Esclarecer as ações da regra de política de controle de acesso do Firepower Threat Defense

Contents

Introduction

Este documento descreve as várias ações disponíveis no Firepower Threat Defense (FTD), na Access Control Policy (ACP) e na política de pré-filtro.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Transferência de fluxo
- Capturas de pacotes em dispositivos Firepower Threat Defense
- Packet Tracer e captura com opção de rastreamento nos dispositivos do FTD

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Firepower 4110 Threat Defense versão 6.4.0 (build 113) e 6.6.0 (build 90)
- Firepower Management Center (FMC) versão 6.4.0 (build 113) e 6.6.0 (build 90)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Produtos Relacionados

Este documento também pode ser usado com as seguintes versões de hardware e software:

- 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), Kernel-based Virtual Machine (KVM)
- Módulos de roteador de serviços integrados (ISR)
- FTD versão de software 6.1.x e posteriores

> **Note**: A transferência de fluxo é permitida somente nas instâncias nativas das aplicações do ASA e do FTD e nas plataformas FPR4100 e FPR9300. As instâncias de contêiner do FTD não permitem a transferência de fluxo.

Informações de Apoio

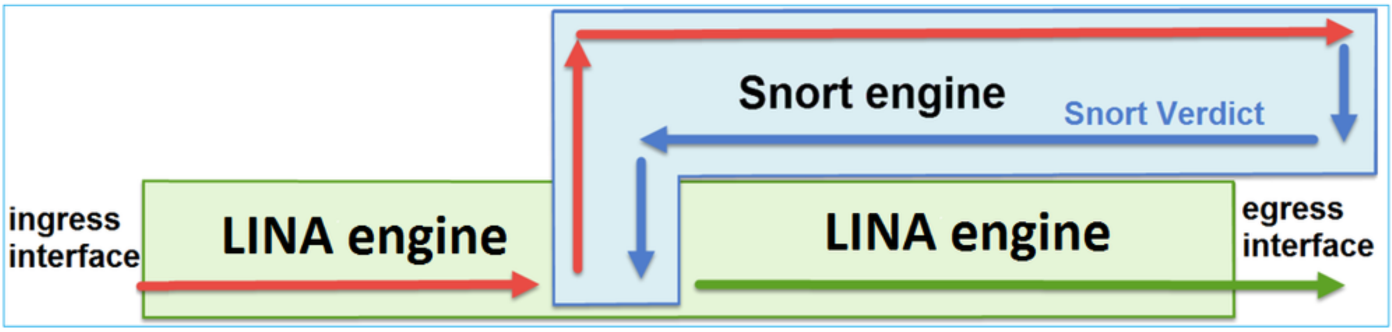
A operação em segundo plano de cada ação é examinada junto com sua interação com outros recursos como o Flow Offload e protocolos que abrem conexões secundárias.

O FTD é uma imagem de software unificada que consiste em dois mecanismos principais:

- Mecanismo LINA

- Mecanismo Snort

Esta figura mostra como os dois mecanismos interagem:



- Um pacote é inserido na interface de entrada e tratado pelo mecanismo LINA
- Se exigido pela política do FTD, o pacote será inspecionado pelo mecanismo Snort
- O mecanismo Snort retorna um veredito (lista de permissão ou de bloqueio) para o pacote
- O mecanismo LINA descarta ou encaminha o pacote de acordo com a conclusão do Snort

Como a ACP é implantada

A política do FTD é configurada no FMC, quando o gerenciamento externo (remoto) é usado, ou no Firepower Device Manager (FDM), quando o gerenciamento local é usado. Em ambos os cenários, a ACP é implantada como:

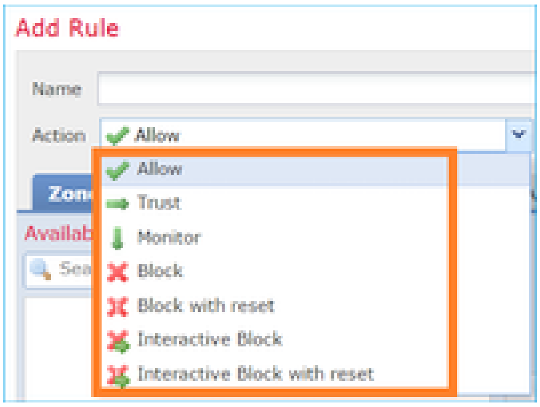
- Uma lista de controle de acesso (ACL - Access Control List) global chamada CSM_FW_ACL_ ao mecanismo LINA do FTD
- Regras de controle de acesso (AC) no arquivo /ngfw/var/sf/detection_engines/<UUID>/ngfw.rules para o mecanismo Snort do FTD

Configurar

Ações disponíveis da ACP

A ACP do FTD contém uma ou mais regras e cada regra pode ter uma destas ações conforme mostrado na imagem:

- **Allow**
- **Trust**
- **Monitor**
- **Block**
- **Block with reset**
- **Interactive Block**
- **Interactive Block with reset**



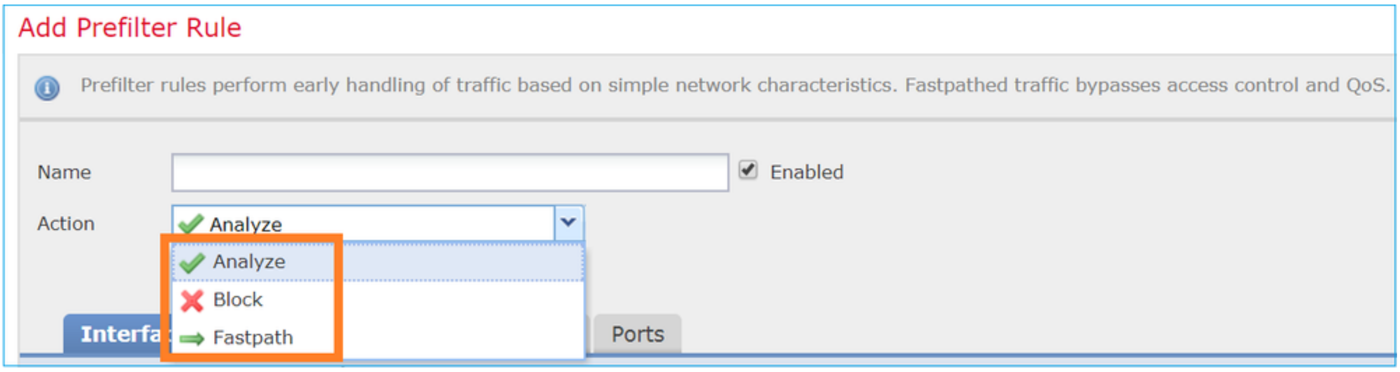
Add Rule

Name

Action: Allow

- Allow
- Trust
- Monitor
- Block
- Block with reset
- Interactive Block
- Interactive Block with reset

Da mesma forma, uma política de pré-filtro pode conter uma ou mais regras, e as ações possíveis são mostradas na imagem:



Add Prefilter Rule

Prefilter rules perform early handling of traffic based on simple network characteristics. Fastpathed traffic bypasses access control and QoS.

Name ☑ Enabled

Action: Analyze

- Analyze
- Block
- Fastpath

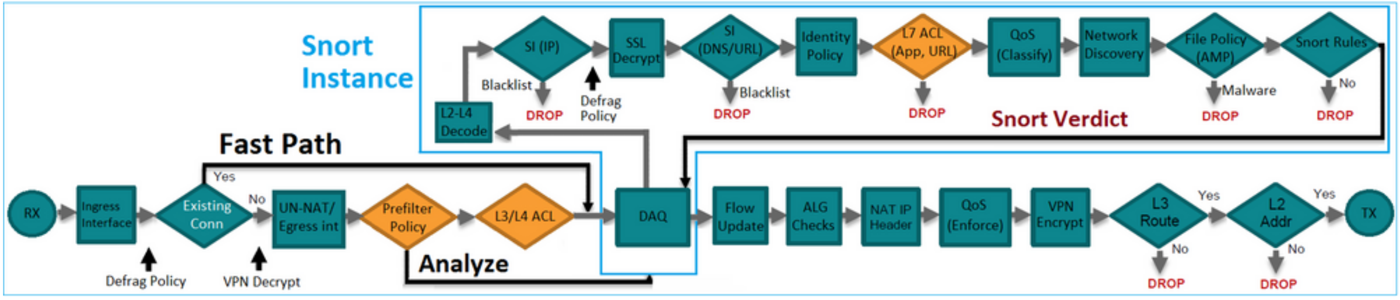
Como a ACP e a política de pré-filtro interagem

A política de pré-filtro foi introduzida na versão 6.1 e tem duas finalidades principais:

1. Permite a inspeção do tráfego em túnel, em que o mecanismo LINA do FTD verifica o cabeçalho IP externo, enquanto o mecanismo Snort verifica o cabeçalho IP interno. Mais especificamente, no caso de tráfego em túnel (por exemplo, GRE), as regras na Política de pré-filtro sempre atuam sobre o **outer headers**, enquanto as regras no ACP são sempre aplicáveis às sessões internas **(inner headers)**. O tráfego em túnel se refere a estes protocolos:

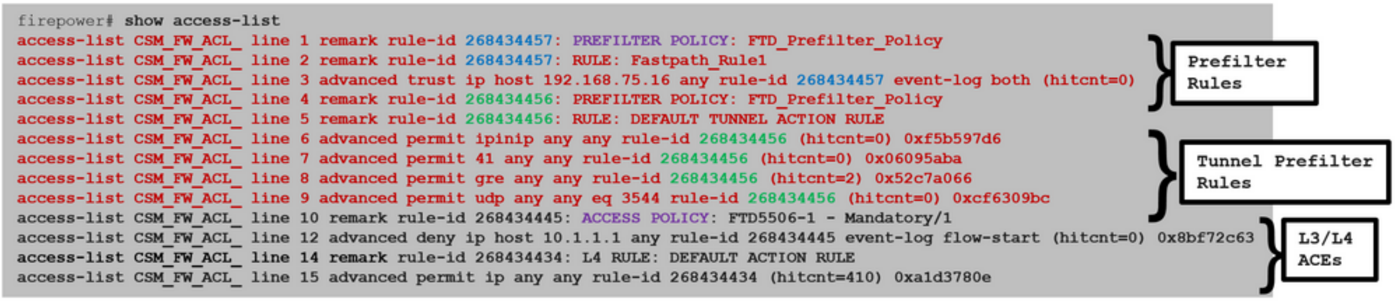
- GRE
- IP em IP
- IPv6 em IP
- Porta 3544 Teredo

2. Ele fornece o Early Access Control (EAC), que permite que o fluxo ignore completamente o mecanismo Snort, como mostrado na imagem.



As Regras de Pré-Filtro são implantadas no FTD como Elementos de Controle de Acesso (ACEs)

L3/L4 e precedem as ACEs L3/L4 configuradas como mostrado na imagem:

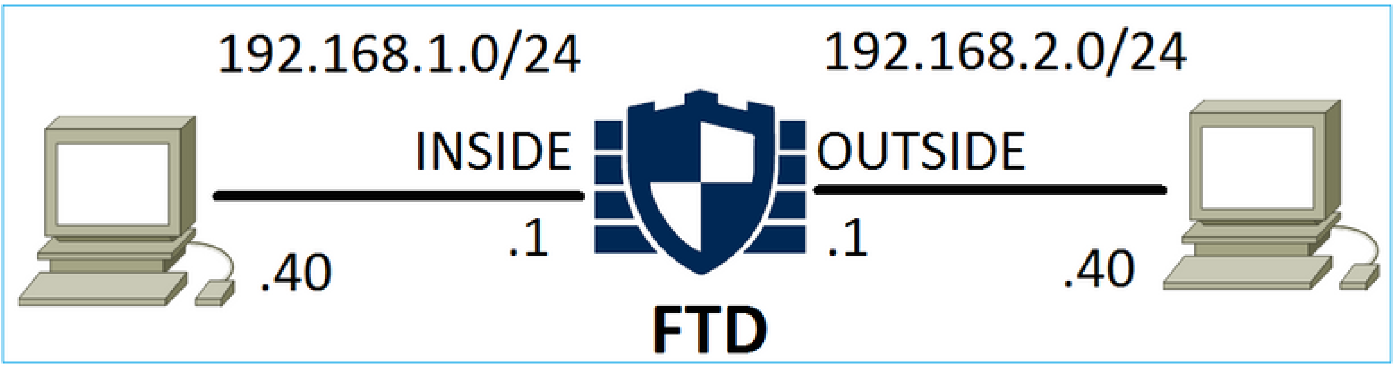


```
firepower# show access-list
access-list CSM_FW_ACL_ line 1 remark rule-id 268434457: PREFILTER POLICY: FTD_Prefilter_Policy
access-list CSM_FW_ACL_ line 2 remark rule-id 268434457: RULE: Fastpath_Rule1
access-list CSM_FW_ACL_ line 3 advanced trust ip host 192.168.75.16 any rule-id 268434457 event-log 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 ipinip 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) 0xa1d3780e
```

Note: Regra de pré-filtro versus regra de ACP = a primeira correspondência é aplicada.

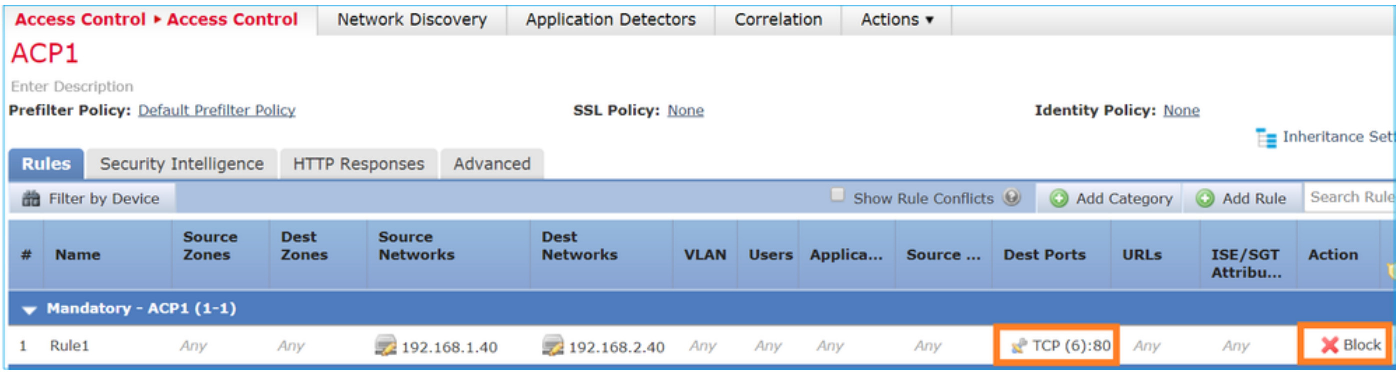
Ação de bloqueio da ACP

Considere a topologia mostrada nesta imagem:



Cenário 1. Queda antecipada de LINA

A ACP contém uma regra de bloqueio que usa uma condição L4 (porta TCP 80 de destino) conforme mostrado na imagem:



ACP1

Enter Description

Prefilter Policy: Default Prefilter Policy **SSL Policy:** None **Identity Policy:** None

#	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

A política implantada no Snort:

```
268435461 deny any 192.168.1.40 32 any any 192.168.2.40 32 80 any 6
```

A política implantada no LINA. Observe que a regra é enviada por push como **deny** ação:

```
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) 0x6149c43c
```

Verifique o comportamento:

Quando o host-A (192.168.1.40) tenta abrir uma sessão HTTP para o host-B (192.168.2.40), os pacotes de sincronização (SYN) do TCP são descartados pelo mecanismo LINA do FTD e não chegam ao Snort Engine ou ao destino:

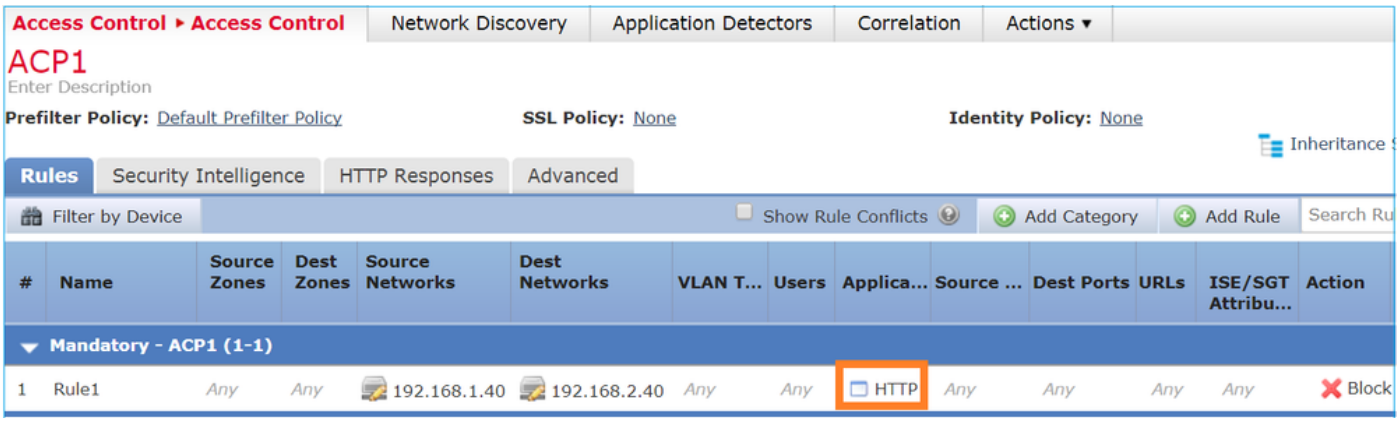
```
firepower# show capture
capture CAPI type raw-data buffer 33554432 trace trace-count 100 interface INSIDE [Capturing -
430 bytes]
  match ip host 192.168.1.40 any
capture CAPO type raw-data buffer 33554432 trace trace-count 100 interface OUTSIDE [Capturing -
0 bytes]
  match ip host 192.168.1.40 any
```

```
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 4063517 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 4069517 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 4081517 0>
```

```
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 event-log flow-start
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
```

Cenário 2. Queda Devido ao Veredito de Snort

A ACP contém uma regra de bloqueio que usa uma condição L7 (HTTP da aplicação) conforme mostrado na imagem:



ACP1

Prefilter Policy: Default Prefilter Policy **SSL Policy:** None **Identity Policy:** None

#	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	HTTP	Any	Any	Any	Any	✖ Block

A política implantada no Snort:

```
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

A política implantada no LINA.

> **Note**: A regra é enviada por push como **permit** porque LINA não pode determinar que a sessão usa HTTP. No FTD, o mecanismo Application Detection está no mecanismo Snort.

