FTD: Hoe kan TCP-statelijke omzeilingsconfiguratie worden ingeschakeld met behulp van FlexConfig-beleid

Inhoud

Inleiding
Voorwaarden
Vereisten
Gebruikte componenten
Achtergrondinformatie
Configuratie
Stap 1. Het configureren van een object met uitgebreide toegangslijst
Stap 2. Het configureren van een FlexConfig-object
Stap 3. Een FlexConfig-beleid aan de FTD toewijzen
Verificatie
Problemen oplossen
Verwante links

Inleiding

In dit document wordt beschreven hoe u Transmission Control Protocol (TCP) kunt implementeren, waarbij Bypass-functie op Firepower Threat Defense (FTD) apparaten via Firepower Management Center (FMC) wordt uitgevoerd met FlexConfig Policy in versies eerder dan 6.3.0.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Kennis van het FireSIGHT Management Center.
- Basiskennis van brandweerraketten.
- Het begrip van de TCP State Bypass optie.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Firepower Threat Defense (FTD) versie 6.2.3.
- Firepower Management Center (FMC) versie 6.2.3.

Achtergrondinformatie

TCP State Bypass is een eigenschap die van de Adaptieve Security Appliance (ASA) wordt geërfd en biedt hulp bij het oplossen van problemen die door TCP-normalisatie-functies, asymmetrische routingvoorwaarden en bepaalde Application Inspecties kunnen worden gedropt.

Deze optie wordt niet ondersteund op FMC beginnende versie 6.3.0. Aanbevolen wordt om de Flexstack-configuratieobjecten na de upgrade te verwijderen en deze configuratie naar het FMC te verplaatsen voorafgaand aan de eerste plaatsing. Voor meer informatie over hoe u TCP State Bypass in versie 6.3.0 of hoger kunt configureren gaat u naar deze configuratiehandleiding.

Firepower Threat Defense gebruikt ASA configuratie opdrachten om bepaalde functies te implementeren, maar niet alle functies. Er zijn geen unieke set Firepower Threat Defense configuratieopdrachten. In plaats daarvan is het punt van FlexConfig om u in staat te stellen functies te configureren die nog niet rechtstreeks worden ondersteund door beleid en instellingen van FireSIGHT Management Center.

> **Opmerking**: De TCP-State Bypass zou alleen gebruikt moeten worden voor het oplossen van problemen of wanneer de asymmetrische routing niet opgelost kan worden. Het gebruik van deze optie schakelt meerdere beveiligingsfuncties uit en kan een groot aantal verbindingen veroorzaken als deze niet correct wordt uitgevoerd.

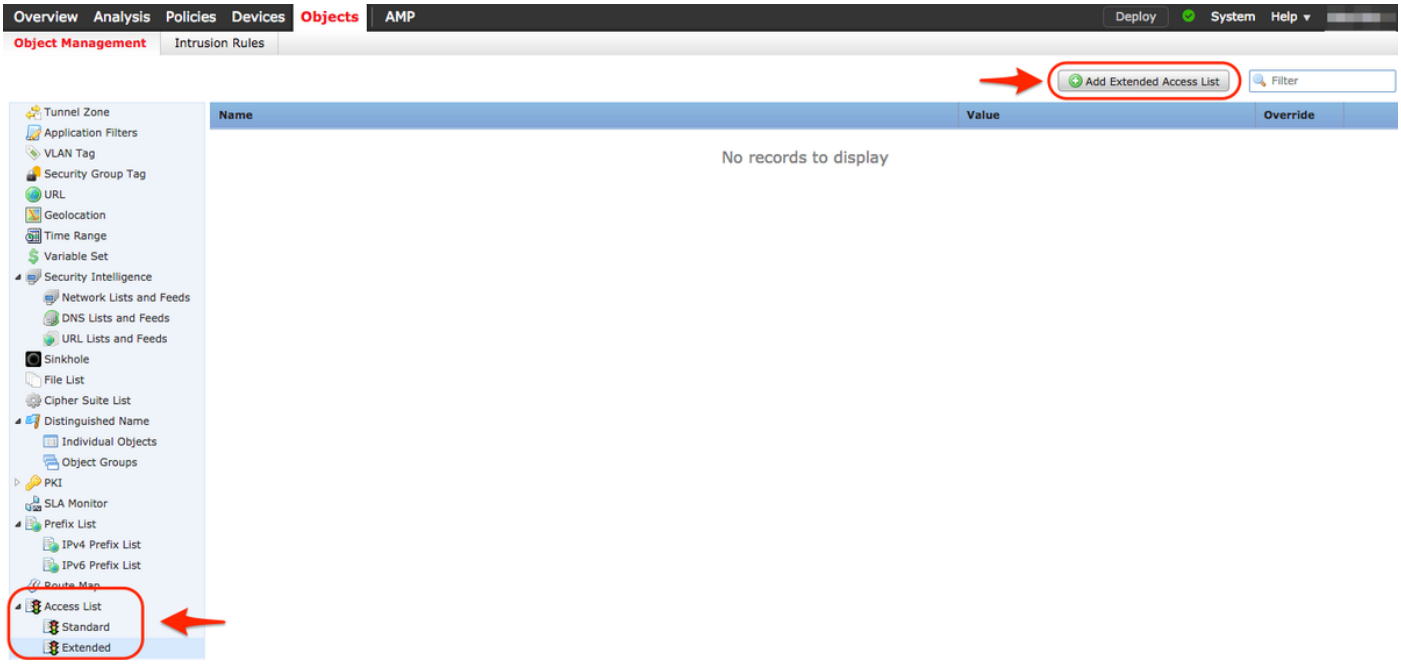
Om meer te weten te komen over de optie TCP-statelijke omzeilingen of de implementatie ervan in ASA, raadpleeg de functie TCP-omzeilen op de ASA 5500 Series en de Cisco ASA 5500 Series Configuration Guide te configureren.

