FTD：FlexConfigポリシーを使用してTCP状態バイパス設定を有効にする方法

内容

概要

このドキュメントでは、6.3.0より前のバージョンのFlexConfigポリシーを使用して、Firepower Management Center(FMC)経由でFirepower Threat Defense(FTD)アプライアンスにTransmission Control Protocol(TCP)状態バイパス機能を実装する方法についてについて説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Firepower Management Centerの知識。
- Firepower Threat Defense(FTD)の基礎知識。
- TCP状態バイパス機能について

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Firepower Threat Defense(FTD)バージョン6.2.3。
- Firepower Management Center（FMC）バージョン 6.2.3.

背景説明

TCP状態バイパス(STB)は、適応型セキュリティアプライアンス(ASA)から継承された機能で、

TCP正規化機能、非対称ルーティング条件、および特定のアプリケーションインスペクションによってドロップされるトラフィックのトラブルシューティングを支援します。

この機能は、バージョン6.3.0以降のFMCでネイティブにサポートされています。アップグレード後にFlexconfigオブジェクトを削除し、最初の展開の前にこの設定をFMCに移動することを推奨します。バージョン6.3.0以降でTCP状態バイパスを設定する方法の詳細については、次の設定ガイドを参照してください。

Firepower Threat Defense(FTD)は、ASA設定コマンドを使用して一部の機能を実装しますが、一部の機能は実装しません。Firepower Threat Defense設定コマンドの固有のセットはありません。代わりに、FlexConfigのポイントは、Firepower Management Centerのポリシーと設定を通じてまだ直接サポートされていない機能を構成できることにあります。

> **注**: TCP状態バイパスは、トラブルシューティングの目的や、非対称ルーティングを解決できない場合にのみ使用してください。この機能を使用すると、複数のセキュリティ機能が無効になり、適切に実装されていない場合は多数の接続が発生する可能性があります。

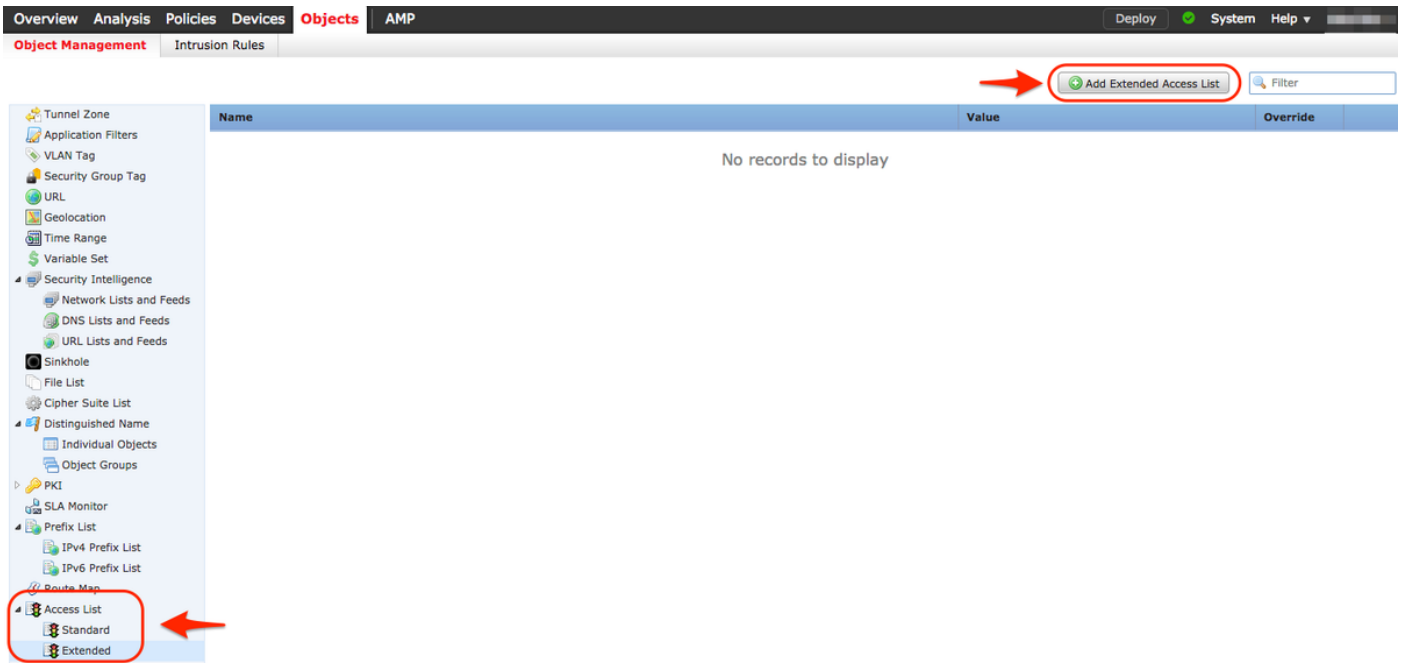
ASAでのTCP状態バイパス機能またはその実装の詳細については、『ASA 5500シリーズでのTCP状態バイパス機能の設定』および『Cisco ASA 5500シリーズ設定ガイド』を参照してください。

