

# Firepower Threat Defense アクセスコントロール ポリシー ルール アクションの明確化

## 内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[ACP の展開方法](#)

[設定](#)

[ACP で実行可能なアクション](#)

[ACP とプレフィルタポリシーの連携方法](#)

[ACP ブロックアクション](#)

[シナリオ 1：早期 LINA ドロップ](#)

[シナリオ 2：Snort 判定によるドロップ](#)

[リセットアクションによる ACP ブロック](#)

[ACP 許可アクション](#)

[シナリオ 1：ACP 許可アクション \(L3/L4 条件\)](#)

[シナリオ 2：ACP 許可アクション \(L3-7 条件\)](#)

[シナリオ 3：許可による Snort 早送り判定](#)

[ACP 信頼アクション](#)

[シナリオ 1：ACP 信頼アクション](#)

[シナリオ2:ACPの信頼アクション \(SI、QoS、およびアイデンティティポリシーなし\)](#)

[プレフィルタ ポリシー ブロック アクション](#)

[プレフィルタポリシー Fastpath アクション](#)

[プレフィルタポリシー Fastpath アクション \(インラインセット\)](#)

[プレフィルタポリシー Fastpath アクション \(タップによるインラインセット\)](#)

[プレフィルタポリシー分析アクション](#)

[シナリオ 1：ACP ブロックルールによるプレフィルタ分析](#)

[シナリオ 2：ACP 許可ルールによるプレフィルタ分析](#)

[シナリオ 3：ACP 信頼ルールによるプレフィルタ分析](#)

[シナリオ 4：ACP 信頼ルールによるプレフィルタ分析](#)

[ACP モニタアクション](#)

[ACP インタラクティブ ブロック アクション](#)

[リセットアクションによる ACP インタラクティブブロック](#)

[FTD セカンダリ接続とピンホール](#)

[FTD ルールのガイドライン](#)

[要約](#)

[関連情報](#)

## 概要

このドキュメントでは、Firepower Threat Defense ( FTD ) アクセス コントロール ポリシー ( ACP ) およびプレフィルタポリシーで実行可能なさまざまなアクションについて説明します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- フロー オフロード
- Firepower Threat Defense アプライアンスでのパケットキャプチャ
- FTD アプライアンスのトレースオプションを使用したパケットトレーサおよびキャプチャ

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Firepower 4110 Threat Defense バージョン 6.4.0 ( ビルド 113 ) および 6.6.0 ( ビルド 90 )
- Firepower Management Center ( FMC ) バージョン 6.4.0 ( ビルド 113 ) および 6.6.0 ( ビルド 90 )

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期 ( デフォルト ) 設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

### 関連製品

このドキュメントは、次のバージョンのハードウェアとソフトウェアにも使用できます。

- 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 ) 、 カーネルベース仮想マシン ( KVM )
- サービス統合型ルータ ( ISR ) ルータモジュール
- FTD ソフトウェアバージョン 6.1.x 以降

注：フローオフロードは、ASAおよびFTDアプリケーションのネイティブインスタンス、FPR4100およびFPR9300プラットフォームでのみサポートされます。FTDコンテナインスタンスはフローオフロードをサポートしません。

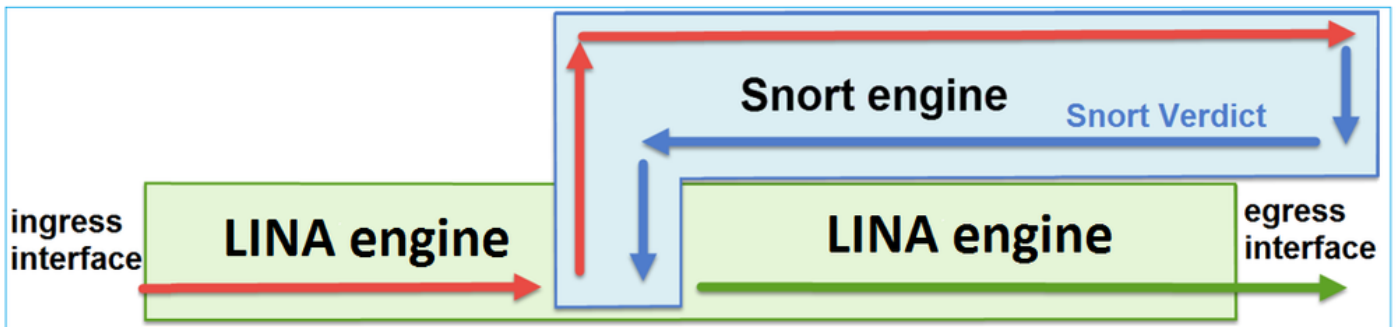
## 背景説明

各アクションのバックグラウンド動作と、フローオフロードやセカンダリ接続を開くプロトコルなどの他の機能との相互作用を調べます。

FTD は、2 つの主要なエンジンで構成される統合ソフトウェアイメージです。

- LINA エンジン
- Snortエンジン

次の図に、2 つのエンジンがどのように連携するかを示します。



- パケットが入カインターフェイスに入り、LINA エンジンによって処理される
- FTD ポリシーで求められている場合、パケットが Snort エンジンによって検査される
- Snortエンジンは、パケットの判定 ( 許可リストまたはブロックリスト ) を返します
- LINA エンジンは、Snort の判定に基づいてパケットをドロップまたは転送する

## ACP の展開方法

FTD ポリシーは、オフボックス ( リモート ) 管理が使用される場合は FMC で、ローカル管理が使用される場合は Firepower Device Manager ( FDM ) で設定されます。どちらのシナリオでも、ACP は次のように展開されます。

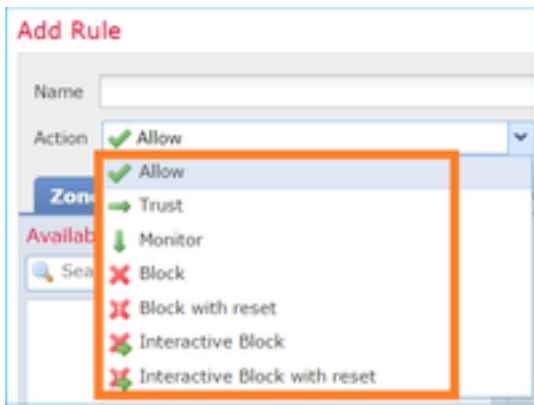
- CSM\_FW\_ACL\_ という名前のグローバルアクセスコントロールリスト (ACL) から FTD LINA エンジンへ
- /ngfw/var/sf/detection\_engines/<UUID>/ngfw.rules ファイルのアクセス制御 ( AC ) ルールが FTD Snort エンジンへ

