FTDプレフィルタポリシーの設定と運用

内容

はじめに

このドキュメントでは、Firepower Threat Defense(FTD)プレフィルタポリシーの設定と動作について説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

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。

- FTDコード6.1.0-195が稼働するASA5506X
- 6.1.0-195が稼働するFireSIGHT Management Center(FMC)
- 15.2イメージを実行する2台の3925 Cisco IOS®ルータ

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、クリアな（デフォルト）設定で作業を開始しています。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。

背景説明

プレフィルタポリシーは6.1バージョンで導入された機能で、主に次の3つの目的に使用されます。

1. 内部ヘッダーと外部ヘッダーの両方に基づいてトラフィックを照合する
2. フローがSnortエンジンを完全にバイパスできる早期アクセス制御を提供
3. 適応型セキュリティアプライアンス(ASA)移行ツールから移行されるアクセスコントロールエントリ(ACE)のプレースホルダとして機能します。

設定

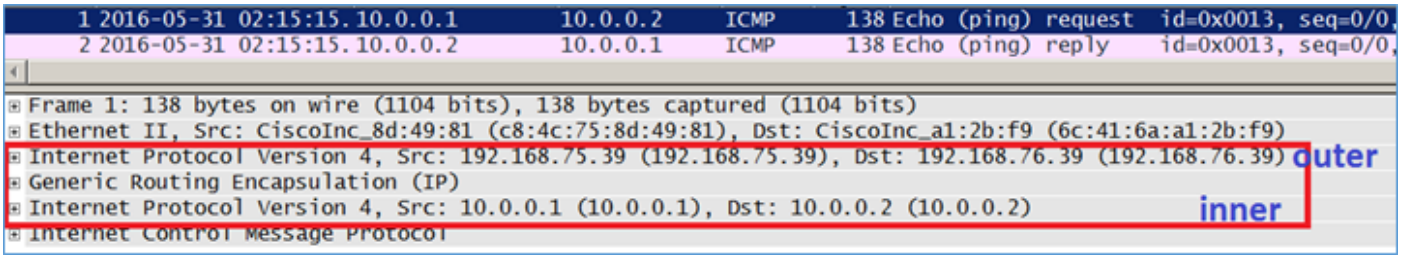
プレフィルタポリシーの使用例1

PrefilterポリシーではTunnel Rule Typeを使用でき、これによりFTDは内部と外部の両方のIPヘッダートンネリングトラフィックに基づいてフィルタリングできます。この記事の執筆時点では、トンネルトラフィックとは次の意味を持っています。

- 総称ルーティング カプセル化（GRE）
- IP-in-IP
- IPv6-IP
- Teredo ポート 3544

図に示すように、GREトンネルを検討します。

GREトンネルを使用してR1からR2にpingを実行すると、トラフィックはファイアウォールを通過し、図のように見えます。



ファイアウォールがASAデバイスの場合は、図に示すように、外部IPヘッダーを確認します。

<#root>

ASA#

show conn

GRE OUTSIDE 192.168.76.39:0 INSIDE 192.168.75.39:0

, idle 0:00:17, bytes 520, flags

ファイアウォールがFirePOWERデバイスの場合、図に示すように、内部IPヘッダーがチェックされます。

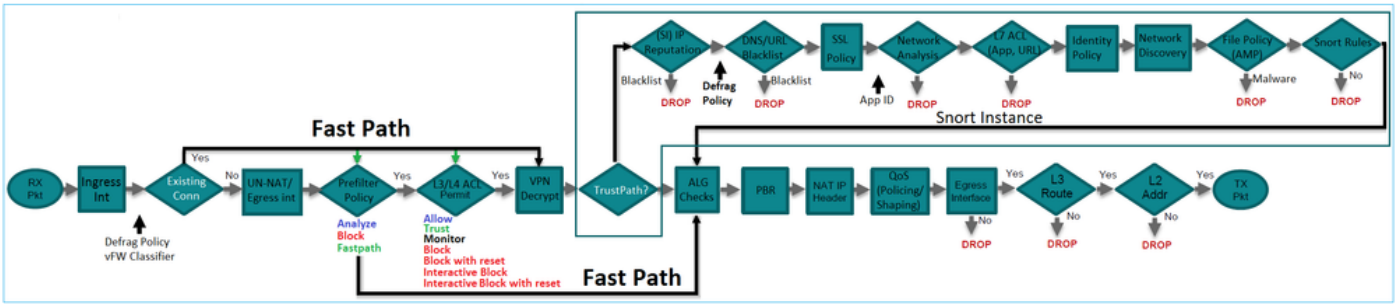
プレフィルタポリシーを使用すると、FTDデバイスは内部ヘッダーと外部ヘッダーの両方に基づいてトラフィックを照合できます。

主要なポイント

デバイス	チェック
ASA	外部IP
Snort	内部IP
FTD	外部（プレフィルタ）+内部IP(アクセスコントロールポリシー(ACP))

