

# Fase 2 de Troubleshooting de Trayectoria de Datos de Firepower: Capa DAQ

## Contenido

[Introducción](#)

[Guía de la plataforma](#)

[Solución de problemas de la fase de Firepower DAQ](#)

[Captura del tráfico en la capa DAQ](#)

[Cómo omitir Firepower](#)

[SFR: Coloque el módulo Firepower en modo de solo supervisión](#)

[FTD \(todos\): coloque los conjuntos en línea en modo TAP](#)

[Uso de Packet Tracer para Resolver Problemas de Tráfico Simulado](#)

[SFR: ejecute Packet Tracer en ASA CLI](#)

[FTD \(todos\): ejecute el rastreador de paquetes en la CLI de FTD](#)

[Uso de Captura con Seguimiento para Resolver Problemas de Tráfico en Directo](#)

[FTD \(todos\): ejecución de captura con seguimiento en la GUI de FMC](#)

[Creación de una regla de ruta de acceso rápida previa al filtro en FTD](#)

[Datos que se deben proporcionar al TAC](#)

[Siguiente paso](#)

## Introducción

Este artículo forma parte de una serie de artículos que explican cómo resolver sistemáticamente los problemas de la ruta de datos en sistemas Firepower para determinar si los componentes de Firepower pueden estar afectando al tráfico. Consulte el [artículo Descripción general](#) para obtener información sobre la arquitectura de las plataformas Firepower y los enlaces a otros artículos de Troubleshooting de Trayectoria de Datos.

En este artículo, veremos la segunda etapa de la solución de problemas de la ruta de datos de Firepower: la capa DAQ (adquisición de datos).



## Guía de la plataforma

En la tabla siguiente se describen las plataformas tratadas en este artículo.

Nombre de código de la plataforma	Descripción	Aplicable Hardware Plataformas	Notas
SFR	Módulo ASA con Firepower Services	Serie ASA-5500-X	N/A

(SFR) instalado.

FTD (todos)	Se aplica a todas las plataformas de Firepower Threat Defense (FTD)	ASA-5500-X Series, plataformas NGFW virtuales, FPR-2100, FPR-9300, FPR-4100	N/A
FTD (sin SSP y FPR-2100)	Imagen FTD instalada en un ASA o una plataforma virtual	ASA-5500-X Series, plataformas NGFW virtuales, FPR-2100	
FTD (SSP)	FTD instalado como dispositivo lógico en un chasis basado en Firepower eXtensible Operative System (FXOS)	FPR-9300, FPR-4100	La serie 2100 no utiliza el administrador de chasis FXOS

## Solución de problemas de la fase de Firepower DAQ

La capa DAQ (adquisición de datos) es un componente de Firepower que traduce los paquetes a una forma que el snort puede entender. Inicialmente, maneja el paquete cuando se envía a snort. Por lo tanto, si los paquetes están ingresando pero no están egresando el dispositivo Firepower o la solución de problemas de ingreso de paquetes no produjo resultados útiles, la solución de problemas de DAQ puede ser útil.

## Captura del tráfico en la capa DAQ

Para obtener la indicación desde la que ejecutar la captura, primero debe conectarse mediante SSH a la dirección IP SFR o FTD.

**Nota:** En los dispositivos FPR-9300 y 4100, ingrese **connect ftd** primero, para terminar en el segundo > prompt. También puede ingresar SSH en la IP del administrador de chasis FXOS, luego ingrese **conectar la consola del módulo 1**, seguido de **conectar ftd**.

Este [artículo](#) explica cómo recopilar capturas de paquetes en el nivel de Firepower DAQ.

