FTD: Cómo habilitar la configuración de omisión de estado TCP mediante la política FlexConfig

Contenido

Introducción

Este documento describe cómo implementar la función de omisión de estado del protocolo de control de transmisión (TCP) en appliances Firepower Threat Defense (FTD) a través de Firepower Management Center (FMC) mediante la política FlexConfig en versiones anteriores a 6.3.0.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento de Firepower Management Center.
- Conocimiento básico de Firepower Threat Defense.
- Introducción a la función de omisión de estado TCP.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

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

Antecedentes

El desvío de estado de TCP es una función heredada del dispositivo de seguridad adaptable (ASA) y proporciona asistencia para la resolución de problemas del tráfico que puede ser descartado por las funciones de normalización de TCP, las condiciones de routing asimétricas y ciertas inspecciones de aplicaciones.

Esta función se admite de forma nativa en FMC a partir de la versión 6.3.0. Se recomienda eliminar los objetos Flexconfig después de la actualización y mover esta configuración al FMC antes de la primera implementación. Para obtener más información sobre cómo configurar el desvío de estado TCP en la versión 6.3.0 o posterior, vaya a esta guía de configuración.

Firepower Threat Defense utiliza comandos de configuración de ASA para implementar algunas funciones, pero no todas. No hay un conjunto único de comandos de configuración de Firepower Threat Defense. En su lugar, el objetivo de FlexConfig es permitirle configurar funciones que aún no son directamente soportadas a través de políticas y configuraciones de Firepower Management Center.

> **Nota**: El desvío de estado TCP sólo se debe utilizar para solucionar problemas o cuando no se puede resolver el ruteo asimétrico. El uso de esta función inhabilita varias funciones de seguridad y puede causar un gran número de conexiones si no se implementa correctamente.

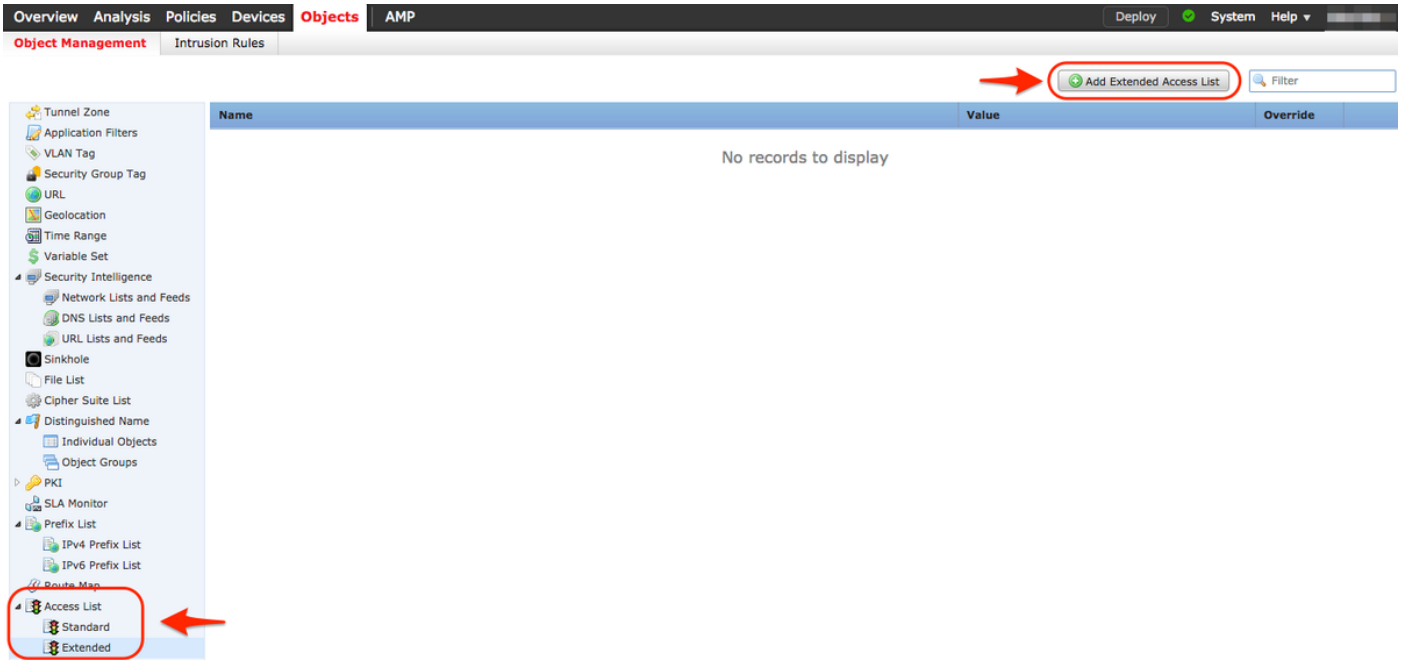
Para obtener más información sobre la función TCP State Bypass o su implementación en ASA, consulte Configuración de la Función TCP State Bypass en la Serie ASA 5500 y la Guía de Configuración de Cisco ASA 5500 Series.

