FTD: Aktivieren der TCP-State-Bypass-Konfiguration mithilfe der FlexConfig-Richtlinie

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie die Transmission Control Protocol (TCP) State Bypass-Funktion auf FirePOWER Threat Defense (FTD)-Appliances über FirePOWER Management Center (FMC) mithilfe der FlexConfig Policy in Versionen vor 6.3.0 implementiert wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Kenntnisse des FirePOWER Management Center.
- Grundlegende Kenntnisse des FirePOWER Threat Defense.
- Informationen über die Funktion zum Umgehen des TCP-Zustands.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

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

Hintergrundinformationen

TCP State Bypass ist eine von der Adaptive Security Appliance (ASA) geerbte Funktion und bietet Unterstützung bei der Fehlerbehebung von Datenverkehr, der entweder durch TCP-Normalisierungsfunktionen, asymmetrische Routing-Bedingungen und bestimmte Anwendungsinspektionen verworfen werden könnte.

Diese Funktion wird nativ auf FMC ab Version 6.3.0 unterstützt. Es wird empfohlen, die Flexconfig-Objekte nach dem Upgrade zu löschen und diese Konfiguration vor der ersten Bereitstellung auf das FMC zu verschieben. Weitere Informationen zum Konfigurieren von TCP-State-Bypass in Version 6.3.0 oder höher finden Sie in diesem Konfigurationsleitfaden.

FirePOWER Threat Defense verwendet ASA-Konfigurationsbefehle, um einige Funktionen, aber nicht alle Funktionen zu implementieren. Es gibt keine eindeutigen Konfigurationsbefehle für FirePOWER Threat Defense. FlexConfig ermöglicht Ihnen stattdessen die Konfiguration von Funktionen, die noch nicht direkt durch die Richtlinien und Einstellungen von Firepower Management Center unterstützt werden.

> **Hinweis**: TCP-Zustandsumgehung sollte nur zu Fehlerbehebungszwecken verwendet werden oder wenn asymmetrisches Routing nicht aufgelöst werden kann. Die Verwendung dieser Funktion deaktiviert mehrere Sicherheitsfunktionen und kann bei unzureichender Implementierung zu einer hohen Anzahl von Verbindungen führen.

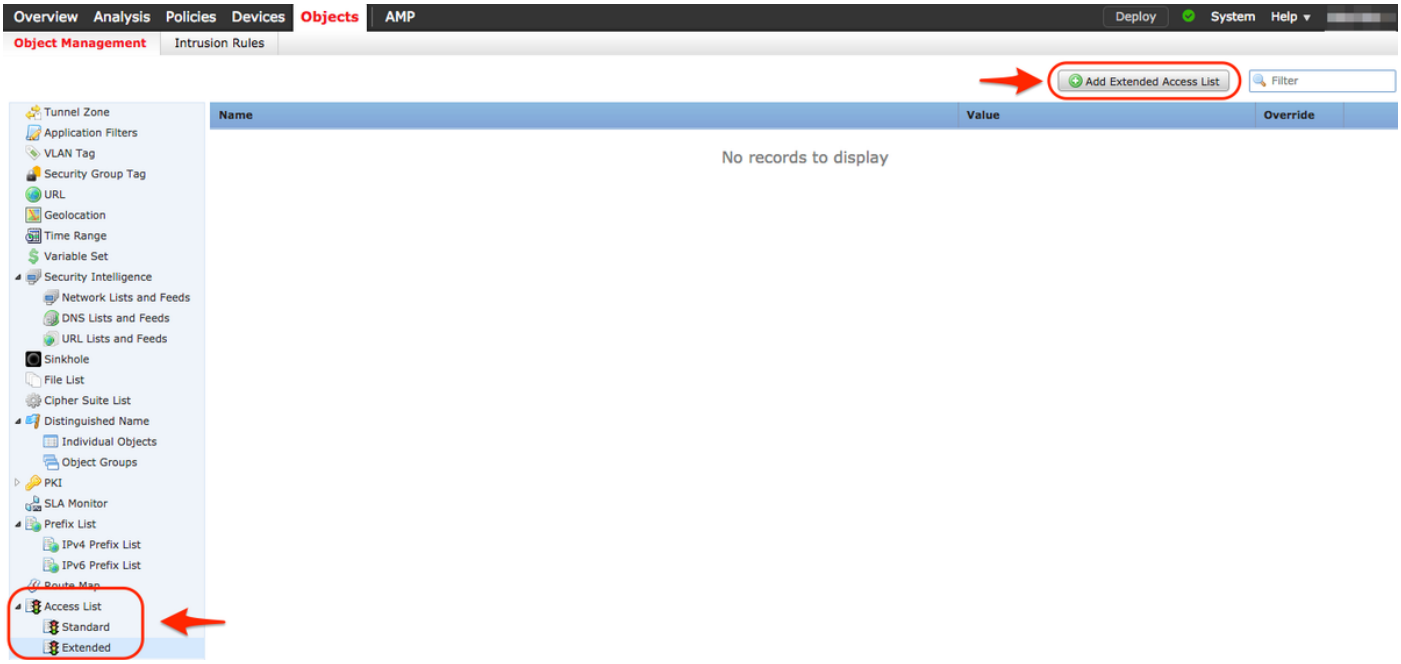
Weitere Informationen zur TCP-State-Bypass-Funktion oder deren Implementierung in ASA finden Sie im Konfigurationshandbuch zur Konfiguration der TCP-State-Bypass-Funktion auf der ASA 5500-Serie und im Konfigurationshandbuch zur Cisco Serie ASA 5500.