コンフィギュレーション

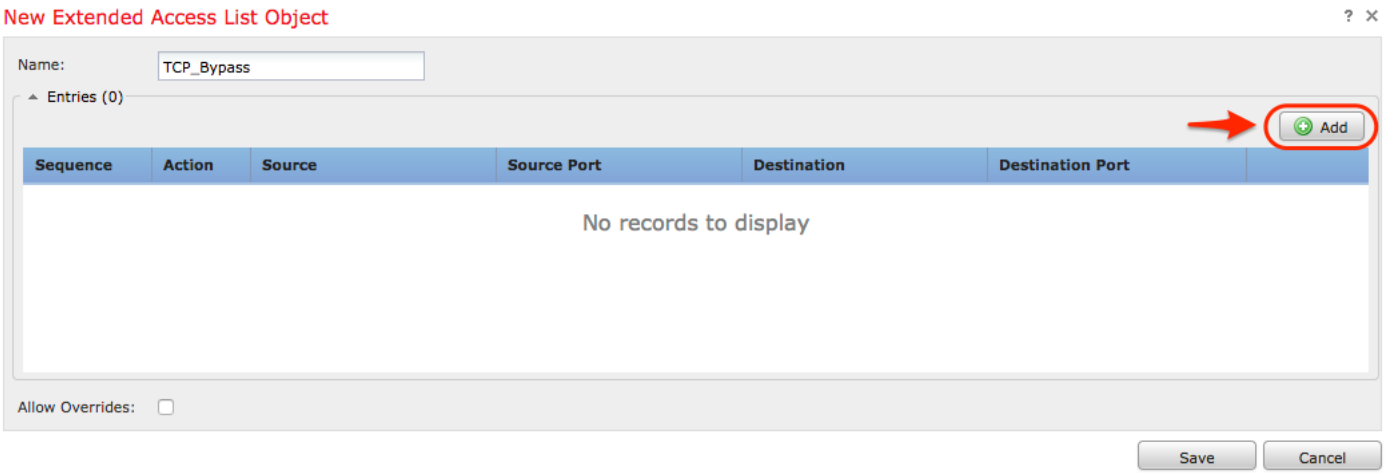
このセクションでは、FlexConfigポリシーを使用してFMCでTCP状態バイパス(STB)を設定する方法について説明します。

ステップ1：拡張アクセスリストオブジェクトの設定

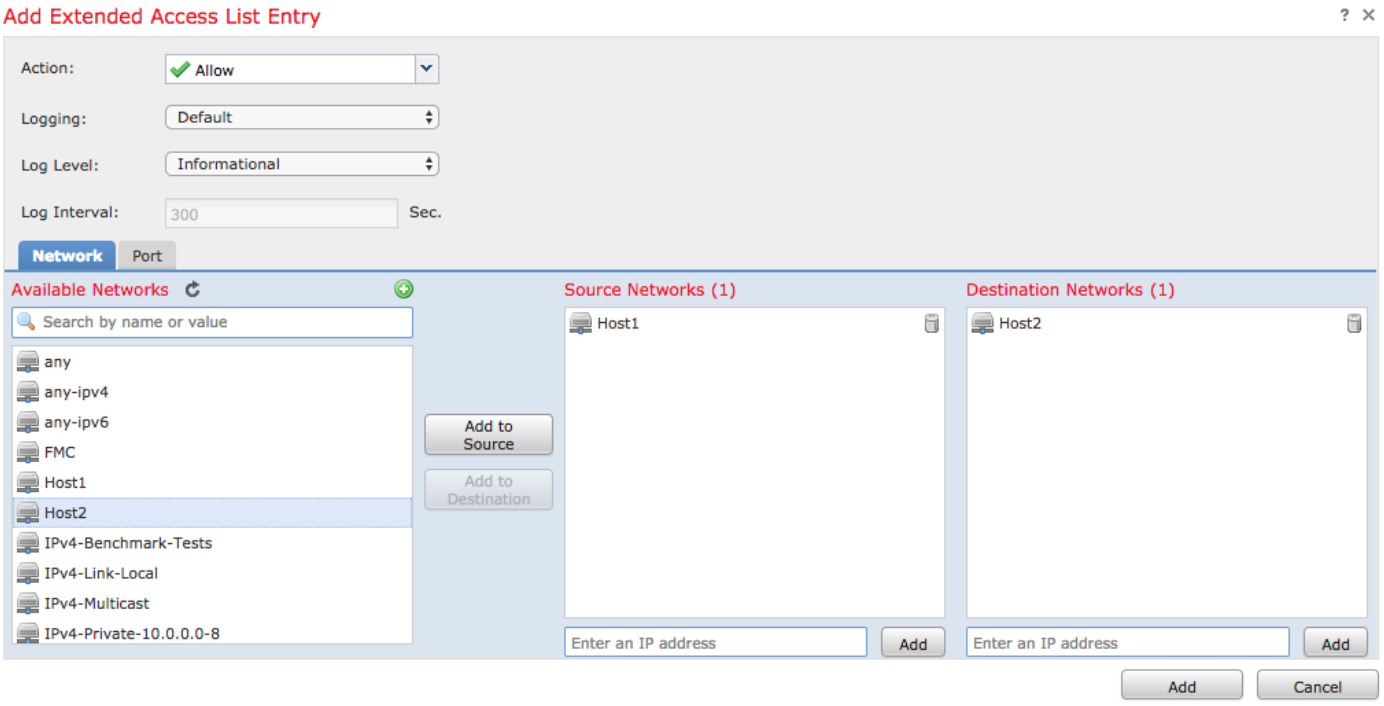
FMCで拡張アクセスリストを作成するには、**[Objects] > [Object Management]に移動し、左側のメニューの[Access List]で**[Extended]を選択**します。[Add Extended Access List]をクリックします**。