Configuratie

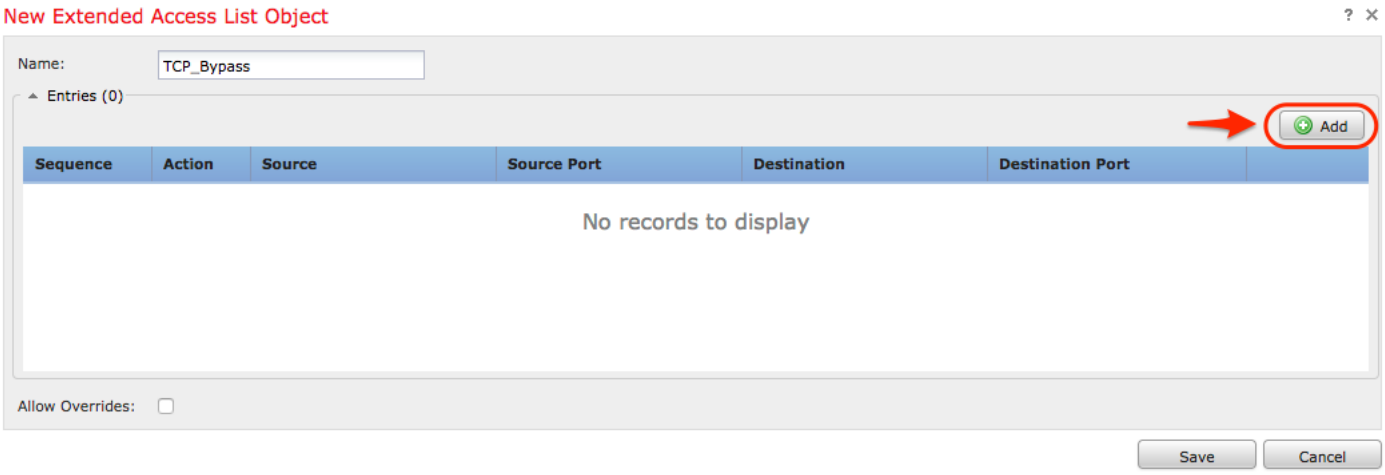
In deze sectie wordt beschreven hoe u TCP-State Bypass op FMC kunt configureren via een FlexConfig-beleid.

Stap 1. Het configureren van een object met uitgebreide toegangslijst

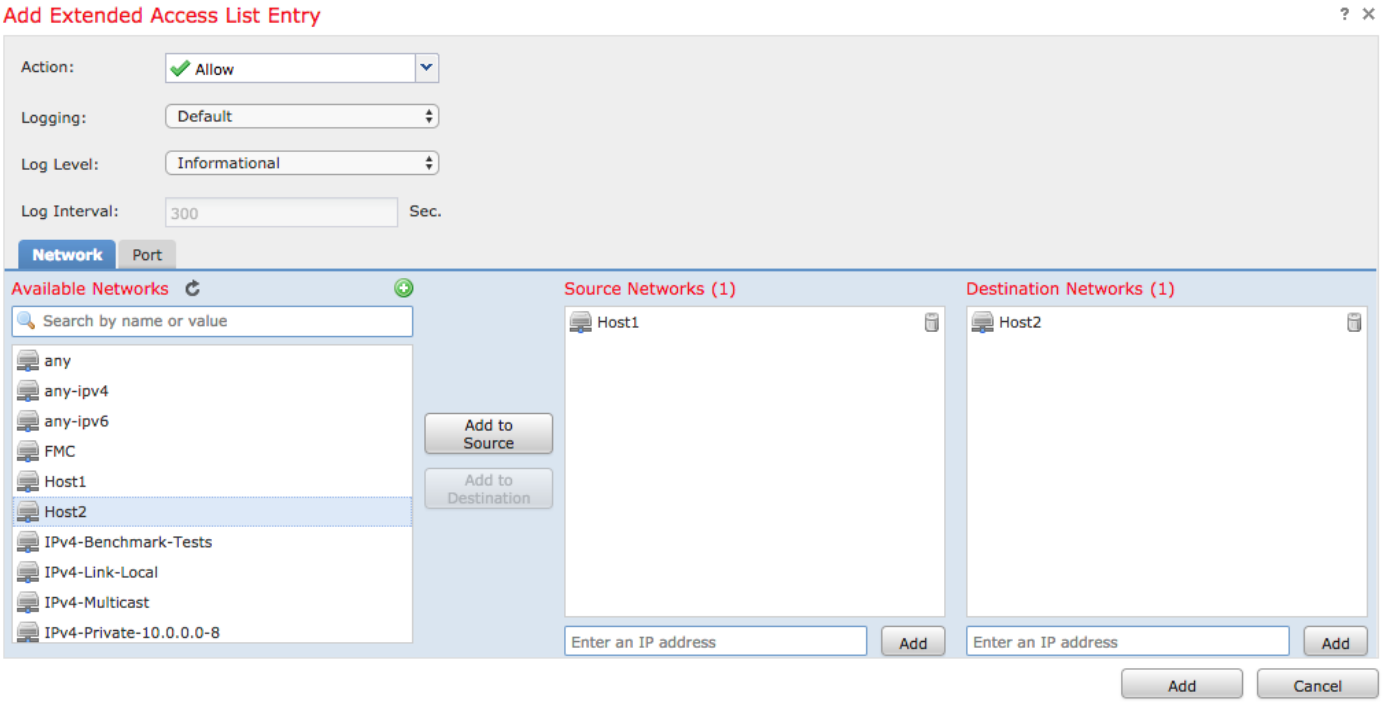
Om een uitgebreide toegangslijst op FMC te maken, gaat u naar **Objecten >**Objectbeheer en in het linkermenu onder **Toegangslijst** selecteer **Uitgebreid.** Klik op Uitgebreide toegangslijst toevoegen.



