

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](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[コンフィギュレーション](#)

[ステップ1: 拡張アクセスリストオブジェクトの設定](#)

[ステップ2: FlexConfigオブジェクトの設定](#)

[ステップ3:FTDへのFlexConfigポリシーの割り当て](#)

[確認](#)

[トラブルシューティング](#)

[関連するリンク](#)

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。

The screenshot shows the Cisco FMC Object Management interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'AMP'. The 'Objects' tab is selected. Below the navigation bar, there are tabs for 'Object Management' and 'Intrusion Rules'. The 'Add Extended Access List' button is highlighted with a red circle and an arrow. The left sidebar shows a tree view of object categories, with 'Access List' selected and 'Extended' highlighted. The main content area displays a table with columns 'Name', 'Value', and 'Override', and the text 'No records to display'.

[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。

New Extended Access List Object

Name:

Entries (0)

Sequence	Action	Source	Source Port	Destination	Destination Port
No records to display					

Allow Overrides:

Save Cancel

このルールアクションは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。

Add Extended Access List Entry

Action:

Logging:

Log Level:

Log Interval: Sec.

Network Port

Available Networks

- any
- any-ipv4
- any-ipv6
- FMC
- Host1
- Host2
- IPv4-Benchmark-Tests
- IPv4-Link-Local
- IPv4-Multicast
- IPv4-Private-10.0.0.0-8

Add to Source

Add to Destination

Source Networks (1)

- Host1

Destination Networks (1)

- Host2

Enter an IP address Add

Enter an IP address Add

Add Cancel

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。

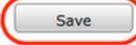
Edit Extended Access List Object

Name:

Entries (1)

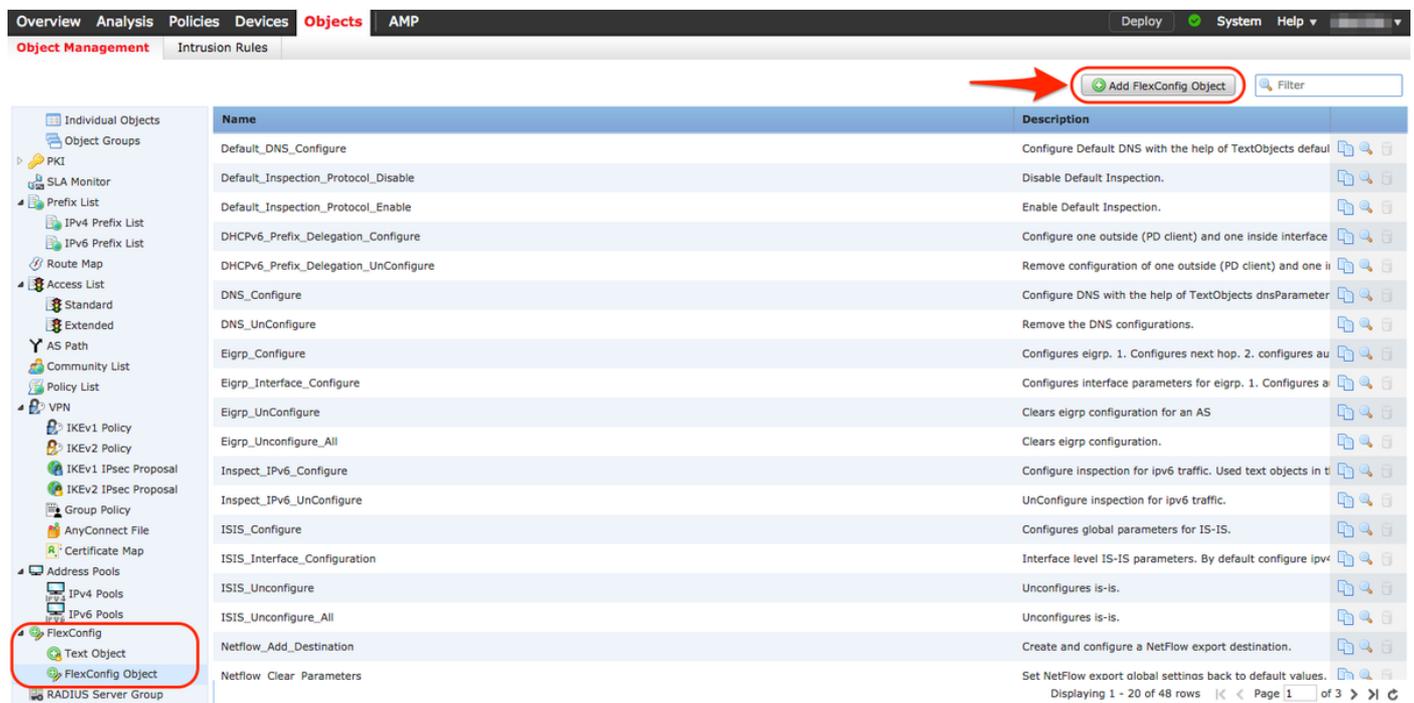
Sequence	Action	Source	Source Port	Destination	Destination Port	
1	✓ Allow	Host1	Any	Host2	Any	 

Allow Overrides:

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。



The screenshot shows the 'Object Management' section of the interface. The 'Add FlexConfig Object' button is highlighted with a red circle and a red arrow. The left sidebar shows a tree view of object categories, with 'FlexConfig' and 'FlexConfig Object' highlighted. The main table lists various configuration objects with their names and descriptions.