## 設定

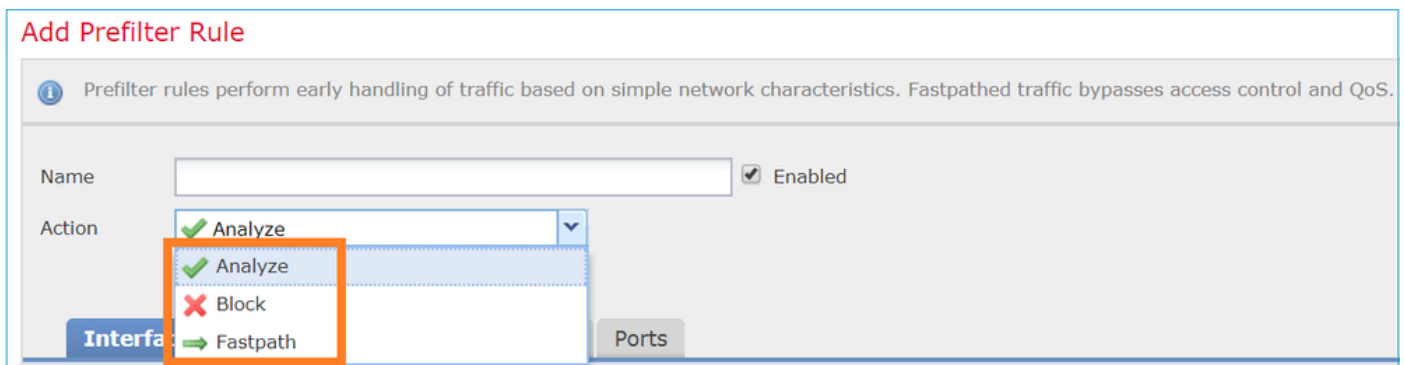
### ACP で実行可能なアクション

FTD ACP には 1 つ以上のルールが含まれており、各ルールには次のいずれかのアクションを設定できます ( 図を参照 )。

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



同様に、プレフィルタポリシーには1つ以上のルールを含めることができます。実行可能なアクションを次の図に示します。



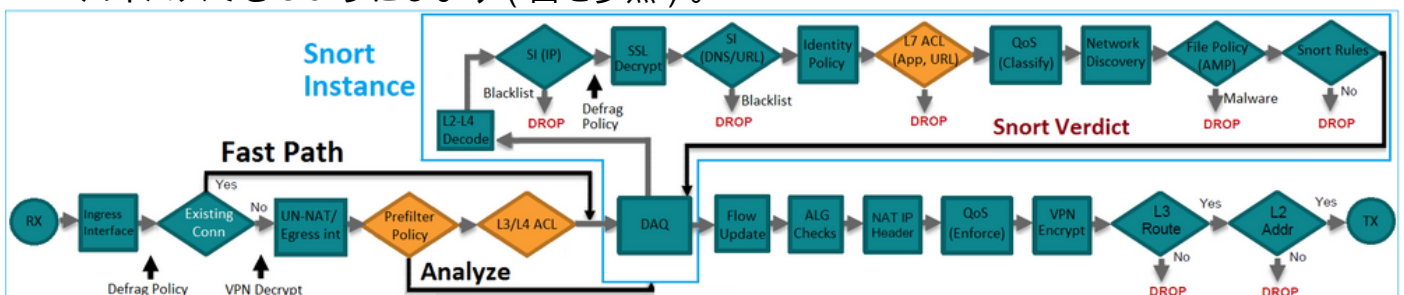
## ACP とプレフィルタポリシーの連携方法

プレフィルタポリシーは6.1バージョンで導入され、主に2つの目的を果たします。

- このポリシーにより、FTD LINA エンジンが外部 IP ヘッダーをチェックし、Snort エンジンが内部 IP ヘッダーをチェックするトンネル化トラフィックの検査が可能になります。具体的には、トンネリングされたトラフィック ( GRE など ) の場合、プレフィルタポリシーのルールは常に outer headers, 一方、ACP のルールは常に内部セッションに適用されます ( inner headers ). トンネル化トラフィックは、次のプロトコルを参照します。

- GRE
- IP-in-IP
- IPv6-IP
- Teredo ポート 3544

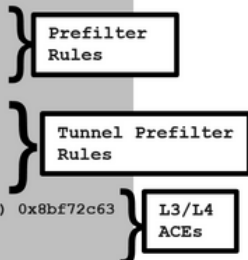
- Early Access Control ( EAC ; 早期アクセス制御 ) により、フローが Snort エンジン を完全にバイパスできるようにします ( 図を参照 ) 。



プレフィルタルールは、図に示すように、L3/L4アクセスコントロールエレメント(ACE)として

FTDに展開され、設定されたL3/L4 ACEの前に配置されます。

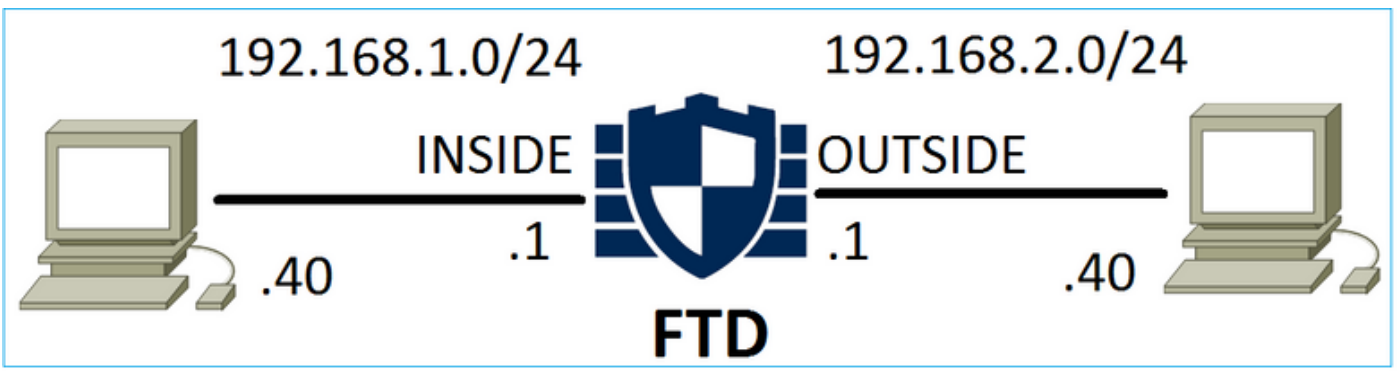
```
firepower# show access-list
access-list CSM_FW_ACL_ line 1 remark rule-id 268434457: PREFILTER POLICY: FTD_Prefilter_Policy
access-list CSM_FW_ACL_ line 2 remark rule-id 268434457: RULE: Fastpath_Rule1
access-list CSM_FW_ACL_ line 3 advanced trust ip host 192.168.75.16 any rule-id 268434457 event-log 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) 0xald3780e
```



注：プレフィルタルールと ACP ルールのうち、最初に一致した方が適用されます。

## ACP ブロックアクション

次の図に示すトポロジについて考えてみます。



### シナリオ 1：早期 LINA ドロップ

ACP には、図に示すように、L4 条件 (宛先ポート TCP 80) を使用する [ブロック (Block)] ルールが含まれています。

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

Snort に展開されたポリシー：

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

LINA に展開されたポリシー。このルールは次のようにプッシュされます。 deny action:

```
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
```

## 動作の検証：

ホストA(192.168.1.40)がホストB(192.168.2.40)へのHTTPセッションを開こうとすると、FTD LINAエンジンによってTCP同期(SYN)パケットがドロップされ、Snortエンジンまたは宛先に到達しません。

```
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
```

## シナリオ 2：Snort 判定によるドロップ

ACP には、図に示すように、L7 条件 ( アプリケーション HTTP ) を使用する [ブロック ( Block ) ] ルールが含まれています。

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

Snort に展開されたポリシー :

```
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

LINA に展開されたポリシー。

注 : このルールは次のようにプッシュされます。 permit LINAはセッションがHTTPを使用していることを判断できないため、アクションを実行します。FTDでは、アプリケーション検出メカニズムはSnortエンジンにあります。

```
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
```

を使用するブロックルールの場合 Application 条件として、実際のパケットのトレースは、Snortエンジンの判定により、LINAによってセッションがドロップされたことを示します。

注 : Snort エンジンがアプリケーションを判別するには、いくつかのパケット ( 通常はアプリケーションデコーダに応じて 3 ~ 10 ) を検査する必要があります。そのため、いくつかのパケットが FTD の通過を許可され、宛先に到達します。許可されたパケットは、引き続きACLに基づく侵入ポリシーチェックの対象となります。 Access Policy > Advanced > 'Intrusion Policy used before Access Control rule is determined' オプション。

動作の検証 :

ホスト A ( 192.168.1.40 ) がホスト B ( 192.168.2.40 ) との HTTP セッションを確立しようとする、LINA の入力キャプチャには次のように表示されます。

```
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>
...
```

出力キャプチャ :

```
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>
```

このトレースは、アプリケーション検出の判定がまだ到達していないために、最初のパケット (TCP SYN)がSnortによって許可されていることを示しています。

```
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**

TCP SYN/ACK パケットについても同様です。

```
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**

3番目のパケットの検査が完了すると、SnortはDROP判定を返します。

```
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
```

コマンドを実行することもできます `system support trace` FTD CLISHモードから実行します。このツールには2つの機能があります。

- Data Acquisition Library(DAQ)に送信され、LINAで確認される各パケットのSnort判定を表示します。DAQは、FTD LINAエンジンとSnortエンジンの間に配置されているコンポーネントです。
- を実行できる `system support firewall-engine-debug` 同時に、Snortエンジン自体で何が起こるかを確認できます

出力は以下のとおりです。

```
> 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
```

## 要約

- ACP ブロックアクション は、ルールの条件に応じて、LINA で permit ルールまたは deny ルールとして展開されます。
- 条件が L3/L4 の場合、LINA はパケットをブロックします。TCP の場合、最初のパケット (TCP SYN) はブロックされます
- 条件が L7 の場合、パケット は追加の検査のために Snort エンジンに転送されます。TCP の場合、Snort が判定に達するまでの間、いくつかのパケット が FTD の通過を許可されます。許可されたパケットは、引き続き ACL に基づく侵入ポリシーチェックの対象となります。  
Access Policy > Advanced > 'Intrusion Policy used before Access Control rule is determined' オプション。

## リセットアクションによる ACP ブロック

FMC UI で設定されたリセットによるブロックルール :

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	Block with reset
2	Block-RST_Rule2	Any	Any	192.168.10.0/24	192.168.11.51	Any	Any	HTTP	Any	Any	Any	Any	Block with reset

Block with resetルールは、FTD LINAエンジン上で次のように展開されます permit Snortエンジンに対して reset rule :

