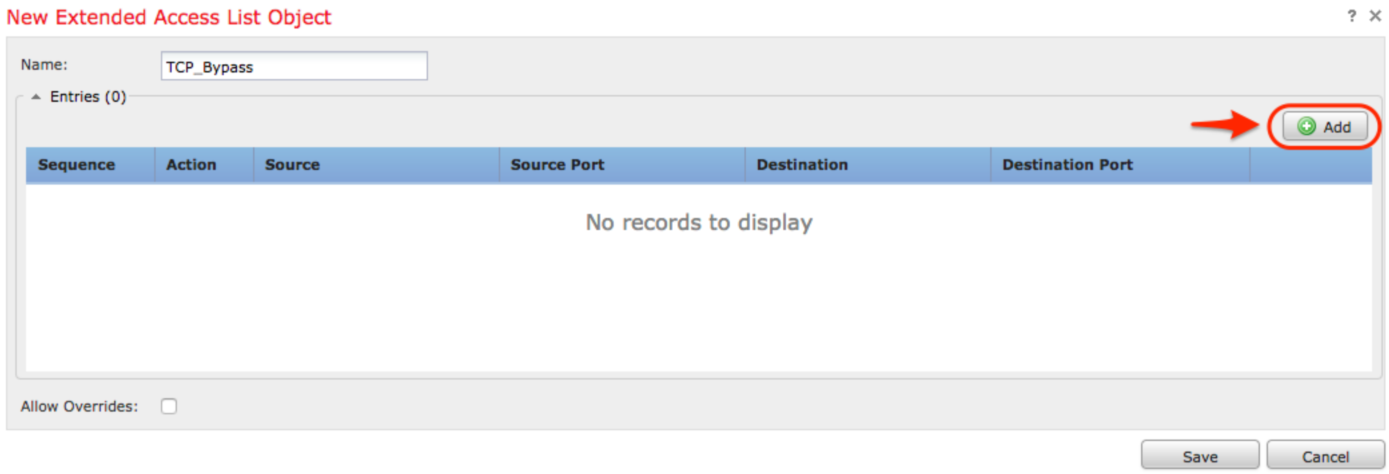
步驟1.配置擴展訪問清單對象

要在FMC上建立擴展訪問清單，請轉到**對象>對象管理**，然後在左側選單的**訪問清單**下選擇**擴展。按一下新增擴展訪問清單。**



No records to display

使用所需的值填充Name欄位。在本例中，名稱為**TCP_Bypass**。按一下「**Add**」按鈕。



New Extended Access List Object

Name: TCP_Bypass

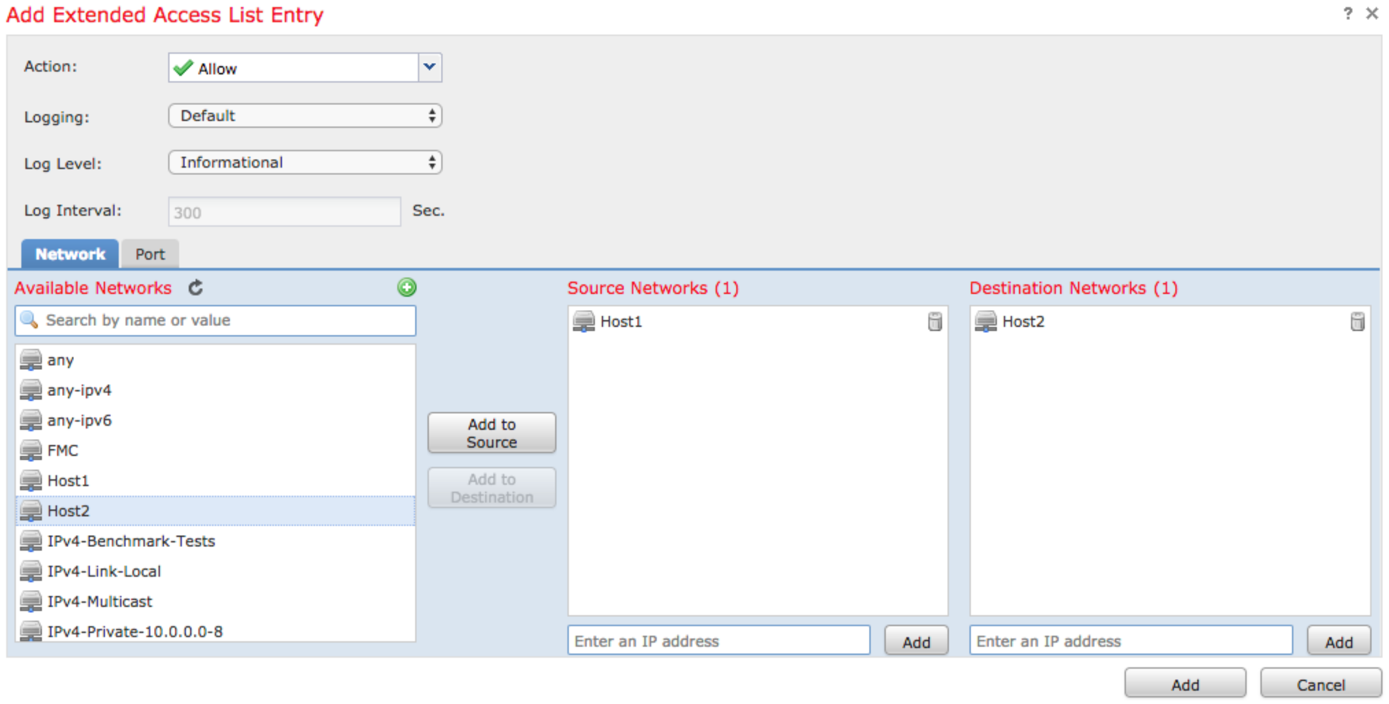
Entries (0)