Konfiguration

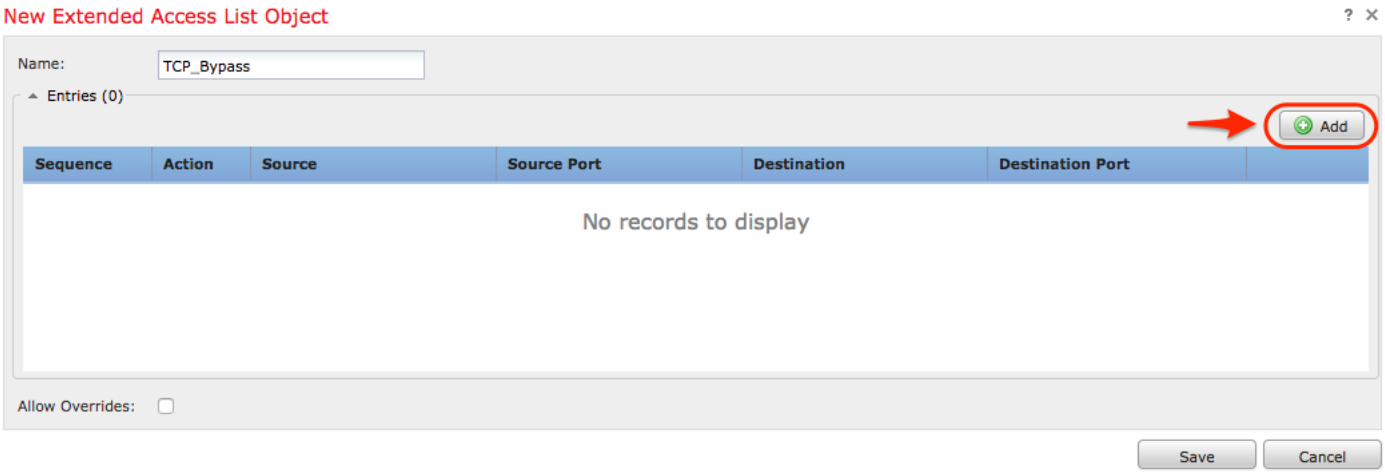
In diesem Abschnitt wird beschrieben, wie der TCP-State-Bypass auf dem FMC mithilfe einer FlexConfig-Richtlinie konfiguriert wird.

Schritt 1: Konfigurieren eines Extended Access List-Objekts

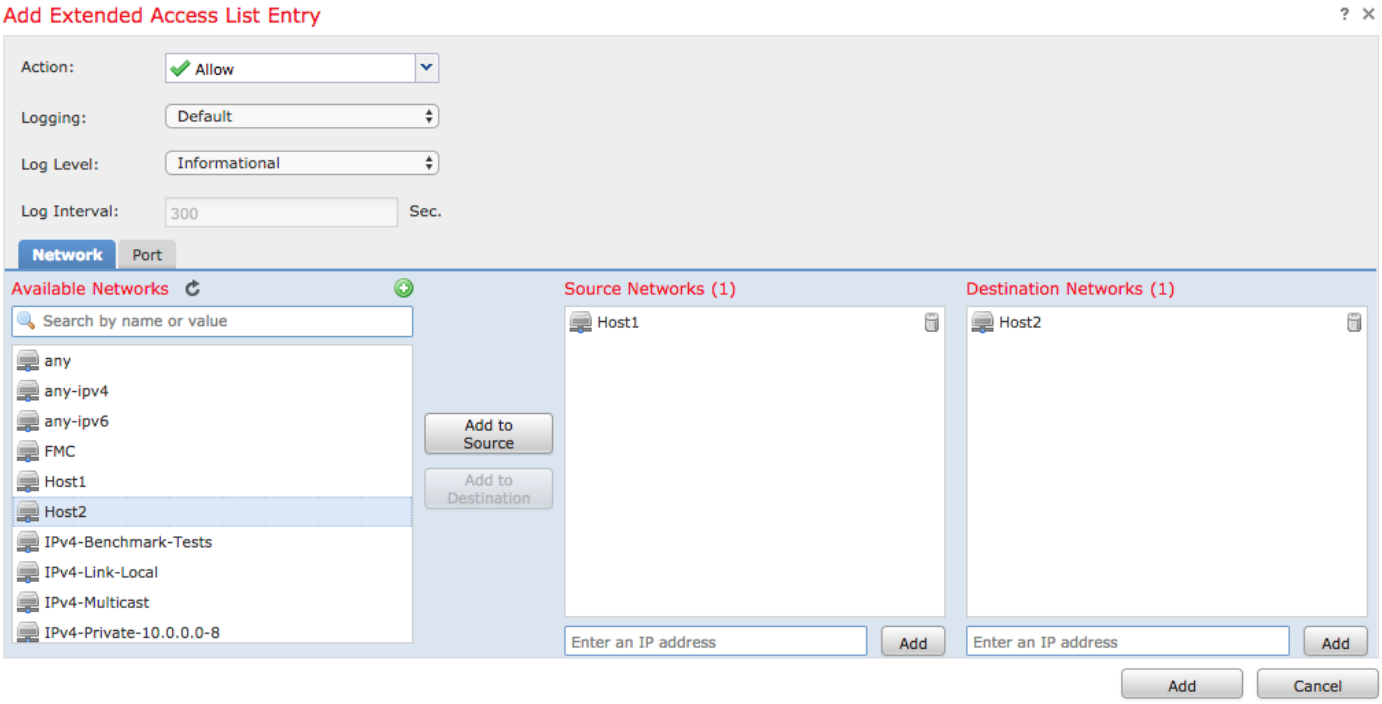
Um eine erweiterte Zugriffsliste auf dem FMC zu erstellen, gehen Sie zu **Objekte >Objektmanagement** und klicken Sie im linken Menü unter **Zugriffsliste** auf **Erweitert.** Klicken Sie auf Erweiterte Zugriffsliste hinzufügen.