```
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
```

Snort エンジン :

```
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
```

パケットがBlock with reset ruleに一致すると、FTDは TCP Reset パケットまたは ICMP Type 3 Code 13 Destination Unreachable ( 管理上フィルタ処理 ) メッセージ :

```
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.
```

次に、FTD 入カインターフェイスで取得されたキャプチャを示します。

```
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 この場合の出力は、Snortの判定によりパケットがドロップされたことを示しています。

> 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
```

## 使用例

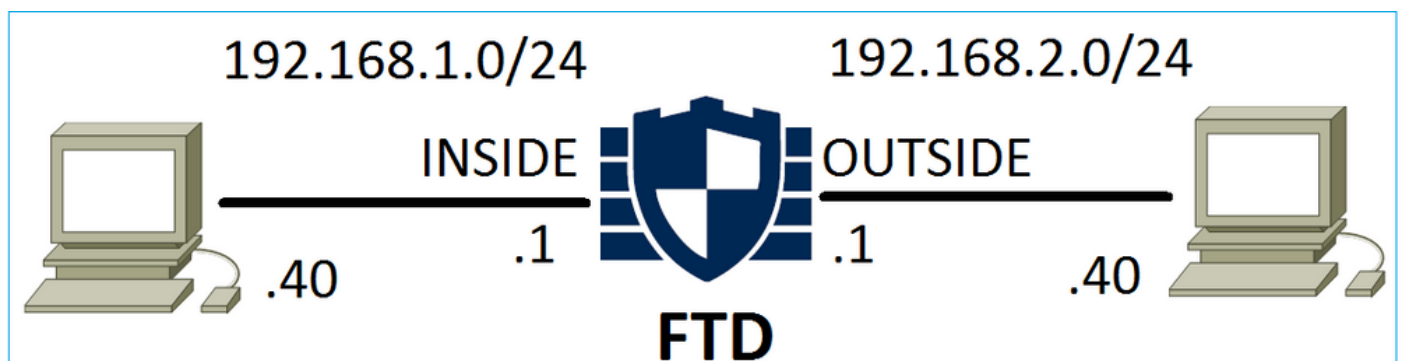
と同じ Block 接続を直ちに終了します。

## ACP 許可アクション

### シナリオ 1： ACP 許可アクション ( L3/L4 条件 )

通常は、侵入ポリシーやファイルポリシーなどの付加的な検査を指定する許可ルールを設定します。この最初のシナリオでは、L3/L4条件が適用された場合のAllowルールの動作を示します。

図に示されているトポロジについて検討します。



このポリシーは、図に示されているように適用されます。

Access Control > Access Control													
			Network Discovery			Application Detectors			Correlation		Actions ▼		
<b>ACP1</b>													
Enter Description													
Prefilter Policy: <a href="#">Default Prefilter Policy</a>				SSL Policy: <a href="#">None</a>				Identity Policy: <a href="#">None</a>					
<a href="#">Inheritance Settings</a>													
<b>Rules</b>   Security Intelligence   HTTP Responses   Advanced													
Filter by Device <input type="checkbox"/> Show Rule Conflicts <input type="checkbox"/> Add Category <input type="button" value="+"/> Add Rule <input type="text" value="Search Rules"/>													
#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN T...	Users	Applica...	Source ...	Dest Ports	URLs	ISE/SGT Action Attribu...	
▼ 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

Snort に展開されたポリシー。このルールはVLAN 1000に対して allow action:

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

LINA 内のポリシー。

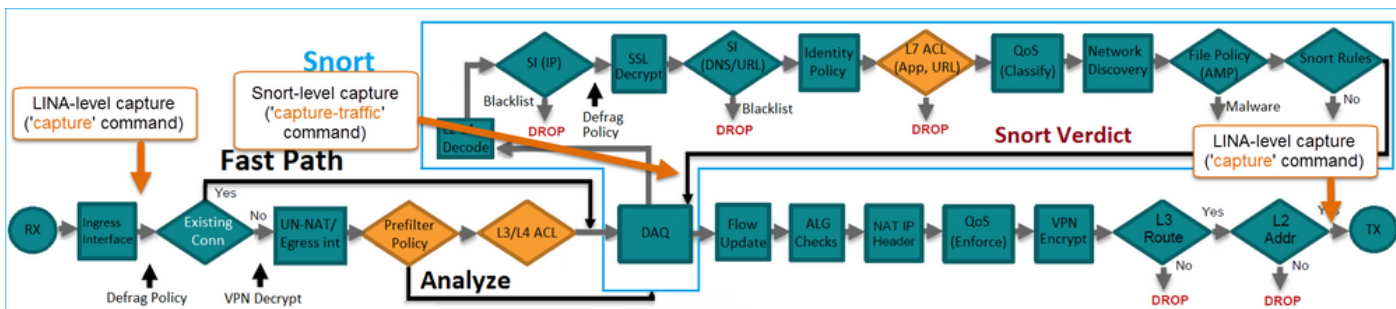
注：このルールは、permit アクションは、基本的に、さらなる検査のためにSnortにリダイレクトされることを意味します。

```
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
```

FTDがAllowルールに一致するフローをどのように処理するかを確認するには、いくつかの方法があります。

- Snort 統計の検証
- system support trace CLISH ツールの使用
- LINA の trace オプションで キャプチャを使用し、オプションとして Snort エンジンで capture-traffic を使用

LINA キャプチャと Snort capture-traffic :



動作の検証 :

Snortの統計情報をクリアし、 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
```

Pass Packetsカウンタが増加します。

```
> 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  
...
```

Passed Packets = Snort エンジンによる検査を受けたパケット

## シナリオ 2 : ACP 許可アクション ( L3-7 条件 )

許可ルールを次のように展開すると、同様の動作が発生します。

図に示すように、L3/L4条件のみ :

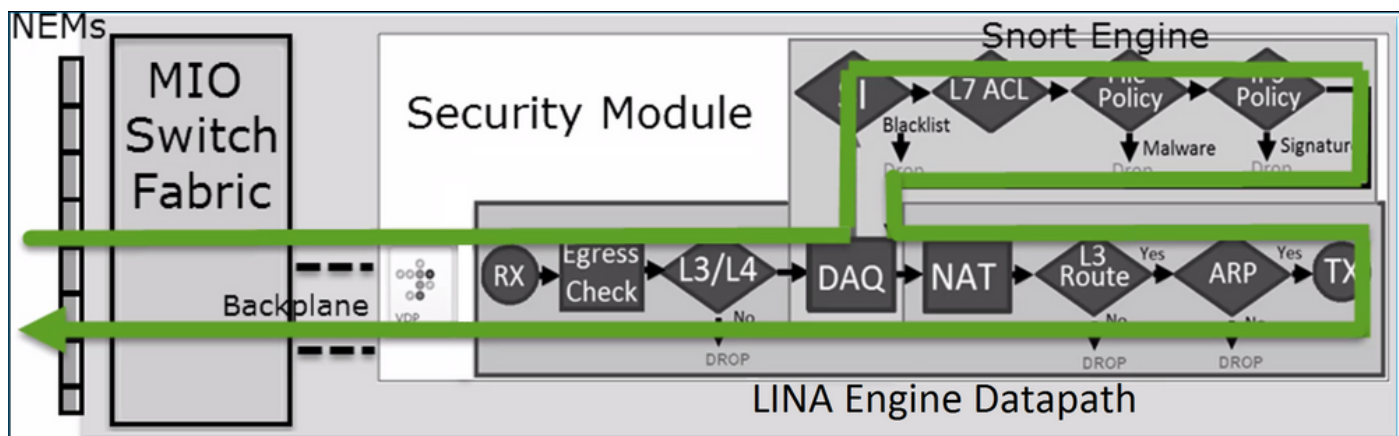
#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN T...	Users	Applica...	Source ...	Dest Ports	URLs	ISE/SGT Attribu...	Action
Mandatory - ACP1 (1-1)													
1	Rule1	Any	Any	192.168.1.40	192.168.2.40	Any	Any	Any	Any	Any	Any	Any	Allow