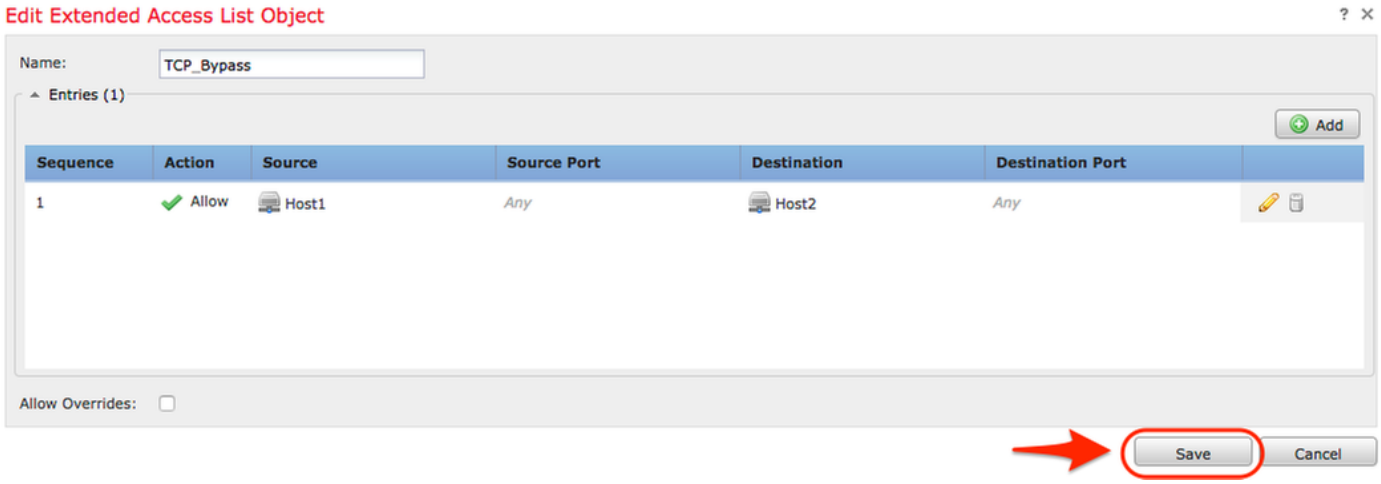
[名前]フィールドに目的の値を入力します。この例では、名前は**TCP_Bypassです**。[追加]ボタン**をクリック**します。



このルールのアクションは**Allowに設定する必要があります**。システム定義のネットワークを使用するか、新しいネットワークオブジェクトをソースと宛先ごとに作成できます。この例では、アクセスリストはHost1からHost2へのIPトラフィックに一致します。これはTCP状態バイパスを適用する通信であるためです。[Port]タブは、オプションで特定のTCPポートまたはUDPポートを照合するために使用できます。[Add]ボタンをクリック**して**続行します。

