

FTD Come abilitare la configurazione di bypass dello stato TCP utilizzando il criterio FlexConfig

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Passaggio 1. Configurare un oggetto elenco accessi esteso](#)

[Passaggio 2. Configurare un oggetto FlexConfig](#)

[Passaggio 3. Assegnare un criterio FlexConfig all'FTD](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Collegamenti correlati](#)

Introduzione

In questo documento viene descritto come implementare la funzione di bypass dello stato del protocollo TCP (Transmission Control Protocol) sugli accessori Firepower Threat Defense (FTD) tramite Firepower Management Center (FMC) utilizzando FlexConfig Policy nelle versioni precedenti alla 6.3.0.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenza di Firepower Management Center.
- Conoscenze base di Firepower Threat Defense.
- Informazioni sulla funzionalità TCP State Bypass.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

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

Premesse

Il bypass dello stato TCP è una funzione ereditata da ASA (Adaptive Security Appliance) e fornisce assistenza durante la risoluzione dei problemi di traffico che potrebbero essere eliminati dalle funzionalità di normalizzazione TCP, dalle condizioni di routing asimmetrico e da alcune ispezioni delle applicazioni.

Questa funzionalità è supportata in modo nativo in FMC a partire dalla versione 6.3.0. Si consiglia di eliminare gli oggetti Flexconfig dopo l'aggiornamento e spostare la configurazione in FMC prima della prima distribuzione. Per ulteriori informazioni su come configurare TCP State Bypass nella versione 6.3.0 o successive, consultare questa [guida alla configurazione](#).

Firepower Threat Defense utilizza i comandi di configurazione ASA per implementare alcune funzionalità, ma non tutte. Non è disponibile un set univoco di comandi di configurazione di Firepower Threat Defense. Lo scopo di FlexConfig è invece quello di consentire la configurazione di funzionalità non ancora supportate direttamente tramite i criteri e le impostazioni di Firepower Management Center.

Nota: il bypass dello stato TCP deve essere utilizzato solo per la risoluzione dei problemi o quando non è possibile risolvere il routing asimmetrico. L'utilizzo di questa funzionalità disabilita più funzionalità di protezione e può causare un numero elevato di connessioni se non viene implementata correttamente.

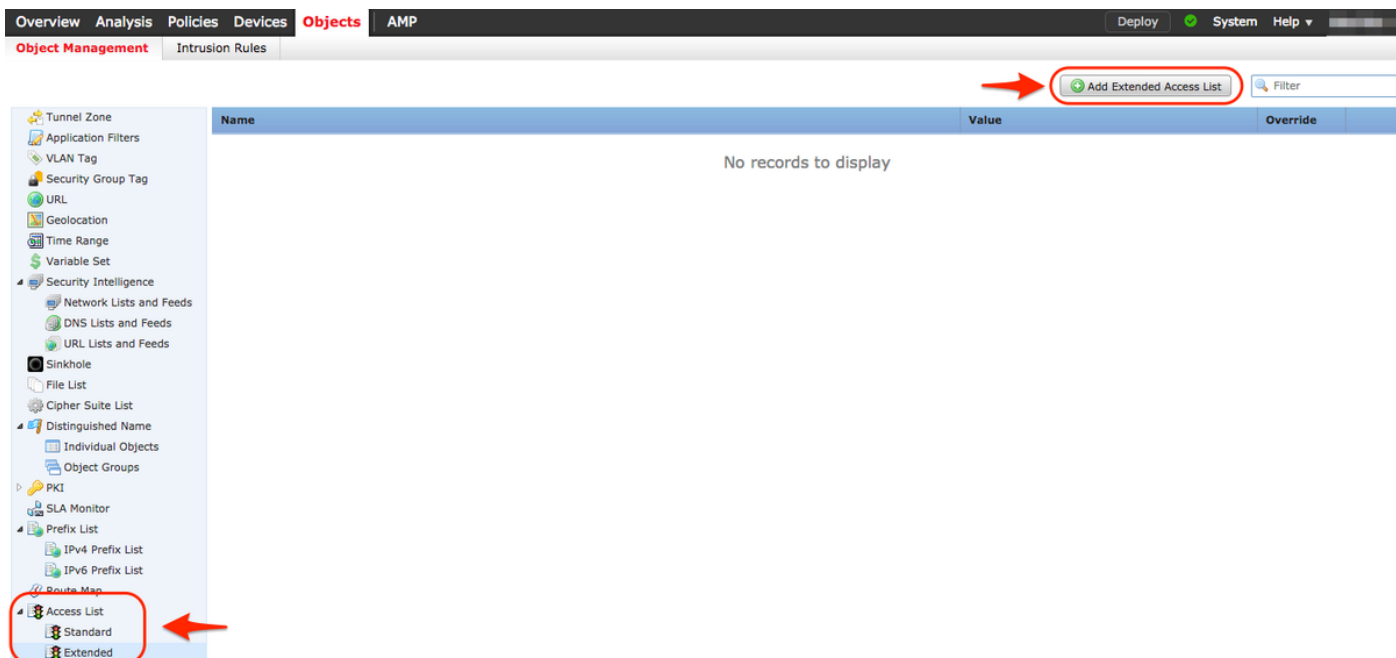
Per ulteriori informazioni sulla funzione TCP State Bypass o sulla sua implementazione nell'ASA, consultare il documento sulla [configurazione della funzione TCP State Bypass sull'appliance ASA serie 5500](#) e la guida alla configurazione di Cisco ASA serie 5500.