Observe cómo la sintaxis no es la misma que el comando **capture** utilizado en ASA, así como el lado LINA de la plataforma FTD. Este es un ejemplo de una captura de paquetes DAQ ejecutada desde un dispositivo FTD:

```
> system support capture-traffic
```

```
Please choose domain to capture traffic from:
```

```
0 - br1
```

```
1 - Router
```

```
2 - my-inline inline set
```

```
Selection? 2
```

```
Please specify tcpdump options desired.
```

```
(or enter '?' for a list of supported options)
```


```
Options: -s 1518 -w ct.pcap
```

```
> expert
```

```
admin@ciscoasa:~$ ls /ngfw/var/common/
```

```
ct.pcap
```

Como se ve en la captura de pantalla anterior, se escribió una captura en formato PCAP llamada ct.pcap en el directorio `/ngfw/var/common` (`/var/common` en la plataforma SFR). Estos archivos de captura pueden copiarse del dispositivo Firepower desde el mensaje `>` utilizando las instrucciones del [artículo](#) mencionado anteriormente.

Alternativamente, en Firepower Management Center (FMC) en Firepower versión 6.2.0 y posterior, navegue hasta **Dispositivos > Administración de dispositivos**. A continuación, haga clic en el botón  junto al dispositivo en cuestión, seguido de **Resolución de problemas avanzada > Descarga de archivos**.

A continuación, puede introducir el nombre del archivo de captura y hacer clic en Descargar.



## Cómo omitir Firepower

Si Firepower ve el tráfico, pero se ha determinado que los paquetes no están saliendo del dispositivo o que hay otro problema con el tráfico, el siguiente paso sería saltar la fase de inspección de Firepower para confirmar que uno de los componentes Firepower está descartando el tráfico. A continuación se muestra un desglose de la manera más rápida de tener tráfico que

sobrepasa Firepower en las diversas plataformas.

## SFR: Coloque el módulo Firepower en modo de solo supervisión

En el ASA que aloja el SFR, puede colocar el módulo SFR en modo de solo supervisión a través de la interfaz de línea de comandos (CLI) de ASA o el administrador adaptable de dispositivos de seguridad (ASDM) de Cisco. Esto hace que solamente se envíe una copia de los paquetes activos al módulo SFR.

Para colocar el módulo SFR en el modo de sólo supervisión a través de la CLI de ASA, primero se debe determinar el mapa de clase y el mapa de política utilizados para la redirección SFR ejecutando el comando **show service-policy sfr**.

```
# show service-policy sfr
```

```
Global policy:
```

```
Service-policy: global_policy
```

```
Class-map: sfr
```

```
SFR: card status Up, mode fail-open
```

```
packet input 10000, packet output 9900, drop 100, reset-drop 0
```

El resultado muestra que el mapa de política global\_policy está imponiendo la acción sfr fail-open en el mapa de clase "sfr".

**Nota:** "fail-close" es también un modo en el que el SFR puede ejecutarse, pero no se utiliza tan comúnmente ya que bloquea todo el tráfico si el módulo SFR está inactivo o no responde.

Para colocar el módulo SFR en el modo de sólo supervisión, puede ejecutar estos comandos para negar la configuración SFR actual e ingresar la configuración de sólo supervisión:

```
# configure terminal
```

```
(config)# policy-map global_policy
```

```
(config-pmap)# class sfr
```

```
(config-pmap-c)# no sfr fail-open
```

```
(config-pmap-c)# sfr fail-open monitor-only
```

```
INFO: The monitor-only mode prevents SFR from denying or altering traffic.
```

```
(config-pmap-c)# write memory
```

```
Building configuration...
```

Una vez que el módulo se ha colocado en modo de sólo supervisión, se puede verificar en el resultado **show service-policy sfr**.

```
# sh service-policy sfr
```

```
Global policy:
```

```
Service-policy: global_policy
```

```
Class-map: sfr
```

```
SFR: card status Up, mode fail-open monitor-only
```

```
packet input 0, packet output 100, drop 0, reset-drop 0
```

**Nota:** Para volver a colocar el módulo SFR en modo en línea, ejecute el comando **no sfr fail-open monitor-only** desde el mensaje **(config-pmap-c)#** que se muestra arriba, seguido por el

comando **sfr {fail-open | fail-close}** que originalmente estaba allí.