```
firepower# show access-list
…
access-list CSM_FW_ACL_ line 9 remark rule-id 268435461: L7 RULE: Rule1
access-list CSM_FW_ACL_ line 10 advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id
268435461 (hitcnt=0) 0xb788b786
```

Para uma regra de bloqueio que usa **Application** como condição, o rastreamento de um pacote real mostra que a sessão é descartada pelo LINA devido ao veredito do mecanismo Snort.

> **Note**: Para que o mecanismo Snort determine a aplicação, ele precisa inspecionar alguns pacotes (geralmente de 3 a 10, dependendo do decodificador da aplicação). Dessa forma, alguns pacotes são permitidos por meio do FTD e chegam ao destino. Os pacotes permitidos ainda estão sujeitos à verificação da política de intrusão com base no **Access Policy > Advanced > 'Intrusion Policy used before Access Control rule is determined'** opção.

Verifique o comportamento:

Quando o host-A (192.168.1.40) tenta estabelecer uma sessão HTTP com o host-B (192.168.2.40), a captura de entrada do LINA mostra:

```
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  192.168.2.40.80 > 192.168.1.40.32790: S 1283931030:1283931030(0) ack
357753152 win 2896 <mss 1380,sackOK,timestamp 5449236 5450579>
   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>
   4: 11:31:20.026899  192.168.1.40.32790 > 192.168.2.40.80: P 357753152:357753351(199) ack
1283931031 win 2920 <nop,nop,timestamp 5450781 5449236>
   5: 11:31:20.428887  192.168.1.40.32790 > 192.168.2.40.80: P 357753152:357753351(199) ack
1283931031 win 2920 <nop,nop,timestamp 5451183 5449236>
 ...
```

A captura de saída:

```
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,sackOK,timestamp 5450579 0>
   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>
   3: 11:31:23.426049  192.168.2.40.80 > 192.168.1.40.32790: S 354801457:354801457(0) ack
1163713180 win 2896 <mss 1460,sackOK,timestamp 5452836 5450579>
   4: 11:31:29.426430  192.168.2.40.80 > 192.168.1.40.32790: S 354801457:354801457(0) ack
1163713180 win 2896 <mss 1460,sackOK,timestamp 5458836 5450579>
   5: 11:31:41.427208  192.168.2.40.80 > 192.168.1.40.32790: S 354801457:354801457(0) ack
1163713180 win 2896 <mss 1460,sackOK,timestamp 5470836 5450579>
```

O rastreamento mostra que o primeiro pacote (TCP SYN) é permitido pelo Snort, já que o veredito de Detecção de Aplicativo ainda não foi alcançado:

```
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
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 268435461
access-list CSM_FW_ACL_ remark rule-id 268435461: ACCESS POLICY: ACP1 - Mandatory
access-list CSM_FW_ACL_ remark rule-id 268435461: L7 RULE: Rule1
Additional Information:
 This packet will be sent to snort for additional processing where a verdict will be reached
...
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 Information:
Snort Trace:
Packet: TCP, SYN, seq 357753151
AppID: service unknown (0), application unknown (0)
Firewall: starting rule matching, zone -1 -> -1, geo 0 -> 0, vlan 0, sgt 65535, user 9999997,
icmpType 0, icmpCode 0
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: OUTSIDE
input-status: up
input-line-status: up
output-interface: OUTSIDE
output-status: up
output-line-status: up
Action: allow
```

O mesmo ocorre para o pacote TCP SYN/ACK:

```
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:
Result: ALLOW
Config:
Additional Information:
Found flow with id 23194, using existing flow
…

Phase: 5
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Trace:
Packet: TCP, SYN, ACK, seq 1283931030, ack 357753152
AppID: service unknown (0), application unknown (0)
Firewall: starting rule matching, zone -1 -> -1, geo 0 -> 0, vlan 0, sgt 65535, user 9999997,
icmpType 0, icmpCode 0
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-status: up
output-line-status: up
Action: allow
```

O Snort retorna um veredito DROP quando uma inspeção do terceiro pacote é concluída:

```
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: ALLOW
Config:
Additional Information:
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 65535, user 9999997,
url http://192.168.2.40/128k.html
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
```

Você também pode executar o comando **system support trace** do modo FTD CLISH. Esta ferramenta oferece duas funções:

- Mostra o veredito do Snort para cada pacote quando ele é enviado para a biblioteca de Aquisição de Dados (DAQ) e visto em LINA. O DAQ é um componente localizado entre o mecanismo LINA e o mecanismo Snort do FTD
- Permite executar **system support firewall-engine-debug** ao mesmo tempo para ver o que acontece dentro do próprio mecanismo Snort

Esta é a saída:

```
> 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
```

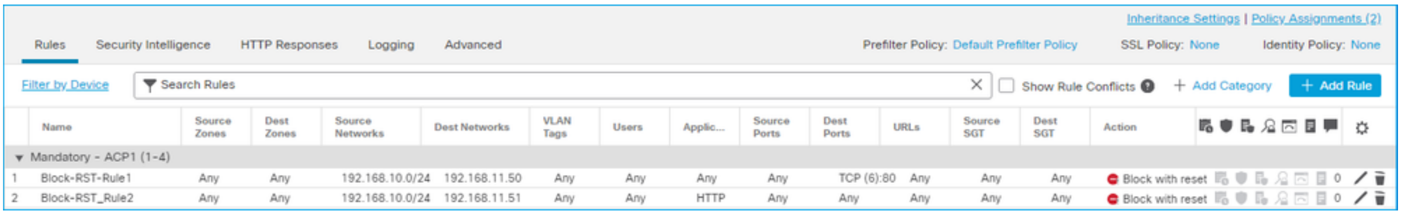
```
192.168.2.40-80 - 192.168.1.40-32791 6 Packet: TCP, SYN, seq 2620409313
192.168.2.40-80 - 192.168.1.40-32791 6 AppID: service unknown (0), application unknown (0)
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 New session
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 Starting with minimum 2, 'Rule1', and SrcZone
first with zones -1 -> -1, geo 0 -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0,
payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.1.40-32791 > 192.168.2.40-80 6 Firewall: starting rule matching, zone -1 -> -1, geo 0 ->
0, vlan 0, sgt 65535, user 9999997, icmpType 0, icmpCode 0
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 pending rule order 2, 'Rule1', AppID
192.168.1.40-32791 > 192.168.2.40-80 6 Firewall: 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 - 192.168.1.40-32791 6 Packet: TCP, SYN, ACK, seq 3700371680, ack 2620409314
192.168.2.40-80 - 192.168.1.40-32791 6 AppID: service unknown (0), application unknown (0)
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 Starting with minimum 2, 'Rule1', and SrcZone
first with zones -1 -> -1, geo 0 -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0,
payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.1.40-32791 > 192.168.2.40-80 6 Firewall: starting rule matching, zone -1 -> -1, geo 0 ->
0, vlan 0, sgt 65535, user 9999997, icmpType 0, icmpCode 0
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 pending rule order 2, 'Rule1', AppID
192.168.1.40-32791 > 192.168.2.40-80 6 Firewall: 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 - 192.168.1.40-32791 6 Packet: 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, 'Rule1', and SrcZone
first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc
676, payload 0, client 686, misc 0, user 9999997, url http://192.168.2.40/128k.html, xff
192.168.1.40-32791 > 192.168.2.40-80 6 Firewall: starting rule matching, zone -1 -> -1, geo 0(0)
-> 0, vlan 0, sgt 65535, user 9999997, 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
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 Deleting session
192.168.1.40-32791 > 192.168.2.40-80 6 NAP id 1, IPS id 0, Verdict BLOCKLIST
192.168.1.40-32791 > 192.168.2.40-80 6 ===> Blocked by Firewall
```

Summary

- A ação de bloqueio da ACP é implantada como regra de permissão ou de negação no LINA, o que depende das condições da regra
- Se as condições forem L3/L4, o LINA bloqueará o pacote. No caso do TCP, o primeiro pacote (TCP SYN) é bloqueado
- Se as condições forem L7, o pacote será encaminhado para o mecanismo Snort para uma inspeção adicional. No caso do TCP, alguns pacotes são permitidos por meio do FTD até que o Snort chegue a uma conclusão. Os pacotes permitidos ainda estão sujeitos à verificação da política de intrusão com base no **Access Policy > Advanced > 'Intrusion Policy used before Access Control rule is determined'** opção.

Ação de bloqueio da ACP com reinicialização

Uma regra de bloqueio com reinicialização configurada na interface do usuário do FMC:



Inheritance Settings | Policy Assignments (2)

Rules | Security Intelligence | HTTP Responses | Logging | Advanced

Prefilter Policy: Default Prefilter Policy   SSL Policy: None   Identity Policy: None

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

	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	

O Bloco com regra de redefinição é implantado no mecanismo LINA do FTD como um **permit** e para o mecanismo Snort como um **reset** regra:

```
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
access-list CSM_FW_ACL_ line 11 remark rule-id 268438865: ACCESS POLICY: ACP1 - Mandatory
access-list CSM_FW_ACL_ line 12 remark rule-id 268438865: L7 RULE: Block-RST_Rule2
access-list CSM_FW_ACL_ line 13 advanced permit ip 192.168.10.0 255.255.255.0 host 192.168.11.51
rule-id 268438865 (hitcnt=0) 0x622350d0
```

Mecanismo Snort:

```
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 268438865
```

Quando um pacote corresponde a Block com a regra de redefinição FTD envia um **TCP Reset** pacote ou um **ICMP Type 3 Code 13** Mensagem de destino inalcançável (filtrado administrativamente):

```
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.
```

Esta é uma captura realizada na interface de entrada do 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,timestamp 3740873275 0,nop,wscale 7>
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 nesse caso, a saída mostra que o pacote foi descartado devido ao veredito de Snort:

```
> 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 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, SYN, seq 3387496622
192.168.10.50-41984 - 192.168.11.50-80 6 AS 1-1 CID 0 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 (0)
192.168.10.50-41984 > 192.168.11.50-80 6 AS 1-1 I 9 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', action Reset and prefilter rule 0
192.168.10.50-41984 > 192.168.11.50-80 6 AS 1-1 I 9 HitCount data sent for rule id: 268438864,
192.168.10.50-41984 > 192.168.11.50-80 6 AS 1-1 I 9 reset action
192.168.10.50-41984 > 192.168.11.50-80 6 AS 1-1 I 9 deleting firewall session flags = 0x0,
fwFlags = 0x0
192.168.10.50-41984 - 192.168.11.50-80 6 AS 1-1 CID 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, drop
192.168.10.50-41984 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 9, NAP id 1, IPS id 0, 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

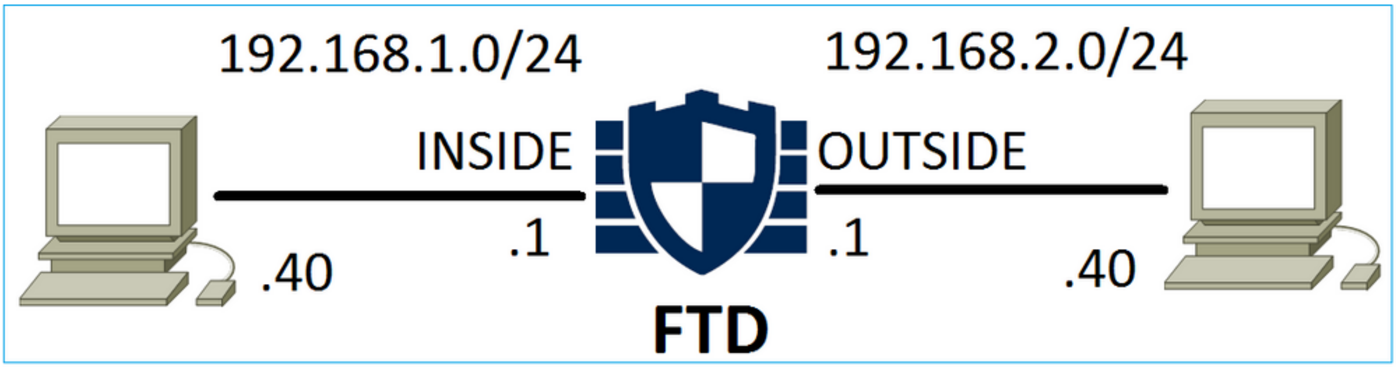
Igual a **Block** mas encerra imediatamente a conexão.

Ação de permissão da ACP

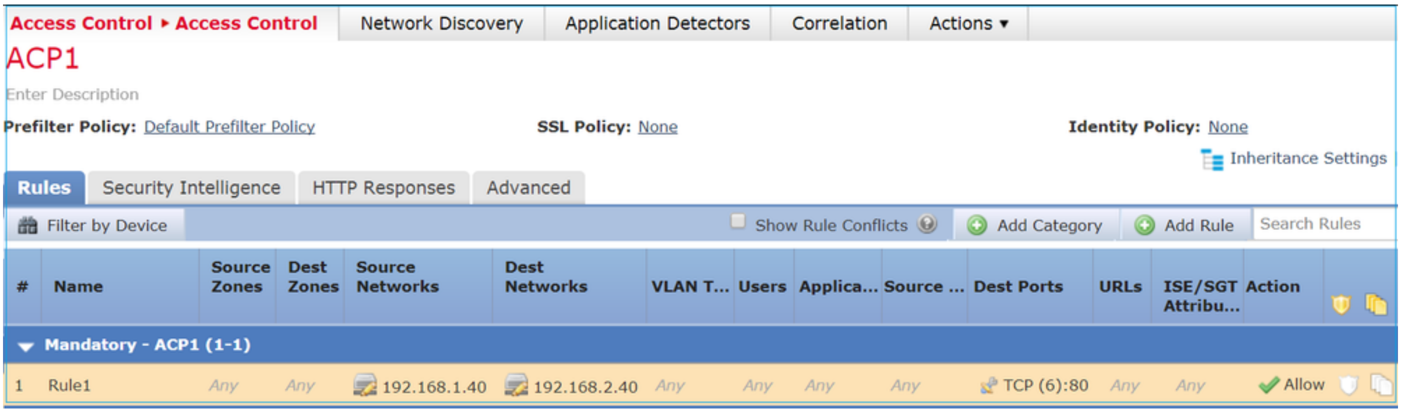
Cenário 1. Ação de Permissão do ACP (Condições L3/L4)

Normalmente, você configuraria uma regra de permissão para especificar as inspeções adicionais, como uma política de invasão e/ou uma política de arquivos. Este primeiro cenário demonstra a operação de uma regra Permitir quando uma condição L3/L4 é aplicada.

Considere esta topologia conforme mostrado na imagem:



Esta política é aplicada conforme mostrado na imagem:



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

A política implantada no Snort. Observe que a regra é implantada como um **allow** ação:

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

A política no LINA.