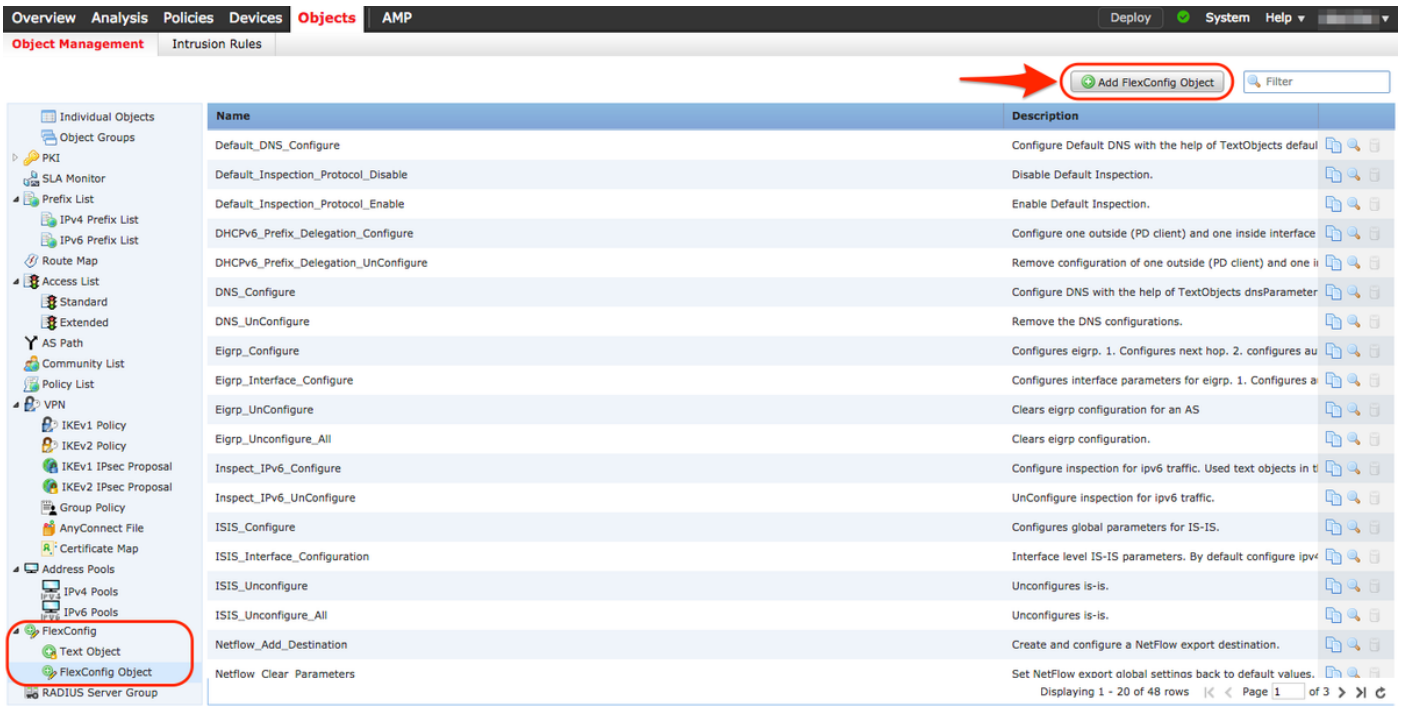


送信元ネットワークと宛先ネットワークまたはホストを選択したら、[保存]をクリック**します**。



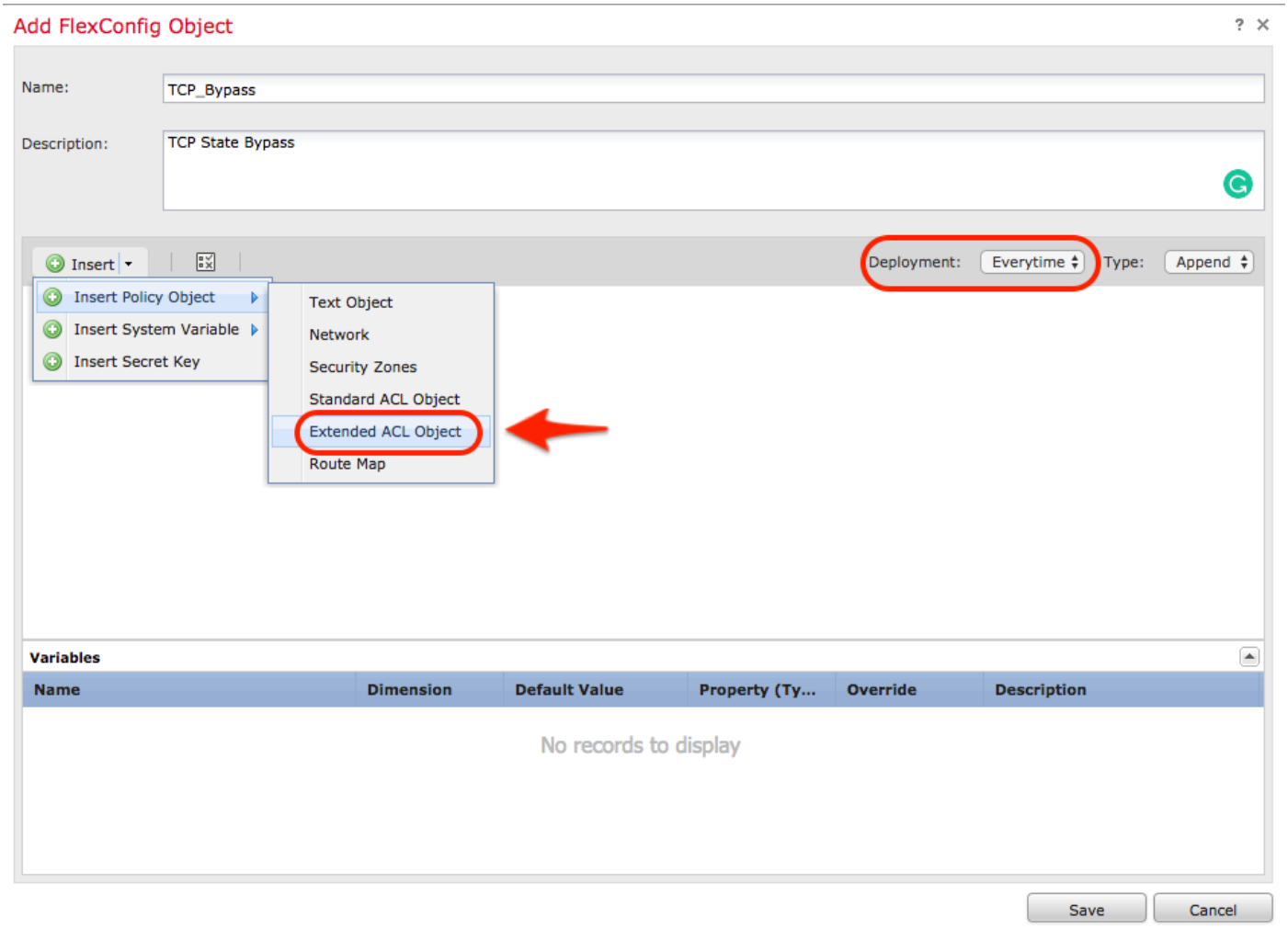
ステップ2: FlexConfigオブジェクトの設定

[Objects] > [Object Management] > [FlexConfig] > [FlexConfig Object]に移動し、[Add FlexConfig Object]ボタンをクリックします。