Sequence	Action	Source	Source Port	Destination	Destination Port

No records to display

Allow Overrides: □

此規則的操作必須配置為**Allow**。可以使用系統定義的網路，或者可以為每個源和目標建立新的網路對象。在本例中，訪問清單匹配從主機1到主機2的IP流量，因為這是應用TCP狀態略過的通訊。埠頁籤可用於匹配特定TCP或UDP埠。按一下**Add**按鈕繼續。



Add Extended Access List Entry

Action: ✓ Allow

Logging: Default

Log Level: Informational

Log Interval: 300 Sec.

Available Networks

- any
- any-ipv4
- any-ipv6
- FMC
- Host1
- Host2
- IPv4-Benchmark-Tests
- IPv4-Link-Local
- IPv4-Multicast
- IPv4-Private-10.0.0.0-8

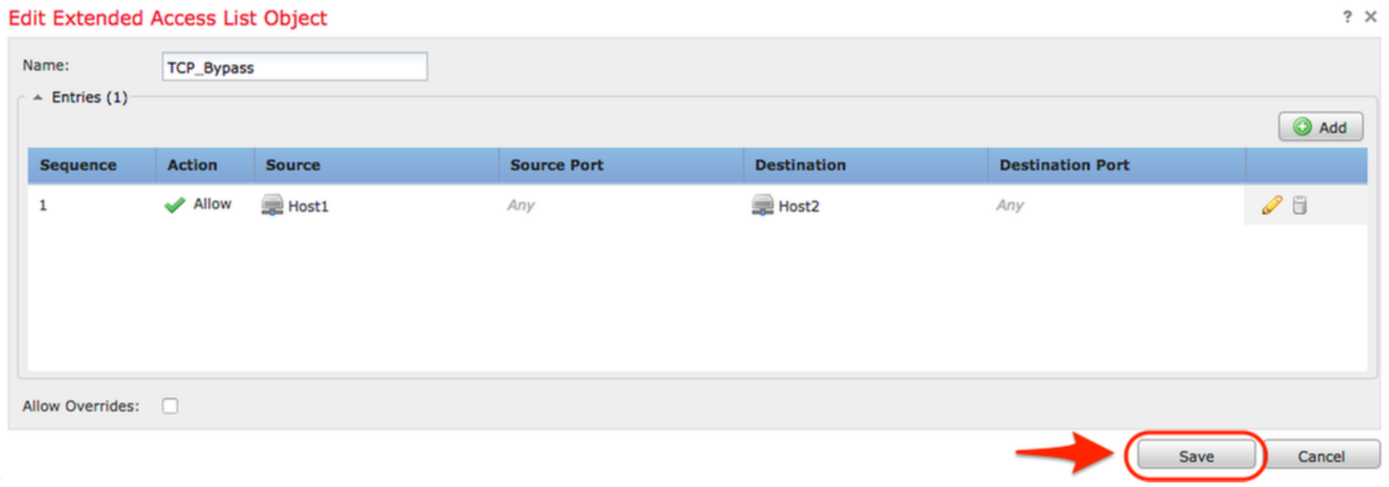
Source Networks (1)

- Host1

Destination Networks (1)

- Host2

選擇源網路和目標網路或主機後，按一下**Save**。



Edit Extended Access List Object

Name: TCP_Bypass

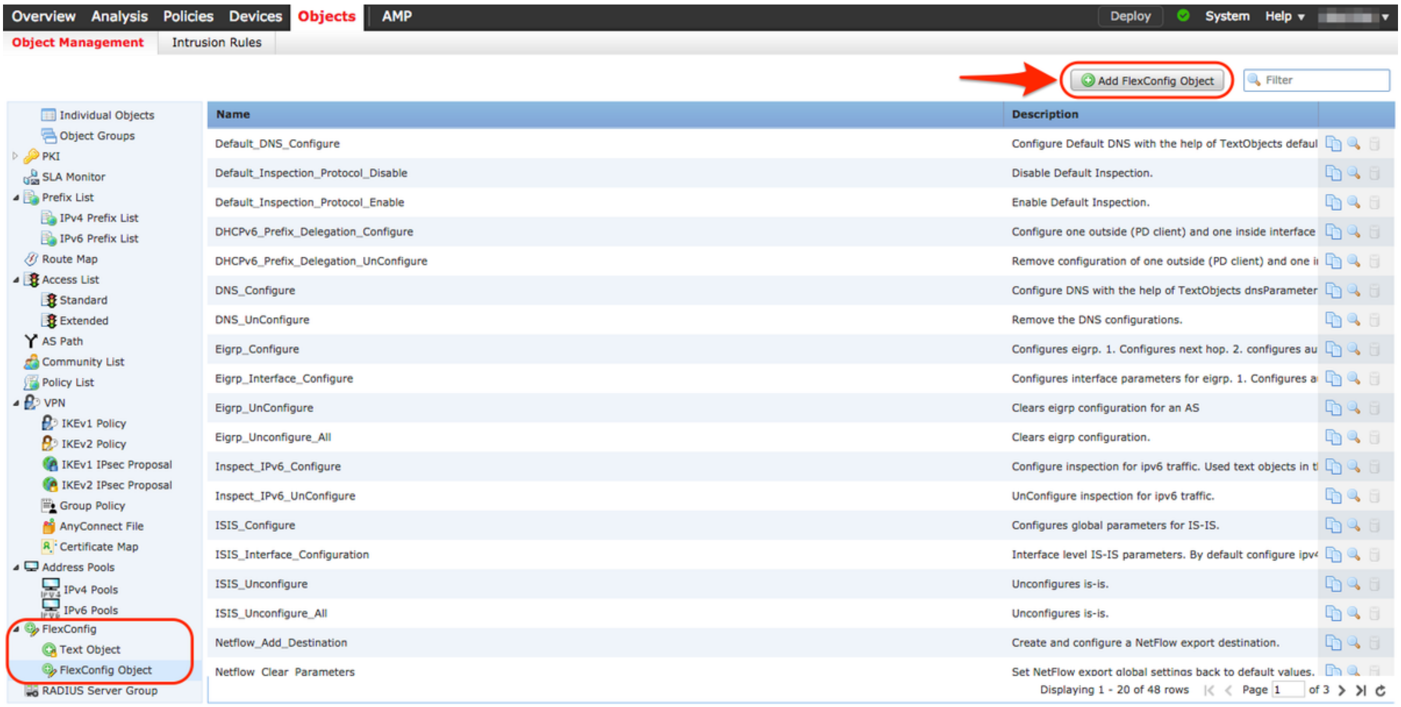
Entries (1)

