Configure and Operate FTD Prefilter Policies

Contents

Introduction

This document describes the configuration and operation of Firepower Threat Defense (FTD) Prefilter Policies.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- ASA5506X that runs FTD code 6.1.0-195
- FireSIGHT Management Center (FMC) that runs 6.1.0-195
- Two 3925 Cisco IOS® routers that runs 15.2 images

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

A Prefilter Policy is a feature introduced in 6.1 version and serves three main purposes:

1. Match traffic based on both inner and outer headers

2. Provide early Access Control which allows a flow to bypass Snort engine completely
3. Work as a placeholder for Access Control Entries (ACEs) that are migrated from Adaptive Security Appliance (ASA) migration tool.

Configure

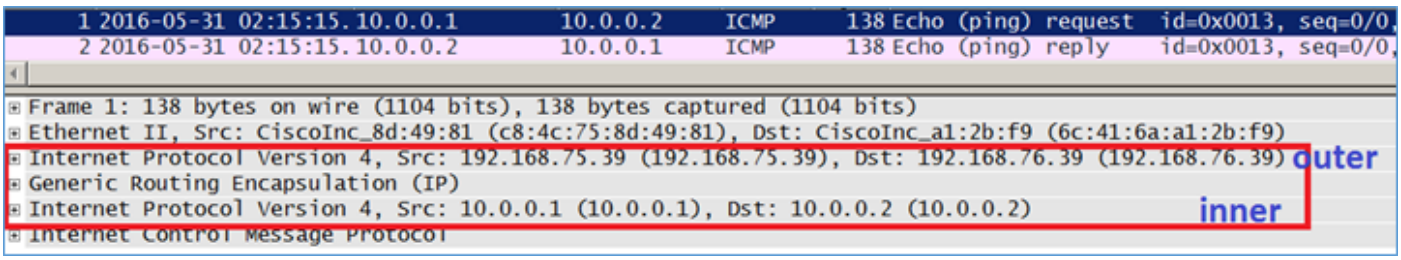
Prefilter Policy Use Case 1

A Prefilter Policy can use a Tunnel Rule Type which allows FTD to filter based on both inside and/or outside IP header tunneled traffic. At the time this article was written, tunneled traffic refers to:

- Generic Routing Encapsulation (GRE)
- IP-in-IP
- IPv6-in-IP
- Teredo Port 3544

Consider a GRE tunnel as shown in the image.

When you ping from R1 to R2 with the use of a GRE tunnel, the traffic goes through the Firewall looks as shown in the image.



If the firewall is an ASA device, it checks the outer IP header as shown in the image.

<#root>

ASA#

show conn

GRE OUTSIDE 192.168.76.39:0 INSIDE 192.168.75.39:0

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

If the firewall is a FirePOWER device, it checks the inner IP header as shown in the image.

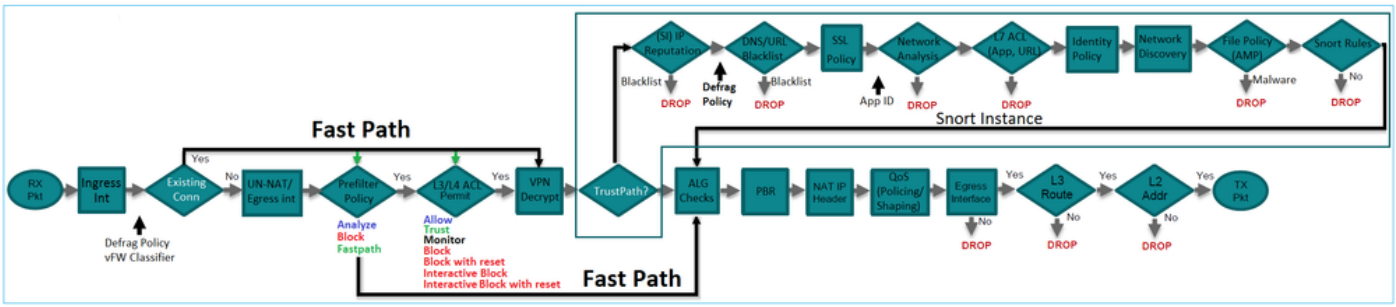
With prefilter policy, an FTD device can match traffic based on both inner and outer headers.

Main point

Device	Checks
ASA	Outer IP
Snort	Inner IP
FTD	Outer (Prefilter) + Inner IP (Access Control Policy(ACP))

Prefilter Policy Use Case 2

A Prefilter Policy can use a Prefilter Rule Type which can provide early Access Control and allow a flow to bypass Snort engine completely as shown in the image.