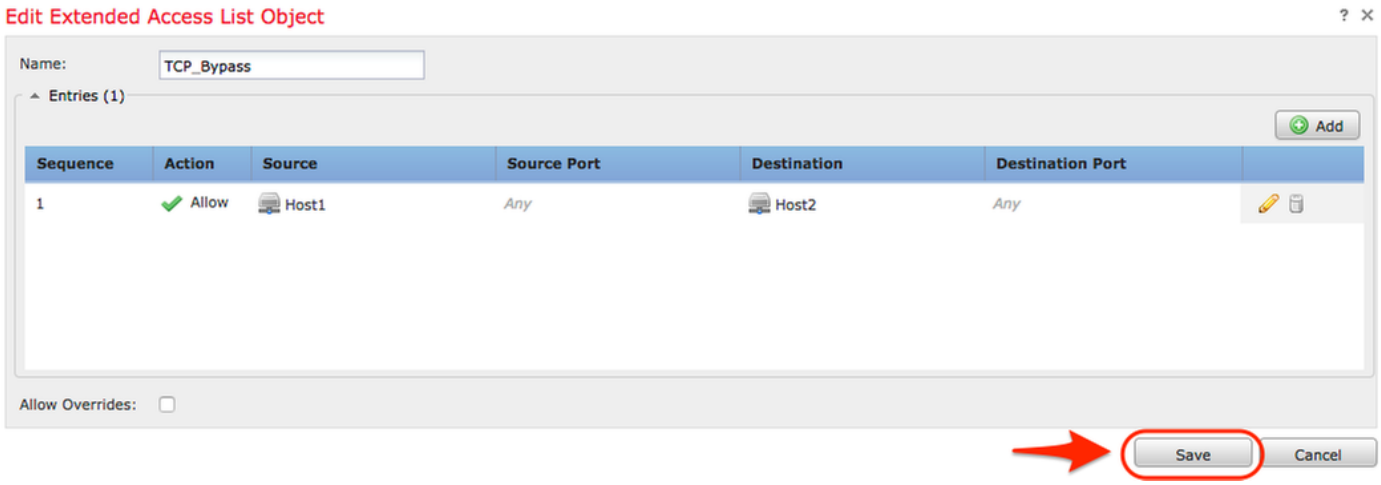
Vul het veld Naam in met de gewenste waarde. In dit voorbeeld is de naam **TCP_Bypass**. Klik op de knop **Toevoegen**.



De actie voor deze regel moet zijn geconfigureerd zoals **toestaan.** Een systeem gedefinieerd netwerk kan worden gebruikt of er kan een nieuw netwerkobject worden gemaakt voor elke bron en bestemming. In dit voorbeeld komt de toegangslijst IP-verkeer van Host1 tot Host2 aan omdat dit de communicatie is om de TCP-State Bypass toe te passen. Het tabblad Port kan optioneel worden gebruikt om een specifieke TCP- of UDP-poort aan te passen. Klik op de knop **Toevoegen** om verder te gaan