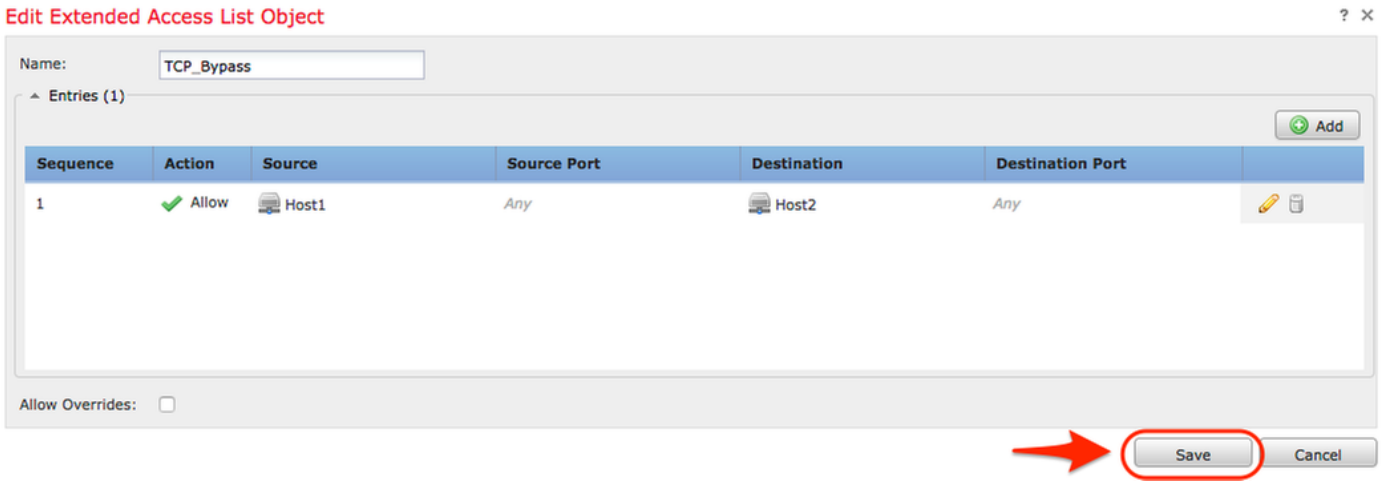
Füllen Sie das Feld Name mit dem gewünschten Wert aus. in diesem Beispiel lautet der Name **TCP_Bypass**. Klicken Sie auf Schaltfläche **Hinzufügen**.



Die Aktion für diese Regel muss als **Zulassen** konfiguriert werden. Es kann ein systemdefiniertes Netzwerk verwendet oder für jede Quelle und jedes Ziel ein neues Netzwerkobjekt erstellt werden. In diesem Beispiel ordnet die Zugriffsliste IP-Datenverkehr von Host1 zu Host2 zu, da dies die Kommunikation zur Anwendung von TCP-State-Bypass ist. Die Registerkarte "Port" kann optional verwendet werden, um einen bestimmten TCP- oder UDP-Port zuzuordnen. Klicken Sie auf die Schaltfläche **Hinzufügen**, um fortzufahren.