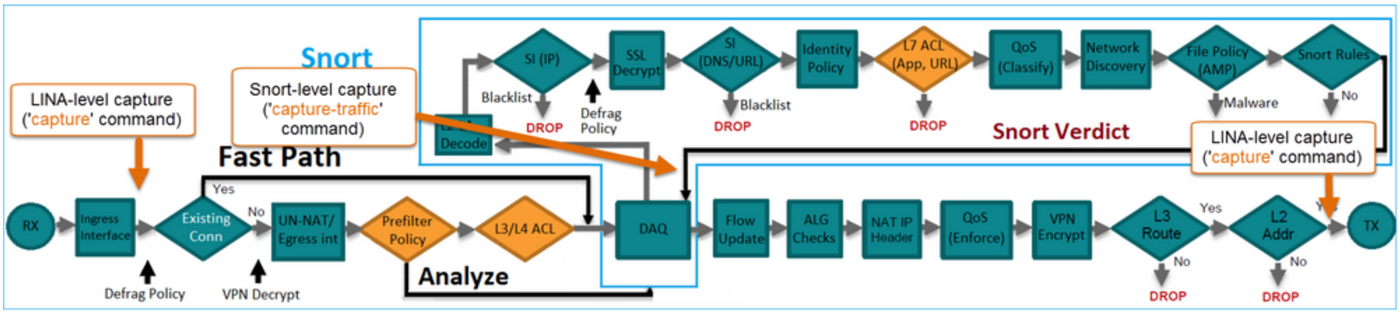
> **Note**: A regra é implantada como um **permit** ação que essencialmente significa redirecionamento para Snort para inspeção posterior.

```
firepower# show access-list
…
access-list CSM_FW_ACL_ line 9 remark rule-id 268435461: L7 RULE: Rule1
access-list CSM_FW_ACL_ line 10 advanced permit tcp host 192.168.1.40 host 192.168.2.40 eq www
rule-id 268435461 (hitcnt=1) 0x641a20c3
```

Para ver como o FTD trata um fluxo que corresponde a uma regra de permissão, há algumas maneiras:

- Verifique as estatísticas do Snort
- Usando o system support trace na ferramenta CLISH
- Usando a captura com a opção de rastreamento no LINA e, como opção, com o capture-traffic no mecanismo Snort

Captura do LINA versus capture-traffic do Snort:



Verifique o comportamento:

Limpar as estatísticas do Snort, ativar **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:

```
firepower# clear snort statistics

> 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
Please specify a server port:
Enable firewall-engine-debug too? [n]:
Monitoring packet tracer debug messages

Tracing enabled by Lina
192.168.2.40-80 - 192.168.1.40-32797 6 Packet: TCP, SYN, seq 361134402
192.168.2.40-80 - 192.168.1.40-32797 6 AppID: service unknown (0), application unknown (0)
192.168.1.40-32797 > 192.168.2.40-80 6 Firewall: allow rule, 'Rule1', allow
192.168.1.40-32797 > 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 - 192.168.1.40-32797 6 Packet: TCP, SYN, ACK, seq 1591434735, ack 361134403
192.168.2.40-80 - 192.168.1.40-32797 6 AppID: service unknown (0), application unknown (0)
192.168.1.40-32797 > 192.168.2.40-80 6 Firewall: allow rule, 'Rule1', allow
192.168.1.40-32797 > 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 - 192.168.1.40-32797 6 Packet: TCP, ACK, seq 361134403, ack 1591434736
192.168.2.40-80 - 192.168.1.40-32797 6 AppID: service HTTP (676), application unknown (0)
192.168.1.40-32797 > 192.168.2.40-80 6 Firewall: allow rule, 'Rule1', allow
192.168.1.40-32797 > 192.168.2.40-80 6 NAP id 1, IPS id 0, Verdict PASS
```

Os contadores Passar pacotes aumentam:

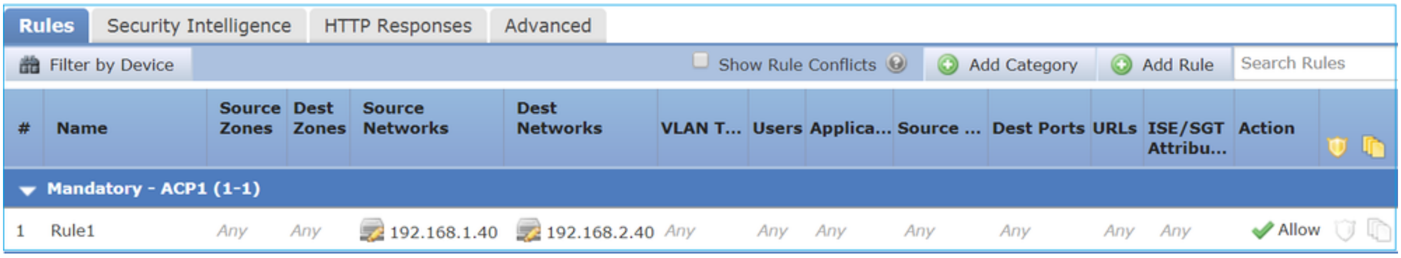
```
> show snort statistics

Packet Counters:
  Passed Packets                                                54
  Blocked Packets                                                0
  Injected Packets                                               0
  Packets bypassed (Snort Down)                                  0
  Packets bypassed (Snort Busy)                                  0

Flow Counters:
  Fast-Forwarded Flows                                           0
  Blocklisted Flows                                              0
...
```

Pacotes aprovados = inspecionados pelo mecanismo Snort

Cenário 2. Ação de Permissão do ACP (Condições L3-7)

Um comportamento semelhante é observado quando a regra de permissão é implantada da seguinte maneira.

Somente uma condição L3/L4 conforme mostrado na imagem:

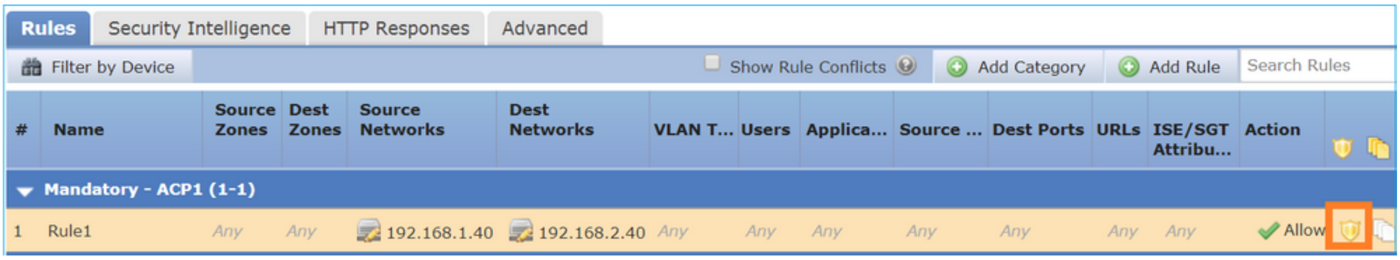


Rules | Security Intelligence | HTTP Responses | Advanced

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	Any	Any	Any	✓ Allow

Uma condição L7 (por exemplo, Diretiva de Intrusão, Diretiva de Arquivo, Aplicativo etc.) é mostrada na imagem:



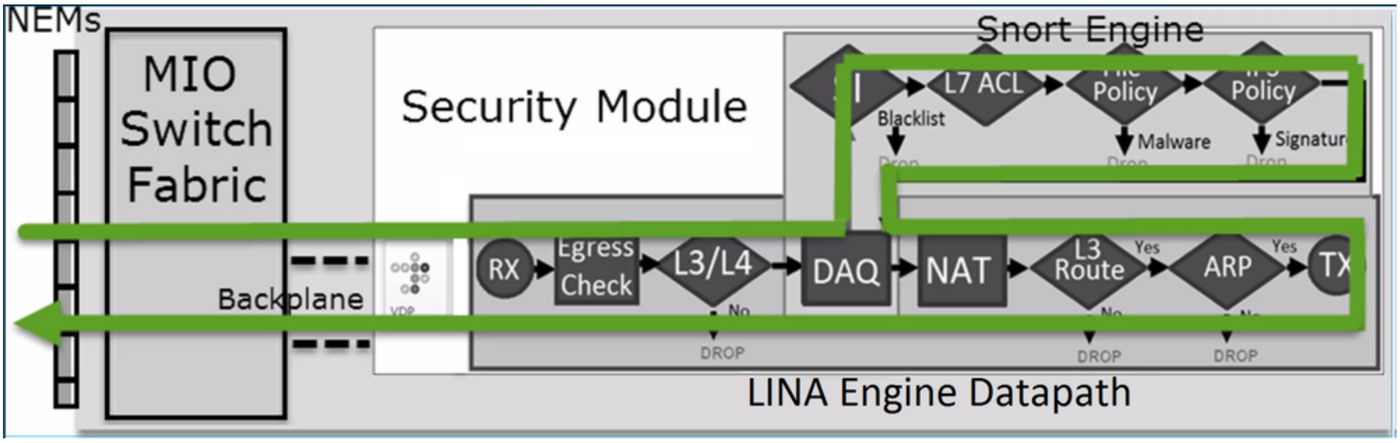
Rules | Security Intelligence | HTTP Responses | Advanced

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	Any	Any	Any	✓ Allow

Summary

Resumindo, é assim que um fluxo é tratado por um FTD implantado em um FP4100/9300, quando uma regra de permissão apresenta correspondência, conforme mostrado na imagem:



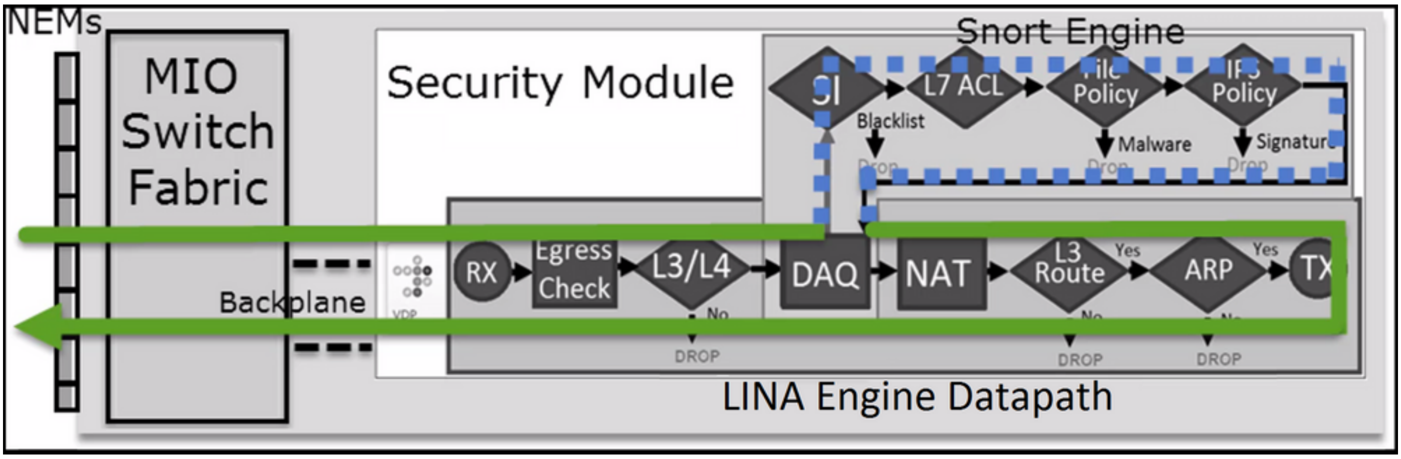
> **Note**: O Management Input Output (MIO) é o mecanismo de supervisão do chassi Firepower.

Cenário 3. Veredito de Encaminhamento Rápido de Snort com Permitir

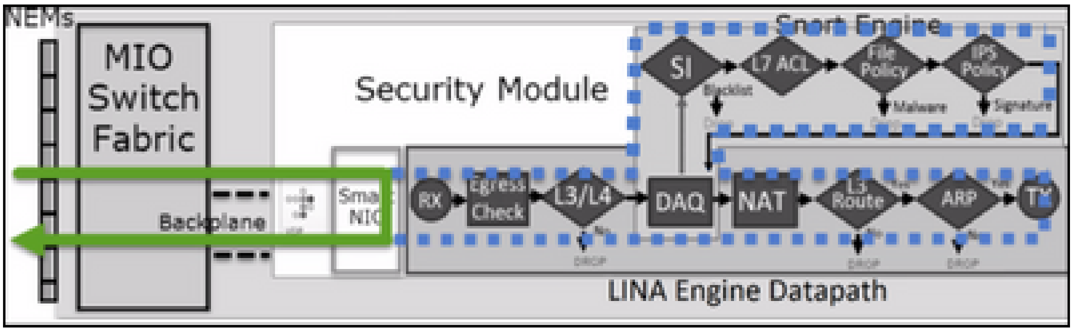
Há cenários específicos em que o mecanismo Snort do FTD fornece um veredito PERMITLIST (fast-forward) e o resto do fluxo é descarregado no mecanismo LINA (em alguns casos, é descarregado no Acelerador de HW - SmartNIC). Estas são:

1. Tráfego SSL sem uma política SSL configurada
2. Intelligent Application Bypass (IAB)

Esta é a representação visual do caminho do pacote:



Ou em alguns casos:



Pontos principais

- A regra de permissão é implantada como **allow** no Snort e **permit** No LINA
- Na maioria dos casos, todos os pacotes de uma sessão são encaminhados ao mecanismo Snort para inspeção adicional

Casos de uso

Você configuraria uma regra de permissão quando precisar de uma inspeção L7 no mecanismo Snort, como:

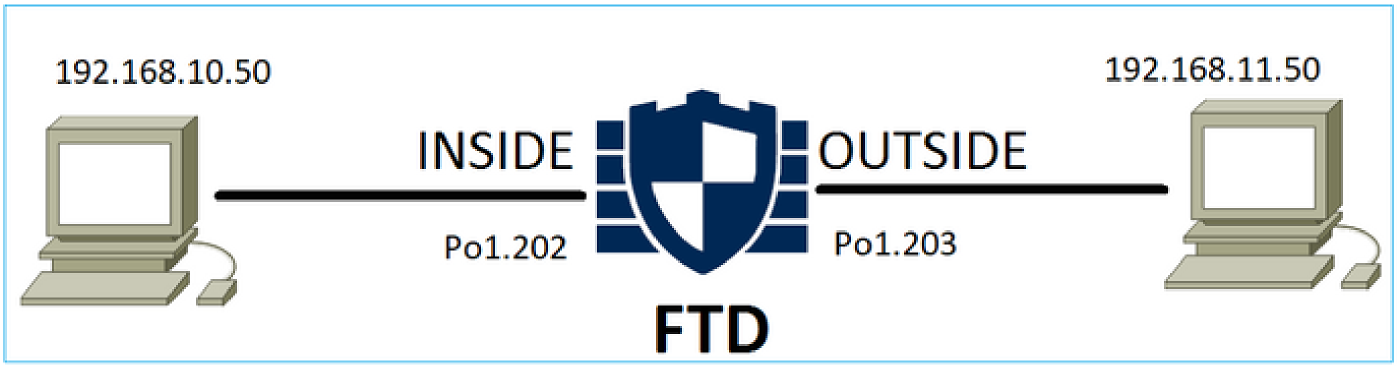
- Política de invasão
- Política de arquivos

Ação de confiança da ACP

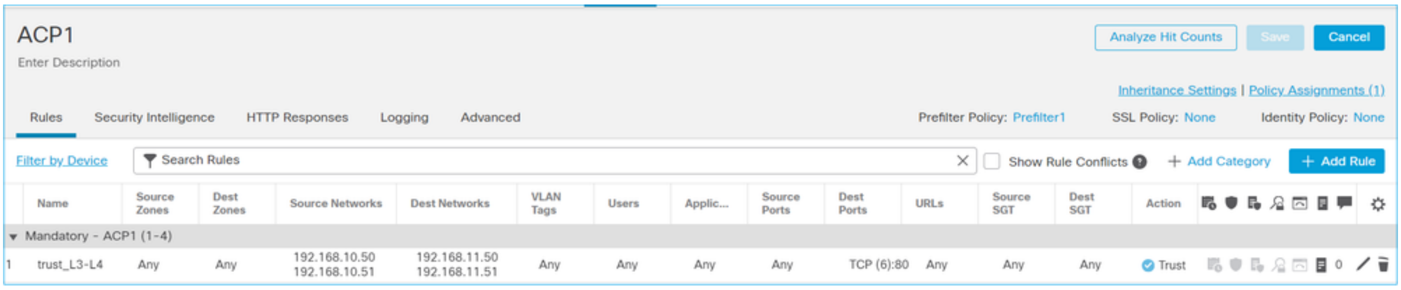
Cenário 1. Ação fiduciária ACP

Se você não quiser aplicar a inspeção L7 avançada no nível Snort (por exemplo, Política de intrusão, Política de arquivo, Descoberta de rede), mas ainda quiser usar recursos como Inteligência de segurança (SI), Política de identidade, QoS etc., é recomendável usar a ação Confiar em sua regra.

Topologia:



A política configurada:



ACP1

Enter Description

Analyze Hit Counts | Save | Cancel

Inheritance Settings | Policy Assignments (1)

Rules | Security Intelligence | HTTP Responses | Logging | Advanced

Prefilter Policy: Prefilter1 | SSL Policy: None | Identity Policy: None

Filter by Device | Search Rules | □ Show Rule Conflicts | + Add Category | + Add Rule

	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	Any	Trust	0

A regra de confiança conforme implantada no mecanismo Snort do FTD:

```
# 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)
```

Note: O número 6 é o protocolo (TCP).