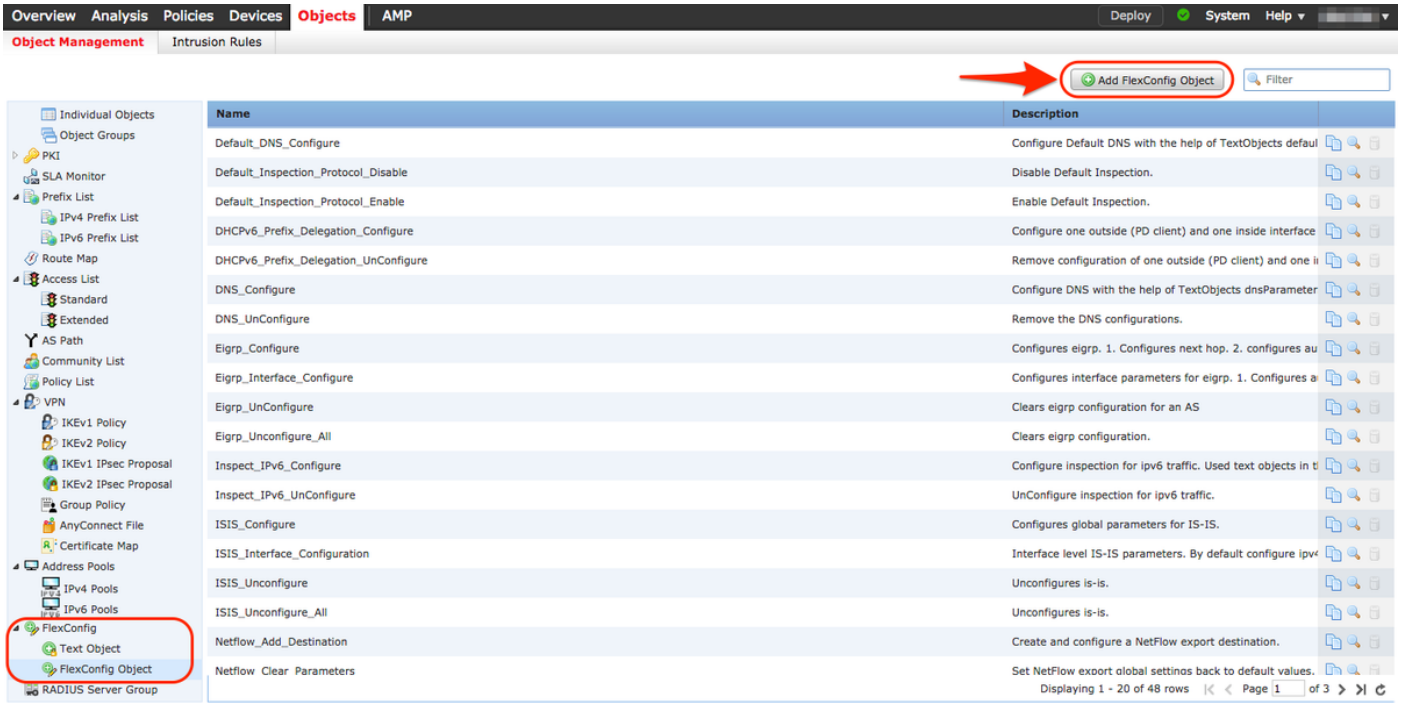


Nadat de bron- en doelnetwerken of -hosts zijn geselecteerd, klikt u op **Opslaan**.



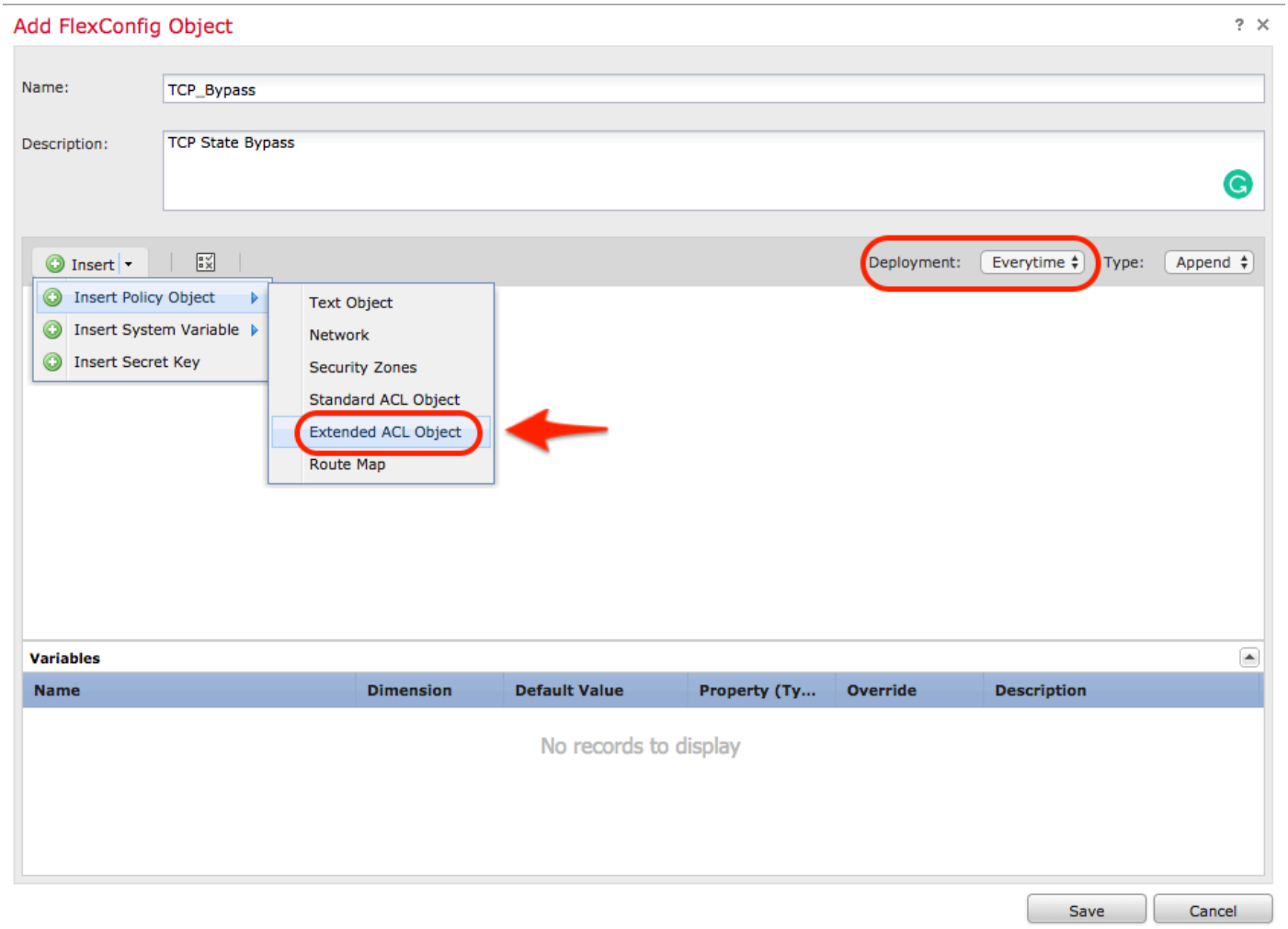
Stap 2. Het configureren van een FlexConfig-object

Navigeer aan **Voorwerpen > Objectbeheer > FlexConfig > FlexConfig** en klik op **Add FlexConfig** knop.



