

# FTD : Comment activer la configuration de contournement d'état de TCP utilisant la stratégie de FlexConfig

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Informations générales](#)

[Configuration](#)

[Étape 1. Configurez un objet étendu de liste d'accès](#)

[Étape 2. Configurez un objet de FlexConfig](#)

[Étape 3. Assignez une stratégie de FlexConfig au FTD](#)

[Vérification](#)

[Dépannez](#)

[Liens connexes](#)

## Introduction

Ce document décrit comment implémenter la caractéristique de contournement de Protocole TCP (Transmission Control Protocol) sur des appliances de la défense contre des menaces de FirePOWER (FTD) par l'intermédiaire du centre de Gestion de FirePOWER (FMC) utilisant la stratégie de FlexConfig.

## Conditions préalables

### Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- La connaissance du centre de Gestion de FirePOWER.
- Connaissance de base de défense contre des menaces de FirePOWER.
- Compréhension de la caractéristique de contournement d'état de TCP.

### [Composants utilisés](#)

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Version 6.2 et ultérieures de la défense contre des menaces de FirePOWER (FTD).
- Version 6.2 et ultérieures du centre de Gestion de FirePOWER (FMC).

## Informations générales

Le contournement d'état de TCP est une caractéristique héritée de l'appliance de sécurité adaptable (ASA) et fournit le trafic de pour le dépannage d'assistance qui pourrait être abandonné par l'un ou l'autre de caractéristiques de normalisation de TCP, d'états asymétriques de routage et de certaines inspections d'application.

Au moment d'écrire ce document, FMC ne le prend en charge pas naturellement pour configurer le contournement d'état de TCP, à moins que la stratégie de FlexConfig soit utilisée.

La défense contre des menaces de FirePOWER utilise des commandes de configuration ASA d'implémenter quelques caractéristiques, mais non toutes les caractéristiques. Il n'y a aucun seul ensemble de commandes de configuration de défense contre des menaces de FirePOWER. Au lieu de cela, le point de FlexConfig est de te permettre pour configurer les caractéristiques qui ne sont pas encore directement prises en charge par des stratégies et des configurations de centre de Gestion de FirePOWER.

**Note:** Le contournement d'état de TCP devrait seulement être utilisé pour dépanner des buts ou quand le routage asymétrique ne peut pas être résolu. L'utilisation de cette caractéristique désactive de plusieurs fonctionnalités de sécurité et peut entraîner le nombre élevé de connexions si elle n'est pas correctement mise en application.

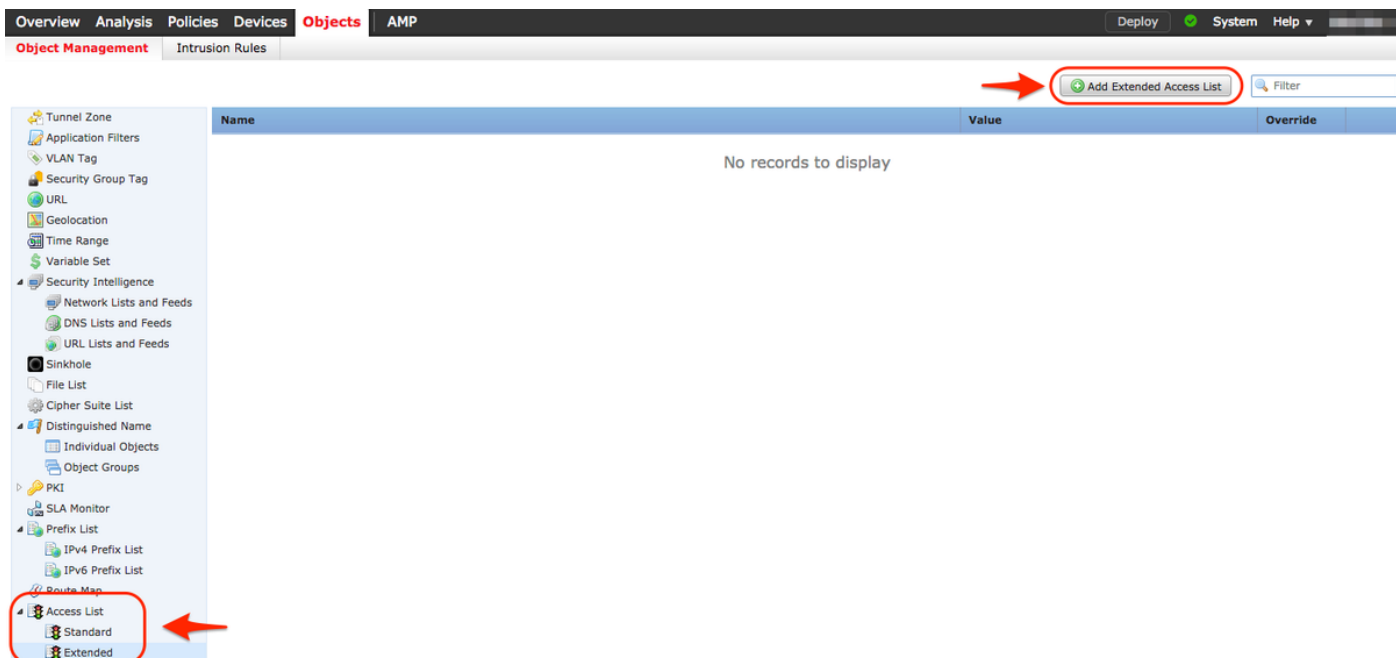
Afin de connaître plus la caractéristique de contournement d'état de TCP ou son implémentation dans l'ASA, référez-vous [configurent la caractéristique de contournement d'état de TCP sur la gamme ASA 5500](#) et le guide de configuration de gamme de Cisco ASA 5500.