Sequence	Action	Source	Source Port	Destination	Destination Port
1	✓ Allow	Host1	Any	Host2	Any

Allow Overrides: □

步驟2.配置FlexConfig對象

導航到**對象>對象管理> FlexConfig > FlexConfig對象**，然後按一下**新增FlexConfig對象**按鈕。

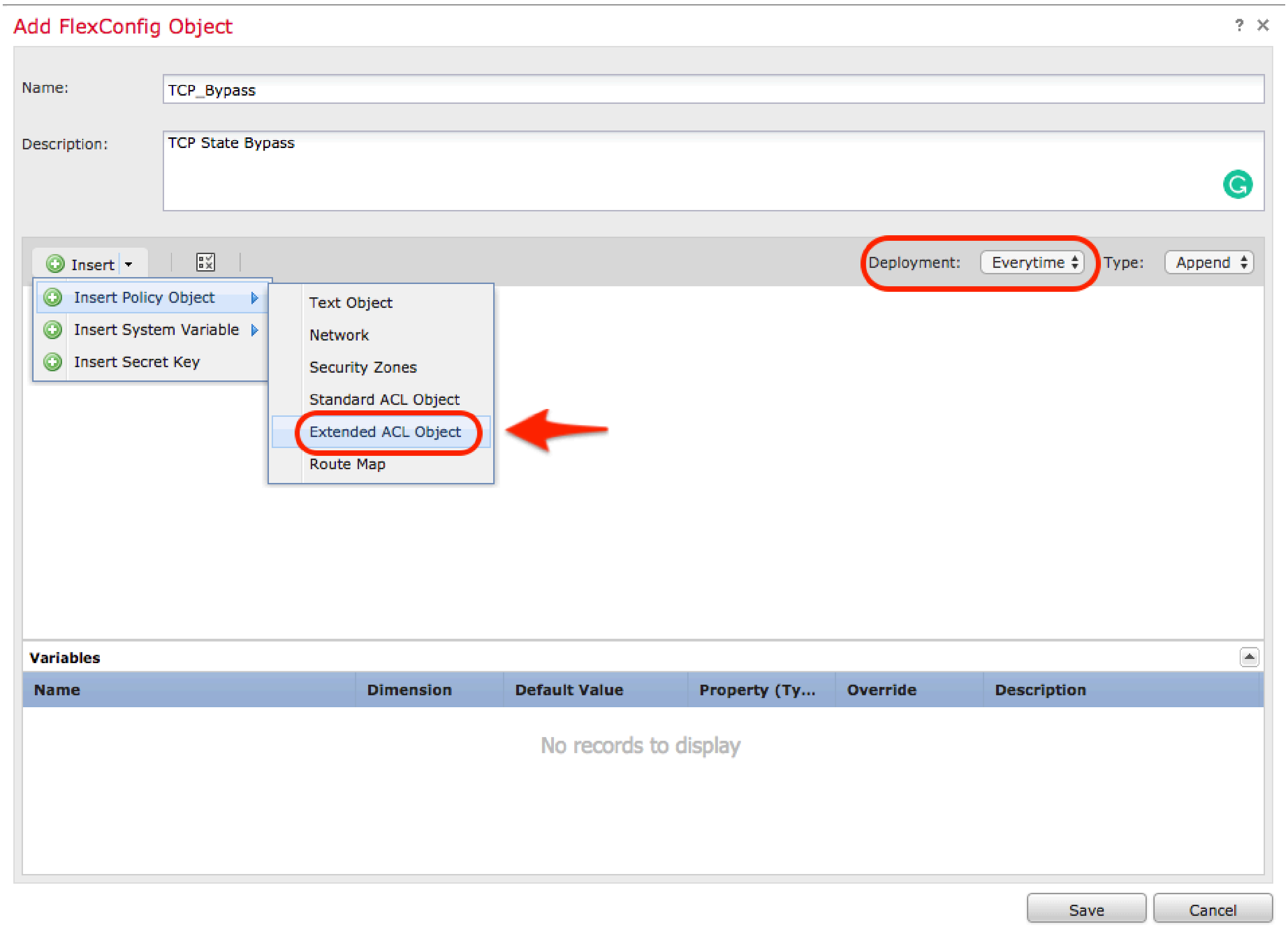


Name	Description
Default_DNS_Configure	Configure Default DNS with the help of TextObjects defaul
Default_Inspection_Protocol_Disable	Disable Default Inspection.
Default_Inspection_Protocol_Enable	Enable Default Inspection.
DHCPv6_Prefix_Delegation_Configure	Configure one outside (PD client) and one inside interface
DHCPv6_Prefix_Delegation_UnConfigure	Remove configuration of one outside (PD client) and one i
DNS_Configure	Configure DNS with the help of TextObjects dnsParameter
DNS_UnConfigure	Remove the DNS configurations.
Eigrp_Configure	Configures eigrp. 1. Configures next hop. 2. configures au
Eigrp_Interface_Configure	Configures interface parameters for eigrp. 1. Configures a
Eigrp_UnConfigure	Clears eigrp configuration for an AS
