FTD : Comment activer la configuration de contournement de l'état TCP à l'aide de la stratégie FlexConfig

Contenu

Introduction

Ce document décrit comment mettre en oeuvre la fonctionnalité de contournement d'état TCP (Transmission Control Protocol) sur les appliances Firepower Threat Defense (FTD) via Firepower Management Center (FMC) à l'aide de la stratégie FlexConfig dans les versions antérieures à la version 6.3.0.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissance du Centre de gestion Firepower.
- Connaissances de base sur la protection contre les menaces de Firepower.
- Compréhension de la fonction TCP State Bypass.

Components Used

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

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

Informations générales

Le contournement d'état TCP est une fonctionnalité héritée de l'appliance de sécurité adaptatif (ASA) et fournit une assistance lors du dépannage du trafic qui pourrait être abandonné par les fonctions de normalisation TCP, les conditions de routage asymétrique et certaines inspections d'applications.

Cette fonctionnalité est nativement prise en charge sur FMC à partir de la version 6.3.0. Il est recommandé de supprimer les objets Flexconfig après la mise à niveau et de déplacer cette configuration vers le FMC avant le premier déploiement. Pour plus d'informations sur la configuration du contournement de l'état TCP dans la version 6.3.0 ou ultérieure, consultez ce guide de configuration.

Firepower Threat Defense utilise des commandes de configuration ASA pour implémenter certaines fonctionnalités, mais pas toutes. Il n'existe pas d'ensemble unique de commandes de configuration Firepower Threat Defense. Au lieu de cela, l'objectif de FlexConfig est de vous permettre de configurer des fonctionnalités qui ne sont pas encore prises en charge directement par le biais des stratégies et paramètres Firepower Management Center.

> **Remarque** : Le contournement de l'état TCP doit être utilisé uniquement à des fins de dépannage ou lorsque le routage asymétrique ne peut pas être résolu. L'utilisation de cette fonctionnalité désactive plusieurs fonctions de sécurité et peut entraîner un nombre élevé de connexions si elle n'est pas correctement implémentée.

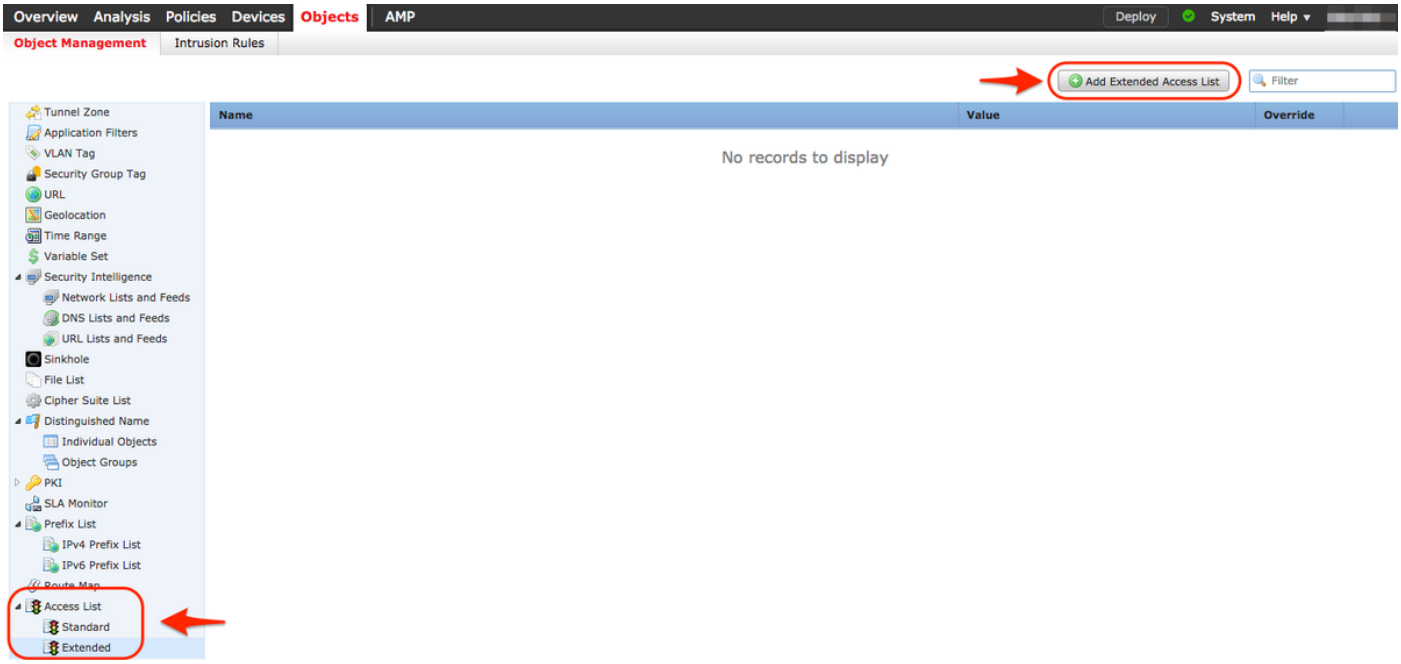
Pour en savoir plus sur la fonctionnalité de contournement d'état TCP ou sa mise en oeuvre dans ASA, référez-vous à Configurer la fonctionnalité de contournement d'état TCP sur la gamme ASA 5500 et au Guide de configuration de la gamme Cisco ASA 5500.

