

Fase 2 da solução de problemas de caminho de dados do Firepower: Camada DAQ

Contents

[Introduction](#)

[Guia da plataforma](#)

[Troubleshooting da Fase DAQ do Firepower](#)

[Captura de tráfego na camada DAQ](#)

[Como ignorar o Firepower](#)

[SFR - Coloque o módulo Firepower no modo somente de monitor](#)

[FTD \(todos\) - Coloque Conjuntos em linha no modo TAP](#)

[Usando o Packet Tracer para Solucionar Problemas de Tráfego Simulado](#)

[SFR - Execute o Packet Tracer na CLI do ASA](#)

[FTD \(todos\) - Execute o packet tracer na CLI do FTD](#)

[Usando Captura com Rastreamento para Solucionar Problemas de Tráfego ao Vivo](#)

[FTD \(todos\) - Execução da captura com rastreamento na GUI do FMC](#)

[Criação de uma regra de caminho rápido de pré-filtro no FTD](#)

[Dados a fornecer ao TAC](#)

[Próxima etapa](#)

Introduction

Este artigo faz parte de uma série de artigos que explicam como solucionar problemas sistematicamente no caminho de dados em sistemas Firepower para determinar se os componentes do Firepower podem estar afetando o tráfego. Consulte o [artigo Visão geral](#) para obter informações sobre a arquitetura das plataformas Firepower e links para outros artigos de solução de problemas de caminho de dados.

Neste artigo, examinaremos o segundo estágio da solução de problemas do caminho de dados do Firepower: a Camada DAQ (Aquisição de Dados).



Guia da plataforma

A tabela a seguir descreve as plataformas abrangidas por este artigo.

Nome do código da plataforma	Descrição	Aplicável Hardware Plataformas	Notas
SFR	Módulo ASA com Firepower Services (SFR) instalado.	ASA-5500-X Series	N/A

FTD (todos)	Aplica-se a todas as plataformas Firepower Threat Defense (FTD)	ASA-5500-X Series, plataformas NGFW virtuais, FPR-2100, FPR-9300, FPR-4100	N/A
FTD (não SSP e FPR-2100)	Imagem FTD instalada em um ASA ou uma plataforma virtual	ASA-5500-X Series, plataformas NGFW virtuais, FPR-2100	N/A
FTD (SSP)	FTD instalado como um dispositivo lógico em um chassi baseado no Firepower eXtensible Operative System (FXOS)	FPR-9300, FPR-4100	A série 2100 não usa o FXOS Chassis Manager

Troubleshooting da Fase DAQ do Firepower

A camada de DAQ (aquisição de dados) é um componente do Firepower que converte pacotes em uma forma que o snort pode entender. Ele inicialmente trata o pacote quando é enviado para snort. Portanto, se os pacotes estão entrando, mas não estão entrando no Firepower appliance ou se a solução de problemas de entrada de pacotes não produziu resultados úteis, a solução de problemas de DAQ pode ser útil.

Captura de tráfego na camada DAQ

Para obter um prompt para executar a captura, primeiro é necessário conectar-se usando SSH ao endereço IP do SFR ou FTD.

Note: Nos dispositivos FPR-9300 e 4100, insira **connect ftd** primeiro para terminar no segundo **>** prompt. Você também pode usar SSH no IP do FXOS Chassis Manager e, em seguida, inserir o **console do módulo de conexão 1**, seguido de **conectar ftd**.

Este [artigo](#) explica como coletar capturas de pacotes no nível de DAQ do Firepower.

Observe como a sintaxe não é a mesma do comando **capture** usado no ASA, assim como o lado LINA da plataforma FTD. Aqui está um exemplo de uma execução de captura de pacote DAQ de um 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 visto na captura de tela acima, uma captura no formato PCAP chamada ct.pcap foi gravada no diretório `/ngfw/var/common` (`/var/common` na plataforma SFR). Esses arquivos de captura podem ser copiados do dispositivo Firepower do prompt `>` usando as instruções no [artigo](#) mencionado acima.