Eigrp_Unconfigure_All	Clears eigrp configuration.
Inspect_IPv6_Configure	Configure inspection for ipv6 traffic. Used text objects in t
Inspect_IPv6_UnConfigure	UnConfigure inspection for ipv6 traffic.
ISIS_Configure	Configures global parameters for IS-IS.
ISIS_Interface_Configuration	Interface level IS-IS parameters. By default configure ipv
ISIS_Unconfigure	Unconfigures is-is.
ISIS_Unconfigure_All	Unconfigures is-is.
Netflow_Add_Destination	Create and configure a NetFlow export destination.
Netflow_Clear_Parameters	Set NetFlow export global settings back to default values.

Displaying 1 - 20 of 48 rows | Page 1 of 3

此示例的對象名稱稱為**TCP_Bypass**，與訪問清單相同。此名稱無需與訪問清單名稱匹配。

選擇**Insert Policy Object** > **Extended ACL Object**。


Add FlexConfig Object

Name: TCP_Bypass

Description: TCP State Bypass

Deployment: Everytime

Type: Append

Variables

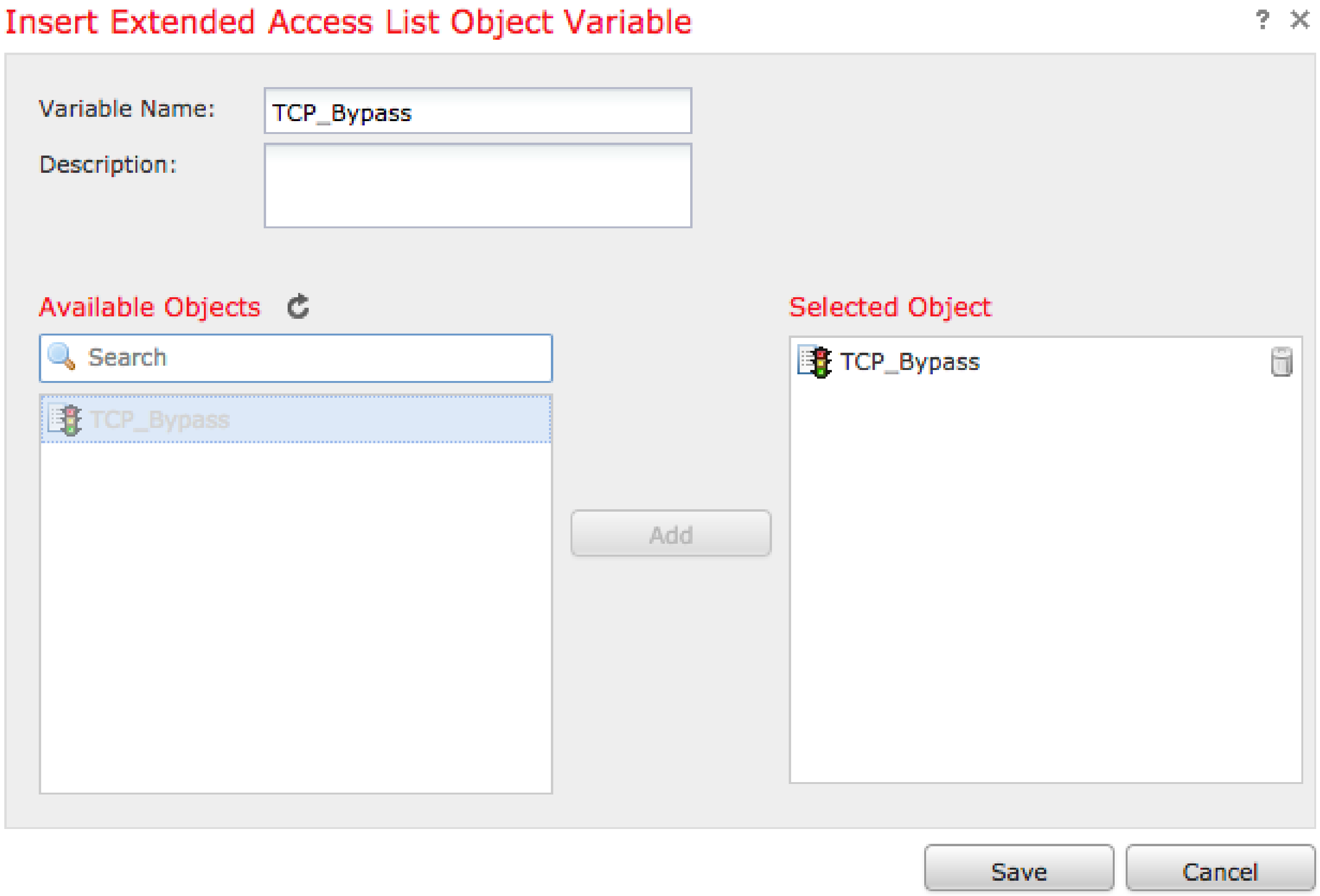
Name	Dimension	Default Value	Property (Ty...	Override	Description

