

# Clarificar acciones de regla de política de control de acceso FTD

## Contenido

---

### [Introducción](#)

### [Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Productos Relacionados](#)

### [Antecedentes](#)

[Cómo se implementa la ACP](#)

### [Configurar](#)

[Acciones disponibles de la ACP](#)

[Cómo interactúan las políticas de prefiltro y la ACP](#)

[Acción de bloqueo de la ACP](#)

[Escenario 1. Descarte temprano de LINA](#)

[Situación hipotética 2. Descarte por veredicto de Snort](#)

[Bloqueo de la ACP con acción de restablecimiento](#)

[Acción de permiso de la ACP](#)

[Escenario 1. Acción de permiso de la ACP \(condiciones L3/L4\)](#)

[Situación hipotética 2. Acción de permiso de la ACP \(condiciones L3 a L7\)](#)

[Situación hipotética 3. Veredicto de avance rápido de Snort con permiso](#)

[Acción de confianza de la ACP](#)

[Escenario 1. Acción de confianza de la ACP](#)

[Situación hipotética 2. Acción de confianza de ACP \(sin SI, QoS y política de identidad\)](#)

[Acción de bloqueo de políticas de prefiltro](#)

[Acción Fastpath de política de prefiltro](#)

[Acción Fastpath de política de prefiltro \(conjunto en línea\)](#)

[Acción Fastpath de política de prefiltro \(conjunto en línea con conector\)](#)

[Acción de análisis de políticas de prefiltro](#)

[Escenario 1. Análisis de prefiltro con regla de bloqueo de la ACP](#)

[Situación hipotética 2. Análisis de prefiltro con regla de permiso de la ACP](#)

[Situación hipotética 3. Análisis de prefiltro con regla de confianza de ACP](#)

[Situación hipotética 4. Análisis de prefiltro con regla de confianza de ACP](#)

[Acción de monitoreo de la ACP](#)

[Acción de bloqueo interactivo de la ACP](#)

[Bloqueo interactivo de la ACP con acción de restablecimiento](#)

[Orificios y conexiones secundarias de FTD](#)

[Pautas de la regla de FTD](#)

### [Summary](#)

### [Información Relacionada](#)

---

# Introducción

Este documento describe las diferentes acciones disponibles en la política de prefiltrado y la política de control de acceso (ACP) de Firepower Threat Defense (FTD).

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Descarga de flujo
- Capturas de paquetes en appliances Firepower Threat Defence
- Packet Tracer y captura con opción de rastreo en dispositivos FTD

### Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Firepower 4110 Threat Defense versión 6.4.0 (compilación 113) y 6.6.0 (compilación 90)
- Centro de administración Firepower (FMC) versión 6.4.0 (compilación 113) y 6.6.0 (compilación 90)


La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

### Productos Relacionados

Este documento también puede utilizarse con estas versiones de software y hardware:

- ASA5506-X, ASA5506W-X, ASA5506H-X, ASA5508-X, ASA5516-X
- ASA5512-X, ASA5515-X, ASA5525-X, ASA5545-X, ASA5555-X
- FPR1000, FPR2100, FPR4100, FPR9300
- VMware (ESXi), Amazon Web Services (AWS), máquina virtual basada en kernel (KVM)
- Módulo de router del router de servicios integrados (ISR)
- Software FTD versión 6.1.x y posteriores

---

 Nota: La descarga de flujo solo se admite en instancias nativas de las aplicaciones ASA y FTD y en las plataformas FPR4100 y FPR9300. Las instancias de contenedor de FTD no admiten la descarga de flujo.

---

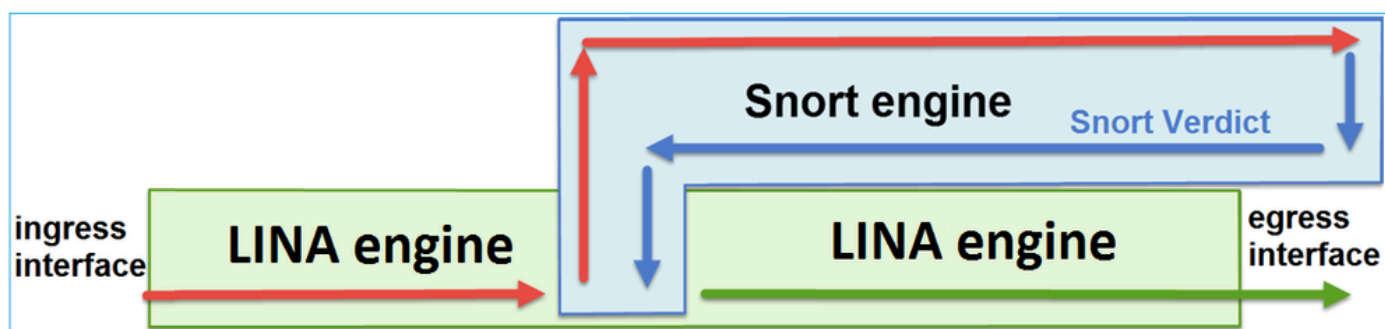
## Antecedentes

Se examina la operación en segundo plano de cada acción junto con su interacción con otras funciones como la descarga de flujo y los protocolos que abren conexiones secundarias.

FTD es una imagen de software unificada que consta de 2 motores principales:

- Motor LINA
- Motor Snort

Esta figura muestra cómo interactúan los 2 motores:



- Un paquete ingresa a la interfaz de ingreso y es manejado por el motor LINA.
- Si lo requiere la política de FTD, el paquete es inspeccionado por el motor Snort.
- El motor Snort devuelve un veredicto (lista de permisos o lista de bloqueo) para el paquete.
- El motor LINA descarta o reenvía el paquete según el veredicto de Snort.

## Cómo se implementa la ACP

La política de FTD se configura en el FMC cuando se usa la administración externa (remota) o en el administrador de dispositivos Firepower (FDM) cuando se usa la administración local. En ambos casos, la ACP se implementa como:

- Una lista de control de acceso (ACL) global denominada CSM\_FW\_ACL\_ para el motor FTD LINA
- Reglas de control de acceso (AC) en el archivo `/ngfw/var/sf/detection_engines/<UUID>/ngfw.rules` para el motor Snort de FTD

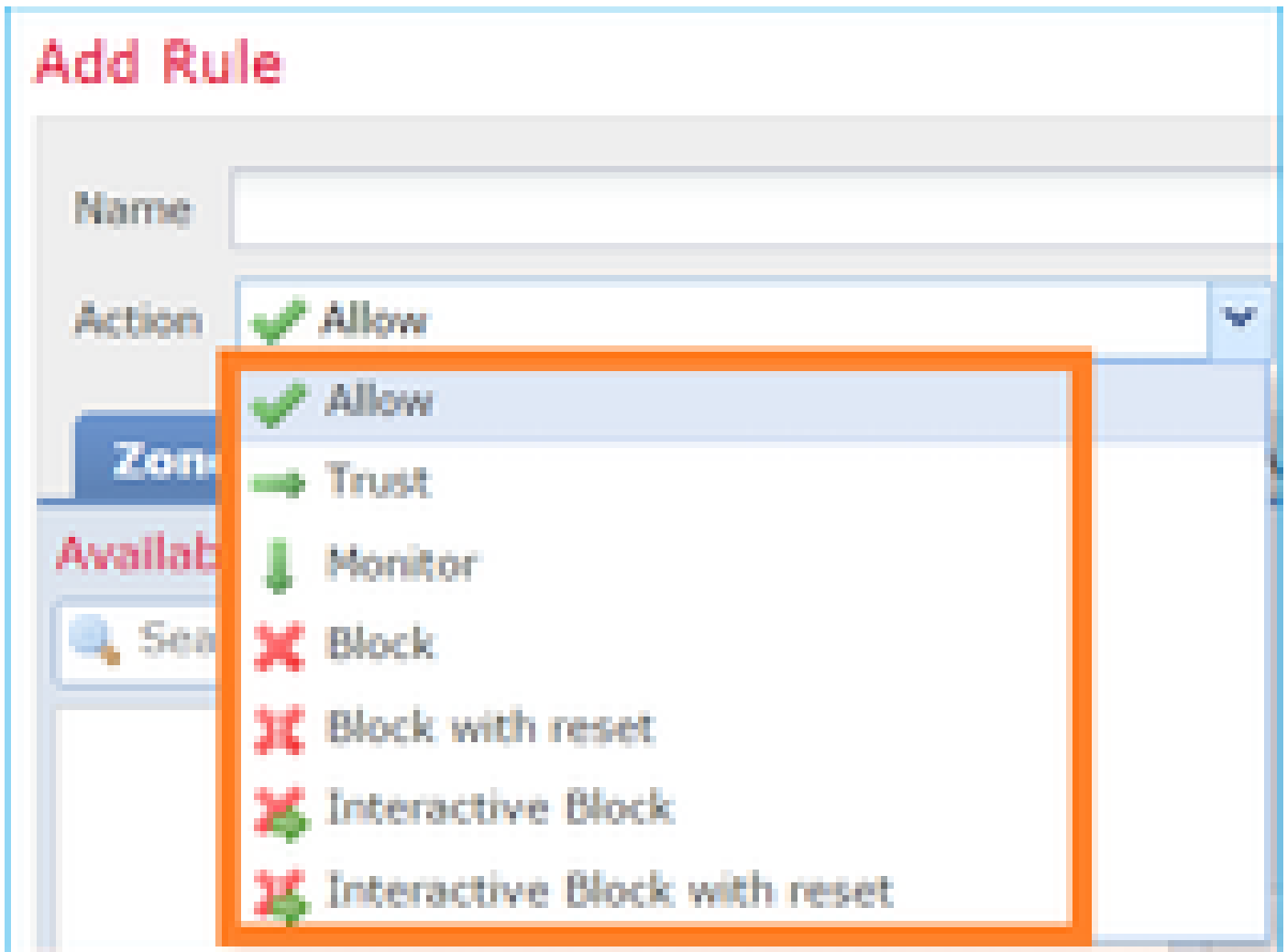
## Configurar

### Acciones disponibles de la ACP

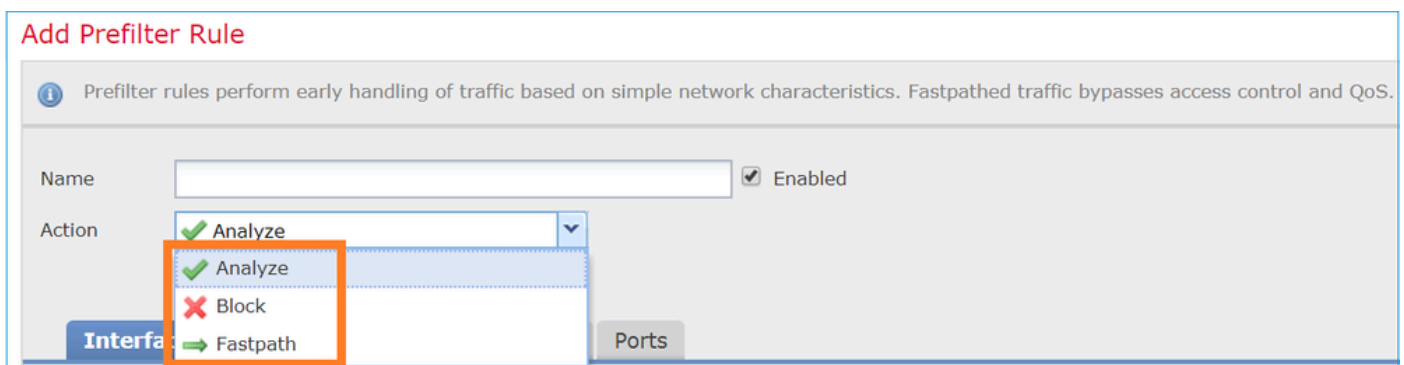
La ACP de FTD contiene una o más reglas y cada regla puede tener una de estas acciones, como se muestra en la imagen:

- Permiso
- Confianza
- Monitor

- Bloqueo
- Bloqueo con restablecimiento
- Bloqueo interactivo
- Bloqueo interactivo con restablecimiento



De manera similar, una política de prefiltro puede contener una o más reglas y las acciones posibles se muestran en la imagen:



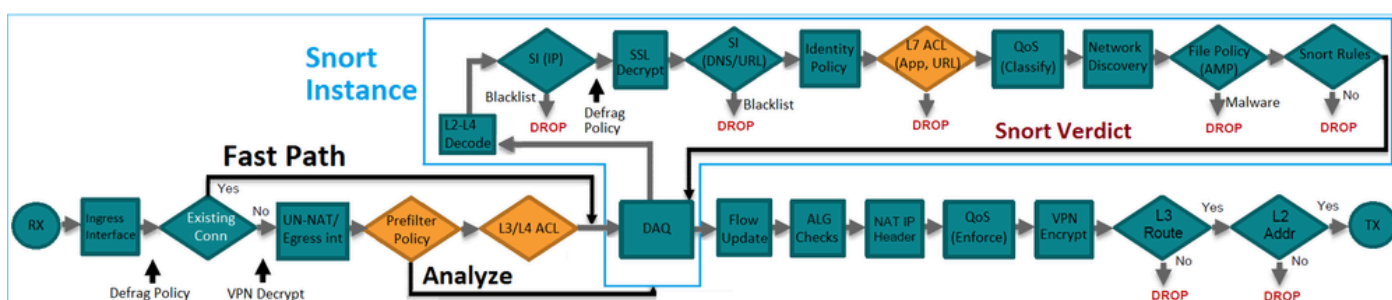
Cómo interactúan las políticas de prefiltro y la ACP

La política de prefiltro se introdujo en la versión 6.1 y tiene dos objetivos principales:

1. Permite la inspección del tráfico tunelizado donde el motor LINA de FTD verifica el encabezado IP externo mientras que el motor Snort verifica el encabezado IP interno. Más específicamente, en el caso del tráfico tunelizado (por ejemplo GRE), las reglas en la Política de Prefiltro siempre actúan sobre los encabezados externos, mientras que las reglas en el ACP siempre se aplican a las sesiones internas (encabezados internos). El tráfico tunelizado se refiere a estos protocolos:

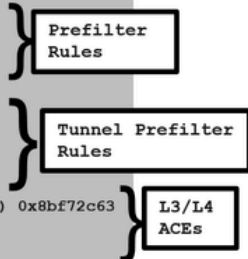
- GRE
- IP en IP
- IPv6 en IP
- Puerto Teredo 3544

2. Proporciona control de acceso temprano (EAC) que permite que el flujo omita por completo el motor Snort como se muestra en la imagen.



