FTD : Comment activer la configuration de contournement d'état de TCP utilisant la stratégie de FlexConfig

Contenu

Introduction

Ce document décrit comment implémenter la caractéristique de contournement de Protocole TCP (Transmission Control Protocol) sur des appliances de la défense contre des menaces de FirePOWER (FTD) par l'intermédiaire du centre de Gestion de FirePOWER (FMC) utilisant la stratégie de FlexConfig.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- La connaissance du centre de Gestion de FirePOWER.
- Connaissance de base de défense contre des menaces de FirePOWER.
- Compréhension de la caractéristique de contournement d'état de TCP.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Version 6.2 et ultérieures de la défense contre des menaces de FirePOWER (FTD).
- Version 6.2 et ultérieures du centre de Gestion de FirePOWER (FMC).

Informations générales

Le contournement d'état de TCP est une caractéristique héritée de l'appliance de sécurité adaptable (ASA) et fournit le trafic de pour le dépannage d'assistance qui pourrait être abandonné par l'un ou l'autre de caractéristiques de normalisation de TCP, d'états asymétriques de routage et de certaines inspections d'application.

Au moment d'écrire ce document, FMC ne le prend en charge pas naturellement pour configurer le contournement d'état de TCP, à moins que la stratégie de FlexConfig soit utilisée.

La défense contre des menaces de FirePOWER utilise des commandes de configuration ASA d'implémenter quelques caractéristiques, mais non toutes les caractéristiques. Il n'y a aucun seul ensemble de commandes de configuration de défense contre des menaces de FirePOWER. Au lieu de cela, le point de FlexConfig est de te permettre pour configurer les caractéristiques qui ne sont pas encore directement prises en charge par des stratégies et des configurations de centre de Gestion de FirePOWER.

> **Note**: Le contournement d'état de TCP devrait seulement être utilisé pour dépanner des buts ou quand le routage asymétrique ne peut pas être résolu. L'utilisation de cette caractéristique désactive de plusieurs fonctionnalités de sécurité et peut entraîner le nombre élevé de connexions si elle n'est pas correctement mise en application.

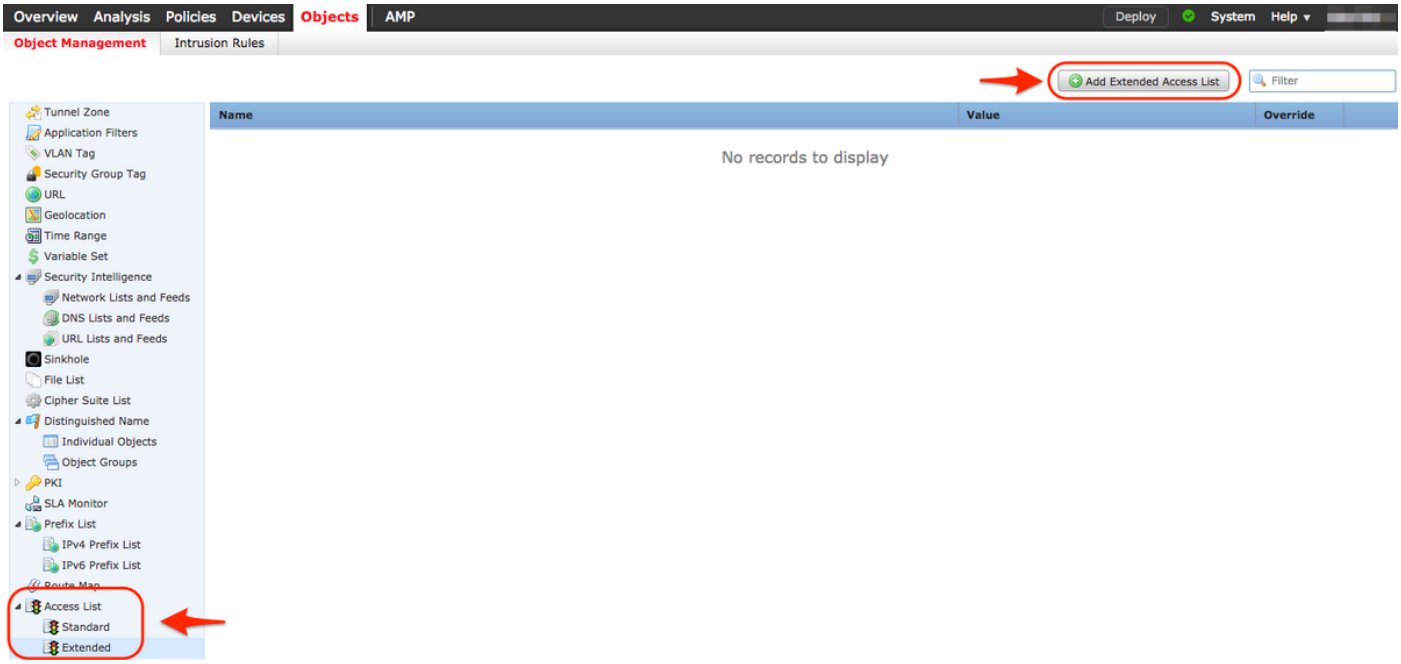
Afin de connaître plus la caractéristique de contournement d'état de TCP ou son implémentation dans l'ASA, référez-vous configurent la caractéristique de contournement d'état de TCP sur la gamme ASA 5500 et le guide de configuration de gamme de Cisco ASA 5500.