No records to display

附註：確保選擇「Everytime」選項。這樣可以在其他部署和升級過程中保留此配置。

從**可用對象**部分選擇在步驟1中建立的訪問清單並分配變數名稱。然後，按一下**Add**按鈕。在本示例中，變數名稱為**TCP_Bypass**。

按一下**Save**。



Insert Extended Access List Object Variable

Variable Name: TCP_Bypass

Description:

Available Objects

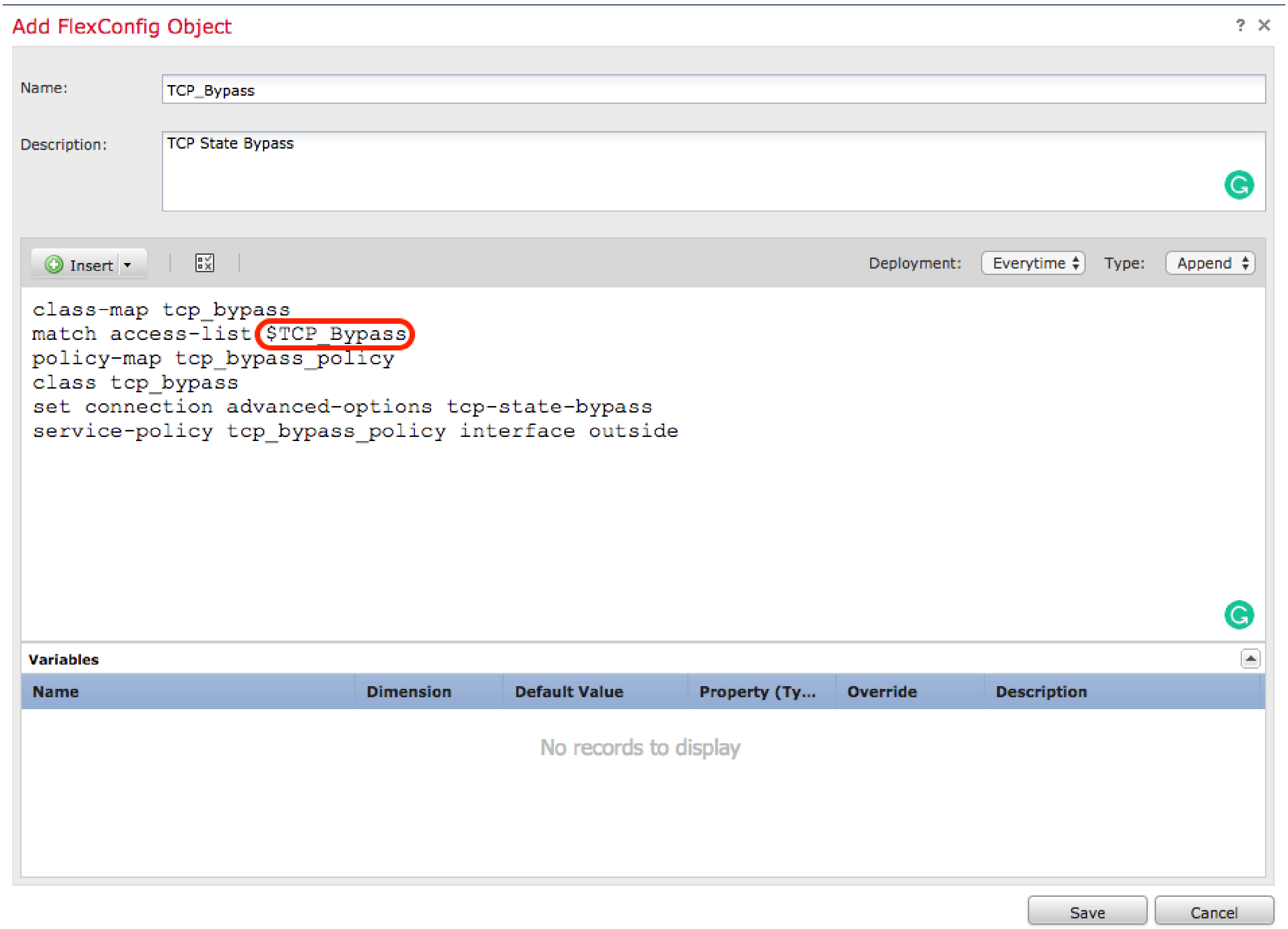
Selected Object: TCP_Bypass

在**Insert**按鈕正下方的空白欄位中新增接下來的配置行，並在**match access-list**配置行中包括以前定義的變數(**$TCP_Bypass**)。請注意，變數名稱前面帶有**$**符號。這有助於定義變數在其後跟隨。

```
class-map tcp_bypass
match access-list $TCP_Bypass
policy-map tcp_bypass_policy
class tcp_bypass
set connection advanced-options tcp-state-bypass
service-policy tcp_bypass_policy interface outside
```