Las reglas de prefiltrado se implementan en FTD como elementos de control de acceso (ACE) L3/L4 y preceden a las ACE L3/L4 configuradas, como se muestra en la imagen:

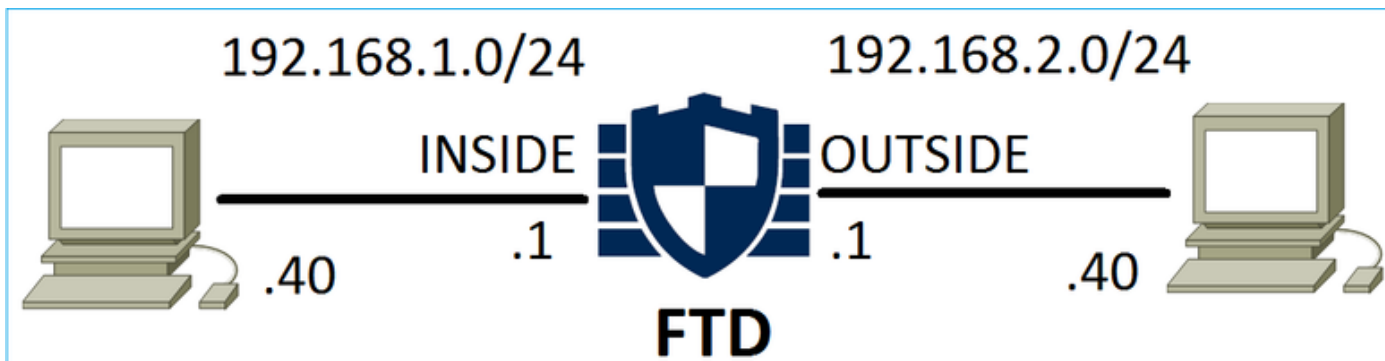
```
firepower# show access-list
access-list CSM_FW_ACL_ line 1 remark rule-id 268434457: PREFILTER POLICY: FTD_Prefilter_Policy
access-list CSM_FW_ACL_ line 2 remark rule-id 268434457: RULE: Fastpath_Rule1
access-list CSM_FW_ACL_ line 3 advanced trust ip host 192.168.75.16 any rule-id 268434457 event-log both (hitcnt=0)
access-list CSM_FW_ACL_ line 4 remark rule-id 268434456: PREFILTER POLICY: FTD_Prefilter_Policy
access-list CSM_FW_ACL_ line 5 remark rule-id 268434456: RULE: DEFAULT TUNNEL ACTION RULE
access-list CSM_FW_ACL_ line 6 advanced permit ipipip any any rule-id 268434456 (hitcnt=0) 0xf5b597d6
access-list CSM_FW_ACL_ line 7 advanced permit 41 any any rule-id 268434456 (hitcnt=0) 0x06095aba
access-list CSM_FW_ACL_ line 8 advanced permit gre any any rule-id 268434456 (hitcnt=2) 0x52c7a066
access-list CSM_FW_ACL_ line 9 advanced permit udp any any eq 3544 rule-id 268434456 (hitcnt=0) 0xcf6309bc
access-list CSM_FW_ACL_ line 10 remark rule-id 268434445: ACCESS POLICY: FTD5506-1 - Mandatory/1
access-list CSM_FW_ACL_ line 12 advanced deny ip host 10.1.1.1 any rule-id 268434445 event-log flow-start (hitcnt=0) 0x8bf72c63
access-list CSM_FW_ACL_ line 14 remark rule-id 268434434: L4 RULE: DEFAULT ACTION RULE
access-list CSM_FW_ACL_ line 15 advanced permit ip any any rule-id 268434434 (hitcnt=410) 0xald3780e
```



Nota: Prefiltrar v/s reglas ACP = se aplica la primera coincidencia.

## Acción de bloqueo de la ACP

Considere la topología que se muestra en esta imagen:



Escenario 1. Descarte temprano de LINA

La ACP contiene una regla de bloqueo que utiliza la condición L4 (puerto de destino TCP 80), como se muestra en la imagen:

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN	Users	Applica...	Source ...	Dest Ports	URLs	ISE/SGT Attribu...	Action
Mandatory - ACP1 (1-1)													
1	Rule1	Any	Any	192.168.1.40	192.168.2.40	Any	Any	Any	Any	TCP (6):80	Any	Any	Block

La política implementada en Snort:

```
<#root>
268435461
deny
  any 192.168.1.40 32 any any 192.168.2.40 32 80 any 6
```

La política implementada en LINA. Tenga en cuenta que la regla se aplica como deny acción:

```
<#root>
firepower#
show access-list
...
access-list CSM_FW_ACL_ line 9 remark rule-id 268435461: L4 RULE: Rule1
access-list CSM_FW_ACL_ line 10 advanced
deny
  tcp host 192.168.1.40 host 192.168.2.40 eq www rule-id 268435461 event-log flow-start (hitcnt=0) 0x614
```

### Verifique el comportamiento:

Cuando el host-A (192.168.1.40) intenta abrir una sesión HTTP para el host-B (192.168.2.40), el motor LINA de FTD descarta los paquetes de sincronización TCP (SYN) y no llegan al motor Snort ni al destino:

```
<#root>
```

```
firepower#
```

```
show capture
```

```
capture CAPI type raw-data buffer 33554432 trace trace-count 100 interface
```

```
INSIDE
```

```
[Capturing -
```

```
430 bytes
```

```
]
  match ip host 192.168.1.40 any
capture CAPO type raw-data buffer 33554432 trace trace-count 100 interface
```

```
OUTSIDE
```

```
[Capturing -
```

```
0 bytes
```

```
]
  match ip host 192.168.1.40 any
```

```
<#root>
```

```
firepower#
```

```
show capture CAPI
```

```
1: 11:08:09.672801 192.168.1.40.32789 > 192.168.2.40.80: S 3249160620:3249160620(0) win 2920 <mss 1460, sackOK, timestamp 4060517 0>
2: 11:08:12.672435 192.168.1.40.32789 > 192.168.2.40.80: S 3249160620:3249160620(0) win 2920 <mss 1460, sackOK, timestamp 4060517 0>
3: 11:08:18.672847 192.168.1.40.32789 > 192.168.2.40.80: S 3249160620:3249160620(0) win 2920 <mss 1460, sackOK, timestamp 4060517 0>
4: 11:08:30.673610 192.168.1.40.32789 > 192.168.2.40.80: S 3249160620:3249160620(0) win 2920 <mss 1460, sackOK, timestamp 4060517 0>
```

```
<#root>
```

```
firepower#
```

```
show capture CAPI packet-number 1 trace
```

```
1: 11:08:09.672801 192.168.1.40.32789 > 192.168.2.40.80:
```

```
S
3249160620:3249160620(0) win 2920 <mss 1460,sackOK,timestamp 4060517 0>
...
```

```
Phase: 4
```

Type: ACCESS-LIST

Subtype: log

Result: DROP

Config:

```
access-group CSM_FW_ACL_ global
```

```
access-list CSM_FW_ACL_ advanced deny tcp host 192.168.1.40 host 192.168.2.40 eq www rule-id 268435461
```

```
access-list CSM_FW_ACL_ remark rule-id 268435461: ACCESS POLICY: ACP1 - Mandatory
```

```
access-list CSM_FW_ACL_ remark rule-id 268435461: L4 RULE: Rule1
```

Additional Information:

<- No Additional Information = No Snort Inspection

Result:

input-interface: INSIDE

input-status: up

input-line-status: up

output-interface: OUTSIDE

output-status: up

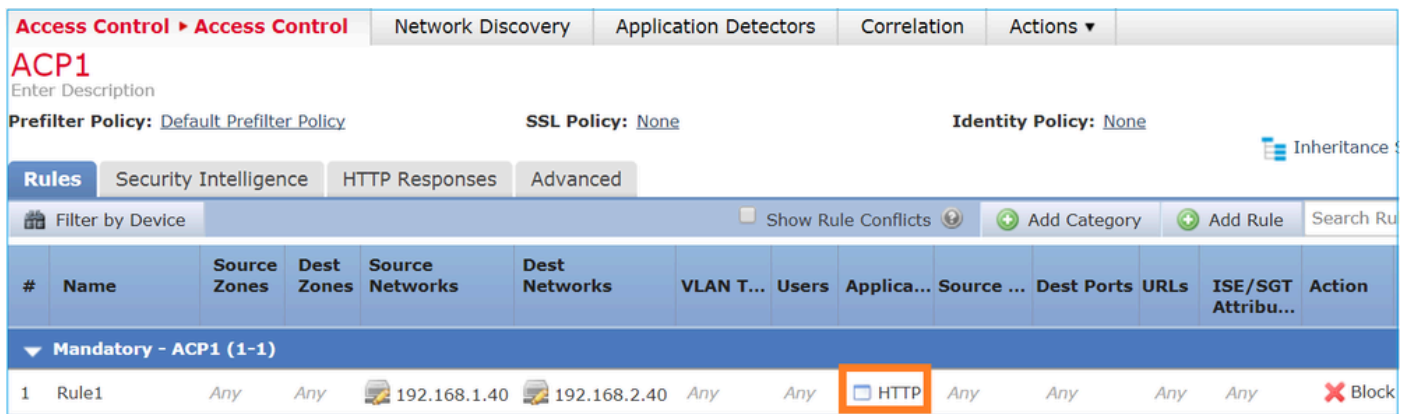
output-line-status: up

Action: drop

Drop-reason: (acl-drop) Flow is denied by configured rule

Situación hipotética 2. Descarte por veredicto de Snort

La ACP contiene una regla de bloqueo que utiliza la condición L7 (HTTP de la aplicación), como se muestra en la imagen:



The screenshot shows the Cisco ISE configuration interface for an Access Control Policy (ACP1). The rule configuration is as follows:

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN T...	Users	Applica...	Source ...	Dest Ports	URLs	ISE/SGT Attribu...	Action
1	Rule1	Any	Any	192.168.1.40	192.168.2.40	Any	Any	HTTP	Any	Any	Any	Any	Block

La política implementada en Snort:

```
<#root>
```

```
268435461
```

```
deny
```

```
any 192.168.1.40 32 any any 192.168.2.40 32 any any any
```


```
(appid 676:1)
```



Appid 676:1 = HTTP

La política implementada en LINA.

---

 **Nota:** La regla se envía como una **permit** acción porque LINA no puede determinar que la sesión utilice HTTP. En FTD, el mecanismo de detección de aplicaciones se encuentra en el motor Snort.

---

```
<#root>
```


```
firepower#
```

```
show access-list
```

```
... access-list CSM_FW_ACL_ line 9 remark rule-id 268435461: L7 RULE: Rule1 access-list CSM_FW_ACL_ line
permit
ip host 192.168.1.40 host 192.168.2.40 rule-id 268435461 (hitcnt=0) 0xb788b786
```

Para una regla de bloqueo que utiliza **Application** como condición, el seguimiento de un paquete real muestra que LINA descarta la sesión debido al veredicto del motor Snort.

---

 **Nota:** Para que el motor Snort determine la aplicación, debe inspeccionar algunos paquetes (generalmente 3-10, que depende del decodificador de la aplicación). Por lo tanto, se permiten algunos paquetes a través de FTD que llegan al destino. Los paquetes permitidos siguen sujetos a la comprobación de directiva de intrusiones basada en la **Access Policy > Advanced > Intrusion Policy used before Access Control rule is determined** opción.

---

#### Verifique el comportamiento:

Cuando el host A (192.168.1.40) intenta establecer una sesión HTTP con el host B (192.168.2.40), la captura de ingreso de LINA muestra lo siguiente:

```
<#root>
```

```
firepower#
```

```
show capture CAPI
```

```
8 packets captured
```

```
1: 11:31:19.825564 192.168.1.40.32790 > 192.168.2.40.80:
```

```
S
```

```
357753151:357753151(0) win 2920 <mss 1460,sackOK,timestamp 5450579 0> 2: 11:31:19.826403 192.168.2.40.
```

```
S
```

```
1283931030:1283931030(0)
```

ack

```
357753152 win 2896 <mss 1380,sackOK,timestamp 5449236 5450579> 3: 11:31:19.826556 192.168.1.40.32790 >
```

ack

```
1283931031 win 2920 <nop,nop,timestamp 5450580 5449236> 4: 11:31:20.026899 192.168.1.40.32790 > 192.168.2.40.80
```

La captura de salida:

<#root>

firepower#

show capture CAPO

5 packets captured

```
1: 11:31:19.825869 192.168.1.40.32790 > 192.168.2.40.80: S 1163713179:1163713179(0) win 2920 <mss 1380
```

El seguimiento muestra que el primer paquete (TCP SYN) está permitido por el Snort, ya que el veredicto de Application Detection aún no se ha alcanzado:

<#root>

firepower#

show capture CAPI packet-number 1 trace

```
1: 11:31:19.825564 192.168.1.40.32790 > 192.168.2.40.80:
```

S

```
357753151:357753151(0) win 2920 <mss 1460,sackOK,timestamp 5450579 0> ... Phase: 4 Type: ACCESS-LIST S
```

Additional Information: This packet will be sent to snort for additional processing where a verdict will

```
... Phase: 10 Type: FLOW-CREATION Subtype: Result: ALLOW Config: Additional Information:
```

New flow created with id 23194

, packet dispatched to next module ... Phase: 12 Type: SNORT Subtype: Result: ALLOW Config: Additional In

pending rule-matching, id 268435461, pending AppID

```
NAP id 1, IPS id 0,
```

Verdict PASS

Snort Verdict: (pass-packet) allow this packet

```
Result: input-interface: OUTSIDE input-status: up input-line-status: up output-interface: OUTSIDE outp
```

Action: allow

Lo mismo ocurre con el paquete ACK/SYN de TCP:

<#root>

firepower#

show capture CAPO packet-number 2 trace

2: 11:31:19.826312 192.168.2.40.80 > 192.168.1.40.32790:

S

354801457:354801457(0)

ack

1163713180 win 2896 <mss 1460,sackOK,timestamp 5449236 5450579> ... Phase: 3 Type: FLOW-LOOKUP Subtype: I

Found flow with id 23194, using existing flow

... Phase: 5 Type: SNORT Subtype: Result: ALLOW Config: Additional Information: Snort Trace: Packet: TCP

Firewall: pending rule-matching, id 268435461, pending AppID

NAP id 1, IPS id 0,

Verdict PASS

Snort Verdict: (pass-packet) allow this packet

Result: input-interface: INSIDE input-status: up input-line-status: up output-interface: INSIDE output

Action: allow

Snort devuelve un veredicto DROP una vez que se completa una inspección del tercer paquete:

<#root>

firepower#

show capture CAPI packet-number 3 trace

3: 11:31:19.826556 192.168.1.40.32790 > 192.168.2.40.80: P 357753152:357753351(199)

ack

1283931031 win 2920 <nop,nop,timestamp 5450580 5449236> Phase: 3 Type: FLOW-LOOKUP Subtype: Result: AL

Found flow with id 23194, using existing flow

Phase: 5 Type: SNORT Subtype:

Result: DROP

Config: Additional Information: Snort Trace: Packet: TCP, ACK, seq 357753152, ack 1283931031

AppID: service HTTP (676)

, application unknown (0) Firewall: starting rule matching, zone -1 -> -1, geo 0(0) -> 0, vlan 0, sgt 6

Firewall: block rule, id 268435461, drop

```
Snort: processed decoder alerts or actions queue, drop NAP id 1, IPS id 0,  
Verdict BLOCKLIST, Blocked by Firewall
```

```
Snort Verdict: (block-list) block list this flow
```

```
Result: input-interface: INSIDE input-status: up input-line-status: up Action: drop
```

```
Drop-reason: (firewall) Blocked by the firewall preprocessor
```

También puede ejecutar el comando **system support trace** desde el modo CLISH de FTD. Esta herramienta proporciona 2 funciones:

- Muestra el veredicto de Snort para cada paquete cuando se envía a la biblioteca de adquisición de datos (DAQ) y se ve en LINA. La DAQ es un componente ubicado entre el motor LINA y el motor Snort de FTD.
- Permite ejecutar `system support firewall-engine-debug` al mismo tiempo para ver qué sucede dentro del propio motor Snort.