A regra no LINA do FTD:

```
firepower# show access-list | i 268438858
access-list CSM_FW_ACL_ line 17 remark rule-id 268438858: ACCESS POLICY: ACP1 - Mandatory
access-list CSM_FW_ACL_ line 18 remark rule-id 268438858: L7 RULE: trust_L3-L4
access-list CSM_FW_ACL_ line 19 advanced permit tcp object-group FMC_INLINE_src_rule_268438858
object-group FMC_INLINE_dst_rule_268438858 eq www rule-id 268438858 (hitcnt=19) 0x29588b4f
  access-list CSM_FW_ACL_ line 19 advanced permit tcp host 192.168.10.50 host 192.168.11.50 eq
www rule-id 268438858 (hitcnt=19) 0x9d442895
  access-list CSM_FW_ACL_ line 19 advanced permit tcp host 192.168.10.50 host 192.168.11.51 eq
www rule-id 268438858 (hitcnt=0) 0xd026252b
  access-list CSM_FW_ACL_ line 19 advanced permit tcp host 192.168.10.51 host 192.168.11.50 eq
www rule-id 268438858 (hitcnt=0) 0x0d785cc4
  access-list CSM_FW_ACL_ line 19 advanced permit tcp host 192.168.10.51 host 192.168.11.51 eq
www rule-id 268438858 (hitcnt=0) 0x3b3234f1
```

Verificação:

Enable **system support trace** e iniciar uma sessão HTTP do host-A (192.168.10.50) para o host-B (192.168.11.50). Três pacotes são encaminhados para o mecanismo Snort. O mecanismo Snort envia para LINA o veredito PERMITLIST que essencialmente descarrega o resto do fluxo para o mecanismo LINA:

```
> 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 CID 0 Packet: TCP, SYN, seq 453426648
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Session: new snort session
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service unknown (0), application
unknown (0)
192.168.10.50-42126 > 192.168.11.50-80 6 AS 1-1 I 2 new firewall session
192.168.10.50-42126 > 192.168.11.50-80 6 AS 1-1 I 2 using HW or preset rule order 5, 'trust_L3-
L4', action Trust and prefilter rule 0
192.168.10.50-42126 > 192.168.11.50-80 6 AS 1-1 I 2 HitCount data sent for rule id: 268438858,
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: trust/fastpath rule, 'trust_L3-
L4', allow
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 2, NAP id 2, IPS id 0, 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 unknown (0), application
unknown (0)
192.168.11.50-80 - 192.168.10.50-42126 6 AS 1-1 CID 0 Firewall: trust/fastpath rule, 'trust_L3-
L4', allow
192.168.11.50-80 - 192.168.10.50-42126 6 AS 1-1 CID 0 Snort id 2, NAP id 2, IPS id 0, 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 unknown (0), application
unknown (0)
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: trust/fastpath rule, 'trust_L3-
L4', allow
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 2, NAP id 2, IPS id 0, Verdict
PERMITLIST
```

Depois que a conexão é encerrada, o mecanismo Snort recebe as informações de metadados do mecanismo LINA e exclui a sessão:

```
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
192.168.10.50-42126 > 192.168.11.50-80 6 AS 1-1 I 2 Logging EOF for event from hardware with
rule_id = 268438858 ruleAction = 3 ruleReason = 0
192.168.10.50-42126 > 192.168.11.50-80 6 AS 1-1 I 2 : 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
192.168.10.50-42126 > 192.168.11.50-80 6 AS 1-1 I 2 deleting firewall session flags = 0x10003,
fwFlags = 0x1115
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Session: deleted snort session using 0
bytes; protocol id:(-1) : LWstate 0xf LWFlags 0x6007
```

A captura Snort mostra os 3 pacotes que vão para o mecanismo Snort:

```
> 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,
options [mss 1380,sackOK,TS val 3789188468 ecr 0,nop,wscale 7], length 0
10:26:16.525928 IP 192.168.11.50.80 > 192.168.10.50.42144: Flags [S.], seq 3581351172, ack
3065553466, win 8192, options [mss 1380,nop,wscale 8,sackOK,TS val 57650410 ecr 3789188468],
length 0
10:26:16.525928 IP 192.168.10.50.42144 > 192.168.11.50.80: Flags [.], ack 1, win 229, options
[nop,nop,TS val 3789188470 ecr 57650410], length 0
```

A captura do LINA mostra o fluxo que passa por ele:

```
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
2459891187:2459891187(0) win 29200 <mss 1460,sackOK,timestamp 3787091387 0,nop,wscale 7>
   2: 09:51:19.431648  802.1Q vlan#202 P0 192.168.11.50.80 > 192.168.10.50.42118: S
2860907367:2860907367(0) ack 2459891188 win 8192 <mss 1380,nop,wscale 8,sackOK,timestamp
57440579 3787091387>
   3: 09:51:19.431847  802.1Q vlan#202 P0 192.168.10.50.42118 > 192.168.11.50.80: . ack
2860907368 win 229 <nop,nop,timestamp 3787091388 57440579>
   4: 09:51:19.431953  802.1Q vlan#202 P0 192.168.10.50.42118 > 192.168.11.50.80: P
2459891188:2459891337(149) ack 2860907368 win 229 <nop,nop,timestamp 3787091388 57440579>
   5: 09:51:19.444816  802.1Q vlan#202 P0 192.168.11.50.80 > 192.168.10.50.42118: .
2860907368:2860908736(1368) ack 2459891337 win 256 <nop,nop,timestamp 57440580 3787091388>
   6: 09:51:19.444831  802.1Q vlan#202 P0 192.168.11.50.80 > 192.168.10.50.42118: .
2860908736:2860910104(1368) ack 2459891337 win 256 <nop,nop,timestamp 57440580 3787091388>

…
```

O rastreamento dos pacotes do LINA é outra maneira de ver as conclusões do Snort. O primeiro pacote recebeu a conclusão de APROVADO:

```
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
Type: NAT
Type: IP-OPTIONS
Type: CAPTURE
Type: CAPTURE
Type: NAT
Type: CAPTURE
```

```
Type: NAT
Type: IP-OPTIONS
Type: CAPTURE
Type: FLOW-CREATION
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
```

Rastreamento do pacote TCP SYN/ACK na interface EXTERNA:

```
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
```

O TCP ACK obtém o veredito PERMITLIST:

```
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
```

Esta é a saída completa da conclusão do Snort (pacote nº 3)

```
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, ack 1029625865
AppID: service unknown (0), application unknown (0)
Firewall: trust/fastpath rule, id 268438858, allow
Snort id 31, NAP id 2, IPS id 0, Verdict PERMITLIST
Snort Verdict: (fast-forward) fast forward this flow
```

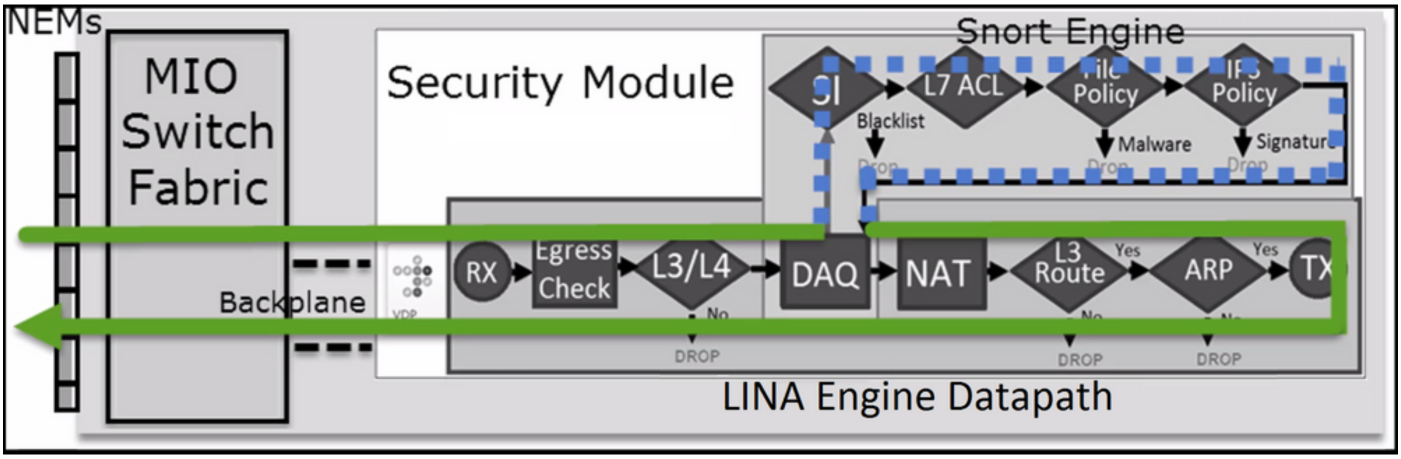
O quarto pacote não é encaminhado para o mecanismo Snort, uma vez que o veredito é armazenado em cache pelo mecanismo LINA:

```
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
164375589:164375738(149) ack 3008397532 win 229 <nop,nop,timestamp 3789654678 57697031>
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 1254, using existing flow

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

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


1 packet shown
```

As estatísticas do Snort confirmam isso:

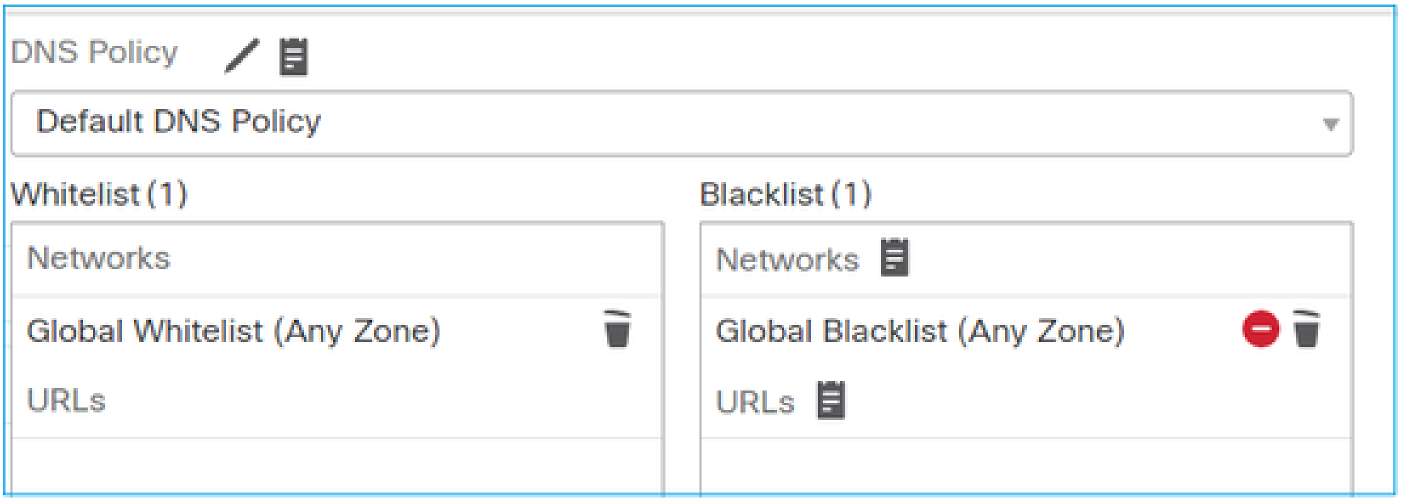
```
firepower# show snort statistics

Packet Counters:
  Passed Packets                                                   2
  Blocked Packets                                                  0
  Injected Packets                                                 0
  Packets bypassed (Snort Down)                                    0
  Packets bypassed (Snort Busy)                                    0

Flow Counters:
  Fast-Forwarded Flows                                      1
  Blacklisted Flows                                         0

Miscellaneous Counters:
  Start-of-Flow events                                      0
  End-of-Flow events                                        1
  Denied flow events                                        0
  Frames forwarded to Snort before drop                     0
  Inject packets dropped                                    0
```

Fluxo de pacotes com regra de confiança. Alguns pacotes são inspecionados pelo Snort e o restante é inspecionado pelo LINA:



Cenário 2. Ação Confiável do ACP (sem SI, QoS e Política de Identidade)

Caso deseje que o FTD aplique verificações de Inteligência de Segurança (SI) a todos os fluxos, o SI já está habilitado no nível do ACP e você pode especificar as origens SI (TALOS, feeds, listas, etc). Por outro lado, se você quiser desativá-lo, desative a SI para redes globalmente por ACP, SI para URL e SI para DNS. A SI para redes e URL está desativada conforme mostrado na imagem:



DNS Policy

Default DNS Policy

Whitelist (1)

Networks

Global Whitelist (Any Zone)

URLs

Blacklist (1)

Networks

Global Blacklist (Any Zone)

URLs

Nesse caso, a regra de confiança é implantada no LINA como confiança:

```
> 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 trust ip host 192.168.1.40 host 192.168.2.40 rule-id
```

```
268435461 event-log flow-end (hitcnt=0) 0x5c1346d6
```

> **Note**: A partir do 6.2.2, o FTD suporta o TID. O TID funciona de forma semelhante à SI, mas se a SI estiver desativada, ela não 'força' o redirecionamento de pacotes para o mecanismo Snort para uma inspeção de TID.

Verifique o comportamento

Inicie uma sessão HTTP do host-A (192.168.1.40) para o host-B (192.168.2.40). Como este é um FP4100 e oferece suporte a descarregamento de fluxo em hardware, estas coisas acontecem:

- Alguns pacotes são encaminhados por meio do mecanismo LINA do FTD e o restante do fluxo é transferido para o SmartNIC (acelerador de HW)
- Nenhum pacote é encaminhado para o mecanismo Snort

A tabela de conexão LINA do FTD mostra a flag ‘**o**’ o que significa que o fluxo foi transferido para o hardware. Além disso, observe a ausência do ‘**N**". Basicamente, isso significa que 'não há redirecionamento do Snort':

```
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 949584, flags UIOo
```

As estatísticas do Snort mostram apenas os eventos de registro no início e no término da sessão:

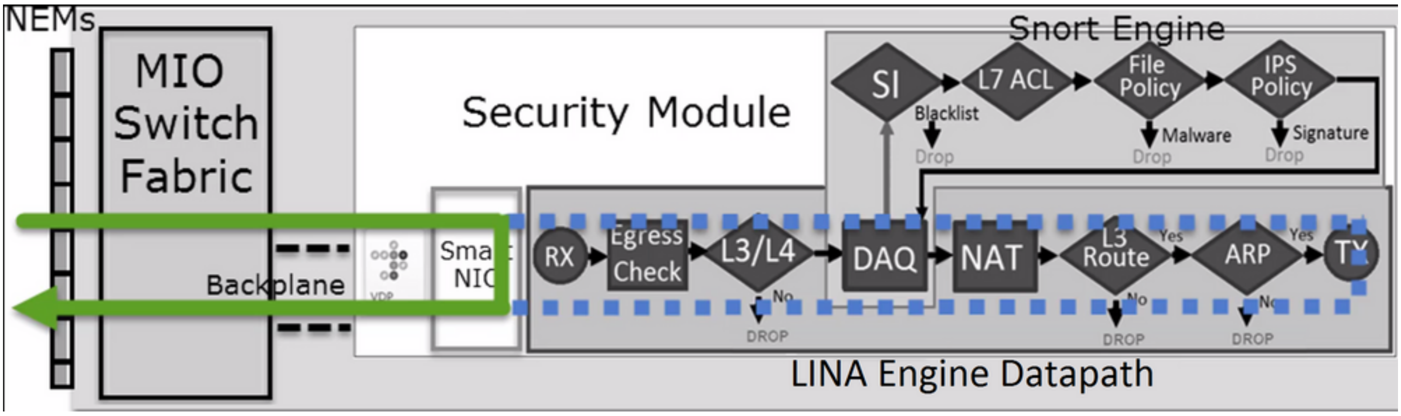
```
firepower# show snort statistics

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

Flow Counters:
  Fast-Forwarded Flows                                      0
  Blacklisted Flows                                         0

Miscellaneous Counters:
  Start-of-Flow events                                      1
  End-of-Flow events                                        1
```

Os registros do LINA do FTD mostram que, para cada sessão, dois fluxos (um para cada direção) foram transferidos para o HW:

```
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 for
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: %ASA-6-805001: 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: %ASA-6-805001: 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: %ASA-6-805002: TCP Flow is no longer offloaded 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: %ASA-6-805002: TCP Flow is no longer offloaded 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: %ASA-6-302014: Teardown TCP connection 25384 for INSIDE:192.168.1.40/32809
to OUTSIDE:192.168.2.40/80 duration 0:00:00 bytes 1055048 TCP FINs
Sep 27 2017 20:16:05: %ASA-7-609002: Teardown local-host INSIDE:192.168.1.40 duration 0:00:00
```

Fluxo de pacotes com a regra de Confiança implantada como **trust** em LINA. Alguns pacotes são inspecionados pelo LINA e o restante é transferido para o SmartNIC (FP4100/FP9300):