Configuration

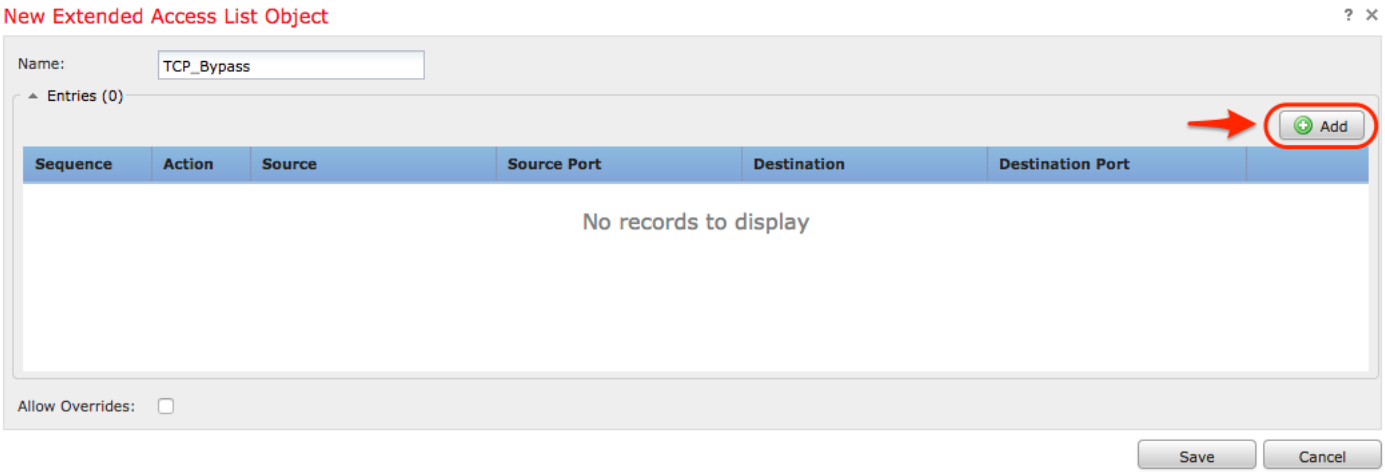
Cette section décrit comment configurer le contournement de l'état TCP sur FMC via une stratégie FlexConfig.

Étape 1. Configurer un objet de liste de contrôle d'accès étendue

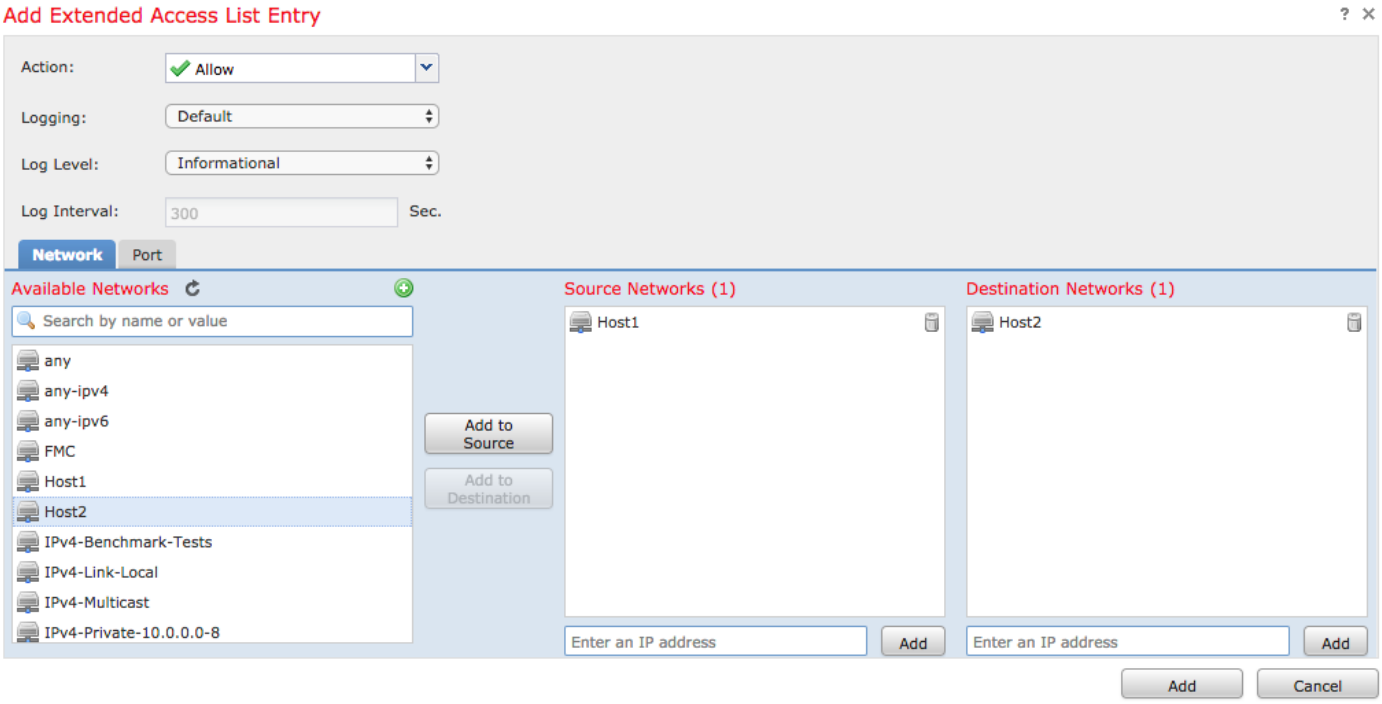
Afin de créer une liste d'accès étendue sur FMC, accédez à **Objets > Gestion des objets** et dans le menu de gauche, sous **Liste d'accès** sélectionnez **Étendue. Cliquez sur Ajouter une liste d'accès étendue.**