Aquí se muestra el resultado:

```
<#root>
```

```
>
```

```
system support trace
```

```
Please specify an IP protocol:
```

```
tcp
```

```
Please specify a client IP address:
```

```
192.168.1.40
```

```
Please specify a client port: Please specify a server IP address:
```

```
192.168.2.40
```

```
Please specify a server port: Enable firewall-engine-debug too? [n]:
```

```
y
```

```
Monitoring packet tracer debug messages Tracing enabled by Lina 192.168.2.40-80 - 192.168.1.40-32791 6  
TCP, SYN
```

```
, seq 2620409313 192.168.2.40-80 - 192.168.1.40-32791 6 AppID: service unknown (0), application unknown  
pending rule-matching, 'Rule1', pending AppID
```

```
192.168.1.40-32791 > 192.168.2.40-80 6 NAP id 1, IPS id 0,
```

```
Verdict PASS
```

```
Trace buffer and verdict reason are sent to DAQ's PDTS Tracing enabled by Lina 192.168.2.40-80 - 192.1  
TCP, SYN, ACK
```

```
, seq 3700371680, ack 2620409314 192.168.2.40-80 - 192.168.1.40-32791 6 AppID: service unknown (0), app
```

pending rule-matching, 'Rule1', pending AppID

192.168.1.40-32791 > 192.168.2.40-80 6 NAP id 1, IPS id 0,

Verdict PASS

Trace buffer and verdict reason are sent to DAQ's PDS Tracing enabled by Lina 192.168.2.40-80 - 192.1

TCP, ACK

, seq 2620409314, ack 3700371681 192.168.2.40-80 - 192.168.1.40-32791 6 AppID:

service HTTP (676)

, application unknown (0) 192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 Starting with minimum 2, 'Ru

url http://192.168.2.40/128k.html

192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0

match rule order 2, 'Rule1', action Block

192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 deny action 192.168.1.40-32791 > 192.168.2.40-80 6

Firewall: block rule, 'Rule1', drop

192.168.1.40-32791 > 192.168.2.40-80 6 Snort: processed decoder alerts or actions queue, drop 192.168.

Verdict BLOCKLIST

192.168.1.40-32791 > 192.168.2.40-80 6 ==>

Blocked by Firewall

### Summary

- La acción de bloqueo de la ACP se implementa como regla de permiso o denegación en LINA, que depende de las condiciones de la regla.
- Si las condiciones son L3/L4, LINA bloquea el paquete. En el caso de TCP, se bloquea el primer paquete (TCP SYN)
- Si las condiciones son L7, el paquete se reenvía al motor Snort para su posterior inspección. En el caso de TCP, se permiten algunos paquetes a través de FTD hasta que Snort llega a un veredicto. Los paquetes permitidos siguen sujetos a la verificación de la política de intrusiones basada en la opción **Política de acceso > Avanzada > Política de intrusiones utilizada antes de que se determine la regla de control de acceso.**

### Bloqueo de la ACP con acción de restablecimiento

Una regla de bloqueo con restablecimiento configurada en la interfaz de usuario de FMC:

Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applic...	Source Ports	Dest Ports	URLs	Source SGT	Dest SGT	Action							
▼ Mandatory - ACP1 (1-4)																				
1	Block-RST-Rule1	Any	Any	192.168.10.0/24	192.168.11.50	Any	Any	Any	Any	TCP (6):80	Any	Any	Any	Block with reset					0	
2	Block-RST_Rule2	Any	Any	192.168.10.0/24	192.168.11.51	Any	Any	HTTP	Any	Any	Any	Any	Any	Block with reset					0	

El bloque con regla de restablecimiento se implementa en el motor FTD LINA como **permit** y en el motor Snort como **reset** regla:

```
<#root>
```

```
firepower#
```

```
show access-list
```

```
... access-list CSM_FW_ACL_ line 10 advanced
```

```
permit
```

```
tcp 192.168.10.0 255.255.255.0 host 192.168.11.50 eq www rule-id 268438864 (hitcnt=0) 0xba785fc0 acces
```

```
permit
```

```
ip 192.168.10.0 255.255.255.0 host 192.168.11.51 rule-id 268438865 (hitcnt=0) 0x622350d0
```

Motor Snort:

```
<#root>
```

```
admin@firepower:~$
```

```
cat /var/sf/detection_engines/9e080e5c-adc3-11ea-9d37-44884cf7e9ba/ngfw.rules
```

```
... # Start of AC rule. 268438864
```

```
reset
```

```
any 192.168.10.0 24 any any 192.168.11.50 32 80 any 6 # End rule 268438864 268438865
```

```
reset
```

```
any 192.168.10.0 24 any any 192.168.11.51 32 any any any (appid 676:1) (ip_protos 6, 17) # End rule 26
```

Cuando un paquete coincide con un bloque con una regla de restablecimiento, FTD envía un **TCP Reset** paquete o un mensaje de **ICMP Type 3 Code 13** destino inalcanzable (filtrado administrativo):

```
<#root>
```

```
root@kali:~/tests#
```

```
wget 192.168.11.50/file1.zip
```

```
--2020-06-20 22:48:10-- http://192.168.11.50/file1.zip Connecting to 192.168.11.50:80... failed:
```

```
Connection refused.
```

Aquí hay una captura tomada en la interfaz de ingreso de FTD:

```
firepower# show capture CAPI
2 packets captured
1: 21:01:00.977259 802.1Q vlan#202 P0 192.168.10.50.41986 > 192.168.11.50.80: S 3120295488:3120295488(0) win 29200 <mss 1460,sackOK,timestan
2: 21:01:00.978114 802.1Q vlan#202 P0 192.168.11.50.80 > 192.168.10.50.41986: R 0:0(0) ack 3120295489 win 0 2 packets shown
```

**System support trace** , en este caso, muestra que el paquete se descarta debido al veredicto de Snort:

```
<#root>
```

```
>
```

```
system support trace
```

```
Enable firewall-engine-debug too? [n]:
```

```
y
```

```
Please specify an IP protocol: tcp Please specify a client IP address:
```

```
192.168.10.50
```

```
Please specify a client port: Please specify a server IP address:
```

```
192.168.11.50
```

```
Please specify a server port: Monitoring packet tracer and firewall debug messages 192.168.10.50-41984
```

```
Session: new snort session
```

```
192.168.10.50-41984 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service unknown (0), application unknown
```

```
new firewall session
```

```
192.168.10.50-41984 > 192.168.11.50-80 6 AS 1-1 I 9 using HW or preset rule order 2, 'Block-RST-Rule1'
```

```
reset action
```

```
192.168.10.50-41984 > 192.168.11.50-80 6 AS 1-1 I 9 deleting firewall session flags = 0x0, fwFlags = 0
```

```
Firewall: block w/ reset rule, 'Block-RST-Rule1', drop
```

```
192.168.10.50-41984 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort: processed decoder alerts or actions queue
```

```
Verdict BLOCKLIST
```

```
192.168.10.50-41984 - 192.168.11.50-80 6 AS 1-1 CID 0 ==>
```

```
Blocked by Firewall
```

```
Verdict reason is sent to DAQ
```

## Casos de uso

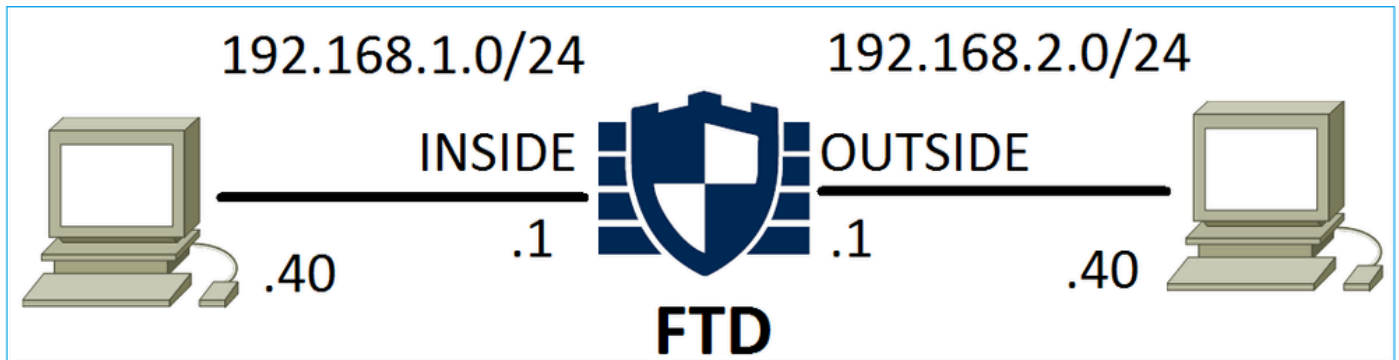
Igual que **Block** action, pero finaliza inmediatamente la conexión.

Acción de permiso de la ACP

Escenario 1. Acción de permiso de la ACP (condiciones L3/L4)

Normalmente, configuraría una regla de permiso para especificar inspecciones adicionales, como una política de intrusiones o una política de archivos. Este primer escenario demuestra el funcionamiento de una regla de permiso cuando se aplica una condición L3/L4.

Considere esta topología como se muestra en la imagen:



Esta política se aplica como se muestra en la imagen:

Access Control > Access Control

Network Discovery Application Detectors Correlation Actions

### ACP1

Enter Description

Prefilter Policy: [Default Prefilter Policy](#) SSL Policy: [None](#) Identity Policy: [None](#)

Inheritance Settings

Rules Security Intelligence HTTP Responses Advanced

Filter by Device Show Rule Conflicts Add Category Add Rule Search Rules

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN T...	Users	Applica...	Source ...	Dest Ports	URLs	ISE/SGT Attribu...	Action
Mandatory - ACP1 (1-1)													
1	Rule1	Any	Any	192.168.1.40	192.168.2.40	Any	Any	Any	Any	TCP (6):80	Any	Any	Allow

La política implementada en Snort. Tenga en cuenta que la regla se implementa como una **allow** acción:

```
<#root>
# Start of AC rule. 268435461
allow
  any 192.168.1.40 32 any any 192.168.2.40 32 80 any 6
```

La política en LINA.

 **Nota:** la regla se implementa como una **permit** acción que básicamente significa redirección a Snort para una inspección adicional.

```
<#root>
firepower#
```



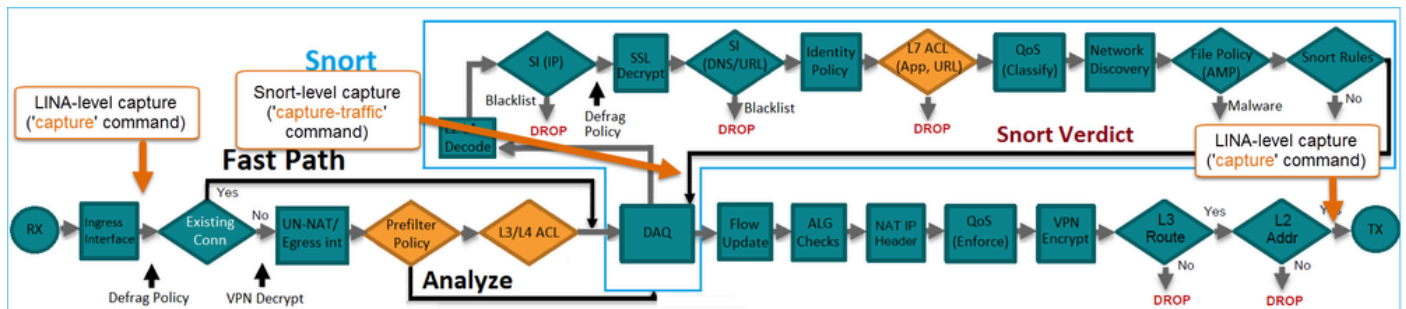
```
show access-list
```

```
... access-list CSM_FW_ACL_ line 9 remark rule-id 268435461: L7 RULE: Rule1 access-list CSM_FW_ACL_ line
permit
tcp host 192.168.1.40 host 192.168.2.40 eq www rule-id 268435461 (hitcnt=1) 0x641a20c3
```

Para ver cómo FTD maneja un flujo que coincide con una regla **Allow** hay algunas maneras:

- Verificación de las estadísticas de Snort.
- Con el uso del soporte del sistema, rastreo de la herramienta CLISH.
- Con el uso de la captura con la opción de rastreo en LINA y, opcionalmente, con el tráfico de captura en el motor Snort.