De naam van het object voor dit voorbeeld wordt **TCP_Bypass** genoemd net als de toegangslijst. Deze naam hoeft niet overeen te komen met de naam Toegangslijst.

Selecteer **Beleidsobject invoegen > Uitgebreide ACL-object.**

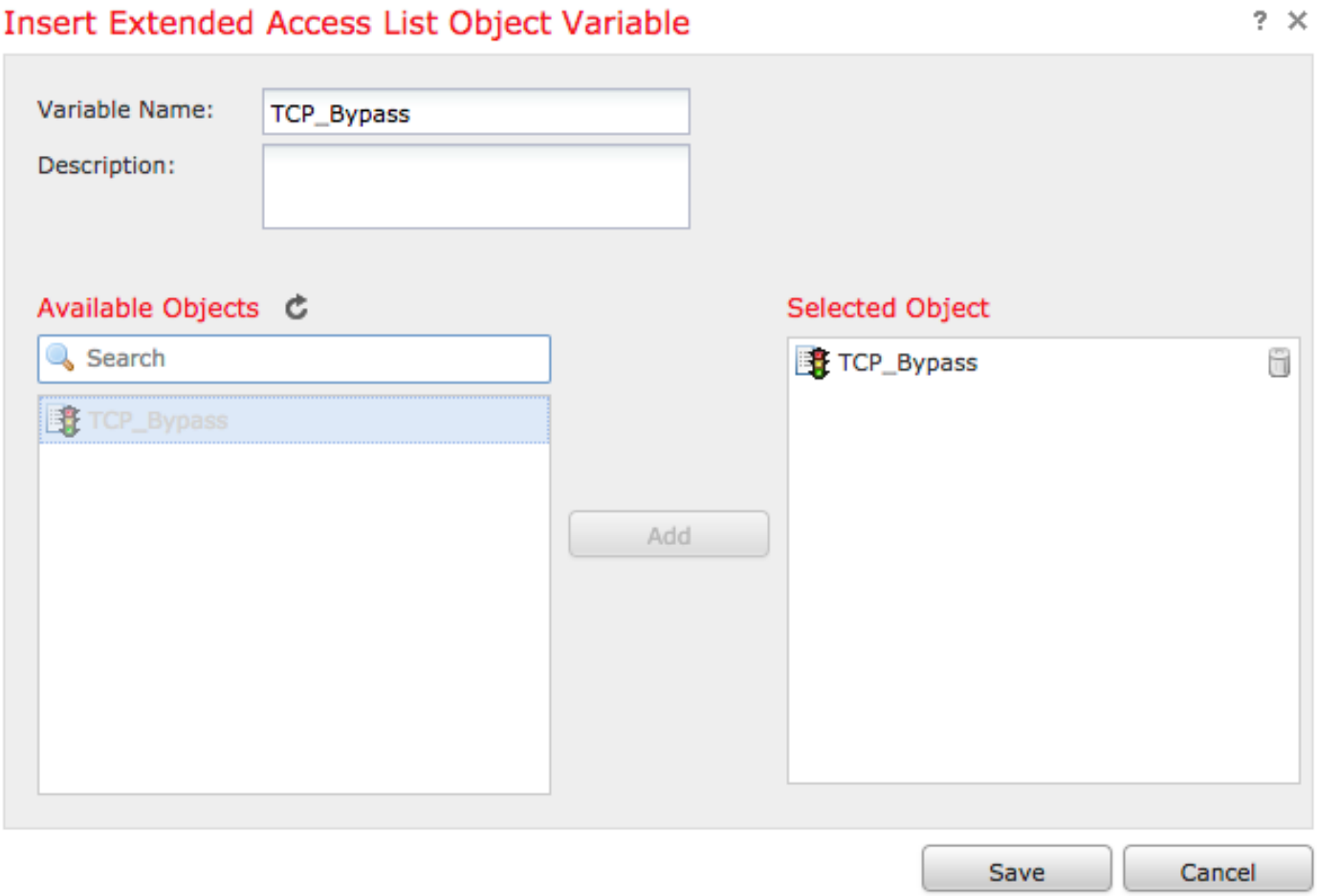


Opmerking: Kies de optie "Overleven". Dit staat voor het bewaren van deze configuratie

tijdens andere implementaties en upgrades.

Selecteer de toegangslijst die in Stap 1 is gemaakt in het gedeelte **Beschikbare objecten** en deel een variabele naam toe. Klik vervolgens op de knop **Toevoegen**. In dit voorbeeld is de Naam variabele **TCP_Bypass**.

Klik op **Opslaan**.