Configuration

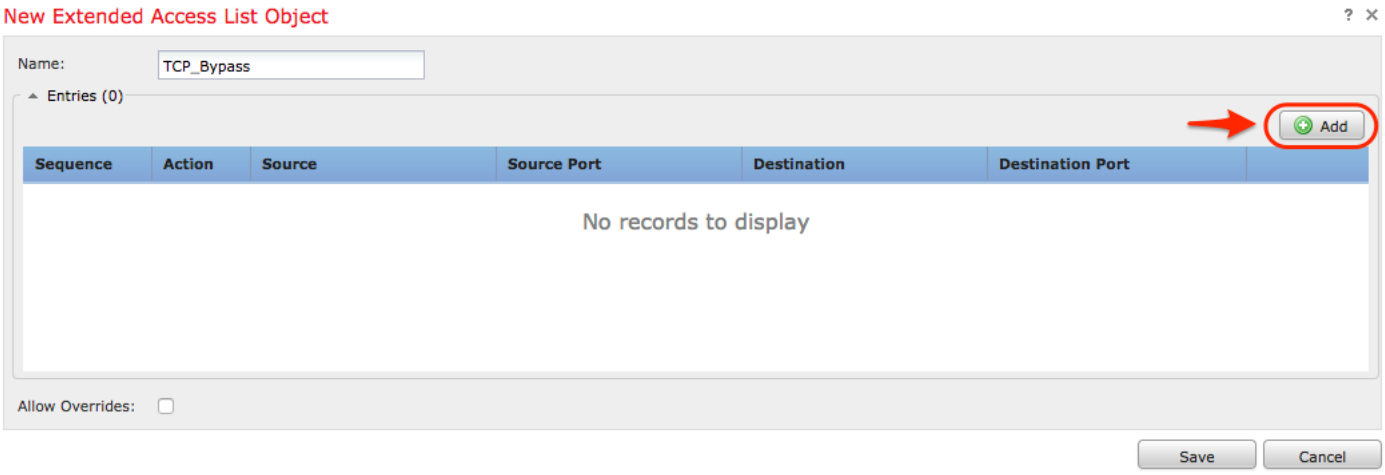
Cette section décrit comment configurer le contournement de TCP sur FMC par une stratégie de FlexConfig.

Étape 1. Configurez un objet étendu de liste d'accès

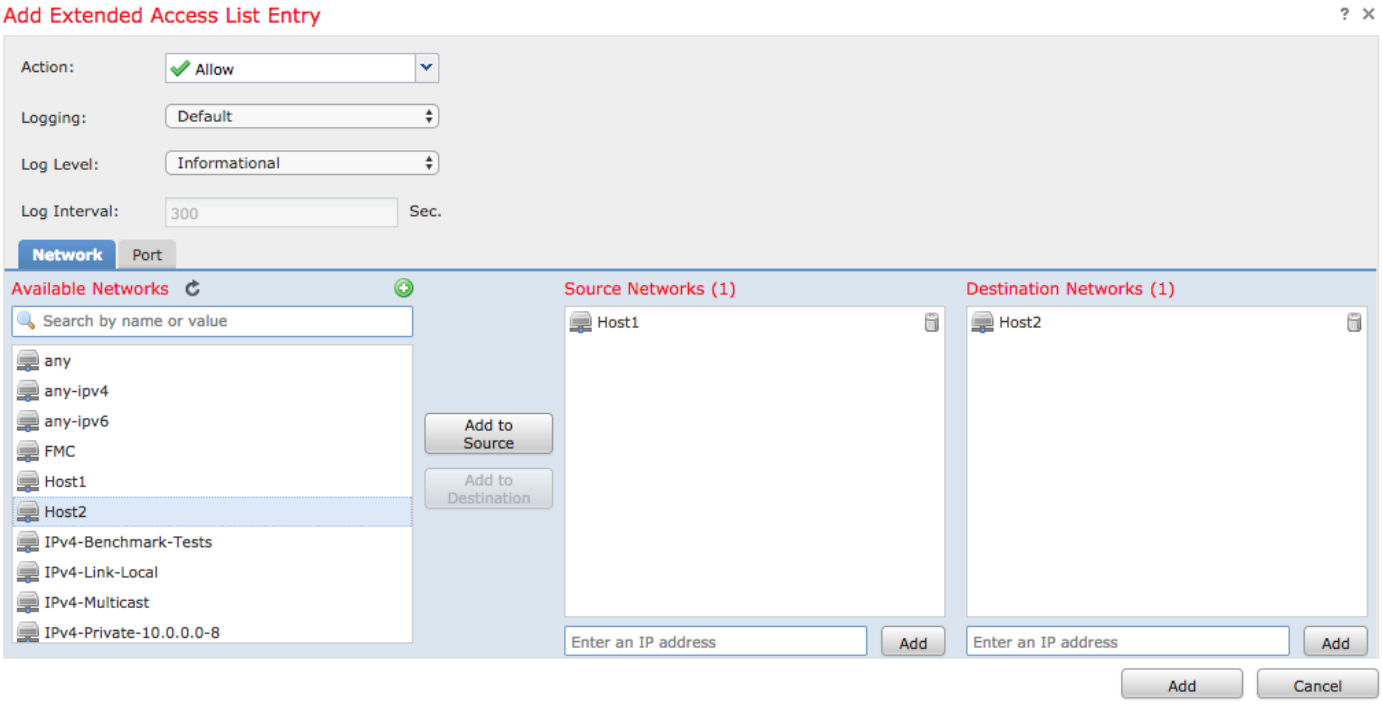
Afin de créer une liste d'accès étendue sur FMC, allez à la **Gestion de >Object d'objets** et sur le menu de gauche, sous **étendu** choisi de **liste d'accès.** ClickAdd **a étendu la liste d'accès.**