プレフィルタポリシーの使用例2

プレフィルタポリシーは、早期アクセス制御を提供し、フローが図のようにSnortエンジンを完全にバイパスできるプレフィルタルールタイプを使用できます。



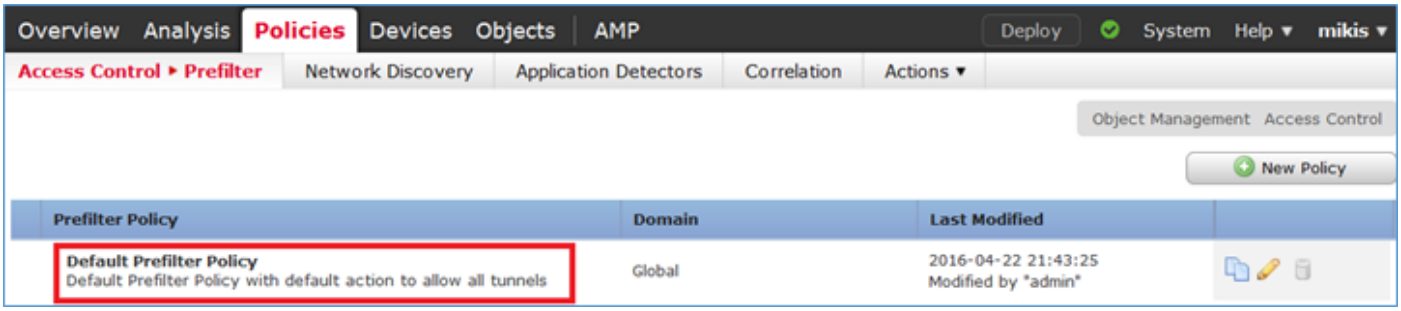
タスク 1.デフォルトのプレフィルタポリシーの確認

タスクの要件

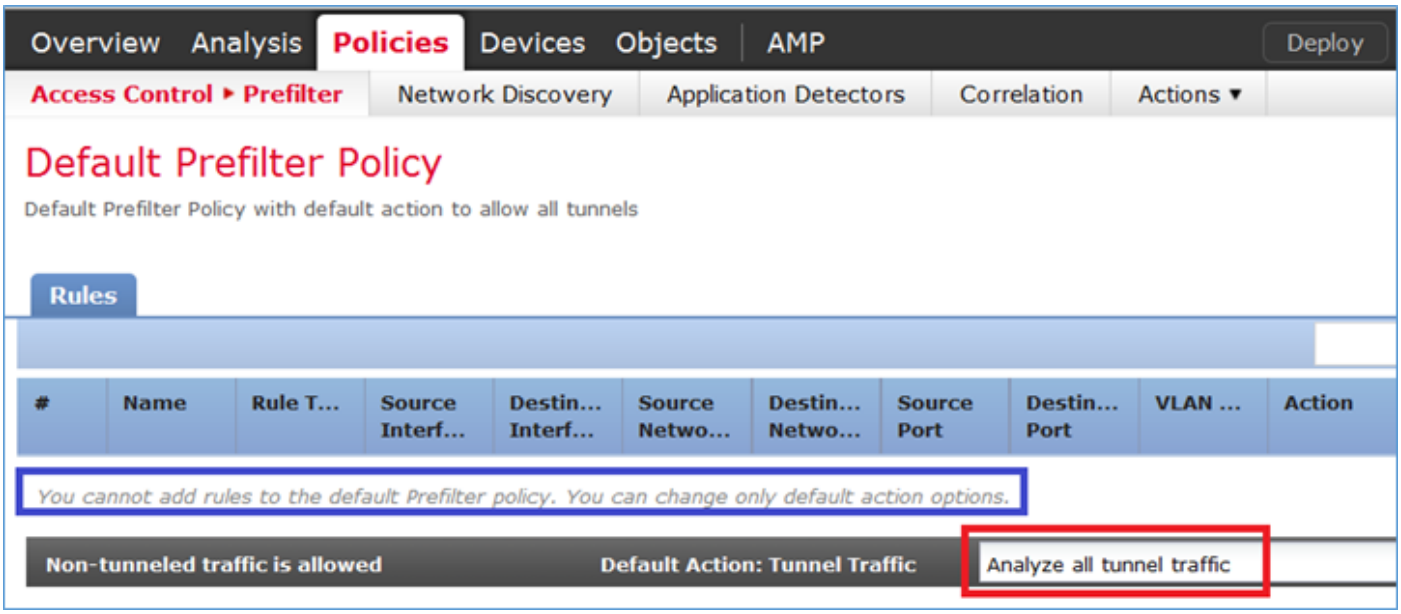
デフォルトのプレフィルタポリシーの確認

解決方法

ステップ 1：Policies > Access Control > Prefilterの順に移動します。図に示すように、デフォルトのプレフィルタポリシーがすでに存在します。



ステップ 2：Editを選択し、図に示すようなポリシー設定を表示します。



ステップ 3：プレフィルタポリシーは、図に示すように、アクセスコントロールポリシーにすでに割り当てられています。

CLI(LINA)の検証

プレフィルタルールはACLの上に追加されます。

```
<#root>

firepower#
```

```
show access-list

access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
            alert-interval 300
access-list CSM_FW_ACL_; 5 elements; name hash: 0x4a69e3f3
access-list CSM_FW_ACL_ line 1 remark rule-id 9998:

PREFILTER POLICY:

 Default Tunnel and Priority Policy
access-list CSM_FW_ACL_ line 2 remark rule-id 9998: RULE: DEFAULT TUNNEL ACTION RULE
access-list CSM_FW_ACL_ line 3 advanced permit ipinip any any rule-id 9998 (hitcnt=0) 0xf5b597d6
access-list CSM_FW_ACL_ line 4 advanced permit 41 any any rule-id 9998 (hitcnt=0) 0x06095aba
access-list CSM_FW_ACL_ line 5 advanced permit gre any any rule-id 9998 (hitcnt=5) 0x52c7a066
access-list CSM_FW_ACL_ line 6 advanced permit udp any any eq 3544 rule-id 9998 (hitcnt=0) 0xcf6309bc
```

タスク 2.タグ付きトンネルトラフィックのブロック

タスクの要件

GREトンネル内でトンネリングされるICMPトラフィックをブロックします。

解決方法

ステップ 1：これらのACPを適用すると、図に示すように、Internet Control Message Protocol（ICMP；インターネット制御メッセージプロトコル）トラフィックが、GREトンネルを通過するかどうかにかかわらず、ブロックされていることがわかります。


```
<#root>

R1#

ping 192.168.76.39

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.76.39, timeout is 2 seconds:

.....

Success rate is 0 percent (0/5)
```

```
<#root>
```

```
R1#

ping 10.0.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout is 2 seconds:

.....
Success rate is 0 percent (0/5)
```

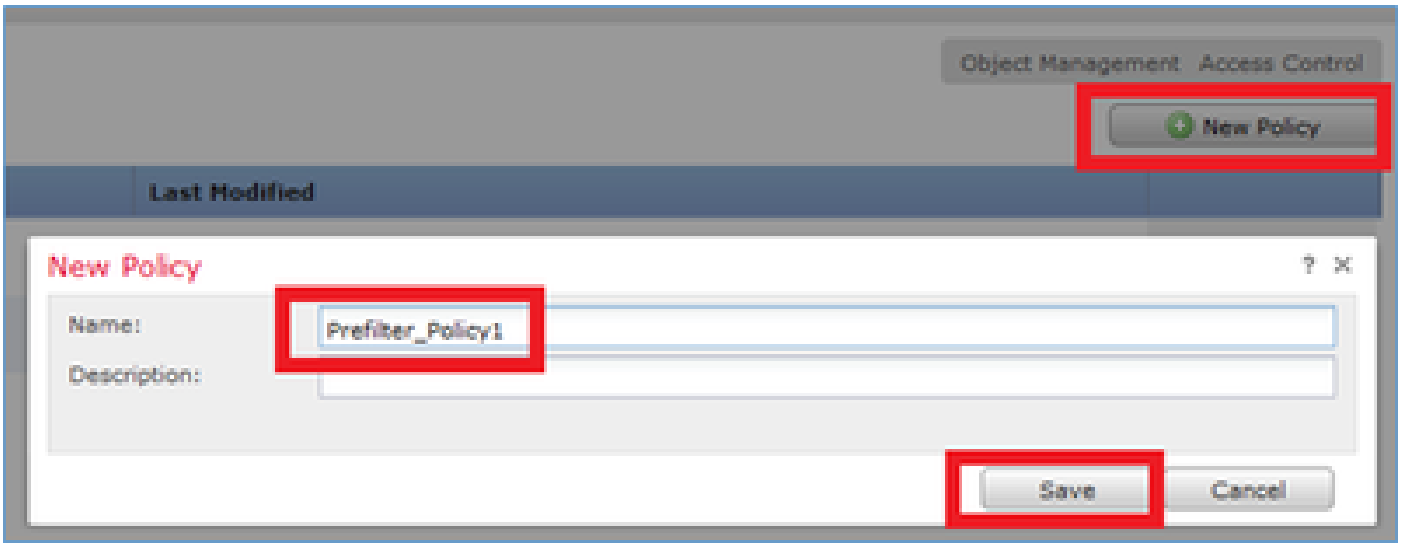
この場合、プレフィルタポリシーを使用してタスク要件を満たすことができます。ロジックは次のとおりです。