Configurazione

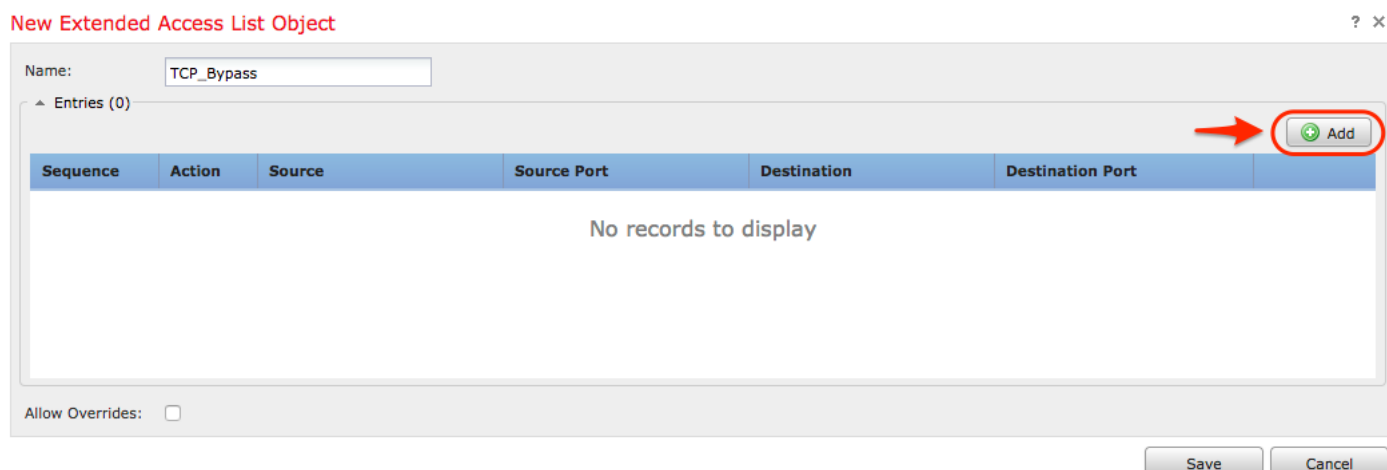
In questa sezione viene descritto come configurare TCP State Bypass in FMC tramite un criterio FlexConfig.

Passaggio 1. Configurare un oggetto elenco accessi esteso

Per creare un elenco degli accessi estesi in FMC, selezionare **Oggetti > Gestione oggetti** e nel menu di sinistra, in **Elenco accessi** selezionare **Esteso**. Fare clic su **Aggiungi elenco accessi esteso**.



Inserire nel campo Nome il valore desiderato. nell'esempio, il nome è **TCP_Bypass**. Fare clic sul pulsante **Aggiungi**.



L'azione per questa regola deve essere configurata come **Consenti**. È possibile utilizzare una rete definita dal sistema oppure creare un nuovo oggetto di rete per ogni origine e destinazione. Nell'esempio, l'elenco degli accessi corrisponde al traffico IP tra l'host 1 e l'host 2, in quanto questa è la comunicazione per applicare il bypass dello stato TCP. La scheda Porta può essere utilizzata facoltativamente per indicare una porta TCP o UDP specifica. Fare clic sul pulsante **Add** (Aggiungi) per continuare.