L7条件 ( 侵入ポリシー、ファイルポリシー、アプリケーションなど ) が図に示されています。

#	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

## 要約

要約すると、次の図に示すように、許可ルールが一致した場合、FP4100/9300 に展開された FTD によってフローが処理されます。



注：管理入出力 ( MIO ) は、Firepower シャーシのスーパーバイザエンジンです。

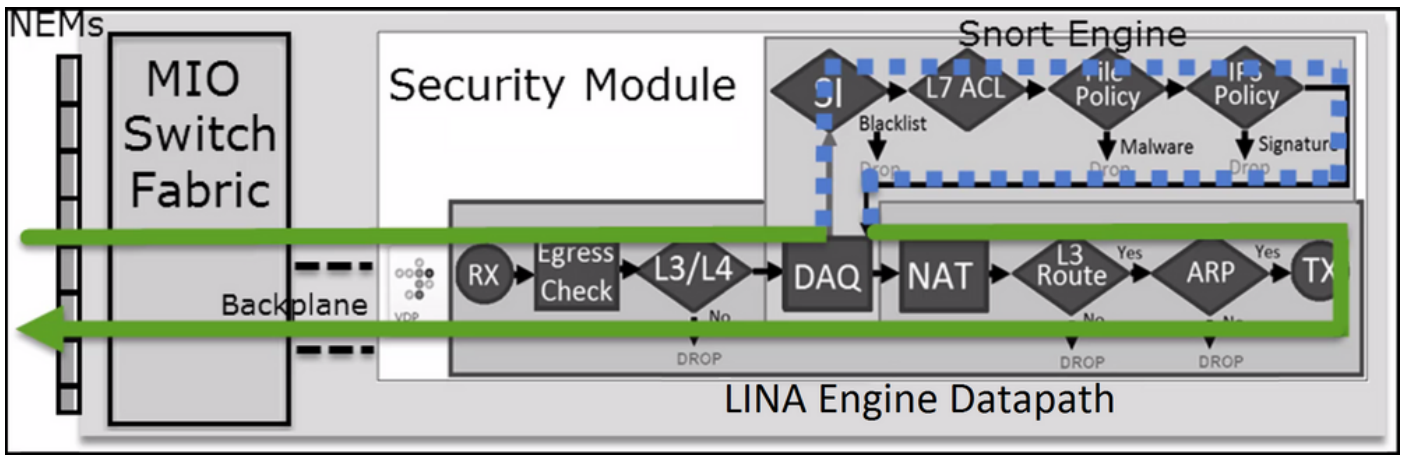
## シナリオ 3：許可による Snort 早送り判定

FTD SnortエンジンがPERMITLIST判定 ( 早送り ) を行い、フローの残りの部分がLINAエンジンにオフロードされる(場合によっては、HWアクセラレータ(SmartNIC)にオフロードされる)特定のシナリオがあります。内容は次のとおりです。

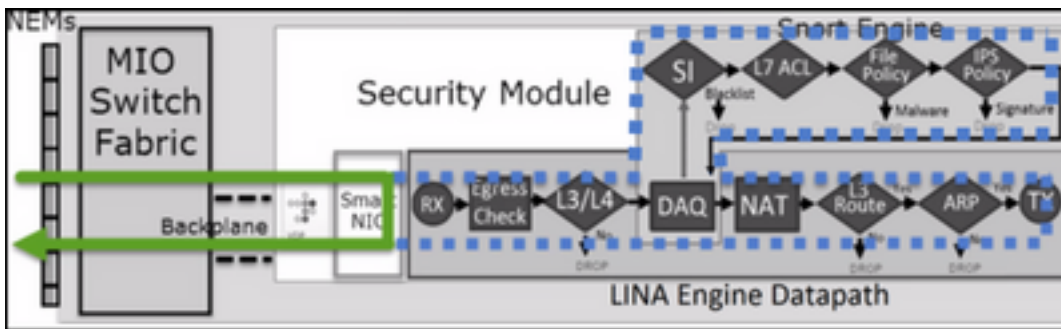
1. SSL ポリシーが設定されていない SSL トラフィック
2. インテリジェント アプリケーション バイパス ( IAB )

パケットパスの視覚的な表現を次に示します。





場合によっては、



## 主なポイント

- 許可ルールは次のように展開されます allow Snortおよび permit リーナ
- ほとんどの場合、セッションのすべてのパケットは追加検査のためにSnortエンジンに転送されます

## 使用例

Snort エンジンによる L7 検査が必要な場合は、次のような許可ルールを設定します。

- 侵入ポリシー
- ファイルポリシー ( File Policy )

## ACP 信頼アクション

### シナリオ 1： ACP 信頼アクション

Snortレベルで高度なL7インスペクション（侵入ポリシー、ファイルポリシー、ネットワークディスカバリなど）を適用せずに、セキュリティインテリジェンス(SI)、アイデンティティポリシー、QoSなどの機能を引き続き使用する場合は、ルールでTrustアクションを使用することをお勧めします。

トポロジ：



設定されたポリシー :

ACP1															Analyze Hit Counts	Save	Cancel			
Enter Description															<a href="#">Inheritance Settings</a>   <a href="#">Policy Assignments (1)</a>					
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	Trust							

FTD Snort エンジンで展開される信頼ルール :

```
# 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)
```

注 : 番号 6 はプロトコル ( TCP ) です。

FTD LINA のルール :

```
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
```

検証 :

Enable system support trace ホストA(192.168.10.50)からホストB(192.168.11.50)へのHTTPセッションを開始します。3つのパケットが Snort エンジンに転送されます。SnortエンジンはLINAに PERMITLIST判定を送信し、LINAエンジンへの残りのフローが実質的にオフロードされます。

> **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
```

接続が終了すると、Snort エンジンは LINA エンジンからメタデータ情報を取得し、セッションを削除します。

```
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
```

Snortキャプチャは、Snortエンジンに送信される3つのパケットを示します。

```
> 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
```

LINA キャプチャには、LINA を通過するフローが表示されます。

```
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>
```

```
...
```

LINA からのパケットのトレースは、Snort 判定を確認するもう 1 つの方法です。最初のパケットは PASS 判定を受けました。

```
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
```

OUTSIDEインターフェイスのTCP SYN/ACKパケットのトレース：

```
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
```

TCP ACKはPERMITLIST判定を取得します。

```
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
```

これは Snort 判定 ( パケット #3 ) の完全な出力です。

```
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
```

判定がLINAエンジンによってキャッシュされるため、4番目のパケットはSnortエンジンに転送されません。

```
firepower# show capture CAPI packet-number 4 trace
```

```
441 packets captured
```

```
4: 10:34:02.741523      802.1Q vlan#202 PO 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
```

Snort 統計でこの点を確認できます。

```
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:
```

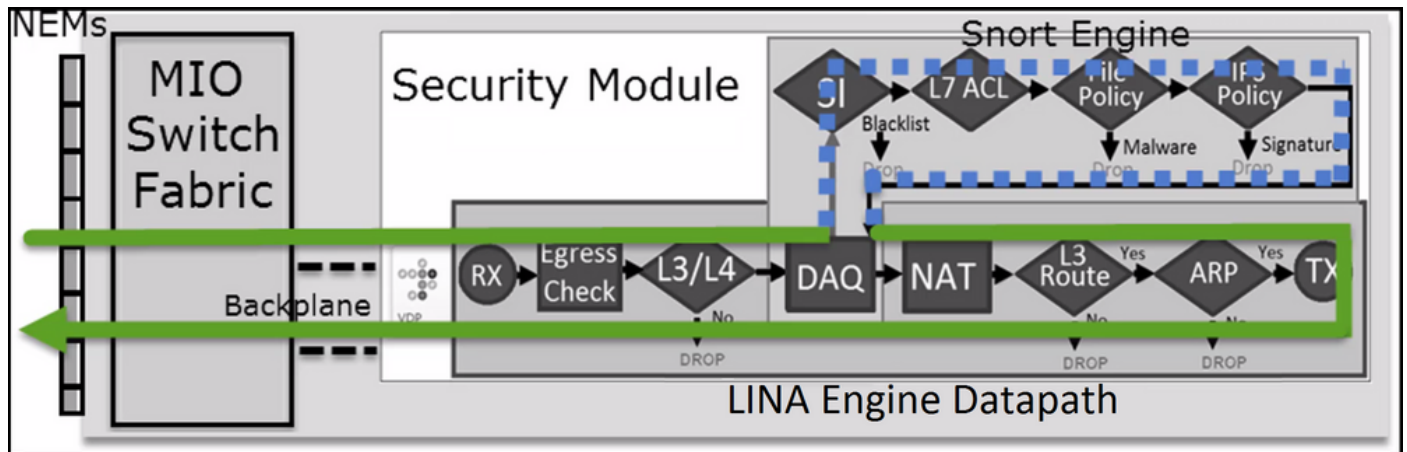
```
Fast-Forwarded Flows 1
```