Como alternativa, no Firepower Management Center (FMC) no Firepower versão 6.2.0 e posterior, navegue para **Dispositivos > Gerenciamento de dispositivos**. Em seguida, clique no botão  ao lado do dispositivo em questão, seguido por **Advanced Troubleshooting > File Download**.

Você pode inserir o nome do arquivo de captura e clicar em Download.



Como ignorar o Firepower

Se o Firepower estiver vendo o tráfego, mas foi determinado que os pacotes não estão egressando o dispositivo ou que há outro problema com o tráfego, a próxima etapa seria ignorar a fase de inspeção do Firepower para confirmar que um dos componentes do Firepower está descartando o tráfego. Veja a seguir uma análise da maneira mais rápida de fazer com que o

tráfego ignore o Firepower em várias plataformas.

SFR - Coloque o módulo Firepower no modo somente de monitor

No ASA que hospeda o SFR, você pode colocar o módulo SFR no modo somente de monitor através da Interface de Linha de Comando (CLI - Command Line Interface) do ASA ou do Cisco Adaptive Security Device Manager (ASDM - Gerenciador de Dispositivos de Segurança Adaptiva). Isso faz com que apenas uma cópia dos pacotes ao vivo seja enviada ao módulo SFR.

Para colocar o módulo SFR no modo somente de monitoramento através da CLI do ASA, o mapa de classe e o mapa de política usados para redirecionamento do SFR devem primeiro ser determinados executando o 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
```

A saída mostra que o mapa de política `global_policy` está aplicando a ação `fail-open` do `sfr` no mapa de classe "sfr".

Note: "fail-close" é também um modo no qual o SFR pode ser executado, mas não é tão usado, pois bloqueia todo o tráfego se o módulo SFR estiver inativo ou sem resposta.

Para colocar o módulo SFR no modo somente de monitor, você pode emitir estes comandos para negar a configuração atual do SFR e inserir a configuração somente de monitor:

```
# 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...
```

Depois que o módulo tiver sido colocado no modo somente monitor, ele poderá ser verificado na saída **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
```

Note: Para colocar o módulo SFR de volta no modo inline, emita o comando `no sfr fail-open monitor-only` no prompt `(config-pmap-c)#` mostrado acima, seguido pelo `sfr {fail-open comando | fail-close}` originalmente presente.

Como alternativa, você pode colocar o módulo somente no monitor via ASDM navegando para **Configuração > Firewall > Regras de Política de Serviço**. Em seguida, clique na regra em questão. Em seguida, acesse a página **Ações da regra** e clique na guia **Inspeção do FirePOWER ASA**. Assim que estiver lá, o **monitor apenas** poderá ser selecionado.