Captura de LINA frente al tráfico de captura de Snort:



Verifique el comportamiento:

Borre las estadísticas de Snort, active **system support trace** from CLISH, and initiate an HTTP flow from host-A (192.168.1.40) to host-B (192.168.2.40). All the packets are forwarded to the Snort engine and get the PASS verdict by the Snort:

```
<#root>
```

```
firepower#
```

```
clear snort statistics
```

```
<#root>
```

```
>
```

```
system support trace
```

```
Please specify an IP protocol: Please specify a client IP address:
```

```
192.168.1.40
```

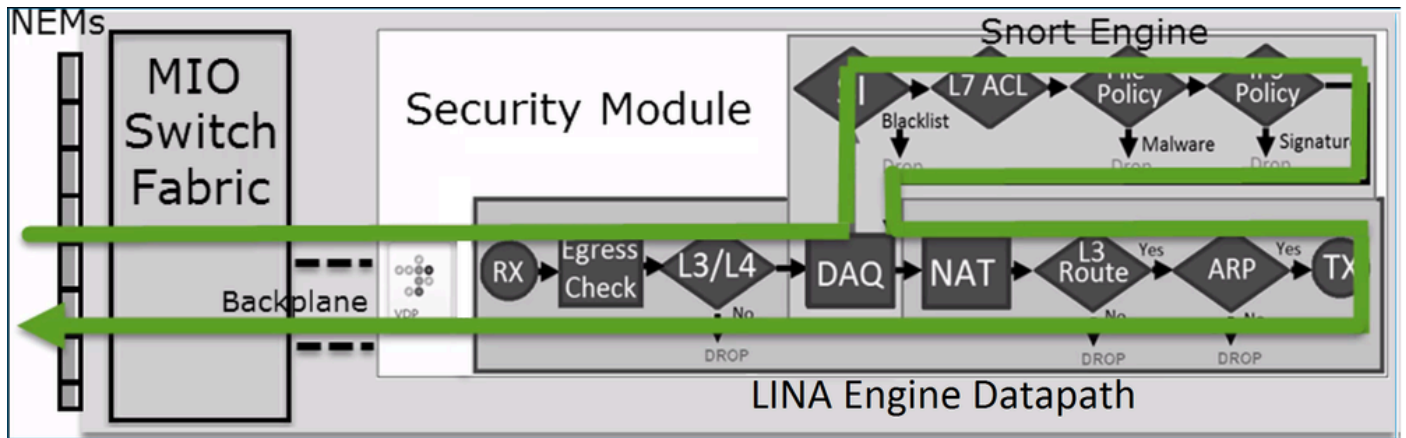
```
Please specify a client port: Please specify a server IP address:
```

```
192.168.2.40
```



## Summary

Para resumir, así es como se administra un flujo mediante FTD implementado en FP4100/9300 cuando una regla de permiso coincide, como se muestra en la imagen:



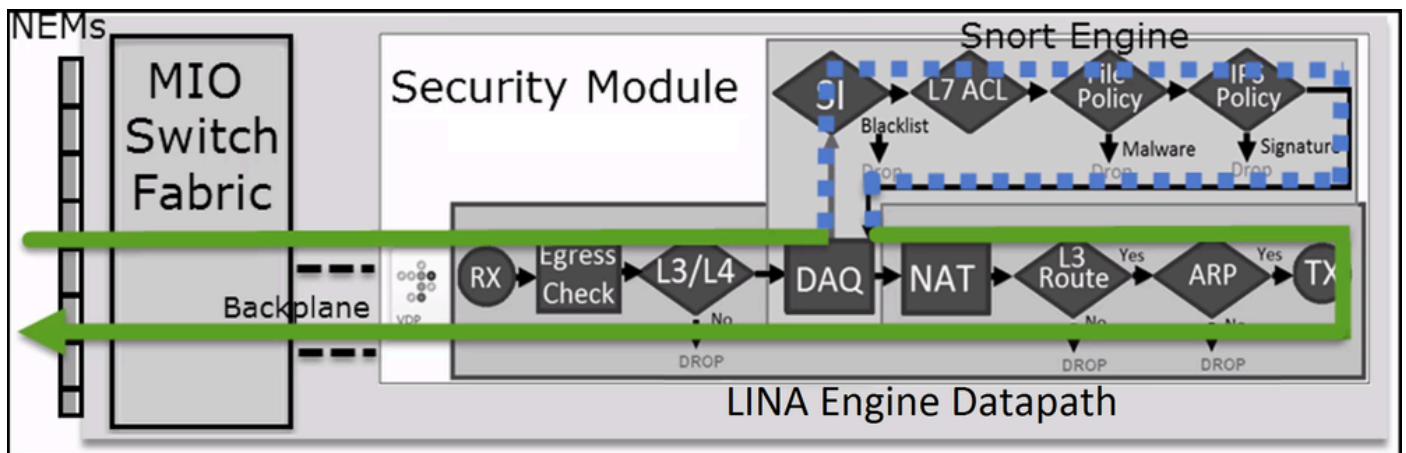
**Nota:** Management Input Output (MIO) es el motor supervisor del chasis FirePOWER.

Situación hipotética 3. Veredicto de avance rápido de Snort con permiso

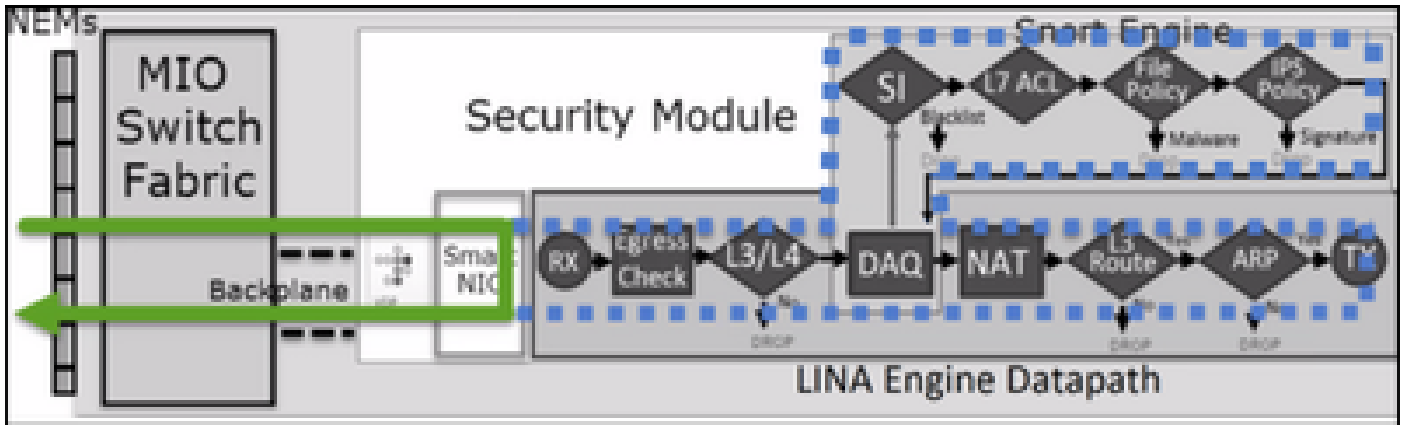
Hay escenarios específicos donde el motor FTD Snort da un veredicto PERMITLIST (avance rápido) y el resto del flujo se descarga al motor LINA (en algunos casos se descarga al acelerador de hardware - SmartNIC). Estos incluyen:

- Tráfico SSL sin política de SSL configurada
- Desvío de aplicaciones inteligente (IAB)

Esta es la representación visual de la trayectoria del paquete:



O en algunos casos:



### Puntos principales

- La regla de permiso se implementa como **permiso en Snort y autorización en LINA**.
- En la mayoría de los casos, todos los paquetes de una sesión se reenvían al motor Snort para una inspección adicional

### Casos de uso

Debería configurar una regla de permiso cuando necesite una inspección de L7 por parte del motor Snort, por ejemplo:

- Política de intrusiones
- Política de archivos

### Acción de confianza de la ACP

#### Escenario 1. Acción de confianza de la ACP

Si no desea aplicar la inspección L7 avanzada en el nivel Snort (por ejemplo, política de intrusiones, política de archivos, detección de red), pero aún desea utilizar funciones como inteligencia de seguridad (SI), política de identidad, QoS, etc., se recomienda utilizar la acción Confiar en la regla.

### Topología:




La política configurada:

Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applic...	Source Ports	Dest Ports	URLs	Source SGT	Dest SGT	Action
▼ Mandatory - ACP1 (1-4)													
1	trust_L3-L4	Any	Any	192.168.10.50 192.168.10.51	192.168.11.50 192.168.11.51	Any	Any	Any	Any	TCP (6):80	Any	Any	Trust

La regla de confianza tal como se implementa en el motor Snort de FTD:

```
<#root>
# Start of AC rule. 268438858
fastpath
  any 192.168.10.50 31 any any 192.168.11.50 31
80
any
6
(log dcforward flowend)
```

---

 **Nota:** El número 6 es el protocolo (TCP).

---

La regla en LINA de FTD:

```
<#root>
firepower#
show access-list | i 268438858
  access-list CSM_FW_ACL_ line 17 remark rule-id 268438858: ACCESS POLICY: ACP1 - Mandatory access-list C
permit
  tcp host 192.168.10.50 host 192.168.11.50 eq www rule-id 268438858 (hitcnt=19) 0x9d442895 access-list C
permit
  tcp host 192.168.10.50 host 192.168.11.51 eq www rule-id 268438858 (hitcnt=0) 0xd026252b access-list C
permit
  tcp host 192.168.10.51 host 192.168.11.50 eq www rule-id 268438858 (hitcnt=0) 0x0d785cc4 access-list C
permit
  tcp host 192.168.10.51 host 192.168.11.51 eq www rule-id 268438858 (hitcnt=0) 0x3b3234f1
```

## Verificación:

Habilite **system support trace** e inicie una sesión HTTP desde el host-A (192.168.10.50) al host-B (192.168.11.50). Hay 3 paquetes reenviados al motor Snort. El motor Snort envía a LINA el veredicto PERMITLIST que, básicamente, descarga el resto del flujo al motor LINA:

```
<#root>
```

```
>
```

```
system support trace
```

```
Enable firewall-engine-debug too? [n]:
```

```
y
```

```
Please specify an IP protocol:
```

```
tcp Please
```

```
specify a client IP address:
```

```
192.168.10.50
```

```
Please specify a client port: Please specify a server IP address:
```

```
192.168.11.50
```

```
Please specify a server port:
```

```
80
```

```
Monitoring packet tracer and firewall debug messages 192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 C
```

```
TCP, SYN
```

```
, seq 453426648 192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Session: new snort session 192.16
```

```
Verdict PASS
```

```
192.168.11.50-80 - 192.168.10.50-42126 6 AS 1-1 CID 0 Packet:
```

```
TCP, SYN, ACK
```

```
, seq 2820426532, ack 453426649 192.168.11.50-80 - 192.168.10.50-42126 6 AS 1-1 CID 0 AppID: service un
```

```
Verdict PASS
```

```
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet:
```

```
TCP, ACK
```

```
, seq 453426649, ack 2820426533 192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service un
```

```
Verdict PERMITLIST
```

Una vez que finaliza la conexión, el motor Snort obtiene la información de metadatos del motor LINA y elimina la sesión:

```
<#root>
```

```
192.168.10.50-42126 > 192.168.11.50-80 6 AS 1-1 I 2
```

```
Got end of flow event
```

```
from hardware with flags 00010001. Rule Match Data: rule_id 0, rule_action 0 rev_id 0, rule_flags 3 19
```

```
Received EOF, deleting the snort session.
```

```
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Session: deleting snort session, reason: timeout
```

La captura de Snort muestra los 3 paquetes que van al motor de Snort:

```
<#root>
```

```
>
```

```
capture-traffic
```

```
Please choose domain to capture traffic from: 0 - management0 1 - management1 2 - Global Selection?
```

```
2
```

```
Please specify tcpdump options desired. (or enter '?' for a list of supported options) Options:
```

```
-n vlan and (host 192.168.10.50 and host 192.168.11.50)
```

```
10:26:16.525928 IP 192.168.10.50.42144 > 192.168.11.50.80: Flags [S], seq 3065553465, win 29200, option
```

La captura de LINA muestra el flujo que lo atraviesa:

```
<#root>
```

```
firepower#
```

```
show capture CAPI
```

```
437 packets captured 1: 09:51:19.431007 802.1Q vlan#202 P0 192.168.10.50.42118 > 192.168.11.50.80: S 2
```

El seguimiento de los paquetes de LINA es otra forma de ver los veredictos de Snort. El primer paquete obtuvo el veredicto de APROBADO:

```
<#root>
```

```
firepower#
```

```
show capture CAPI packet-number 1 trace | i Type|Verdict
```

```
Type: CAPTURE Type: ACCESS-LIST Type: ROUTE-LOOKUP Type: ACCESS-LIST Type: CONN-SETTINGS Type: NAT Typ
```

```
Type: SNORT
```

```
Snort id 22, NAP id 2, IPS id 0, Verdict PASS
```

Snort Verdict: (pass-packet) allow this packet

Type: INPUT-ROUTE-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP Type: ADJACENCY-LOOKUP Type: CAPTURE

Seguimiento del paquete TCP SYN/ACK en la interfaz OUTSIDE:

<#root>

firepower#

show capture CAPO packet-number 2 trace | i Type|Verdict

Type: CAPTURE Type: ACCESS-LIST Type: FLOW-LOOKUP Type: EXTERNAL-INSPECT Type: SNORT

Snort id 22, NAP id 2, IPS id 0, Verdict PASS Snort Verdict: (pass-packet) allow this packet

Type: INPUT-ROUTE-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP Type: ADJACENCY-LOOKUP Type: CAPTURE

El ACK TCP obtiene el veredicto PERMITLIST:

<#root>

firepower#

show capture CAPI packet-number 3 trace | i Type|Verdict

Type: CAPTURE Type: ACCESS-LIST Type: FLOW-LOOKUP Type: EXTERNAL-INSPECT Type: SNORT

Snort id 22, NAP id 2, IPS id 0, Verdict PERMITLIST

Snort Verdict: (fast-forward) fast forward this flow Type: CAPTURE

Este es el resultado completo del veredicto de Snort (paquete n.º 3):

<#root>

firepower#

show capture CAPI packet-number 3 trace | b Type: SNORT

Type: SNORT

Subtype: Result: ALLOW Config: Additional Information: Snort Trace: Packet: TCP, ACK, seq 687485179, a

Verdict PERMITLIST

Snort Verdict: (fast-forward) fast forward this flow

El cuarto paquete no se reenvía al motor Snort, ya que el veredicto se almacena en caché en el motor LINA:



<#root>

firepower#

show capture CAPI packet-number 4 trace

441 packets captured 4: 10:34:02.741523 802.1Q vlan#202 P0 192.168.10.50.42158 > 192.168.11.50.80: P 1

Found flow with id 1254, using existing flow

Phase: 4 Type: SNORT Subtype: Result: ALLOW Config: Additional Information: Snort Verdict: (fast-forward

Result: input-interface: INSIDE(vrfid:0) input-status: up input-line-status: up Action: allow 1 packet

Las estadísticas de Snort confirman esto:

<#root>

firepower#

show snort statistics

Packet Counters:

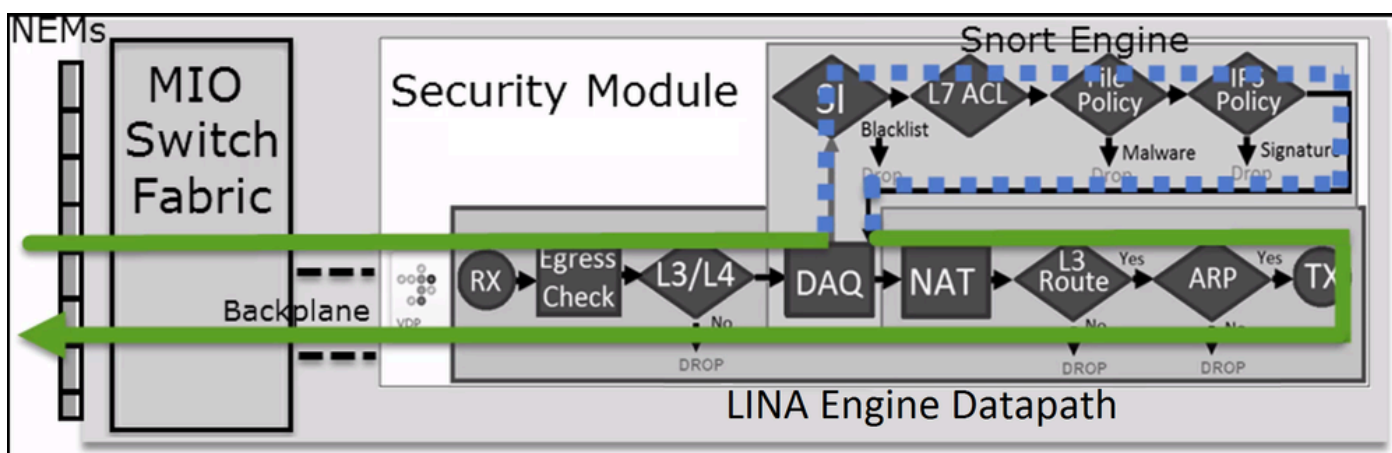
Passed Packets 2

Blocked Packets 0 Injected Packets 0 Packets bypassed (Snort Down) 0 Packets bypassed (Snort Busy) 0 F

Fast-Forwarded Flows 1



Blacklisted Flows 0 Miscellaneous Counters: Start-of-Flow events 0 End-of-Flow events 1 Denied flow ev


Flujo de paquetes con regla de confianza. Snort inspecciona algunos paquetes y LINA inspecciona el resto:








Situación hipotética 2. Acción de confianza de ACP (sin SI, QoS y política de identidad)

Si desea que el FTD aplique comprobaciones de inteligencia de seguridad (SI) a todos los flujos, SI ya está activado en el nivel de ACP y puede especificar los orígenes de SI (TALOS, fuentes, listas, etc.). Por otro lado, en caso de que desee deshabilitarla, deshabilite la SI para redes globalmente por ACP, la SI para URL y la SI para DNS. La SI para redes y URL está deshabilitada, como se muestra en la imagen:

DNS Policy  

Default DNS Policy 

Whitelist (1)	Blacklist (1)
Networks	Networks 
Global Whitelist (Any Zone) 	Global Blacklist (Any Zone)  
URLs	URLs 

En este caso, la regla de confianza se implementa en LINA como Confianza:

```
<#root>
```


```
>
```

```
show access-list
```

```
...
```

```
access-list CSM_FW_ACL_ line 9 remark rule-id 268435461: L4 RULE: Rule1 access-list CSM_FW_ACL_ line 1
```

---

 **Nota:** A partir de 6.2.2, FTD admite TID. El TID funciona de manera similar a la SI, pero en caso de que la SI esté deshabilitada, no "fuerza" el redireccionamiento de paquetes al motor Snort para la inspección del TID.

