

FTD : Comment activer la configuration de contournement de l'état TCP à l'aide de la stratégie FlexConfig

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[Configuration](#)

[Étape 1. Configurer un objet de liste de contrôle d'accès étendue](#)

[Étape 2. Configurer un objet FlexConfig](#)

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

[Vérification](#)

[Dépannage](#)

[Liens connexes](#)

Introduction

Ce document décrit comment mettre en oeuvre la fonctionnalité de contournement d'état TCP (Transmission Control Protocol) sur les appliances Firepower Threat Defense (FTD) via Firepower Management Center (FMC) à l'aide de la stratégie FlexConfig dans les versions antérieures à la version 6.3.0.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissance du Centre de gestion Firepower.
- Connaissances de base sur la protection contre les menaces de Firepower.
- Compréhension de la fonction TCP State Bypass.

Components Used

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

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

Informations générales

Le contournement d'état TCP est une fonctionnalité héritée de l'appliance de sécurité adaptatif (ASA) et fournit une assistance lors du dépannage du trafic qui pourrait être abandonné par les fonctions de normalisation TCP, les conditions de routage asymétrique et certaines inspections d'applications.

Cette fonctionnalité est nativement prise en charge sur FMC à partir de la version 6.3.0. Il est recommandé de supprimer les objets Flexconfig après la mise à niveau et de déplacer cette configuration vers le FMC avant le premier déploiement. Pour plus d'informations sur la configuration du contournement de l'état TCP dans la version 6.3.0 ou ultérieure, consultez ce [guide de configuration](#).

Firepower Threat Defense utilise des commandes de configuration ASA pour implémenter certaines fonctionnalités, mais pas toutes. Il n'existe pas d'ensemble unique de commandes de configuration Firepower Threat Defense. Au lieu de cela, l'objectif de FlexConfig est de vous permettre de configurer des fonctionnalités qui ne sont pas encore prises en charge directement par le biais des stratégies et paramètres Firepower Management Center.

Remarque : Le contournement de l'état TCP doit être utilisé uniquement à des fins de dépannage ou lorsque le routage asymétrique ne peut pas être résolu. L'utilisation de cette fonctionnalité désactive plusieurs fonctions de sécurité et peut entraîner un nombre élevé de connexions si elle n'est pas correctement implémentée.

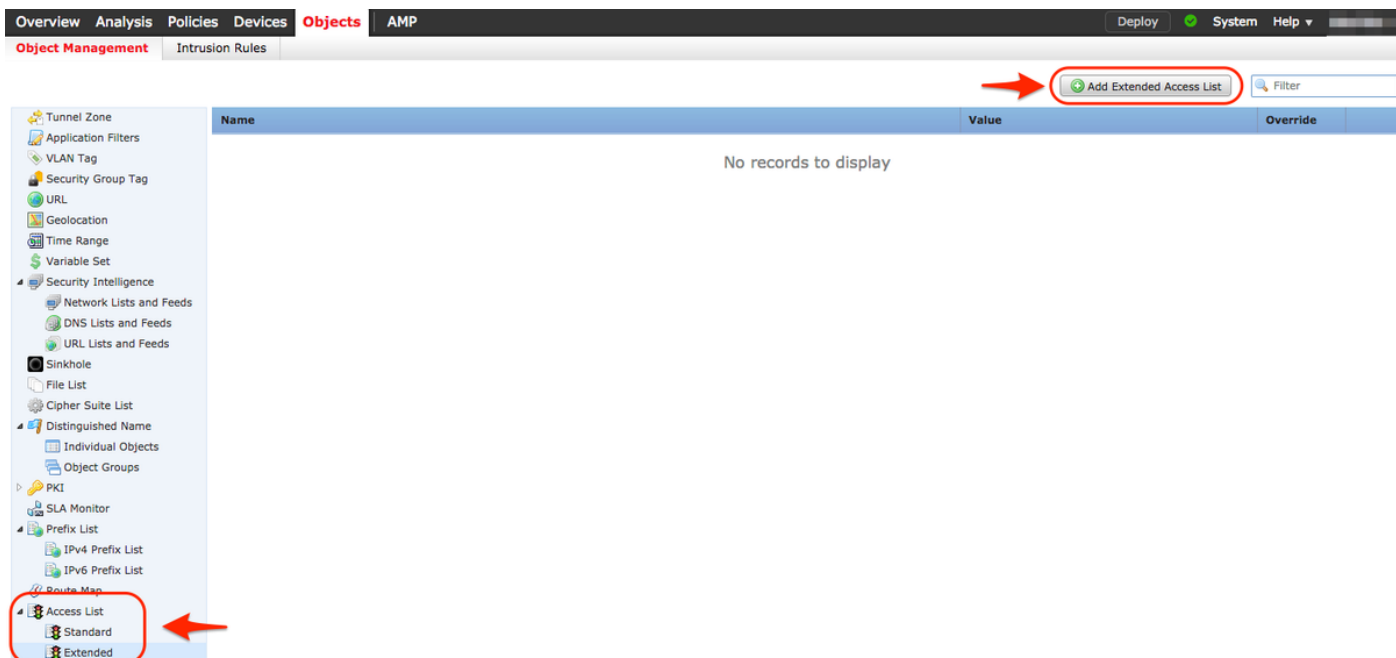
Pour en savoir plus sur la fonctionnalité de contournement d'état TCP ou sa mise en oeuvre dans ASA, référez-vous à [Configurer la fonctionnalité de contournement d'état TCP sur la gamme ASA 5500](#) et au Guide de configuration de la gamme Cisco ASA 5500.