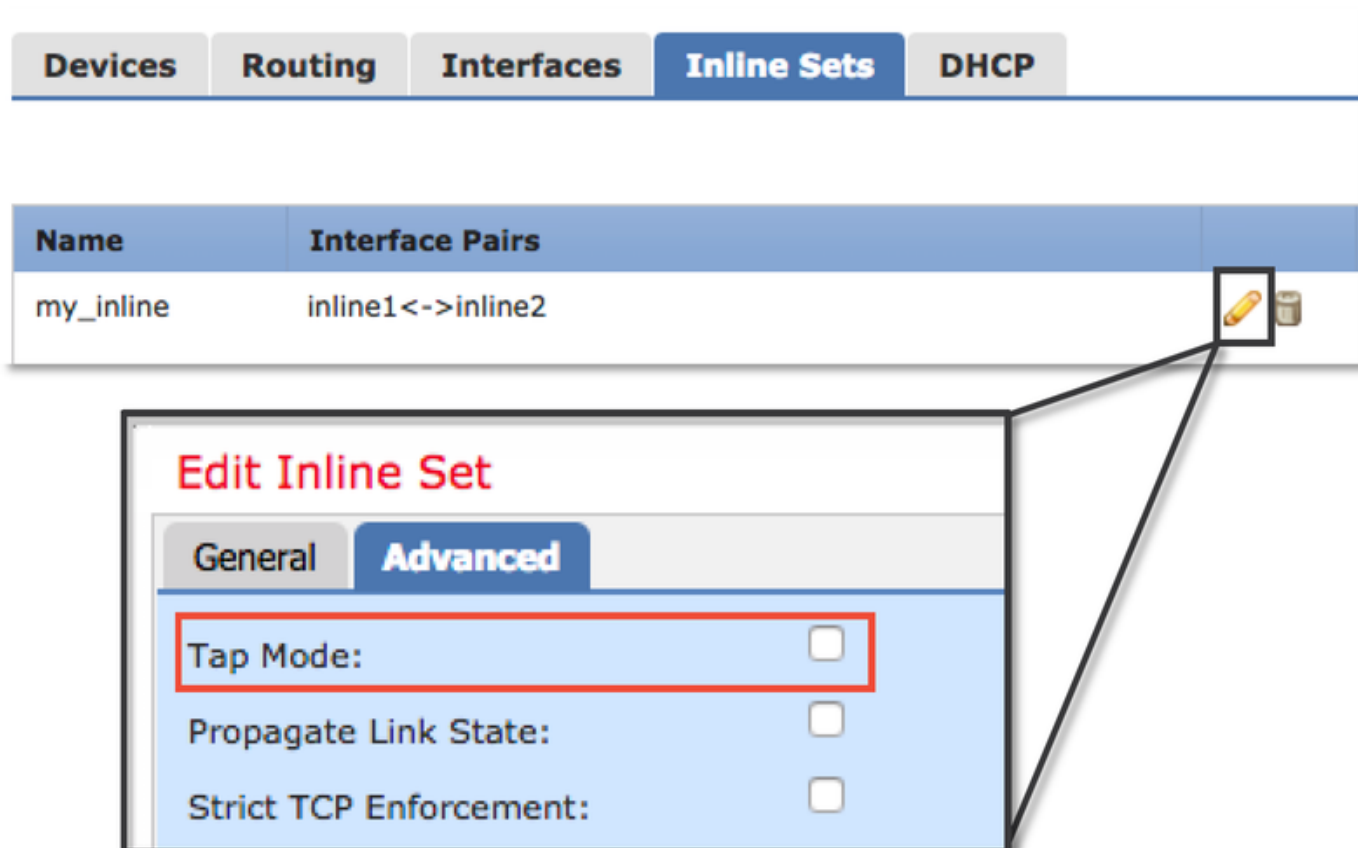
Se o problema de tráfego continuar mesmo depois que o módulo SFR tiver sido confirmado para estar no modo somente monitor, o módulo Firepower não está causando o problema. O Packet Tracer pode então ser executado para diagnosticar mais os problemas no nível do ASA.

Se o problema não continuar, a próxima etapa seria solucionar os problemas dos componentes do software Firepower.


FTD (todos) - Coloque Conjuntos em linha no modo TAP

Se o tráfego estiver passando por pares de interface configurados em conjuntos em linha, o conjunto em linha poderá ser colocado no modo TAP. Isso faz com que o Firepower não tome uma ação no pacote ao vivo. Ele não se aplica ao modo de roteador ou transparente sem conjuntos de linha, pois o dispositivo deve modificar os pacotes antes de enviá-los para o próximo salto e não pode ser colocado em um modo de desvio sem descartar o tráfego. Para o modo roteado e transparente sem conjuntos inline, continue com a etapa packet tracer.

Para configurar o modo TAP na Interface de Usuário (UI) da FMC, navegue até **Dispositivos > Gerenciamento de Dispositivos** e edite o dispositivo em questão. Na guia **Inline Sets**, marque a opção para **TAP Mode**.



The screenshot shows the FMC configuration interface. At the top, there are tabs for 'Devices', 'Routing', 'Interfaces', 'Inline Sets', and 'DHCP'. Below these is a table with the following content:

Name	Interface Pairs	
my_inline	inline1<->inline2	

An inset window titled 'Edit Inline Set' is shown, with the 'Advanced' tab selected. The 'Tap Mode' checkbox is checked and highlighted with a red box. Other options include 'Propagate Link State' and 'Strict TCP Enforcement', both of which are unchecked.

Se o modo TAP resolver o problema, a próxima etapa seria solucionar os componentes do software Firepower.

Se o modo TAP não resolver o problema, o problema estará fora do software Firepower. O Packet

Tracer pode ser usado para diagnosticar o problema.

