Configurazione e funzionamento dei criteri di prefiltro FTD

Sommario

Introduzione

Questo documento descrive la configurazione e il funzionamento dei criteri di prefiltro Firepower Threat Defense (FTD).

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- ASA5506X con codice FTD 6.1.0-195
- Centro di gestione FireSIGHT (FMC) con versione 6.1.0-195
- Due router 3925 Cisco IOS® con immagini 15.2

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Un criterio di prefiltro è una funzione introdotta nella versione 6.1 e serve a tre scopi principali:

1. Trova la corrispondenza del traffico in base alle intestazioni sia interne che esterne
2. Fornire un controllo dell'accesso anticipato che consente a un flusso di ignorare completamente il motore Snort
3. Fungere da segnaposto per le voci di controllo di accesso (ACE) di cui viene eseguita la migrazione dallo strumento di migrazione Adaptive Security Appliance (ASA).

Configurazione

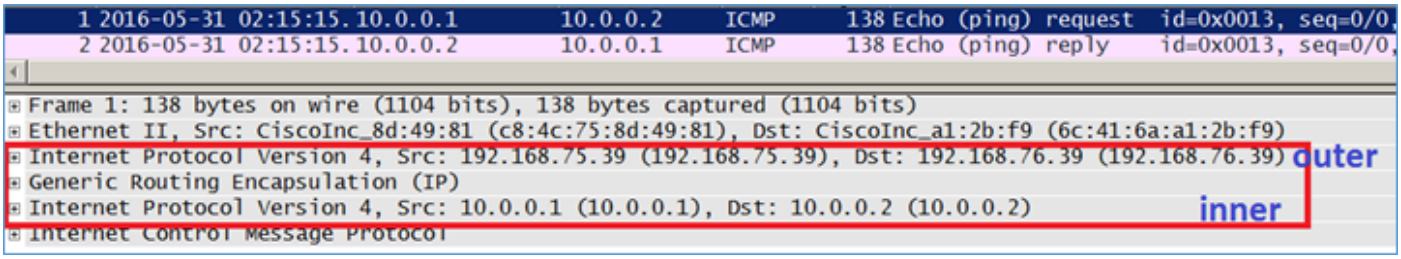
Usa caso 1 criterio di prefiltro

Un criterio di prefiltro può utilizzare un tipo di regola tunnel che consente a FTD di filtrare in base al traffico di tunneling dell'intestazione IP sia all'interno che all'esterno. Al momento in cui è stato scritto questo articolo, il traffico di tunneling si riferisce a:

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

Considerare un tunnel GRE come mostrato nell'immagine.

Quando si esegue il ping da R1 a R2 con l'uso di un tunnel GRE, il traffico attraversa il firewall come mostrato nell'immagine.



Se il firewall è un dispositivo ASA, controlla l'intestazione IP esterna come mostrato nell'immagine.

<#root>

ASA#

show conn

GRE OUTSIDE 192.168.76.39:0 INSIDE 192.168.75.39:0

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

Se il firewall è un dispositivo FirePOWER, controlla l'intestazione IP interna come mostrato nell'immagine.

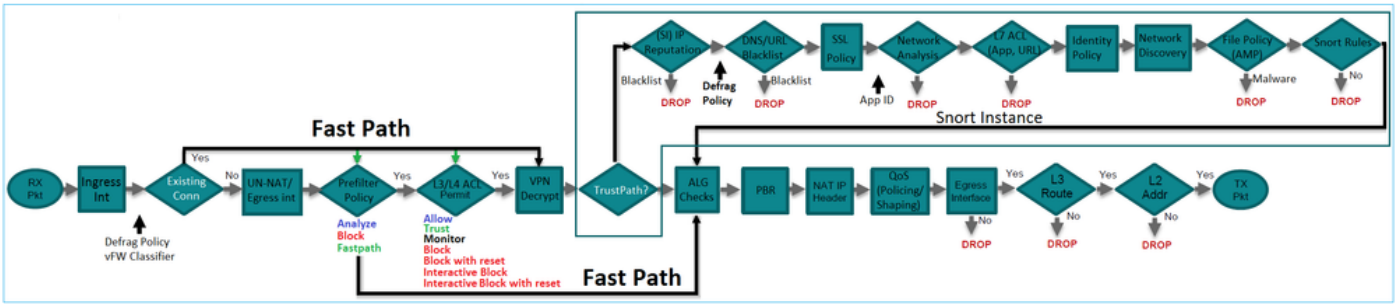
Con i criteri di prefiltro, un dispositivo FTD può abbinare il traffico in base alle intestazioni interne ed esterne.