Configuration

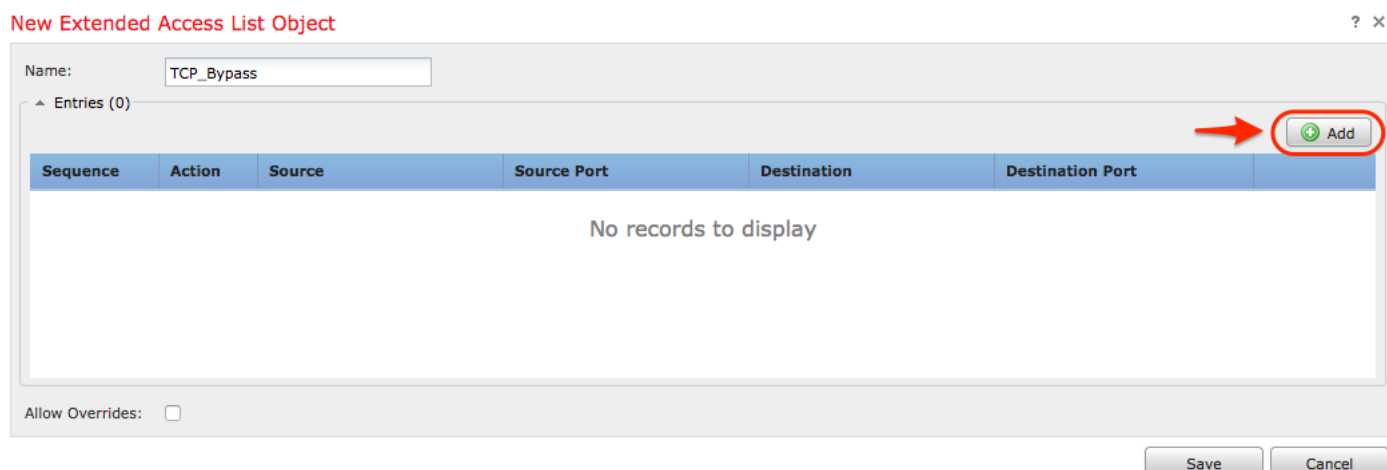
Cette section décrit comment configurer le contournement de l'état TCP sur FMC via une stratégie FlexConfig.

Étape 1. Configurer un objet de liste de contrôle d'accès étendue

Afin de créer une liste d'accès étendue sur FMC, accédez à **Objets > Gestion des objets** et dans le menu de gauche, sous **Liste d'accès** sélectionnez **Étendue**. Cliquez sur **Ajouter une liste d'accès étendue**.



Remplissez le champ Nom avec la valeur souhaitée. dans cet exemple, le nom est **TCP_Bypass**. Cliquez sur le bouton **Ajouter**.