## Configuration

Cette section décrit comment configurer le contournement de TCP sur FMC par une stratégie de FlexConfig.

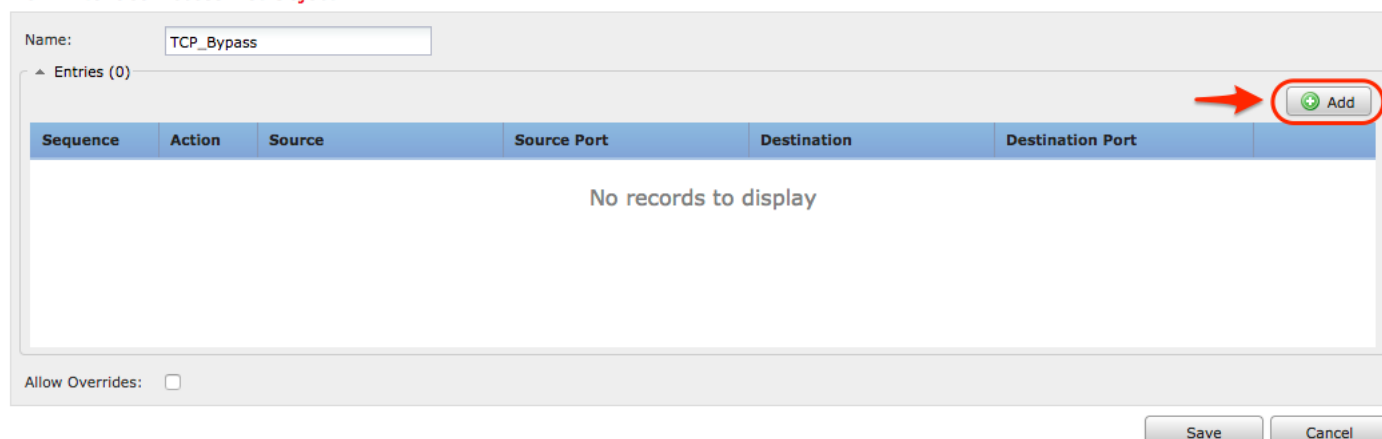
### Étape 1. Configurez un objet étendu de liste d'accès

Afin de créer une liste d'accès étendue sur FMC, allez à la **Gestion de >Object d'objets** et sur le menu de gauche, sous **étendu** choisi de **liste d'accès**. ClickAdd a **étendu la liste d'accès**.



Remplissez zone d'identification de valeur désirée. dans cet exemple, le nom est **TCP\_Bypass**. Cliquez sur **Add le bouton**.

#### New Extended Access List Object



L'action pour cette règle doit être configurée comme **laissent**. Un réseau défini par système peut être utilisé ou un nouvel objet de réseau peut être créé pour chaque source et destination. Dans cet exemple, la liste d'accès apparie le trafic IP de Host1 à Host2 car c'est la transmission pour appliquer le contournement d'état de TCP. L'onglet de port peut sur option être utilisé pour apparie un TCP ou un port UDP spécifique. Cliquez sur en fonction le bouton d'**ajouter** pour continuer.

## Add Extended Access List Entry

? X



Action:  Allow

Logging: Default

Log Level: Informational

Log Interval: 300 Sec.

**Network** Port

Available Networks  

Search by name or value

- 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



Une fois que la source et les réseaux ou les hôtes de destination sont sélectionnés, cliquez sur en fonction la **sauvegarde**.

## Edit Extended Access List Object


? X

Name: TCP\_Bypass

Entries (1) 

Sequence	Action	Source	Source Port	Destination	Destination Port	
1	<input checked="" type="checkbox"/> Allow	Host1	Any	Host2	Any	 

Allow Overrides:

 Save Cancel

## Étape 2. Configurez un objet de FlexConfig

Naviguez vers les objets > la Gestion d'objet > le FlexConfig > l'objet de FlexConfig et cliquez sur en fonction le bouton d'objet Add FlexConfig.

