FTD-Vorfilterrichtlinien konfigurieren und ausführen

Inhalt

Einleitung

Dieses Dokument beschreibt die Konfiguration und den Betrieb von Firepower Threat Defense (FTD) Prefilter Policies.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- ASA5506X mit FTD-Code 6.1.0-195
- FireSIGHT Management Center (FMC) mit 6.1.0-195
- Zwei 3925 Cisco IOS® Router mit 15.2 Images

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Eine Prefilter Policy wurde in Version 6.1 eingeführt und erfüllt drei Hauptaufgaben:

1. Datenverkehr auf Basis der inneren und äußeren Kopfzeile zuordnen
2. Frühzeitige Zugriffskontrolle, die eine vollständige Umgehung der Snort-Engine ermöglicht
3. Sie fungieren als Platzhalter für Zugriffskontrolleinträge (Access Control Entries, ACEs), die vom Migrationstool der Adaptive Security Appliance (ASA) migriert wurden.

Konfigurieren

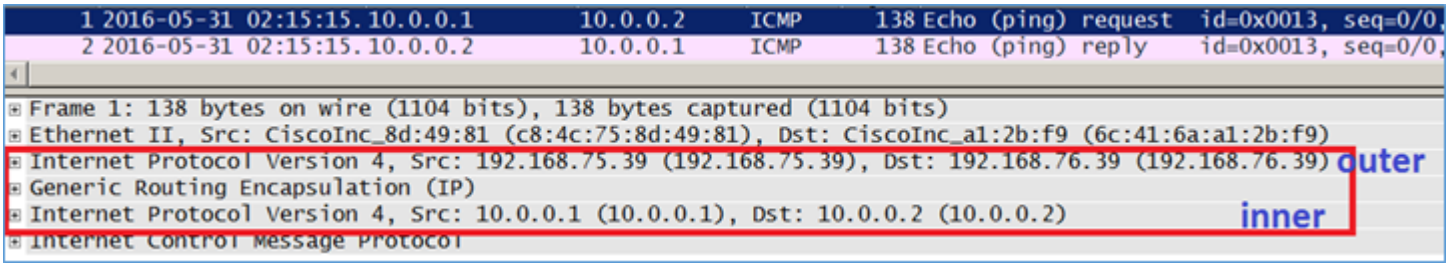
Anwendungsfall 1 der Prefilter-Richtlinie

Eine Prefilter-Richtlinie kann einen Tunnel-Regeltyp verwenden, mit dem FTD auf Basis des internen und/oder externen getunnelten IP-Header-Datenverkehrs filtern kann. Zum Zeitpunkt der Erstellung dieses Artikels bezieht sich der getunnelte Datenverkehr auf:

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

Betrachten Sie einen GRE-Tunnel, wie in der Abbildung dargestellt.

Wenn Sie unter Verwendung eines GRE-Tunnels einen Ping von R1 an R2 senden, wird der Datenverkehr durch die Firewall geleitet. Dies sieht im Bild so aus.



Wenn es sich bei der Firewall um ein ASA-Gerät handelt, wird der äußere IP-Header wie im Abbild dargestellt überprüft.

<#root>

ASA#

show conn

GRE OUTSIDE 192.168.76.39:0 INSIDE 192.168.75.39:0

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

Wenn es sich bei der Firewall um ein FirePOWER-Gerät handelt, wird der innere IP-Header wie im Bild dargestellt überprüft.

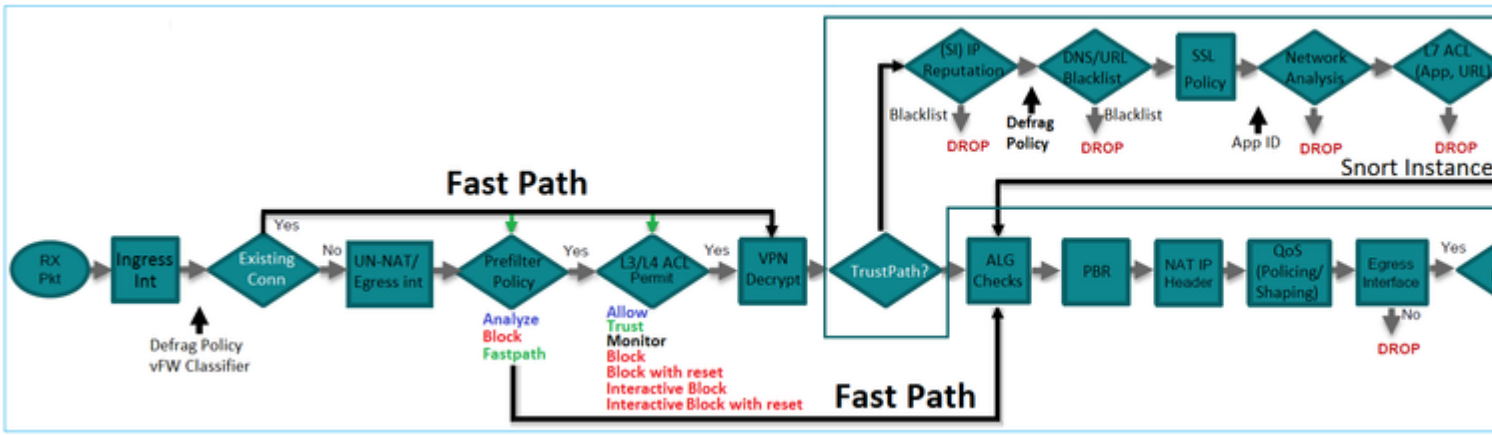
Mit der Prefilter-Richtlinie kann ein FTD-Gerät den Datenverkehr auf Basis der inneren und äußeren Kopfzeilen abgleichen.

Hauptpunkt:

"Slot0:"	**Prüfungen**
ASA	Äußeres IP
Snort	Interne IP
FTD	Äußeres (Prefilter) + Inneres IP (Zugriffskontrollrichtlinie (ACP))

Anwendungsfall 2 der Vorfilterrichtlinie

Eine Prefilter-Richtlinie kann einen Prefilter-Regeltyp verwenden, der eine frühe Zugriffskontrolle ermöglicht und einen Fluss vollständig an der Snort-Engine vorbeileitet, wie im Bild dargestellt.