L'action de cette règle doit être configurée comme **Autoriser**. Un réseau défini par le système peut être utilisé ou un nouvel objet réseau peut être créé pour chaque source et destination. Dans cet exemple, la liste de contrôle d'accès fait correspondre le trafic IP de l'hôte 1 à l'hôte 2, car il s'agit de la communication pour appliquer le contournement de l'état TCP. L'onglet Port peut éventuellement être utilisé pour correspondre à un port TCP ou UDP spécifique. Cliquez sur le bouton **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 les réseaux ou hôtes source et de destination sont sélectionnés, cliquez sur **Enregistrer**.

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. Configurer un objet FlexConfig

Accédez à **Objets > Gestion des objets > FlexConfig > FlexConfig Object** et cliquez sur le bouton **Ajouter un objet 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 est appelé **TCP_Bypass** comme la liste d'accès. Ce nom ne doit pas nécessairement correspondre au nom de la liste d'accès.

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

Add FlexConfig Object ? x

Name: TCP_Bypass

Description: TCP State Bypass

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: Veuillez à choisir l'option « Tout le temps ». Cela permet de conserver cette

configuration lors d'autres déploiements et mises à niveau.

Sélectionnez la liste d'accès créée à l'étape 1 dans la section **Objets disponibles** et attribuez un nom de variable. Ensuite, cliquez sur le bouton **Ajouter**. Dans cet exemple, le nom de variable est **TCP_Bypass**.

Cliquez sur **Enregistrer**.

Insert Extended Access List Object Variable

The screenshot shows a dialog box titled "Insert Extended Access List Object Variable". At the top, there are two input fields: "Variable Name:" containing "TCP_Bypass" and "Description:" which is empty. Below these are two panels. The left panel, "Available Objects", has a search bar and a list with "TCP_Bypass" selected. The right panel, "Selected Object", shows "TCP_Bypass" with a trash icon. An "Add" button is positioned between the two panels. At the bottom right, there are "Save" and "Cancel" buttons.

Ajoutez les lignes de configuration suivantes dans le champ vide situé juste en dessous du bouton **Insertion** et incluez la variable précédemment définie (**\$TCP_Bypass**) dans la ligne de configuration *match access-list*. Notez qu'un symbole **\$** est précédé du nom de la variable. Cela permet de définir qu'une variable suit.

```
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, une carte-politique est créée et appliquée à l'interface externe. Si le contournement de l'état TCP doit être configuré dans le cadre de la stratégie de service globale, la carte de classe `tcp_bypass` peut être appliquée à `global_policy`.

Cliquez sur **Enregistrer** lorsque vous avez terminé.

Add FlexConfig Object

Name:

Description:

Deployment: Type:

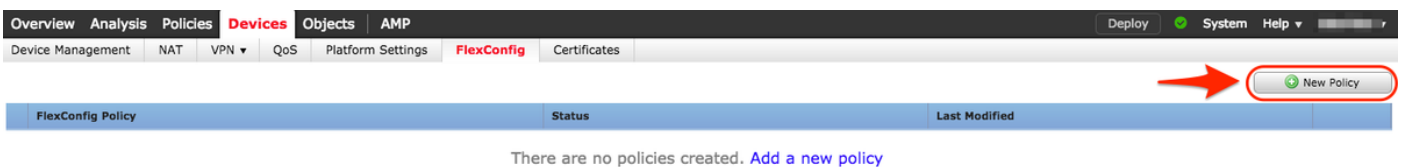
```
class-map tcp_bypass
match access-list $TCP_Bypass
policy-map tcp_bypass_policy
class tcp_bypass
set connection advanced-options tcp-state-bypass
service-policy tcp_bypass_policy interface outside
```

Variables

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

Étape 3. Affecter une stratégie FlexConfig au FTD

Accédez à **Périphériques > FlexConfig** et créez une nouvelle stratégie (sauf si une stratégie a déjà été créée à une autre fin et affectée au même FTD). Dans cet exemple, la nouvelle stratégie FlexConfig est appelée **TCP_Bypass**.



Affectez la stratégie FlexConfig **TCP_Bypass** 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 FlexConfig appelé **TCP_Bypass** créé à l'étape 2 sous la section **Défini par l'utilisateur** et cliquez sur 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

Enregistrer les modifications et les déployer,

✓	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

Vérification

Accédez au FTD via SSH ou la console et utilisez la commande **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
!
```

Dépannage

Pour dépanner cette fonctionnalité, ces commandes vous permettent de vous aider.

- **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/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