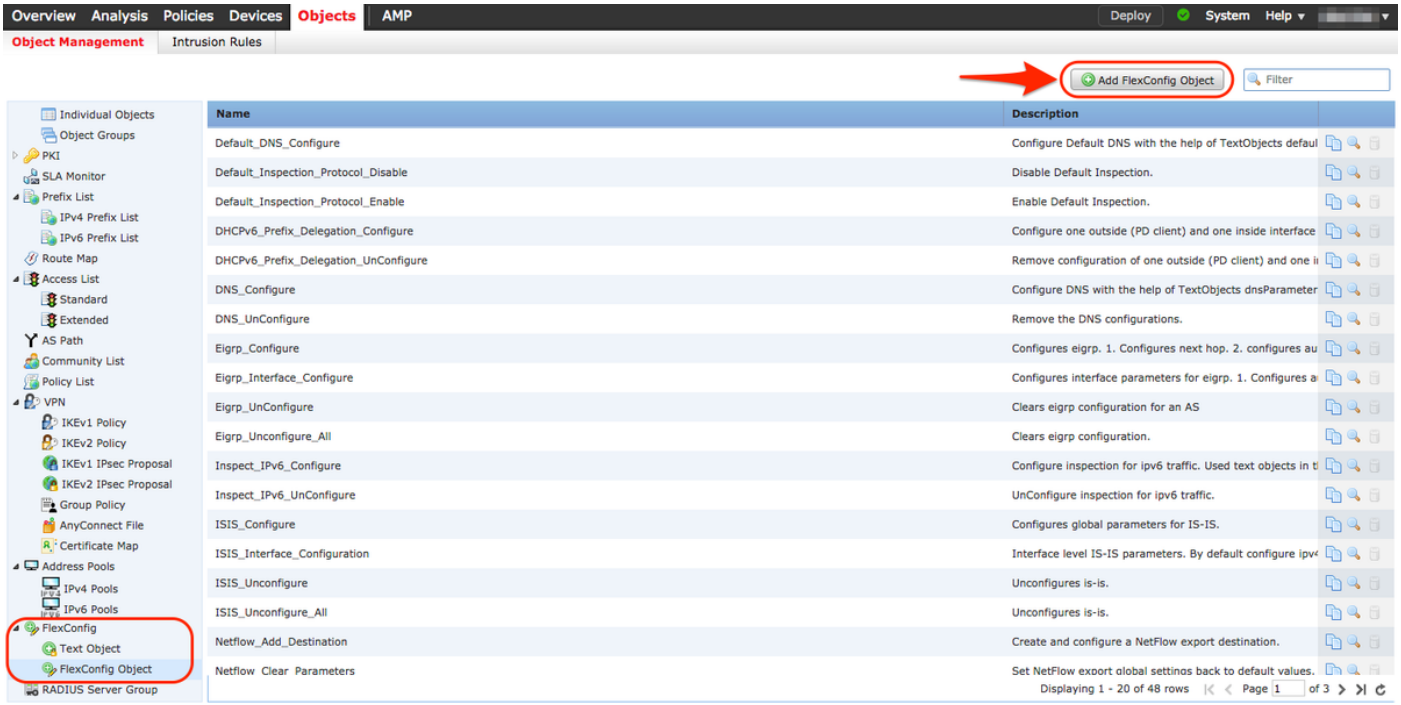


Wenn Sie die Quell- und Zielnetzwerke oder -Hosts ausgewählt haben, klicken Sie auf **Speichern**.



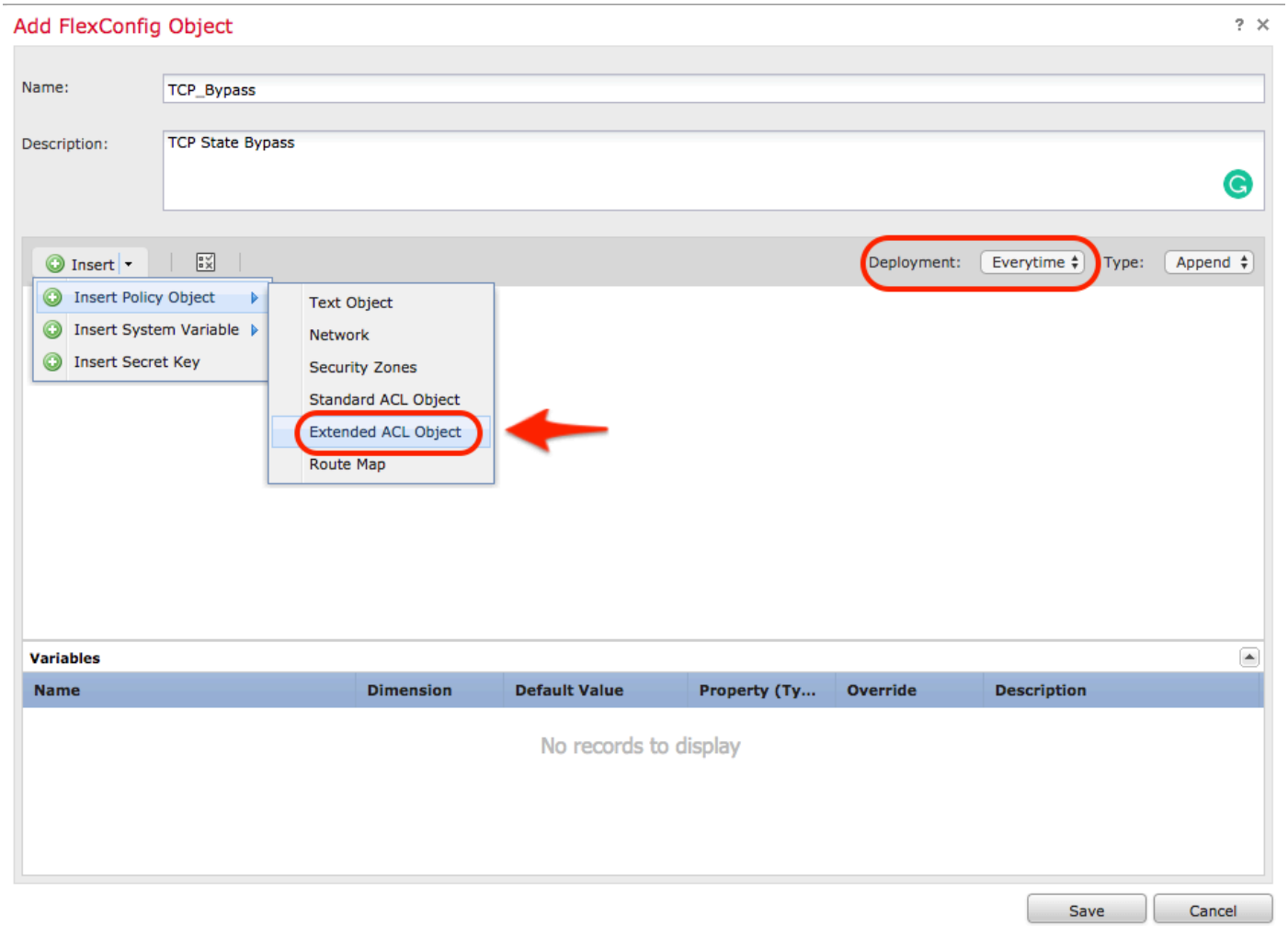
Schritt 2: Konfigurieren eines FlexConfig-Objekts

Navigieren Sie zu **Objekte > Objektmanagement > FlexConfig > FlexConfig Object,** und klicken Sie auf die Schaltfläche **FlexConfig-Objekt hinzufügen**.



Der Name des Objekts für dieses Beispiel heißt **TCP_Bypass** genau wie die Zugriffsliste. Dieser Name muss nicht mit dem Namen der Zugriffsliste übereinstimmen.