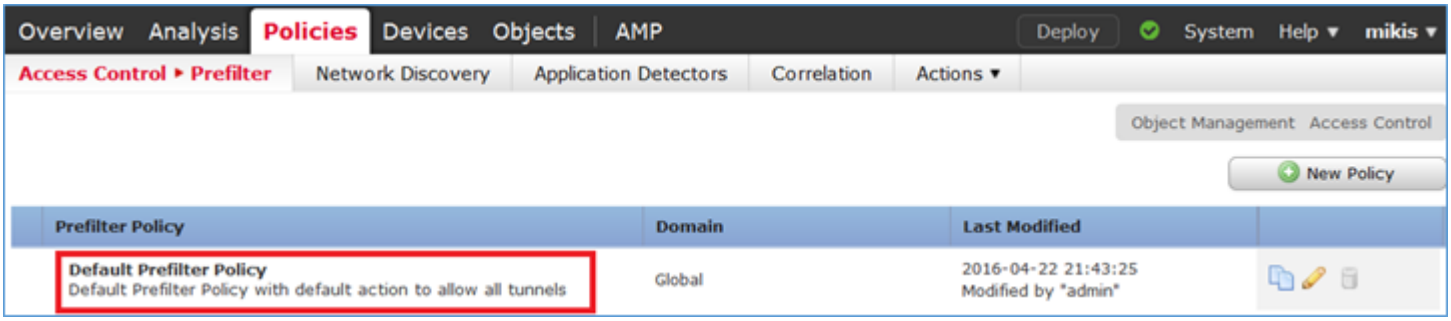
Aufgabe 1: Standard-Vorfilterrichtlinie überprüfen

Voraussetzung für diese Aufgabe:

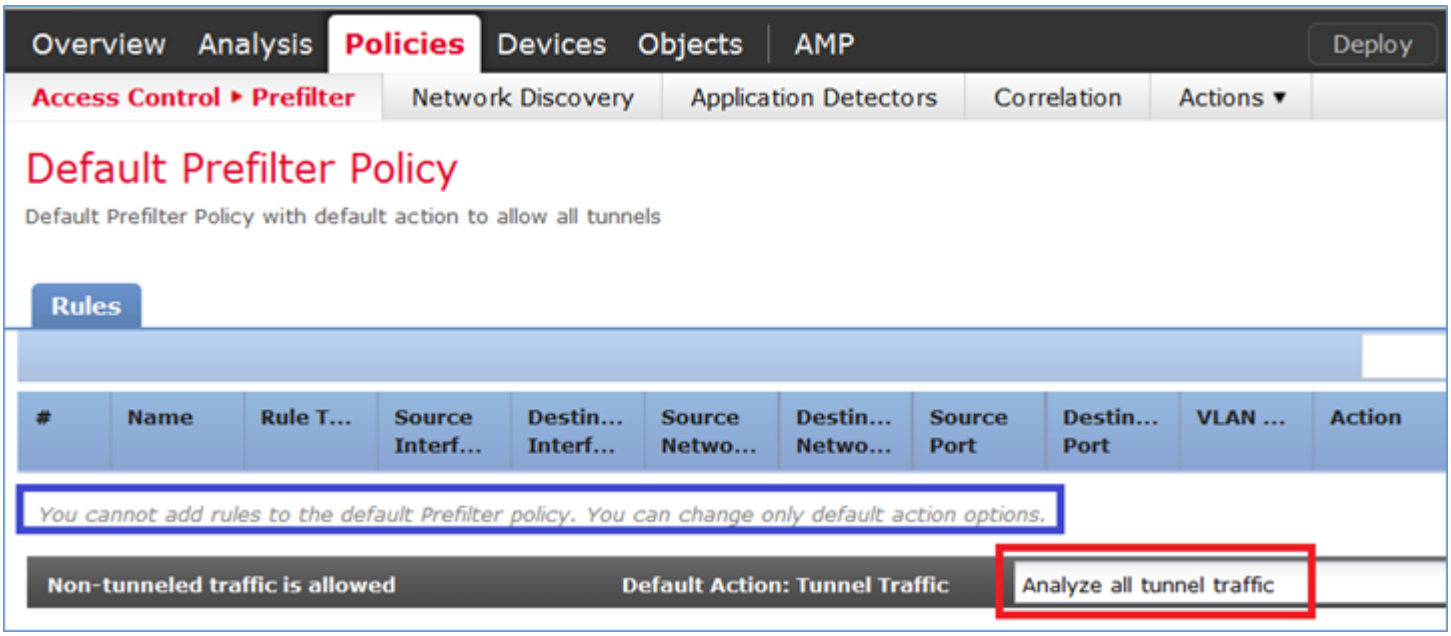
Überprüfen der standardmäßigen Vorfilterrichtlinie

Lösung:

Schritt 1: Navigieren Sie zu **Richtlinien > Zugriffskontrolle > Vorfilter**. Es ist bereits eine Standardvorfilterrichtlinie vorhanden, wie im Bild dargestellt.



Schritt 2: Wählen Sie **Bearbeiten**, um die Richtlinieneinstellungen wie im Bild dargestellt anzuzeigen.



Schritt 3: Die Vorfilterrichtlinie ist bereits der Zugriffskontrollrichtlinie angefügt, wie im Bild gezeigt.

CLI (LINA)-Überprüfung

Vorfilterregeln werden zusätzlich zu den ACLs hinzugefügt:

<#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
```

Aufgabe 2: Getunnelten Verkehr mit Tag blockieren

Voraussetzung für diese Aufgabe:

Blockieren von ICMP-Datenverkehr, der innerhalb des GRE-Tunnels getunnelt wird

Lösung:

Schritt 1: Wenn Sie diese ACPs anwenden, können Sie sehen, dass Internet Control Message Protocol (ICMP)-Datenverkehr blockiert ist, egal ob er den GRE-Tunnel durchquert oder nicht, wie im Bild gezeigt.

<#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)
```

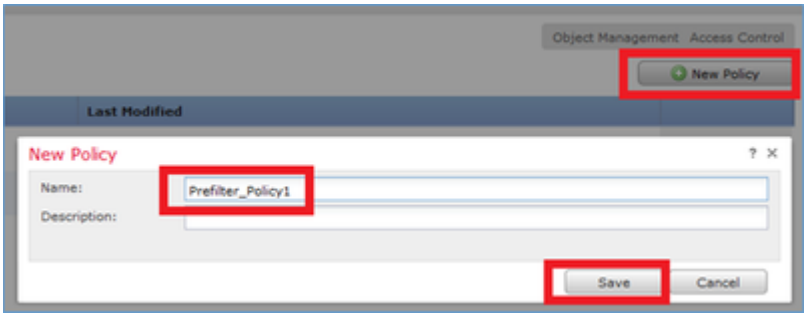
In diesem Fall können Sie eine Vorfilterrichtlinie verwenden, um die Aufgabenanforderung zu erfüllen. Die Logik ist wie folgt:

1. Sie kennzeichnen alle Pakete, die in GRE gekapselt sind.
2. Sie erstellen eine Zugriffskontrollrichtlinie, die mit den gekennzeichneten Paketen übereinstimmt und ICMP blockiert.