Alternativamente, puede colocar el módulo en solo supervisión a través del ASDM navegando a **Configuración > Firewall > Reglas de política de servicio**. A continuación, haga clic en la regla en cuestión. A continuación, vaya a la página **Acciones de Regla** y haga clic en la ficha **Inspección de FirePOWER de ASA**. Una vez allí, se puede seleccionar **Monitor-only**.

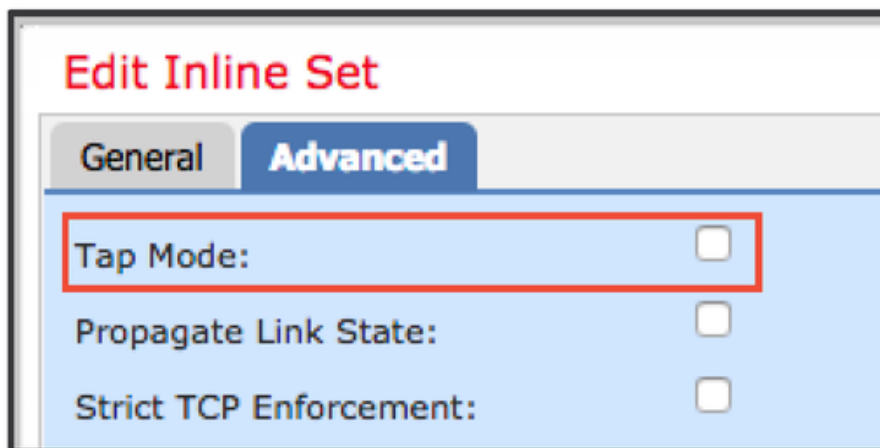
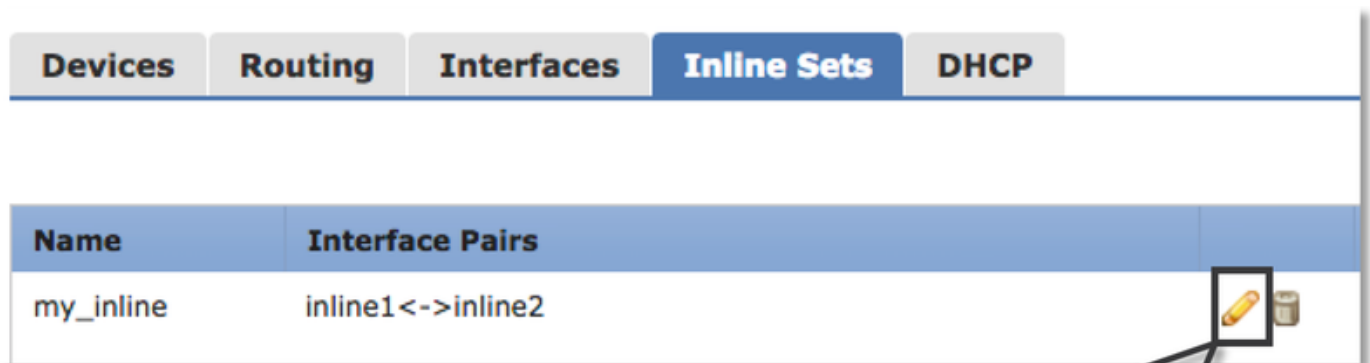
Si el problema de tráfico permanece incluso después de que se haya confirmado que el módulo SFR está en modo de sólo supervisión, el módulo Firepower no está causando el problema. El trazador de paquetes se puede ejecutar para diagnosticar problemas en el nivel ASA.

Si el problema ya no persiste, el siguiente paso sería resolver los problemas de los componentes de software Firepower.

## FTD (todos): coloque los conjuntos en línea en modo TAP

Si el tráfico pasa por pares de interfaces configurados en conjuntos en línea, el conjunto en línea se puede colocar en el modo TAP. Esto hace que Firepower no tome acción en el paquete activo. No se aplica al router o al modo transparente sin conjuntos en línea ya que el dispositivo debe modificar los paquetes antes de enviarlos al salto siguiente y no se puede colocar en el modo de omisión sin descartar el tráfico. Para el modo ruteado y transparente sin conjuntos en línea, continúe con el paso del trazador de paquetes.