Usando o Packet Tracer para Solucionar Problemas de Tráfego Simulado

O Packet Tracer é um utilitário que pode ajudar a identificar a localização de um descarte de pacote. É um simulador, portanto, executa um rastreamento de um pacote artificial.

SFR - Execute o Packet Tracer na CLI do ASA

Aqui está um exemplo de como executar o packet-tracer no ASA CLI para tráfego SSH. Para obter informações mais detalhadas sobre a sintaxe do comando packet tracer, consulte esta [seção](#) no guia de referência de comando da série 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
```

No exemplo acima, vemos o módulo ASA e o módulo SFR permitindo os pacotes, bem como informações úteis sobre como o ASA lidaria com o fluxo do pacote.

FTD (todos) - Execute o packet tracer na CLI do FTD

Em todas as plataformas FTD, o comando packet tracer pode ser executado a partir da CLI do

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
```

Neste exemplo, o packet tracer mostra o motivo da queda. Nesse caso, é a lista negra de IP dentro do recurso Security Intelligence no Firepower que bloqueia o pacote. A próxima etapa seria solucionar os problemas do componente de software Firepower individual que está causando a queda.

Usando Captura com Rastreamento para Solucionar Problemas de Tráfego ao Vivo

O tráfego ao vivo também pode ser rastreado através do recurso de captura com rastreamento, que está disponível em todas as plataformas via CLI. Abaixo está um exemplo de execução de uma captura com rastreamento em relação ao tráfego 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
```

Neste exemplo, o quarto pacote na captura foi rastreado, pois esse é o primeiro pacote com dados de aplicativo definidos. Como mostrado, o pacote acaba sendo whitelisted pelo snort, o que significa que nenhuma inspeção de snort adicional é necessária para o fluxo, e é permitida em geral.

Para obter mais informações sobre a captura com sintaxe de rastreamento, consulte esta [seção](#) no Guia de referência de comando da série ASA.

FTD (todos) - Execução da captura com rastreamento na GUI do FMC

Nas plataformas FTD, a captura com rastreamento pode ser executada na IU do FMC. Para acessar o utilitário, navegue até **Dispositivos > Gerenciamento de dispositivos**.

Em seguida, clique no botão  ao lado do dispositivo em questão, seguido por **Advanced Troubleshooting > Capture w/Trace**.

Abaixo está um exemplo de como executar uma captura com rastreamento via GUI.

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

Name	Interface	Type	Trace	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