Aus architektonischer Sicht werden die Pakete mit den LINA-Vorfilterregeln (LInux NAtively), dann mit den Snort-Vorfilterregeln und ACP verglichen, und schließlich weist Snort LINA an, das Paket zu löschen. Das erste Paket durchläuft das FTD-Gerät.

Schritt 1: Definieren eines Tags für getunnelten Datenverkehr.

Navigieren Sie zu **Policies > Access Control > Prefilter (Richtlinien > Zugriffskontrolle > Prefilter),** und erstellen Sie eine neue Prefilter Policy (Vorfilterrichtlinie). Beachten Sie, dass die Standardvorfilterrichtlinie nicht wie im Bild dargestellt bearbeitet werden kann.

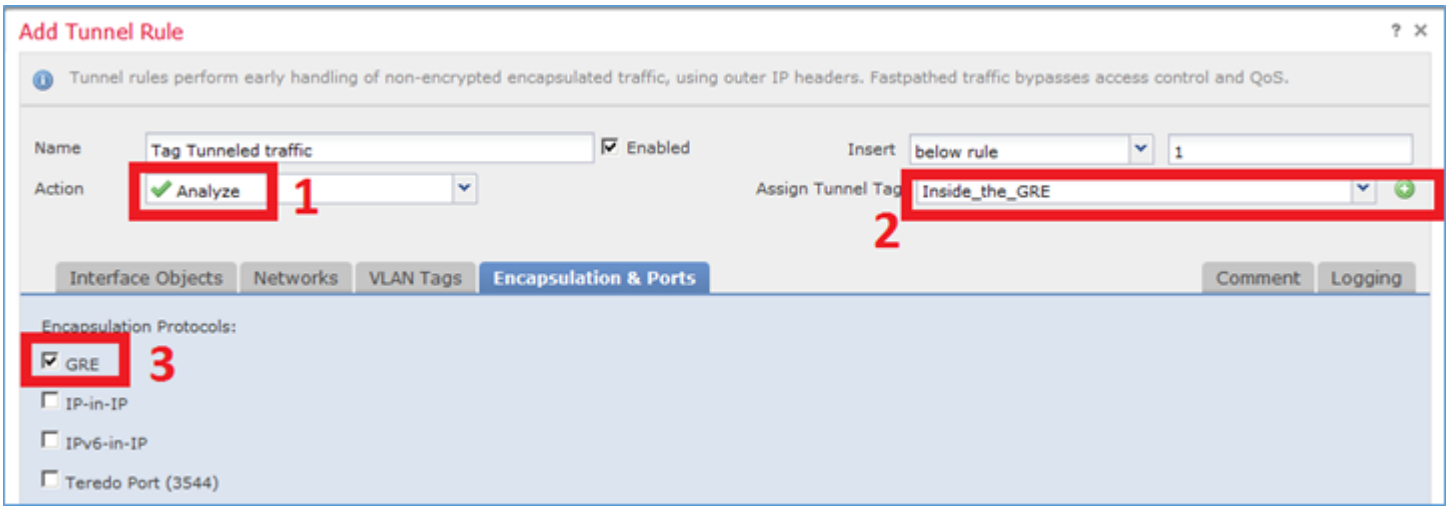


Innerhalb der Vorfilterrichtlinie können Sie zwei Regeltypen definieren:

1. Tunnelregel
2. Vorfilterregel

Sie können sich diese beiden als völlig unterschiedliche Funktionen vorstellen, die in einer Vorfilterrichtlinie konfiguriert werden können.

Für diese Aufgabe ist es notwendig, eine Tunnelregel zu definieren, wie im Bild dargestellt.

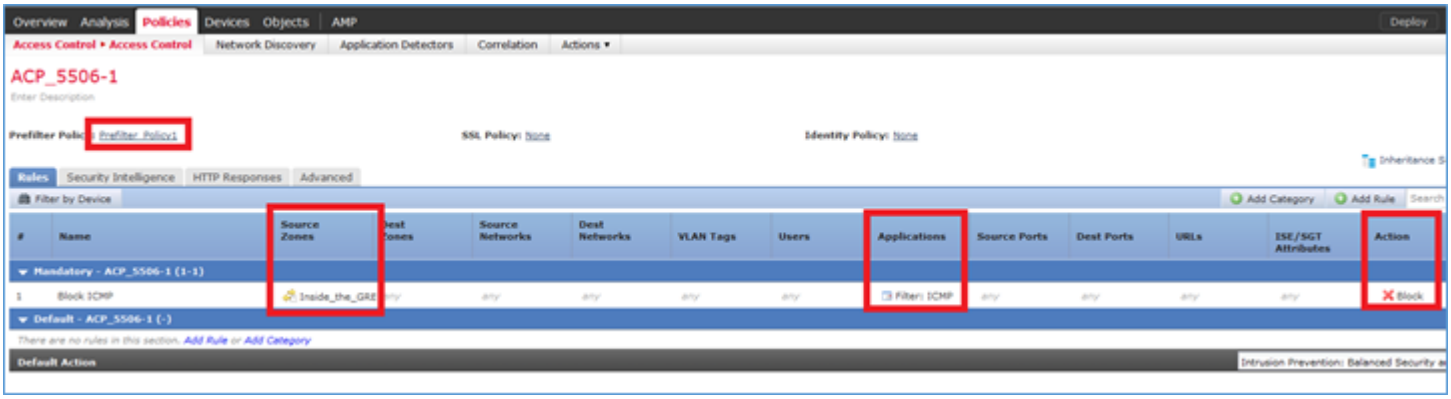


Zu den Maßnahmen:

Aktion	**Beschreibung**
Analysieren	Nach LINA wird der Fluss von der Snort Engine überprüft. Optional kann dem getunnelten Datenverkehr ein Tunnel-Tag zugewiesen werden.
Blockieren	Der Fluss wird durch LINA blockiert. Der äußere Header ist zu prüfen.
FastPath	Der Fluss wird nur von LINA verwaltet, ohne dass die Snort-Engine aktiviert werden muss.