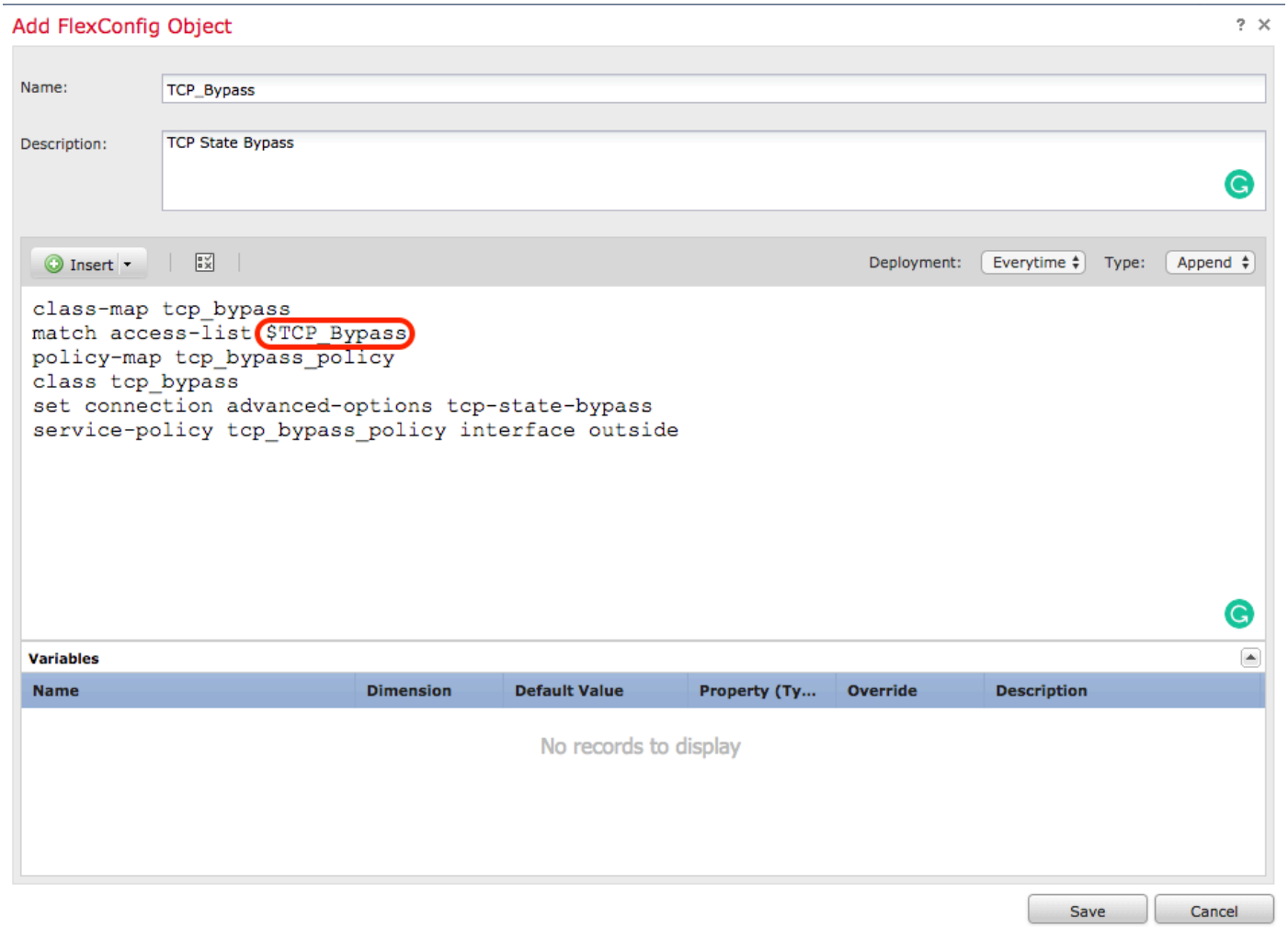


Voeg de volgende configuratielijnen in het blancoveld rechts onder de knop **invoegen** toe en neem de eerder gedefinieerde variabele (**$TCP_Bypass**) op in de *overeenkomende toegangslijst*-configuratielijn. Let op dat er een **$** symbool wordt toegevoegd aan de naam van de variabele. Dit helpt definiëren dat een variabele daarna volgt.

```
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
```

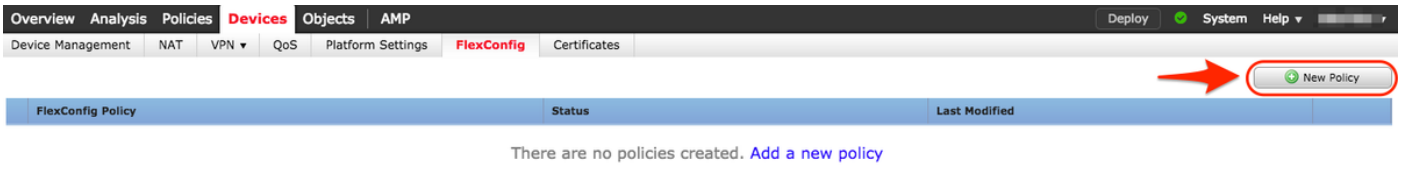
In dit voorbeeld wordt er een beleidskaart gemaakt die op de interface wordt toegepast. Als de TCP State Bypass vereist te worden geconfigureerd als onderdeel van het globale service beleid, kan de tcp_bypass class map worden toegepast op global_policy.

Klik op **Opslaan** na voltooiing.