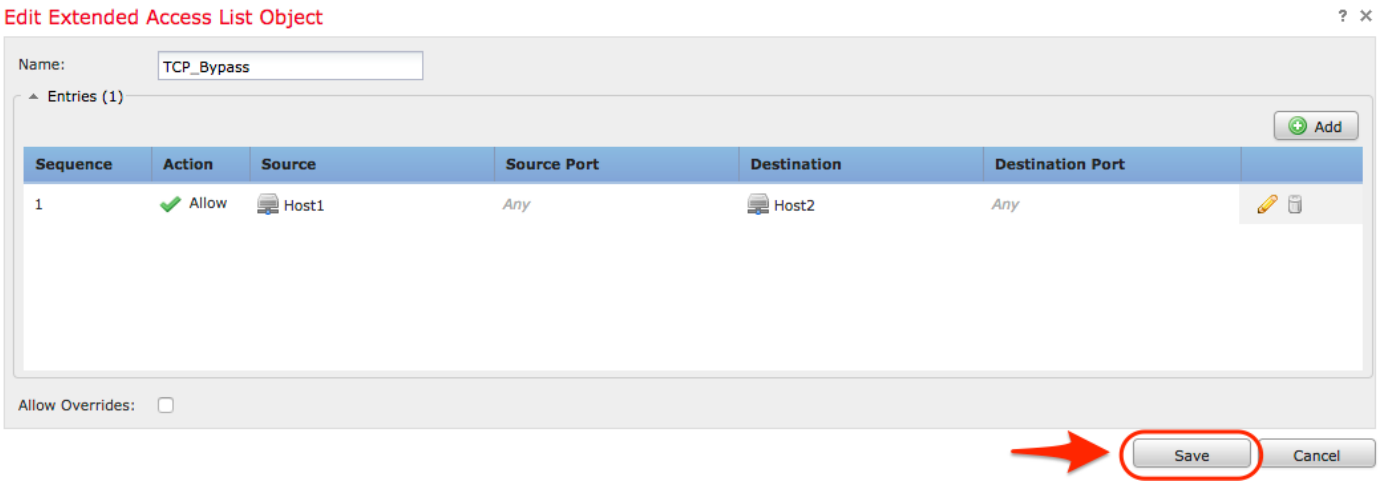
Remplissez zone d'identification de valeur désirée. dans cet exemple, le nom est **TCP_Bypass**. Cliquez sur Add **le bouton.**



L'action pour cette règle doit être configurée comme **laissent.** Un réseau défini par système peut être utilisé ou un nouvel objet de réseau peut être créé pour chaque source et destination. Dans cet exemple, la liste d'accès apparie le trafic IP de Host1 à Host2 car c'est la transmission pour appliquer le contournement d'état de TCP. L'onglet de port peut sur option être utilisé pour apparier un TCP ou un port UDP spécifique. Cliquez sur en fonction le bouton d'**ajouter** pour continuer.