1. GRE内にカプセル化されているすべてのパケットにタグを付けます。
2. タグ付きパケットに一致し、ICMPをブロックするアクセスコントロールポリシーを作成します。

アーキテクチャの観点からは、パケットはLInux NAatively(LINA)プレフィルタルールに照らしてチェックされ、次にSnortプレフィルタルールとACPがチェックされ、最後にSnortからLINAに廃棄が指示されます。最初のパケットはFTDデバイスを経由します。

ステップ 1：トンネルトラフィックのタグを定義します。

Policies > Access Control > Prefilterの順に移動し、新しいプレフィルタポリシーを作成します。図に示すように、デフォルトのプレフィルタポリシーは編集できないことに注意してください。

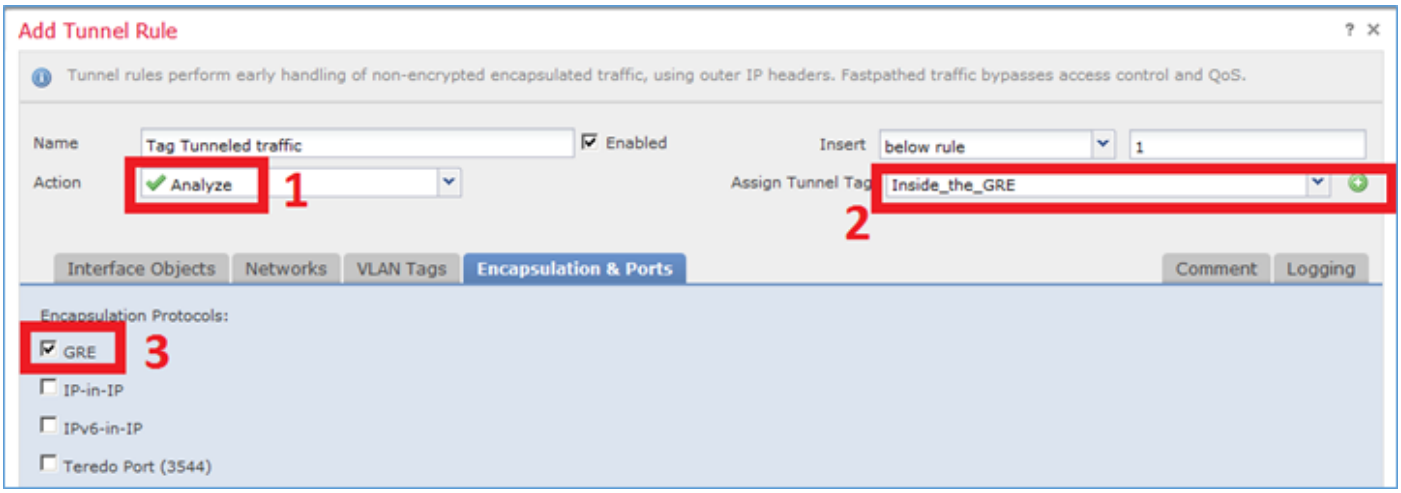


プレフィルタポリシー内で、次の2種類のルールを定義します。

1. トンネル規則
2. プレフィルタルール

これら2つは、プレフィルタポリシーで設定できる完全に異なる機能と考えることができます。

この作業では、図に示すようにトンネル規則を定義する必要があります。

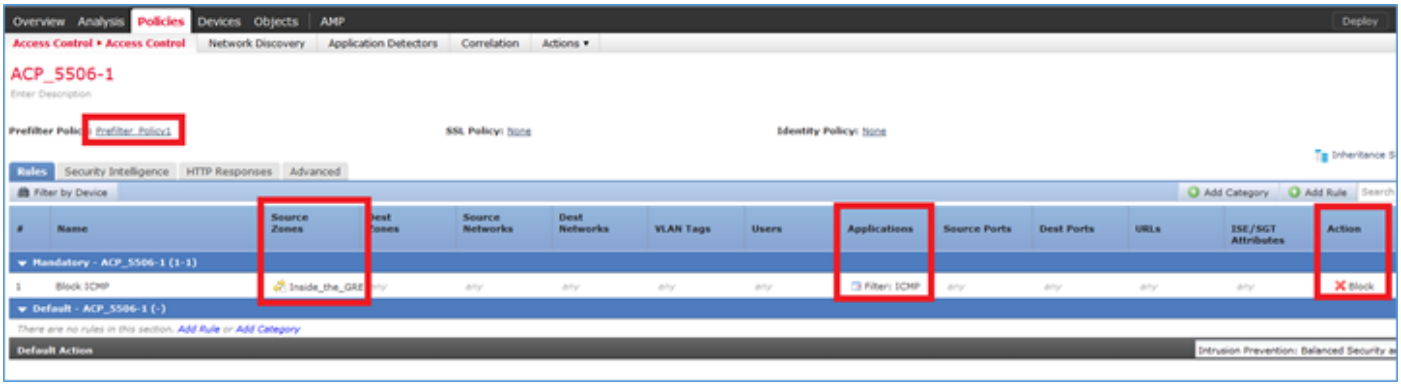


アクションに関して

アクション	説明
分析	LINAの後、フローはSnortエンジンによってチェックされます。必要に応じて、トンネルタグをトンネルトラフィックに割り当てることができます。
Block	フローがLINAによってブロックされています。外側のヘッダーをチェックする必要があります。
高速パス	Snortエンジンを使用せずに、フローを処理できるのはLINAだけです。

ステップ 2：タグ付きトラフィックのアクセスコントロールポリシーを定義します。

最初はあまり直感的ではありませんが、アクセスコントロールポリシールール(ACL)で送信元ゾーンとしてトンネルタグを使用できます。Policies > Access Controlの順に移動し、図に示すように、タグ付きトラフィックのICMPをブロックするルールを作成します。



注：新しいプレフィルタポリシーがアクセスコントロールポリシーに適用されます。

検証

LINAおよびCLISHでキャプチャを有効にします。

```
<#root>

firepower#

show capture

capture CAPI type raw-data trace interface inside [Capturing - 152 bytes]
capture CAPO type raw-data trace interface outside [Capturing - 152 bytes]
```

```
<#root>

>

capture-traffic

Please choose domain to capture traffic from:
  0 - br1
  1 - Router

Selection?

1


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

-n
```