Para configurar el modo TAP desde la interfaz de usuario de FMC, navegue hasta **Dispositivos > Administración de dispositivos** y, a continuación, edite el dispositivo en cuestión. En la pestaña **Conjuntos en línea**, desmarque la opción **Modo TAP**.



Si el modo TAP resuelve el problema, el siguiente paso sería resolver los problemas de los

componentes del software Firepower.

Si el modo TAP no resuelve el problema, el problema estaría fuera del software Firepower. El trazador de paquetes se puede utilizar entonces para diagnosticar el problema.

## Uso de Packet Tracer para Resolver Problemas de Tráfico Simulado

Packet Tracer es una utilidad que puede ayudar a identificar la ubicación de una pérdida de paquetes. Es un simulador, por lo que realiza un seguimiento de un paquete artificial.

### SFR: ejecute Packet Tracer en ASA CLI

Este es un ejemplo de cómo ejecutar packet-tracer en ASA CLI para el tráfico SSH. Para obtener información más detallada sobre la sintaxis del comando packet tracer, consulte esta [sección](#) en la Guía de Referencia de Comandos de la Serie ASA.

```
asa# packet-tracer input inside tcp 192.168.62.60 10000 10.10.10.10 ssh

Phase: 1
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 2
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 10.151.37.1 using egress ifc outside

Phase: 3
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 4
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 5
Type: SFR
Subtype:
Result: ALLOW
Config:
class-map inspection_default
match any
policy-map global_policy
class inspection_default
sfr fail-open
service-policy global_policy global
Additional Information:
```

```
Phase: 6
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
class-map inspection_default
match any
policy-map global_policy
class inspection_default
inspect icmp
service-policy global_policy global
Additional Information:

Phase: 7
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 9
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 756, packet dispatched to next module

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow
```

En el ejemplo anterior, vemos tanto el módulo ASA como el módulo SFR que permiten los paquetes, así como información útil sobre cómo el ASA manejaría el flujo de paquetes.

## FTD (todos): ejecute el rastreador de paquetes en la CLI de FTD

En todas las plataformas FTD, el comando packet tracer se puede ejecutar desde la CLI FTD.

```
> packet-tracer input inside tcp 192.168.62.60 10000 10.10.10.10 ssh

Phase: 1
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 2
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 192.168.100.1 using egress ifc outside

Phase: 3
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_global
access-list CSM_FW_ACL_advanced permit ip any any rule-id 268434433
access-list CSM_FW_ACL_remark rule-id 268434433: ACCESS POLICY:
My_AC_Policy - Mandatory
access-list CSM_FW_ACL_remark rule-id 268434433: L7 RULE: Block urls
Additional Information:
This packet will be sent to snort for additional processing where a verdict will
be reached

Phase: 4
Type: CONN-SETTINGS
Subtype:
Result: ALLOW
Config:
class-map class-default
match any
policy-map global_policy
class class-default
set connection advanced-options UM_STATIC_TCP_MAP
service-policy global_policy global
Additional Information:

Phase: 5
Type: NAT
Subtype:
Result: ALLOW
Config:
object network 62_network
nat (inside,outside) dynamic interface
Additional Information:
Dynamic translate 192.168.62.60/10000 to 192.168.100.51/10000

Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 9
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 10
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 612016, packet dispatched to next module
```



```
Phase: 11
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Config:
Additional Information:
Application: 'SNORT Inspect'
```

```
Phase: 12
Type: SNORT
Subtype:
Result: DROP
Config:
Additional Information:
Snort Trace:
Packet: TCP, SYN, seq 1821549761
Reputation: packet blacklisted, drop
Snort: processed decoder alerts or actions queue, drop
IPS Event: gid 136, sid 1, drop
Snort detect_drop: gid 136, sid 1, drop
NAP id 1, IPS id 0, Verdict BLACKLIST, Blocked by Reputation
Snort Verdict: (black-list) black list this flow
```

En este ejemplo, packet tracer muestra la razón de la caída. En este caso, es la lista negra de IP dentro de la función de inteligencia de seguridad en Firepower que bloquea el paquete. El siguiente paso sería resolver los problemas del componente de software Firepower individual que causa la caída.