この例のオブジェクトの名前は、アクセスリストと同じようにTCP_Bypassと呼ばれます。この名前は、アクセスリスト名と一致する必要はありません。

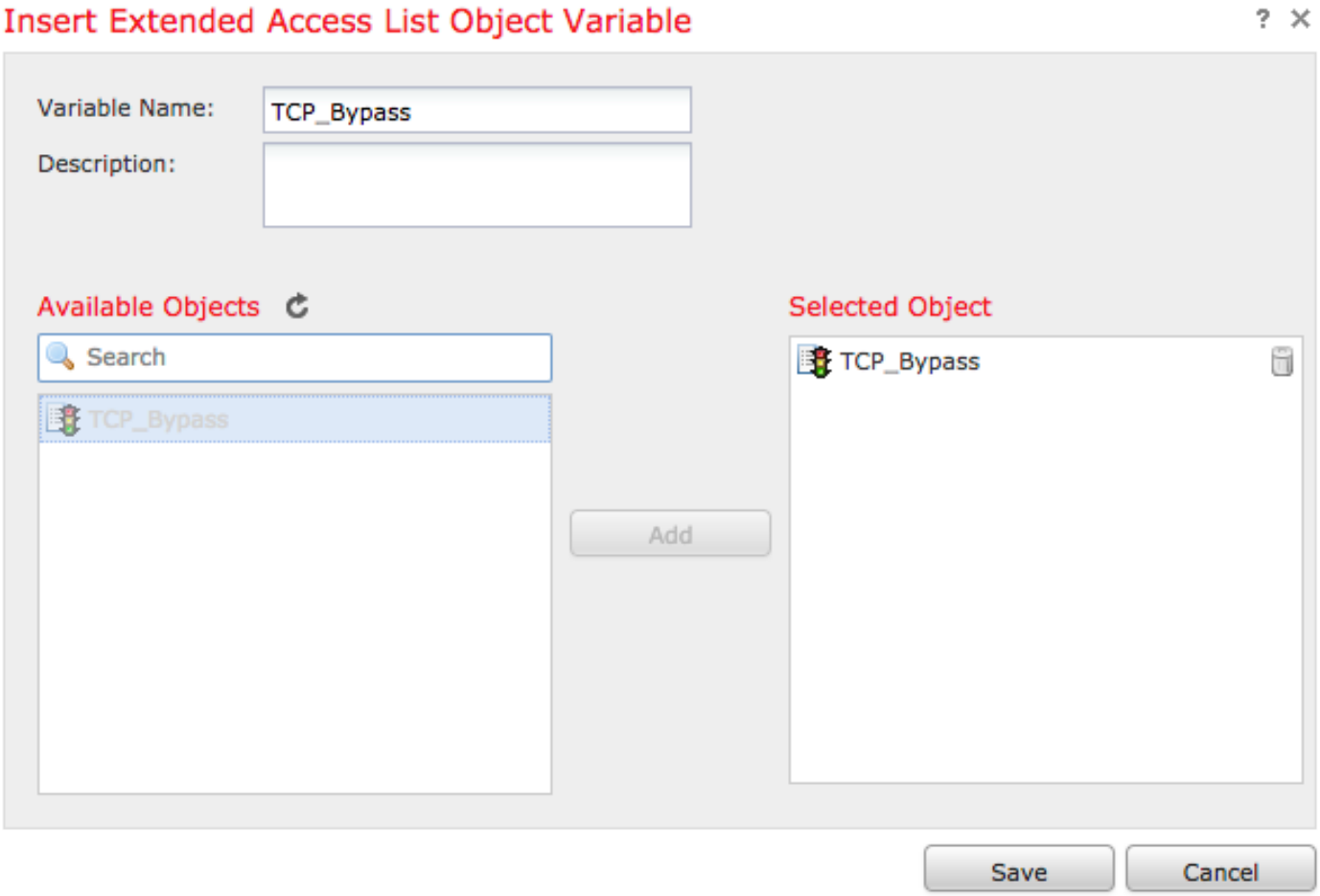
[Insert Policy Object] > [Extended ACL Object]を選択します。



注：[Everytime]オプションを選択してください。これにより、他の導入およびアップグレード時にこの設定を保持できます。

「使用可能なオブジェクト」セクションからステップ1で作成した**アクセスリ**ストを選択し、変数名を割り当てます。次に、[Add]ボタンを**クリック**します。この例では、変数名は**TCP_Bypassです**。