Schritt 2: Definieren der Zugriffskontrollrichtlinie für den getaggten Datenverkehr

Obwohl es zunächst nicht sehr intuitiv sein kann, kann das Tunnel-Tag von einer Zugriffskontrollrichtlinienregel als Quellzone verwendet werden. Navigieren Sie zu **Policies > Access Control (Richtlinien > Zugriffskontrolle),** und erstellen Sie eine Regel, die ICMP für den getaggten Datenverkehr blockiert, wie im Bild dargestellt.



Hinweis: Die neue Vorfilterrichtlinie ist der Zugriffskontrollrichtlinie angefügt.

Überprüfen:

Aktivieren Sie die Erfassung für LINA und 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
```

Versuchen Sie, von R1 aus einen Ping an den entfernten GRE-Tunnel-Endpunkt zu senden. Der Ping schlägt fehl:

```
<#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)
```

Die CLISH-Erfassung zeigt, dass die erste Echo-Anfrage über FTD gesendet wurde und die Antwort blockiert wurde:

```
<#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 r

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 r
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 r
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 r
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 r
```

Die LINA-Aufzeichnung bestätigt dies:

```
<#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
```

Aktivieren Sie CLISH firewall-engine-debug, deaktivieren Sie LINA ASP-Ablagerungsindikatoren, und führen Sie den gleichen Test durch. Das CLISH-Debugging zeigt, dass Sie für die Echo-Anforderung die Vorfilterregel und für die Echo-Reply die ACP-Regel zugeordnet haben:

```
<#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, g

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, g

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-Dropdown zeigt, dass Snort die Pakete verworfen hat:

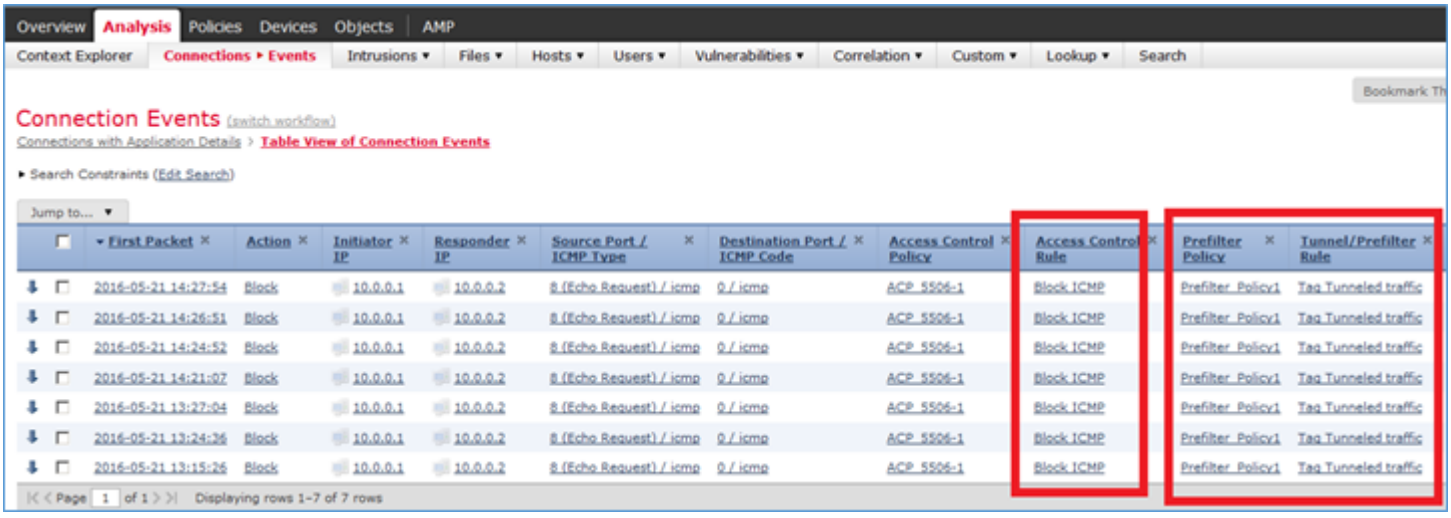
<#root>

>

show asp drop

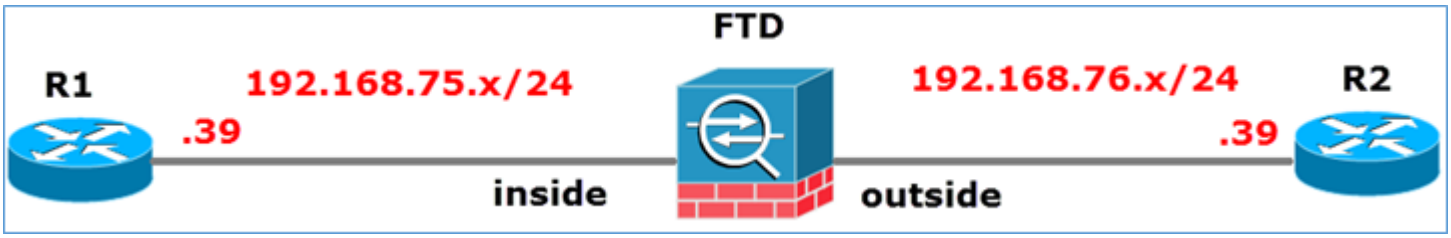
```
Frame drop:
  No route to host (no-route)                                  366
  Reverse-path verify failed (rpf-violated)                      2
  Flow is denied by configured rule (acl-drop)                   2

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

Unter Connection Events (Verbindungsereignisse) können Sie die Prefilter Policy (Vorfilterrichtlinie) und Rule (Regel) sehen, die Sie wie im Bild dargestellt zugeordnet haben.



Aufgabe 3: Snort Engine mit Fastpath-Vorfilterregeln umgehen

Netzwerkdiagramm

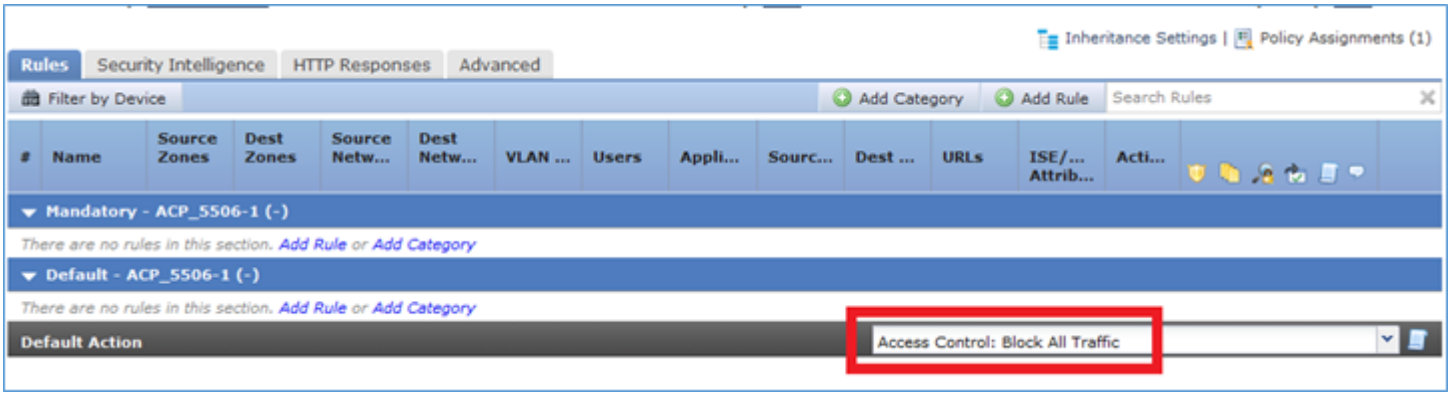


Voraussetzung für diese Aufgabe:

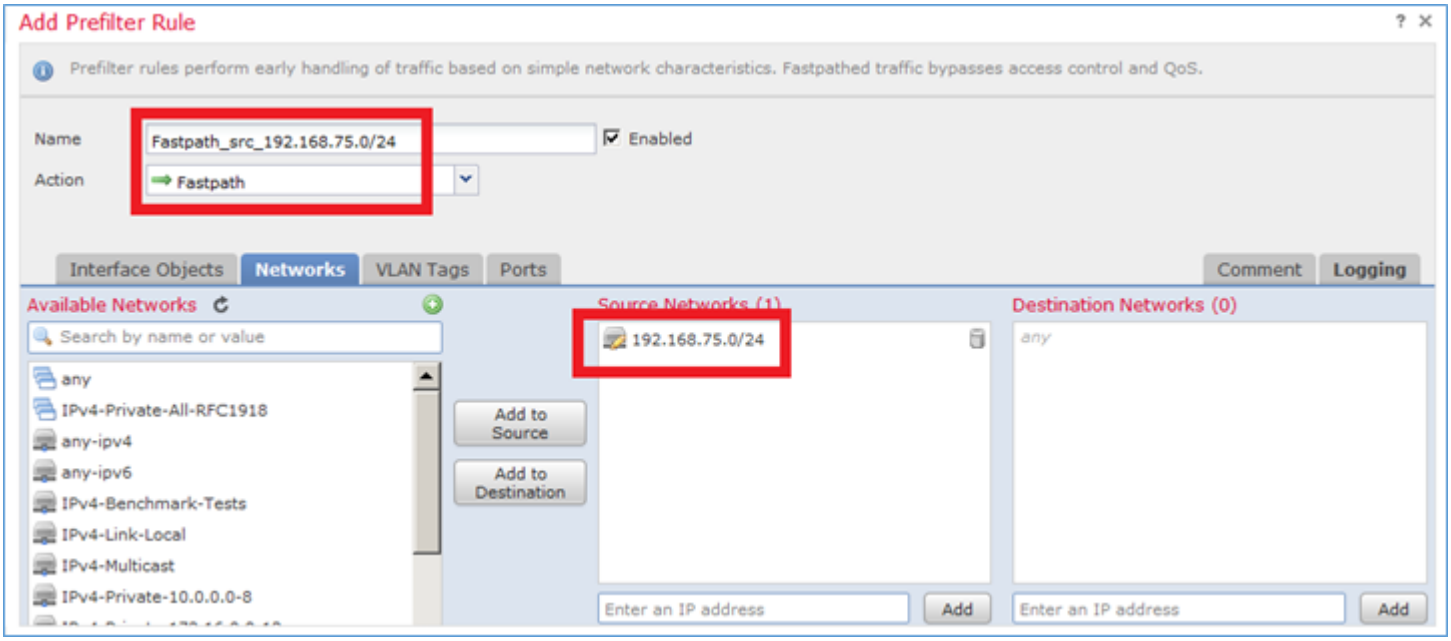
1. Entfernen Sie die aktuellen Richtlinien für die Zugriffskontrolle, und fügen Sie eine Regel für die Zugriffskontrollrichtlinie hinzu, die den gesamten Datenverkehr blockiert.
2. Konfigurieren Sie eine Vorfilterrichtlinienregel, die die Snort Engine für Datenverkehr umgeht, der aus dem Netzwerk 192.168.75.0/24 stammt.

Lösung:

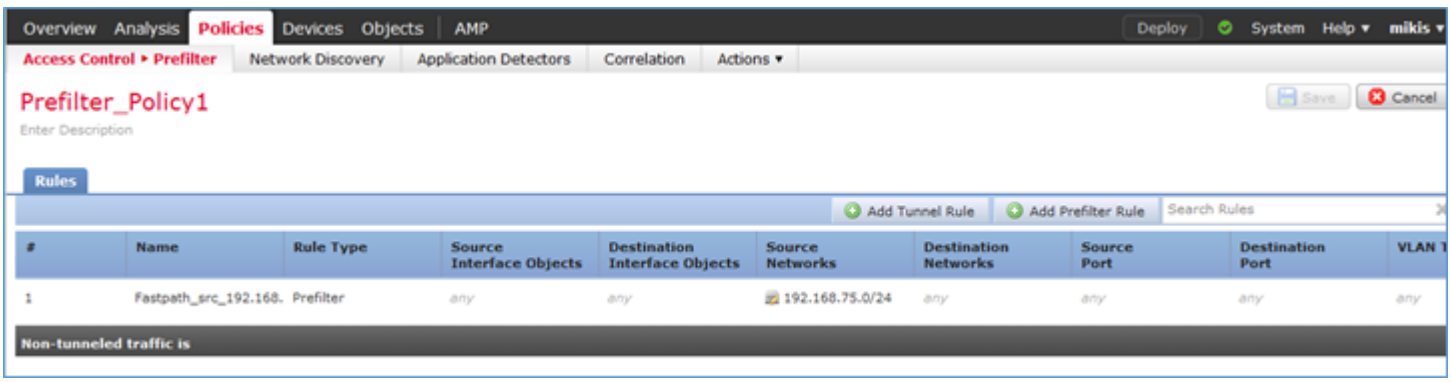
Schritt 1: Die Zugriffskontrollrichtlinie, die den gesamten Datenverkehr blockiert, ist im Bild dargestellt.



Schritt 2: Fügen Sie eine Vorfilterregel mit Fastpath als Aktion für das Quellnetzwerk 192.168.75.0/24 hinzu, wie im Bild gezeigt.



Schritt 3: Das Ergebnis ist wie im Bild dargestellt.



Schritt 4: **Speichern** und **Bereitstellen**.

Aktivieren Sie die Erfassung mit Ablaufverfolgung auf beiden FTD-Schnittstellen:

<#root>