Wählen Sie **Policy Object einfügen > Extended ACL Object aus.**

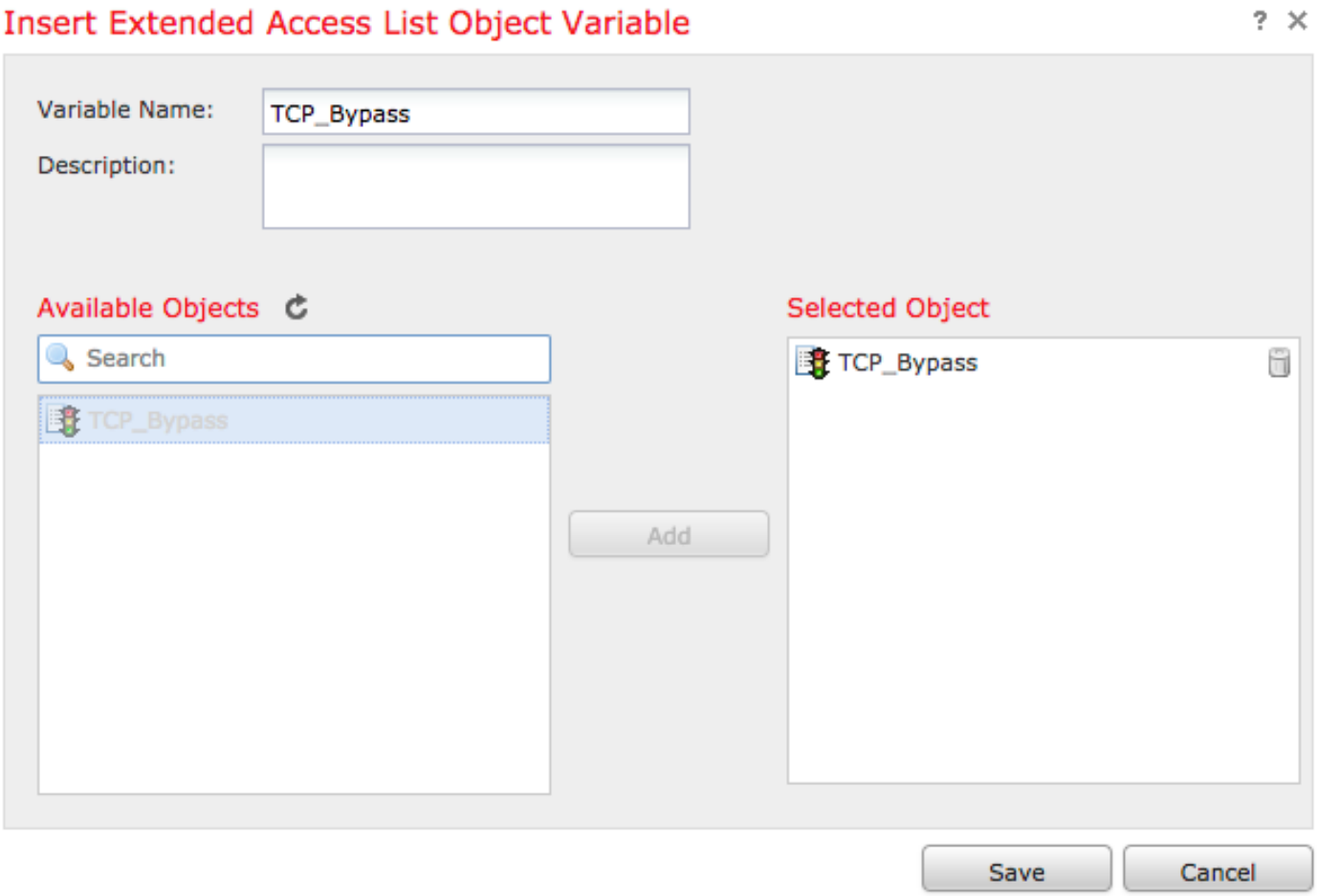


Hinweis: Wählen Sie die Option "Everytime" aus. Dadurch kann diese Konfiguration auch bei

anderen Bereitstellungen und Upgrades beibehalten werden.

Wählen Sie im Abschnitt **Verfügbare Objekte** die in Schritt 1 erstellte Zugriffsliste aus, und weisen Sie einen Variablennamen zu. Klicken Sie anschließend auf die Schaltfläche **Hinzufügen**. In diesem Beispiel lautet der Variablenname **TCP_Bypass**.

Klicken Sie auf **Speichern**.