---

### Verifique el comportamiento:

Inicie una sesión HTTP del host A (192.168.1.40) al host B (192.168.2.40). Dado que se trata de un FP4100 y admite la descarga de flujo en el hardware, suceden estas cosas:

- Algunos paquetes se reenvían a través del motor LINA de FTD y el resto del flujo se descarga en SmartNIC (acelerador de HW).
- No se reenvían paquetes al motor Snort

La tabla de conexiones LINA de FTD muestra el "o" indicador, lo que significa que el flujo se ha descargado al hardware. Además, observe la ausencia de la bandera "N". Esto esencialmente significa 'sin redireccionamiento de Snort':

```
<#root>
```

```
firepower#
```

```
show conn
```

```
1 in use, 15 most used TCP OUTSIDE 192.168.2.40:80 INSIDE 192.168.1.40:32809, idle 0:00:00, bytes 9495
```

```
o
```

Las estadísticas de Snort muestran solo los eventos de registro al comienzo y al final de la sesión:

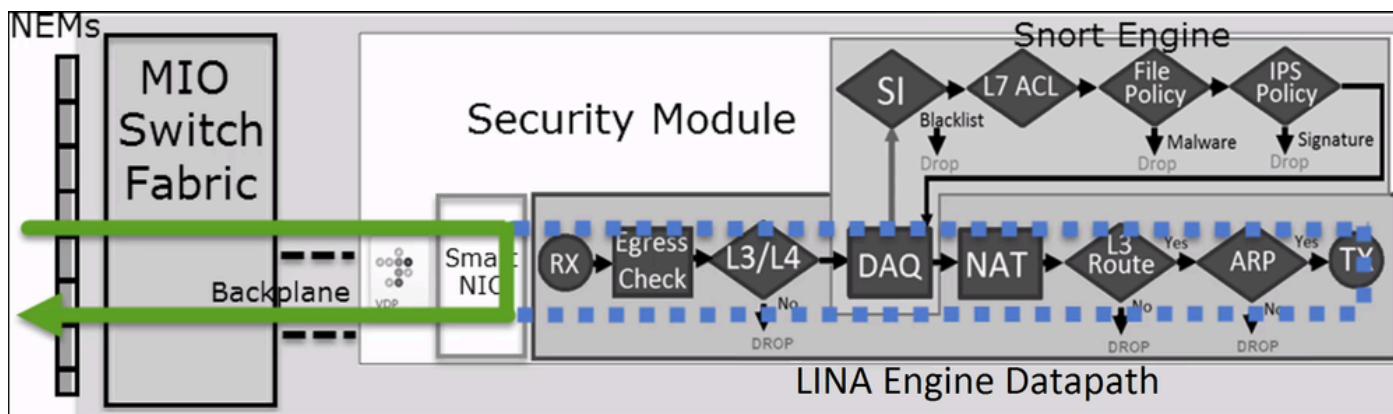
```
<#root>
firepower#
show snort statistics

Packet Counters: Passed Packets 0 Blocked Packets 0 Injected Packets 0 Packets bypassed (Snort Down) 0
Start-of-Flow events 1 End-of-Flow events 1
```

Los registros de LINA de FTD muestran que para cada sesión hubo 2 flujos (uno por cada dirección) descargados en el HW:

```
<#root>
Sep 27 2017 20:16:05: %ASA-7-609001: Built local-host INSIDE:192.168.1.40 Sep 27 2017 20:16:05: %ASA-6-302013: Built inbound TCP connection 25384
Offloaded TCP Flow for connection 25384 from INSIDE
:192.168.1.40/32809 (192.168.1.40/32809) to OUTSIDE:192.168.2.40/80 (192.168.2.40/80) Sep 27 2017 20:16:05:
Offloaded TCP Flow for connection 25384 from OUTSIDE
:192.168.2.40/80 (192.168.2.40/80) to INSIDE:192.168.1.40/32809 (192.168.1.40/32809) Sep 27 2017 20:16:05:
```

Flujo de paquetes con regla de confianza implementada como **trust** acción en LINA. LINA inspecciona algunos paquetes y el resto se descarga en SmartNIC (FP4100/FP9300):

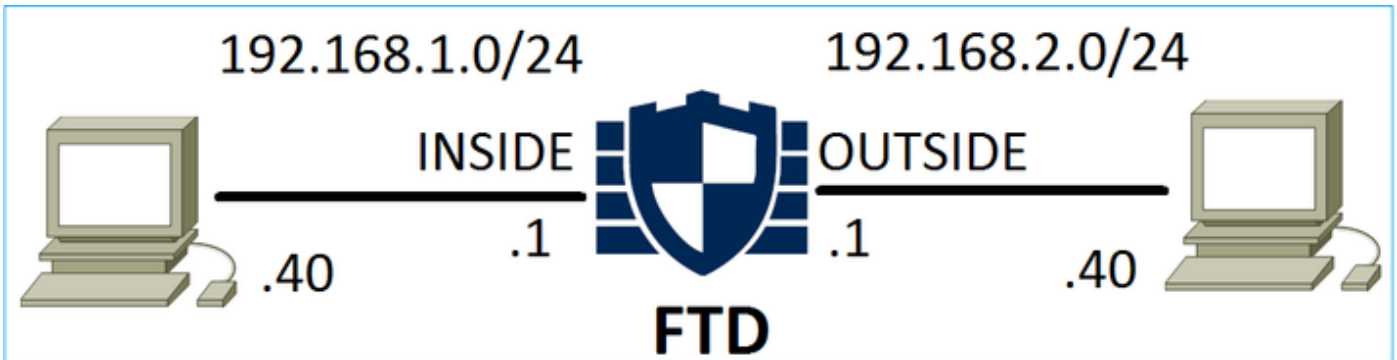


### Casos de uso

- Debe utilizar la acción **Trust** cuando desee que sólo unos pocos paquetes sean verificados por el motor Snort (por ejemplo, detección de aplicaciones, verificación SI) y que el resto del flujo se descargue al motor LINA
- Si utiliza FTD en FP4100/9300 y desea que el flujo omita por completo la inspección de Snort, considere la regla de prefiltro con la acción **Fastpath** (consulte la sección relacionada en este documento)

Acción de bloqueo de políticas de prefiltro

Considere la topología como se muestra en la imagen:



Considere también la política como se muestra en la imagen:

Access Control > Prefilter									
FTD_Prefilter									
Enter Description									
Rules									
Add Tunnel Rule Add Prefilter Rule Search Rules									
#	Name	Rule T...	...	De Source Int Networks	Destination Networks	Source Port	Destinat... Port	VLAN Tag	Action
1	Prefilter1	Prefilter	any any	192.168.1.40	192.168.2.40	any	any	any	Block

Esta es la política implementada en el motor Snort de FTD (archivo ngfw.rules):

```
<#root>
# Start of tunnel and priority rules. #
These rules are evaluated by LINA
. Only tunnel tags are used from the matched rule id. 268437506
deny
any 192.168.1.40 32 any any 192.168.2.40 32 any any any (tunnel -1
```

En LINA:

```
<#root>
access-list CSM_FW_ACL_line 1 remark rule-id 268437506: PREFILTER POLICY: FTD_Prefilter access-list CSM_FW_ACL_line 2 remark rule-id 268437506:
deny
ip host 192.168.1.40 host 192.168.2.40 rule-id 268437506 event-log flow-start (hitcnt=0) 0x76476240
```

Cuando rastrea un paquete virtual, muestra que LINA descarta el paquete y nunca lo reenvía a Snort:

```
<#root>
```

```
firepower# packet-tracer input INSIDE icmp 192.168.1.40 8 0 192.168.2.40 ... Phase: 4
```

```
Type: ACCESS-LIST
```

```
Subtype: log
```

```
Result: DROP
```

```
Config: access-group CSM_FW_ACL_ global
```

```
access-list CSM_FW_ACL_ advanced deny ip host 192.168.1.40 host 192.168.2.40 rule-id 268437506 event-log
```

```
access-list CSM_FW_ACL_ remark rule-id 268437506:
```

```
PREFILTER POLICY: FTD_Prefilter
```

```
access-list CSM_FW_ACL_ remark rule-id 268437506: RULE: Prefilter1 Additional Information: Result: inp
```

```
Drop-reason: (acl-drop) Flow is denied by configured rule
```

Las estadísticas de Snort muestran:

```
<#root>
```

```
firepower#
```

```
show snort statistics
```

```
Packet Counters: Passed Packets 0 Blocked Packets 0 Injected Packets 0 Packets bypassed (Snort Down) 0
```

```
Denied flow events 1
```

Los descartes de la ASP en LINA muestran:

```
<#root>
```

```
firepower#
```

```
show asp drop
```

```
Frame drop:
```

```
Flow is denied by configured rule (acl-drop)
```

```
1
```

Casos de uso

Puede utilizar una regla de bloqueo de filtro previo cuando desee bloquear el tráfico según las condiciones L3/L4 y sin necesidad de realizar ninguna inspección de Snort del tráfico.

Acción Fastpath de política de prefiltro

Considere la regla de política de prefiltro como se muestra en la imagen:

#	Name	Rule T...	Sou Int	De Int	Source Networks	Destination Networks	Source Port	Destinati... Port	VLAN Tag	Action
1	Prefilter1	Prefilter	any	any	192.168.1.40	192.168.2.40	any	TCP (6):80	any	→ Fastpath

Esta es la política implementada en el motor FTD Snort:

```
<#root>
```

```
268437506
```

```
fastpath
```

```
any any any any any any any (log dcforward flowend) (tunnel -1)
```

En LINA de FTD:

```
<#root>
```

```
access-list CSM_FW_ACL_ line 1 remark rule-id 268437506:
```

```
PREFILTER POLICY: FTD_Prefilter
```

```
access-list CSM_FW_ACL_ line 2 remark rule-id 268437506: RULE: Prefilter1 access-list CSM_FW_ACL_ line
```

```
trust
```

```
tcp host 192.168.1.40 host 192.168.2.40 eq www rule-id 268437506 event-log flow-end (hitcnt=0) 0xf3410
```

**Verifique el comportamiento:**

Cuando el host A (192.168.1.40) intenta abrir una sesión HTTP en el host B (192.168.2.40), algunos paquetes pasan por LINA y el resto se descarga en SmartNIC. En este caso, **system support trace** con **firewall-engine-debug** activados muestra:

```
<#root>
```

```
>
```

system support trace

```
Please specify an IP protocol: tcp Please specify a client IP address: 192.168.1.40 Please specify a c
192.168.1.40-32840 > 192.168.2.40-80 6 AS 1 I 8 Got end of flow event from hardware
with flags 04000000
```

Los registros de LINA muestran el flujo descargado:

<#root>

```
Oct 01 2017 14:36:51: %ASA-7-609001: Built local-host INSIDE:192.168.1.40 Oct 01 2017 14:36:51: %ASA-7-609001: Built local-host OUTSIDE:192.168.2.40
Offloaded TCP Flow for connection 966 from INSIDE
:192.168.1.40/32840 (192.168.1.40/32840) to OUTSIDE:192.168.2.40/80 (192.168.2.40/80) Oct 01 2017 14:36:51: %ASA-7-609001: Built local-host OUTSIDE:192.168.2.40
Offloaded TCP Flow for connection 966 from OUTSIDE
:192.168.2.40/80 (192.168.2.40/80) to INSIDE:192.168.1.40/32840 (192.168.1.40/32840)
```

Las capturas LINA muestran 8 paquetes que pasan:

<#root>

```
firepower# show capture capture CAPI type raw-data buffer 33554432 trace trace-count 100 interface INSIDE [Capturing -
3908 bytes]
match ip host 192.168.1.40 host 192.168.2.40 capture CAP0 type raw-data buffer 33554432 trace trace-co
3908 bytes]
match ip host 192.168.1.40 host 192.168.2.40
```

<#root>

firepower#

show capture CAPI

8 packets captured

```
1: 14:45:32.700021 192.168.1.40.32842 > 192.168.2.40.80: S 3195173118:3195173118(0) win 2920 <mss 1460
```

Las estadísticas del flujo descargado de FTD muestran 22 paquetes descargados en el HW:

<#root>

firepower#

show flow-offload statistics

Packet stats of port : 0

Tx Packet count : 22

Rx Packet count : 22

Dropped Packet count : 0 VNIC transmitted packet : 22 VNIC transmitted bytes : 15308 VNIC Dropped packet :

También puede utilizar el **show flow-offload flow** comando para ver información adicional relacionada con los flujos descargados. Aquí tiene un ejemplo:

<#root>

firepower#

show flow-offload flow

Total offloaded flow stats: 2 in use, 4 most used, 20% offloaded, 0 collisions

TCP intfc 103 src 192.168.1.40:39301 dest 192.168.2.40:20, static, timestamp 616063741, packets 33240,

TCP intfc 104 src 192.168.2.40:20 dest 192.168.1.40:39301, static, timestamp 616063760, packets 249140,

firepower#

show conn

5 in use, 5 most used

Inspect Snort:

preserve-connection: 1 enabled, 0 in effect, 4 most enabled, 0 most in effect

TCP OUTSIDE 192.168.2.40:21 INSIDE 192.168.1.40:40988, idle 0:00:00, bytes 723, flags UIO