```
Blacklisted Flows 0
```

Miscellaneous Counters:

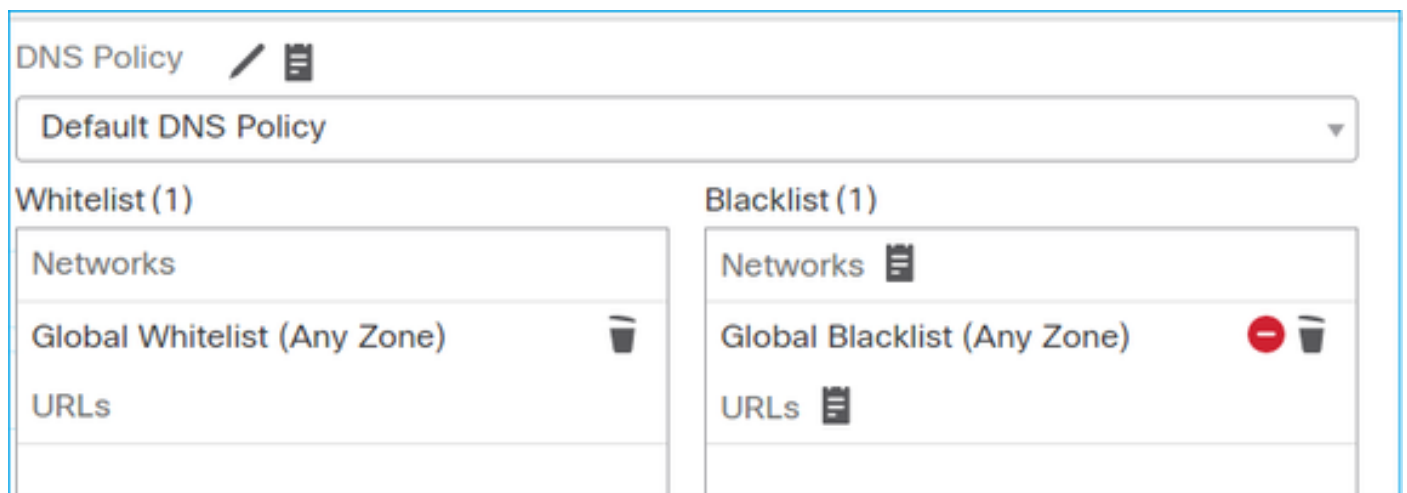
Start-of-Flow events	0
End-of-Flow events	1
Denied flow events	0
Frames forwarded to Snort before drop	0
Inject packets dropped	0

信頼ルールによるパケットフロー。いくつかのパケットは Snort によって検査され、残りは LINA によって検査されます。



シナリオ2: ACPの信頼アクション ( SI、QoS、およびアイデンティティポリシーなし )

FTDがすべてのフローにセキュリティインテリジェンス(SI)チェックを適用する場合、SIはすでに ACPレベルで有効になっており、SIソース ( TALOS、フィード、リストなど ) を指定できます。一方、無効にする場合は、ACP ごとにネットワークの SI、URL の SI、および DNS の SI をグローバルに無効にします。図に示すように、ネットワークおよび URL の SI が無効になります。



この場合、信頼ルールは trust として LINA に展開されます。

```
> 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
```

注：6.2.2の時点で、FTDはTIDをサポートしています。TIDはSIと同様の方法で機能しますが、SIが無効になっている場合、TID検査を目的としたSnortエンジンへのパケットリダイレクトを「強制」することはしません。

## 動作の検証

ホスト A ( 192.168.1.40 ) からホスト B ( 192.168.2.40 ) への HTTP セッションを開始します。これはFP4100であり、ハードウェアでフローオフロードをサポートするため、次のことが起こります。

- いくつかのパケットが FTD LINA エンジンを通じて転送され、残りのフローは SmartNIC ( HW アクセラレータ ) にオフロードされる
- Snortエンジンに転送されるパケットはありません

FTD LINA接続テーブルにフラグ「o」。フローがHWにオフロードされたことを意味します。また、「N」フラグ。これは実質的に「Snortリダイレクトなし」を意味しています。

```
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
```

Snort 統計には、セッションの開始時と終了時のロギングイベントのみが表示されます。

```
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:

<b>Start-of-Flow events</b>	<b>1</b>
<b>End-of-Flow events</b>	<b>1</b>

FTD LINA ログには、セッションごとに2つのフロー（各方向に1つ）がHWにオフロードされたことが示されています。

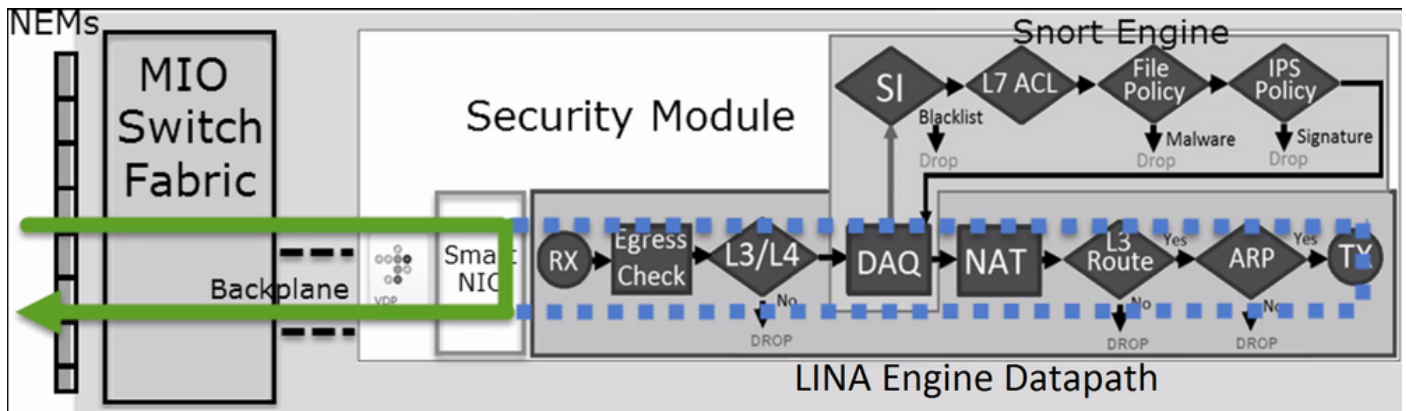
```
Sep 27 2017 20:16:05: %ASA-7-609001: Built local-host INSIDE:192.168.1.40
Sep 27 2017 20:16:05: %ASA-6-302013: Built inbound TCP connection 25384 for
INSIDE:192.168.1.40/32809 (192.168.1.40/32809) to OUTSIDE:192.168.2.40/80 (192.168.2.40/80)
Sep 27 2017 20:16:05: %ASA-6-805001: Offloaded TCP Flow 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

信頼ルールが展開されたパケットフロー trust LINAでのアクション。いくつかのパケットが LINA によって検査され、残りは SmartNIC ( FP4100/FP9300 ) にオフロードされます。

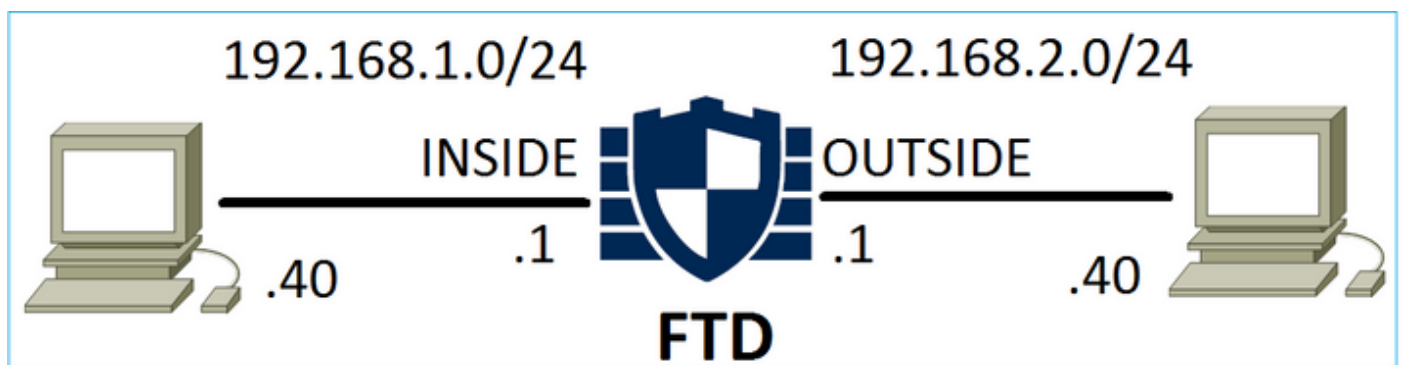


## 使用例

- を使用する必要があります。Trust Snortエンジンで少数のパケットだけをチェックし ( アプリケーション検出、SIチェックなど )、残りのフローをLINAエンジンにオフロードする場合のアクション
- FP4100/9300でFTDを使用し、フローがSnort検査を完全にバイパスするようにするには、次のコマンドを使用してプレフィルタルールを検討します。 Fastpath アクション ( このドキュメントの関連セクションを参照 )

## プレフィルタ ポリシー ブロック アクション

図に示されているトポロジについて検討します。



図に示されているポリシーについても検討します。

Access Control ▶ Prefilter										
		Network Discovery		Application Detectors		Correlation		Actions ▼		
FTD_Prefilter										
Enter Description										
Rules										
<span>➕ Add Tunnel Rule</span> <span>➕ Add Prefilter Rule</span> <span>Search Rules</span>										
#	Name	Rule T...	...	De	Source	Destination	Source	Destinat...	VLAN Tag	Action
				Ini	Networks	Networks	Port	Port		
1	Prefilter1	Prefilter	any any		192.168.1.40	192.168.2.40	any	any	any	✖ Block

これは、FTD Snortエンジン ( ngfw.rulesファイル ) に導入されたポリシーです。