```
firepower#
capture CAPI int inside trace match icmp any any
firepower#
capture CAPO int outsid trace match icmp any any
```

Versuchen Sie, einen Ping von R1 (192.168.75.39) an R2 (192.168.76.39) über die FTD zu senden. Ping schlägt fehl:

<#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)
```

Die Erfassung auf der internen Schnittstelle zeigt Folgendes:

<#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
```

Nachverfolgung des ersten Pakets (Echoanfrage) zeigt an (wichtige Punkte hervorgehoben):

Spoiler (Zum Lesen markieren)

firepower# show capture CAPI-Paketnummer 1 trace

5 erfasste Pakete

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

Phase: 1

Typ: CAPTURE

Untertyp:

Ergebnis: ZULÄSSIG

Konfiguration:

Zusätzliche Informationen:

MAC-Zugriffsliste

Phase: 2

Typ: ACCESS-LIST

Untertyp:

Ergebnis: ZULÄSSIG

Konfiguration:

Implizite Regel

Zusätzliche Informationen:

MAC-Zugriffsliste

Phase 3:

Typ: ROUTENSUCHE

Subtyp: Ausgangsschnittstelle auflösen

Ergebnis: ZULÄSSIG

Konfiguration:

Zusätzliche Informationen:

found next-hop 192.168.76.39 nutzt Ausgangs-IFC außen

Phase: 4

Typ: ACCESS-LIST

Untertyp: log

Ergebnis: ZULÄSSIG

Konfiguration:

Zugriffsgruppe CSM_FW_ACL_ global

access-list CSM_FW_ACL_ advanced trust ip 192.168.75.0 255.255.0 any rule-id 268434448 event-log both

Zugriffsliste CSM_FW_ACL_ Anmerkung Regel-ID 268434448: VORFILTERRICHTLINIE: Prefilter_Policy1

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

Zusätzliche Informationen:

Phase: 5

Typ: CONN-SETTINGS

Untertyp:

Ergebnis: ZULÄSSIG

Konfiguration:

class-map class-default

 mit allen

Richtlinienzuordnung global_policy

 class class-default

  Verbindung festlegen erweiterte Optionen UM_STATIC_TCP_MAP

service-policy global

Zusätzliche Informationen:

Phase: 6

Typ: NAT

Untertyp: pro Sitzung

Ergebnis: ZULÄSSIG

Konfiguration:

Zusätzliche Informationen:

Phase: 7

Typ: IP-OPTIONEN

Untertyp:

Ergebnis: ZULÄSSIG

Konfiguration:

Zusätzliche Informationen:

Phase: 8

Typ: INSPECT

Untertyp: np-inspect

Ergebnis: ZULÄSSIG

Konfiguration:

class-map inspection_default

Übereinstimmung mit Standard-Prüfdatenverkehr

Richtlinienzuordnung global_policy

Klassenprüfung_default

ICMP überprüfen

service-policy global

Zusätzliche Informationen:

Phase: 9

Typ: INSPECT

Untertyp: np-inspect

Ergebnis: ZULÄSSIG

Konfiguration:

Zusätzliche Informationen:

Phase: 10

Typ: NAT

Untertyp: pro Sitzung

Ergebnis: ZULÄSSIG

Konfiguration:

Zusätzliche Informationen:

Phase: 11

Typ: IP-OPTIONEN

Untertyp:

Ergebnis: ZULÄSSIG

Konfiguration:

Zusätzliche Informationen:

Phase: 12

Typ: FLOW-CREATION

Untertyp:

Ergebnis: ZULÄSSIG

Konfiguration:

Zusätzliche Informationen:

Neuer Datenstrom mit ID 52 erstellt, Paket an nächstes Modul gesendet

Phase: 13

Typ: ACCESS-LIST

Untertyp: log

Ergebnis: ZULÄSSIG

Konfiguration:

Zugriffsgruppe CSM_FW_ACL_ global

access-list CSM_FW_ACL_ advanced trust ip 192.168.75.0 255.255.0 any rule-id 268434448 event-log both

Zugriffsliste CSM_FW_ACL_ Anmerkung Regel-ID 268434448: VORFILTERRICHTLINIE: Prefilter_Policy1

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

Zusätzliche Informationen:

Phase: 14

Typ: CONN-SETTINGS

Untertyp:

Ergebnis: ZULÄSSIG

Konfiguration:

class-map class-default

mit allen

Richtlinienzuordnung global_policy

class class-default

Verbindung festlegen erweiterte Optionen UM_STATIC_TCP_MAP

service-policy global

Zusätzliche Informationen:

Phase: 15

Typ: NAT

Untertyp: pro Sitzung

Ergebnis: ZULÄSSIG

Konfiguration:

Zusätzliche Informationen:

Phase: 16

Typ: IP-OPTIONEN

Untertyp:

Ergebnis: ZULÄSSIG

Konfiguration:

Zusätzliche Informationen:

Phase: 17

Typ: ROUTENSUCHE

Subtyp: Ausgangsschnittstelle auflösen

Ergebnis: ZULÄSSIG

Konfiguration:

Zusätzliche Informationen:

found next-hop 192.168.76.39 nutzt Ausgangs-IFC außen

Phase: 18

Typ: BENACHBARUNG

Subtyp: Next-Hop und Adjacency

Ergebnis: ZULÄSSIG

Konfiguration:

Zusätzliche Informationen:

Adjacency Aktiv

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

Phase: 19

Typ: CAPTURE

Untertyp:

Ergebnis: ZULÄSSIG

Konfiguration:

Zusätzliche Informationen:

MAC-Zugriffsliste

Ergebnis:

Eingabeschnittstelle: außen

Eingabestatus: nach oben

Eingabeleitungsstatus: aktiv

Ausgabeschnittstelle: außen

Ausgabestatus: aktiv

Ausgabeleitungsstatus: aktiv

Aktion: Zulassen

1 Paket abgebildet

Feuerkraft#

firepower# show capture CAPI-Paketnummer 1 trace 5 erfasste Pakete 1: 23:35:07.281738 192.168.75.39 > 192.168.76.39: icmp: echo request Phase: 1 Typ: CAPTURE Subtyp: Ergebnis: ALLOW Konfiguration: Zusätzliche Informationen: MAP C Access list Phase: 2 Typ: ACCESS-LIST Subtyp: Ergebnis: ALLOW Konfig: Implizite Regel Zusätzliche Informationen: MAC Access list Phase: 3 Typ: ROUTE-LOOKUP Subtyp: Resolve Egress Interface Ergebnis: ALLOW Konfig: Zusätzliche Informationen: found next-hop 192.168.76.39 uses egress ifc outside Phase: 4 Typ: ACCESS-LIST Subtyp: Protokoll Ergebnis: ALLOW Konfiguration: Zugriffsgruppe CSM_FW_ACL_ globale Zugriffsliste 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 Weitere Informationen: Phase: 5 Typ: CONN-SETTINGS Subtyp: Ergebnis: ALLOW Konfig: class-map class-default match any policy-map global_DE policy class class-default set connection advanced-options UM_STATIC_TCP_MAP service-policy global_policy global Weitere Informationen: Phase: 6 Typ: NAT Subtyp: pro Sitzung Ergebnis: ALLOW Konfig: Weitere Informationen: Phase: 7 Typ: IP-OPTIONEN Subtyp: Ergebnis: ALLOW Konfig: Weitere Informationen: Phase: 8 Typ: INSPECT Subtyp: np-inspect Ergebnis: ALLOW Konfig.: class-map inspection_default match default-inspection-traffic policy-map global_policy class inspection_default inspect icmp service-policy global Weitere Informationen: Phase: 9 Typ: INSPECT Subtyp: np-inspect Ergebnis: ALLOW Konfig: Weitere Informationen: Phase: 10 Typ: NAT Subtyp: pro Sitzung Ergebnis: ALLOW Konfig: Weitere Informationen: Phase: 11 Typ: IP-OPTIONEN Subtyp: Ergebnis: ALLOW Konfig: Zusätzliche Informationen: Phase: 12 Typ: FLOW-CREATION Subtyp: Ergebnis: ALLOW Konfig: Zusätzliche Informationen: Neuer Fluss mit ID 52 erstellt, Paket an nächstes Modul gesendet Phase: 13 Typ: ACCESS-LIST Subtyp: log Ergebnis: ALLOW Konfig: access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ advanced trust ip 192.168.75.0 255.255.0 any rule-id 268434448 event-log

both access-list CSM_FW_ACL_ remark rule-id 268434448: PREFILTER POLICY: Prefilter_Policy1 access-list CSM_FW W_ACL_ remark rule-id 268434448: RULE: Fastpath_src_192.168.75.0/24 Weitere Informationen: Phase: 14 Typ: CONN-SETTINGS Subtyp: Ergebnis: ALLOW Konfiguration: 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 Weitere Informationen: Phase: 15 Typ: NAT Subtyp: pro Sitzung Ergebnis: ZULASSEN Konfig: Zusätzliche Informationen: Phase: 16 Typ: IP-OPTIONEN Subtyp: Ergebnis: ZULASSEN Konfig: Zusätzliche Informationen: Phase: 17 Typ: ROUTE-LOOKUP Subtyp: Auflösen Ausgangsschnittstelle Ergebnis: ZULASSEN Konfig: Zusätzliche Informationen: next-hop 192.16 gefunden 8.76.39 benutzt Egress-IFC außerhalb Phase: 18 Typ: ADJACENCY-LOOKUP Subtyp: next-hop und Adjacency Ergebnis: ALLOW Konfig: Zusätzliche Informationen: Adjacency Aktiv Next-hop mac address 0004.deab.681b hits 140372416161507 Phase: 19 Typ: CAPTURE Subtyp: Ergebnis: ALT LOW Config: Additional Information: MAC Access list Ergebnis: Eingabeschnittstelle: außerhalb Eingabestatus: oben Eingabeleitungsstatus: oben Ausgabeschnittstelle: außerhalb Ausgabestatus: oben Ausgabeleitungsstatus: oben Aktion: 1 Paket anzeigen firepower#

Die Erfassung auf der externen Schnittstelle zeigt Folgendes:

<#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
```