Configuración

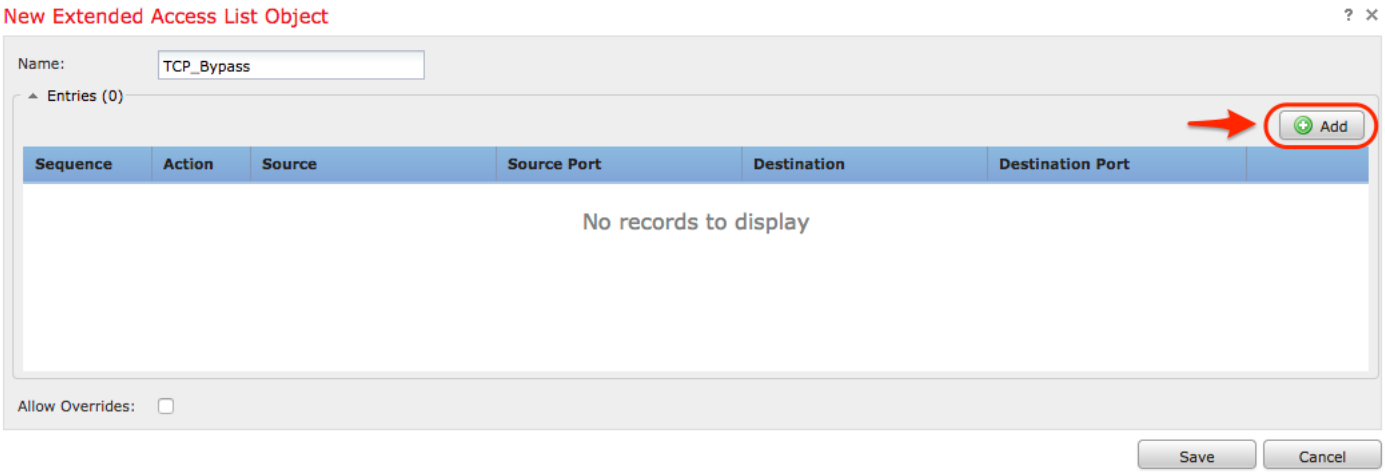
Esta sección describe cómo configurar el desvío de estado TCP en FMC a través de una política FlexConfig.

Paso 1. Configurar un objeto de lista de acceso extendido

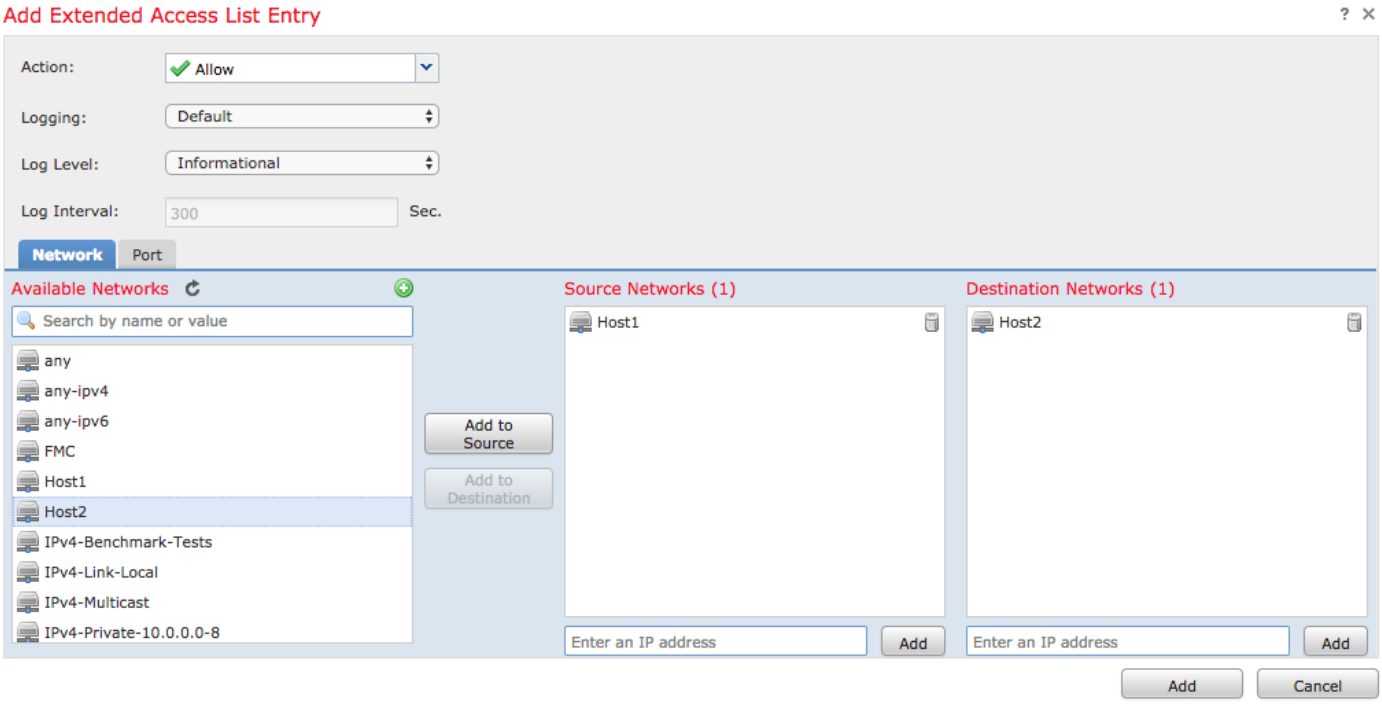
Para crear una lista de acceso ampliada en FMC, vaya a **Objetos >Administración de objetos** y en el menú de la izquierda, en **Lista de acceso** seleccione **Ampliado. Haga clic en Agregar lista de acceso ampliada.**