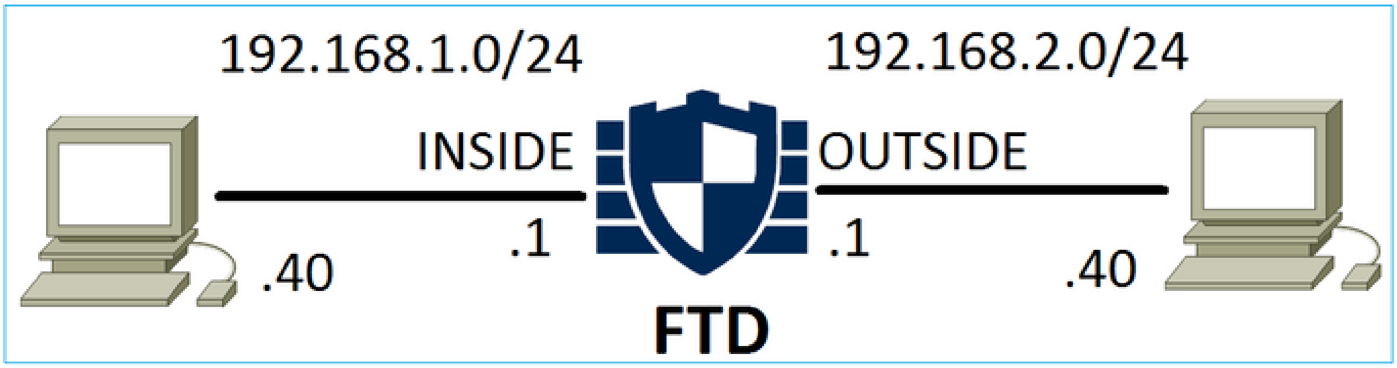


Casos de uso

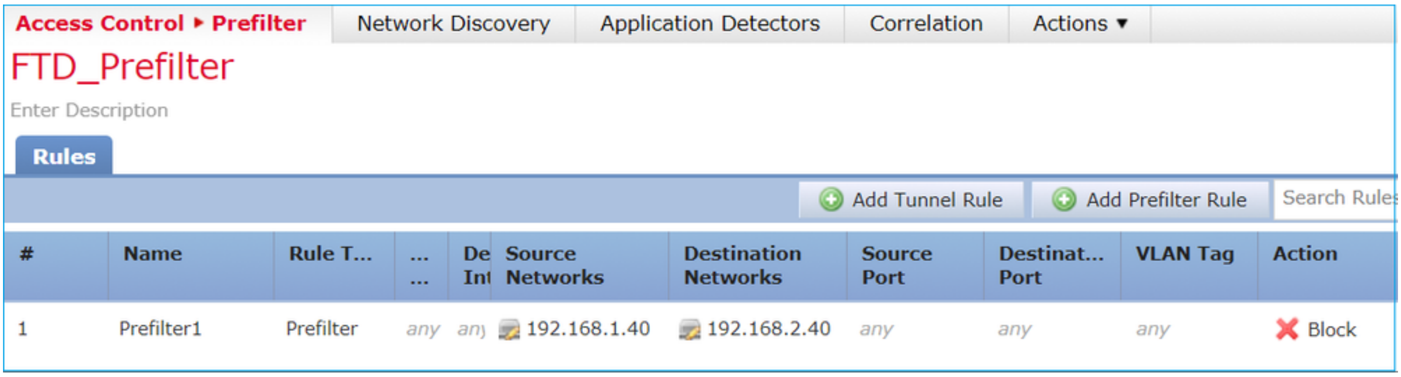
- Você deve usar **Trust** quando você quiser que apenas alguns pacotes sejam verificados pelo mecanismo Snort (por exemplo, detecção de aplicativos, verificação de SI) e o restante do fluxo seja transferido para o mecanismo LINA
- Se você usar o FTD em FP4100/9300 e quiser que o fluxo ignore completamente a inspeção de Snort, considere a regra de Pré-filtro com **Fastpath** ação (consulte a seção relacionada neste documento)

Ação de bloqueio da política de pré-filtro

Considere a topologia conforme mostrado na imagem:



Considere também a política conforme mostrado na imagem:



FTD_Prefilter

#	Name	Rule T...	... ...	De Int	Source 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 é a política implantada no mecanismo Snort do FTD (arquivo ngfw.rules):

```
# 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
```

No LINA:

```
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 3 advanced deny ip host 192.168.1.40 host 192.168.2.40 rule-id
268437506 event-log flow-start (hitcnt=0) 0x76476240
```

quando você rastreia um pacote virtual, ele mostra que o pacote é descartado pelo LINA e nunca encaminhado para o Snort:

```
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 flow-start
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:
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
```

As estatísticas do Snort mostram:

```
firepower# show snort statistics
```

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

Flow Counters:
  Fast-Forwarded Flows                                    0
  Blacklisted Flows                                       0

Miscellaneous Counters:
  Start-of-Flow events                                    0
  End-of-Flow events                                      0
  Denied flow events                                      1
```

Os descartes da ASP do LINA mostram:

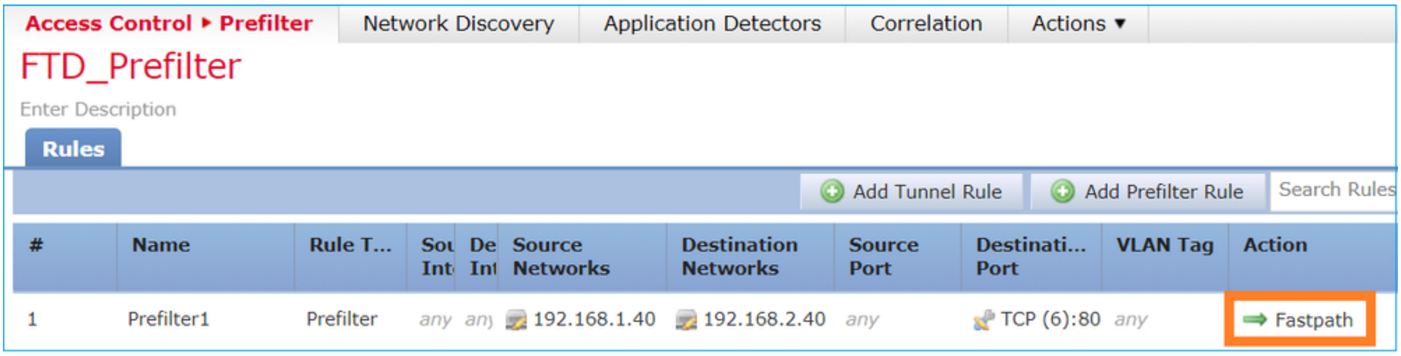
```
firepower# show asp drop

Frame drop:
  Flow is denied by configured rule (acl-drop)              1
```

Casos de uso

Você pode usar uma regra de Bloqueio de pré-filtro quando quiser bloquear o tráfego com base nas condições L3/L4 e sem a necessidade de fazer qualquer inspeção Snort do tráfego.

Ação de fastpath da política de pré-filtro

Considere a regra de política de pré-filtro conforme mostrado na imagem:



FTD_Prefilter

Enter Description

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

Esta é a política implantada no mecanismo Snort do FTD:

```
268437506 fastpath any any any any any any any any (log dcforward flowend) (tunnel -1)
```

No LINA do FTD:

```
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 3 advanced trust tcp host 192.168.1.40 host 192.168.2.40 eq www
rule-id 268437506 event-log flow-end (hitcnt=0) 0xf3410b6f
```

Verifique o comportamento

Quando o host-A (192.168.1.40) tenta abrir uma sessão HTTP para o host-B (192.168.2.40), alguns pacotes passam pelo LINA e o restante é transferido para o SmartNIC. Nesse caso **system support trace** com **firewall-engine-debug** habilitado mostra:

```
> 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

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
```

Os registros do LINA mostram o fluxo transferido:

```
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
Oct 01 2017 14:36:51: %ASA-6-302013: Built inbound TCP connection 966 for
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-6-805001: 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-6-805001: 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)
```

As capturas LINA mostram que 8 pacotes passam por:

```
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 CAPO type raw-data buffer 33554432 trace trace-count 100 interface OUTSIDE [Capturing -
3908 bytes]
  match ip host 192.168.1.40 host 192.168.2.40
```

```
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,sackOK,timestamp 332569060 0>
   2: 14:45:32.700372  192.168.2.40.80 > 192.168.1.40.32842: S 184794124:184794124(0) ack
3195173119 win 2896 <mss 1380,sackOK,timestamp 332567732 332569060>
   3: 14:45:32.700540  192.168.1.40.32842 > 192.168.2.40.80: P 3195173119:3195173317(198) ack
184794125 win 2920 <nop,nop,timestamp 332569060 332567732>
   4: 14:45:32.700876  192.168.2.40.80 > 192.168.1.40.32842: . 184794125:184795493(1368) ack
3195173317 win 2698 <nop,nop,timestamp 332567733 332569060>
   5: 14:45:32.700922  192.168.2.40.80 > 192.168.1.40.32842: P 184795493:184796861(1368) ack
```

```
3195173317 win 2698 <nop,nop,timestamp 332567733 332569060>
   6: 14:45:32.701425  192.168.2.40.80 > 192.168.1.40.32842: FP 184810541:184810851(310) ack
3195173317 win 2698 <nop,nop,timestamp 332567733 332569061>
   7: 14:45:32.701532  192.168.1.40.32842 > 192.168.2.40.80: F 3195173317:3195173317(0) ack
184810852 win 2736 <nop,nop,timestamp 332569061 332567733>
   8: 14:45:32.701639  192.168.2.40.80 > 192.168.1.40.32842: . ack 3195173318 win 2697
<nop,nop,timestamp 332567734 332569061>
```

As estatísticas de flow-offload do FTD mostram 22 pacotes transferidos para o HW:

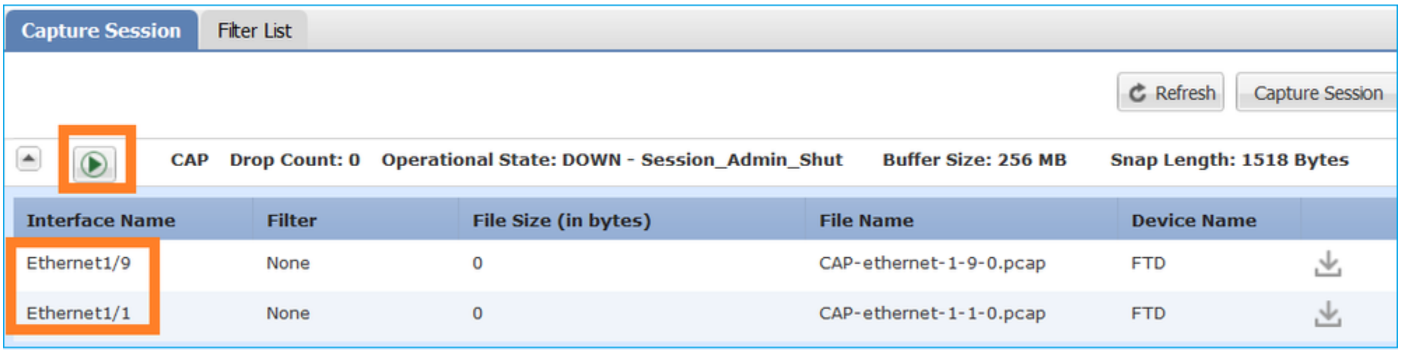
```
firepower# show flow-offload statistics
 Packet stats of port : 0
        Tx Packet count                 :               22
        Rx Packet count                 :               22
        Dropped Packet count            :                0
        VNIC transmitted packet         :               22
        VNIC transmitted bytes          :            15308
        VNIC Dropped packets            :                0
        VNIC erroneous received         :                0
        VNIC CRC errors                 :                0
        VNIC transmit failed            :                0
        VNIC multicast received         :                0
```

Você também pode usar o comando **show flow-offload flow** para ver informações adicionais relacionadas aos fluxos descarregados. Aqui está um exemplo:

```
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, bytes 2326800
TCP intfc 104 src 192.168.2.40:20 dest 192.168.1.40:39301, static, timestamp 616063760, packets
249140, bytes 358263320
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 Uo
<- offloaded flow
TCP OUTSIDE  192.168.2.40:20 INSIDE  192.168.1.40:34713, idle 0:02:40, bytes 821799360, flags
UFRIO
```

- A porcentagem é baseada no '**show conn**'saída. Por exemplo, se um total de 5 conexões passar pelo mecanismo LINA do FTD e um deles for descarregado, 20% será relatado como descarregado
- O limite máximo de sessões descarregadas depende da versão do software (por exemplo, o ASA 9.8.3 e o FTD 6.2.3 suportam 4 milhões de fluxos descarregados bidirecionais (ou 8 milhões unidirecionais))
- Caso o número de fluxos descarregados atinja o limite (por exemplo, 4 milhões de fluxos bidirecionais), nenhuma nova conexão é descarregada até que as conexões atuais sejam removidas da tabela descarregada

Para ver todos os pacotes no FP4100/9300 que passam pelo FTD (transferidos + LINA), é necessário ativar a captura no nível do chassi conforme mostrado na imagem:



CAP Drop Count: 0 Operational State: DOWN - Session_Admin_Shut Buffer Size: 256 MB Snap Length: 1518 Bytes

Interface Name	Filter	File Size (in bytes)	File Name	Device Name
Ethernet1/9	None	0	CAP-ethernet-1-9-0.pcap	FTD
Ethernet1/1	None	0	CAP-ethernet-1-1-0.pcap	FTD

A captura do painel traseiro do chassi mostra as duas direções. Em virtude da arquitetura da captura do FXOS (dois pontos de captura por direção), cada pacote é mostrado **duas vezes**, conforme mostrado na imagem:

Estatísticas do pacote:

- Total de pacotes que passam pelo FTD: 30
- Pacotes que passam pelo LINA do FTD: 8
- Pacotes transferidos para o acelerador de HW do SmartNIC: 22

No caso de uma plataforma diferente de FP4100/FP9300, todos os pacotes são manipulados pelo mecanismo LINA, já que o descarregamento de fluxo não é suportado (observe a ausência da flag **o**):

```
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 most in effect

TCP OUTSIDE  192.168.2.40:80 INSIDE  192.168.1.40:50890, idle 0:00:09, bytes 175, flags UxIO
```

Os syslogs do LINA mostram apenas os eventos de configuração e encerramento de conexão:

```
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)
Jun 21 2020 14:30:30: %FTD-6-302014: 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 OUTSIDE
```

Casos de uso

- Uso **Prefilter Fastpath** ação quando desejar ignorar completamente a inspeção Snort. Normalmente, você vai querer fazer isso para grandes fluxos confiáveis, como backups, transferências de banco de dados etc.
- Em aparelhos FP4100/9300, o **Fastpath** A ação aciona o descarregamento de fluxo e apenas alguns pacotes passam pelo mecanismo LINA do FTD. O restante é tratado pelo SmartNIC, o que diminui a latência

Ação de fastpath da política de pré-filtro (conjunto em linha)

Caso uma ação de política de pré-filtro Fastpath seja aplicada ao tráfego que passa por um conjunto em linha (interfaces NGIPS), esses pontos devem ser considerados:

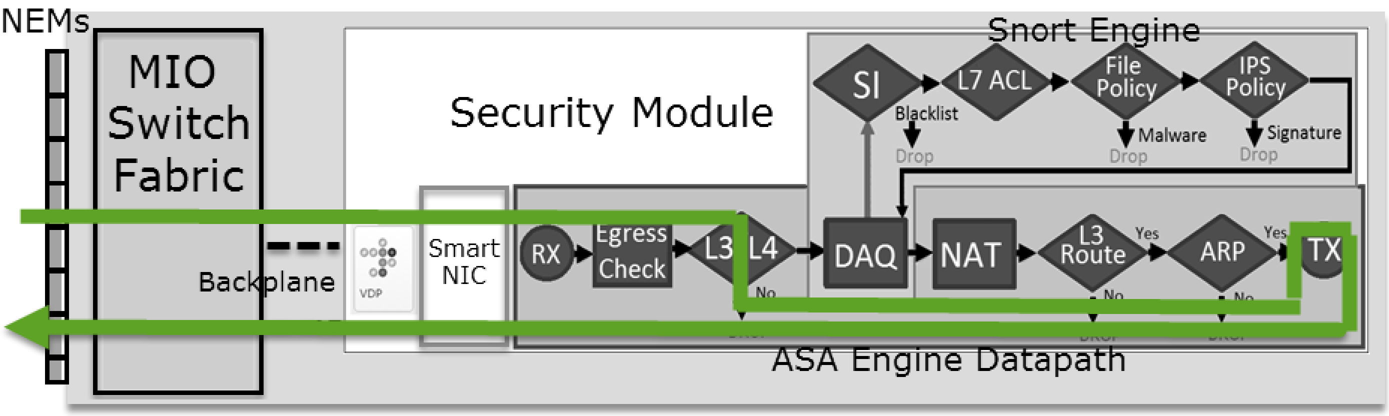
- A regra é aplicada ao mecanismo LINA como um **trust** ação
- O fluxo não é inspecionado pelo mecanismo Snort
- A transferência de fluxo (aceleração de HW) não ocorre, pois a transferência de fluxo não é aplicável em interfaces NGIPS

Aqui está um exemplo de um rastreamento de pacote no caso da ação Prefilter Fastpath aplicada em um conjunto em linha:

```
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: ALLOW
Config:
Additional Information:
The flow ingressed an interface configured for NGIPS mode and NGIPS services will be applied
Forward Flow based lookup yields rule:
in id=0x2ad7ac48b330, priority=501, domain=ips-mode, deny=false
hits=2, user_data=0x2ad80d54abd0, cs_id=0x0, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=inside, output_ifc=any

Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced trust ip object 192.168.1.0 object 192.168.1.0 rule-id
268438531 event-log flow-end
access-list CSM_FW_ACL_ remark rule-id 268438531: PREFILTER POLICY: PF1
access-list CSM_FW_ACL_ remark rule-id 268438531: RULE: 1
Additional Information:
Forward Flow based lookup yields rule:
in id=0x2ad9f9f8a7f0, priority=12, domain=permit, trust
hits=1, user_data=0x2ad9b23c5d40, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
src ip/id=192.168.1.0, mask=255.255.255.0, port=0, tag=any, ifc=any
dst ip/id=192.168.1.0, mask=255.255.255.0, port=0, tag=any, ifc=any, vlan=0, dscp=0x0
input_ifc=any, output_ifc=any

Phase: 3
Type: NGIPS-EGRESS-INTERFACE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
Ingress interface inside is in NGIPS inline mode.
Egress interface outside is determined by inline-set configuration

Phase: 4
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 7, packet dispatched to next module
```

```
Module information for forward flow ...
snp_fp_ips_tcp_state_track_lite
snp_fp_ips_mode_adj
snp_fp_tracer_drop
snp_ifc_stat

Module information for reverse flow ...
snp_fp_ips_tcp_state_track_lite
snp_fp_ips_mode_adj
snp_fp_tracer_drop
snp_ifc_stat

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

Esta é a representação visual do caminho do pacote:



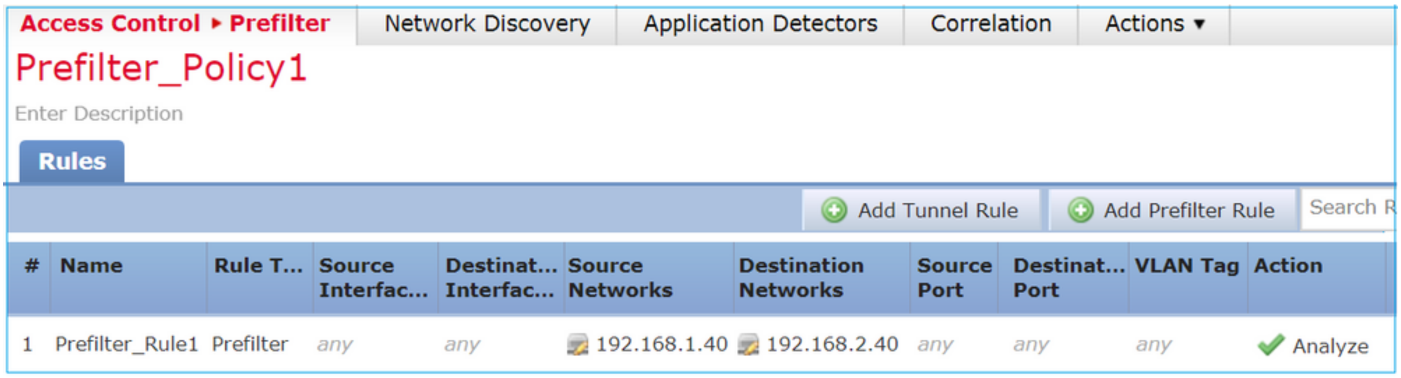
Ação de fastpath da política de pré-filtro (conjunto em linha com toque)

Igual ao caso de conjunto em linha

Ação de análise da política de pré-filtro

Cenário 1. Análise de Pré-Filtro com Regra de Bloqueio ACP

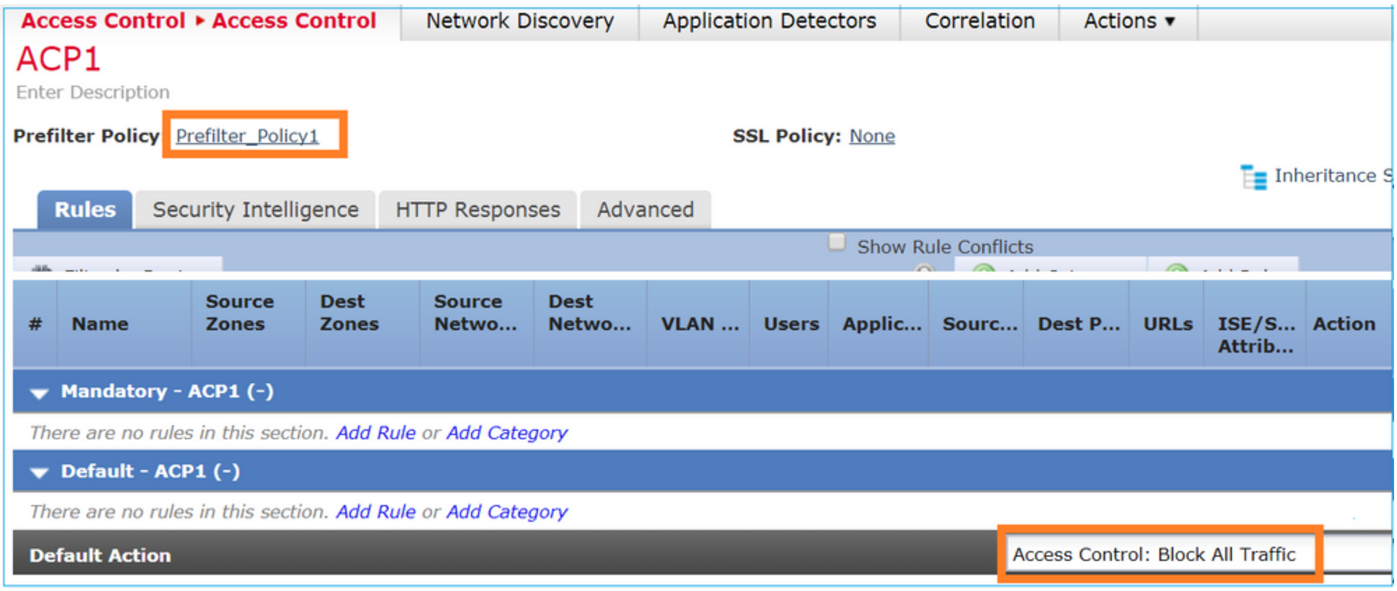
Considere a regra de política de pré-filtro que contém uma regra de análise conforme mostrado na imagem:



Prefilter_Policy1

#	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

O ACP contém apenas a regra padrão definida como **Block All Traffic** conforme mostrado na imagem:



Access Control ▸ Access Control | Network Discovery | Application Detectors | Correlation | Actions ▾

ACP1

Enter Description

Prefilter Policy: Prefilter_Policy1   SSL Policy: None

Inheritance S

Rules | Security Intelligence | HTTP Responses | Advanced

□ Show Rule Conflicts

#	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 é a política implantada no mecanismo Snort do FTD (arquivo ngfw.rules):

```
# 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 any  1025-65535 any any  3544 any 17  (tunnel -1)
268435459 allow any any  3544 any any  1025-65535 any 17  (tunnel -1)
268435459 allow any any  any any any  any any 47  (tunnel -1)
268435459 allow any any  any any any  any any 41  (tunnel -1)
268435459 allow any any  any any any  any any 4  (tunnel -1)
# End of tunnel and priority rules.
# Start of AC rule.
268435458 deny any any  any any any  any any any  (log dcforward flowstart)
# End of AC rule.
```

Esta é a política implantada no mecanismo LINA do FTD:

```
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 o comportamento

O Packet Tracer mostra que o pacote é permitido pelo LINA e é encaminhado ao mecanismo Snort (devido a **permit** ação) e o Snort Engine retorna um **Block** uma vez que a ação padrão do AC é correspondida.

> **Note**: O Snort não avalia o tráfego com base nas regras de túnel

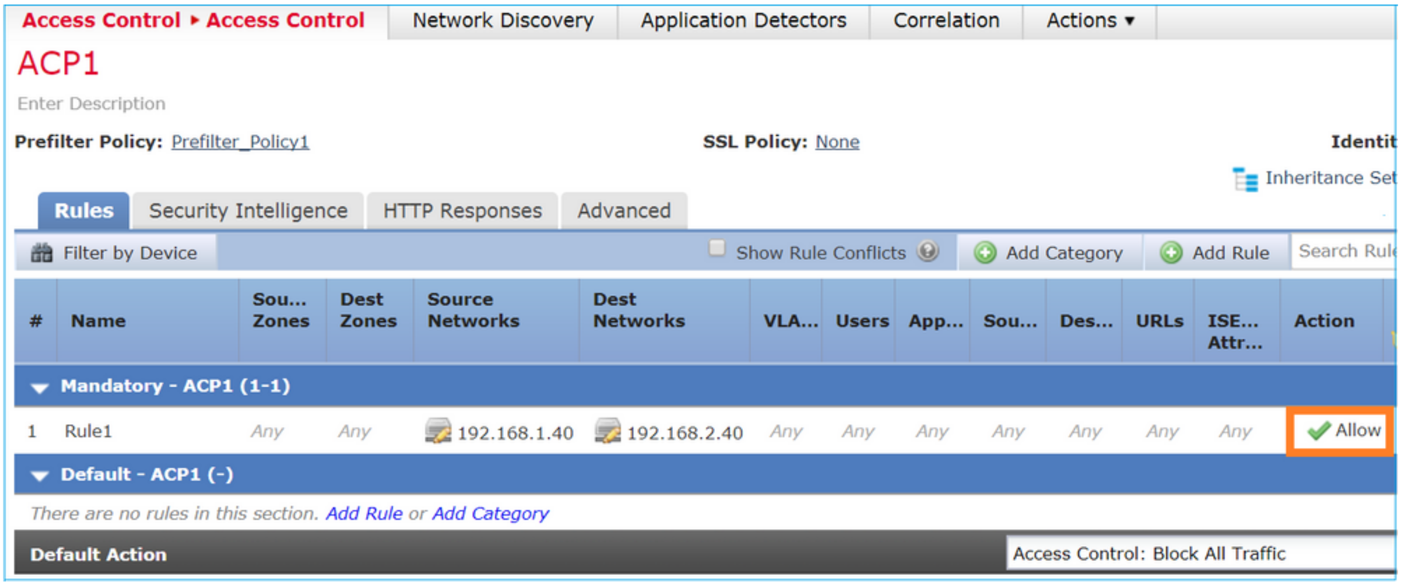
Quando você rastreia um pacote, ele revela o mesmo:

```
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_ remark rule-id 268435460: RULE: Prefilter_Rule1
Additional Information:
 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 (0)
Firewall: starting rule matching, zone -1 -> -1, geo 0 -> 0, vlan 0, sgt 65535, user 9999997,
icmpType 8, icmpCode 0
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-status: up
output-line-status: up
Action: drop
Drop-reason: (firewall) Blocked by the firewall preprocessor
```

Cenário 2. Análise de Pré-Filtro com Regra de Permissão de ACP

Se a meta for permitir que o pacote passe pelo FTD, será necessário adicionar uma regra na ACP. A Ação pode ser Permitir ou Confiar, que depende do objetivo (por exemplo, se você quiser aplicar uma inspeção L7, deverá usar **Allow** ação) conforme mostrado na imagem:



ACP1

Enter Description

Prefilter Policy: Prefilter_Policy1

SSL Policy: None

Identit

#	Name	Sou... Zones	Dest Zones	Source Networks	Dest Networks	VLA...	Users	App...	Sou...	Des...	URLs	ISE... Attr...	Action
▾ Mandatory - ACP1 (1-1)													
1	Rule1	Any	Any	192.168.1.40	192.168.2.40	Any	Any	Any	Any	Any	Any	Any	✓ Allow
▾ Default - ACP1 (-)													
There are no rules in this section. Add Rule or Add Category													
Default Action													Access Control: Block All Traffic

A política implantada no mecanismo Snort do FTD:

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

No mecanismo LINA:

```
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
```

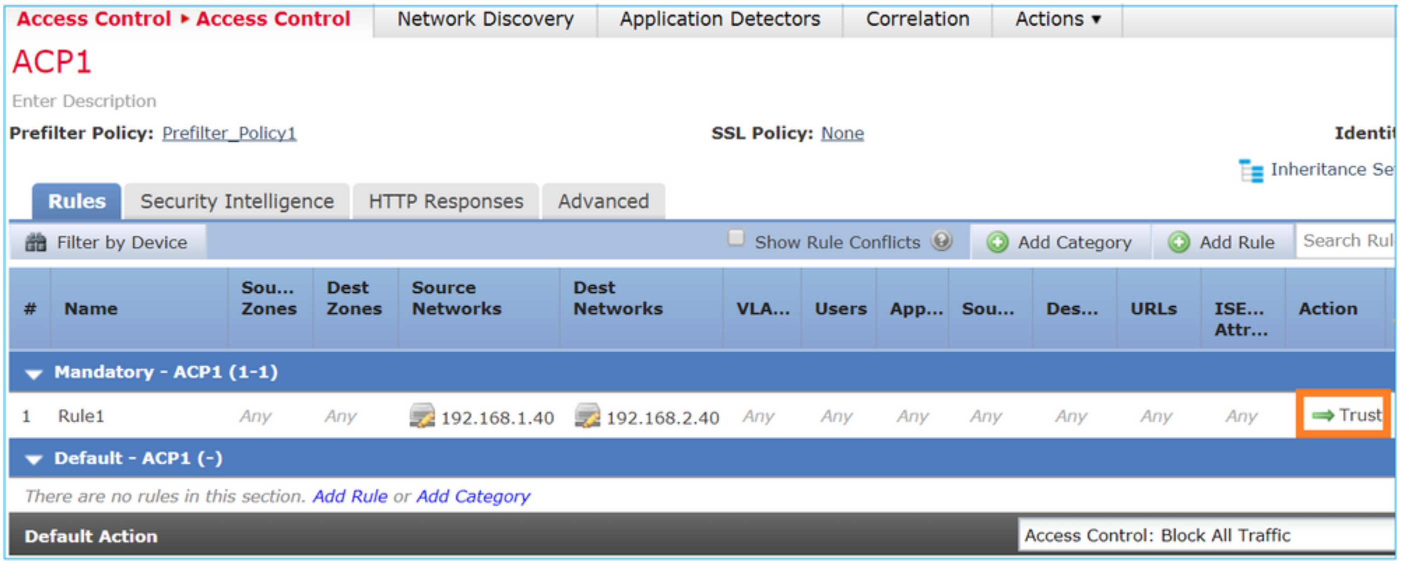
Verifique o comportamento

O Packet Tracer mostra que o pacote corresponde à regra **268435460** na LINA e **268435461** no mecanismo Snort:

```
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_ remark rule-id 268435460: RULE: Prefilter_Rule1
Additional Information:
 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
AppID: service ICMP (3501), application unknown (0)
Firewall: starting rule matching, zone -1 -> -1, geo 0 -> 0, vlan 0, sgt 65535, user 9999997,
icmpType 8, icmpCode 0
Firewall: 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
output-line-status: up
Action: allow
```

Cenário 3. Análise de Pré-Filtro com Regra de Confiança do ACP

Se a ACP contiver uma regra de confiança, você terá o seguinte conforme mostrado na imagem:



ACP1

Enter Description

Prefilter Policy: Prefilter_Policy1

SSL Policy: None

Identi

#	Name	Sou... Zones	Dest Zones	Source Networks	Dest Networks	VLA...	Users	App...	Sou...	Des...	URLs	ISE... Attr...	Action
Mandatory - ACP1 (1-1)													
1	Rule1	Any	Any	192.168.1.40	192.168.2.40	Any	Any	Any	Any	Any	Any	Any	➡ Trust
Default - ACP1 (-)													
There are no rules in this section. Add Rule or Add Category													

Default Action Access Control: Block All Traffic

Snort:

```
# 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:

```
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
```

Lembre-se de que, como o SI é habilitado por padrão, a regra de Confiança é implantada como **permit** ação no LINA para que pelo menos alguns pacotes sejam redirecionados para o mecanismo Snort para inspeção.

Verifique o comportamento

O Packet Tracer mostra que o mecanismo Snort permite o pacote e essencialmente descarrega o fluxo restante para LINA:

```
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_ remark rule-id 268435460: RULE: Prefilter_Rule1
Additional Information:
 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
AppID: service ICMP (3501), application unknown (0)
Firewall: starting rule matching, zone -1 -> -1, geo 0 -> 0, vlan 0, sgt 65535, user 9999997,
icmpType 8, icmpCode 0
Firewall: 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
output-status: up
output-line-status: up
Action: allow
```

Cenário 4. Análise de Pré-Filtro com Regra de Confiança do ACP

Nesse cenário, a SI foi desativada manualmente.