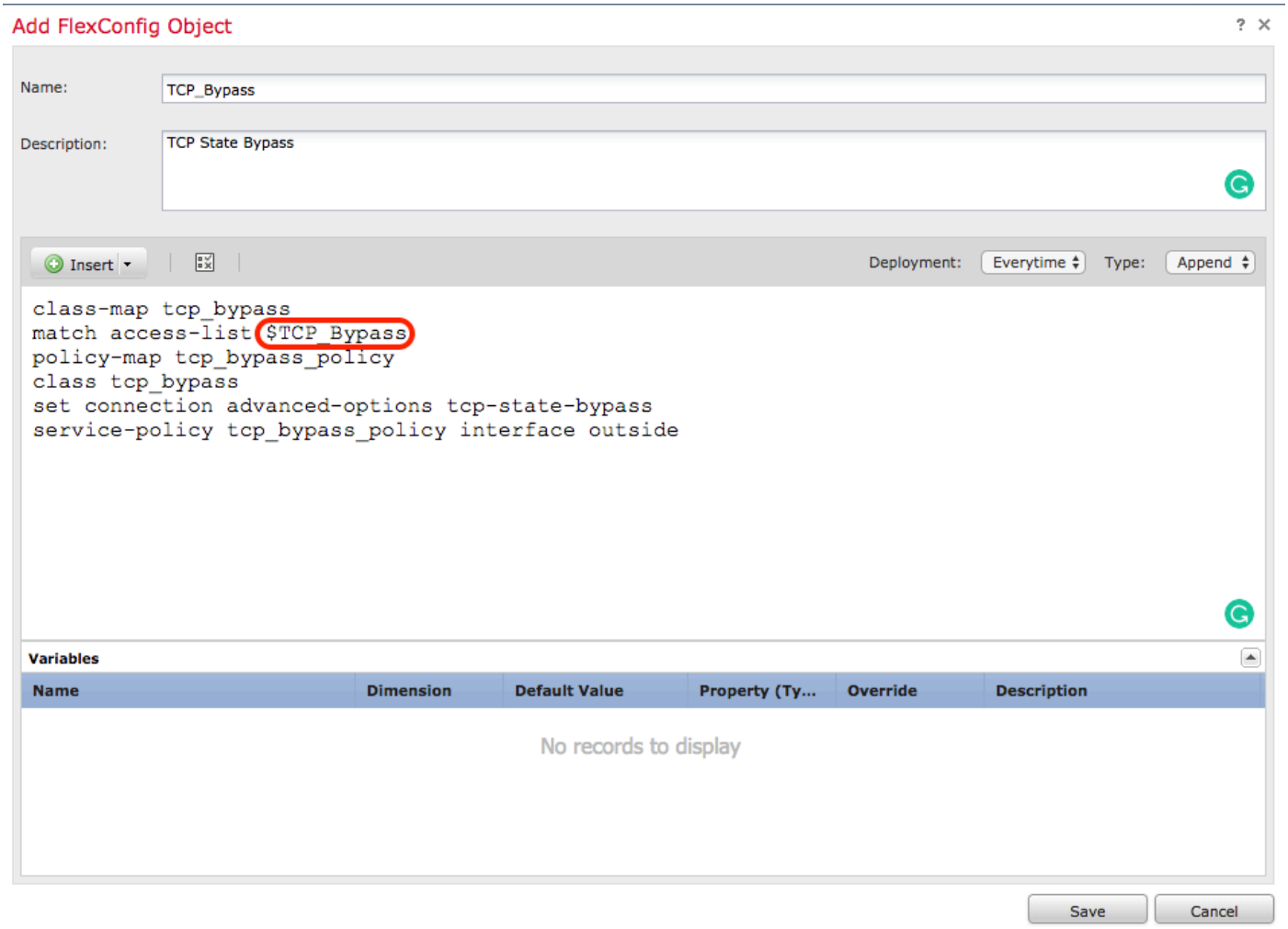


Fügen Sie die nächsten Konfigurationszeilen im leeren Feld direkt unter der Schaltfläche **Einfügen** hinzu, und fügen Sie die zuvor definierte Variable (**$TCP_Bypass**) in die Konfigurationszeile *Match-Zugriffsliste ein*. Beachten Sie, dass ein **$**-Symbol dem Variablennamen vorangestellt wird. Dies hilft zu definieren, dass eine Variable danach folgt.

```
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
```

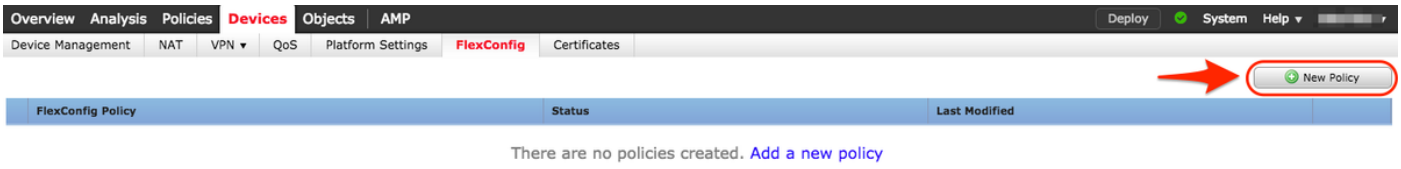
In diesem Beispiel wird eine Richtlinienzuordnung erstellt und auf die externe Schnittstelle angewendet. Wenn der TCP-State-Bypass als Teil der globalen Dienstrichtlinie konfiguriert werden muss, kann die Klassenzuordnung "tcp_bypass" auf global_policy angewendet werden.

Klicken Sie abschließend auf **Speichern**.