Se a captura com rastreamento mostrar a causa da queda do pacote, a próxima etapa seria solucionar os problemas dos componentes individuais do software.

Se ele não mostrar claramente a causa do problema, a próxima etapa será o caminho rápido do tráfego.

Criação de uma regra de caminho rápido de pré-filtro no FTD

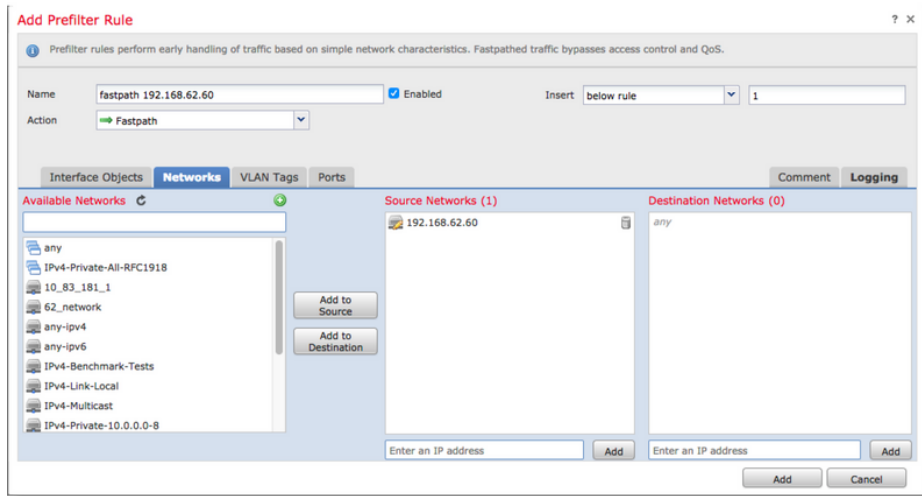
Em todas as plataformas FTD, há uma política de pré-filtro, que pode ser usada para desviar o tráfego da inspeção do Firepower (snort).

No FMC, isso é encontrado em **Políticas > Controle de acesso > Prefiltro**. Não é possível editar a política de pré-filtro predefinida, pelo que será necessário criar uma política personalizada.

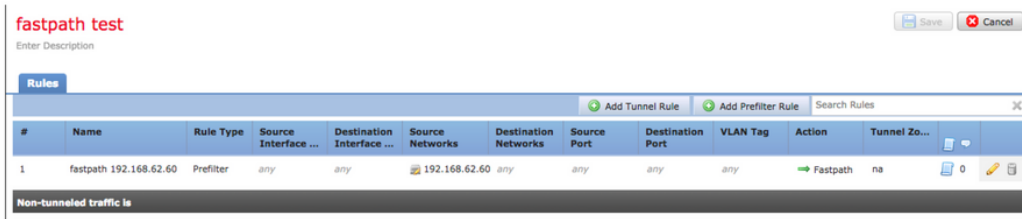
Depois, a política de pré-filtro recém-criada precisa ser associada à política de controle de acesso. Isso é configurado na guia Avançado da Política de controle de acesso na seção

Configurações de política de pré-filtro.

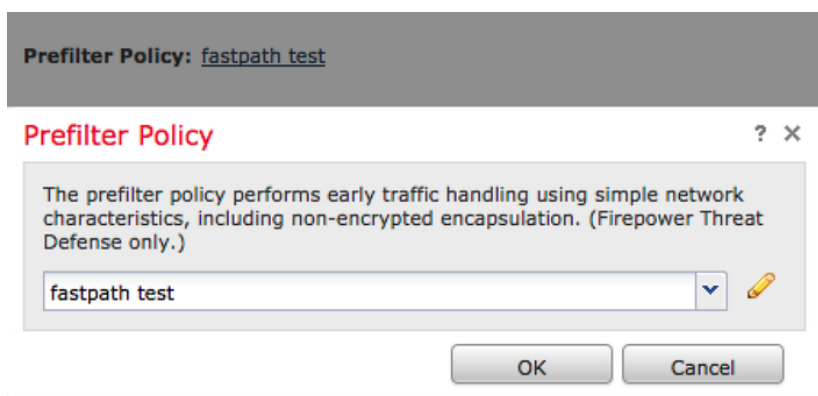
Abaixo está um exemplo de como criar uma regra de Fastpath em uma política de pré-filtro e verificar a contagem de ocorrências.



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

[Clique aqui](#) para obter mais detalhes sobre a operação e a configuração das Políticas de pré-filtro.

Se a adição de uma política de pré-filtro resolver o problema de tráfego, a regra pode ser mantida no lugar, se desejado. No entanto, não é efetuada qualquer nova inspeção a esse fluxo. A solução de problemas adicional do software Firepower precisará ser executada.

Se a adição da política de pré-filtro não resolver o problema, o pacote com etapa de rastreamento pode ser executado novamente para rastrear o novo caminho do pacote.

Dados a fornecer ao TAC

Dados	Instruções
Saídas de comando	Consulte este artigo para obter instruções
Capturas de pacotes	Para ASA/LINA: https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-asa-00.html Para Firepower: http://www.cisco.com/c/en/us/support/docs/security/sourcefire-firepower-8000-sourcefire-00.html
Saída 'show tech' do ASA	Faça login no ASA CLI e salve a sessão do terminal em um log. Digite o comando show tech e salve a sessão de terminal ao TAC. Esse arquivo pode ser salvo em disco ou em um sistema de armazenamento externo com esse comando: show tech redirecionar disco0:/show_tech.log
Solucionar problemas do dispositivo Firepower que inspeciona o tráfego	http://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technot

Próxima etapa

Se for determinado que um componente de software Firepower é a causa do problema, a próxima etapa seria excluir sistematicamente cada componente, começando pela inteligência de segurança.

Clique [aqui](#) para continuar com o próximo guia.