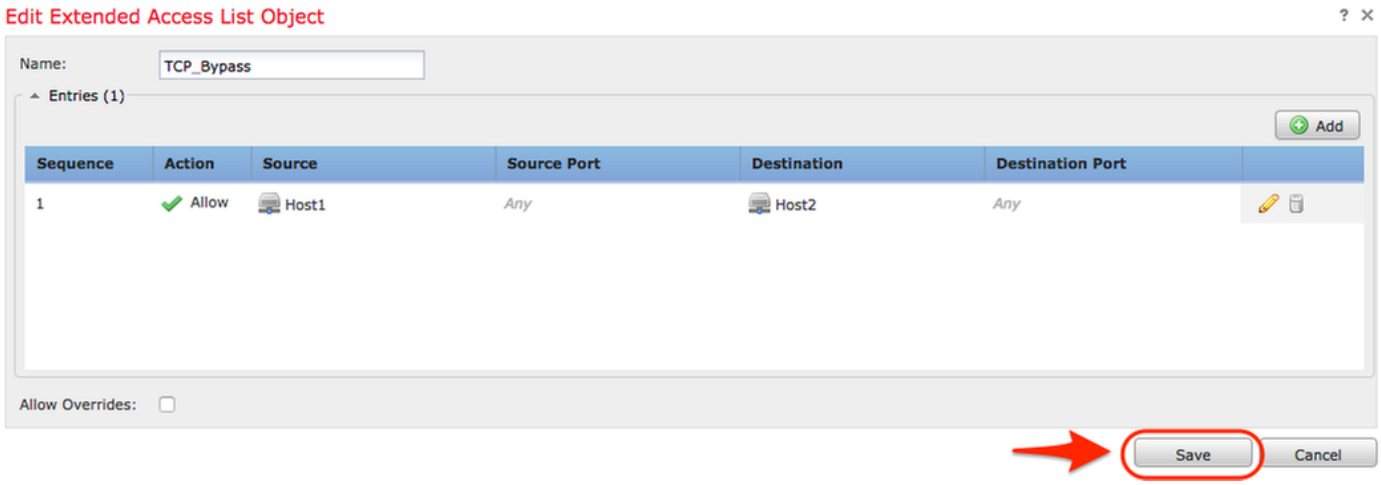
Remplissez le champ Nom avec la valeur souhaitée. dans cet exemple, le nom est **TCP_Bypass**. Cliquez sur le bouton **Ajouter**.



L'action de cette règle doit être configurée comme **Autoriser.** Un réseau défini par le système peut être utilisé ou un nouvel objet réseau peut être créé pour chaque source et destination. Dans cet exemple, la liste de contrôle d'accès fait correspondre le trafic IP de l'hôte 1 à l'hôte 2, car il s'agit de la communication pour appliquer le contournement de l'état TCP. L'onglet Port peut éventuellement être utilisé pour correspondre à un port TCP ou UDP spécifique. Cliquez sur le bouton **Ajouter** pour continuer.