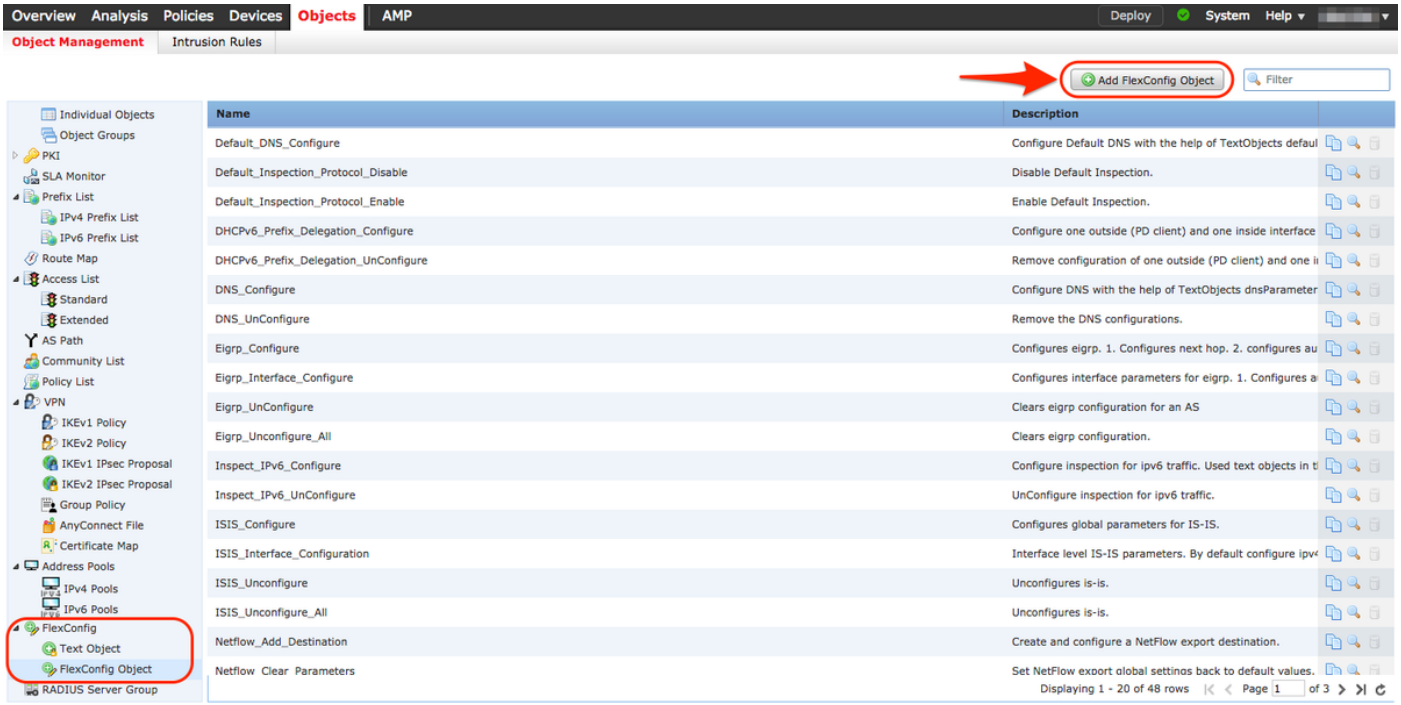


Une fois que la source et les réseaux ou les hôtes de destination sont sélectionnés, cliquez sur en fonction la **sauvegarde**.



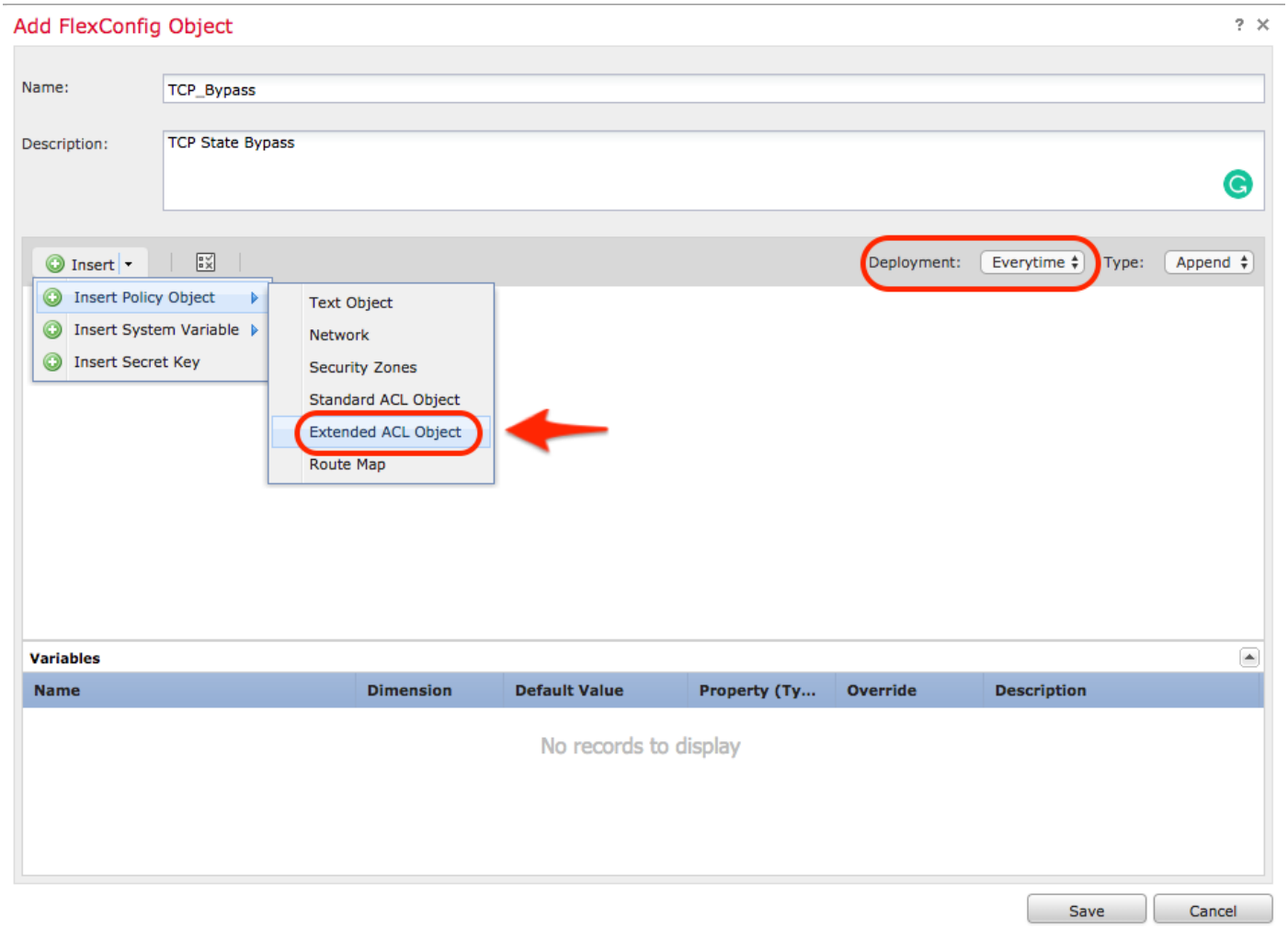
Étape 2. Configurez un objet de FlexConfig

Naviguez vers les **objets > la Gestion d'objet > le FlexConfig > l'objet de FlexConfig** et cliquez sur en fonction le bouton d'**objet Add FlexConfig**.



Le nom de l'objet pour cet exemple s'appelle **TCP_Bypass** juste comme la liste d'accès. Ce nom n'a pas besoin d'apparier le nom de liste d'accès.