R1から、リモートGREトンネルのエンドポイントにpingを実行してみます。pingが失敗します。

```
<#root>

R1#

ping 10.0.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout is 2 seconds:

.....
Success rate is 0 percent (0/5)
```

CLISHキャプチャは、最初のエコー要求がFTDを通過し、応答がブロックされたことを示しています。

```
<#root>
```

```
Options: -n
18:21:07.759939 IP 192.168.75.39 > 192.168.76.39: GREv0, length 104: IP 10.0.0.1 > 10.0.0.2: ICMP echo

18:21:07.759939 IP 192.168.76.39 > 192.168.75.39: GREv0, length 104: IP 10.0.0.2 > 10.0.0.1: ICMP echo r

18:21:09.759939 IP 192.168.75.39 > 192.168.76.39: GREv0, length 104: IP 10.0.0.1 > 10.0.0.2: ICMP echo
18:21:11.759939 IP 192.168.75.39 > 192.168.76.39: GREv0, length 104: IP 10.0.0.1 > 10.0.0.2: ICMP echo
18:21:13.759939 IP 192.168.75.39 > 192.168.76.39: GREv0, length 104: IP 10.0.0.1 > 10.0.0.2: ICMP echo
18:21:15.759939 IP 192.168.75.39 > 192.168.76.39: GREv0, length 104: IP 10.0.0.1 > 10.0.0.2: ICMP echo
```

LINAキャプチャによってこれを確認します。

```
<#root>

>

show capture CAPI | include ip-proto-47

 102: 18:21:07.767523  192.168.75.39 > 192.168.76.39:  ip-proto-47, length 104
 107: 18:21:09.763739  192.168.75.39 > 192.168.76.39:  ip-proto-47, length 104
 111: 18:21:11.763769  192.168.75.39 > 192.168.76.39:  ip-proto-47, length 104
 115: 18:21:13.763784  192.168.75.39 > 192.168.76.39:  ip-proto-47, length 104
 120: 18:21:15.763830  192.168.75.39 > 192.168.76.39:  ip-proto-47, length 104
>
>

show capture CAPO | include ip-proto-47

  93: 18:21:07.768133  192.168.75.39 > 192.168.76.39:  ip-proto-47, length 104

  94: 18:21:07.768438  192.168.76.39 > 192.168.75.39:  ip-proto-47, length 104
```

CLISH firewall-engine-debugを有効にし、LINA ASP dropカウンタをクリアして、同じテストを実行します。CLISHデバッグは、エコー要求に対してプレフィルタルールに一致し、エコー応答に対してACPルールが一致したことを示しています。

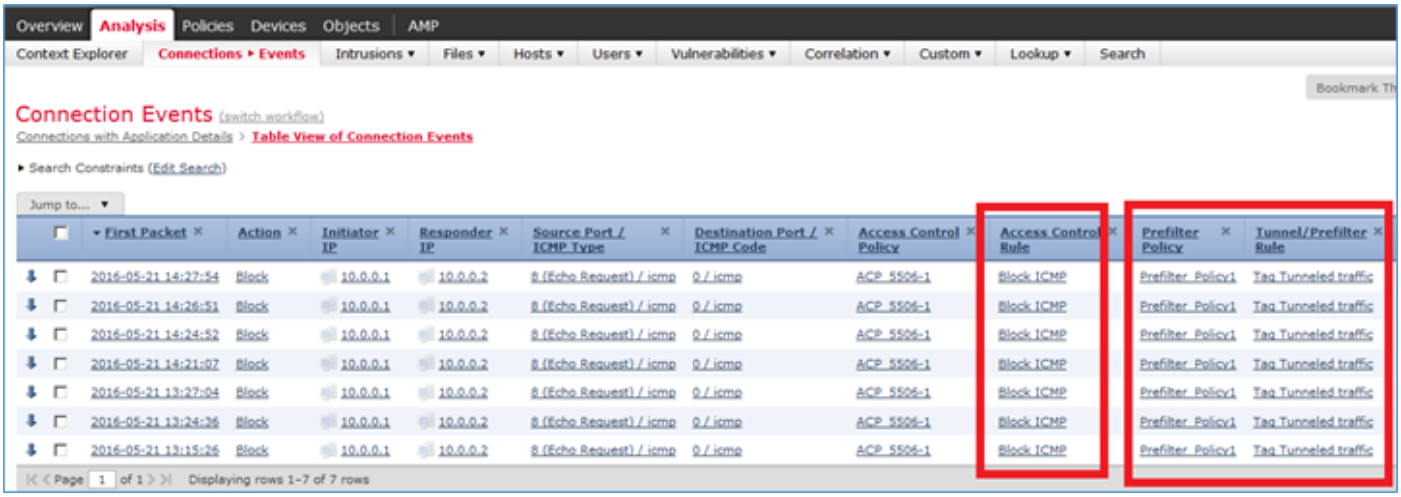
```
<#root>

10.0.0.1-8 > 10.0.0.2-0 1 AS 1 I 0

New session

10.0.0.1-8 > 10.0.0.2-0 1 AS 1 I 0

uses prefilter rule 268434441 with tunnel zone 1

10.0.0.1-8 > 10.0.0.2-0 1 AS 1 I 0 Starting with minimum 0, id 0 and SrcZone first with zones 1 -> -1,

icmpType 8, icmpCode 0

10.0.0.1-8 > 10.0.0.2-0 1 AS 1 I 0 pending rule order 3, 'Block ICMP', AppId
10.0.0.1-8 > 10.0.0.2-0 1 AS 1 I 0

uses prefilter rule 268434441 with tunnel zone 1

10.0.0.1-8 > 10.0.0.2-0 1 AS 1 I 0 Starting with minimum 0, id 0 and SrcZone first with zones 1 -> -1,

icmpType 0, icmpCode 0
```

```
10.0.0.1-8 > 10.0.0.2-0 1 AS 1 I 0
match rule order 3, 'Block ICMP', action Block
10.0.0.1-8 > 10.0.0.2-0 1 AS 1 I 0 deny action
```

ASPドロップは、Snortによってパケットがドロップされたことを示します。

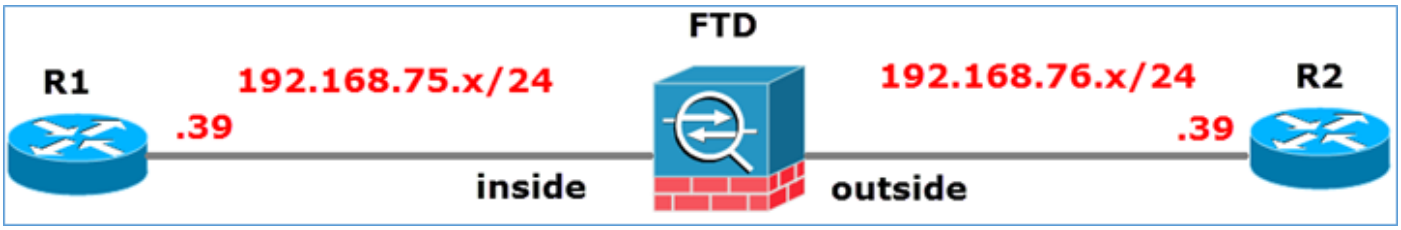
```
<#root>
>
show asp drop

Frame drop:
  No route to host (no-route)                                    366
  Reverse-path verify failed (rpf-violated)                        2
  Flow is denied by configured rule (acl-drop)                     2

 Snort requested to drop the frame (snort-drop)                    5
```