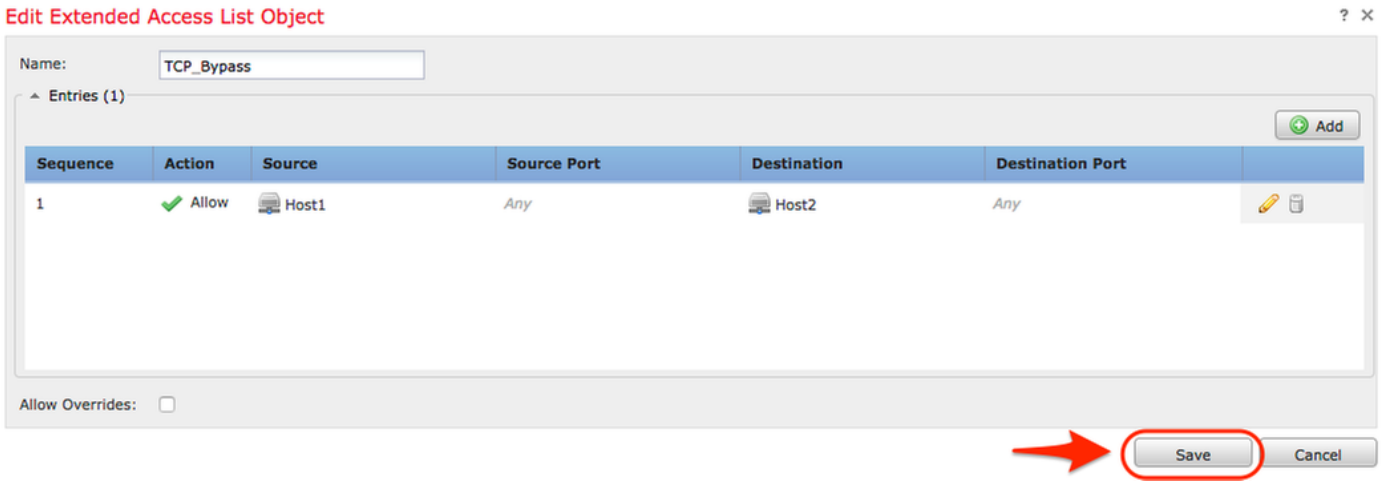
Rellene el campo Nombre con el valor deseado. en este ejemplo, el nombre es **TCP_Bypass**. Haga clic en el botón **Add**.



La acción para esta regla debe configurarse como **Permitir.** Se puede utilizar una red definida por el sistema o se puede crear un nuevo objeto de red para cada origen y destino. En este ejemplo, la Lista de Acceso coincide con el tráfico IP del Host1 al Host2, ya que ésta es la comunicación para aplicar la Omisión de Estado TCP. La ficha Puerto se puede utilizar opcionalmente para hacer coincidir un puerto TCP o UDP específico. Haga clic en el botón **Add** para continuar.