Objet choisi de **stratégie d'insertion > objet étendu d'ACL.**

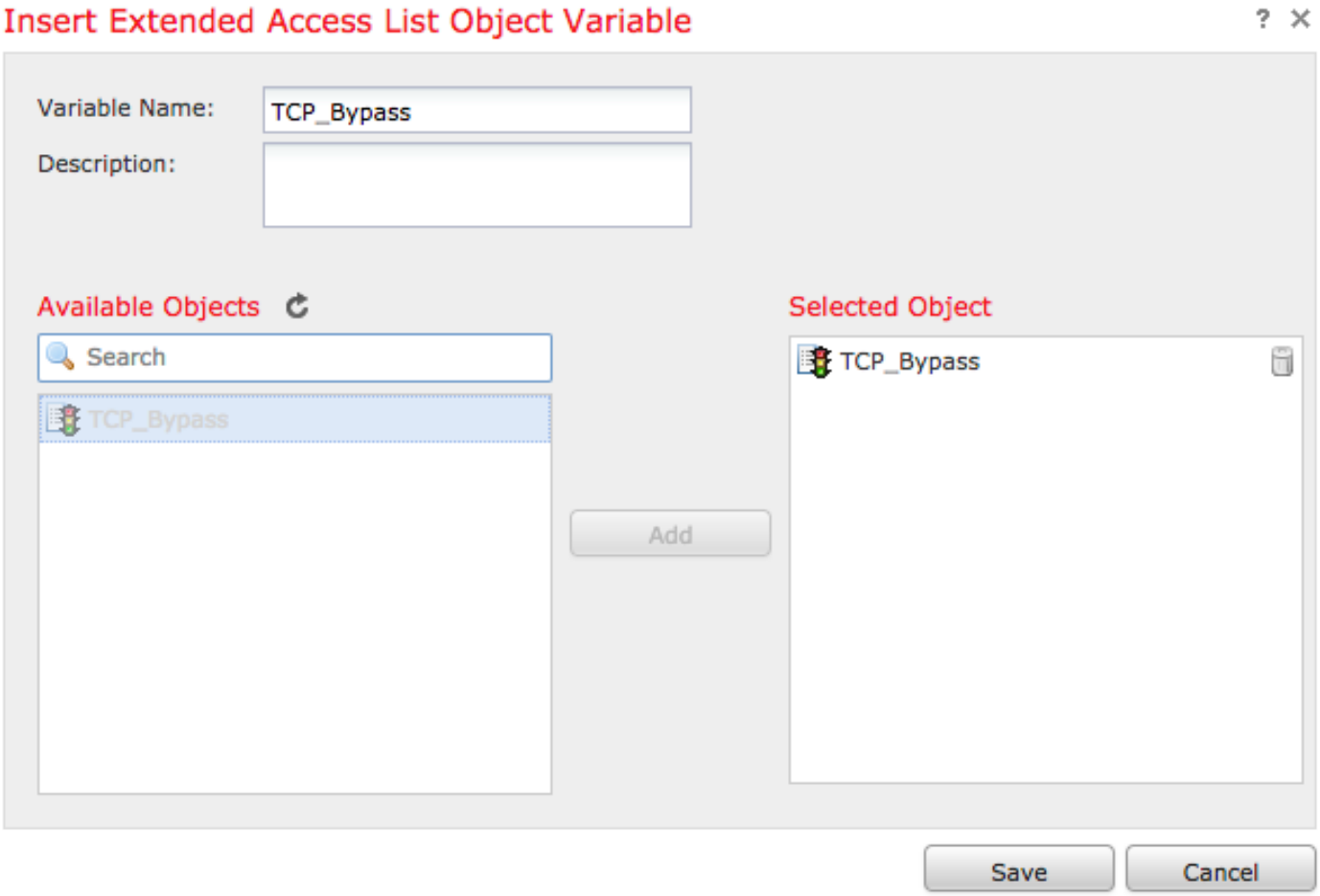


Note: Actuellement, et selon des BU, quand un policy-map est appliqué sur une interface il

est retiré dans le prochain déploiement et c'est comportement prévu. Le contournement pour cette question est de créer l'objet de flexible-config avec « chaque fois » l'option configurée pour le mode de déploiement.

Sélectionnez la liste d'accès créée dans l'étape 1 de la section **disponible d'objets** et assignez un nom de la variable. Puis, cliquez sur en fonction le bouton **Add**. Dans cet exemple, le nom de la variable est **TCP_Bypass**.

Cliquez sur en fonction la **sauvegarde**.

