

FTD: How to enable TCP State Bypass Configuration using FlexConfig Policy

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Configuration](#)

[Step 1. Configure an Extended Access List Object](#)

[Step 2. Configure a FlexConfig Object](#)

[Step 3. Assign a FlexConfig Policy to the FTD](#)

[Verification](#)

[Troubleshoot](#)

[Related Links](#)

Introduction

This document describes how to implement Transmission Control Protocol (TCP) State Bypass feature on Firepower Threat Defense (FTD) appliances via Firepower Management Center (FMC) using FlexConfig Policy in versions previous to 6.3.0.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Knowledge of Firepower Management Center.
- Basic Knowledge of Firepower Threat Defense.
- Understanding of the TCP State Bypass feature.

Components Used

The information in this document is based on these software and hardware versions:

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

Background Information

TCP State Bypass is a feature inherited from the Adaptive Security Appliance (ASA) and provides

assistance when troubleshooting traffic that could be dropped by either TCP normalization features, asymmetric routing conditions, and certain Application Inspections.

This feature is natively supported on FMC starting version 6.3.0. It is recommended to delete the Flexconfig objects after the upgrade and move this configuration to the FMC prior to the first deployment. For more information on how to configure TCP State Bypass in version 6.3.0 or later, go to this [configuration guide](#).

Firepower Threat Defense uses ASA configuration commands to implement some features, but not all features. There is no unique set of Firepower Threat Defense configuration commands. Instead, the point of FlexConfig is to allow you to configure features that are not yet directly supported through Firepower Management Center policies and settings.

Note: TCP State Bypass should only be used for troubleshooting purposes or when asymmetric routing cannot be resolved. The use of this feature disables multiple security features and can cause high number of connections if it is not properly implemented.

In order to know more about TCP State Bypass feature or its implementation in ASA, refer to [Configure the TCP State Bypass Feature on the ASA 5500 Series](#) and the Cisco ASA 5500 Series Configuration Guide.

Configuration

This section describes how to configure TCP State Bypass on FMC through a FlexConfig Policy.

Step 1. Configure an Extended Access List Object

In order to create an Extended Access List on FMC, go to **Objects > Object Management** and on the left menu, under **Access List** select **Extended**. Click **Add Extended Access List**.

The screenshot shows the FMC interface with the following elements:

- Top navigation bar: Overview, Analysis, Policies, Devices, **Objects**, AMP. Right side: Deploy, System, Help.
- Sub-navigation: **Object Management**, Intrusion Rules.
- Left sidebar menu: Tunnel Zone, Application Filters, VLAN Tag, Security Group Tag, URL, Geolocation, Time Range, Variable Set, Security Intelligence (expanded), Network Lists and Feeds, DNS Lists and Feeds, URL Lists and Feeds, Sinkhole, File List, Cipher Suite List, Distinguished Name, Individual Objects, Object Groups, PKI, SLA Monitor, Prefix List (expanded), 1Pv4 Prefix List, 1Pv6 Prefix List, Route Map, **Access List** (expanded), Standard, **Extended**.
- Main content area: A table with columns Name, Value, and Override. The table is empty with the text "No records to display".
- Buttons: "Add Extended Access List" (circled in red) and "Filter".
- Red arrows: One points to the "Add Extended Access List" button, and another points to the "Extended" option in the left sidebar.

Fill the Name field with the desired value. in this example, the name is **TCP_Bypass**. Click **Add** button.

New Extended Access List Object

Name:

Entries (0)

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

Allow Overrides:

Save Cancel

The action for this rule must be configured as **Allow**. A system defined network can be used or a new network object can be created for each source and destination. In this example, the Access List matches IP traffic from Host1 to Host2 as this is the communication to apply TCP State Bypass. Port tab can optionally be used to match a specific TCP or UDP port. Click on the **Add** button to continue.

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

Once the source and destination networks or hosts are selected, click on **Save**.


Edit Extended Access List Object

Name:

Entries (1)