## Uso de Captura con Seguimiento para Resolver Problemas de Tráfico en Directo

El tráfico en directo también se puede rastrear a través de la función de captura con seguimiento, que está disponible en todas las plataformas a través de la CLI. A continuación se muestra un ejemplo de cómo ejecutar una captura con seguimiento contra el tráfico SSH.

```
> capture ssh_traffic trace interface inside match tcp any any eq 22
> show capture ssh_traffic

7 packets captured

 1: 01:17:38.498906 192.168.62.70.48560 > 10.83.180.173.22: S 4250994241:4250994241(0) win 29200 <mss 1460,sackOK,timestamp 1045829951
0,nop,wscale 7>
 2: 01:17:38.510898 10.83.180.173.22 > 192.168.62.70.48560: S 903999422:903999422(0) ack 4250994242 win 17896 <mss 1380,sackOK,timestamp
513898266 1045829951,nop,wscale 7>
 3: 01:17:38.511402 192.168.62.70.48560 > 10.83.180.173.22: . ack 903999423 win 229 <nop,nop,timestamp 1045829956 513898266>
 4: 01:17:38.511982 192.168.62.70.48560 > 10.83.180.173.22: P 4250994242:4250994283(41) ack 903999423 win 229 <nop,nop,timestamp
1045829957 513898266>
 5: 01:17:38.513294 10.83.180.173.22 > 192.168.62.70.48560: . ack 4250994283 win 140 <nop,nop,timestamp 513898268 1045829957>
 6: 01:17:38.528125 10.83.180.173.22 > 192.168.62.70.48560: P 903999423:903999444(21) ack 4250994283 win 140 <nop,nop,timestamp 513898282
1045829957>
 7: 01:17:38.528613 192.168.62.70.48560 > 10.83.180.173.22: . ack 903999444 win 229 <nop,nop,timestamp 1045829961 513898282>
```



```
> show capture ssh_traffic packet-number 4 trace

7 packets captured

4: 01:17:38.511982 192.168.62.70.48560 > 10.83.180.173.22: P
4250994242:4250994283(41) ack 903999423 win 229 <nop,nop,timestamp
1045829957 513898266>
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3
Type: FLOW-LOOKUP
Subtype:
Result: ALLOW
Config:
Additional Information:
Found flow with id 626406, using existing flow

Phase: 4
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Config:
Additional Information:
Application: 'SNORT Inspect'
```

```
Phase: 5
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Trace:
Packet: TCP, ACK, seq 4250994242, ack 903999423
AppID: service SSH (846), application unknown (0)
Firewall: starting rule matching, zone 1 -> 2, geo 0 -> 0, vlan 0, sgt 65535, user 2, icmpType 0, icmpCode 0
Firewall: trust/fastpath rule, id 268435458, allow
NAP id 1, IPS id 0, Verdict WHITELIST
Snort Verdict: (fast-forward) fast forward this flow


Result:
input-interface: inside
input-status: up
input-line-status: up
Action: allow
```

En este ejemplo, se rastreó el cuarto paquete de la captura, ya que éste es el primer paquete con datos de la aplicación definidos. Como se muestra, el paquete termina siendo blanqueado por el snort, lo que significa que no es necesaria una inspección adicional del snort para el flujo y se permite en general.

Para obtener más información sobre la captura con sintaxis de seguimiento, consulte esta [sección](#) en la Guía de Referencia de Comandos de la Serie ASA.

## FTD (todos): ejecución de captura con seguimiento en la GUI de FMC

En las plataformas FTD, la captura con seguimiento se puede ejecutar en la interfaz de usuario de FMC. Para acceder a la utilidad, navegue hasta **Dispositivos > Administración de dispositivos**.