[Save] をクリックします。

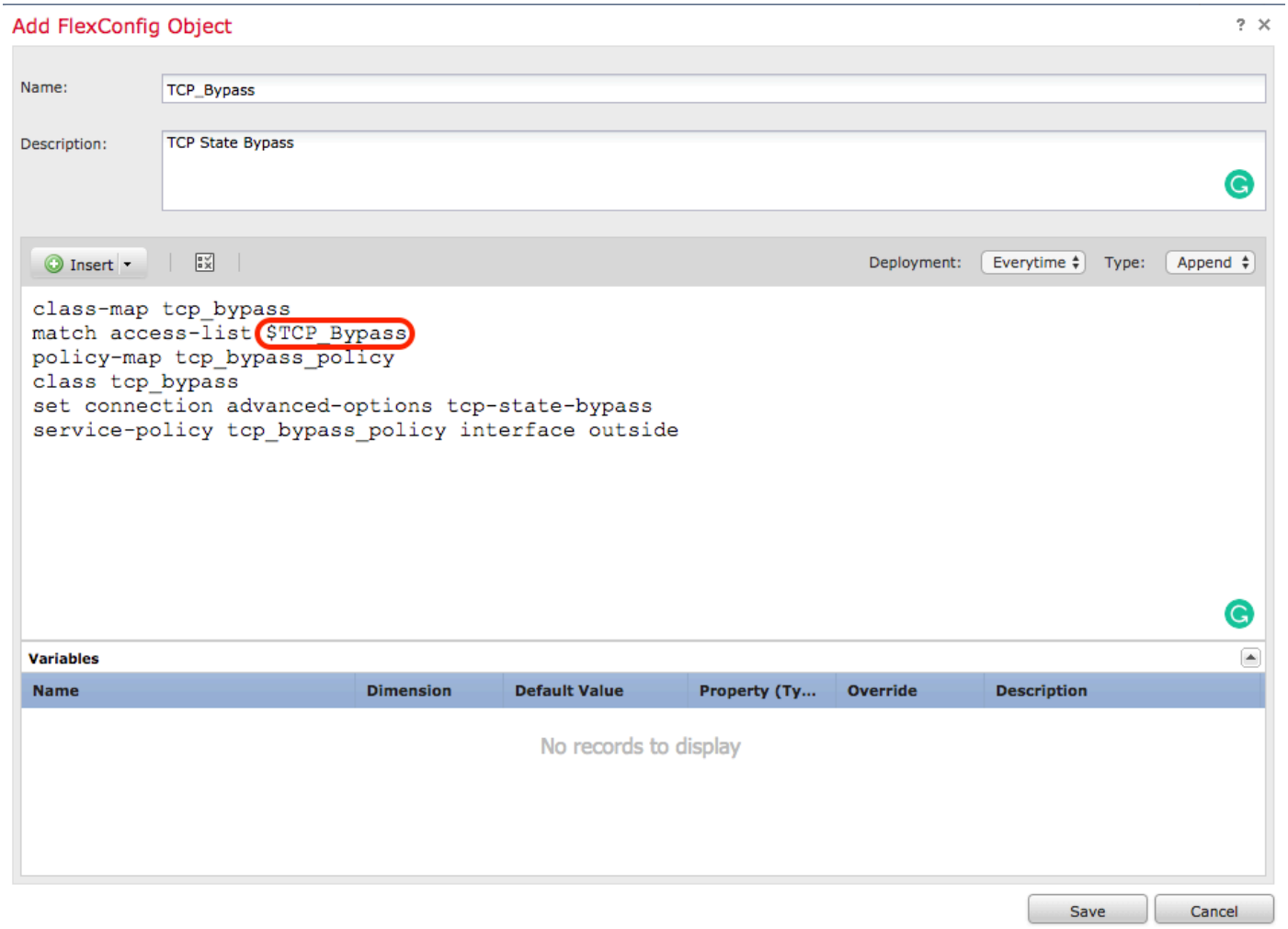


[Insert]ボタンのすぐ下の空白のフィールドに次の設定行を追加し、以前に定義した変数(**$TCP_Bypass**)を*match access-list設定行に含*めます。変数名の前に**$記号**が付加されていることに注意してください。これにより、変数がその後に続くことを定義できます。

```
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
```

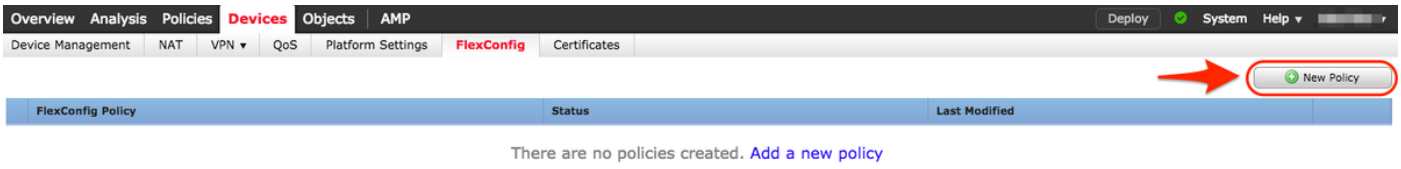
この例では、ポリシーマップが作成され、外部インターフェイスに適用されます。TCP状態バイパスをグローバルサービスポリシーの一部として設定する必要がある場合、tcp_bypassクラスマップをglobal_policyに適用できます。