在此示例中，將建立策略對映並將其應用於外部介面。如果需要將TCP狀態旁路配置為全域性服務策略的一部分，則tcp_bypass類對映可以應用於global_policy。

完成後按一下**Save**。



Add FlexConfig Object

Name: TCP_Bypass

Description: TCP State Bypass

Deployment: Everytime   Type: Append

```
class-map tcp_bypass
match access-list $TCP_Bypass
policy-map tcp_bypass_policy
class tcp_bypass
set connection advanced-options tcp-state-bypass
service-policy tcp_bypass_policy interface outside
```

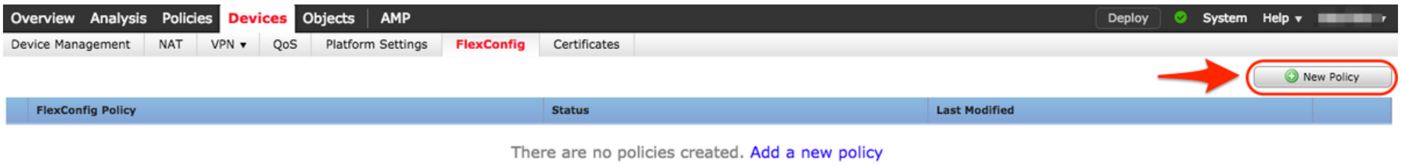
Variables

Name	Dimension	Default Value	Property (Ty...	Override	Description

No records to display

步驟3.將FlexConfig原則指定給FTD

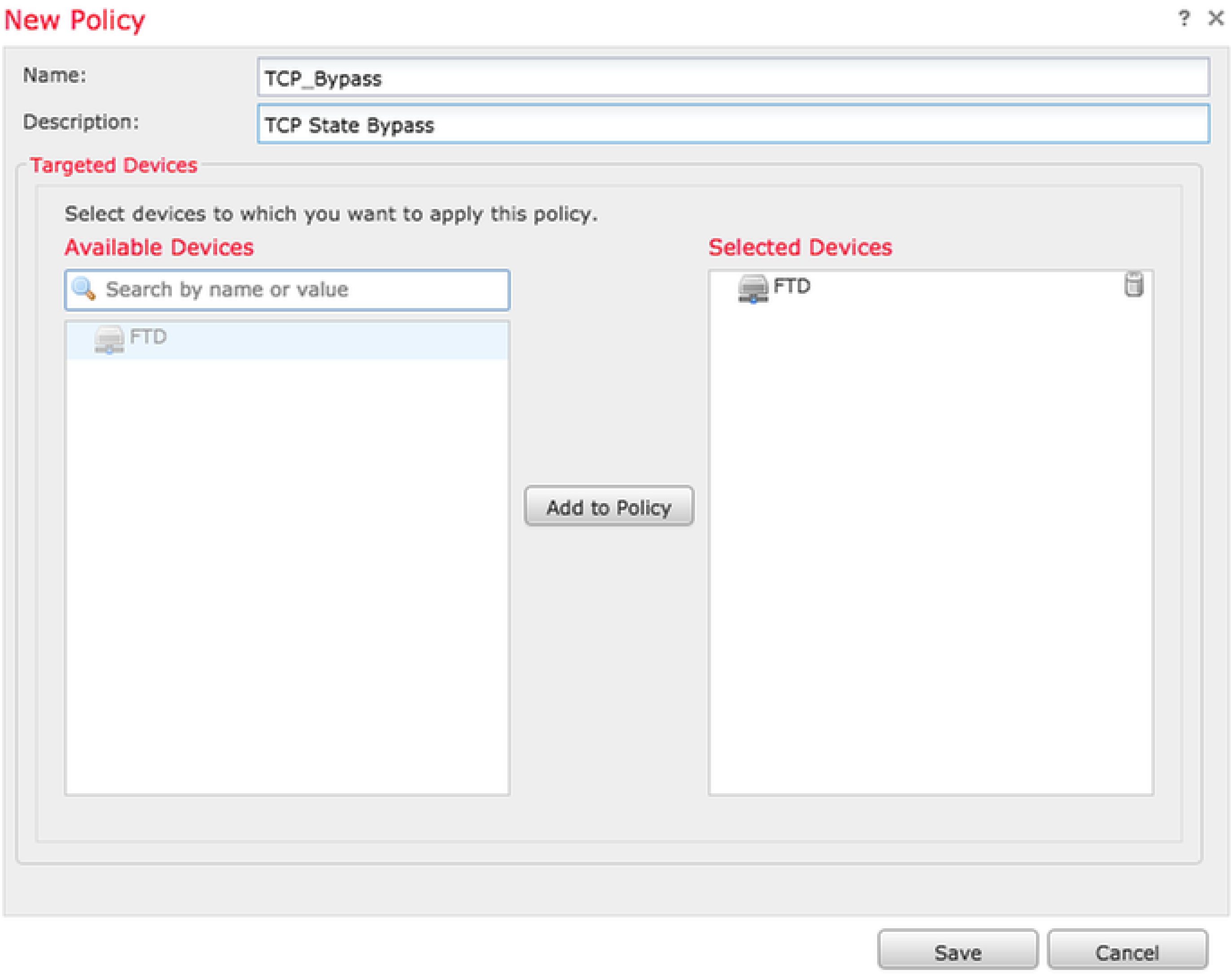
轉至**Devices > FlexConfig**，然後建立新的策略（除非已經建立了另一個策略並將其分配給同一個FTD）。在此示例中，新的FelxConfig策略稱為**TCP_Bypass**。