Die Ablaufverfolgung des Rückgabepakets zeigt, dass es mit dem aktuellen Fluss übereinstimmt (52), aber von der ACL blockiert wird:

<#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

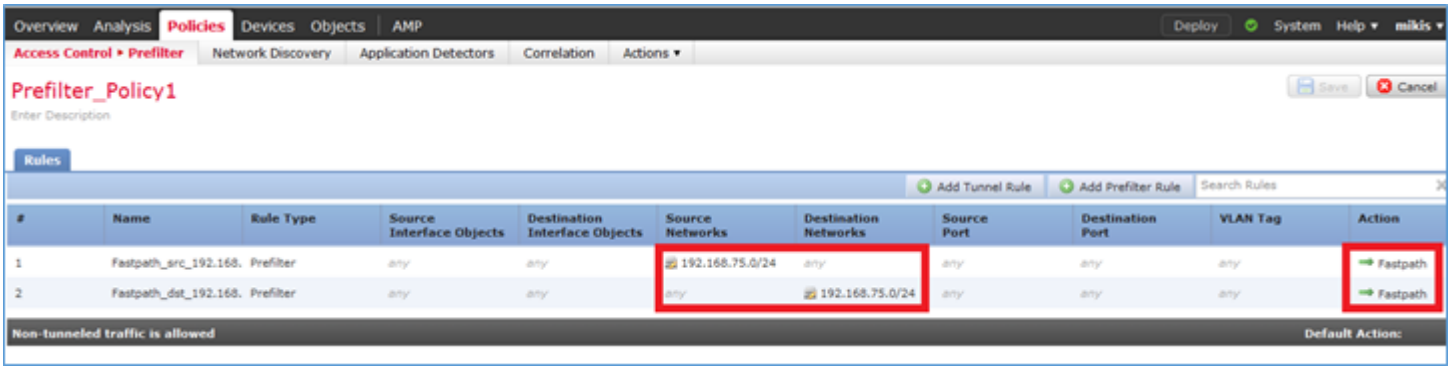
```
Subtype: log
```

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

Schritt 5: Fügen Sie eine weitere Vorfilterregel für den zurückkehrenden Datenverkehr hinzu. Das Ergebnis ist wie im Bild dargestellt.