Punto principale:

Sul dispositivo bootflash o slot0:	Assegni
ASA	IP esterno
Snort	IP interno
FTD	Esterno (prefiltro) + IP interno (criteri di controllo di accesso)

Caso di utilizzo 2 del criterio di pre-filtro

Un criterio di prefiltro può utilizzare un tipo di regola di prefiltro che fornisce un controllo di accesso anticipato e consente a un flusso di ignorare completamente il motore di snort, come mostrato nell'immagine.



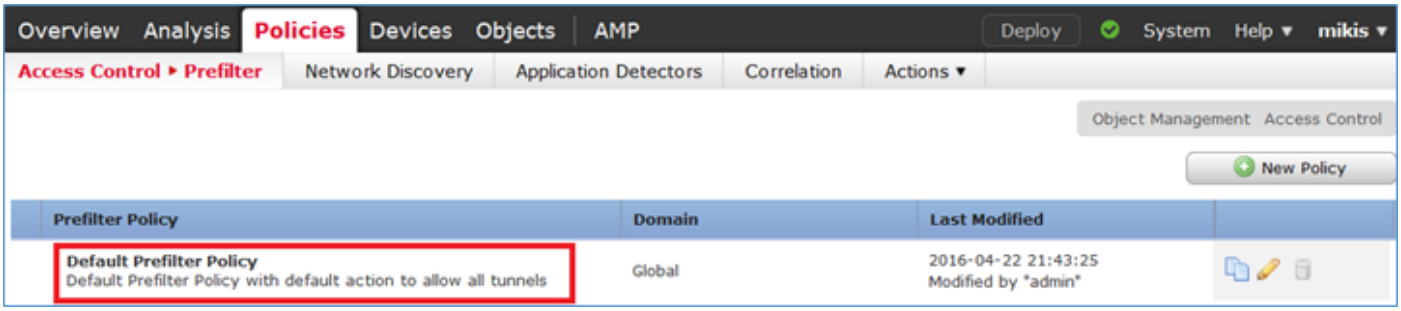
Attività 1. Verifica criterio prefiltro predefinito

Attività richiesta:

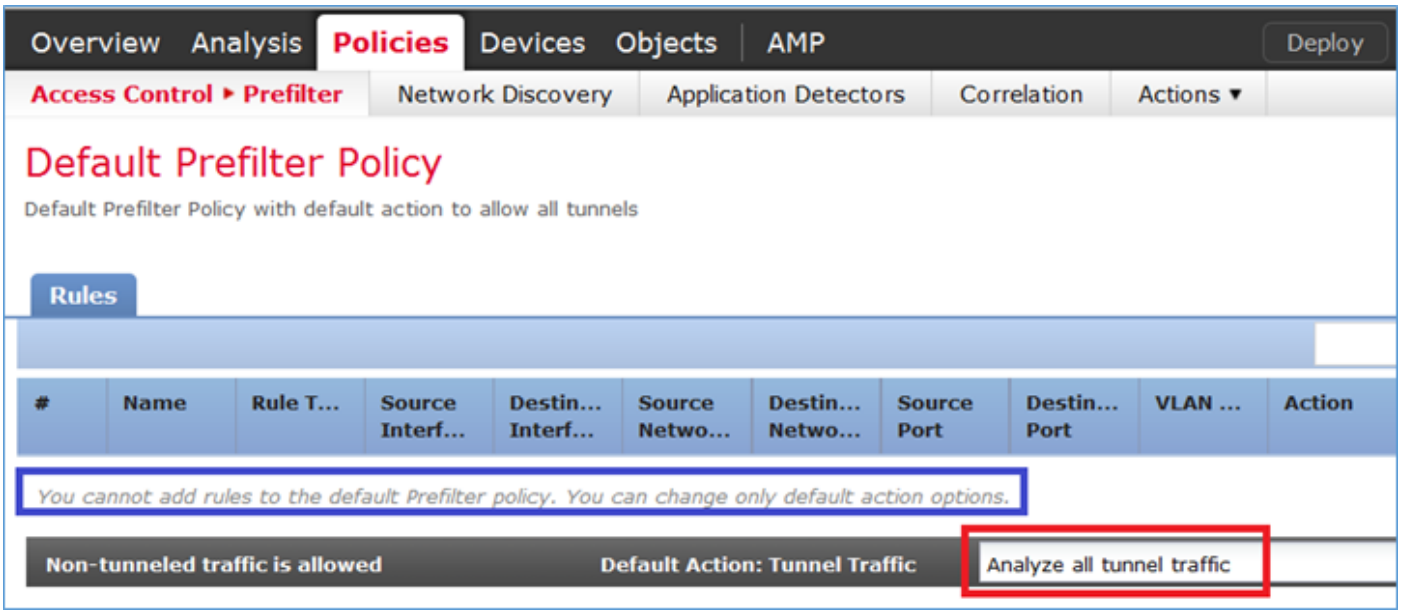
Verificare i criteri di prefiltro predefiniti

Soluzione:

Passaggio 1. Passare a Criteri > Controllo d'accesso > Prefiltro. Esiste già un criterio di prefiltro predefinito, come mostrato nell'immagine.



Passaggio 2. Scegliere Modifica per visualizzare le impostazioni dei criteri come illustrato nell'immagine.



Passaggio 3. Il criterio di prefiltro è già associato al criterio di controllo dell'accesso come mostrato nell'immagine.

Verifica CLI (LINA)

Le regole di prefiltro vengono aggiunte sugli ACL:

<#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
```

Attività 2. Blocca traffico tunneling con tag

Attività richiesta:

Blocca il traffico ICMP tunneling all'interno del tunnel GRE.

Soluzione:

Passaggio 1. Se si applicano questi punti ACP, il traffico ICMP (Internet Control Message Protocol) viene bloccato, a prescindere dal fatto che attraversi o meno il tunnel GRE, come mostrato nell'immagine.

<#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)
```