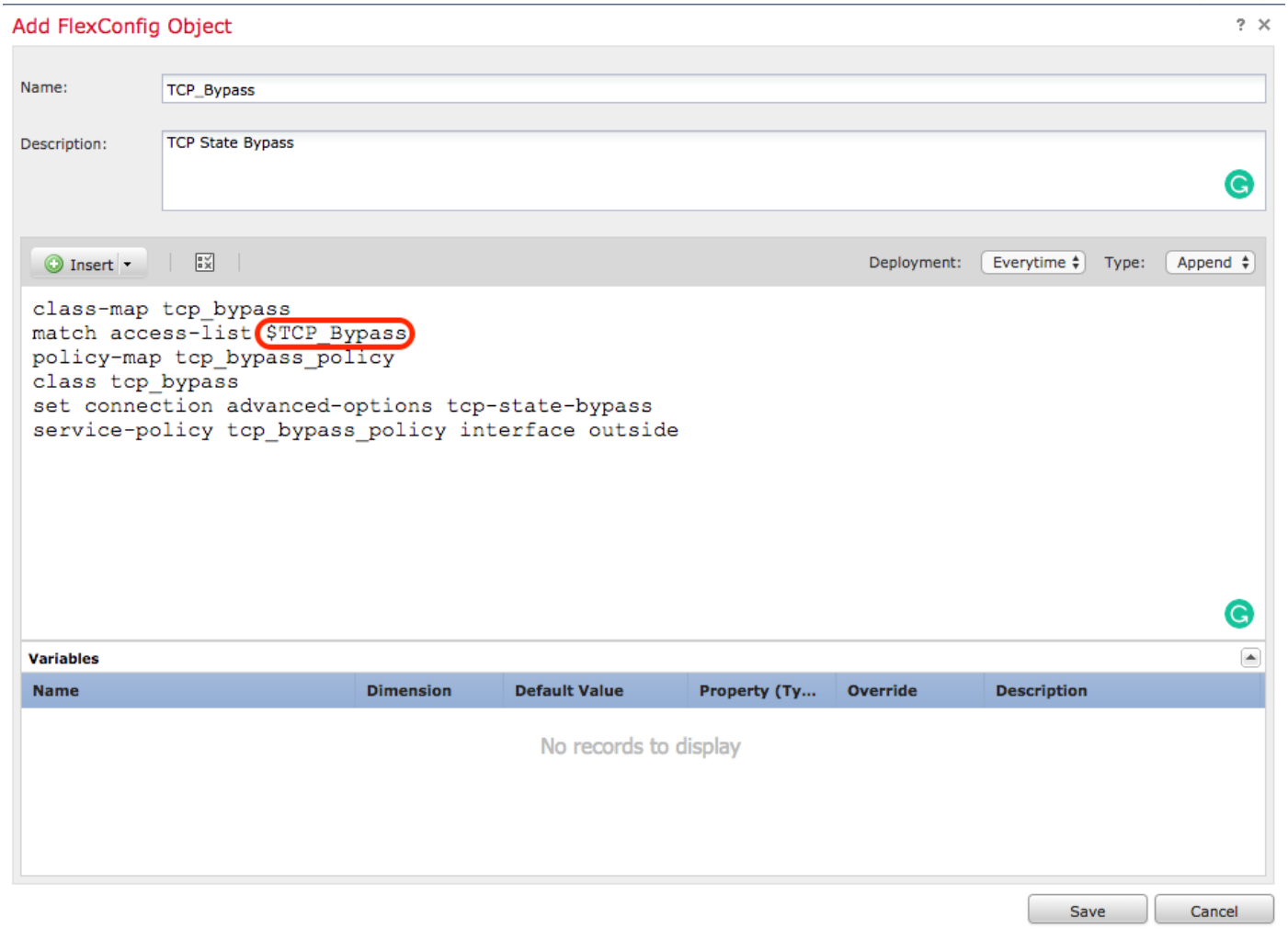


Ajoutez les prochaines lignes de configuration dans le juste de champ vide au-dessous du bouton d'**insertion** et incluez la variable précédemment définie (**$TCP_Bypass**) dans la ligne de configuration de *match access-list*. Notez qu'un symbole **$** est ajouté au début au nom de la variable. Ceci aide à définir qu'une variable suit après elle.

```
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
```

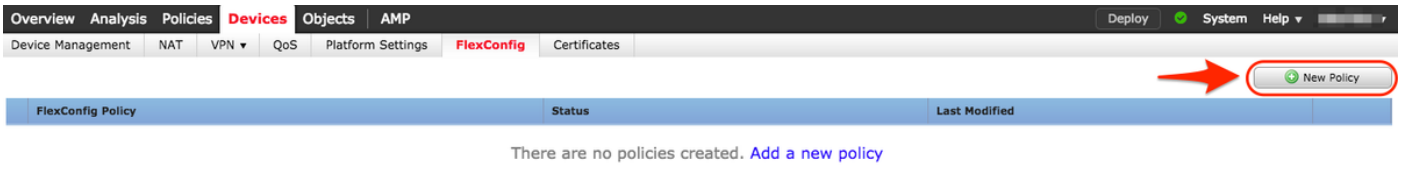
Dans cet exemple, un policy-map est créé et il est appliqué à l'interface extérieure. Si le contournement d'état de TCP exige d'être configuré en tant qu'élément de la stratégie de service mondial, le class map de tcp_bypass peut être appliqué au global_policy.

Cliquez sur en fonction la **sauvegarde** une fois terminé.