Name	Description
Default_DNS_Configure	Configure Default DNS with the help of TextObjects default
Default_Inspection_Protocol_Disable	Disable Default Inspection.
Default_Inspection_Protocol_Enable	Enable Default Inspection.
DHCPv6_Prefix_Delegation_Configure	Configure one outside (PD client) and one inside interface
DHCPv6_Prefix_Delegation_UnConfigure	Remove configuration of one outside (PD client) and one i
DNS_Configure	Configure DNS with the help of TextObjects dnsParameter
DNS_UnConfigure	Remove the DNS configurations.
Eigrp_Configure	Configures eigrp. 1. Configures next hop. 2. configures au
Eigrp_Interface_Configure	Configures interface parameters for eigrp. 1. Configures a
Eigrp_UnConfigure	Clears eigrp configuration for an AS
Eigrp_Unconfigure_All	Clears eigrp configuration.
Inspect_IPv6_Configure	Configure inspection for ipv6 traffic. Used text objects in t
Inspect_IPv6_UnConfigure	UnConfigure inspection for ipv6 traffic.
ISIS_Configure	Configures global parameters for IS-IS.
ISIS_Interface_Configuration	Interface level IS-IS parameters. By default configure ipv6
ISIS_Unconfigure	Unconfigures is-is.
ISIS_Unconfigure_All	Unconfigures is-is.
Netflow_Add_Destination	Create and configure a NetFlow export destination.
Netflow_Clear_Parameters	Set NetFlow export global settings back to default values.

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。

Add FlexConfig Object

Name: TCP_Bypass

Description: TCP State Bypass

Deployment: Everytime Type: Append

- Insert Policy Object
- Insert System Variable
- Insert Secret Key
- Text Object
- Network
- Security Zones
- Standard ACL Object
- Extended ACL Object
- Route Map

Variables

Name	Dimension	Default Value	Property (Ty...	Override	Description
No records to display					

Save Cancel

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 Extended Access List Object Variable

? X

Variable Name:

Description:

Available Objects

TCP_Bypass

Add

Selected Object

TCP_Bypass

Save Cancel

[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。

Add FlexConfig Object

Name:

Description:

Deployment: Type:

```
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
```

Variables

Name	Dimension	Default Value	Property (Ty...	Override	Description
No records to display					

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FlexConfig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。

New Policy

? X

Name:

Description:

Targeted Devices

Select devices to which you want to apply this policy.

Available Devices

FTD

Selected Devices

FTD

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。

Overview Analysis Policies **Devices** Objects AMP Deploy System Help

Device Management NAT VPN QoS Platform Settings **FlexConfig** Certificates

TCP_Bypass You have unsaved changes

TCP State Bypass Policy Assignments (1)

Available FlexConfig

- User Defined
 - TCP_Bypass**
- System Defined
 - Default_DNS_Configure
 - Default_Inspection_Protocol_Disable
 - Default_Inspection_Protocol_Enable
 - DHCPv6_Prefix_Delegation_Configure
 - DHCPv6_Prefix_Delegation_UnConfigure
 - DNS_Configure
 - DNS_UnConfigure
 - Eigrp_Configure
 - Eigrp_Interface_Configure
 - Eigrp_UnConfigure
 - Eigrp_Unconfigure_All
 - Inspect_IPv6_Configure
 - Inspect_IPv6_UnConfigure
 - ISIS_Configure
 - ISIS_Interface_Configuration
 - ISIS_UnConfigure
 - ISIS_Unconfigure_All
 - Netflow_Add_Destination
 - Netflow_Clear_Parameters

Selected Prepend FlexConfigs

#	Name	Description
---	------	-------------

Selected Append FlexConfigs

#	Name	Description
1	TCP_Bypass	TCP State Bypass

変更を保存して導入します

<input checked="" type="checkbox"/>	Device	Group	Current Version
<input checked="" type="checkbox"/>	FTD		2017-08-18 01:06 AM
	<input checked="" type="checkbox"/> Nat Policy: NAT-Lab		
	<input checked="" type="checkbox"/> NGFW Settings: Platform_Lab		
	<input type="checkbox"/> FlexConfig Policy: TCP_Bypass		
	<input checked="" type="checkbox"/> Access Control Policy: Policy_FTD		
	<input checked="" type="checkbox"/> Intrusion Policy: Balanced Security and Connectivity		
	<input checked="" type="checkbox"/> DNS Policy: Default DNS Policy		
	<input checked="" type="checkbox"/> Prefilter Policy: Default Prefilter Policy		
	<input checked="" type="checkbox"/> Network Discovery		
	<input checked="" type="checkbox"/> Device Configuration(Details)		

Selected devices: 1

Deploy

Cancel

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
!
```

トラブルシューティング

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_configuration/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-configuration-guide-v62/flexconfig_policies.html