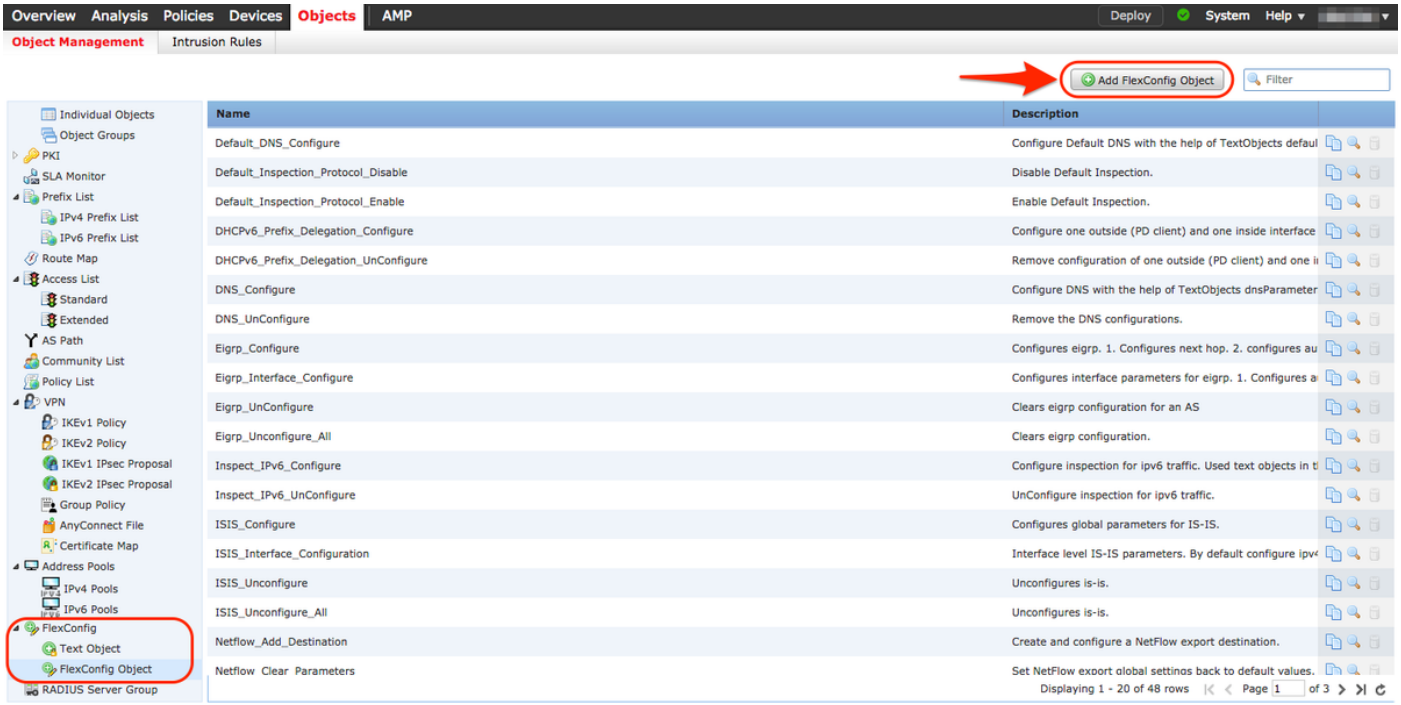


Una vez que se seleccionen las redes o hosts de origen y destino, haga clic en **Guardar**.



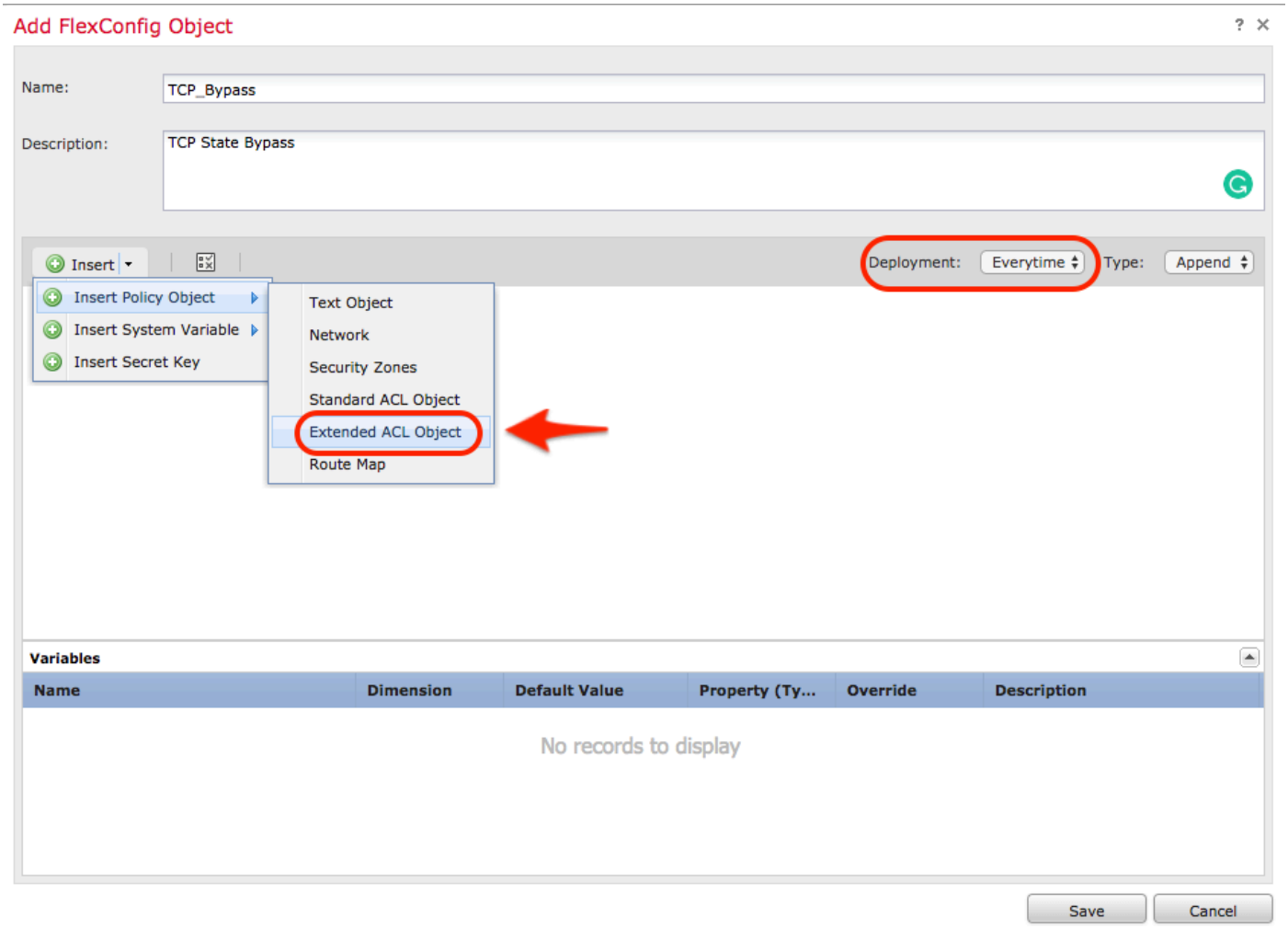
Paso 2. Configurar un objeto FlexConfig

Vaya a **Objects > Object Management > FlexConfig > FlexConfig Object** y haga clic en el botón **Add FlexConfig Object**.



El nombre del objeto para este ejemplo se denomina **TCP_Bypass** igual que la lista de acceso. Este nombre no necesita coincidir con el nombre de la lista de acceso.