Connection Eventsでは、次の図に示すように、一致したプレフィルタポリシーとルールを確認できます。



タスク 3.Fastpathプレフィルタルールによるスナートエンジンのバイパス

ネットワーク図

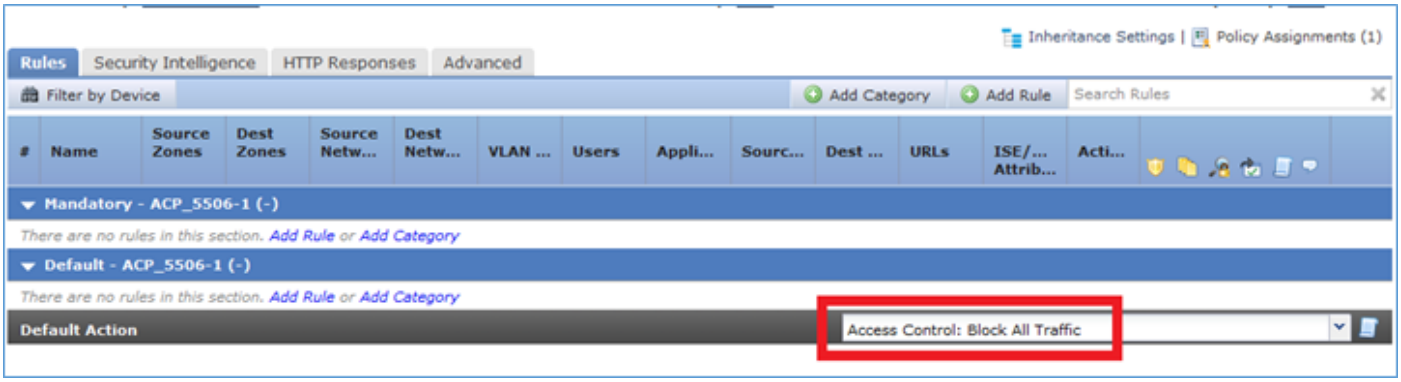


タスクの要件

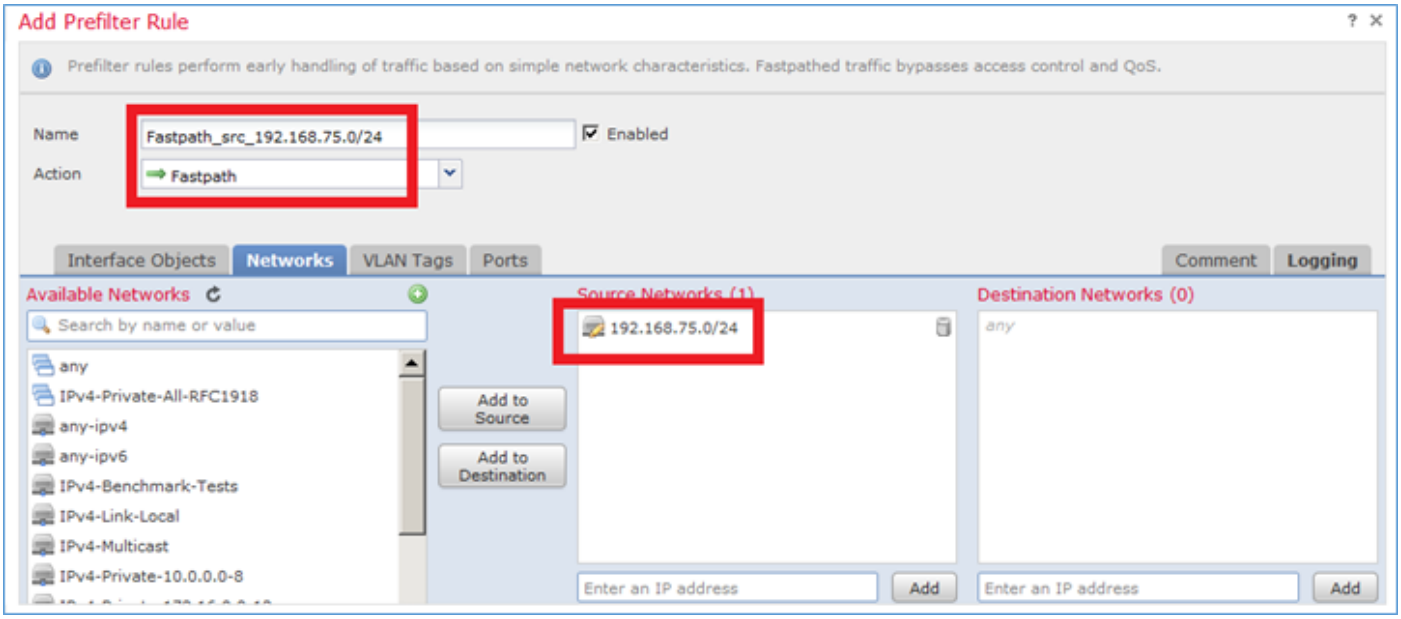
1. 現在のアクセスコントロールポリシールールを削除し、すべてのトラフィックをブロックするアクセスコントロールポリシールールを追加します。
2. 192.168.75.0/24ネットワークから送信されたトラフィックのSnortエンジンをバイパスするプレフィルタポリシールールを設定する。