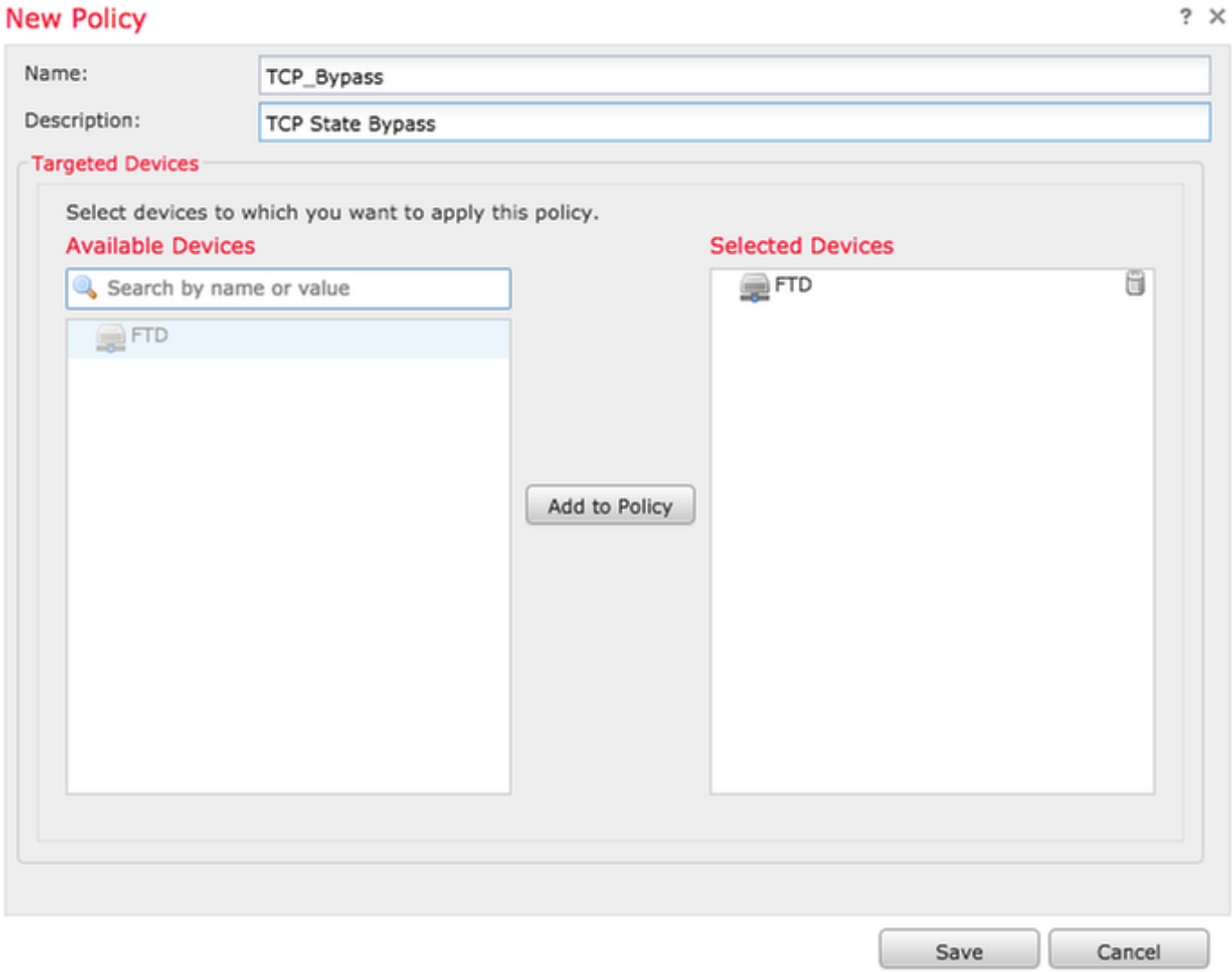


Schritt 3: Zuweisen einer FlexConfig-Richtlinie zum FTD

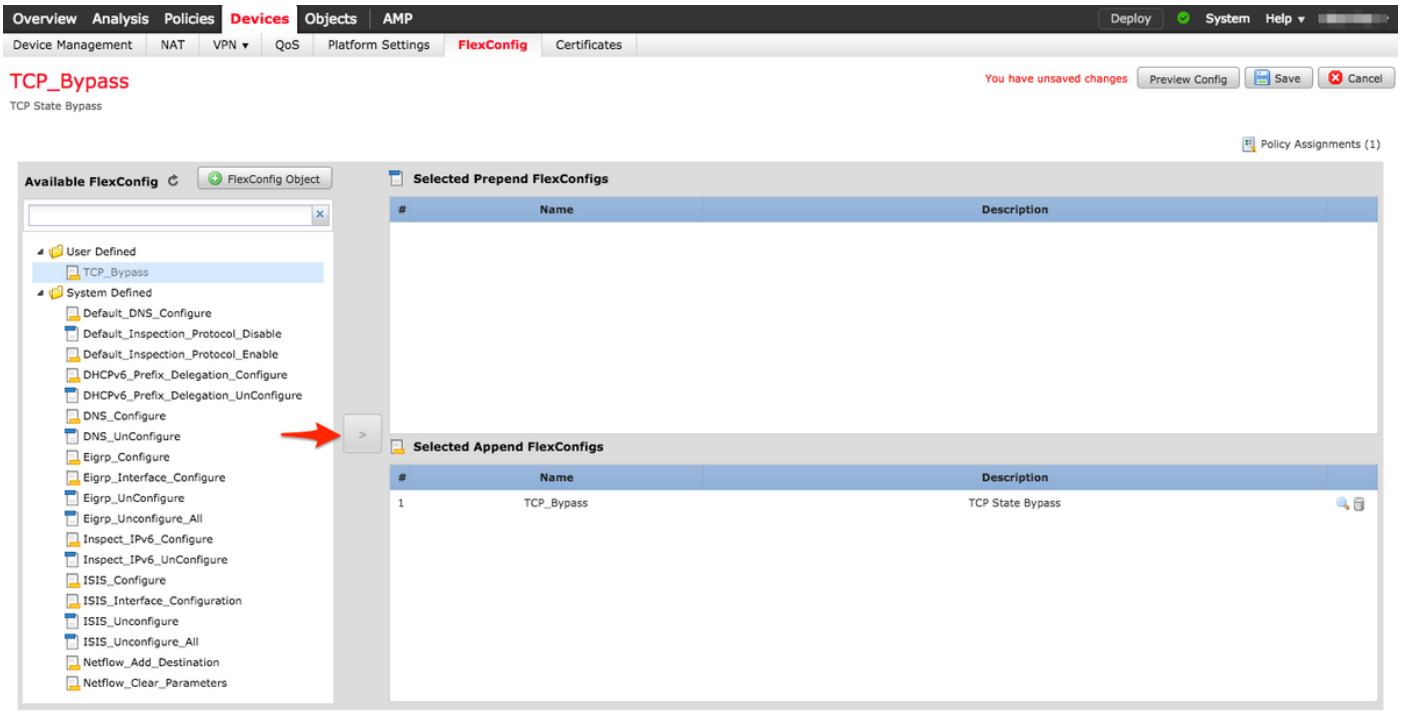
Gehen Sie zu **Devices > FlexConfig**, und erstellen Sie eine neue Richtlinie (es sei denn, es wurde bereits eine Richtlinie für einen anderen Zweck erstellt und derselben FTD zugewiesen).In diesem Beispiel wird die neue FelxConfig-Richtlinie als **TCP_Bypass** bezeichnet.