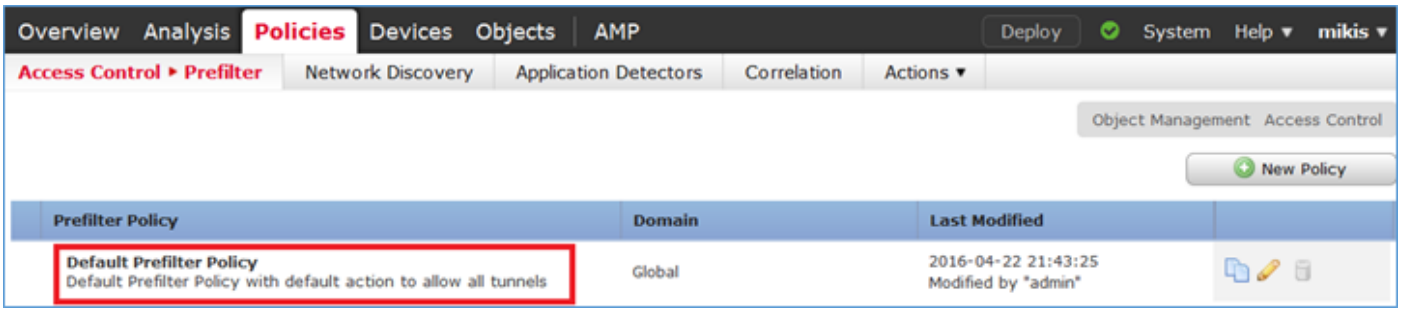
Task 1. Verify Default Prefilter Policy

Task requirement

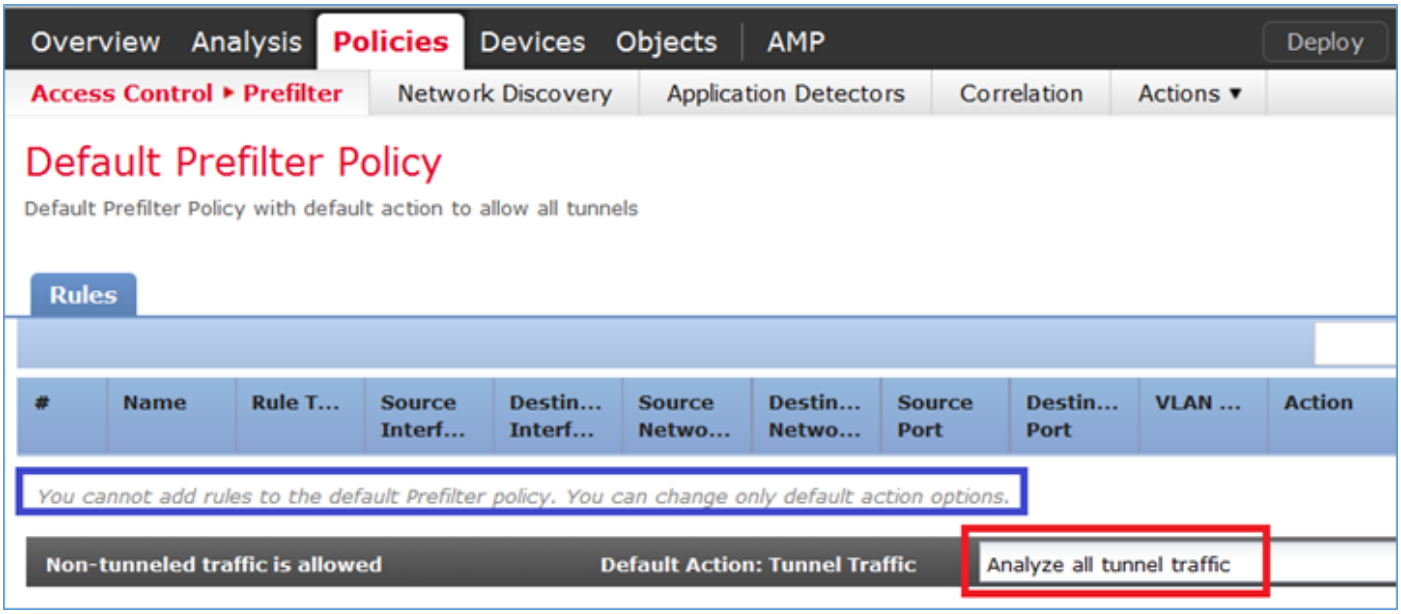
Verify the default Prefilter Policy

Solution

Step 1. Navigate to **Policies > Access Control > Prefilter**. A default Prefilter Policy already exists as shown in the image.



Step 2. Choose **Edit** to see the policy settings as shown in the image.



Step 3. The Prefilter Policy is already attached to the Access Control Policy as shown in the image.

CLI (LINA) Verification

Prefilter rules are added on top of ACLs:

<#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
```

Task 2. Block Tunneled Traffic with Tag

Task requirement

Block ICMP traffic that is tunneled inside GRE tunnel.

Solution

Step 1. If you apply these ACP, you can see that Internet Control Message Protocol (ICMP) traffic is blocked, no matter if it goes through the GRE tunnel or not, as shown in the image.

<#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)

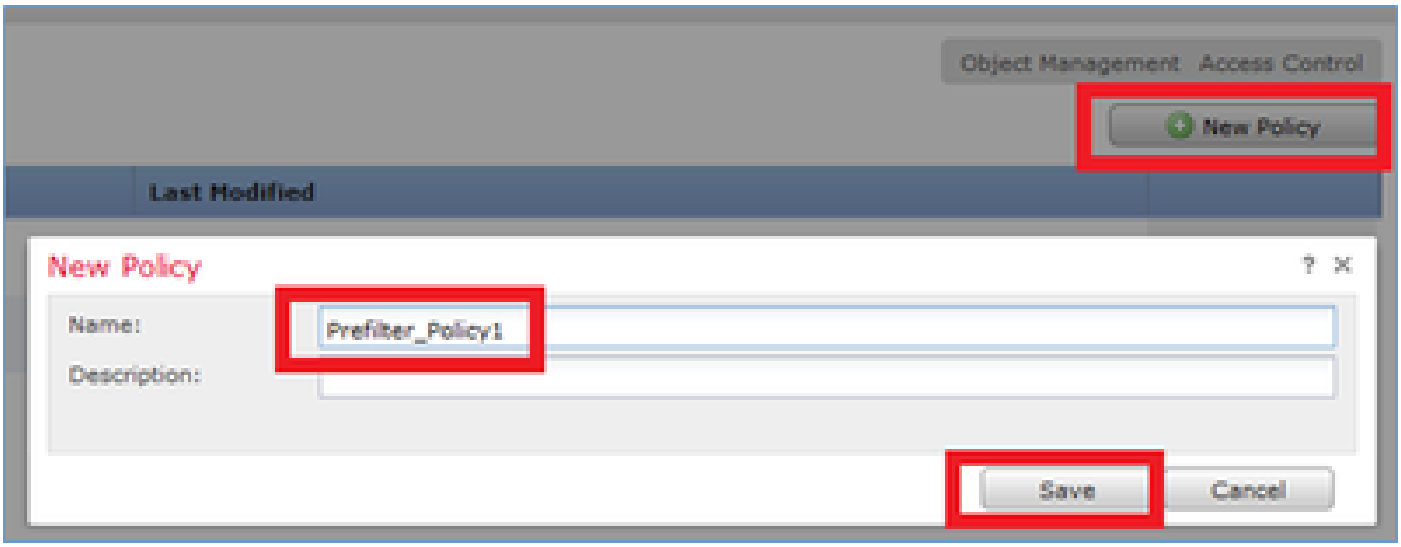
In this case, you can use a Prefilter Policy to meet the task requirement. The logic is as follows:

1. Tag all packets that are encapsulated inside GRE.
2. Create an Access Control Policy that matches the tagged packets and blocks ICMP.

From architecture point of view, the packets are checked against the LInux NAtively (LINA) pre-filter rules, then Snort pre-filter rules and ACP, and finally Snort instructs LINA to drop. The first packet makes it through the FTD device.

Step 1. Define a Tag for tunneled traffic.

Navigate to **Policies > Access Control > Prefilter** and create a new Prefilter Policy. Remember that the default Prefilter Policy cannot be edited as shown in the image.

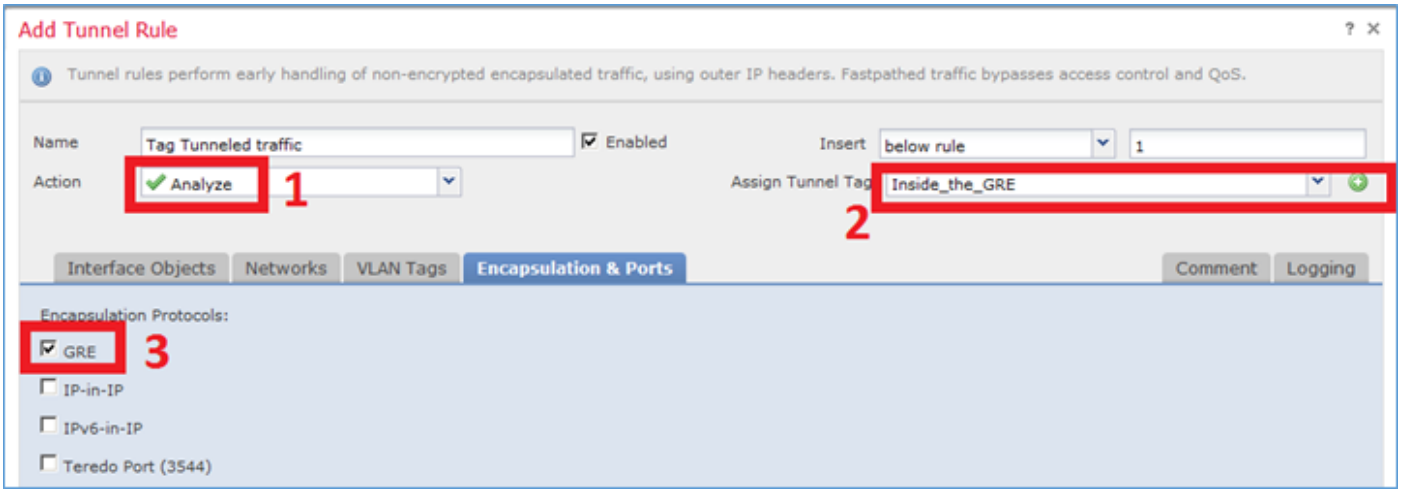


Inside the Prefilter Policy, define two types of rules:

1. Tunnel Rule
2. Prefilter Rule

You can think of these two as totally different features that can be configured in a Prefilter Policy.

For this task, it is necessary to define a Tunnel Rule as shown in the image.

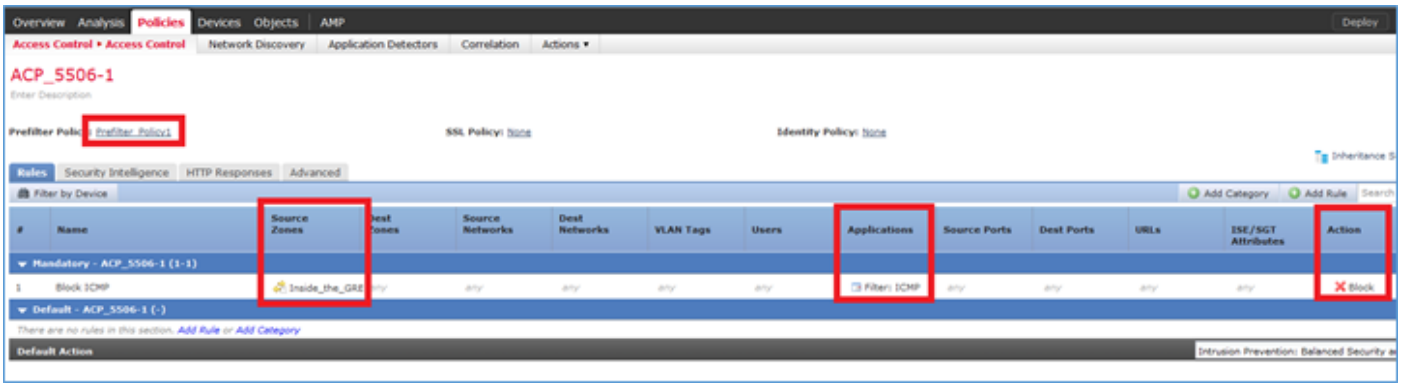


With regards to the Actions:

Action	**Description**
Analyze	After LINA, the flow is checked by Snort Engine. Optionally, a Tunnel Tag can be assigned to the tunneled traffic.
Block	The flow is blocked by LINA. The outer header is to be checked.
Fastpath	The flow is handled only by LINA without the need to engage the Snort engine.

Step 2. Define the Access Control Policy for the tagged traffic.

Although it cannot be very intuitive at first, the Tunnel Tag can be used by an Access Control Policy Rule as a Source Zone. Navigate to **Policies > Access Control** and create a Rule that blocks ICMP for the tagged traffic as shown in the image.



Note: The new Prefilter Policy is attached to the Access Control Policy.

Verification

Enable capture on LINA and on CLISH:

```
<#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
```

From R1, try to ping the remote GRE tunnel endpoint. The ping fails:

```
<#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)
```

The CLISH capture shows that the first echo-request went through FTD and the reply was blocked:

```
<#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
```

The LINA capture confirms this:

```
<#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
```

Enable CLISH firewall-engine-debug, clear LINA ASP drop counters and do the same test. The CLISH debug shows that for the Echo-Request you matched the prefilter rule and for the Echo-Reply the ACP rule:

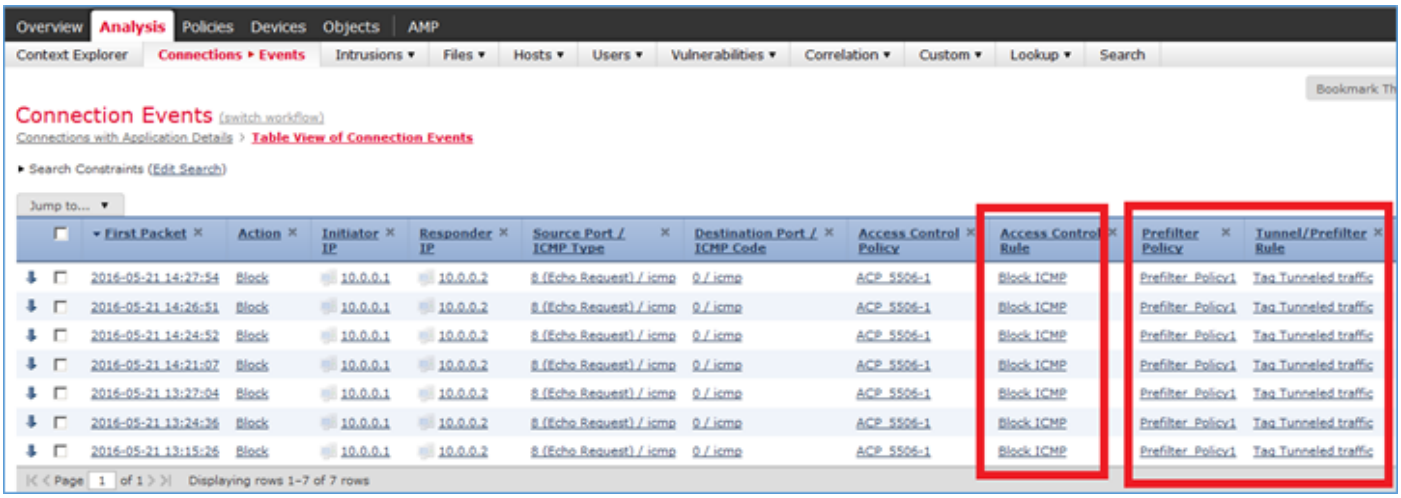
```
<#root>
```