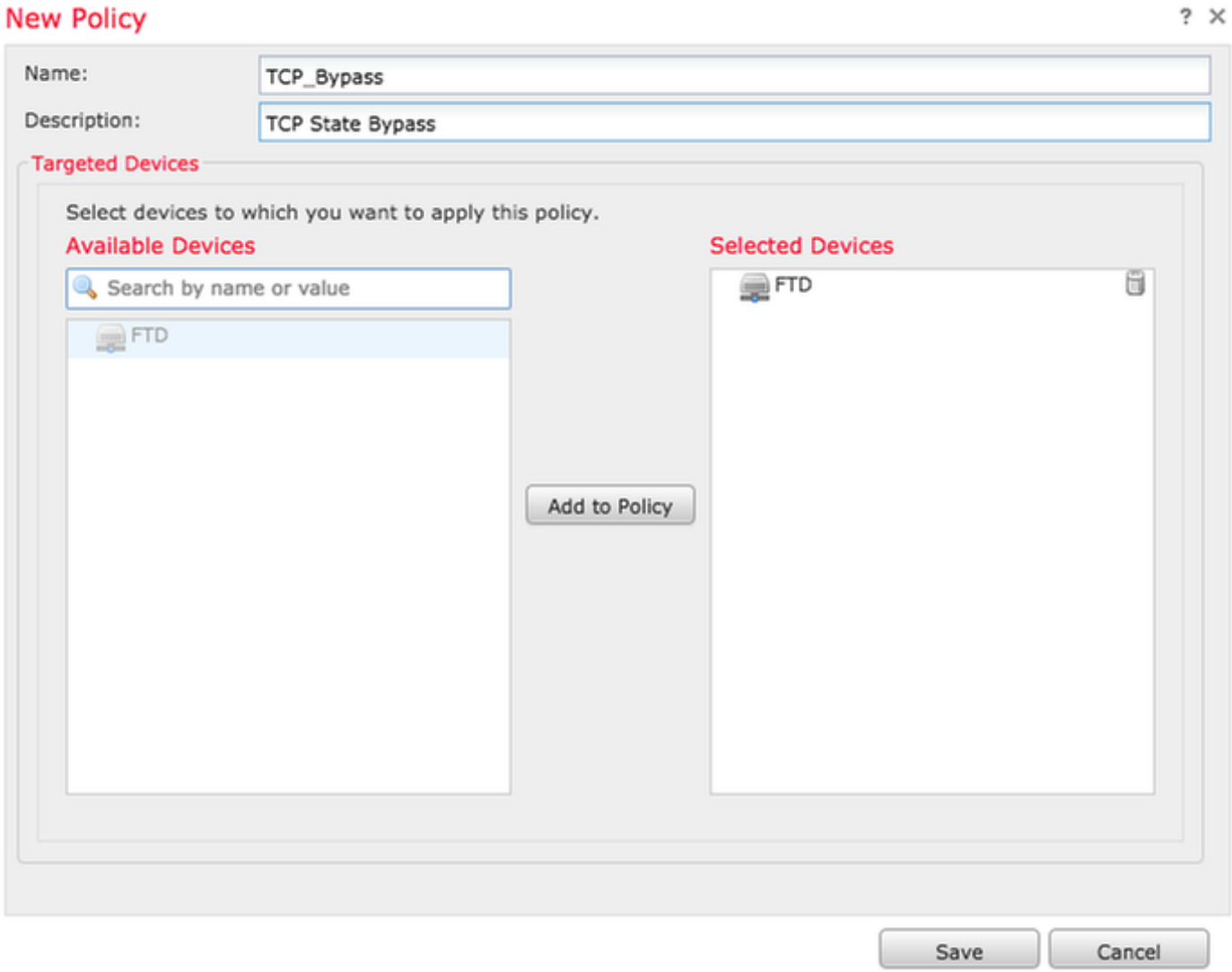


Stap 3. Een FlexConfig-beleid aan de FTD toewijzen

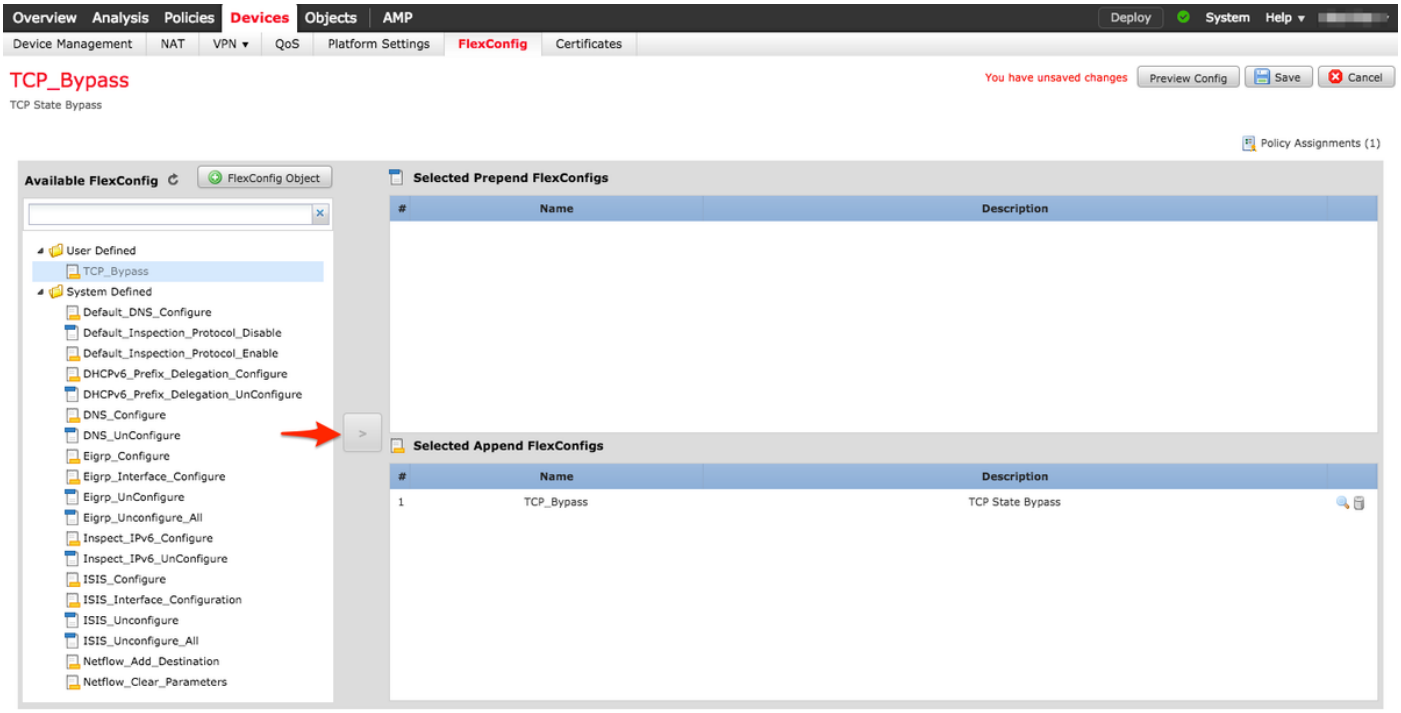
Ga naar **Apparaten > FlexConfig** en maak een nieuw beleid (tenzij er al een is gemaakt voor een ander doel en toegewezen aan dezelfde FTD).In dit voorbeeld wordt het nieuwe FelxConfig-beleid **TCP_Bypass** genoemd.