解決方法

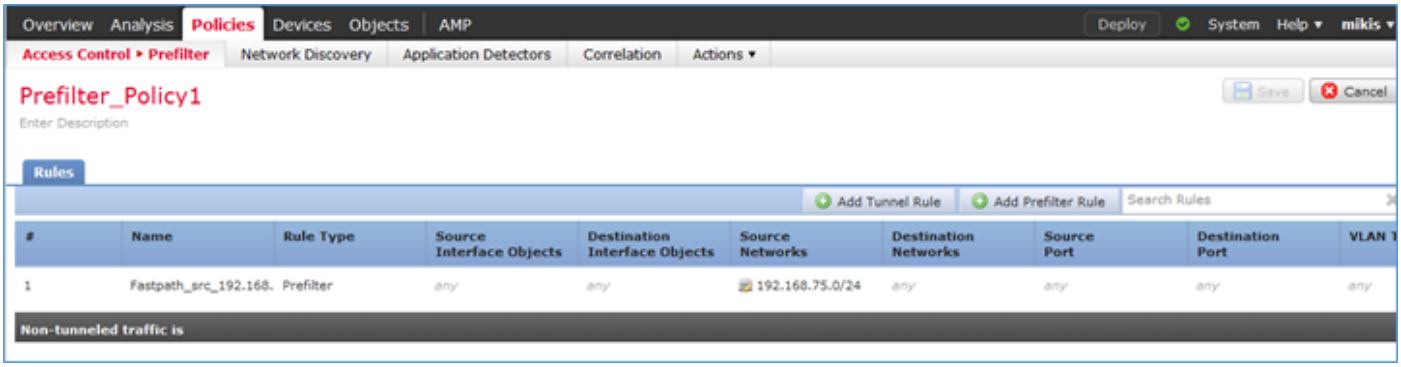
ステップ 1：すべてのトラフィックをブロックするアクセスコントロールポリシーを図に示します。



ステップ 2：図に示すように、ソースネットワーク192.168.75.0/24のアクションとしてFastpathを使用するプレフィルタルールを追加します。



ステップ 3：結果は図のようになります。



ステップ 4：保存して展開します。

両方のFTDインターフェイスでトレースによるキャプチャを有効にします。

<#root>

```
firepower#
```

capture CAPI int inside trace match icmp any any

```
firepower#
```

capture CAPO int outsid trace match icmp any any

FTDを介してR1(192.168.75.39)からR2(192.168.76.39)へのpingを試みます。pingが失敗します。

<#root>

```
R1#
```

ping 192.168.76.39

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.76.39, timeout is 2 seconds:

.....
```
Success rate is 0 percent (0/5)

内部インターフェイスのキャプチャは次のように表示されます。

<#root>

```
firepower#
```

show capture CAPI

```
5 packets captured
```

```
   1: 23:35:07.281738   192.168.75.39 > 192.168.76.39: icmp: echo request
   2: 23:35:09.278641   192.168.75.39 > 192.168.76.39: icmp: echo request
   3: 23:35:11.279251   192.168.75.39 > 192.168.76.39: icmp: echo request
   4: 23:35:13.278778   192.168.75.39 > 192.168.76.39: icmp: echo request
   5: 23:35:15.279282   192.168.75.39 > 192.168.76.39: icmp: echo request
5 packets shown
```

最初のパケットのトレース（エコー要求）は、次のように表示されます（重要なポイントは強調表示されています）。

スポイラー（参照用に強調表示）

firepower# show capture CAPIパケット番号1トレース

5 packets captured

1: 23:35:07.281738 192.168.75.39 > 192.168.76.39: icmp：エコー要求

フェーズ： 1

タイプ：CAPTURE

Subtype:

結果： ALLOW

Config:

Additional Information:

MAC Access list

フェーズ： 2

タイプ：ACCESS-LIST

Subtype:

結果： ALLOW

Config:

Implicit Rule

Additional Information:

MAC Access list

フェーズ： 3

タイプ：ROUTE-LOOKUP

サブタイプ：出力インターフェイスの解決

結果： ALLOW

Config:

Additional Information:

ネクストホップ192.168.76.39が出力ifc外部を使用していることが判明しました

フェーズ： 4

タイプ：ACCESS-LIST

サブタイプ：ログ

結果： ALLOW

Config:

access-group CSM_FW_ACL_ global

access-list CSM_FW_ACL_ advanced trust ip 192.168.75.0 255.255.255.0 any rule-id 268434448 event-log both

access-list CSM_FW_ACL_ remark rule-id 268434448：プレフィルタポリシー：Prefilter_Policy1

access-list CSM_FW_ACL_ remark rule-id 268434448：ルール：Fastpath_src_192.168.75.0/24

Additional Information:

フェーズ：5

タイプ： CONN-SETTINGS

Subtype:

結果： ALLOW

Config:

クラスマップクラスデフォルト

 match any

policy-map global_policy

 class class-default

  接続の詳細設定オプションUM_STATIC_TCP_MAPを設定する

service-policy global_policy global

Additional Information:

フェーズ：6

タイプ：NAT

サブタイプ：セッションごと

結果： ALLOW

Config:

Additional Information:

フェーズ：7

タイプ：IP-OPTIONS

Subtype:

結果： ALLOW

Config:

Additional Information:

フェーズ：8

タイプ：INSPECT

サブタイプ： np-inspect

結果： ALLOW

Config:

class-map inspection_default

 match default-inspection-traffic

policy-map global_policy

 class inspection_default

  インスペクションICMP

service-policy global_policy global

Additional Information:

フェーズ：9

タイプ：INSPECT

サブタイプ： np-inspect

結果： ALLOW

Config:

Additional Information:

フェーズ： 10

タイプ：NAT

サブタイプ：セッションごと

結果： ALLOW

Config:

Additional Information:

フェーズ：11

タイプ：IP-OPTIONS

Subtype:

結果： ALLOW

Config:

Additional Information:

フェーズ：12

タイプ：FLOW-CREATION

Subtype:

結果： ALLOW

Config:

Additional Information:

ID 52で作成された新しいフロー、次のモジュールにパケットがディスパッチされました

フェーズ：13

タイプ：ACCESS-LIST

サブタイプ：ログ

結果： ALLOW

Config:

access-group CSM_FW_ACL_ global

access-list CSM_FW_ACL_ advanced trust ip 192.168.75.0 255.255.255.0 any rule-id 268434448 event-log both

access-list CSM_FW_ACL_ remark rule-id 268434448：プレフィルタポリシー：Prefilter_Policy1

access-list CSM_FW_ACL_ remark rule-id 268434448：ルール：Fastpath_src_192.168.75.0/24

Additional Information:

フェーズ：14

タイプ： CONN-SETTINGS

Subtype:

結果： ALLOW

Config:

クラスマップクラスデフォルト

match any

policy-map global_policy

class class-default

接続の詳細設定オプションUM_STATIC_TCP_MAPを設定する

service-policy global_policy global

Additional Information:

フェーズ：15

タイプ：NAT

サブタイプ：セッションごと

結果： ALLOW

Config:

Additional Information:

フェーズ：16

タイプ：IP-OPTIONS

Subtype:

結果： ALLOW

Config:

Additional Information:

フェーズ：17

タイプ：ROUTE-LOOKUP

サブタイプ：出力インターフェイスの解決

結果： ALLOW

Config:

Additional Information:

ネクストホップ192.168.76.39が出力ifc外部を使用していることが判明しました

フェーズ：18

タイプ：ADJACENCY-LOOKUP

サブタイプ：ネクストホップと隣接関係

結果： ALLOW

Config:

Additional Information:

隣接関係アクティブ

ネクストホップmacアドレス0004.deab.681bが140372416161507にヒット

フェーズ：19

タイプ：CAPTURE

Subtype:

結果： ALLOW

Config:

Additional Information:

MAC Access list

Result:

入力インターフェイス：外部

入力ステータス：アップ

input-line-status:up（入力回線ステータス：アップ）

出力インターフェイス：外部

出力ステータス：アップ

出力回線ステータス：アップ

アクション：許可

1 packet shown

firepower#

firepower# show capture CAPI packet-number 1 trace 5キャプチャされたパケット1: 23:35:07.281738 192.168.75.39 > 192.168.76.39: icmp: echo request Phase: 1タイプ： CAPTURE Subtype: Result: ALLOW Config: Additional Information: MAC Access list Phase: 2タイプ： ACCESS-LIST Subtype: Result: ALLOW Config: ImPLICIT Rule AdDITIONAL Information: MAC Access Information: フェーズ： 3タイプ： ROUTE-LOOKUPサブタイプ：出力インターフェイスの解決結果：許可する構成：追加情報：検出されたネクストホップ192.168.76.39は出力ifc外部を使用しますフェーズ： 4タイプ： ACCESS-LISTサブタイプ：ログ結果： ALLOW構成：access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ advanced trust ip 192.168.75.055.255.255.0 any rule-id 268434448 event-log both access-list CSM_FW_ACL_ remark rule-id 268434448: PREFILTER POLICY: Prefilter_Policy1 access-list CSM_FW_ACL_ remark rule-id 268434448: RULE: Fastpath_src_192.168.75.0/24追加情報： Phase: 5 Type: CONN-SETTINGS Subtype: Result: ALLOW Config: class-map-class-match any policy map global-policy class default-class-class default connection advanced-options UM_STATIC_TCP_MAP service-policy global_policy global追加情報：フェーズ： 6タイプ： NATサブタイプ：セッション単位の結果：許可設定：追加情報：フェーズ： 7タイプ： IP-OPTIONSサブタイプ：許可設定：追加情報：フェーズ： 8タイプ： INSPECTサブタイプ： np-inspect結果： ALLOW Config: class-map inspection_default match-inspection-policy global_policy class inspect icmp service-policy global_policy情報：フェーズ： 9タイプ： INSPECTサブタイプ： np-inspect結果：許可Config：追加情報：フェーズ： 10タイプ： NATサブタイプ：セッションごとの結果：許可Config：追加情報：フェーズ： 11タイプ： IP-OPTIONSサブタイプ：結果： ALLOW Config：追加情報：フェーズ： 12タイプ： FLOW-CREATIONサブタイプ：結果： ALLOW Config：追加情報：新しいフローがID 52で作成され、次のモジュールにディスパッチされたフェーズ： 1 3 Type: ACCESS-LIST Subtype: log Result: ALLOW Config: access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ advanced trust ip 192.168.75.0 255.255.255.0 any rule-id 268434448 268434448 event-log both access-list CSM_FW_ACL_ remark rule-id: PREFILTER POLICY: Prefilter_Policy access-list CSM 268434448: RULE: Fastpath_src_192.168.75.0/24追加情報：フェーズ： 14タイプ： CONN-SETTINGSサブタイプ：結果： ALLOW Config: class-map class-default match any policy-map global_policy class-default set connection advanced-options UM_STATIC_TCP_MAP service-policy global_policy global追加情報：フェーズ： 15タイプ： NATサブタイプ： per-session結果： ALLOW Config：追加情報：フェーズ： 16タイプ： IP-OPTIONSサブタイプ：結果：許可Config：追加情報：フェーズ： 17タイプ： ROUTE-

LOOKUPサブタイプ：解決Egressインターフェイス結果：許可Config：追加情報： found next-hop 192.168.76.39 uses egress ifc outsideフェーズ： 18タイプ： ADJACENCY-LOOKUPサブタイプ：ネクストホップおよびアジャセンシー結果：許可Config：追加情報：アジャセンシー関係Activeアドレスmac 0004.deab.681b hits 140372416161507 Phase: 19タイプ： CAPTUREサブタイプ：結果： ALLOW Config：追加情報： MACアクセスリスト結果： input-interface: outside input-status: up input-line-status: up output-interface: outside output-status: up output-line-status: upアクション： allow 1パケットが表示されたfirepower#

Outsideインターフェイスのキャプチャは次のように表示されます。

<#root>