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

Object Management Intrusion Rules Add FlexConfig Object Filter

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.

Displaying 1 - 20 of 48 rows Page 1 of 3

Le nom de l'objet pour cet exemple s'appelle **TCP\_Bypass** juste comme la liste d'accès. Ce nom n'a pas besoin d'apparier le nom de liste d'accès.

**Objet choisi de stratégie d'insertion > objet étendu d'ACL.**

### Add FlexConfig Object

Name:

Description:

Deployment: Everytime Type: Append

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

**Variables**

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

Save Cancel

**Note:** Actuellement, et selon des BU, quand un policy-map est appliqué sur une interface il

est retiré dans le prochain déploiement et c'est comportement prévu. Le contournement pour cette question est de créer l'objet de flexible-config avec « chaque fois » l'option configurée pour le mode de déploiement.

Sélectionnez la liste d'accès créée dans l'étape 1 de la section **disponible d'objets** et assignez un nom de la variable. Puis, cliquez sur en fonction le bouton **Add**. Dans cet exemple, le nom de la variable est **TCP\_Bypass**.

Cliquez sur en fonction la **sauvegarde**.

### Insert Extended Access List Object Variable

? X

Variable Name:

Description:

Available Objects

TCP\_Bypass

Add

Selected Object

TCP\_Bypass

Save Cancel

Ajoutez les prochaines lignes de configuration dans le juste de champ vide au-dessous du bouton d'**insertion** et incluez la variable précédemment définie (**\$TCP\_Bypass**) dans la ligne de configuration de *match access-list*. Notez qu'un symbole **\$** est ajouté au début au nom de la variable. Ceci aide à définir qu'une variable suit après elle.

```
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
```

Dans cet exemple, un policy-map est créé et il est appliqué à l'interface extérieure. Si le contournement d'état de TCP exige d'être configuré en tant qu'élément de la stratégie de service mondial, le class map de tcp\_bypass peut être appliqué au global\_policy.

Cliquez sur en fonction la **sauvegarde** une fois terminé.

## Add FlexConfig Object

Name:

Description:

Deployment:  Type:

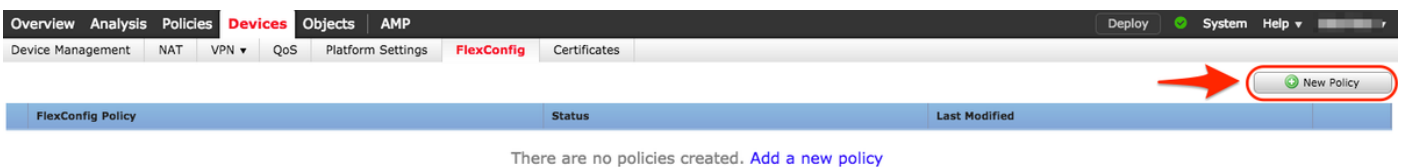
```
class-map tcp_bypass
match access-list $TCP_Bypass
policy-map tcp_bypass_policy
class tcp_bypass
set connection advanced-options tcp-state-bypass
service-policy tcp_bypass_policy interface outside
```

**Variables**

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

### Étape 3. Assignez une stratégie de FlexConfig au FTD

Allez aux **périphériques** > au **FlexConfig** et créez une nouvelle stratégie (à moins qu'il y a déjà d'une créée pour un autre but et assignée au même FTD). Dans cet exemple la nouvelle stratégie de FlexConfig s'appelle **TCP\_Bypass**.



Assignez la stratégie de **TCP\_Bypass** FlexConfig au périphérique FTD.

## New Policy



Name:

Description:

**Targeted Devices**

Select devices to which you want to apply this policy.

**Available Devices**

FTD

**Selected Devices**

FTD

Sélectionnez l'objet de FlexConfig appelé **TCP\_Bypass** créé dans l'étape 2 sous la section **définie par l'utilisateur** et cliquez sur en fonction la flèche pour ajouter cet objet à la stratégie.

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

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

**TCP\_Bypass** You have unsaved changes Preview Config Save Cancel

TCP State Bypass Policy Assignments (1)

**Available FlexConfig** FlexConfig Object

- 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

Sauvegardez les modifications et déployez-vous,



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

Selected devices: 1

Deploy

Cancel

## Vérification

Accédez au FTD par le SSH ou la console et utilisez l'**assistance technique diagnostic-cli de commande**.

```
> 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
!
```

## Dépannez

Pour dépanner cette caractéristique, résultat de ces commandes utile.

### - **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

## Liens connexes

[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/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](https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-configuration-guide-v62/flexconfig_policies.html)