終了したら、[Save]をクリックします。

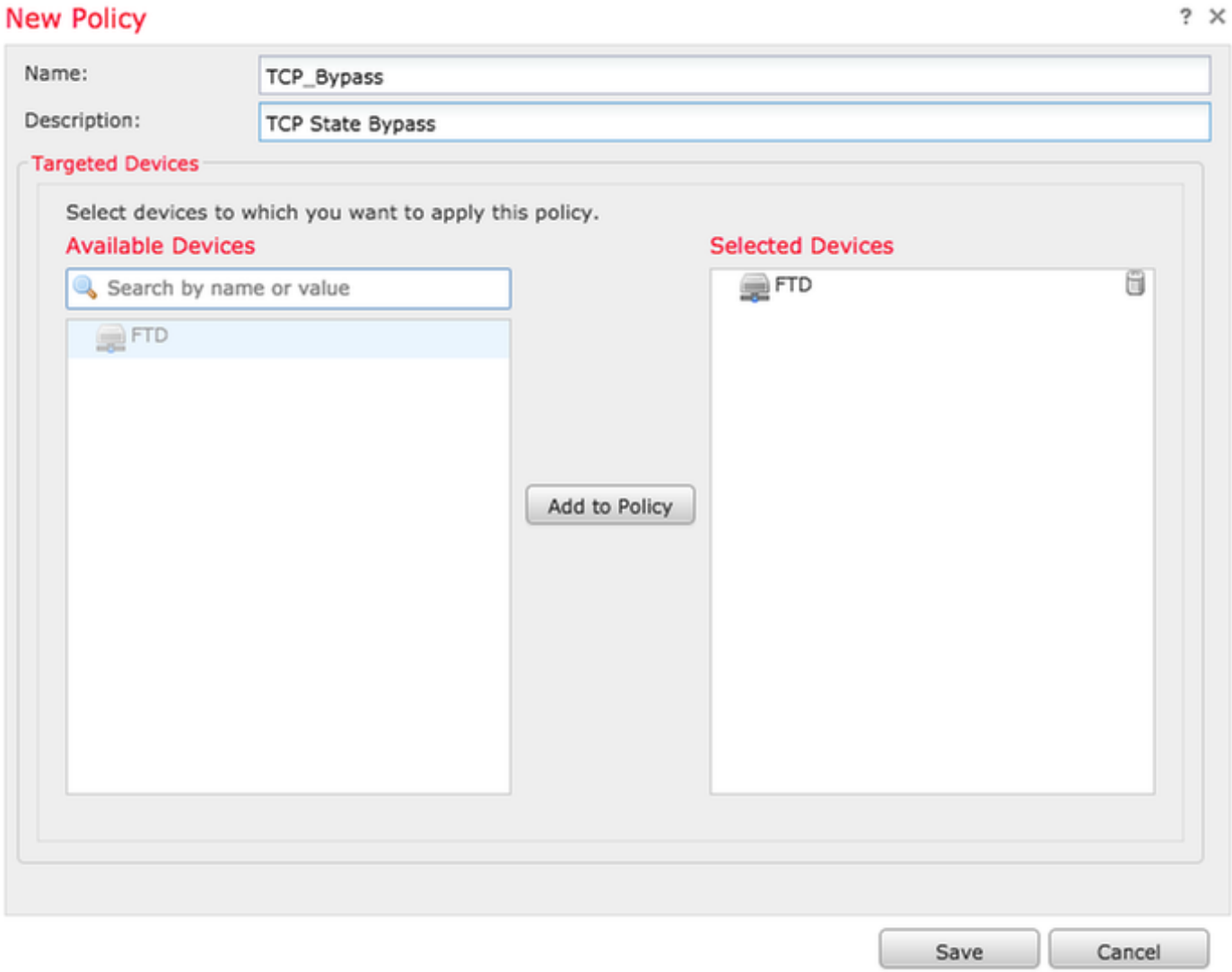


ステップ3:FTDへのFlexConfigポリシーの割り当て

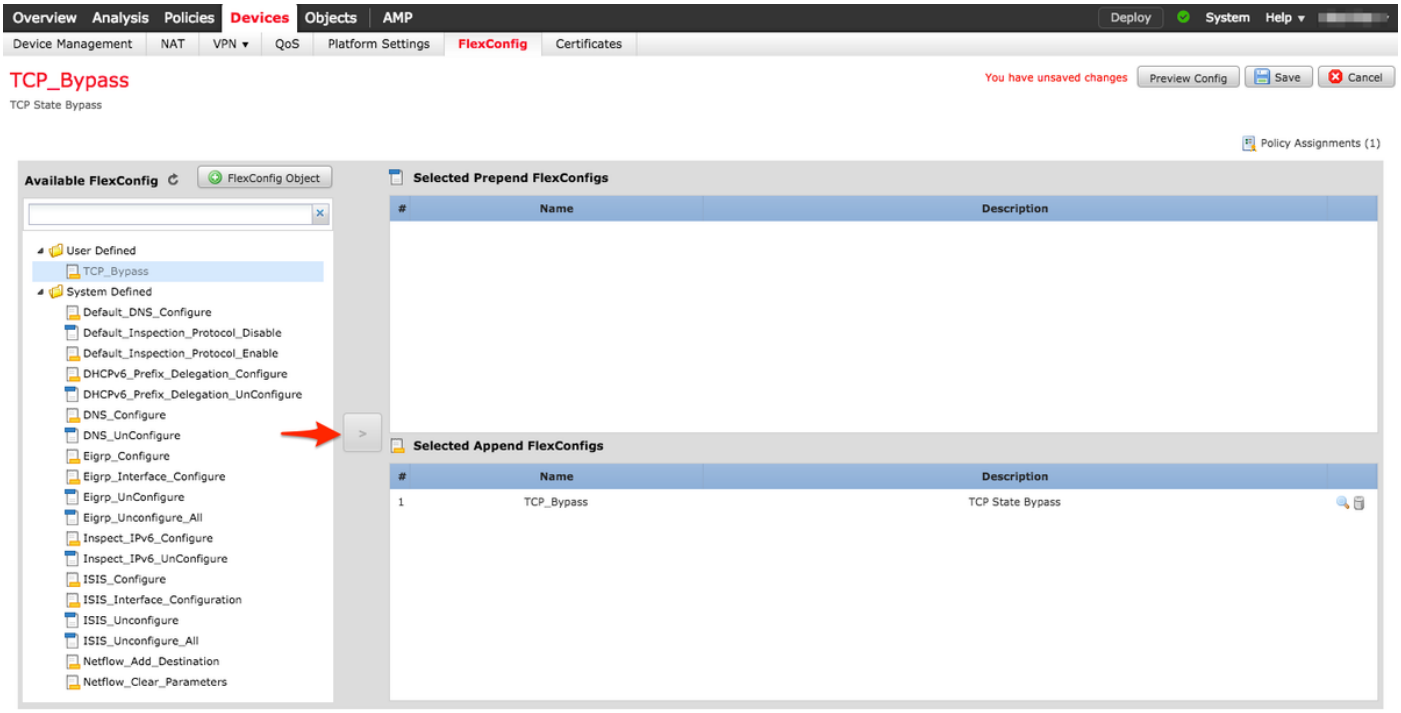
[Devices] > [FlexConfig] に移動し、新しいポリシーを作成します（別の目的で作成され、同じFTDに割り当てられているポリシーが存在しない場合）。この例では、新しいFelxConfigポリシーはTCPバイパスです。