```
firepower#

show capture CAPO


10 packets captured

   1: 23:35:07.282044   192.168.75.39 > 192.168.76.39: icmp: echo request
   2: 23:35:07.282227   192.168.76.39 > 192.168.75.39: icmp: echo reply
   3: 23:35:09.278717   192.168.75.39 > 192.168.76.39: icmp: echo request
   4: 23:35:09.278962   192.168.76.39 > 192.168.75.39: icmp: echo reply
   5: 23:35:11.279343   192.168.75.39 > 192.168.76.39: icmp: echo request
   6: 23:35:11.279541   192.168.76.39 > 192.168.75.39: icmp: echo reply
   7: 23:35:13.278870   192.168.75.39 > 192.168.76.39: icmp: echo request
   8: 23:35:13.279023   192.168.76.39 > 192.168.75.39: icmp: echo reply
   9: 23:35:15.279373   192.168.75.39 > 192.168.76.39: icmp: echo request
  10: 23:35:15.279541   192.168.76.39 > 192.168.75.39: icmp: echo reply
10 packets shown
```

戻りパケットのトレースには、現在のフロー(52)と一致することが示されますが、ACLによってブロックされています。

<#root>

```
firepower#

show capture CAPO packet-number 2 trace


10 packets captured


2: 23:35:07.282227       192.168.76.39 > 192.168.75.39: icmp: echo reply

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 52, uses current flow

```
Phase: 4
```