Seleccione **Insertar objeto de política > Objeto ACL extendido.**

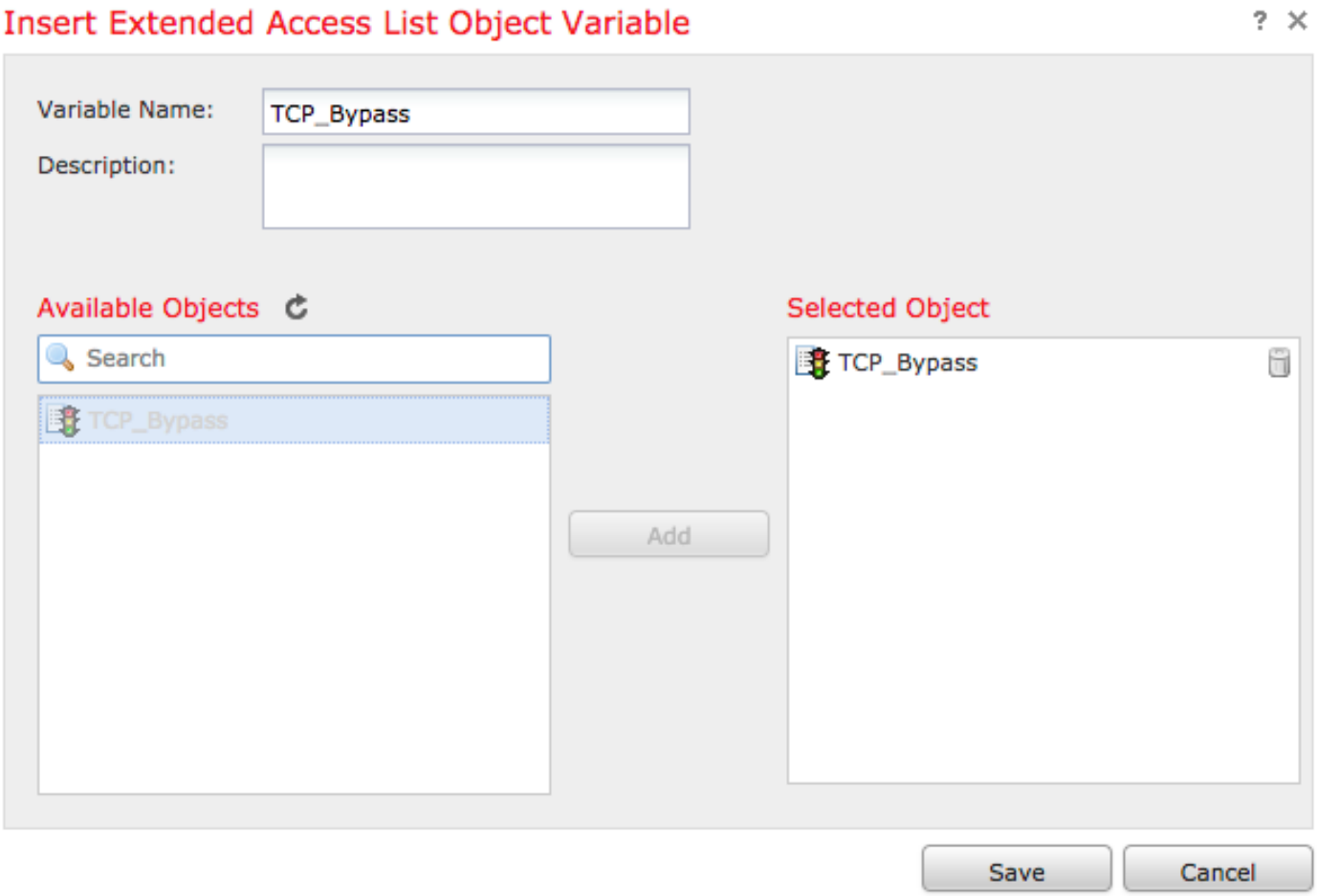


Nota: Asegúrese de elegir la opción "Todo el tiempo". Esto permite conservar esta

configuración durante otras implementaciones y actualizaciones.

Seleccione la lista de acceso creada en el paso 1 de la sección **Objetos disponibles** y asigne un nombre de variable. A continuación, haga clic en el botón **Agregar**. En este ejemplo, el nombre de variable es **TCP_Bypass**.

Haga clic en **Guardar**.