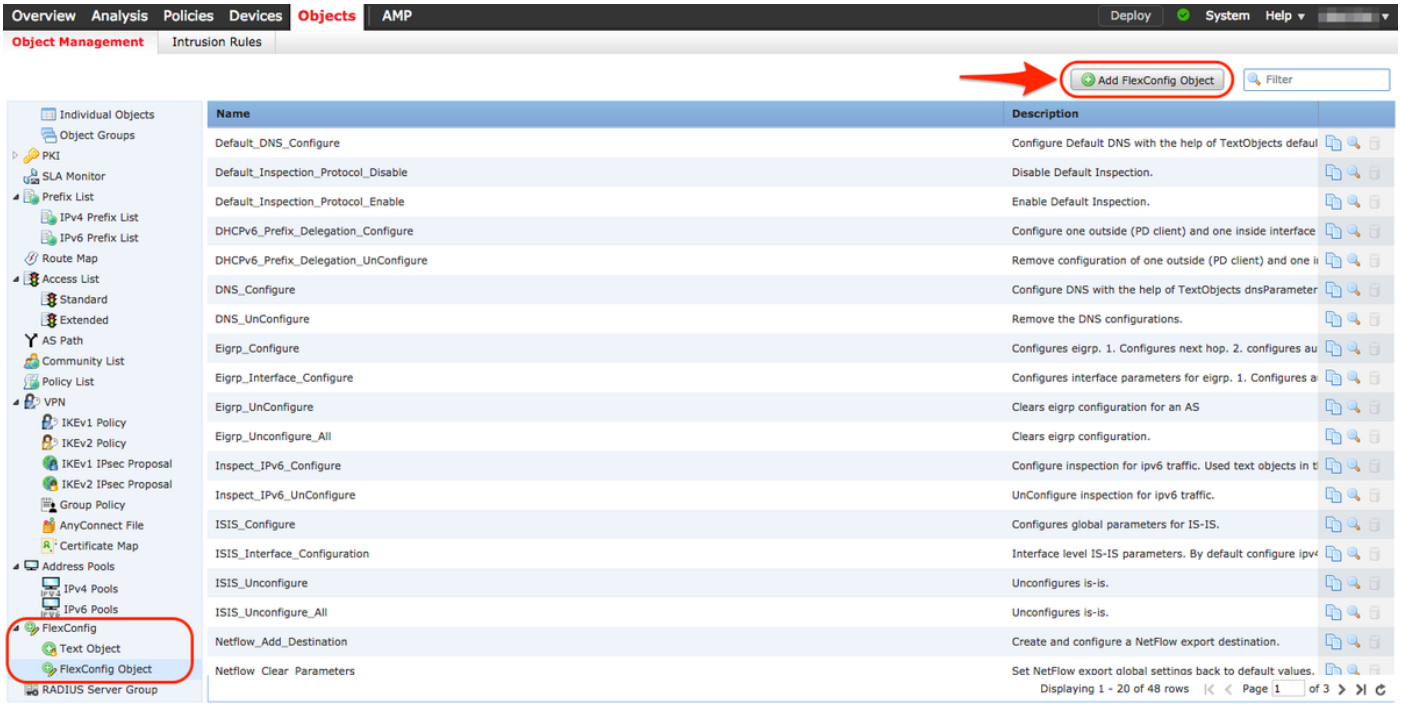


Une fois que les réseaux ou hôtes source et de destination sont sélectionnés, cliquez sur **Enregistrer**.



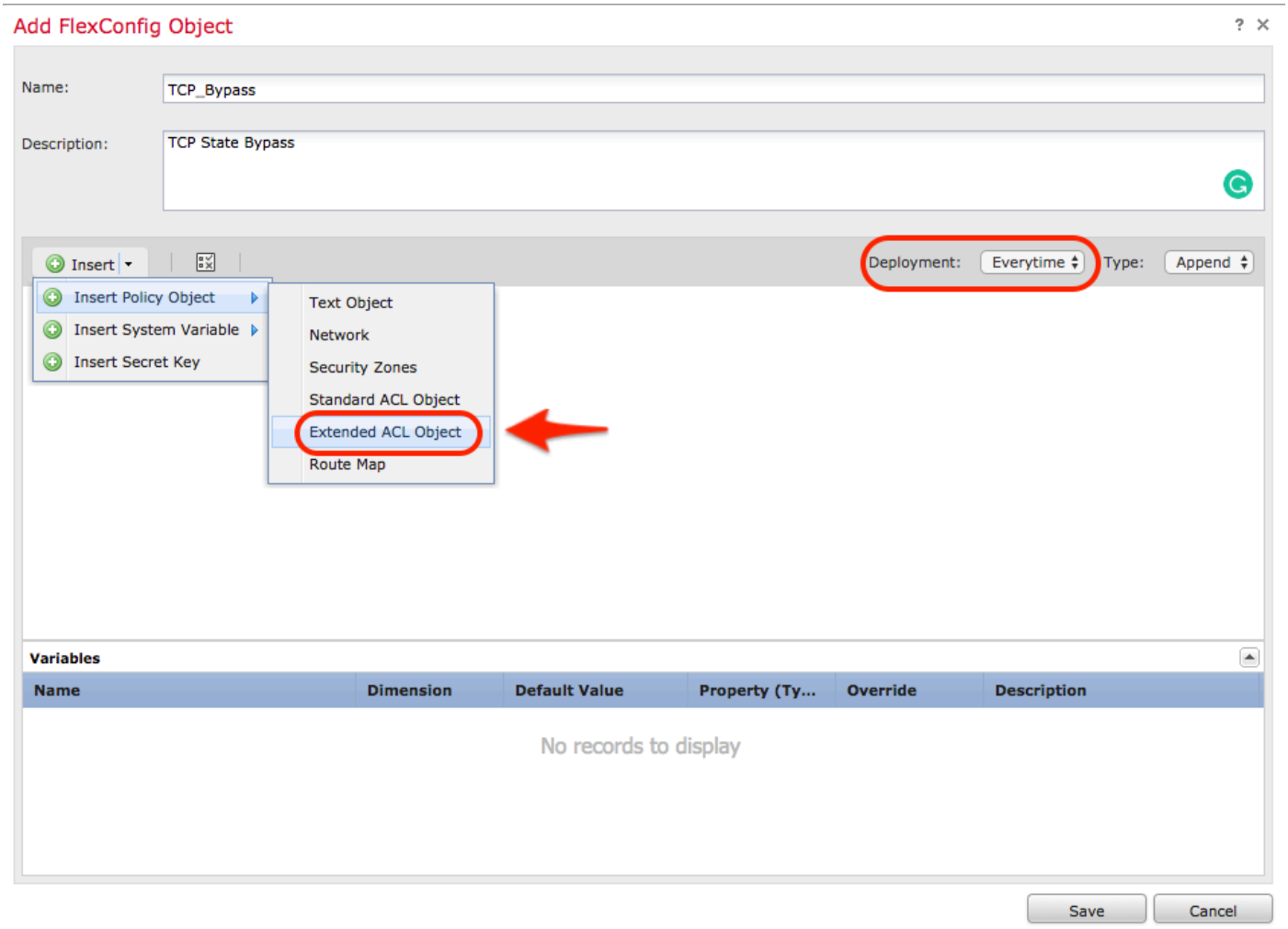
Étape 2. Configurer un objet FlexConfig

Accédez à **Objets > Gestion des objets > FlexConfig > FlexConfig Object** et cliquez sur le bouton **Ajouter un objet FlexConfig**.