Add Extended Access List Entry

? x

Action: Allow

Logging: Default

Log Level: Informational

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

Dopo aver selezionato le reti o gli host di origine e di destinazione, fare clic su **Save** (Salva).

Edit Extended Access List Object

? x

Name:

Entries (1)

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

Allow Overrides:

Save Cancel

Passaggio 2. Configurare un oggetto FlexConfig

Selezionare **Oggetti > Gestione oggetti > FlexConfig > Oggetto FlexConfig** e fare clic sul pulsante **Aggiungi oggetto 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

Il nome dell'oggetto in questo esempio è **TCP_Bypass** come nell'elenco degli accessi. Non è necessario che questo nome corrisponda al nome dell'elenco degli accessi.

Selezionare **Inserisci oggetto criterio > Oggetto ACL esteso**.

Add FlexConfig Object ? x

Name:

Description:

Deployment: Everytime Type: Append

Insert Policy 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

Nota: Assicurarsi di scegliere l'opzione "Everytime". Ciò consente di mantenere la

configurazione durante altre distribuzioni e aggiornamenti.

Selezionare l'elenco degli accessi creato al passo 1 dalla sezione **Oggetti disponibili** e assegnare un nome alla variabile. Quindi fai clic sul pulsante **Aggiungi**. Nell'esempio, il nome della variabile è **TCP_Bypass**.

Fare clic su **Save** (Salva).

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 main sections. The left section, "Available Objects", has a search bar with "Search" text and a list containing one item, "TCP_Bypass", which is highlighted. The right section, "Selected Object", contains a list with one item, "TCP_Bypass". Between these two sections is an "Add" button. At the bottom right of the dialog are "Save" and "Cancel" buttons.

Aggiungere le righe di configurazione successive nel campo vuoto immediatamente sotto il pulsante **Insert** e includere la variabile precedentemente definita (**\$TCP_Bypass**) nella riga di configurazione *match access-list*. Si noti che al nome della variabile viene anteposto il simbolo **\$**. In questo modo è possibile definire che una variabile segua la sequenza.

```
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 questo esempio viene creata una mappa dei criteri che viene applicata all'interfaccia esterna. Se è necessario configurare il bypass dello stato TCP come parte dei criteri del servizio globale, è possibile applicare la mappa di classe tcp_bypass a global_policy.

Al termine, fare clic su **Save** (Salva).

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
```

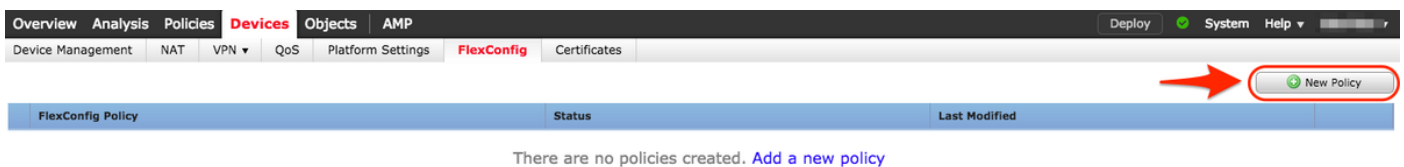
Variables

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

Save Cancel

Passaggio 3. Assegnare un criterio FlexConfig all'FTD

Andare su **Dispositivi > FlexConfig** e creare un nuovo criterio (a meno che non ne sia già stato creato uno per un altro scopo e assegnato allo stesso FTD). In questo esempio, il nuovo criterio FlexConfig è chiamato **TCP_Bypass**.



Assegnare il criterio **TCP_Bypass** FlexConfig al dispositivo FTD.

New Policy



Name:

Description:

Targeted Devices

Select devices to which you want to apply this policy.

Available Devices

FTD

Selected Devices

FTD

Selezionare l'oggetto FlexConfig denominato **TCP_Bypass** creato nel passaggio 2 nella sezione **Definito dall'utente** e fare clic sulla freccia per aggiungere l'oggetto al criterio.

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

Salvare le modifiche e distribuire

✓	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

Verifica

Accedere all'FTD tramite SSH o la console e usare il comando **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
!
```

Risoluzione dei problemi

Per risolvere i problemi relativi a questa funzionalità, questi comandi risultano utili.

- **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

Collegamenti correlati

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