TCP OUTSIDE 192.168.2.40:21 INSIDE 192.168.1.40:40980, idle 0:02:40, bytes 1086, flags UIO

TCP OUTSIDE 192.168.2.40:80 INSIDE 192.168.1.40:49442, idle 0:00:00, bytes 86348310, flags UIO N1

TCP OUTSIDE 192.168.2.40:20 INSIDE 192.168.1.40:39301, idle 0:00:00, bytes 485268628, flags U

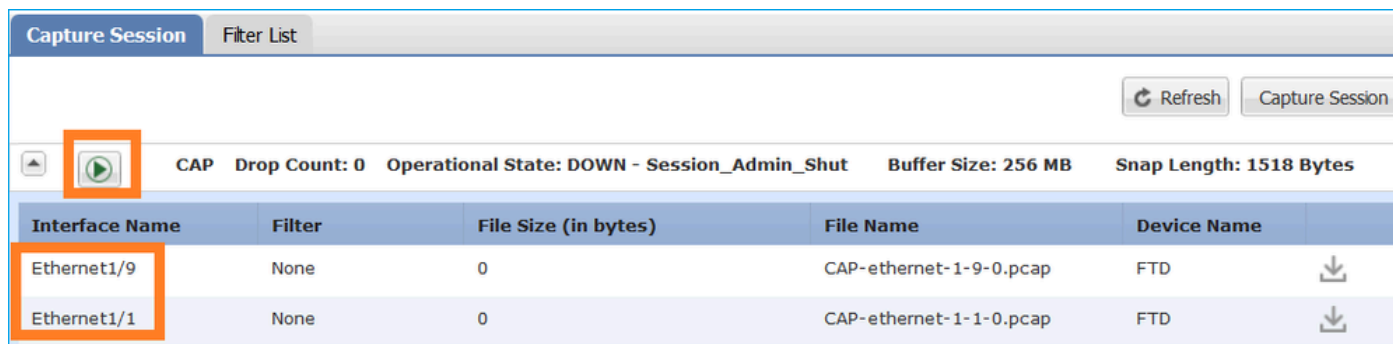
o <- offloaded flow

TCP OUTSIDE 192.168.2.40:20 INSIDE 192.168.1.40:34713, idle 0:02:40, bytes 821799360, flags UFRIO

- El porcentaje se basa en la salida "**show conn**". Por ejemplo, si 5 conns en total pasan a través del motor FTD LINA y 1 de ellos se descarga, el 20% se informa como descargado
- El límite máximo de sesiones descargadas depende de la versión de software (por ejemplo, ASA 9.8.3 y FTD 6.2.3 admiten 4 millones de flujos descargados bidireccionales (u 8 millones unidireccionales))
- En caso de que el número de flujos descargados alcance el límite (por ejemplo, 4 millones de flujos bidireccionales), no se descargarán nuevas conexiones hasta que se eliminen las conexiones actuales de la tabla de descargas



Para ver todos los paquetes en FP4100/9300 que pasan por FTD (descargados + LINA), es necesario habilitar la captura a nivel del chasis, como se muestra en la imagen:



La captura del plano posterior del chasis muestra ambas direcciones. Debido a la arquitectura de captura FXOS (2 puntos de captura por dirección), cada paquete se muestra **dos veces**, como se muestra en la imagen:

Estadísticas de paquetes:

- Paquetes totales mediante FTD: 30
- Paquetes a través de FTD LINA: 8
- Paquetes descargados al acelerador de hardware SmartNIC: 22

En el caso de una plataforma diferente a FP4100/FP9300, todos los paquetes son manejados por el motor LINA ya que no se soporta la descarga de flujo (observe la ausencia del indicador **o**):

```
<#root>
```

```
FP2100-6#
```

```
show conn addr 192.168.1.40
```

```
33 in use, 123 most used Inspect Snort: preserve-connection: 0 enabled, 0 in effect, 2 most enabled, 0
```

```
UxIO
```

Los syslogs de LINA solo muestran la configuración de la conexión y los eventos de finalización de la conexión:

```
<#root>
```

```
FP2100-6#
```

```
show log | i 192.168.2.40
```

```
Jun 21 2020 14:29:44: %FTD-6-302013:
```

**Built inbound TCP**

connection 6914 for INSIDE:192.168.1.40/50900 (192.168.11.101/50900) to OUTSIDE:192.168.2.40/80 (192.168.2.40/80)

**Teardown TCP connection**

6914 for INSIDE:192.168.1.40/50900 to OUTSIDE:192.168.2.40/80 duration 0:00:46 bytes 565 TCP FINs from

**Casos de uso**

- Utilice la acción Fastpath de prefiltro cuando desee omitir por completo la inspección de Snort. Por lo general, querrá hacer esto para los flujos grandes y pesados en los que confía, como copias de seguridad, transferencias de bases de datos, etc.
- En los dispositivos FP4100/9300, la acción Fastpath activa la descarga de flujo y solo unos pocos paquetes pasan por el motor LINA de FTD. El resto se maneja a través de SmartNIC, lo que disminuye la latencia.

**Acción Fastpath de política de prefiltro (conjunto en línea)**

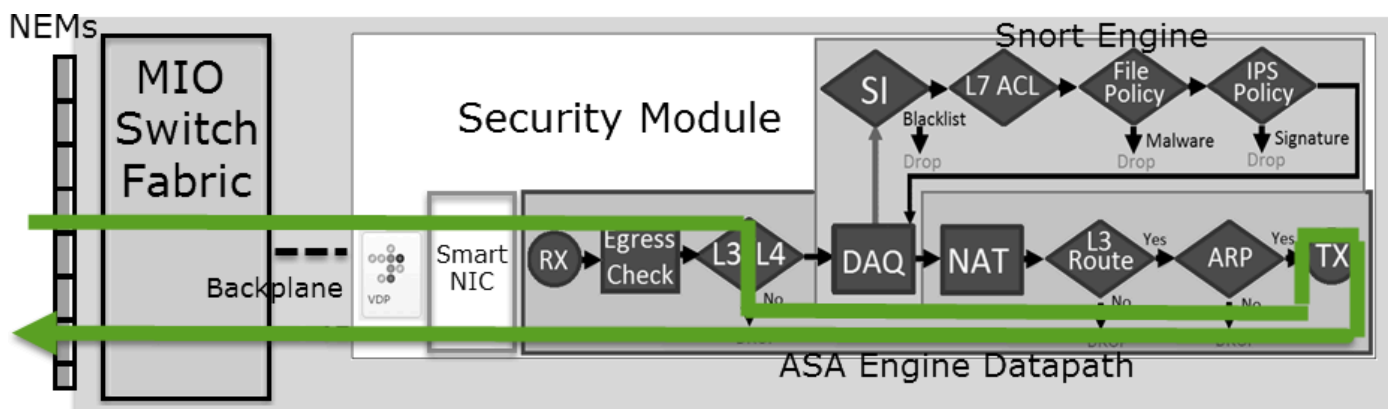
En caso de que se aplique una acción Prefilter Policy Fastpath al tráfico que pasa por un conjunto en línea (interfaces NGIPS), se deben tener en cuenta estos puntos:

- La regla se aplica al motor LINA como acción de **confianza**.
- El flujo no es inspeccionado por el motor Snort.
- La descarga de flujo (aceleración de hardware) no se produce porque la descarga de flujo no se aplica a las interfaces NGIPS.

A continuación se muestra un ejemplo de un seguimiento de paquetes en el caso de la acción Prefilter Fastpath aplicada en un conjunto en línea:

firepower# packet-tracer input inside tcp 192.168.1.40 12345 192.168.1.50 80 detailed Phase: 1 Type: NGIPS-MODE Subtype: ngips-mode Result: ALLOWED

Esta es la representación visual de la trayectoria del paquete:



Acción Fastpath de política de prefiltro (conjunto en línea con conector)

Igual que en el caso del conjunto en línea.

### Acción de análisis de políticas de prefiltro

#### Escenario 1. Análisis de prefiltro con regla de bloqueo de la ACP

Considere la política de prefiltro que contiene una regla de análisis, como se muestra en la imagen:

#	Name	Rule T...	Source Interfac...	Destinat... Interfac...	Source Networks	Destination Networks	Source Port	Destinat... Port	VLAN Tag	Action
1	Prefilter_Rule1	Prefilter	any	any	192.168.1.40	192.168.2.40	any	any	any	Analyze

El ACP contiene solamente la regla por defecto que se fija en **Block All Traffic** como se muestra en la imagen:

#	Name	Source Zones	Dest Zones	Source Netwo...	Dest Netwo...	VLAN ...	Users	Applic...	Sourc...	Dest P...	URLs	ISE/S... Attrib...	Action
Mandatory - ACP1 (-)													
There are no rules in this section. Add Rule or Add Category													
Default - ACP1 (-)													
There are no rules in this section. Add Rule or Add Category													
Default Action													
Access Control: Block All Traffic													

Esta es la política implementada en el motor Snort de FTD (archivo ngfw.rules):

```
<#root>
```

```
# Start of tunnel and priority rules.
```

```
# These rules are evaluated by LINA. Only tunnel tags are used from the matched rule id.
```

```
268435460 allow any 192.168.1.40 32 any any 192.168.2.40 32 any any any (tunnel -1) 268435459 allow any
```

```
# start of AC rule.
```

```
268435458 deny any any any any any any any any (log dcforward flowstart)
```

```
# End of AC rule.
```

Esta es la política implementada en el motor LINA de FTD:

```
<#root>
```

```
access-list CSM_FW_ACL_ line 3 advanced
```

```
permit
```

```
ip host 192.168.1.40 host 192.168.2.40 rule-id 268435460 (hitcnt=0) 0xb788b786
```

### Verifique el comportamiento:

Packet-tracer muestra que el paquete está permitido por LINA, se reenvía al motor Snort (debido a una **permit** acción) y el motor Snort devuelve un **Block** veredicto ya que la acción predeterminada de AC coincide.



**Nota:** Snort no evalúa el tráfico según las reglas del túnel

---

Cuando rastrea un paquete, revela lo mismo:

```
<#root>
```

```
firepower#
```

```
packet-tracer input INSIDE icmp 192.168.1.40 8 0 192.168.2.40
```

```
... Phase: 4 Type: ACCESS-LIST Subtype: log Result: ALLOW Config: access-group CSM_FW_ACL_ global
```

```
access-list CSM_FW_ACL_ advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id 268435460
```

```
access-list CSM_FW_ACL_ remark rule-id 268435460: PREFILTER POLICY: Prefilter_Policy1 access-list CSM_FW_ACL_
```

```
This packet will be sent to snort for additional processing where a verdict will be reached
```

```
... Phase: 14
```

```
Type: SNORT
```

```
Subtype:
```

```
Result: DROP
```

```
Config: Additional Information: Snort Trace: Packet: ICMP AppID: service ICMP (3501), application unknown
```

```
Firewall: block rule, id 268435458, drop
```

```
Snort: processed decoder alerts or actions queue, drop NAP id 1, IPS id 0,
```

```
Verdict BLOCKLIST, Blocked by Firewall
```

```
Snort Verdict:
```

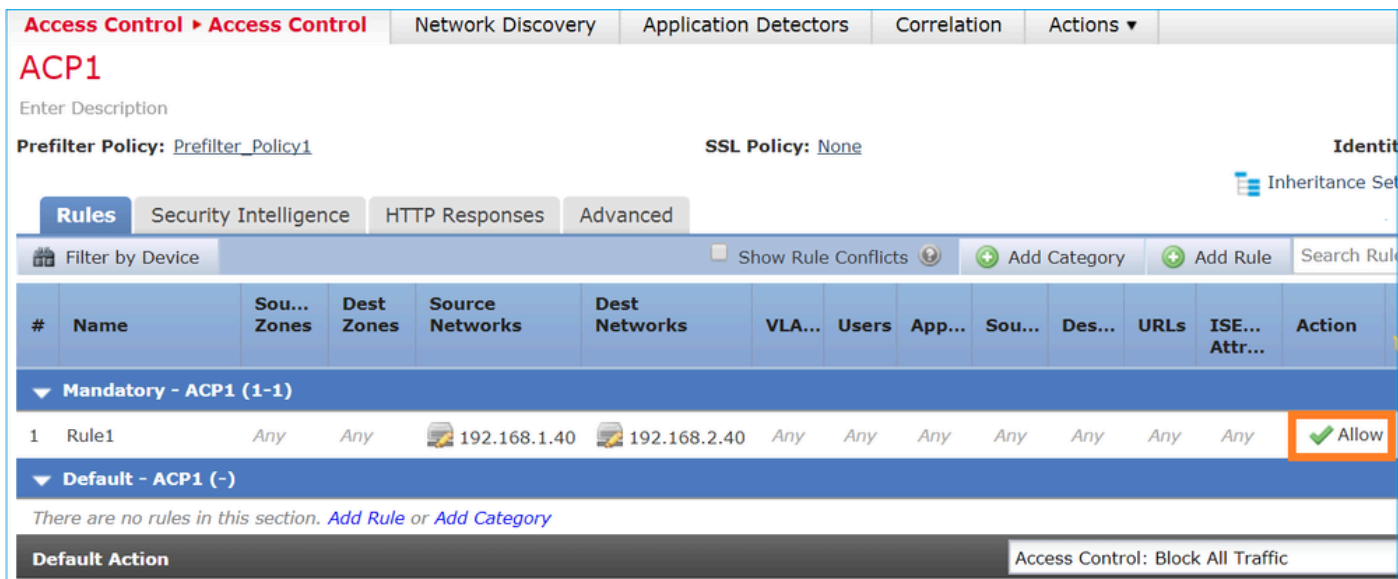
(block-list) block list this flow

Result: input-interface: INSIDE input-status: up input-line-status: up output-interface: OUTSIDE output

Drop-reason: (firewall) Blocked by the firewall preprocessor

Situación hipotética 2. Análisis de prefiltro con regla de permiso de la ACP

Si el objetivo es permitir que el paquete atraviese FTD, es necesario agregar una regla a la ACP. La acción puede ser Allow (Permitir) o Trust (Confiar), que depende del objetivo (por ejemplo, si desea aplicar una inspección L7, debe utilizar **Allow** acción), como se muestra en la imagen:



La política implementada en el motor Snort de FTD:

<#root>

# Start of AC rule.

268435461 allow any 192.168.1.40 32 any any 192.168.2.40 32 any any any

268435458 deny any any any any any any any (log dcforward flowstart) # End of AC rule.