```
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
```

The ASP drop shows that Snort dropped the packets:

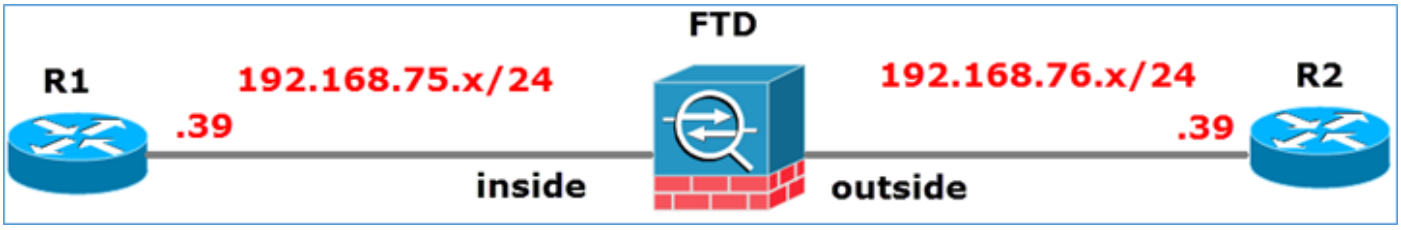
```
<#root>
>
show asp drop

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
```

In the Connection Events, you can see the Prefilter Policy and Rule that you matched as shown in the image.



Task 3. Bypass Snort Engine with Fastpath Prefilter Rules

Network Diagram

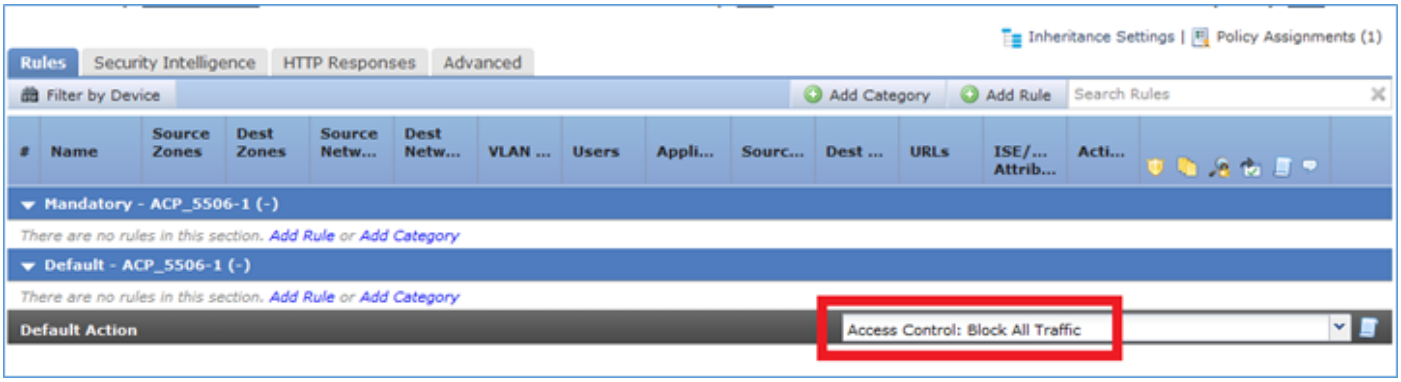


Task requirement

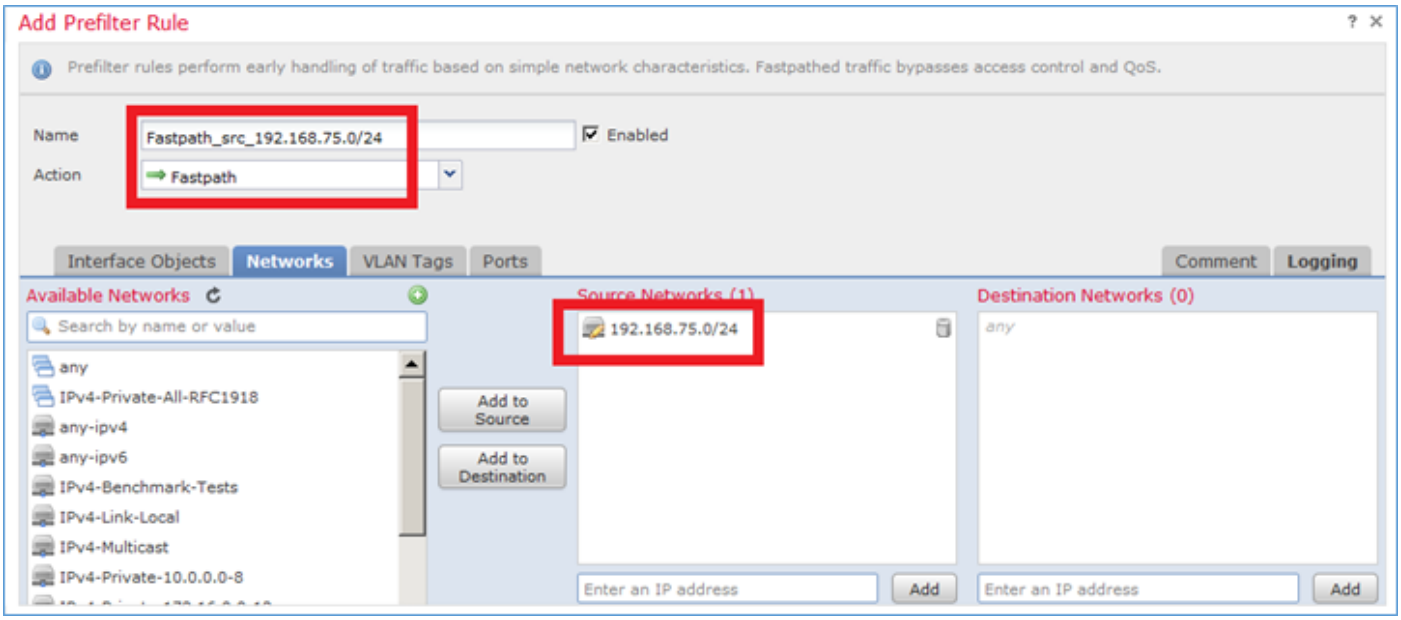
1. Remove current Access Control Policy rules and add an Access Control Policy rule that Blocks all traffic.
2. Configure a Prefilter Policy rule that bypasses the Snort Engine for traffic sourced from the 192.168.75.0/24 network.