Le nom de l'objet pour cet exemple est appelé **TCP_Bypass** comme la liste d'accès. Ce nom ne doit pas nécessairement correspondre au nom de la liste d'accès.

Sélectionnez **Insert Policy Object > Extended ACL Object.**

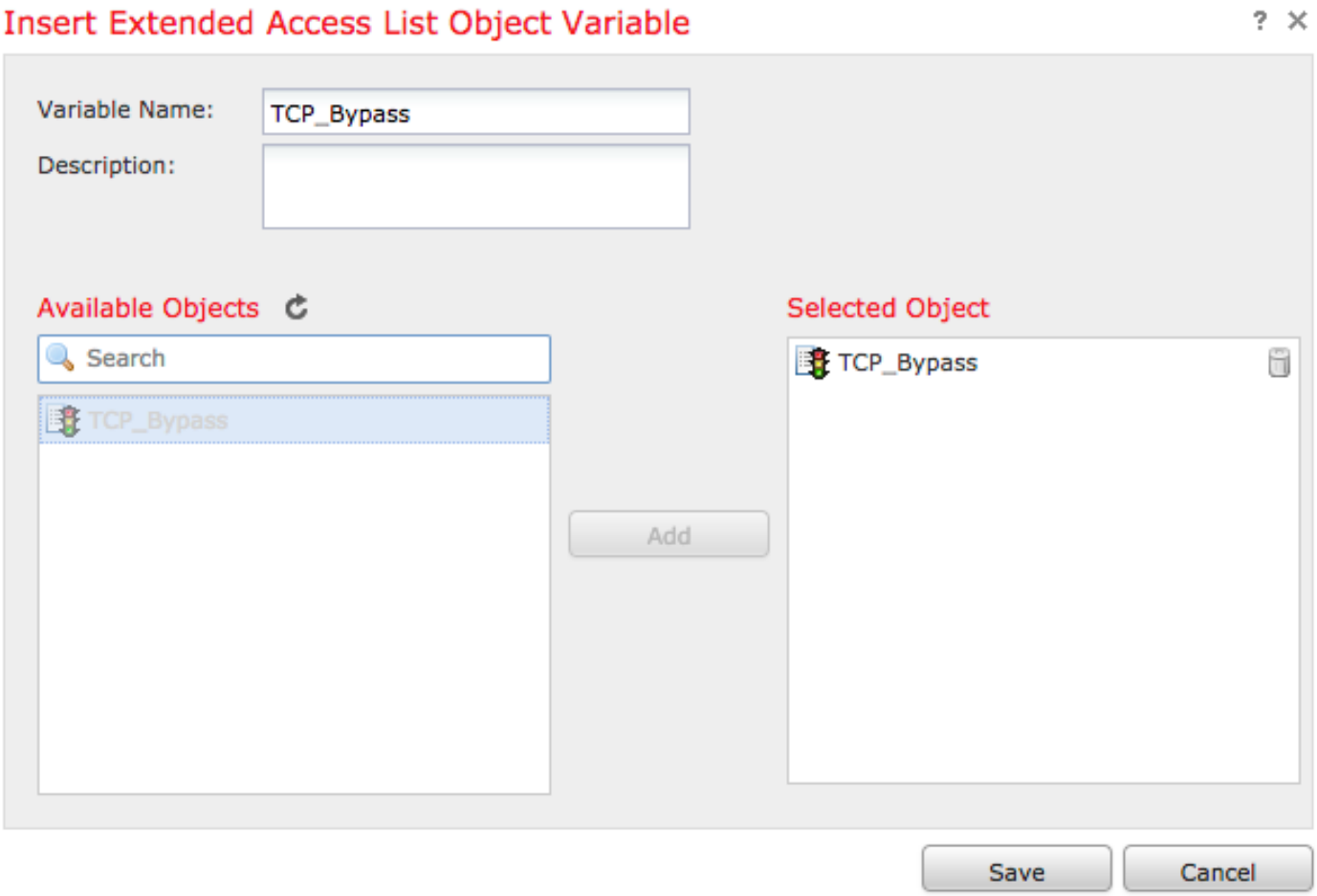


Note: Veillez à choisir l'option « Tout le temps ». Cela permet de conserver cette

configuration lors d'autres déploiements et mises à niveau.

Sélectionnez la liste d'accès créée à l'étape 1 dans la section **Objets disponibles** et attribuez un nom de variable. Ensuite, cliquez sur le bouton **Ajouter**. Dans cet exemple, le nom de variable est **TCP_Bypass**.

Cliquez sur **Enregistrer**.