En el motor LINA:

<#root>

access-list CSM\_FW\_ACL\_line 3 advanced

permit

ip host 192.168.1.40 host 192.168.2.40 rule-id 268435460 (hitcnt=1) 0xb788b786

Verifique el comportamiento:

Packet-tracer muestra que el paquete coincide con la regla 268435460 en LINA y 268435461 en el motor Snort:

<#root>

firepower#

packet-tracer input INSIDE icmp 192.168.1.40 8 0 192.168.2.40

... Phase: 4 Type: ACCESS-LIST Subtype: log Result: ALLOW Config: access-group CSM\_FW\_ACL\_ global access-list CSM\_FW\_ACL\_ permit

ip host 192.168.1.40 host 192.168.2.40 rule-id 268435460 access-list CSM\_FW\_ACL\_ remark rule-id 268435460

This packet will be sent to snort for additional processing where a verdict will be reached

... Phase: 14 Type: SNORT Subtype: Result: ALLOW Config: Additional Information: Snort Trace: Packet: ICMP

allow rule, id 268435461, allow

NAP id 1, IPS id 0,

Verdict PASS

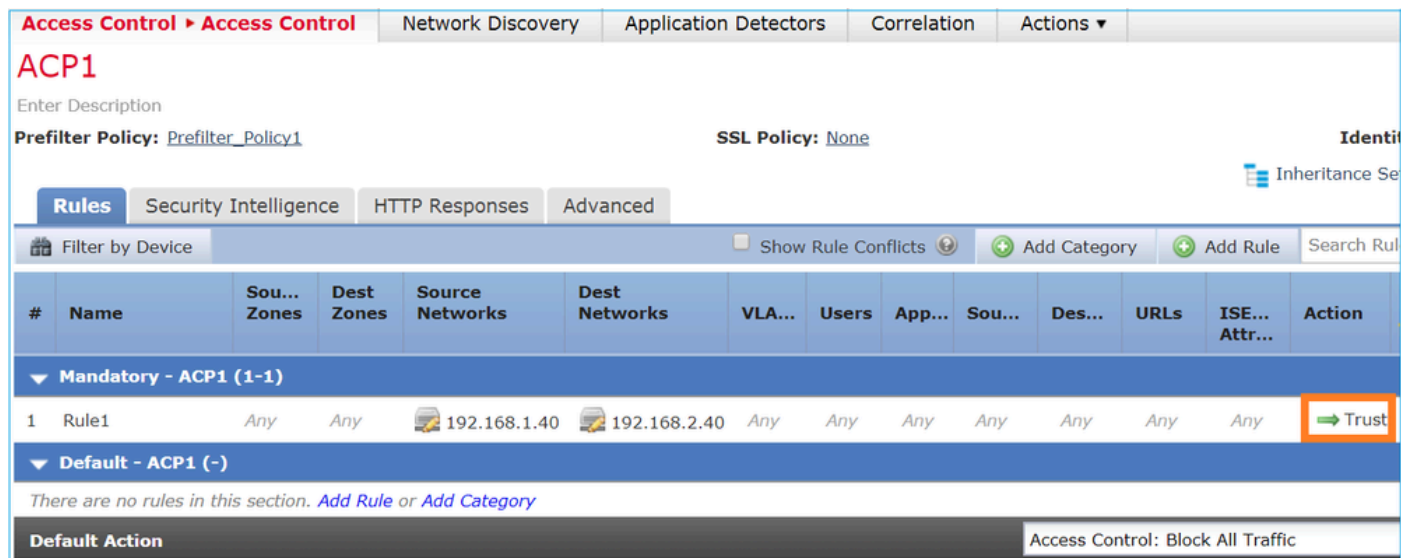
Snort Verdict: (pass-packet) allow this packet

... Result: input-interface: INSIDE input-status: up input-line-status: up output-interface: OUTSIDE output-status: up

Action: allow

Situación hipotética 3. Análisis de prefiltro con regla de confianza de ACP

En caso de que la ACP contenga una regla de confianza, la tendrá como se muestra en la imagen:



Snort:

<#root>

# Start of AC rule.

```
268435461 fastpath any 192.168.1.40 32 any any 192.168.2.40 32 any any any
```

```
268435458 deny any any any any any any any any (log dcforward flowstart) # End of AC rule.
```

LINA:

```
<#root>
```

```
access-list CSM_FW_ACL_ line 3 advanced
```

```
permit
```

```
ip host 192.168.1.40 host 192.168.2.40 rule-id 268435460 (hitcnt=2) 0xb788b786
```

Recuerde que, dado que el SI está activado de forma predeterminada, la regla de confianza se implementa como **permit** acción en LINA, de modo que al menos unos pocos paquetes se redirigen al motor Snort para su inspección.

#### Verifique el comportamiento:

Packet-tracer muestra que el Permiso del motor Snort enumera el paquete y básicamente descarga el resto del flujo a LINA:

```
<#root>
```

```
firepower#
```

```
packet-tracer input INSIDE icmp 192.168.1.40 8 0 192.168.2.40
```

```
... Phase: 4 Type: ACCESS-LIST Subtype: log Result: ALLOW Config: access-group CSM_FW_ACL_ global
```

```
access-list CSM_FW_ACL_ advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id 268435460
```

```
access-list CSM_FW_ACL_ remark rule-id 268435460: PREFILTER POLICY: Prefilter_Policy1 access-list CSM_
```

```
This packet will be sent to snort for additional processing where a verdict will be reached
```

```
... Phase: 14 Type: SNORT Subtype: Result: ALLOW Config: Additional Information: Snort Trace: Packet: IC
```

```
trust/fastpath rule, id 268435461, allow
```

```
NAP id 1, IPS id 0,
```

```
Verdict PERMITLIST
```

```
Snort Verdict: (fast-forward) fast forward this flow
```

```
... Result: input-interface: INSIDE input-status: up input-line-status: up output-interface: OUTSIDE out
```

```
Action: allow
```

Situación hipotética 4. Análisis de prefiltro con regla de confianza de ACP

En esta situación, la SI se deshabilitó manualmente.

La regla se implementa en Snort de la siguiente manera:

<#root>

# Start of AC rule. 268435461

**fastpath**

any 192.168.1.40 32 any any 192.168.2.40 32 any any any 268435458 deny any any any any any any any any

En LINA, la regla se implementa como Confianza. Sin embargo, un paquete coincide con la regla de permiso (consulte recuentos de aciertos ACE) que se implementa debido a la regla de análisis de filtro previo y el motor Snort inspecciona el paquete:

<#root>

access-list CSM\_FW\_ACL\_line 3 advanced

**permit ip host 192.168.1.40 host 192.168.2.40**

rule-id 268435460 (hitcnt=3) 0xb788b786 ... access-list CSM\_FW\_ACL\_line 13 advanced

**trust ip host 192.168.1.40 host 192.168.2.40**

rule-id 268435461 event-log flow-end (hitcnt=0) 0x5c1346d6 ... access-list CSM\_FW\_ACL\_line 16 advanced

**deny ip any any**

rule-id 268435458 event-log flow-start (hitcnt=0) 0x97aa021a

**Verifique el comportamiento:**

<#root>

firepower#

**packet-tracer input INSIDE icmp 192.168.1.40 8 0 192.168.2.40**

... Phase: 4 Type: ACCESS-LIST Subtype: log Result: ALLOW Config: access-group CSM\_FW\_ACL\_global access-

**permit**

ip host 192.168.1.40 host 192.168.2.40 rule-id 268435460 access-list CSM\_FW\_ACL\_remark rule-id 268435

**This packet will be sent to snort for additional processing where a verdict will be reached**

... Phase: 14 Type: SNORT Subtype: Result: ALLOW Config: Additional Information: Snort Trace: Packet: 1

**trust/fastpath rule, id 268435461, allow**

NAP id 1, IPS id 0,

**Verdict PERMITLIST**

Snort Verdict: (fast-forward) fast forward this flow ... Result: input-interface: INSIDE input-status: u



Action: allow

## Puntos principales

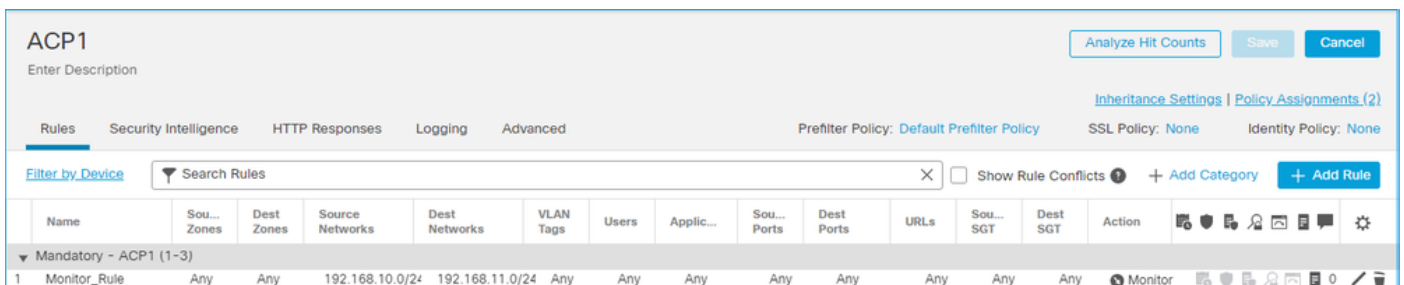
- La acción **Analyze** se implementa como una regla de permiso en el motor LINA. Esto tiene un efecto en el paquete que se reenvía al motor Snort para su inspección
- La acción **Analyze** no despliega ninguna regla en el motor Snort, por lo que debe asegurarse de configurar una regla en el ACP que coincida en Snort<
- Depende de la regla ACP que se implemente en el motor Snort (**block** vs **allow** vs **fastpath**), Snort permite ninguno o todos o algunos paquetes

## Casos de uso

- Un caso de uso de la acción de análisis es cuando tiene una regla Fastpath amplia en la política de prefiltro y desea establecer algunas excepciones para flujos específicos para que Snort los inspeccione.

## Acción de monitoreo de la ACP

Una regla de monitoreo configurada en la interfaz de usuario del FMC:



The screenshot shows the FMC configuration page for ACP1. The rule 'Monitor\_Rule' is configured with the following parameters:

Name	Sou... Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applic...	Sou... Ports	Dest Ports	URLs	Sou... SGT	Dest SGT	Action	Icons
Monitor_Rule	Any	Any	192.168.10.0/24	192.168.11.0/24	Any	Any	Any	Any	Any	Any	Any	Any	Monitor	Icons

La regla de supervisión se implementa en el motor LINA de FTD como una **permit** acción y en el motor Snort como una **audit** acción.

```
<#root>
```

```
firepower#
```

```
show access-list
```

```
... access-list CSM_FW_ACL_ line 10 advanced
```

```
permit
```

```
ip 192.168.10.0 255.255.255.0 192.168.11.0 255.255.255.0 rule-id
```

```
268438863
```

```
(hitcnt=0) 0x61bbaf0c
```

La regla de Snort:

```
<#root>
```

```
admin@firepower:~$
```

```
cat /var/sf/detection_engines/9e080e5c-adc3-11ea-9d37-44884cf7e9ba/ngfw.rules
```

```
... # Start of AC
```

```
rule. 268438863 audit
```

```
any 192.168.10.0 24 any any 192.168.11.0 24 any any any (log dcforward flowend) # End rule 268438863
```

### Puntos principales

- La regla de supervisión no descarta ni permite el tráfico, pero genera un evento de conexión. El paquete se compara con las reglas posteriores y se permite o descarta.
- Los eventos de conexión FMC muestran que el paquete coincidió con 2 reglas:

	First Packet ×	Last Packet ×	Action ×	Initiator IP ×	Responder IP ×	Source Port / ICMP Type ×	Destination Port / ICMP Code ×	Access Control Policy ×	Access Control Rule ×
▼	2020-06-20 22:17:40	2020-06-20 22:17:43	Trust	192.168.10.50	192.168.11.50	41920 / tcp	80 (http) / tcp	ACP1	trust_L3-L4, Monitor_Rule

**System support trace** El resultado muestra que los paquetes coinciden con ambas reglas:

```
<#root>
```

```
>
```

```
system support trace
```

```
Enable firewall-engine-debug too? [n]:
```

```
y
```

```
Please specify an IP protocol: tcp Please specify a client IP address:
```

```
192.168.10.50
```

```
Please specify a client port: Please specify a server IP address:
```

```
192.168.11.50
```

```
Please specify a server port: Monitoring packet tracer and firewall debug messages 192.168.10.50-41922
```

```
match rule order 2, 'Monitor_Rule', action Audit
```

```
192.168.10.50-41922 > 192.168.11.50-80 6 AS 1-1 I 19
```

```
match rule order 3, 'trust_L3-L4', action Trust
```

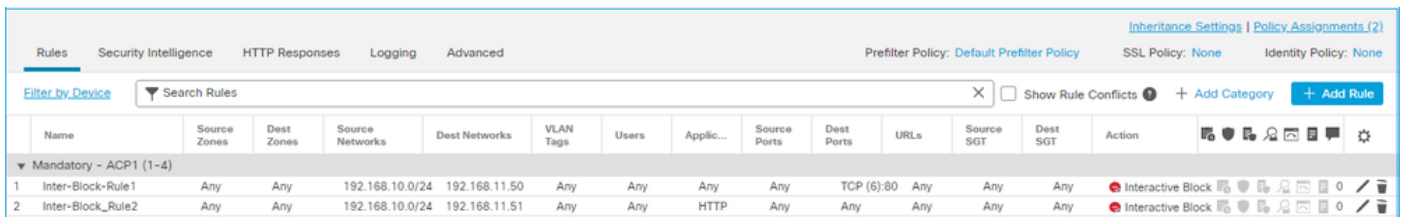
```
192.168.10.50-41922 > 192.168.11.50-80 6 AS 1-1 I 19 MidRecovery data sent for rule id: 268438858,rule.
```

## Casos de uso

Se utiliza para monitorear la actividad de la red y generar un evento de conexión.