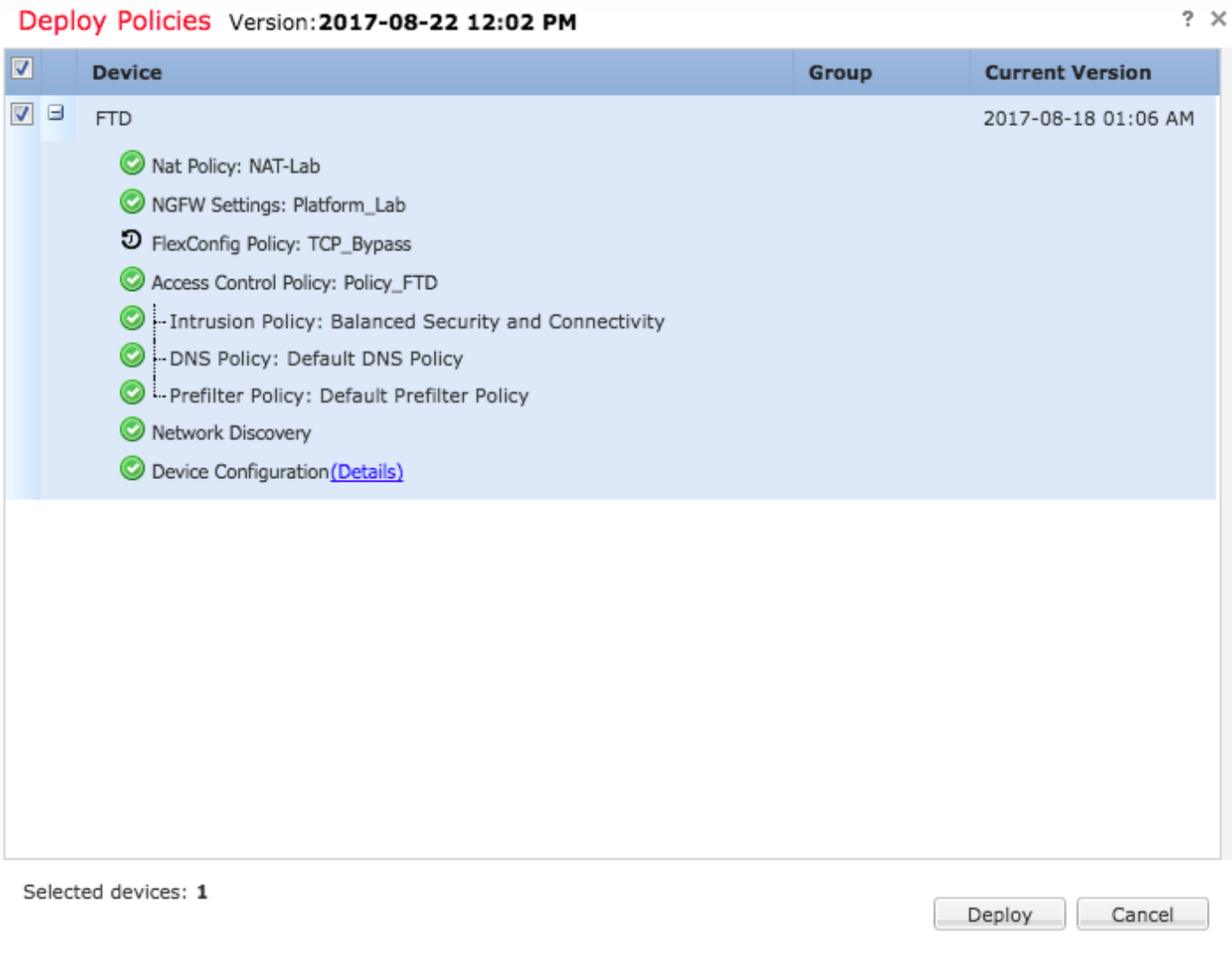
Wijs het **TCP_Bypass** FlexConfig beleid aan het FTD-apparaat toe.



Selecteer het object FlexConfig met de naam **TCP_Bypass** dat in Stap 2 is gemaakt onder de **door gebruiker gedefinieerde** sectie en klik op de pijl om dat object aan het beleid toe te voegen.



de wijzigingen opslaan en inzetten;



Verificatie

Toegang tot de FTD via SSH of console en gebruik de **ondersteuning voor diagnostische cli van het** opdrachtsysteem.

```
> 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
!
```

Problemen oplossen

Om deze optie te kunnen oplossen, resulteren deze opdrachten in behulpzaam.

```
- 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
```

Verwante links

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