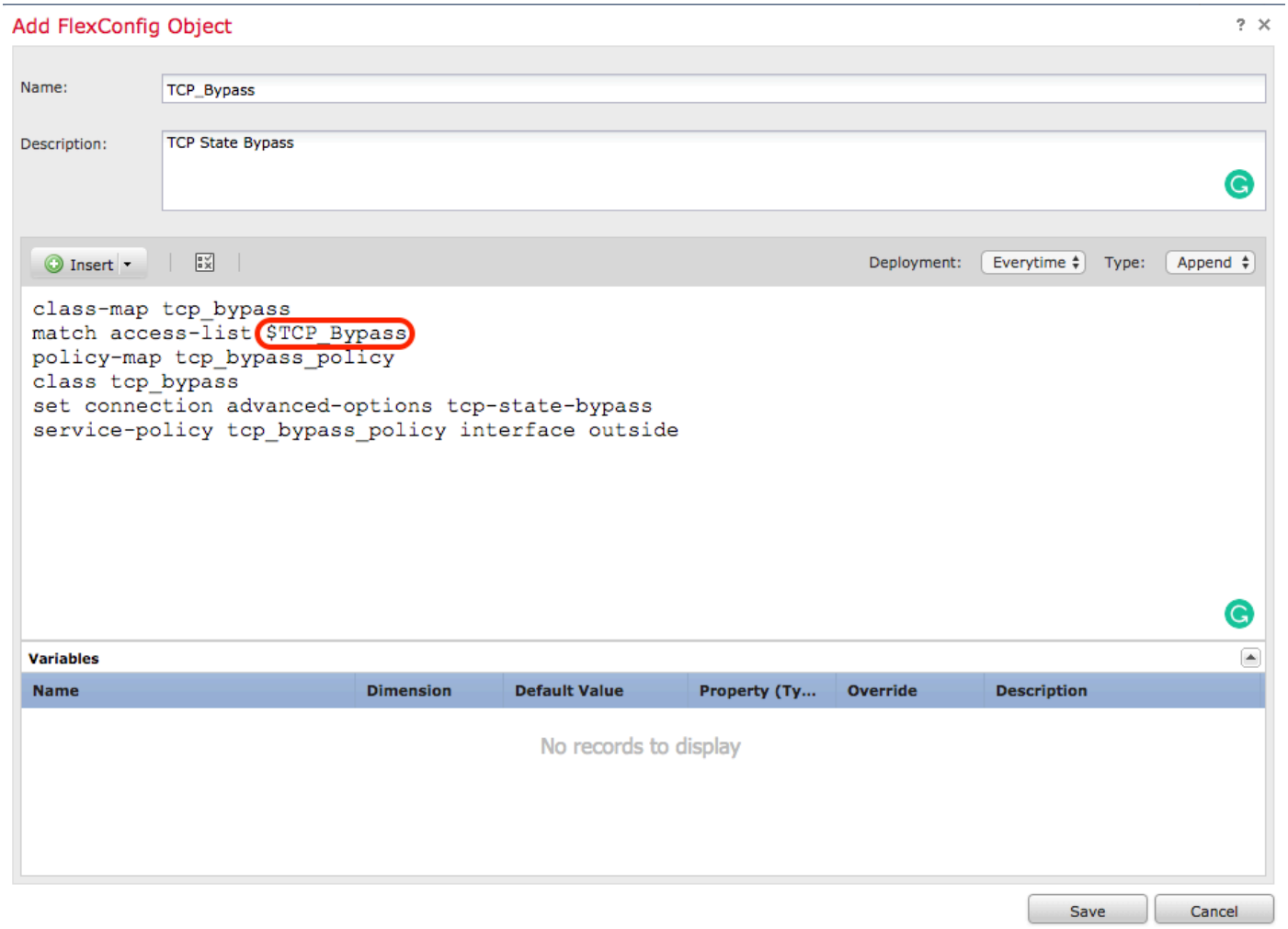


Ajoutez les lignes de configuration suivantes dans le champ vide situé juste en dessous du bouton **Insertion** et incluez la variable précédemment définie (**$TCP_Bypass**) dans la ligne de configuration *match access-list*. Notez qu'un symbole **$** est précédé du nom de la variable. Cela permet de définir qu'une variable suit.

```
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
```

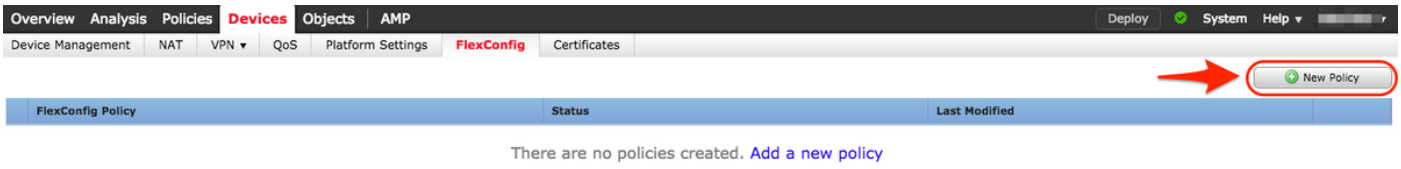
Dans cet exemple, une carte-politique est créée et appliquée à l'interface externe. Si le contournement de l'état TCP doit être configuré dans le cadre de la stratégie de service globale, la carte de classe tcp_bypass peut être appliquée à global_policy.

Cliquez sur **Enregistrer** lorsque vous avez terminé.