Verfolgen Sie jetzt das angezeigte Rücksendepaket (wichtige Punkte hervorgehoben):

Spoiler (Zum Lesen markieren)

firepower# show capture CAPO-Paketnummer 2 trace

10 Pakete erfasst

2: 00:01:38.873123 192.168.76.39 > 192.168.75.39: icmp: echo reply

Phase: 1

Typ: CAPTURE

Untertyp:

Ergebnis: ZULÄSSIG

Konfiguration:

Zusätzliche Informationen:

MAC-Zugriffsliste

Phase: 2

Typ: ACCESS-LIST

Untertyp:

Ergebnis: ZULÄSSIG

Konfiguration:

Implizite Regel

Zusätzliche Informationen:

MAC-Zugriffsliste

Phase 3:

Typ: FLUSSSUCHE

Untertyp:

Ergebnis: ZULÄSSIG

Konfiguration:

Zusätzliche Informationen:

Fluss mit ID 62 gefunden, verwendet den aktuellen Fluss

Phase: 4

Typ: ACCESS-LIST

Untertyp: log

Ergebnis: ZULÄSSIG

Konfiguration:

Zugriffsgruppe CSM_FW_ACL_ global

access-list CSM_FW_ACL_ advanced trust ip any 192.168.75.0 255.255.0 rule-id 268434450 event-log both

Zugriffsliste CSM_FW_ACL_ Anmerkung Regel-ID 268434450: VORFILTERRICHTLINIE: Prefilter_Policy1

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

Zusätzliche Informationen:

Phase: 5

Typ: CONN-SETTINGS

Untertyp:

Ergebnis: ZULÄSSIG

Konfiguration:

class-map class-default

mit allen

Richtlinienzuordnung global_policy

class class-default

Verbindung festlegen erweiterte Optionen UM_STATIC_TCP_MAP

service-policy global

Zusätzliche Informationen:

Phase: 6

Typ: NAT

Untertyp: pro Sitzung

Ergebnis: ZULÄSSIG

Konfiguration:

Zusätzliche Informationen:

Phase: 7

Typ: IP-OPTIONEN

Untertyp:

Ergebnis: ZULÄSSIG

Konfiguration:

Zusätzliche Informationen:

Phase: 8

Typ: ROUTENSUCHE

Subtyp: Ausgangsschnittstelle auflösen

Ergebnis: ZULÄSSIG

Konfiguration:

Zusätzliche Informationen:

found next-hop 192.168.75.39 uses egress ifc inside

Phase: 9

Typ: BENACHBARUNG

Subtyp: Next-Hop und Adjacency

Ergebnis: ZULÄSSIG

Konfiguration:

Zusätzliche Informationen:

Adjacency Aktiv

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

Phase: 10

Typ: CAPTURE

Untertyp:

Ergebnis: ZULÄSSIG

Konfiguration:

Zusätzliche Informationen:

MAC-Zugriffsliste

Ergebnis:

Eingabeschnittstelle: innen

Eingabestatus: nach oben

Eingabeleitungsstatus: aktiv

Ausgabeschnittstelle: innen

Ausgabestatus: aktiv

Ausgabeleitungsstatus: aktiv

Aktion: Zulassen

firepower# show capture CAPO-Paketnummer 2 trace 10 erfasste Pakete 2: 00:01:38.873123 192.168.76.39 > 192.168.75.39: icmp: echo reply Phase: 1 Typ: CAPTURE Subtyp: Ergebnis: ALLOW Konfiguration: Zusätzliche Informationen: MAC-Zugriffsliste Phase: 2 Typ: ACCESS-LIST Subtyp: Ergebnis: ZULASSEN Konfig: Implizite Regel Zusätzliche Informationen: MAC-Zugriffsliste Phase: 3 Typ: FLOW-LOOKUP Subtyp: Ergebnis: ZULASSEN Konfig: Zusätzliche Informationen: Gefundener Fluss mit ID 62, verwendet aktuellen Fluss Phase: 4 Typ: ACCESS-LIST Subtyp: Protokoll Ergebnis: ZULASSEN Konfig : 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 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 Weitere Informationen: Phase: 5 Typ: CONN-SETTINGS Subtyp: Ergebnis: ALLOW Konfiguration: class-map class-default match any policy-map global_policy class-default set connection advanced-options UM_STATIC_TCP_MAP service global_policy global Zusätzliche Informationen: Phase: 6 Typ: NAT Subtyp: pro Sitzung Ergebnis: ALLOW Konfig: Zusätzliche Informationen: Phase: 7 Typ: IP-OPTIONEN Subtyp: Ergebnis: ALLOW Konfig: Zusätzliche Informationen: Phase: 8 Typ: ROUTE-LOOKUP Subtyp: Resolve Egress Interface Ergebnis: ALLOW Konfig: Zusätzliche Informationen: found next-hop 192.0 168.75.39 benutzt Egress-IFC innerhalb Phase: 9 Typ: ADJACENCY-LOOKUP Subtyp: next-hop und adjacency Ergebnis: ALLOW Konfig: Zusätzliche Informationen: adjacency Aktive next-hop mac address c84c.758d.4981 hits 140376711128802 Phase: 10 Typ: CAPTURE Subtyp Typ: Ergebnis: ZULASSEN Konfig: Zusätzliche Informationen: MAC-Zugriffsliste Ergebnis: Eingabe-Schnittstelle: Innen Eingabe-Status: Oben Eingabe-Leitungsstatus: Oben Ausgabe-Schnittstelle: Innen Ausgabe-Status: Oben Ausgabe-Leitungsstatus: Oben Aktion: Zulassen

Überprüfung

Verwenden Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Die Verifizierung wurde in den jeweiligen Aufgabenabschnitten erläutert.

Fehlerbehebung

Es sind derzeit keine spezifischen Informationen zur Fehlerbehebung für diese Konfiguration verfügbar.

Zugehörige Informationen

- Alle Versionen des Konfigurationsleitfadens für das Cisco FirePOWER Management Center finden Sie hier:

Navigieren in der Cisco Secure Firewall Threat Defense-Dokumentation

- Das Cisco Global Technical Assistance Center (TAC) empfiehlt dringend diese visuelle Anleitung, um detailliertes praktisches Wissen über die Cisco FirePOWER Sicherheitstechnologien der nächsten Generation zu erlangen, einschließlich der in diesem Artikel erwähnten Technologien:

Cisco Firepower Threat Defense (FTD)

- Für alle TechNotes zu Konfiguration und Fehlerbehebung:

Cisco Secure Firewall Management Center

- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.