```
# 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
```

LINA の場合 :

```
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
```

仮想パケットをトレースすると、パケットが LINA によってドロップされ、Snort に転送されないことが示されます。

```
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
```

Snort 統計の表示 :

```
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

```

LINA ASP ドロップの表示 :

```

firepower# show asp drop

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

```

## 使用例

L3/L4条件に基づいてトラフィックをブロックし、トラフィックのSnort検査を行う必要がない場合は、プレフィルタブロックルールを使用できます。

## プレフィルタポリシー Fastpath アクション

図に示されているプレフィルタポリシールールについて検討します。

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

これは、FTD Snortエンジンに導入されたポリシーです。

```

268437506 fastpath any any any any any any any (log dcforward flowend) (tunnel -1)
FTD LINA の場合 :

```

```

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

```

## 動作の検証

ホスト A ( 192.168.1.40 ) がホスト B ( 192.168.2.40 ) への HTTP セッションを開こうとすると、いくつかのパケットが LINA を通過し、残りは SmartNIC にオフロードされます。この場合 `system support trace` さらにトラブルシューティングを行うために、`firewall-engine-debug enabled` は次を示します。

```
> 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
```

LINA ログはオフロードされたフローを示します。

```
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)
```

LINAキャプチャは8パケットが通過することを示します。

```
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>

```

FTD フローオフロード統計は、HW にオフロードされた 22 のパケットを示します。

```

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

```

また、`show flow-offload flow` コマンドを使用して、オフロードされたフローに関連する追加情報を表示します。以下が一例です。

```

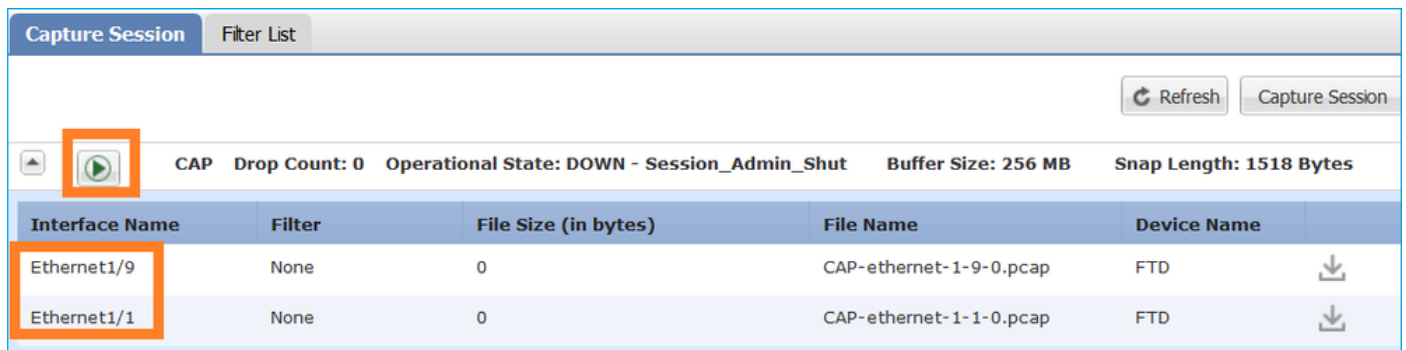
firepower# show flow-offload flow
Total offloaded flow stats: 2 in use, 4 most used, 20% offloaded, 0 collisions
TCP intf0 103 src 192.168.1.40:39301 dest 192.168.2.40:20, static, timestamp 616063741, packets
33240, bytes 2326800
TCP intf0 104 src 192.168.2.40:20 dest 192.168.1.40:39301, static, timestamp 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

```

- パーセンテージは、`show conn` エラーが表示される場合があります。たとえば、合計で5つの `conn` が FTD LINA エンジンを通り、そのうち1つがオフロードされると、20% がオフロードとして報告されます
- オフロードセッションの最大数は、ソフトウェアのバージョンによって異なります(たとえば、ASA 9.8.3 および FTD 6.2.3 は、400 万の双方向 (または 800 万の単方向) オフロードフローをサポートします)
- オフロードされるフローの数が制限に達した場合 (たとえば、400 万の双方向フロー)、現在の接続がオフロードされたテーブルから削除されるまで、新しい接続はオフロードされません

FTD ( オフロード + LINA ) を 通過する FP4100/9300 上のすべてのパケットを表示するには、図に示すように、シャーシレベルでキャプチャを有効にする必要があります。



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	↓

シャーシ バックプレーン キャプチャは両方向のフローを示します。FXOS キャプチャのアーキテクチャ ( 方向ごとに 2 つのキャプチャポイント ) により、図に示すように、すべてのパケットが 2 回表示されます。

パケット統計情報：

- FTD 経由のパケットの総数：30
- FTD LINA 経由のパケット：8
- SmartNIC HW アクセラレータにオフロードされたパケット：22

FP4100/FP9300以外のプラットフォームの場合は、フローオフロードがサポートされていないため、すべてのパケットがLINAエンジンによって処理されます(オフラグがないことに注意してください)。

```
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
```

LINA Syslog には、接続セットアップイベントと接続終了イベントのみが表示されます。

```
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
```

## 使用例

- 利用 Prefilter Fastpath Snortインスペクションを完全にバイパスする場合のアクション。通常は、バックアップやデータベース転送など、信頼できる大容量のフローに対してこれを実行します。
- FP4100/9300アプライアンスでは、Fastpath アクションはフローオフロードをトリガーし、少数のパケットだけがFTD LINAエンジンを通過します。残りは、遅延を軽減する SmartNIC によって処理されます。

## プレフィルタポリシー Fastpath アクション ( インラインセット )

インラインセット ( NGIPSインターフェイス ) を通過するトラフィックに対してプレフィルタポリシーFastpathアクションが適用される場合は、次の点を考慮する必要があります。

- このルールは、LINAエンジンに次のように適用されます。 trust action
- フローは Snort エンジンによって検査されません。
- フローオフロードは NGIPS インターフェイスに適用されないため、フローオフロード ( HW アクセラレーション ) は発生しません。

インラインセットに適用されるPrefilter Fastpathアクションの場合のパケットトレースの例を次に示します。

```
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:

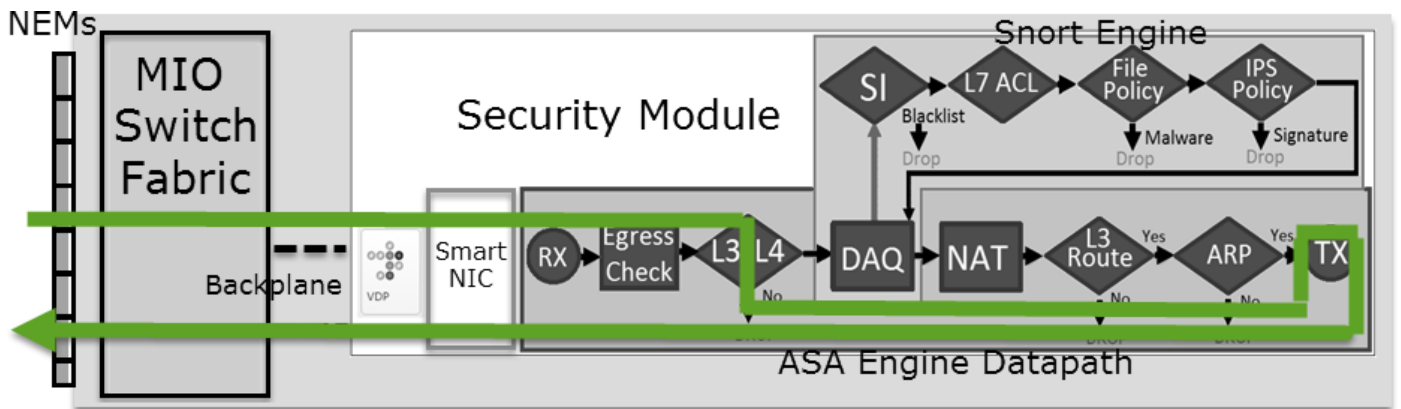
input-interface: inside

input-status: up

input-line-status: up

Action: allow

パケットパスの視覚的な表現を次に示します。



プレフィルタポリシー Fastpath アクション ( タップによるインラインセット )

インラインセットの場合と同じ

プレフィルタポリシー分析アクション

シナリオ 1 : ACP ブロックルールによるプレフィルタ分析

図に示されている [分析 ( Analyze ) ] ルールを含むプレフィルタポリシーについて検討します。

#	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

ACPには、デフォルトのルールだけが含まれます。このルールは Block All Traffic 図に示すように :



Access Control ▶ Access Control    Network Discovery    Application Detectors    Correlation    Actions ▼

## ACP1

Enter Description

Prefilter Policy: **Prefilter\_Policy1**      SSL Policy: None

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. <a href="#">Add Rule</a> or <a href="#">Add Category</a>													
▼ Default - ACP1 (-)													
There are no rules in this section. <a href="#">Add Rule</a> or <a href="#">Add Category</a>													
Default Action												Access Control: Block All Traffic	

これは、FTD Snortエンジン ( ngfw.rulesファイル ) に導入されたポリシーです。

```
# 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 any 47 (tunnel -1)
268435459 allow any any any any any any any any 41 (tunnel -1)
268435459 allow any 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 any (log dcforward flowstart)
# End of AC rule.
```

これは FTD LINA エンジンに展開されたポリシーです。

```
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
```

### 動作の検証

Packet-tracerは、パケットがLINAによって許可され、Snortエンジンに転送されることを示します (原因: permit アクション) を実行し、Snortエンジンが Block ACからのデフォルトアクションが一致しているため、判定されます。

注: Snort がトンネルルールに基づいてトラフィックを評価することはありません。

パケットをトレースすると、そのことがわかります。

```
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

```

## シナリオ 2：ACP 許可ルールによるプレフィルタ分析

パケットが FTD を通過できるようにすることが目的の場合は、ACP にルールを追加する必要があります。[Action]には、目標に応じて[Allow]または[Trust]を指定できます(たとえば、L7インスプレクションを適用する場合は、Allow アクション)を次の図に示します。

The screenshot shows the 'Access Control' configuration page for ACP1. The 'Rules' tab is selected, showing a table of rules. Rule 1 is highlighted with an orange border, indicating it is the active rule. The rule is named 'Rule1' and has an 'Allow' action. The source and destination networks are 192.168.1.40 and 192.168.2.40, respectively. The rule is part of the 'Mandatory - ACP1 (1-1)' group.

#	Name	Sou... Zones	Dest Zones	Source Networks	Dest Networks	VLA...	Users	App...	Sou...	Des...	URLs	ISE... Attr...	Action
1	Rule1	Any	Any	192.168.1.40	192.168.2.40	Any	Any	Any	Any	Any	Any	Any	Allow

FTD Snort エンジンに展開されたポリシー：

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

## LINA エンジンの場合：

```
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
```

## 動作の検証

パケットトレーサは、パケットがルールに一致することを示します 268435460 LINAおよび 268435461 snortエンジンの場合：

```
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
```

## シナリオ 3：ACP 信頼ルールによるプレフィルタ分析

ACPに [信頼 ( Trust ) ] ルールが含まれている場合は、図に示されているような表示になります。

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

## ACP1

Enter Description

Prefilter Policy: [Prefilter\\_Policy1](#)      SSL Policy: [None](#)      Identif

Inheritance Se

Rules    Security Intelligence    HTTP Responses    Advanced

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

#	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. <a href="#">Add Rule</a> or <a href="#">Add Category</a>													
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 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
```

SIはデフォルトで有効になっているため、信頼ルールは次のように展開されます permit 少なくとも数個の packets が検査のために Snort エンジンにリダイレクトされるように、LINA に対するアクション。

## 動作の検証

パケットトレーサは、Snort エンジンがパケットを許可し、基本的に残りのフローを LINA にオフロードすることを示します。

```
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**

## シナリオ 4：ACP 信頼ルールによるプレフィルタ分析

このシナリオでは、SI が手動で無効にされました。

ルールは次のように Snort に展開されます。

```
# 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 any (log dcforward flowstart)
```

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

LINA では、ルールは trust として展開されます。パケットは、Analyze Prefilterルールによって導入された許可ルール (ACE ヒットカウントを参照) に一致し、Snort エンジンによって検査されません。

```
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
```

## 動作の検証

```
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**

## 主なポイント

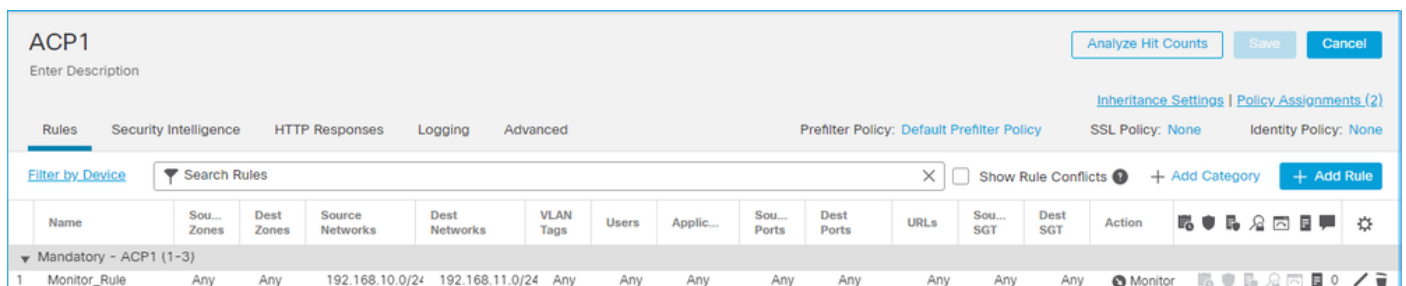
- 「Analyze アクションは、LINAエンジンの許可ルールとして導入されます。これは、検査のためにSnortエンジンに転送されるパケットに影響します
- 「Analyze アクションはSnortエンジンにルールを導入しないため、Snortで一致するACPでルールを設定する必要があります。
- これは、Snortエンジン(block VS allow VS fastpath)Snortでは、パケットがまったく許可されない、またはいくつかある

## 使用例

- 使用例 Analyze アクションは、プレフィルタポリシーに幅広いFastpathルールがあり、特定のフローに対して例外を設定して、Snortによって検査されるようにする場合です

## ACP モニタアクション

FMC UI で設定されたモニタルール :



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

モニタルールは、FTD LINAエンジン上に次のように展開されます。 permit Snortエンジンに対するアクションおよび audit アクション。

```
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
```

Snort ルール :

```
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 dcfoward flowend)  
# End rule 268438863
```

## 主なポイント

- Monitor Ruleはトラフィックをドロップまたは許可しませんが、Connection Eventを生成します。パケットは後続のルールと照合され、許可またはドロップされます。
- FMC接続イベントは、パケットが2つのルールに一致したことを示します。

	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 出力は、パケットが両方のルールに一致することを示しています。