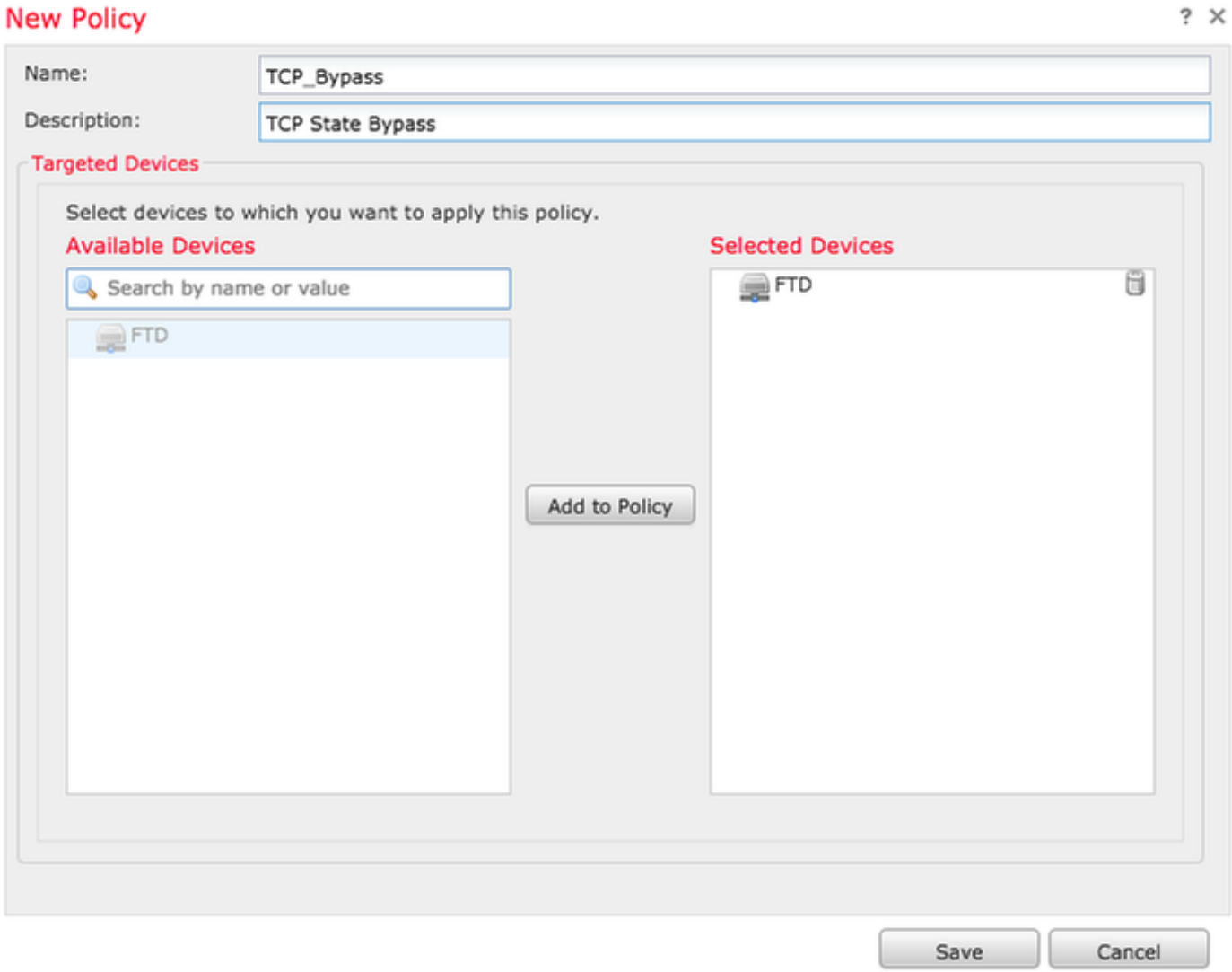


Étape 3. Affecter une stratégie FlexConfig au FTD

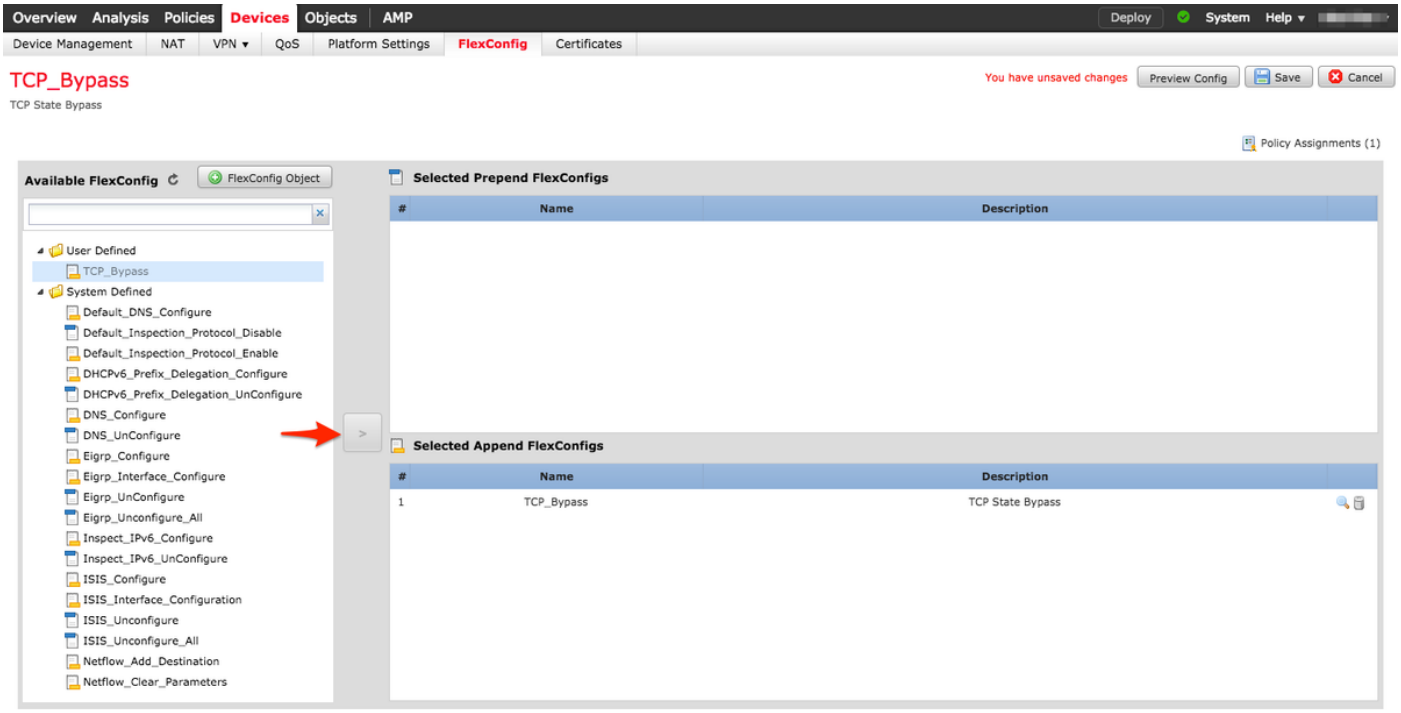
Accédez à **Périphériques > FlexConfig** et créez une nouvelle stratégie (sauf si une stratégie a déjà été créée à une autre fin et affectée au même FTD).Dans cet exemple, la nouvelle stratégie FelxConfig est appelée **TCP_Bypass**.