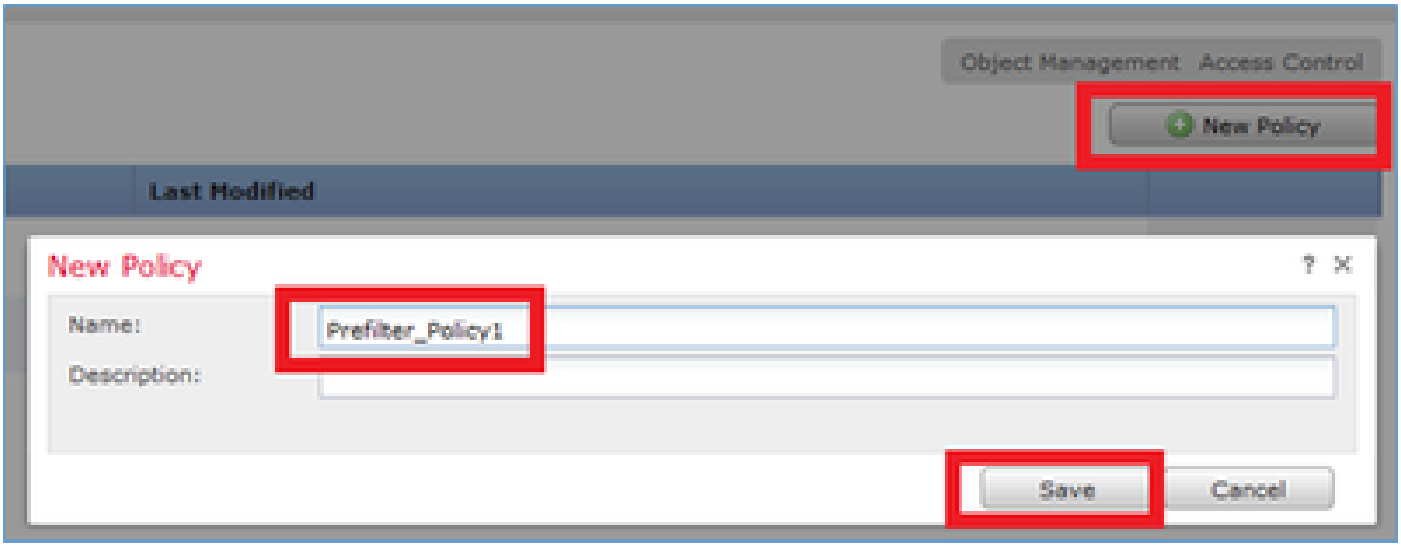
In questo caso, è possibile utilizzare un criterio di prefiltro per soddisfare il requisito dell'attività. La logica è la seguente:

1. È possibile assegnare tag a tutti i pacchetti incapsulati nel GRE.
2. È possibile creare un criterio di controllo dell'accesso che corrisponda ai pacchetti con tag e blocchi l'ICMP.

Dal punto di vista dell'architettura, i pacchetti vengono controllati rispetto alle regole di pre-filtro LINA (Linux NAtively), quindi vengono applicate le regole di pre-filtro Snort e ACP e infine Snort indica a LINA di eliminare. Il primo pacchetto passa attraverso il dispositivo FTD.

Passaggio 1. Definire un tag per il traffico tunneling.

Passare a Criteri > Controllo d'accesso > Prefiltro e creare un nuovo criterio di prefiltro. Tenere presente che il criterio di prefiltro predefinito non può essere modificato come mostrato nell'immagine.