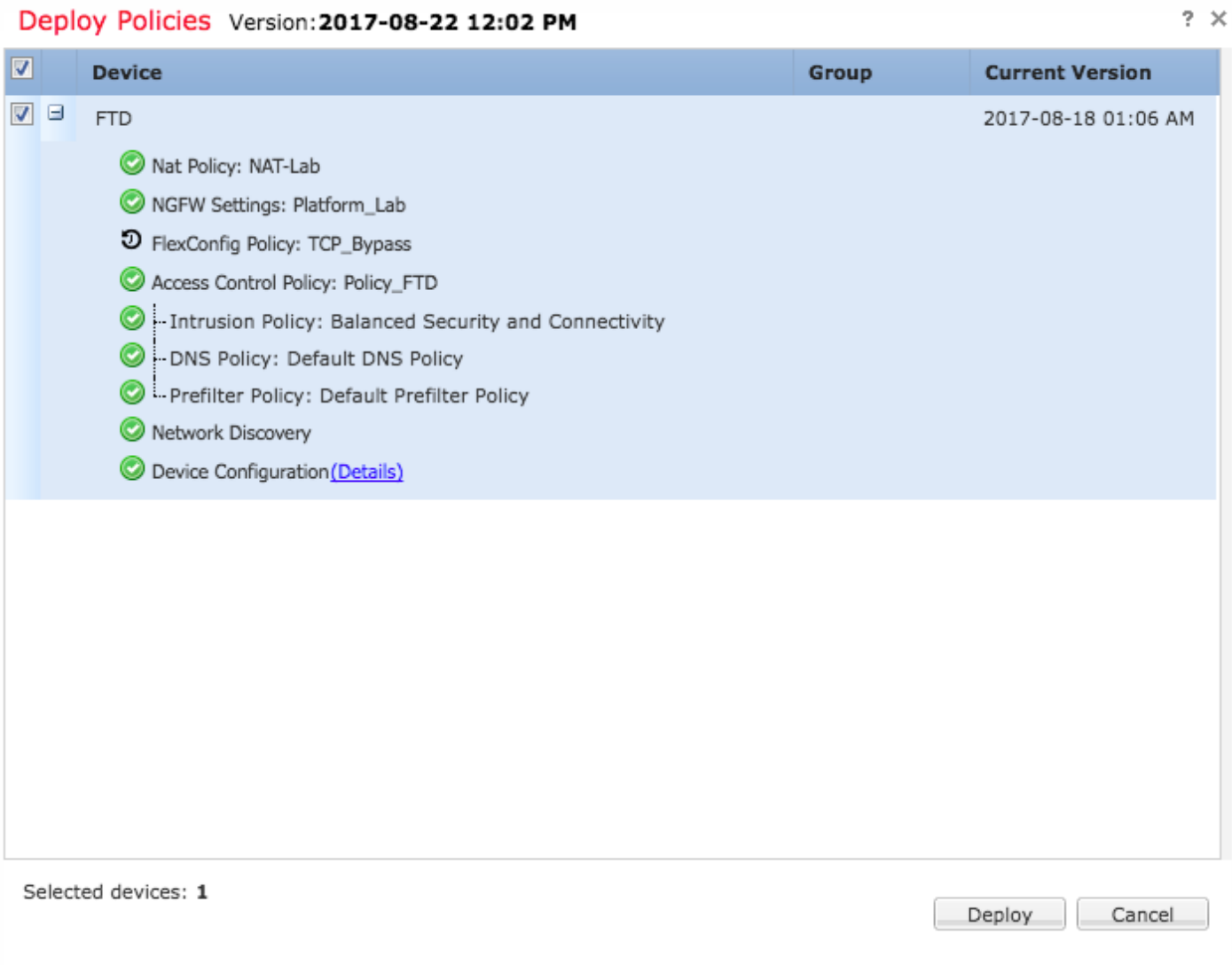
FTDデバイスにTCP_Bypass FlexConfigポリシーを割り当てます。



ステップ2で作成したTCP_Bypassという名前のFlexConfigオブジェクトを[User Defined]セクションで選択し、矢印をクリックしてそのオブジェクトをポリシーに追加します。



変更を保存して導入します



確認

SSHまたはコンソールからFTDにアクセスし、コマンドsystem support diagnostic-cliを使用します。

```
> 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
!
```

トラブルシュート

この機能をトラブルシューティングするには、次のコマンドが役に立ちます。

- 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

関連するリンク

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