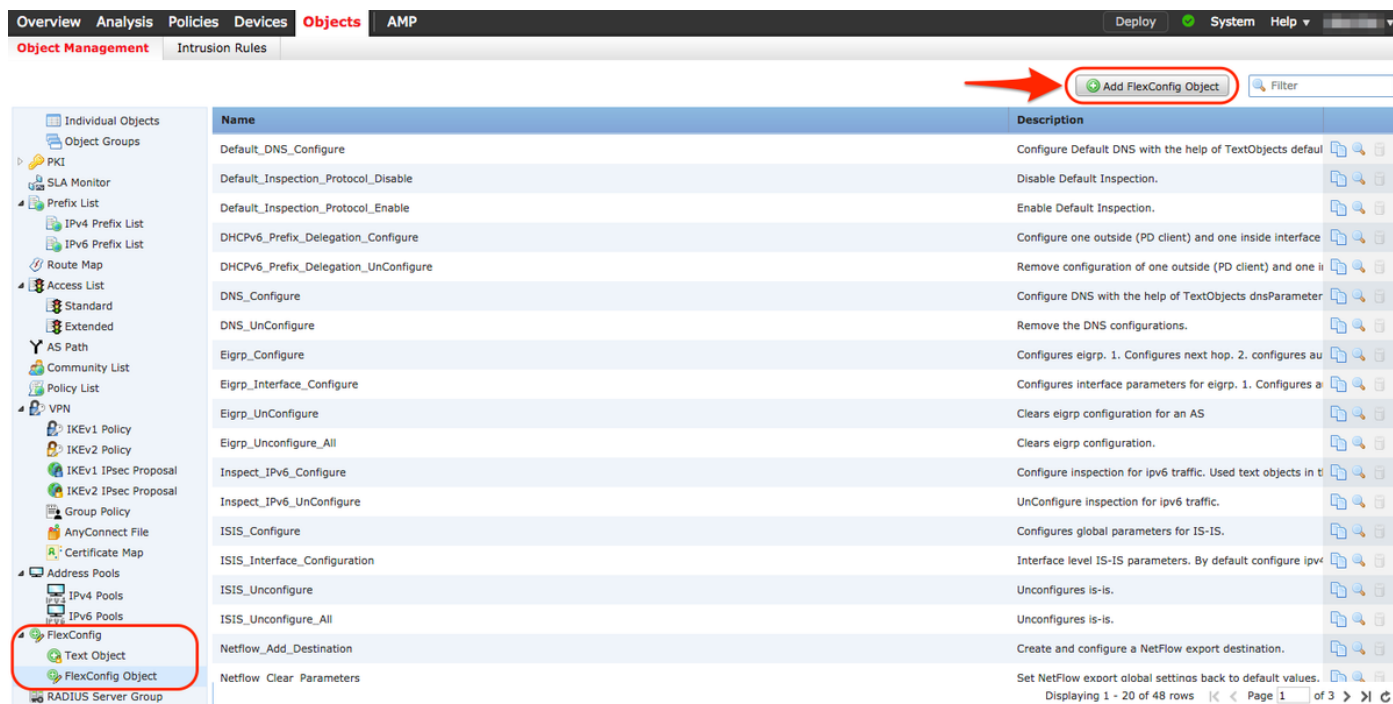
Sequence	Action	Source	Source Port	Destination	Destination Port	
1	✓ Allow	Host1	Any	Host2	Any	 

Allow Overrides:

Step 2. Configure a FlexConfig Object

Navigate to **Objects > Object Management > FlexConfig > FlexConfig Object** and click on **Add FlexConfig Object** button.



The screenshot shows the 'Object Management' interface. The 'Add FlexConfig Object' button is highlighted with a red circle and a red arrow. The interface includes a navigation menu on the left and a table of objects on the right.

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.

The name of the object for this example is called **TCP_Bypass** just as the Access List. This name doesn't need to match the Access List name.

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

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

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

Save Cancel

Note: Make sure to choose the "Everytime" option. This allows for preserving this configuration during other deployments and upgrades.

Select the Access List created in Step 1 from the **Available Objects** section and assign a Variable Name. Then, click on **Add** button. In this example, the Variable Name is **TCP_Bypass**.

Click on **Save**.

Insert Extended Access List Object Variable

? X

Variable Name:

Description:

Available Objects

TCP_Bypass

Add

Selected Object

TCP_Bypass

Save Cancel

Add the next configuration lines in the blank field right below the **Insert** button and include the variable previously defined (**\$TCP_Bypass**) in the *match access-list* configuration line. Note that a **\$** symbol is prepended to the variable name. This helps define that a variable follows after it.

```
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 this example, a policy-map is created and it is applied to the outside interface. If TCP State Bypass requires to be configured as part of the global service policy, the tcp_bypass class map can be applied to global_policy.

Click on **Save** when finished.

Add FlexConfig Object

Name:

Description:

Deployment: Type:

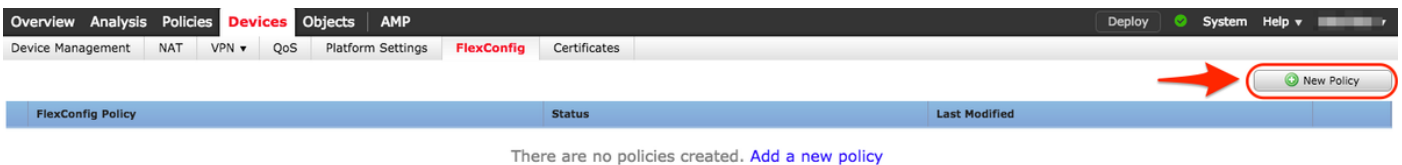
```
class-map tcp_bypass
match access-list $TCP_Bypass
policy-map tcp_bypass_policy
class tcp_bypass
set connection advanced-options tcp-state-bypass
service-policy tcp_bypass_policy interface outside
```

Variables

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

Step 3. Assign a FlexConfig Policy to the FTD

Go to **Devices > FlexConfig** and create a new policy (unless there is already one created for another purpose and assigned to the same FTD). In this example, the new FlexConfig policy is called **TCP_Bypass**.



Assign the **TCP_Bypass** FlexConfig policy to the FTD device.

New Policy



Name:

Description:

Targeted Devices

Select devices to which you want to apply this policy.

Available Devices

FTD

Selected Devices

FTD

Select the FlexConfig Object called **TCP_Bypass** created in Step 2 under the **User Defined** section and click on the arrow to add that object to the policy.

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

Save the changes and deploy,

✓	Device	Group	Current Version
✓	FTD		2017-08-18 01:06 AM
	<ul style="list-style-type: none"> ✓ Nat Policy: NAT-Lab ✓ NGFW Settings: Platform_Lab ⌚ FlexConfig Policy: TCP_Bypass ✓ Access Control Policy: Policy_FTD ✓ ---Intrusion Policy: Balanced Security and Connectivity ✓ ---DNS Policy: Default DNS Policy ✓ ---Prefilter Policy: Default Prefilter Policy ✓ Network Discovery ✓ Device Configuration(Details) 		

Selected devices: 1

Deploy

Cancel

Verification

Access the FTD through SSH or console and use the command **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

To troubleshoot this feature, these commands result in helpful.

- **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

Related 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