A continuación, haga clic en el botón  junto al dispositivo en cuestión, seguido de **Resolución de problemas avanzada > Captura con seguimiento**.

A continuación se muestra un ejemplo de cómo ejecutar una captura con seguimiento a través de la GUI.

Clicking **Add Capture** button will display this popup window

Name	Interface	Type	Trace	Buffer Mode	Buffer Size	Packet Length	Buffer Status	Protocol	Source	Destination	Status
Test	Inside	raw-data	✓	524288	1518	Capturing	TCP	192.168.1.200	any	Running	

View of all current captures

```

Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 3
Type: FLOW-LOOKUP
Subtype:
Result: ALLOW
Config:
Additional Information:
Found flow with id 2672128, using existing flow

Phase: 4
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Config:
Additional Information:
Application: 'SNORT inspect'

Phase: 5
Type: SNORT
Subtype:
Result: DROP
Config:
Additional Information:
Snort Verdict: (block-packet) drop this packet
Result:
Input-interfaces: Inside
Input-status: up

```

Example output shows the packet was blocked by Snort

Si la captura con seguimiento muestra la causa de la caída del paquete, el siguiente paso sería resolver los problemas de los componentes de software individuales.

Si no muestra claramente la causa del problema, el siguiente paso sería la ruta rápida del tráfico.

## Creación de una regla de ruta de acceso rápida previa al filtro en FTD

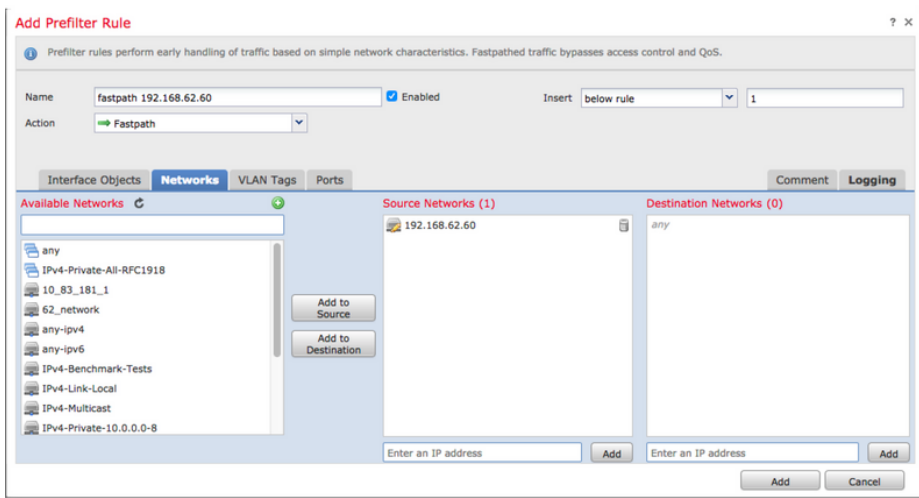
En todas las plataformas FTD, existe una política de prefiltro, que se puede utilizar para desviar el tráfico de la inspección de Firepower (snort).

En el FMC, esto se encuentra en **Políticas > Control de acceso > Prefiltro**. No se puede editar la política prefiltro predeterminada, por lo que será necesario crear una directiva personalizada.

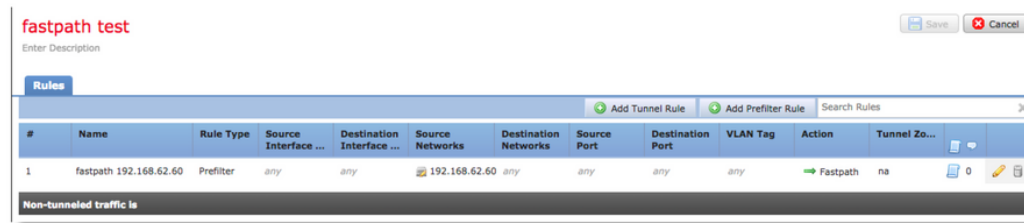
Después, la política de prefiltro recién creada debe asociarse a la política de control de acceso.