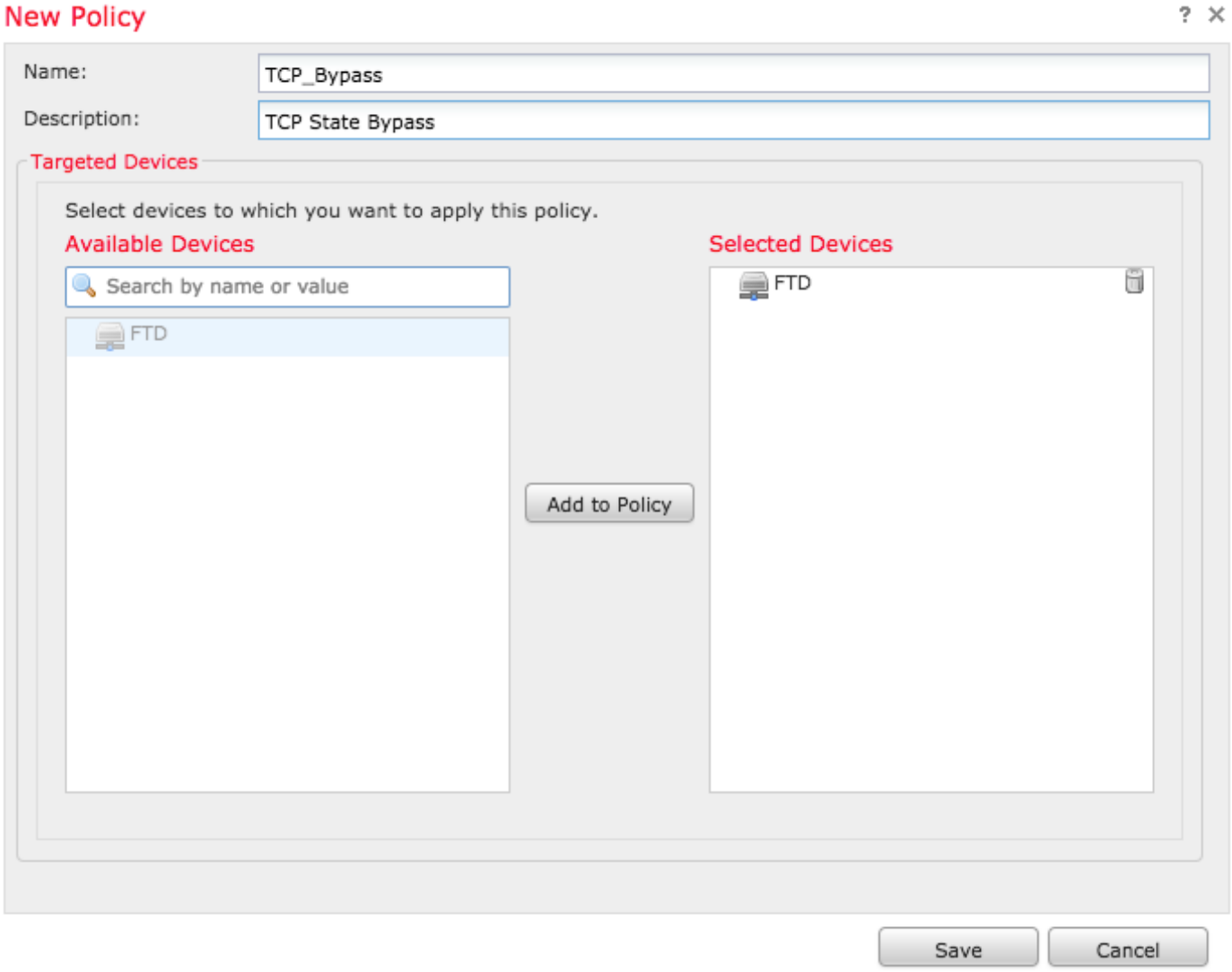


Étape 3. Assignez une stratégie de FlexConfig au FTD

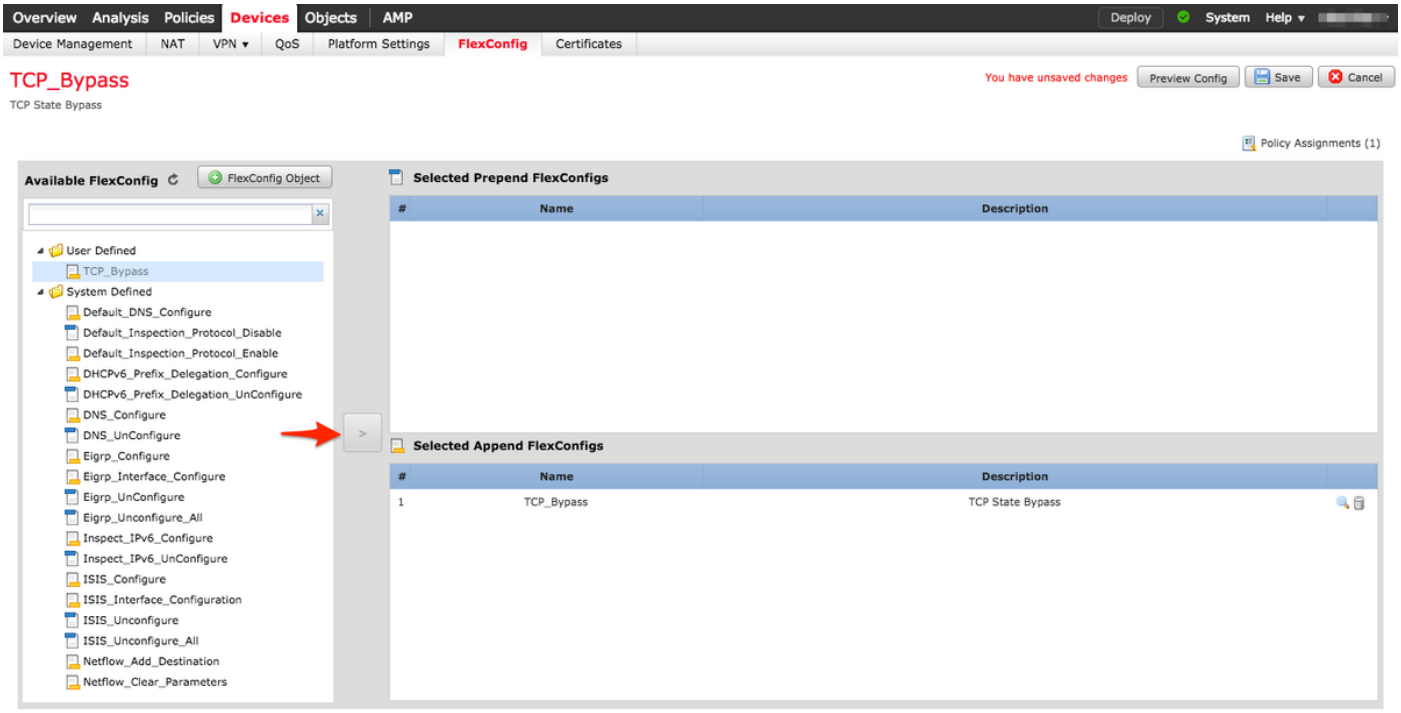
Allez aux **périphériques > au FlexConfig** et créez une nouvelle stratégie (à moins qu'il y a déjà d'une créée pour un autre but et assignée au même FTD). Dans cet exemple la nouvelle stratégie de FelxConfig s'appelle **TCP_Bypass**.