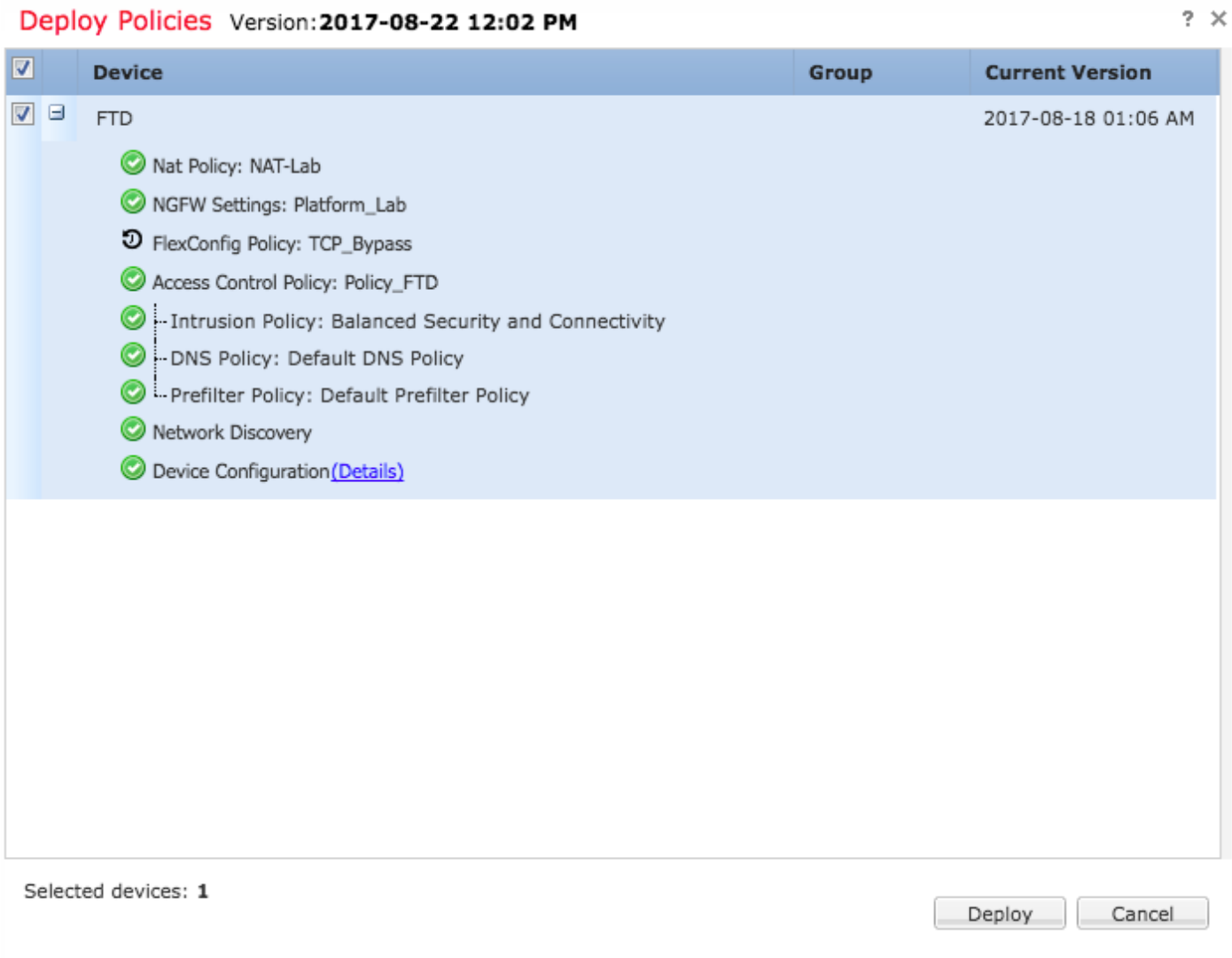
Weisen Sie dem FTD-Gerät die **TCP_Bypass** FlexConfig-Richtlinie zu.



Wählen Sie das FlexConfig-Objekt mit dem Namen **TCP_Bypass** aus, das in Schritt 2 unter dem Abschnitt **User Defined** erstellt wurde, und klicken Sie auf den Pfeil, um dieses Objekt der Richtlinie hinzuzufügen.



Speichern und Bereitstellen der Änderungen



Überprüfung

Zugriff auf das FTD über SSH oder Konsole und Verwendung der **Diagnosesystemunterstützung.**

```
> 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
!
```

Fehlerbehebung

Zur Fehlerbehebung führen diese Befehle zu hilfreichen Ergebnissen.

- 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

Verwandte 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