```
> 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
```

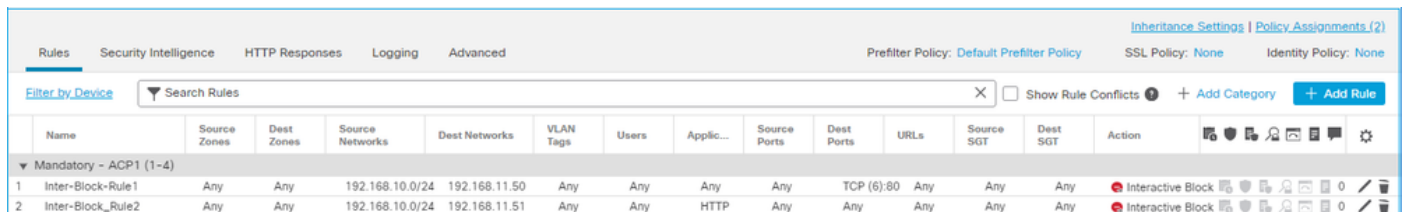
192.168.10.50-41922 > 192.168.11.50-80 6 AS 1-1 I 19 MidRecovery data sent for rule id:  
268438858,rule\_action:3, rev id:1078 02206, rule\_match flag:0x2

## 使用例

ネットワークアクティビティをモニタし、接続イベントを生成するために使用されます。

## ACP インタラクティブ ブロック アクション

FMC UI で設定されたインタラクティブ ブロック ルール :



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	TCP (6):80	Any	Any	Any	Interactive Block
2	Inter-Block_Rule2	Any	Any	192.168.10.0/24	192.168.11.51	Any	Any	HTTP	Any	Any	Any	Any	Interactive Block

インタラクティブブロックルールは、FTD LINAエンジン上で次のように展開されます。 permit Snortエンジンに対してバイパスルールとして次のアクションを実行します。

```
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
```

Snort エンジン :

```
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
```

インタラクティブ ブロック ルールは、宛先が禁止されていることをユーザーに示します。



# 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.

Continue

デフォルトでは、ファイアウォールはブロックを 600 秒間バイパスさせることができます。

Rules	Security Intelligence	HTTP Responses	Logging	Advanced
<b>General Settings</b> 				
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

内 `system support trace` 出力を見ると、ファイアウォールが最初にトラフィックをブロックし、ブロックページが表示されていることがわかります。

```
> 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
```

ユーザが選択したら、Continue (またはブラウザページを更新) デバッグでは、パケットが同じルールによって許可されていることが示されます。このルールは、Allow action:

```
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
```

## 使用例

Web ユーザーに警告ページを表示し、続行するオプションを提示します。

## リセットアクションによる ACP インタラクティブブロック

FMC UI でリセットルールが設定されたインタラクティブブロック :

Name	Source Zones	Destination Zones	Source Networks	Destination Networks	VLAN Tags	Users	Applications	Source Ports	Destination Ports	URLs	Source SGT	Destination SGT	Action
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
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

リセットルールを含むインタラクティブブロックは、FTD LINAエンジン上に permit Snortエンジンに対してイントレセットルールとしてアクションを実行します。

```
firepower# show access-list
```

...

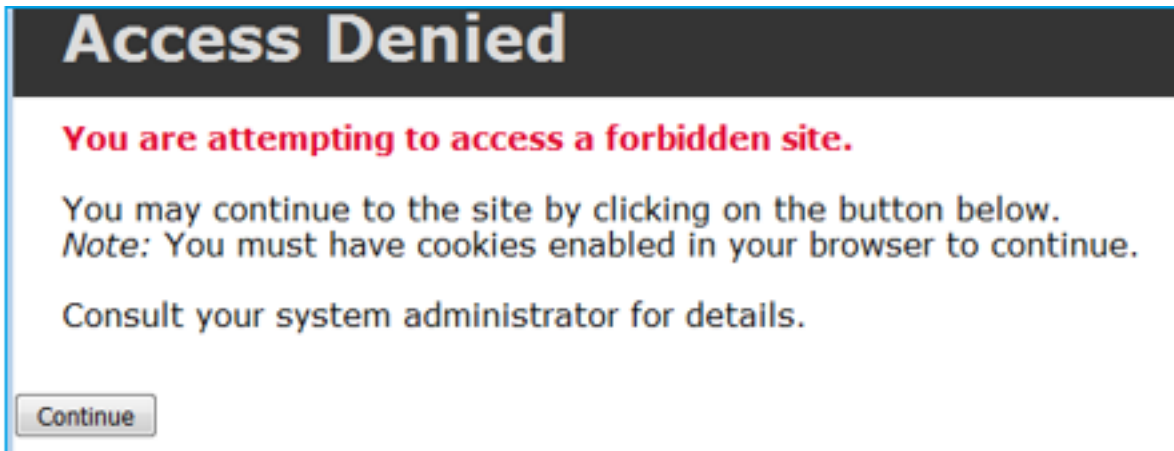
```
access-list CSM_FW_ACL_ line 9 remark rule-id 268438864: L7 RULE: Inter-Block-Rule1
access-list CSM_FW_ACL_ line 10 advanced permit tcp 192.168.10.0 255.255.255.0 host
192.168.11.50 eq www rule-id 268438864 (hitcnt=13) 0xba785fc0
access-list CSM_FW_ACL_ line 11 remark rule-id 268438865: ACCESS POLICY: 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
```

Snort エンジン :

```
# 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
```

[リセット付きのブロック]と同様に、ユーザは次のものを選択できます。 **Continue** オプション：



Snort のデバッグで Interactive Reset に示されるアクション：

```
> 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
```

この時点で、ブロックページがエンドユーザに表示されます。ユーザが **Continue** (またはWebページを更新) 今度はトラフィックの通過を許可する同じルールが一致します。

```
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
```

リセットルールによるインタラクティブブロックは、非 Web トラフィックに TCP RST を送信し  
ます。

```
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
```

## FTDセカンダリ接続およびピンホール

古いリリース ( 6.2.2、6.2.3 など ) では、Snort エンジン は、FTD データ などのセカンダリ接続用のピンホールを開きません。Trust アクション。最近のリリースでは、この動作が変更され、Snort エンジン は Snort エンジンの CLI で Trust アクション。

## FTD ルールのガイドライン

- through-the-box の遅延を軽減するため、プレフィルタポリシー Fastpath ルールを使用して大容量のフローを実現します。
- L3/L4 条件に基づいてブロックする必要があるトラフィックにプレフィルタブロックルールを使用します。
- Snort チェックの多くをバイパスする一方で、ID ポリシー、QoS、SI、アプリケーション検出、URL フィルタなどの機能を引き続き利用する場合は、ACP 信頼ルールを使用します。
- 次のガイドラインを使用して、アクセスコントロールポリシーの先頭に、ファイアウォールのパフォーマンスへの影響がより小さいルールを配置します。

1. ブロックルール ( レイヤ 1 ~ 4 ) : プレフィルタブロック
2. 許可ルール ( レイヤ 1 ~ 4 ) : プレフィルタ Fastpath
3. ACP ブロックルール ( レイヤ 1 ~ 4 )
4. 信頼ルール ( レイヤ 1 ~ 4 )
5. ブロックルール ( レイヤ 5 ~ 7 : アプリケーション検出、URL フィルタリング )
6. 許可ルール ( レイヤ 1 ~ 7 : アプリケーション検出、URL フィルタリング、侵入ポリシー / ファイルポリシー )
7. ブロックルール ( デフォルトルール )

- 過剰なロギングを回避します ( 開始 時または終了時にログを記録し、両方を同時に回避します )。
- LINA のルールの数を確認するため、ルール拡張に注意してください。

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

## 要約

### プレフィルタアクション

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

### ACP アクション

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

注：6.3 FTDソフトウェアコードから見ると、ダイナミックフローオフロードは、Snortインスペクションを必要とする信頼できるパケットなど、追加の基準を満たす接続をオフロードできます。詳細については、『Firepower Management Center Configuration Guide』の「Offload Large Connections (Flows)」セクションを参照してください。

## 関連情報

- [FTD アクセスコントロールルール](#)
- [FTD プレフィルタとプレフィルタポリシー](#)
- [ネットワークの問題を効果的にトラブルシューティングするための Firepower ファイアウォールキャプチャの分析](#)
- [Firepower Threat Defense \( FTD \) のキャプチャおよびパケット トレーサの使用](#)
- [FMC を介して FTD にロギングを設定](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)
- [大規模接続のオフロード](#)

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。