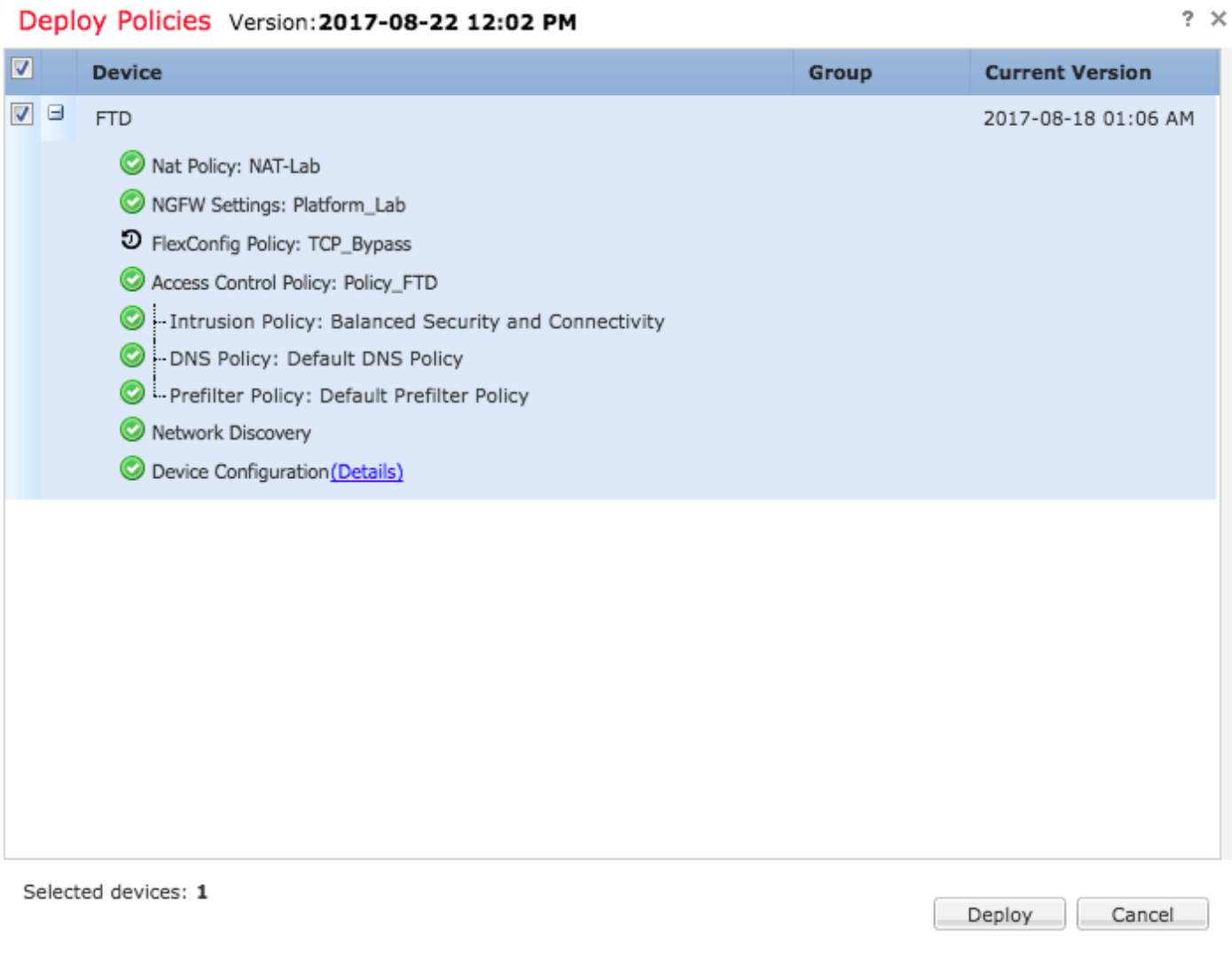
Assignez la stratégie de **TCP_Bypass** FlexConfig au périphérique FTD.



Sélectionnez l'objet de FlexConfig appelé **TCP_Bypass** créé dans l'étape 2 sous la section **définie par l'utilisateur** et cliquez sur en fonction la flèche pour ajouter cet objet à la stratégie.



Sauvegardez les modifications et déployez-vous,



Vérification

Accédez au FTD par le SSH ou la console et utilisez l'**assistance technique diagnostic-cli de** commande.

```
> 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
!
```

Dépannez

Pour dépanner cette caractéristique, résultat de ces commandes utile.

- 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

Liens connexes

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