FlexConfig Policy	Status	Last Modified

There are no policies created. Add a new policy

將**TCP_Bypass FlexConfig**策略分配給FTD裝置。



New Policy

Name: TCP_Bypass

Description: TCP State Bypass

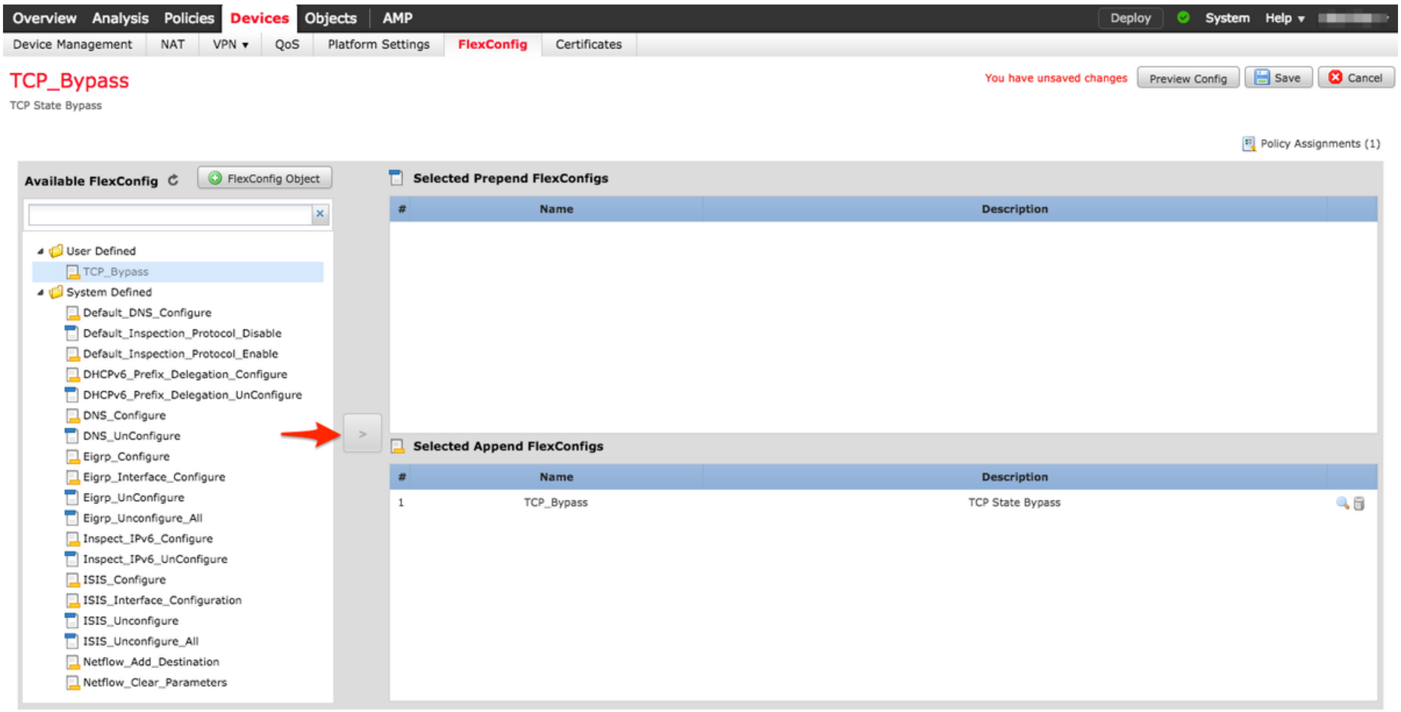
Targeted Devices

Select devices to which you want to apply this policy.

Available Devices: FTD

Selected Devices: FTD

在**User Defined**部分下，選擇在步驟2中建立的**TCP_Bypass** FlexConfig對象，然後按一下箭頭將該對象新增到策略中。



TCP_Bypass

TCP State Bypass

You have unsaved changes

Available FlexConfig

- User Defined
  - TCP_Bypass
- System Defined
  - Default_DNS_Configure
  - Default_Inspection_Protocol_Disable
  - Default_Inspection_Protocol_Enable
  - DHCPv6_Prefix_Delegation_Configure
  - DHCPv6_Prefix_Delegation_UnConfigure
  - DNS_Configure
  - DNS_UnConfigure
  - Eigrp_Configure
  - Eigrp_Interface_Configure
  - Eigrp_UnConfigure
  - Eigrp_Unconfigure_All
  - Inspect_IPv6_Configure
  - Inspect_IPv6_UnConfigure
  - ISIS_Configure
  - ISIS_Interface_Configuration
  - ISIS_Unconfigure
  - ISIS_Unconfigure_All
  - Netflow_Add_Destination
  - Netflow_Clear_Parameters