Solution

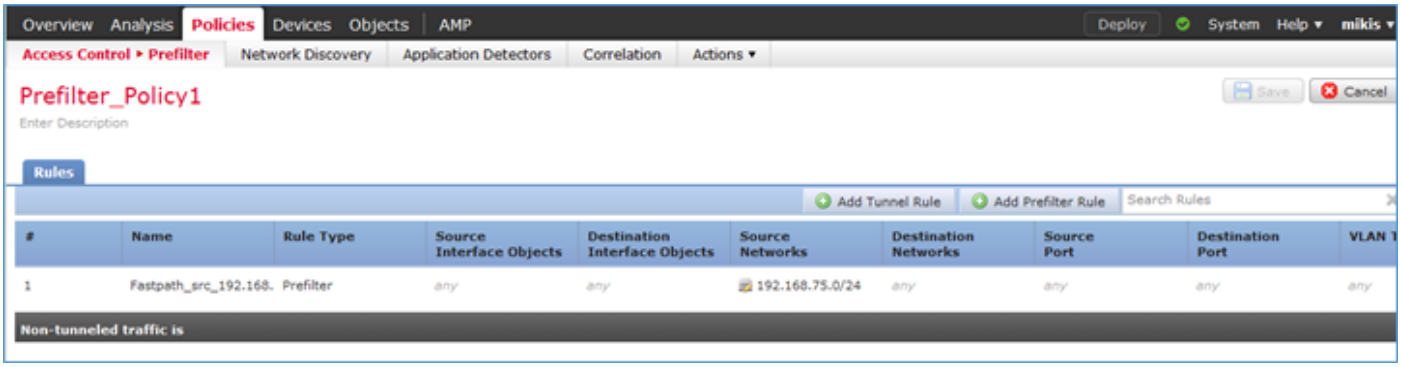
Step 1. Access Control Policy that Blocks all the traffic is as shown in the image.



Step 2. Add a Prefilter Rule with Fastpath as an action for source network 192.168.75.0/24 as shown in the image.



Step 3. The result is as shown in the image.



Step 4. **Save** and **Deploy**.

Enable capture with trace on both FTD interfaces:

<#root>

```
firepower#
```

capture CAPI int inside trace match icmp any any

```
firepower#
```

capture CAPO int outsid trace match icmp any any

Try to ping from R1 (192.168.75.39) to R2 (192.168.76.39) through the FTD. Ping fails:

<#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)
```

Capture on the inside interface shows:

<#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
```

Trace of first packet (echo-request) shows (important points highlighted):

Spoiler (Highlight to read)

firepower# show capture CAPI packet-number 1 trace

5 packets captured

1: 23:35:07.281738 192.168.75.39 > 192.168.76.39: icmp: echo request

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: ROUTE-LOOKUP

Subtype: Resolve Egress Interface

Result: ALLOW

Config:

Additional Information:

found next-hop 192.168.76.39 uses egress ifc outside

Phase: 4

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 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

Additional Information:

Phase: 5

Type: CONN-SETTINGS

Subtype:

Result: ALLOW

Config:

class-map class-default

 match any

policy-map global_policy

class class-default

set connection advanced-options UM_STATIC_TCP_MAP

service-policy global_policy global

Additional Information:

Phase: 6

Type: NAT

Subtype: per-session

Result: ALLOW

Config:

Additional Information:

Phase: 7

Type: IP-OPTIONS

Subtype:

Result: ALLOW

Config:

Additional Information:

Phase: 8

Type: INSPECT

Subtype: np-inspect

Result: ALLOW

Config:

class-map inspection_default

match default-inspection-traffic

policy-map global_policy

class inspection_default

inspect icmp

service-policy global_policy global

Additional Information:

Phase: 9

Type: INSPECT

Subtype: np-inspect

Result: ALLOW

Config:

Additional Information:

Phase: 10

Type: NAT

Subtype: per-session

Result: ALLOW

Config:

Additional Information:

Phase: 11

Type: IP-OPTIONS

Subtype:

Result: ALLOW

Config:

Additional Information:

Phase: 12

Type: FLOW-CREATION

Subtype:

Result: ALLOW

Config:

Additional Information:

New flow created with id 52, packet dispatched to next module

Phase: 13

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 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

Additional Information:

Phase: 14

Type: CONN-SETTINGS

Subtype:

Result: ALLOW

Config:

class-map class-default

 match any

policy-map global_policy

 class class-default

  set connection advanced-options UM_STATIC_TCP_MAP

service-policy global_policy global

Additional Information:

Phase: 15

Type: NAT

Subtype: per-session

Result: ALLOW

Config:

Additional Information:

Phase: 16

Type: IP-OPTIONS

Subtype:

Result: ALLOW

Config:

Additional Information:

Phase: 17

Type: ROUTE-LOOKUP

Subtype: Resolve Egress Interface

Result: ALLOW

Config:

Additional Information:

found next-hop 192.168.76.39 uses egress ifc outside

Phase: 18

Type: ADJACENCY-LOOKUP

Subtype: next-hop and adjacency

Result: ALLOW

Config:

Additional Information:

adjacency Active

next-hop mac address 0004.deab.681b hits 140372416161507

Phase: 19

Type: CAPTURE

Subtype:

Result: ALLOW

Config:

Additional Information:

MAC Access list

Result:

input-interface: outside

input-status: up

input-line-status: up

output-interface: outside

output-status: up

output-line-status: up

Action: allow

1 packet shown

firepower#

firepower# show capture CAPI packet-number 1 trace 5 packets captured 1: 23:35:07.281738 192.168.75.39 > 192.168.76.39: icmp: echo request 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: ROUTE-LOOKUP Subtype: Resolve Egress Interface Result: ALLOW Config: Additional Information: found next-hop 192.168.76.39 uses egress ifc outside Phase: 4 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 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 Additional Information: Phase: 5 Type: CONN-SETTINGS Subtype: Result: ALLOW Config: class-map class-default match any policy-map global_policy class class-default set connection advanced-options UM_STATIC_TCP_MAP service-policy global_policy global Additional Information: Phase: 6 Type: NAT Subtype: per-session Result: ALLOW Config: Additional Information: Phase: 7 Type: IP-OPTIONS Subtype: Result: ALLOW Config: Additional Information: Phase: 8 Type: INSPECT Subtype: np-inspect Result: ALLOW Config: class-map inspection_default match default-inspection-traffic policy-map global_policy class inspection_default inspect icmp service-policy global_policy global Additional Information: Phase: 9 Type: INSPECT Subtype: np-inspect Result: ALLOW Config: Additional Information: Phase: 10 Type: NAT Subtype: per-session Result: ALLOW Config: Additional Information: Phase: 11 Type: IP-OPTIONS Subtype: Result: ALLOW Config: Additional Information: Phase: 12 Type: FLOW-CREATION Subtype: Result: ALLOW Config: Additional Information: New flow created with id 52, packet dispatched to next module Phase: 13 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 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 Additional Information: Phase: 14 Type: CONN-SETTINGS Subtype: Result: ALLOW Config: class-map class-default match any policy-map global_policy class class-default set connection advanced-options UM_STATIC_TCP_MAP service-policy global_policy global Additional Information: Phase: 15 Type: NAT Subtype: per-session Result: ALLOW Config: Additional Information: Phase: 16 Type: IP-OPTIONS Subtype: Result: ALLOW Config: Additional Information: Phase: 17 Type: ROUTE-LOOKUP Subtype: Resolve Egress Interface Result: ALLOW Config: Additional Information: found next-hop 192.168.76.39 uses egress ifc outside Phase: 18 Type: ADJACENCY-LOOKUP Subtype: next-hop and adjacency Result: ALLOW Config: Additional Information: adjacency Active next-hop mac address 0004.deab.681b hits 140372416161507 Phase: 19 Type: CAPTURE Subtype: Result: ALLOW Config: Additional Information: MAC Access list Result: input-interface: outside input-status: up input-line-status: up output-interface: outside output-status: up output-line-status: up Action: allow 1 packet shown firepower#

Capture on the outside interface shows:

<#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
```

Trace of the return packet shows that it matches the current flow (52), but it is blocked by the ACL:

<#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

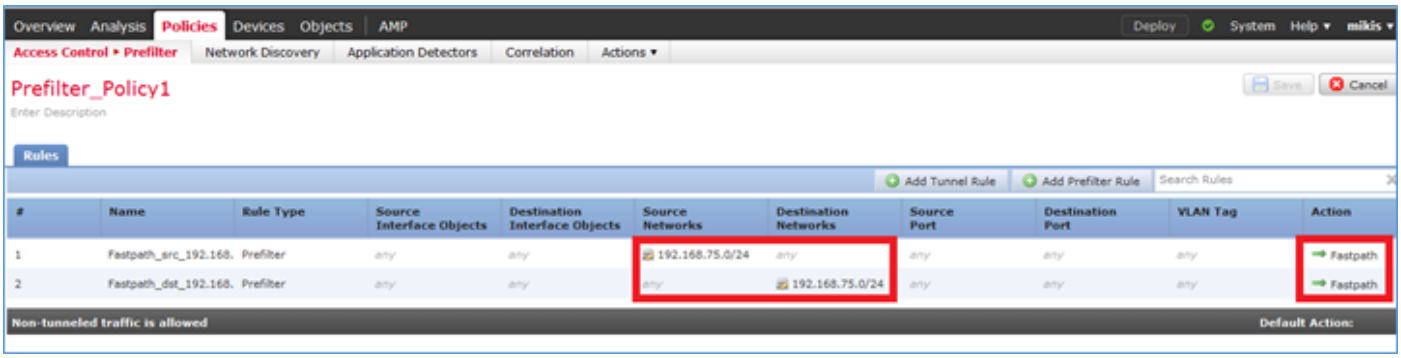
Subtype: log

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`

Step 5. Add one more prefilter rule for the return traffic. The result is as shown in the image.



Now trace the return packet you see (important points highlighted):

Spoiler (Highlight to read)

firepower# show capture CAPO packet-number 2 trace

10 packets captured

2: 00:01:38.873123 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 62, uses current flow

Phase: 4

Type: ACCESS-LIST

Subtype: log

Result: 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: PREFILTER POLICY: Prefilter_Policy1

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

Additional Information:

Phase: 5

Type: CONN-SETTINGS

Subtype:

Result: ALLOW

Config:

class-map class-default

match any

policy-map global_policy

class class-default

set connection advanced-options UM_STATIC_TCP_MAP

service-policy global_policy global

Additional Information:

Phase: 6

Type: NAT

Subtype: per-session

Result: ALLOW

Config:

Additional Information:

Phase: 7

Type: IP-OPTIONS

Subtype:

Result: ALLOW

Config:

Additional Information:

Phase: 8

Type: ROUTE-LOOKUP

Subtype: Resolve Egress Interface

Result: ALLOW

Config:

Additional Information:

found next-hop 192.168.75.39 uses egress ifc inside

Phase: 9

Type: ADJACENCY-LOOKUP

Subtype: next-hop and adjacency

Result: ALLOW

Config:

Additional Information:

adjacency Active

next-hop mac address c84c.758d.4981 hits 140376711128802

Phase: 10

Type: CAPTURE

Subtype:

Result: ALLOW

Config:

Additional Information:

MAC Access list

Result:

input-interface: inside

input-status: up

input-line-status: up

output-interface: inside

output-status: up

output-line-status: up

Action: allow

firepower# show capture CAPO packet-number 2 trace 10 packets captured 2: 00:01:38.873123 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 62, uses current flow Phase: 4 Type: ACCESS-LIST Subtype: log Result: 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: PREFILTER POLICY: Prefilter_Policy1 access-list CSM_FW_ACL_ remark rule-id 268434450: RULE: Fastpath_dst_192.168.75.0/24 Additional Information: Phase: 5 Type: CONN-SETTINGS Subtype: Result: ALLOW Config: class-map class-default match any policy-map global_policy class class-default set connection advanced-options UM_STATIC_TCP_MAP service-policy global_policy global Additional Information: Phase: 6 Type: NAT Subtype: per-session Result: ALLOW Config: Additional Information: Phase: 7 Type: IP-OPTIONS Subtype: Result: ALLOW Config: Additional Information: Phase: 8 Type: ROUTE-LOOKUP Subtype: Resolve Egress Interface Result: ALLOW Config: Additional Information: found next-hop 192.168.75.39 uses egress ifc inside Phase: 9 Type: ADJACENCY-LOOKUP Subtype: next-hop and adjacency Result: ALLOW Config: Additional Information: adjacency Active next-hop mac address c84c.758d.4981 hits 140376711128802 Phase: 10 Type: CAPTURE Subtype: Result: ALLOW Config: Additional Information: MAC Access list Result: input-interface: inside input-status: up input-line-status: up output-interface:

inside output-status: up output-line-status: up Action: allow

Verify

Use this section in order to confirm that your configuration works properly.

The verification has been explained in the respective tasks sections.

Troubleshoot

There is currently no specific information available to troubleshoot this configuration.

Related Information

- All versions of the Cisco Firepower Management Center configuration guide can be found here:

Navigating the Cisco Secure Firewall Threat Defense Documentation

- Cisco Global Technical Assistance Center (TAC) strongly recommends this visual guide for in-depth practical knowledge on Cisco Firepower Next Generation Security Technologies, that includes the ones mentioned in this article:

Cisco Firepower Threat Defense (FTD)

- For all Configuration and Troubleshooting TechNotes:

Cisco Secure Firewall Management Center

- Technical Support & Documentation - Cisco Systems