Type: ACCESS-LIST

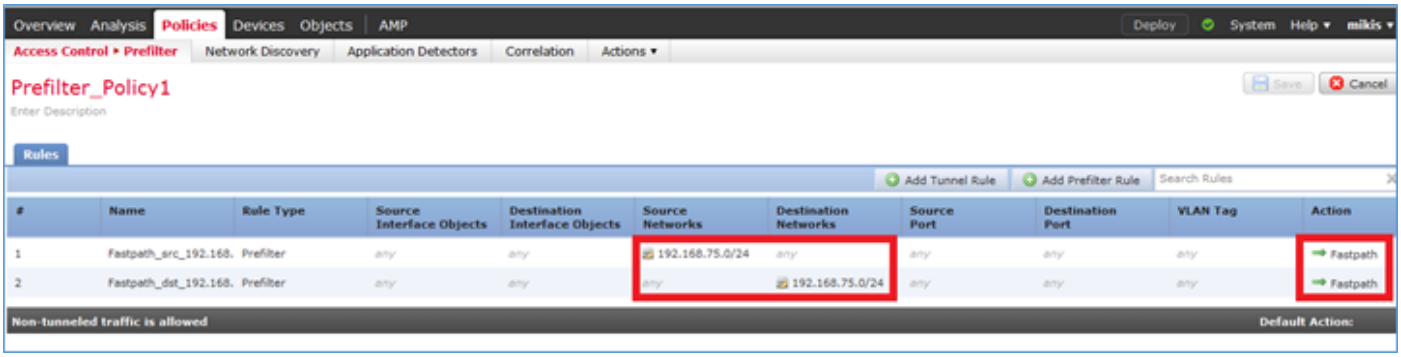
```
Subtype: log
```

Result: DROP

```
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced deny ip any any rule-id 268434432 event-log flow-start
access-list CSM_FW_ACL_ remark rule-id 268434432: ACCESS POLICY: ACP_5506-1 - Default/1
access-list CSM_FW_ACL_ remark rule-id 268434432: L4 RULE: DEFAULT ACTION RULE
Additional Information:

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

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

ステップ 5：リターントラフィック用にプレフィルタルールをもう1つ追加します。結果は図のようになります。



次に、表示された戻りパケットをトレースします（重要な点が強調表示されています）。

スポイラー（参照用に強調表示）

```
firepower# show capture CAPO packet-number 2トレース

10 packets captured

2: 00:01:38.873123 192.168.76.39 > 192.168.75.39: icmp：エコー応答

フェーズ： 1

タイプ：CAPTURE

Subtype:

結果： ALLOW

Config:

Additional Information:

MAC Access list

フェーズ： 2

タイプ：ACCESS-LIST

Subtype:

結果： ALLOW

Config:

Implicit Rule

Additional Information:

MAC Access list

フェーズ： 3

タイプ：FLOW-LOOKUP

Subtype:

結果： ALLOW

Config:

Additional Information:

ID 62のフローが見つかりました。現在のフローを使用します

フェーズ： 4

タイプ：ACCESS-LIST
```

サブタイプ：ログ

結果： ALLOW

Config:

access-group CSM_FW_ACL_ global

access-list CSM_FW_ACL_ advanced trust ip any 192.168.75.0 255.255.255.0 rule-id 268434450 event-log both

access-list CSM_FW_ACL_ remark rule-id 268434450：プレフィルタポリシー：Prefilter_Policy1

access-list CSM_FW_ACL_ remark rule-id 268434450：ルール：Fastpath_dst_192.168.75.0/24

Additional Information:

フェーズ：5

タイプ： CONN-SETTINGS

Subtype:

結果： ALLOW

Config:

クラスマップクラスデフォルト

match any

policy-map global_policy

class class-default

接続の詳細設定オプションUM_STATIC_TCP_MAPを設定する

service-policy global_policy global

Additional Information:

フェーズ：6

タイプ：NAT

サブタイプ：セッションごと

結果： ALLOW

Config:

Additional Information:

フェーズ：7

タイプ：IP-OPTIONS

Subtype:

結果： ALLOW

Config:

Additional Information:

フェーズ：8

タイプ：ROUTE-LOOKUP

サブタイプ：出力インターフェイスの解決

結果： ALLOW

Config:

Additional Information:

ネクストホップ192.168.75.39が内部で出力ifcを使用していることが判明しました

フェーズ：9

タイプ：ADJACENCY-LOOKUP

サブタイプ：ネクストホップと隣接関係

結果： ALLOW

Config:

Additional Information:

隣接関係アクティブ

ネクストホップmacアドレスc84c.758d.4981が140376711128802にヒット

フェーズ： 10

タイプ：CAPTURE

Subtype:

結果： ALLOW

Config:

Additional Information:

MAC Access list

Result:

入力インターフェイス：内部

入力ステータス：アップ

input-line-status:up（入力回線ステータス：アップ）

出力インターフェイス：内部

出力ステータス：アップ

出力回線ステータス：アップ

アクション：許可

firepower# show capture CAPO packet-number 2 trace 10キャプチャされたパケット2: 00:01:38.873123 192.168.76.39 > 192.168.75.39: icmp: echo reply Phase: 1タイプ： CAPTURE Subtype: Result: ALLOW Config: Additional Information: MAC Access list Phase: 2タイプ： ACCESS-LIST Subtype: Result: ALLOW Config: Implicit Rule Additional Information: MAC Information: MAC アクセスリストフェーズ： 3タイプ： FLOW-LOOKUPサブタイプ：結果： ALLOW Config：追加情報： ID 62のフローが見つかりました。現在のフローを使用しています。フェーズ： 4タイプ： ACCESS-LISTサブタイプ：ログ結果： ALLOW Config: access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ advanced trust ip any 192.168.75.0 255.255.0 rule-id 268434450 -log both access-list CSM_FW_ACL_ remark rule-id 268434450: PREFILTER POLICY: Prefilter_Policy1 access-list CSM_FW_ACL_ remark rule-id 268434450: RULE: Fastpath_dst_192.168.75.0/24追加情報： Phase: 5タイプ： CONN-SETTINGSサブタイプ：結果：許可する構成： class-map class-default match any-policy-map global_policy class-default set connection advanced-options UM_STATIC_TCP-MAP policy global_policy global追加情報： Phase: 6タイプ： NATサブタイプ： per-session結果： ALLOW Config：追加情報： Phase: 7タイプ： IP-OPTIONSサブタイプ： Result: ALLOW Config：追加情報： Phase: 8タイプ： ROUTE-LOOKUPサブタイプ： Resolve Egressインターフェイス結果： ALLOW Config：追加情報： found next-hop 192.168.75.39 uses egifc inside Phase: 9タイプ： ADJACENCY LOOKUPサブタイプ：ネクストホップとアジャセンシー結果：許可Config：追加情報：アジャセンシー関係アクティブなネクストホップmacアドレスc84c.758d.4981ヒット140376711128802フェーズ：10タイプ：CAPTUREサブタイプ：結果：許可Config：追加情報：MACアクセスリスト結果：入力インターフェイス：内部input-status:up入力ラインステータス：up出力インターフェイス：内部output-status:up出力ラインステータス：upアクション：許可

確認

ここでは、設定が正常に機能しているかどうかを確認します。

検証については、それぞれのタスクセクションで説明しています。

トラブルシュート

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- Cisco Firepower Management Center(FMC)コンフィギュレーションガイドのすべてのバージョンは、次の場所にあります。

Cisco Secure Firewall Threat Defenseに関するドキュメントの参照

- Cisco Global Technical Assistance Center(TAC)では、このドキュメントで説明されている内容を含む、Cisco Firepower次世代セキュリティテクノロジーに関する詳細で実用的な知識を得るために、このビジュアルガイドを強く推奨しています。

Cisco Firepower Threat Defense（FTD）

- 設定とトラブルシューティングに関するすべてのテクニカルノート：

Cisco Secureファイアウォール管理センター

- テクニカル サポートとドキュメント - Cisco Systems

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。