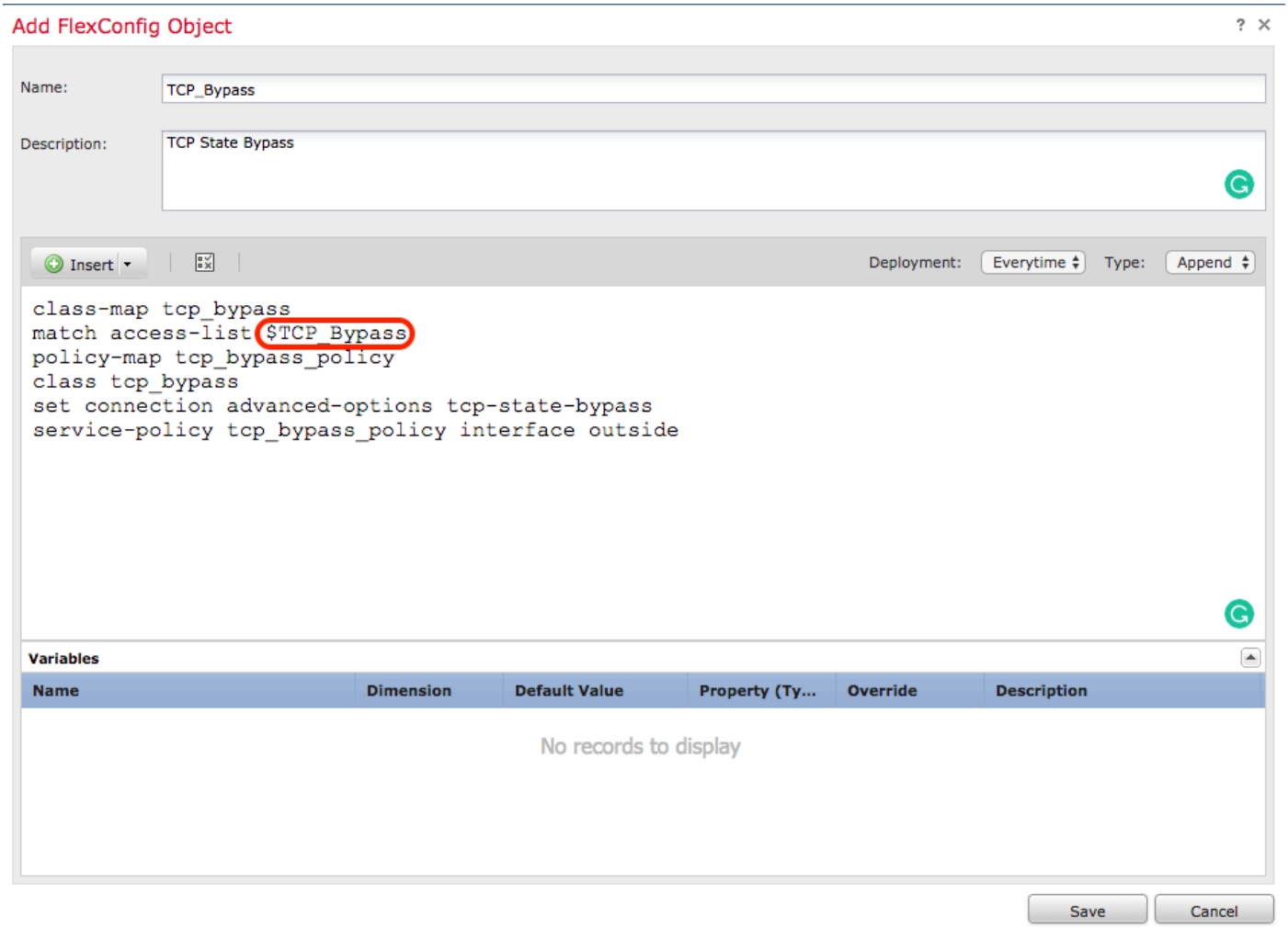


Agregue las siguientes líneas de configuración en el campo en blanco justo debajo del botón **Insertar** e incluya la variable previamente definida (**$TCP_Bypass**) en la línea de configuración *coincidencia de lista de acceso*. Observe que un símbolo **$** se antepone al nombre de la variable. Esto ayuda a definir que una variable sigue después.

```
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
```

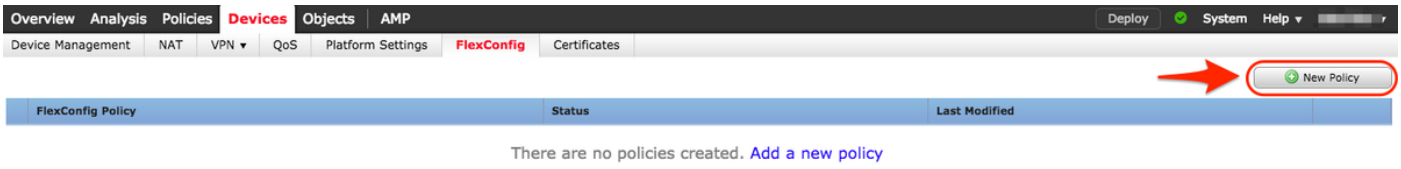
En este ejemplo, se crea un policy-map y se aplica a la interfaz externa. Si el desvío de estado de TCP debe configurarse como parte de la política de servicio global, el mapa de clase tcp_bypass se puede aplicar a global_policy.

Haga clic en **Guardar** cuando haya terminado.