## Acción de bloqueo interactivo de la ACP

Una regla de bloqueo interactivo configurada en la interfaz de usuario del FMC:



Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applic...	Source Ports	Dest Ports	URLs	Source SGT	Dest SGT	Action
Mandatory - ACP1 (1-4)													
1 Inter-Block-Rule1	Any	Any	192.168.10.0/24	192.168.11.50	Any	Any	Any	Any	TCP (6):80	Any	Any	Any	Interactive Block
2 Inter-Block_Rule2	Any	Any	192.168.10.0/24	192.168.11.51	Any	Any	HTTP	Any	Any	Any	Any	Any	Interactive Block

La regla de bloqueo interactivo se implementa en el motor LINA de FTD como una **permit** acción y en el motor Snort como una regla de derivación:

```
<#root>
```

```
firepower#
```

```
show access-list
```

```
... access-list CSM_FW_ACL_ line 9 remark rule-id 268438864: L7 RULE: Inter-Block-Rule1 access-list CSM_
permit
tcp 192.168.10.0 255.255.255.0 host 192.168.11.50 eq www rule-id 268438864 (hitcnt=3) 0xba785fc0 acces
permit
ip 192.168.10.0 255.255.255.0 host 192.168.11.51 rule-id 268438865 (hitcnt=0) 0x622350d0
```

Motor Snort:

```
<#root>
```

```
admin@firepower:~$
```

```
cat /var/sf/detection_engines/9e080e5c-adc3-11ea-9d37-44884cf7e9ba/ngfw.rules
```

```
... # Start of AC rule. 268438864
```

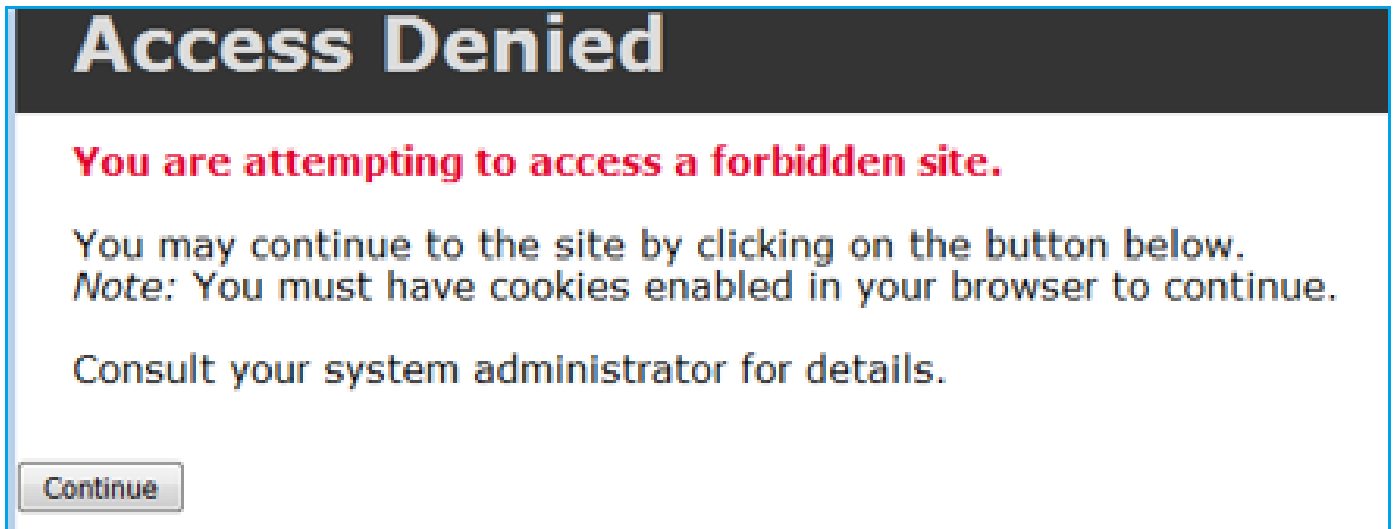
```
bypass
```

```
any 192.168.10.0 24 any any 192.168.11.50 32 80 any 6 # End rule 268438864 268438865
```

```
bypass
```

```
any 192.168.10.0 24 any any 192.168.11.51 32 any any any (appid 676:1) (ip_protos 6, 17) # End rule 26
```

La regla de bloqueo interactivo le indica al usuario que el destino está prohibido.



De manera predeterminada, el firewall permite omitir el bloqueo durante 600 segundos:

Rules	Security Intelligence	HTTP Responses	Logging	Advanced
General Settings				
Maximum URL characters to store in connection events				1024
Allow an Interactive Block to bypass blocking for (seconds)				600
Retry URL cache miss lookup				Yes
Enable Threat Intelligence Director				Yes
Inspect traffic during policy apply				Yes

En la **system support trace** salida puede ver que inicialmente el firewall bloquea el tráfico y muestra la página de bloqueo:

```
<#root>
```

```
>
```

```
system support trace
```

```
... 192.168.10.52-58717 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, ACK, seq 983273680, ack 201487958
```

```
action Interactive
```

```
192.168.10.52-58717 > 192.168.11.50-80 6 AS 1-1 I 22
```

```
bypass action sending HTTP interactive response of 1093 bytes
```

```
192.168.10.52-58717 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: interactive block rule, 'Inter-Block-R
```

Verdict BLACKLIST

192.168.10.52-58717 - 192.168.11.50-80 6 AS 1-1 CID 0 ==>

Blocked by Firewall

Verdict reason is sent to DAQ

Una vez que el usuario selecciona **Continue** (o actualiza la página del navegador) la depuración muestra que los paquetes están permitidos por la misma regla que imita y **Allow** acción:

<#root>

192.168.10.52-58718 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, ACK, seq 1357413630, ack 2607625293 192.168.10.52-58718 - 192.168.11.50-80

action Interactive

192.168.10.52-58718 > 192.168.11.50-80 6 AS 1-1 I 8

bypass action interactive bypass

192.168.10.52-58718 > 192.168.11.50-80 6 AS 1-1 I 8

allow action

192.168.10.52-58718 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: allow rule, 'Inter-Block-Rule1', allow

Verdict PASS

### Casos de uso

Muestre una página de advertencia a los usuarios web y deles la opción de continuar.

### Bloqueo interactivo de la ACP con acción de restablecimiento

Un bloqueo interactivo con una regla de restablecimiento configurada en la interfaz de usuario del FMC:

Name	Sour... Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Appl...	Sour... Ports	Dest Ports	URLs	Sour... SGT	Dest SGT	Action	Icons
▼ Mandatory - ACP1 (1-4)														
1	Any	Any	192.168.10.0/24	192.168.11.50	Any	Any	Any	Any	TCP (6):80	Any	Any	Any	Interactive Block with reset	Icons
2	Any	Any	192.168.10.0/24	192.168.11.51	Any	Any	HTTP	Any	Any	Any	Any	Any	Interactive Block with reset	Icons

El Bloqueo interactivo con regla de restablecimiento se implementa en el motor FTD LINA como una **permit** acción y en el motor Snort como regla de restablecimiento:

<#root>

firepower#

show access-list

... access-list CSM\_FW\_ACL\_ line 9 remark rule-id 268438864: L7 RULE: Inter-Block-Rule1 access-list CSM\_

permit

```
tcp 192.168.10.0 255.255.255.0 host 192.168.11.50 eq www rule-id 268438864 (hitcnt=13) 0xba785fc0
```

permit

```
ip 192.168.10.0 255.255.255.0 host 192.168.11.51 rule-id 268438865 (hitcnt=0) 0x622350d0
```

Motor Snort:

<#root>

# Start of AC rule. 268438864

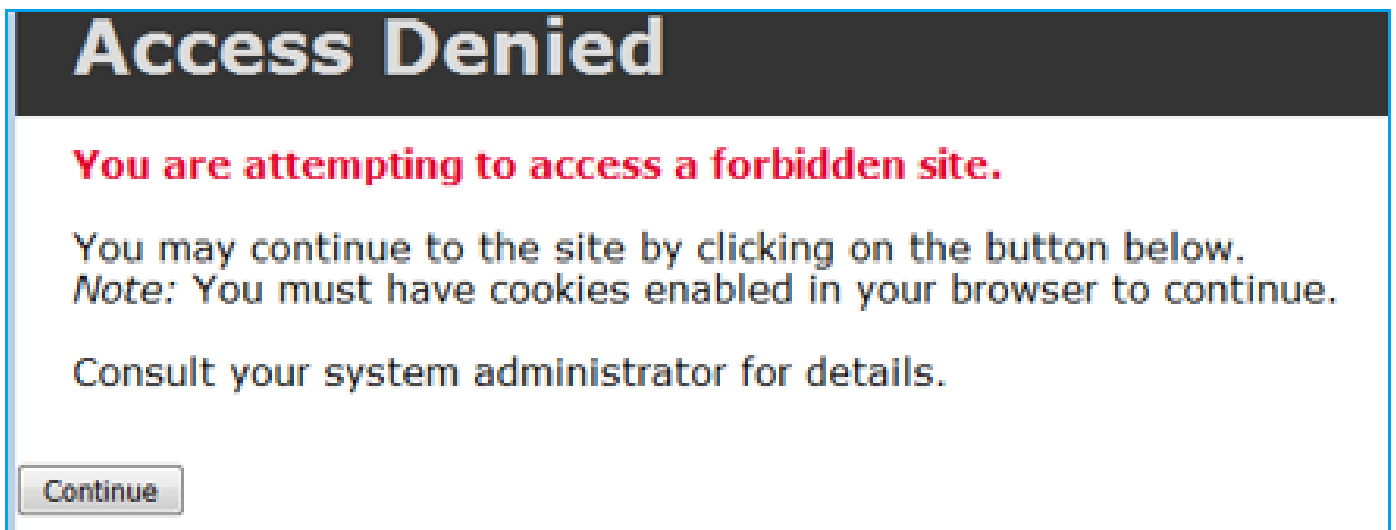
intreset

```
any 192.168.10.0 24 any any 192.168.11.50 32 80 any 6 # End rule 268438864 268438865
```

intreset

```
any 192.168.10.0 24 any any 192.168.11.51 32 any any any (appid 676:1) (ip_protos 6, 17) # End rule 268438865
```

Al igual que el bloque con restablecimiento, el usuario puede seleccionar la **Continue** opción:



En la depuración de Snort, la acción que se muestra en Restablecimiento interactivo:

<#root>

>

system support trace

```
Enable firewall-engine-debug too? [n]:
```

y

```
Please specify an IP protocol: tcp Please specify a client IP address:
```

```
192.168.10.52
```

Please specify a client port: Please specify a server IP address:

192.168.11.50

Please specify a server port: Monitoring packet tracer and firewall debug messages 192.168.10.52-58958

action Interactive Reset

192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24

bypass action sending HTTP interactive response of 1093 bytes

192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: interactive block rule, 'Inter-Block-R

Verdict BLACKLIST

192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 ==>

Blocked by Firewall

Verdict reason is sent to DAQ

En este momento, la página de bloqueo se muestra al usuario final. Si el usuario selecciona **Continue** (o actualiza la página web) la misma regla coincide y esta vez permite el tráfico a través de:

<#root>

192.168.10.52-58962 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, ACK, seq 1593478294, ack 3135589307 192.168.10.52-58962 - 192.168.11.50-80

action Interactive Reset

192.168.10.52-58962 > 192.168.11.50-80 6 AS 1-1 I 14

bypass action interactive bypass

192.168.10.52-58962 > 192.168.11.50-80 6 AS 1-1 I 14 allow action 192.168.10.52-58962 - 192.168.11.50-

Verdict PASS

192.168.11.50-80 - 192.168.10.52-58962 6 AS 1-1 CID 0 Packet: TCP, ACK, seq 3135589307, ack 1593478786

Verdict PASS

El bloqueo interactivo con regla de restablecimiento envía un RST de TCP al tráfico no web:

<#root>

firepower#

show cap CAPI | i 11.50

2: 22:13:33.112954 802.1Q vlan#202 P0 192.168.10.50.40010 > 192.168.11.50.21: S 3109534920:3109534920(C

R

3422362570:3422362570(0) ack 3109534931 win 0

## Orificios y conexiones secundarias de FTD

En las versiones anteriores (por ejemplo, 6.2.2, 6.2.3, etc.), el motor Snort no abre agujeros para conexiones secundarias (por ejemplo, datos FTD) si se utiliza la **Trust** acción. En las últimas versiones, este comportamiento cambia y el motor Snort abre agujeros incluso con la **Trust** acción.

## Pautas de la regla de FTD

- Utilice las reglas Fastpath de la política de prefiltro para los grandes flujos y para disminuir la latencia del cuadro.
- Utilice las reglas de bloqueo de prefiltro para el tráfico que debe bloquearse según las condiciones L3/L4.
- Utilice las reglas de confianza de la ACP si desea omitir muchas de las verificaciones de Snort, pero aún así quiere aprovechar las características tales como política de identidad, QoS, SI, detección de aplicaciones, filtro de URL.
- Coloque reglas que afecten menos el rendimiento del firewall en la parte superior de la política de control de acceso con el uso de estas pautas:
  - Reglas de bloqueo (capas 1 a 4): bloqueo de prefiltro
  - Reglas de permiso (capas 1 a 4): Fastpath de prefiltro
  - Reglas de bloqueo de la ACP (capas 1 a 4)
  - Reglas de confianza (capas 1 a 4)
  - Reglas de bloqueo (capas 5 a 7: detección de aplicaciones, filtrado de URL)
  - Reglas de permiso (capas 1 a 7: detección de aplicaciones, filtrado de URL, política de intrusiones/política de archivos)
  - Regla de bloqueo (regla predeterminada)
- Evite el registro excesivo (inicie sesión al principio o al final y evite ambos al mismo tiempo).
- Tenga en cuenta la expansión de reglas para verificar la cantidad de reglas en LINA.

<#root>

firepower#

```
show access-list | include elements
```

```
access-list CSM_FW_ACL_;
```

```
7 elements
```

```
; name hash: 0x4a69e3f3
```




## Summary

### Acciones de prefiltro

Rule Action (FMC UI)	LINA Action	Snort Action	Notes
Fastpath	Trust	Fastpath	Static Flow Offload to SmartNIC (4100/9300). <b>No packets</b> are sent to Snort engine.
Analyze	Permit	-	The ACP rules are checked. <b>Few or all packets</b> are sent to Snort engine for inspection. Traffic is allowed or dropped based on Snort engine verdict
Block (Prefilter)	Deny	-	Early drop by FTD LINA <b>No packets</b> are sent to Snort engine

### Acciones de la ACP

Rule Action (FMC UI)	Additional Conditions	LINA Action	Snort Action	Notes
Block	The rule matches L3/L4 conditions	Deny	Deny	
Block	The rule has L7 conditions	Permit	Deny	
Allow		Permit	Allow	6.3+ supports Dynamic Flow Offload (4100/9300)
Trust	(SI, QoS, or ID) enabled	Permit	Fastpath	6.3+ supports Dynamic Flow Offload (4100/9300)
Trust	(SI, QoS, and ID) disabled	Trust	Fastpath	Static Flow Offload (4100/9300)
Monitor		Permit	Audit	Monitor Rule doesn't drop or permit traffic, but it generates a Connection Event. The packet is checked against subsequent rules and it is either allowed or dropped
Block with reset		Permit	Reset	When a packet matches Block with reset rule FTD sends a TCP Reset packet or an ICMP Type 3 Code 13 Destination Unreachable (Administratively filtered) message
Interactive Block		Permit	Bypass	Interactive Block Rule prompts the user that the destination is forbidden If bypassed, by default, the firewall allows to bypass the block for 600 seconds
Interactive Block with reset		Permit	Intreset	Same as Interactive Block with the addition of a TCP RST in case of non-web traffic

 **Nota:** a partir de la versión 6.3 del código de software FTD, la descarga de flujo dinámica puede descargar conexiones que cumplan criterios adicionales; por ejemplo, paquetes de confianza que requieran inspección de Snort. Consulte la sección **Descarga de conexiones grandes (flujos)** de la **Guía de configuración de Firepower Management Center** para obtener más detalles

### Información Relacionada

- [Reglas de control de acceso de FTD](#)
- [Políticas de prefiltro y prefiltrado de FTD](#)
- [Análisis de las capturas de firewall de Firepower para solucionar problemas de red de manera eficaz](#)

- [Trabajo con capturas de Firepower Threat Defense \(FTD\) y Packet Tracer](#)
- [Configuración del inicio de sesión en FTD mediante el FMC](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)
- [Descarga de conexiones grandes](#)

## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).