A regra é implantada no Snort da seguinte maneira:

```
# 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.
```

No LINA, a regra é implantada como confiança. Um pacote corresponde à regra de permissão (consulte as contagens de ocorrências de ACE) que é implantada devido à regra Analisar pré-filtro e o pacote é inspecionado pelo mecanismo Snort:

```
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 o comportamento

```
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_ remark rule-id 268435460: RULE: Prefilter_Rule1
```

```
Additional Information:
 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
AppID: service ICMP (3501), application unknown (0)
Firewall: starting rule matching, zone -1 -> -1, geo 0 -> 0, vlan 0, sgt 65535, user 9999997,
icmpType 8, icmpCode 0
Firewall: 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
output-status: up
output-line-status: up
Action: allow
```

Pontos principais

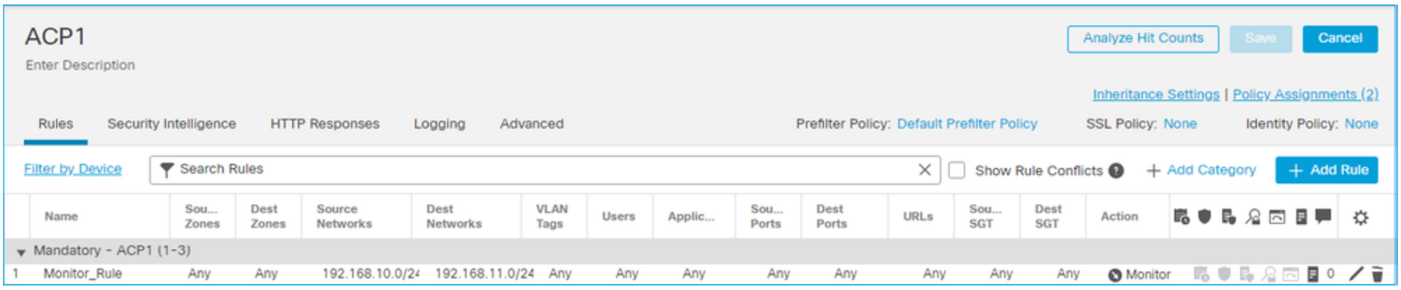
- O **Analyze** A ação é implantada como uma regra de permissão no mecanismo LINA. Isso afeta o pacote a ser encaminhado ao mecanismo Snort para inspeção
- O **Analyze** A ação não implanta nenhuma regra no mecanismo Snort, portanto, é necessário garantir que você configure uma regra no ACP que corresponda ao Snort<
- Depende da regra ACP implantada no mecanismo Snort (**block** vs **allow** vs **fastpath**) nenhum ou todos ou alguns pacotes são permitidos pelo Snort

Casos de uso

- Um caso de uso de **Analyze** A ação é quando você tem uma regra Fastpath ampla na política de Pré-filtro e deseja colocar algumas exceções para fluxos específicos para que eles sejam inspecionados pelo Snort

Ação de monitoramento da ACP

Uma regra de monitoramento configurada na interface do usuário do FMC:



Prefilter Policy: Default Prefilter Policy SSL Policy: None Identity Policy: None

	Name	Sou... Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applic...	Sou... Ports	Dest Ports	URLs	Sou... SGT	Dest SGT	Action	
▾ Mandatory - ACP1 (1-3)															
1	Monitor_Rule	Any	Any	192.168.10.0/24	192.168.11.0/24	Any	Any	Any	Any	Any	Any	Any	Any	Monitor	0

A regra de monitoramento é implantada no mecanismo LINA do FTD como um **permit** e ao mecanismo Snort como um **audit** ação.

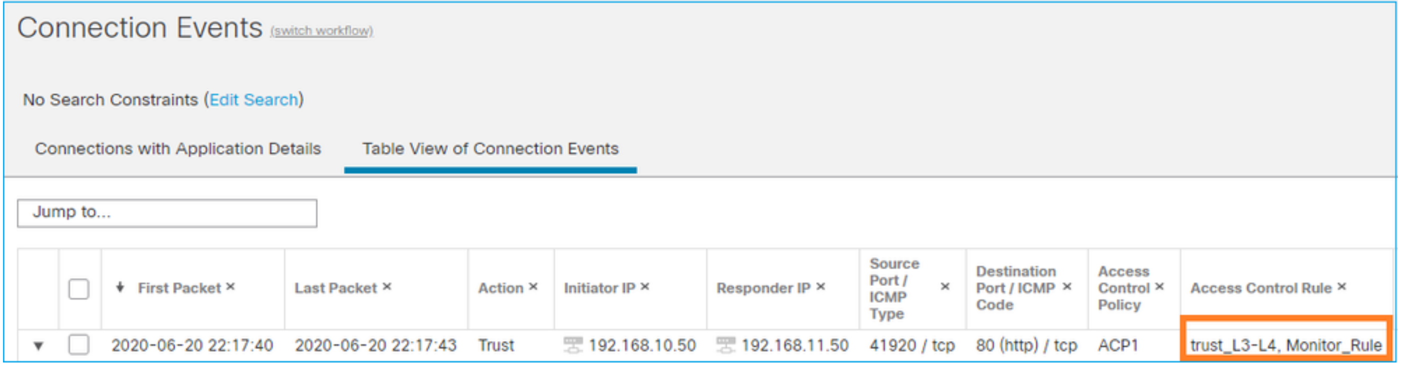
```
firepower# show access-list
…
access-list CSM_FW_ACL_ line 10 advanced permit ip 192.168.10.0 255.255.255.0 192.168.11.0
255.255.255.0 rule-id 268438863 (hitcnt=0) 0x61bbaf0c
```

A regra do Snort:

```
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
```

Pontos principais

- A regra de monitoramento não descarta nem permite tráfego, mas gera um evento de conexão. O pacote é verificado em relação às regras subsequentes e permitido ou descartado
- Os eventos de conexão FMC mostram que o pacote correspondeu a duas regras:



Connection Events (switch workflow)

No Search Constraints (Edit Search)

Connections with Application Details | Table View of Connection Events

Jump to...

		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 mostra que os pacotes correspondem às duas regras:

```
> 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 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, SYN, seq 419031630
192.168.10.50-41922 - 192.168.11.50-80 6 AS 1-1 CID 0 Session: new snort session
192.168.10.50-41922 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service unknown (0), application
unknown (0)
192.168.10.50-41922 > 192.168.11.50-80 6 AS 1-1 I 19 new firewall session
192.168.10.50-41922 > 192.168.11.50-80 6 AS 1-1 I 19 Starting AC with minimum 2, 'Monitor_Rule',
and IPProto first with zone           s -1 -> -1, geo 0 -> 0, vlan 0, source sgt type: 0, source
sgt tag: 0, ISE sgt id: 0, dest sgt type: 0, ISE dest sgt tag: 0,            svc 0, payload 0,
client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.10.50-41922 > 192.168.11.50-80 6 AS 1-1 I 19 match rule order 2, 'Monitor_Rule', action
```

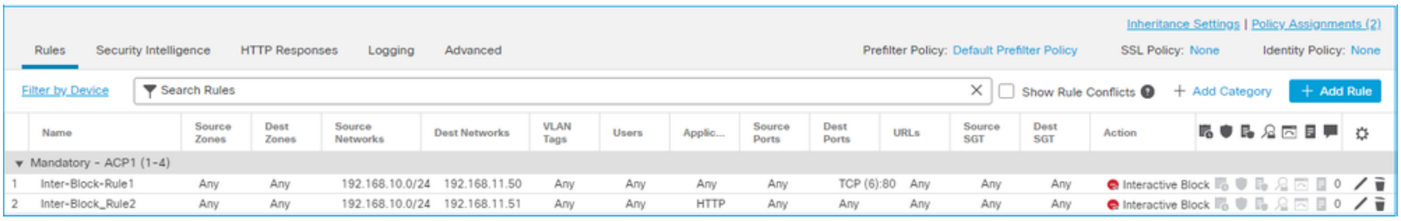
```
Audit
192.168.10.50-41922 > 192.168.11.50-80 6 AS 1-1 I 19 match rule order 3, 'trust_L3-L4', action
Trust
192.168.10.50-41922 > 192.168.11.50-80 6 AS 1-1 I 19 MidRecovery data sent for rule id:
268438858,rule_action:3, rev id:1078           02206, rule_match flag:0x2
```

Casos de uso

Usado para monitorar a atividade de rede e gerar um evento de conexão

Ação de bloqueio interativo da ACP

Uma regra de bloqueio interativo configurada na interface do usuário do 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	0
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	0

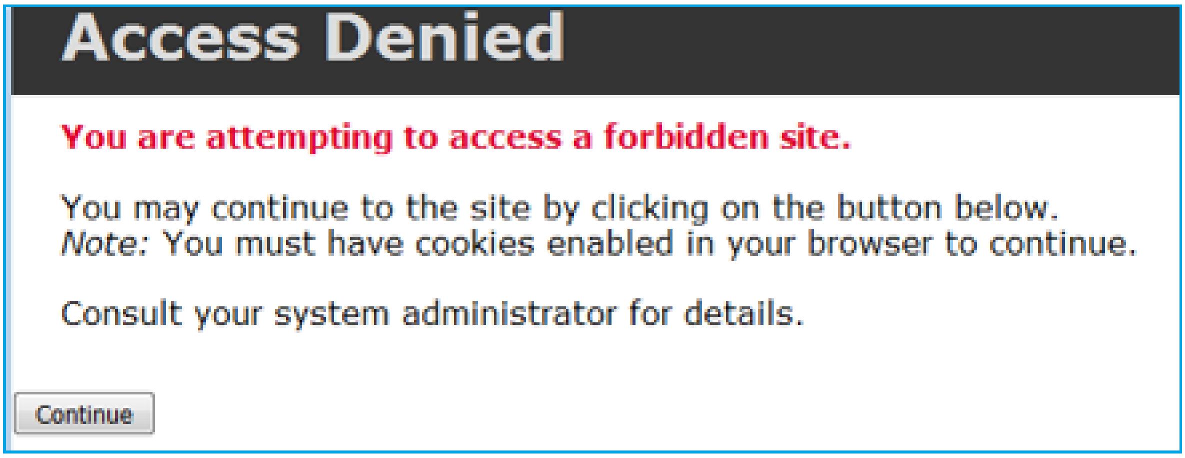
A regra Bloco Interativo é implantada no mecanismo LINA do FTD como um **permit** e para o mecanismo Snort como uma regra de desvio:

```
firepower# show access-list
…
access-list CSM_FW_ACL_ line 9 remark rule-id 268438864: L7 RULE: Inter-Block-Rule1
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=3) 0xba785fc0
access-list CSM_FW_ACL_ line 11 remark rule-id 268438865: ACCESS POLICY: ACP1 - Mandatory
access-list CSM_FW_ACL_ line 12 remark rule-id 268438865: L7 RULE: Inter-Block_Rule2
access-list CSM_FW_ACL_ line 13 advanced permit ip 192.168.10.0 255.255.255.0 host 192.168.11.51
rule-id 268438865 (hitcnt=0) 0x622350d0
```

Mecanismo Snort:

```
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 268438865
```

A regra de bloqueio interativo informa ao usuário que o destino é proibido



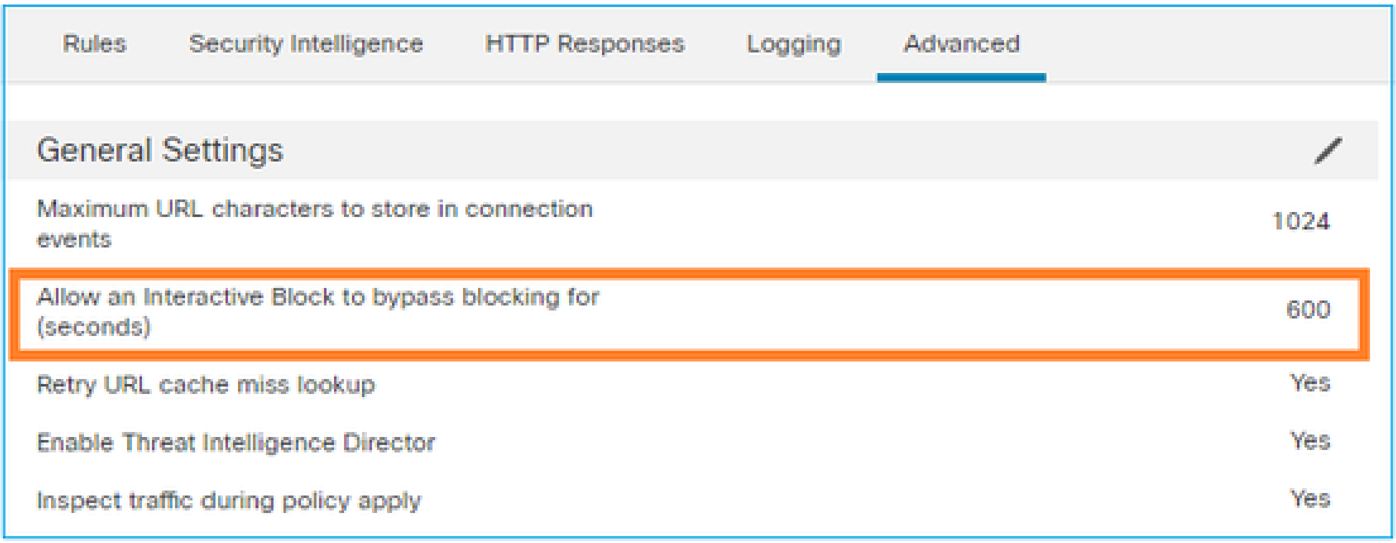
Access Denied

You are attempting to access a forbidden site.

You may continue to the site by clicking on the button below.
Note: You must have cookies enabled in your browser to continue.

Consult your system administrator for details.

Por padrão, o firewall permite ignorar o bloqueio por 600 segundos:



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

No **system support trace** você pode ver que inicialmente o firewall bloqueia o tráfego e mostra a página bloquear:

```
> 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
2014879580
192.168.10.52-58717 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service HTTP (676), application
unknown (0)
192.168.10.52-58717 > 192.168.11.50-80 6 AS 1-1 I 22 Starting AC with minimum 2, 'Inter-Block-
Rule1', and IPProto first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, source sgt type: 0, sgt
tag: 0, ISE sgt id: 0, dest sgt type: 0, ISE dest_sgt_tag: 0, svc 676, payload 0, client 589,
misc 0, user 9999997, min url-cat-list 0-0-0, url http://192.168.11.50/, xff
192.168.10.52-58717 > 192.168.11.50-80 6 AS 1-1 I 22 match rule order 2, 'Inter-Block-Rule1',
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-Rule1', drop
192.168.10.52-58717 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort: processed decoder alerts or actions
queue, drop
192.168.10.52-58717 > 192.168.11.50-80 6 AS 1-1 I 22 deleting firewall session flags = 0x800,
fwFlags = 0x1002
192.168.10.52-58717 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 22, NAP id 1, IPS id 0, 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
```

Depois que o usuário selecionar **Continue** (ou atualiza a página do navegador) a depuração mostra que os pacotes são permitidos pela mesma regra que imita e **Allow** ação:

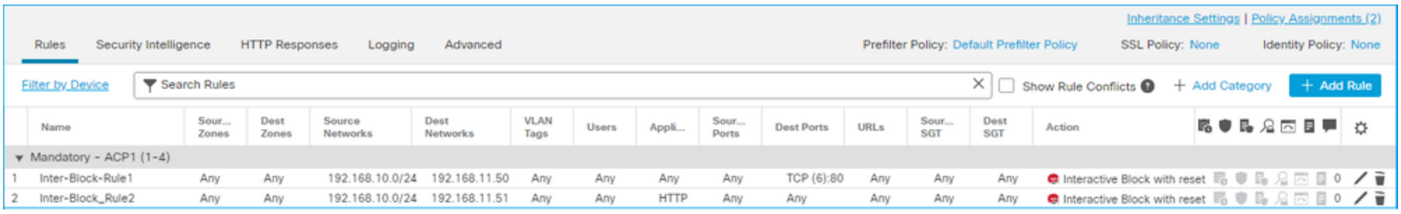
```
192.168.10.52-58718 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, ACK, seq 1357413630, ack
2607625293
192.168.10.52-58718 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service HTTP (676), application
unknown (0)
192.168.10.52-58718 > 192.168.11.50-80 6 AS 1-1 I 8 Starting AC with minimum 2, 'Inter-Block-
Rule1', and IPProto first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, source sgt type: 0, sgt
tag: 0, ISE sgt id: 0, dest sgt type: 0, ISE dest_sgt_tag: 0, svc 676, payload 0, client 589,
misc 0, user 9999997, min url-cat-list 0-0-0, url http://192.168.11.50/, xff
192.168.10.52-58718 > 192.168.11.50-80 6 AS 1-1 I 8 match rule order 2, 'Inter-Block-Rule1',
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
192.168.10.52-58718 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: interactive bypass rule, 'Inter-
Block-Rule1', allow
192.168.10.52-58718 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 8, NAP id 1, IPS id 0, Verdict
PASS
```

Casos de uso

Mostre uma página de aviso aos usuários da Web e dê a eles a opção de continuar.

Ação de bloqueio interativo da ACP com reinicialização

Uma regra de bloqueio interativo com reinicialização configurada na interface do usuário do FMC:



Prefilter Policy: Default Prefilter Policy SSL Policy: None Identity Policy: None

	Name	Sour... Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Appli...	Sour... Ports	Dest Ports	URLs	Sour... 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 with reset	0
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 with reset	0

O Bloco Interativo com regra de redefinição é implantado no mecanismo LINA FTD como um **permit** e para o mecanismo Snort como regra de inserção:

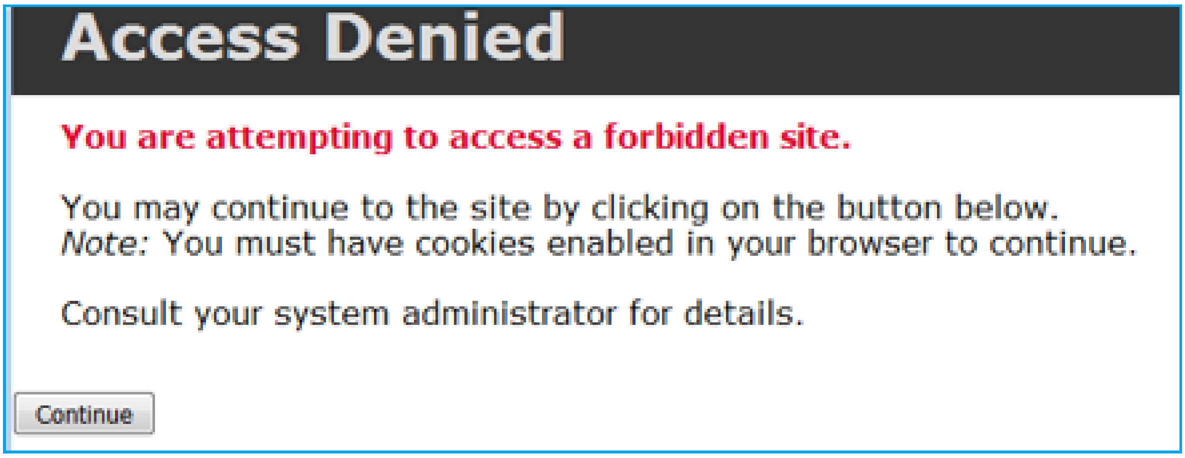
```
firepower# show access-list
…
access-list CSM_FW_ACL_ line 9 remark rule-id 268438864: L7 RULE: Inter-Block-Rule1
access-list CSM_FW_ACL_ line 10 advanced permit tcp 192.168.10.0 255.255.255.0 host
192.168.11.50 eq www rule-id 268438864 (hitcnt=13) 0xba785fc0
access-list CSM_FW_ACL_ line 11 remark rule-id 268438865: ACCESS POLICY: ACP1 - Mandatory
access-list CSM_FW_ACL_ line 12 remark rule-id 268438865: L7 RULE: Inter-Block_Rule2
access-list CSM_FW_ACL_ line 13 advanced permit ip 192.168.10.0 255.255.255.0 host 192.168.11.51
rule-id 268438865 (hitcnt=0) 0x622350d0
```

Mecanismo Snort:

```
# 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
```

Como Bloquear com Redefinição, o usuário pode selecionar o **Continue** opção:



Access Denied

You are attempting to access a forbidden site.

You may continue to the site by clicking on the button below.
Note: You must have cookies enabled in your browser to continue.

Consult your system administrator for details.

Na depuração do Snort, a ação mostrada na reinicialização interativa:

```
> 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 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, SYN, seq 3232128039
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Session: new snort session
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service unknown (0), application
unknown (0)
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 new firewall session
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 Starting AC with minimum 2, 'Inter-Block-
Rule1', and IPProto first with zones -1 -> -1, geo 0 -> 0, vlan 0, source sgt type: 0, source
sgt tag: 0, ISE sgt id: 0, dest sgt type: 0, ISE dest sgt tag: 0, svc 0, payload 0, client 0,
misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 match rule order 2, 'Inter-Block-Rule1',
action Interactive Reset
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 MidRecovery data sent for rule id:
268438864,rule_action:8, rev id:1099034206, rule_match flag:0x0
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 HitCount data sent for rule id: 268438864,
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 24, NAP id 1, IPS id 0, Verdict
PASS

192.168.11.50-80 - 192.168.10.52-58958 6 AS 1-1 CID 0 Packet: TCP, SYN, ACK, seq 2228213518, ack
3232128040
192.168.11.50-80 - 192.168.10.52-58958 6 AS 1-1 CID 0 AppID: service unknown (0), application
unknown (0)
192.168.11.50-80 - 192.168.10.52-58958 6 AS 1-1 CID 0 Snort id 24, NAP id 1, IPS id 0, Verdict
PASS

192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, ACK, seq 3232128040, ack
2228213519
```

```
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service unknown (0), application
unknown (0)
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 24, NAP id 1, IPS id 0, Verdict
PASS

192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, ACK, seq 3232128040, ack
2228213519
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service HTTP (676), application
unknown (0)
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 Starting AC with minimum 2, 'Inter-Block-
Rule1', and IPProto first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, source sgt type: 0, sgt
tag: 0, ISE sgt id: 0, dest sgt type: 0, ISE dest_sgt_tag: 0, svc 676, payload 0, client 589,
misc 0, user 9999997, min url-cat-list 0-0-0, url http://192.168.11.50/, xff
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 match rule order 2, 'Inter-Block-Rule1',
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-Rule1', drop
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort: processed decoder alerts or actions
queue, drop
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 deleting firewall session flags = 0x800,
fwFlags = 0x1002
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 24, NAP id 1, IPS id 0, 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
```

Nesse ponto, a página de bloqueio é mostrada para o usuário final. Se o usuário selecionar **Continue** (ou atualiza a página da Web) a mesma regra corresponde à qual esse horário permite o tráfego:

```
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 6 AS 1-1 CID 0 AppID: service HTTP (676), application
unknown (0)
192.168.10.52-58962 > 192.168.11.50-80 6 AS 1-1 I 14 Starting AC with minimum 2, 'Inter-Block-
Rule1', and IPProto first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, source sgt type: 0, sgt
tag: 0, ISE sgt id: 0, dest sgt type: 0, ISE dest_sgt_tag: 0, svc 676, payload 0, client 589,
misc 0, user 9999997, min url-cat-list 0-0-0, url http://192.168.11.50/, xff
192.168.10.52-58962 > 192.168.11.50-80 6 AS 1-1 I 14 match rule order 2, 'Inter-Block-Rule1',
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 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: allow rule, 'Inter-Block-Rule1',
allow
192.168.10.52-58962 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: interactive bypass rule, 'Inter-
Block-Rule1', allow
192.168.10.52-58962 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 14, NAP id 1, IPS id 0, 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
192.168.11.50-80 - 192.168.10.52-58962 6 AS 1-1 CID 0 AppID: service HTTP (676), application
unknown (0)
192.168.11.50-80 - 192.168.10.52-58962 6 AS 1-1 CID 0 Firewall: allow rule, 'Inter-Block-Rule1',
allow
192.168.11.50-80 - 192.168.10.52-58962 6 AS 1-1 CID 0 Firewall: interactive bypass rule, 'Inter-
Block-Rule1', allow
192.168.11.50-80 - 192.168.10.52-58962 6 AS 1-1 CID 0 Snort id 14, NAP id 1, IPS id 0, Verdict
PASS
```

A regra de bloqueio interativo com reinicialização envia um TCP RST para o tráfego fora da Web:

```
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(0) win 29200 <mss 1460,sackOK,timestamp 3745225378 0,nop,wscale 7>
   3: 22:13:33.113626       802.1Q vlan#202 P0 192.168.11.50.21 > 192.168.10.50.40010: S
3422362500:3422362500(0) ack 3109534921 win 8192 <mss 1380,nop,wscale 8,sackOK,timestamp
53252448 3745225378>
   4: 22:13:33.113824       802.1Q vlan#202 P0 192.168.10.50.40010 > 192.168.11.50.21: . ack
3422362501 win 229 <nop,nop,timestamp 3745225379 53252448>
   5: 22:13:33.114953       802.1Q vlan#202 P0 192.168.11.50.21 > 192.168.10.50.40010: P
3422362501:3422362543(42) ack 3109534921 win 256 <nop,nop,timestamp 53252448 3745225379>
   6: 22:13:33.114984       802.1Q vlan#202 P0 192.168.11.50.21 > 192.168.10.50.40010: P
3422362543:3422362549(6) ack 3109534921 win 256 <nop,nop,timestamp 53252448 3745225379>
   7: 22:13:33.114984       802.1Q vlan#202 P0 192.168.11.50.21 > 192.168.10.50.40010: P
3422362549:3422362570(21) ack 3109534921 win 256 <nop,nop,timestamp 53252448 3745225379>
   8: 22:13:33.115182       802.1Q vlan#202 P0 192.168.10.50.40010 > 192.168.11.50.21: . ack
3422362543 win 229 <nop,nop,timestamp 3745225381 53252448>
   9: 22:13:33.115411       802.1Q vlan#202 P0 192.168.10.50.40010 > 192.168.11.50.21: . ack
3422362549 win 229 <nop,nop,timestamp 3745225381 53252448>
  10: 22:13:33.115426       802.1Q vlan#202 P0 192.168.10.50.40010 > 192.168.11.50.21: . ack
3422362570 win 229 <nop,nop,timestamp 3745225381 53252448>
  12: 22:13:34.803699       802.1Q vlan#202 P0 192.168.10.50.40010 > 192.168.11.50.21: P
3109534921:3109534931(10) ack 3422362570 win 229 <nop,nop,timestamp 3745227069 53252448>
  13: 22:13:34.804523       802.1Q vlan#202 P0 192.168.11.50.21 > 192.168.10.50.40010: R
3422362570:3422362570(0) ack 3109534931 win 0
```

Conexões secundárias de FTD e Pinholes

Em versões mais antigas (por exemplo, 6.2.2, 6.2.3, etc.), o mecanismo Snort não abrirá buracos para conexões secundárias (por exemplo, dados de FTD) se você usar o **Trust** ação. Em versões recentes, esse comportamento é alterado e o mecanismo Snort abre os buracos mesmo com o **Trust** ação.

Diretrizes e regras do FTD

- Use as regras de fastpath da política de pré-filtro para grandes fluxos e para diminuir a latência através da caixa
- Use as regras de bloqueio de pré-filtro para o tráfego que deve ser bloqueado de acordo com as condições L3/L4
- Use as regras de confiança da ACP, se desejar ignorar muitas das verificações do Snort, mas ainda aproveitar recursos como política de identidade, QoS, SI, detecção de aplicações, filtro de URL
- Coloque as regras que afetam menos o desempenho do firewall na parte superior da política de controle de acesso seguindo destas diretrizes:

1. Regras de bloqueio (camadas de 1 a 4) – Bloqueio de pré-filtro
2. Regras de permissão (camadas de 1 a 4) – Fastpath de pré-filtro
3. Regras de bloqueio da ACP (camadas de 1 a 4)
4. Regras de confiança (camadas de 1 a 4)
5. Regras de bloqueio (camadas de 5 a 7 – detecção de aplicações, filtragem de URL)
6. Regras de permissão (camadas de 1 a 7 – detecção de aplicações, filtragem de URL,

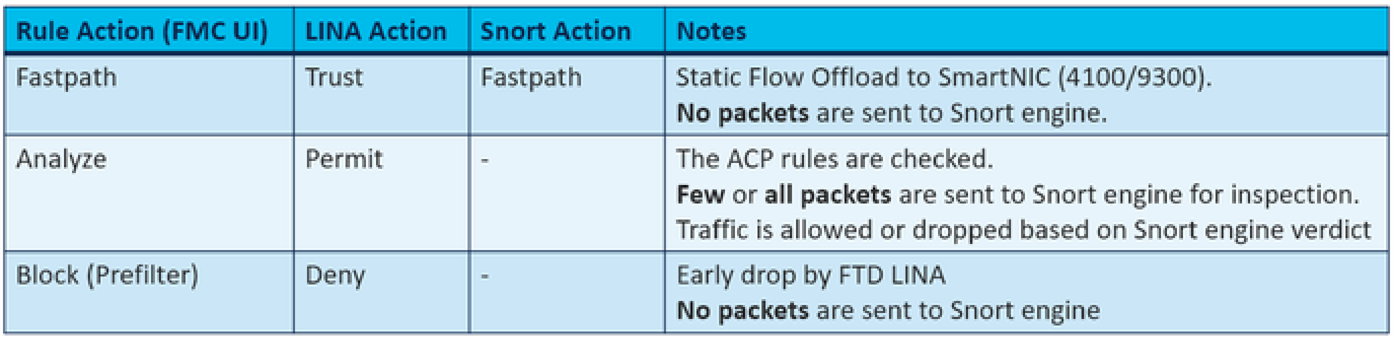
política de invasão/política de arquivos)
7. Regra de bloqueio (regra padrão)

- Evite o registro excessivo (faça login no início ou no término e evite ambos ao mesmo tempo)
- Não se esqueça da expansão da regra para verificar o número de regras no LINA

```
firepower# show access-list | include elements
access-list CSM_FW_ACL_; 7 elements; name hash: 0x4a69e3f3
```

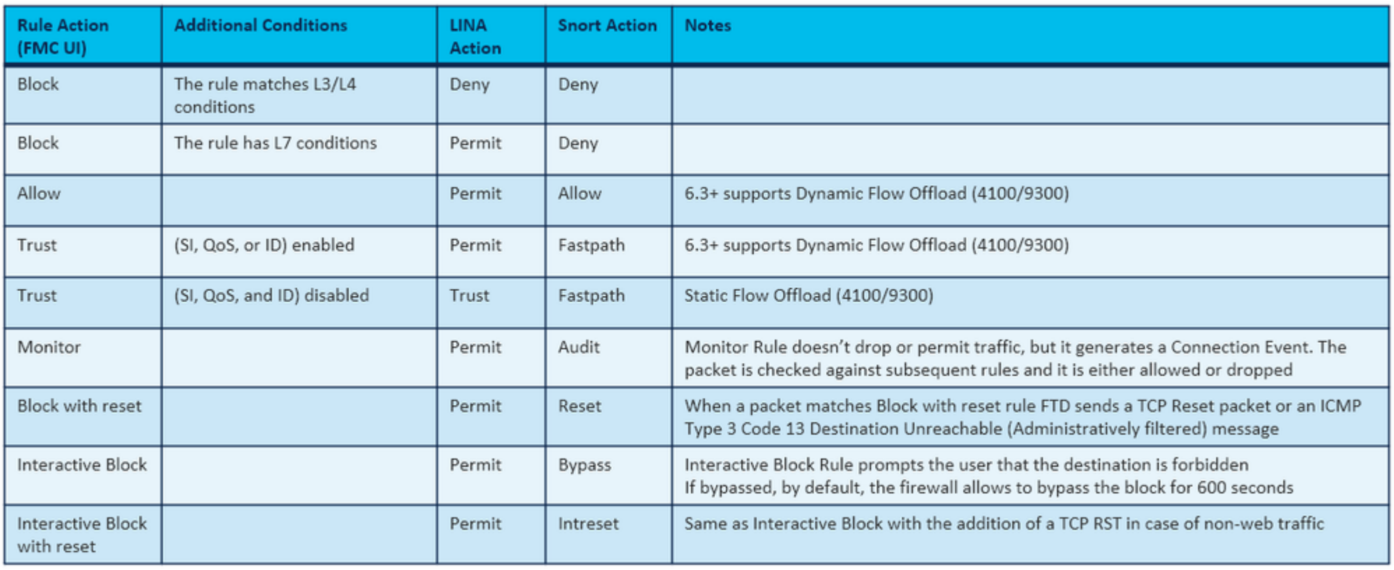
Summary

Ações de pré-filtro



Rule Action (FMC UI)	LINA Action	Snort Action	Notes
Fastpath	Trust	Fastpath	Static Flow Offload to SmartNIC (4100/9300). **No packets** are sent to Snort engine.
Analyze	Permit	-	The ACP rules are checked. **Few** or **all packets** 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 **No packets** are sent to Snort engine

Ações da 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

Note: A partir do código 6.3 do software FTD, o descarregamento dinâmico de fluxo pode descarregar conexões que atendam a critérios adicionais, por exemplo, pacotes confiáveis que exigem inspeção Snort. Verifique a seção 'Transferir grandes conexões (fluxos)' no guia de configuração do Firepower Management Center para obter mais detalhes

Informações Relacionadas

- Regras de controle de acesso do FTD
- Pré-filtragem e políticas de pré-filtro do FTD
- Analisar as capturas do Firepower Firewall para solucionar problemas de rede com eficiência
- Como trabalhar com as capturas do Firepower Threat Defense (FTD) e Packet-Tracer
- Configurar o registro no FTD usando o FMC
- Suporte Técnico e Documentação - Cisco Systems
- Transferência de grandes conexões

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.