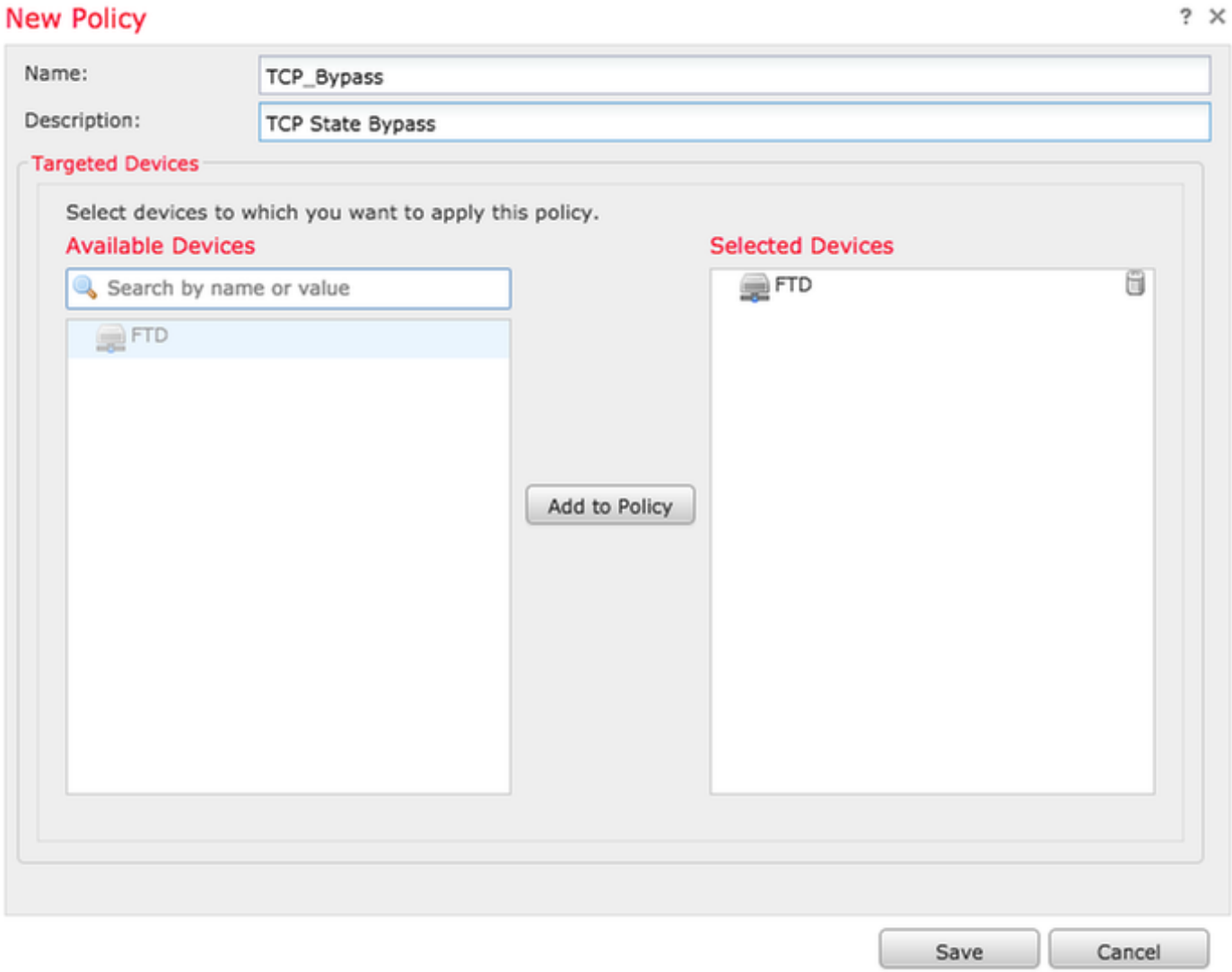


Paso 3. Asignar una política FlexConfig al FTD

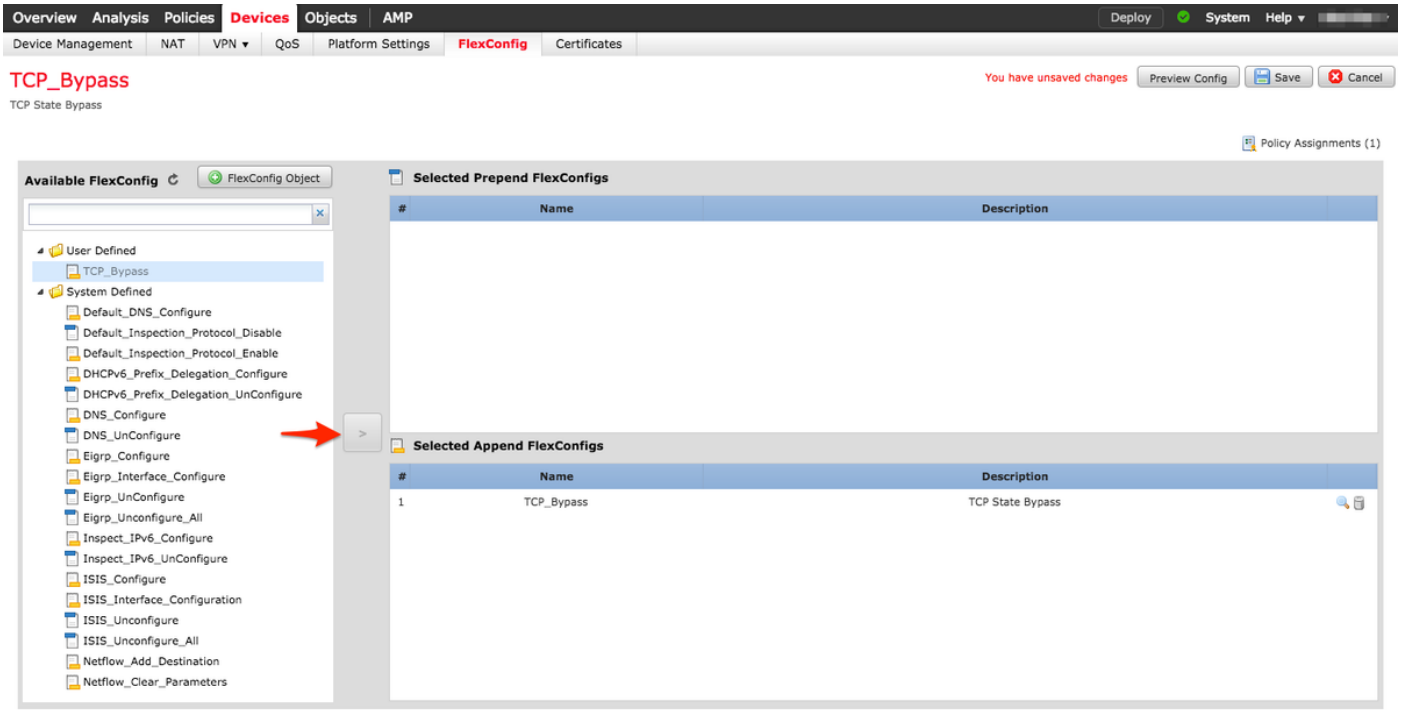
Vaya a **Dispositivos > FlexConfig** y cree una nueva política (a menos que ya haya una creada para otro propósito y asignada al mismo FTD).En este ejemplo, la nueva política FelxConfig se denomina **TCP_Bypass**.