Esto se configura en la ficha Avanzadas de la política de control de acceso en la sección **Configuración de política de prefiltro**.

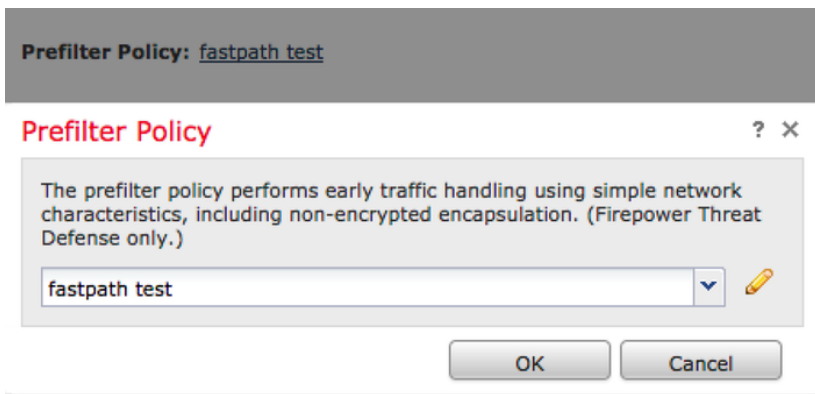
A continuación se muestra un ejemplo de cómo crear una regla Fastpath dentro de una política de prefiltro y verificar el recuento de visitas.



Clicking **Add Prefilter Rule** button will display this popup window.



View of all rules in the **fastpath test** Prefilter policy



From AC policy make sure the Prefilter Policy is set to the custom Prefilter Policy

View of connection events matching prefilter rule

First Packet	Last Packet	Action	Reason	Initiator IP	Responder IP	Source Port / ICMP Type	Destination Port / ICMP Code	Prefilter Policy	Tunnel/Prefilter Rule
2017-05-15 16:05:14	2017-05-15 16:05:14	Fastpath		192.168.62.60	10.83.180.173	48480 / tcp	22 (ssh) / tcp	fastpath.test	fastpath 192.168.62.60

[Haga clic aquí](#) para obtener más detalles sobre el funcionamiento y la configuración de las políticas de prefiltro.

Si al agregar una política de prefiltro se resuelve el problema de tráfico, la regla se puede dejar en su lugar si se desea. Sin embargo, no se realiza ninguna otra inspección de ese flujo. Será necesario llevar a cabo la resolución de problemas del software Firepower.

Si la adición de la política de prefiltro no resuelve el problema, el paquete con el paso de seguimiento se puede ejecutar de nuevo para rastrear la nueva trayectoria del paquete.

## Datos que se deben proporcionar al TAC

Datos	Instrucciones
Resultados del comando	Consulte este artículo para obtener instrucciones
Capturas de paquetes	Para ASA/LINA: <a href="https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation/asa-00.html">https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation/asa-00.html</a> Para Firepower: <a href="http://www.cisco.com/c/en/us/support/docs/security/sourcefire-firepower-8000/sourcefire-00.html">http://www.cisco.com/c/en/us/support/docs/security/sourcefire-firepower-8000/sourcefire-00.html</a>
Salida 'show tech' de ASA	Inicie sesión en ASA CLI y guarde la sesión de terminal en un registro. Ingrese el comando <code>show tech</code> de salida de la sesión de terminal al TAC. Este archivo se puede guardar en disco o en un sistema de almacenamiento externo con el comando <code>show tech   redirect disk0:/show_tech.log</code>
Solución de problemas de archivo del dispositivo Firepower que inspecciona el tráfico	<a href="http://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technical-topics/117663-technical-topics.html">http://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technical-topics/117663-technical-topics.html</a>

## Siguiente paso

Si se ha determinado que un componente de software Firepower es la causa del problema, el siguiente paso sería descartar sistemáticamente cada componente, empezando por la inteligencia de seguridad.

Haga clic [aquí](#) para continuar con la siguiente guía.