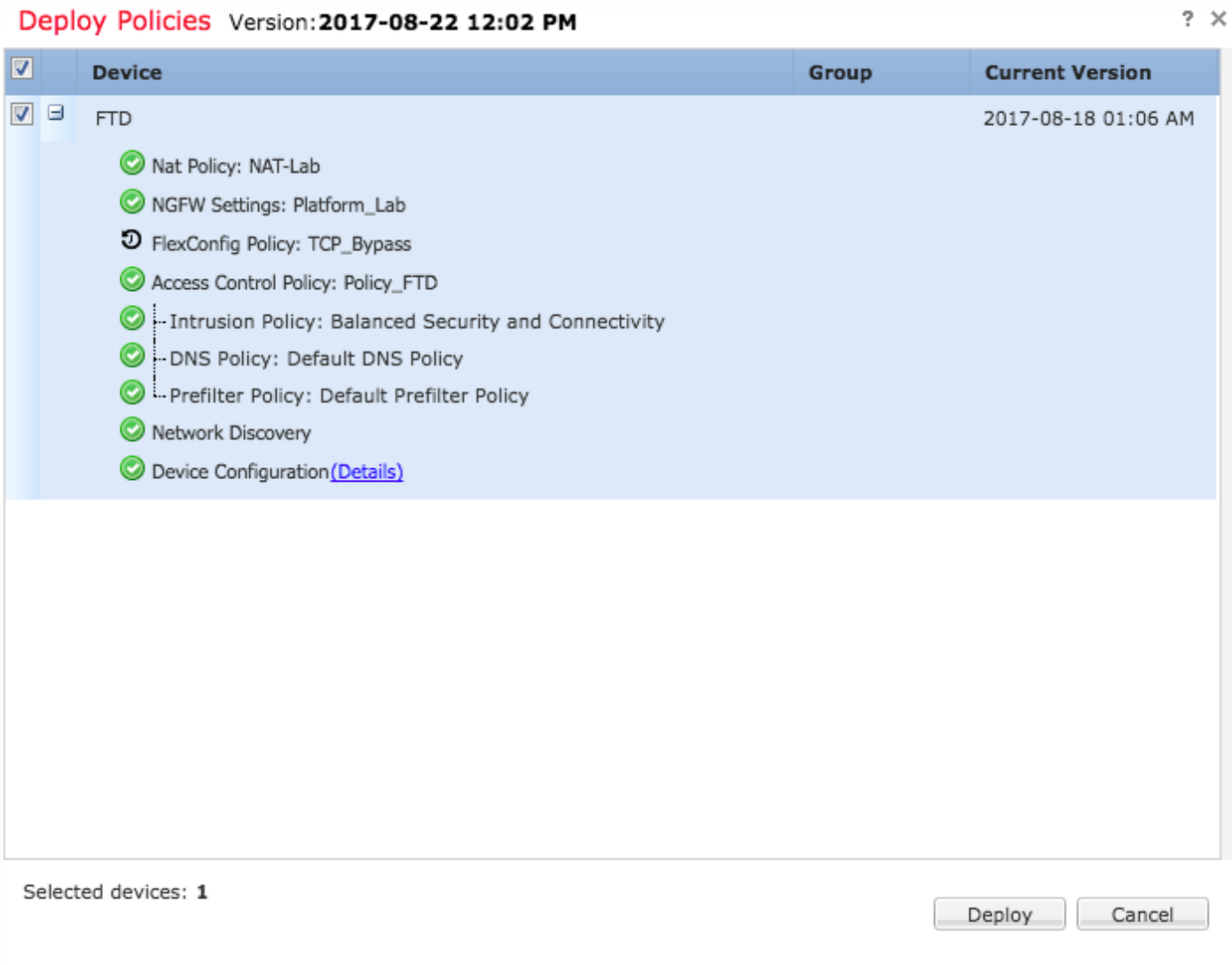
Affectez la stratégie FlexConfig **TCP_Bypass** au périphérique FTD.



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



Enregistrer les modifications et les déployer,



Vérification

Accédez au FTD via SSH ou la console et utilisez la commande **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
!
```

Dépannage

Pour dépanner cette fonctionnalité, ces commandes vous permettent de vous aider.

- 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