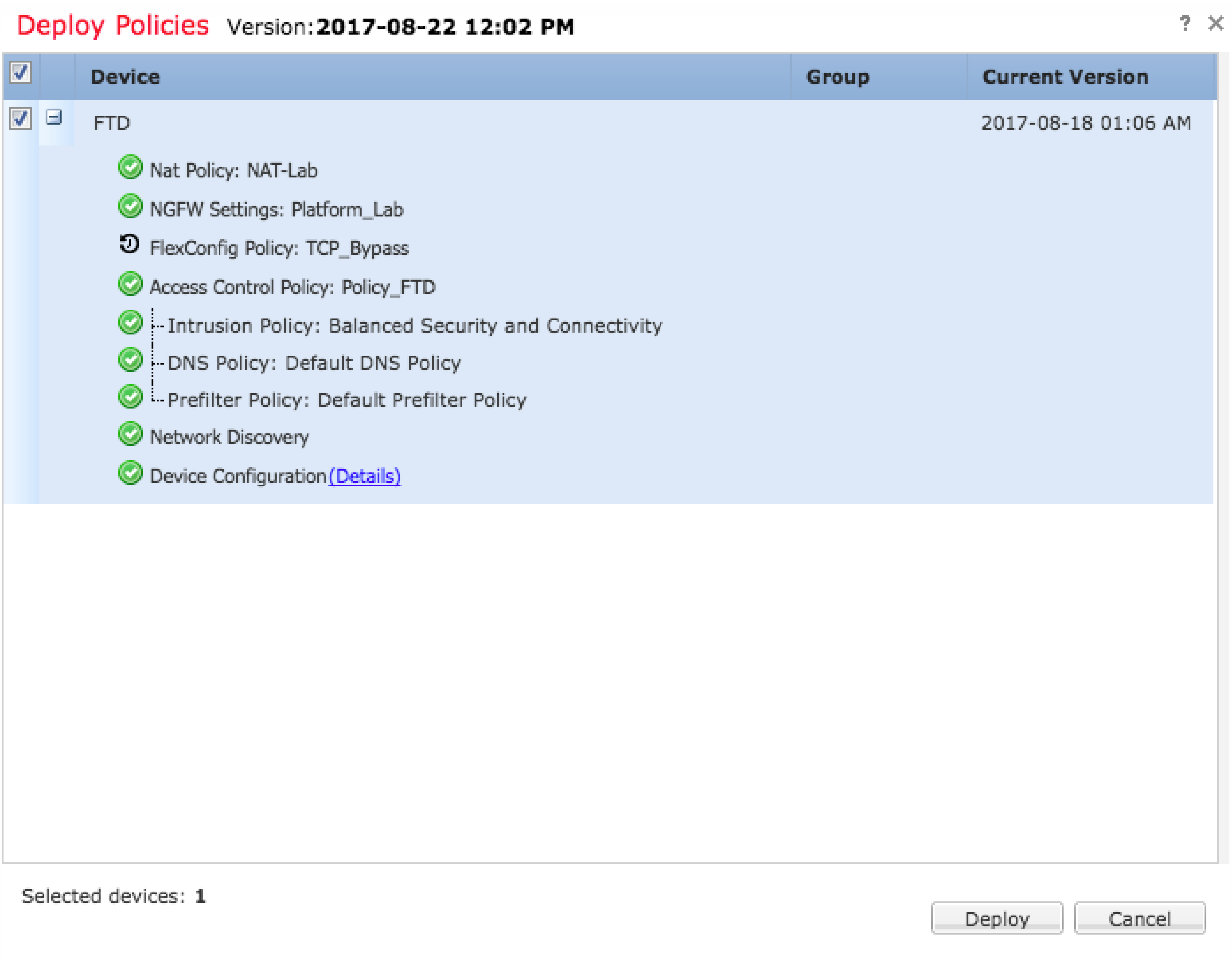
Selected Prepend FlexConfigs

#	Name	Description

Selected Append FlexConfigs

#	Name	Description
1	TCP_Bypass	TCP State Bypass

儲存更改並進行部署，



Deploy Policies Version:**2017-08-22 12:02 PM**

☑	Device	Group	Current Version
☑	FTD		2017-08-18 01:06 AM
	✓ Nat Policy: NAT-Lab		
	✓ NGFW Settings: Platform_Lab		
	FlexConfig Policy: TCP_Bypass		
	✓ Access Control Policy: Policy_FTD		
	✓ Intrusion Policy: Balanced Security and Connectivity		
	✓ DNS Policy: Default DNS Policy		
	✓ Prefilter Policy: Default Prefilter Policy		
	✓ Network Discovery		
	✓ Device Configuration(Details)		

Selected devices: **1**

驗證

通過SSH或控制檯訪問FTD，然後使用命令**system support diagnostic-cli。**

```
> 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 TCP_Bypass
access-list TCP_Bypass; 1 elements; name hash: 0xec2b41eb
access-list TCP_Bypass line 1 extended permit object-group ProxySG_ExtendedACL_34359739205
object Host1 object Host2 log informational interval 300 (hitcnt=0) 0x42940b0e
access-list TCP_Bypass line 1 extended permit ip host 1.1.1.1 host 1.1.1.2 log informational
interval 300 (hitcnt=0) 0x769561fc

firepower# show running-config class-map
!
class-map inspection_default
match default-inspection-traffic
class-map tcp_bypass
match access-list TCP_Bypass
!
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
class class-default
set connection advanced-options UM_STATIC_TCP_MAP
policy-map tcp_bypass_policy
class tcp_bypass
set connection advanced-options tcp-state-bypass
!
```

疑難排解

若要對此功能進行疑難排解，這些命令可提供幫助。

```
- show conn [detail]
Shows connection information. Detailed information uses flags to indicate special connection
characteristics.
For example, the “b” flag indicates traffic subject to TCP State Bypass

- show service-policy
Shows service policy statistics, including Dead Connection Detection (DCD) statistics
```

相關連結

https://www.cisco.com/c/en/us/td/docs/security/asa/asa91/configuration/firewall/asa_91_firewall_config/conns_connlimits.html

https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/118995-configure-asa-00.html

https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/flexconfig_policies.html