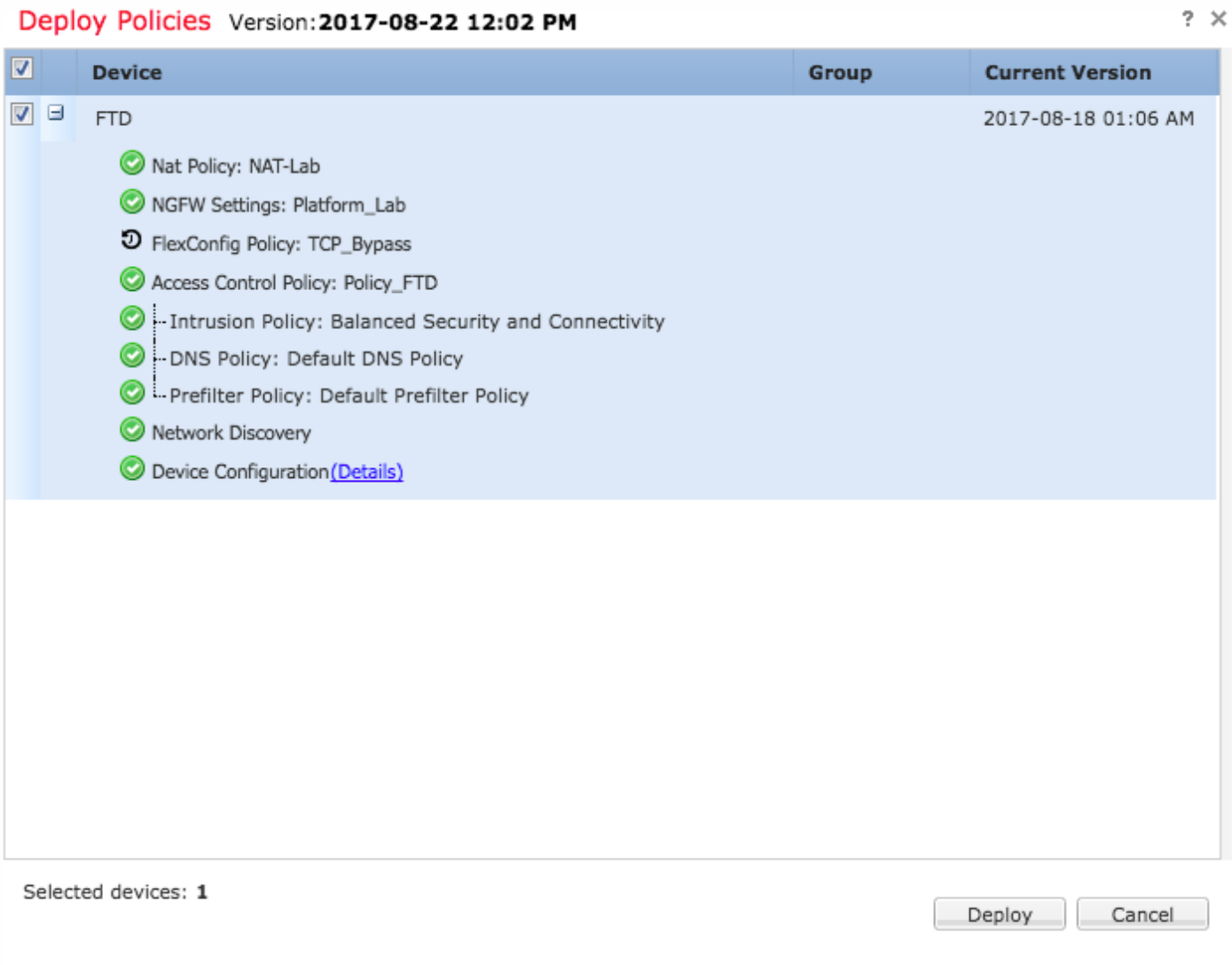
Asigne la política FlexConfig **TCP_Bypass** al dispositivo FTD.



Seleccione el objeto FlexConfig denominado **TCP_Bypass** creado en el paso 2 bajo la sección **Definido por el usuario** y haga clic en la flecha para agregar ese objeto a la política.



Guarde los cambios e implemente



Verificación

Acceda al FTD a través de SSH o consola y utilice el comando **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
!
```

Troubleshoot

Para solucionar este problema, estos comandos resultan útiles.

- 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

Enlaces relacionados

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