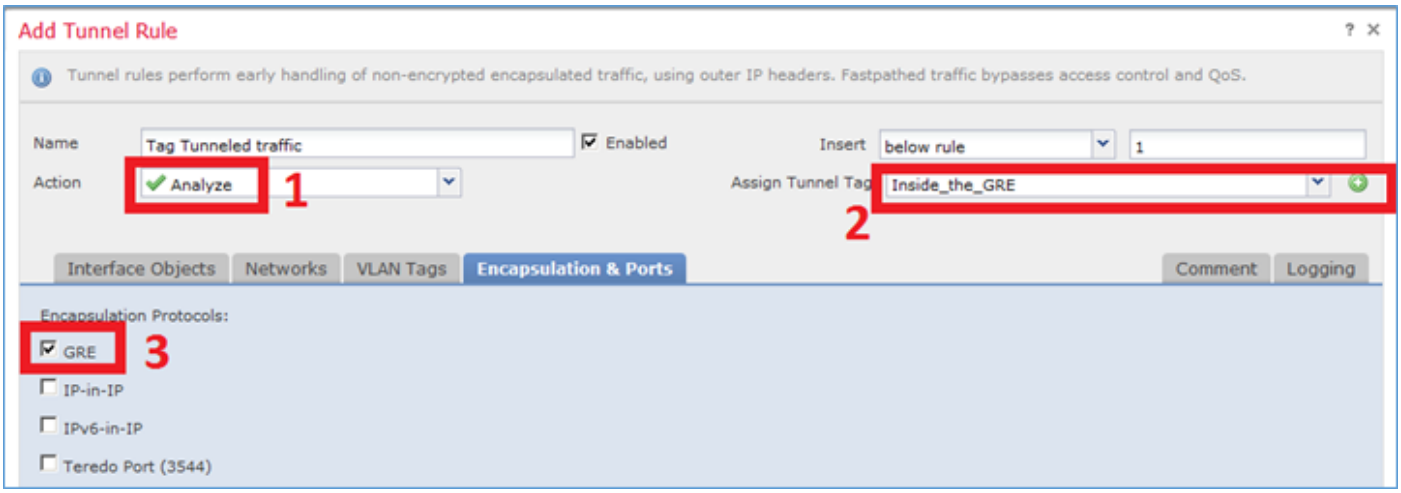


All'interno dei criteri di prefiltro, è possibile definire due tipi di regole:

1. Regola tunnel
2. Regola prefiltro

Queste due funzionalità possono essere configurate in modo completamente diverso in un criterio di prefiltro.

Per questa operazione, è necessario definire una regola di tunnel come mostrato nell'immagine.

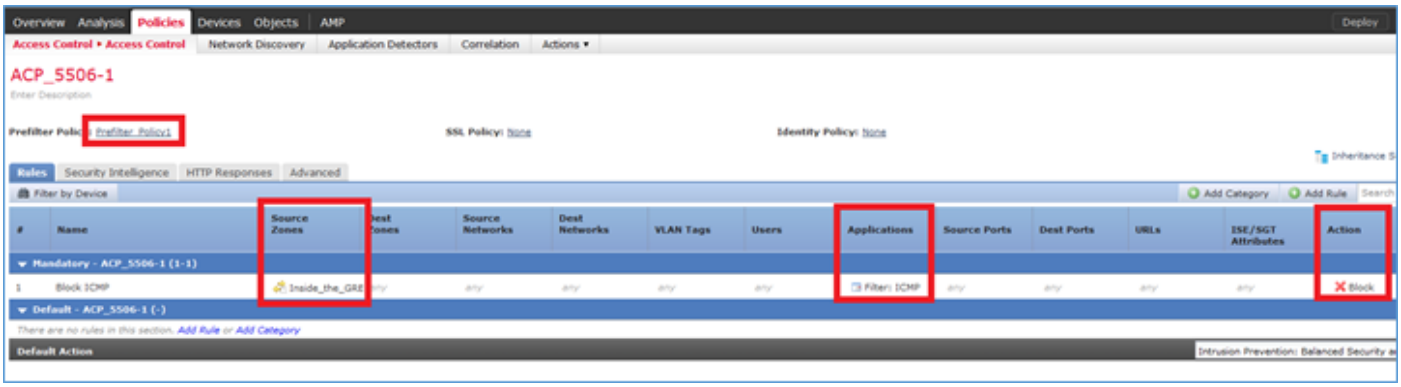


Per quanto riguarda le azioni:

Azione	Descrizione
Analizza	Dopo LINA, il flusso viene controllato dal motore Snort. Facoltativamente, è possibile assegnare un tag tunnel al traffico tunneling.
Block (Blocca)	Il flusso è bloccato da LINA. L'intestazione esterna deve essere controllata.
Percorso rapido	Il flusso viene gestito solo da LINA senza la necessità di inserire il motore Snort.

Passaggio 2. Definire i criteri di controllo di accesso per il traffico con tag.

Anche se inizialmente non può essere molto intuitivo, il tag Tunnel può essere utilizzato da una regola dei criteri di controllo di accesso come zona di origine. Passare a Policy > Controllo di accesso e creare una regola che blocchi l'ICMP per il traffico con tag, come mostrato nell'immagine.



Nota: il nuovo criterio di prefiltro è associato al criterio di controllo dell'accesso.

Verifica:

Abilitare l'acquisizione su LINA e su 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
```

Da R1, provare a eseguire il ping dell'endpoint del tunnel GRE remoto. Il ping ha esito negativo:

<#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)
```

L'acquisizione CLISH mostra che la prima richiesta echo è passata attraverso l'FTD e la risposta è stata bloccata:

<#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
```

La cattura di LINA conferma quanto segue:

```
<#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
```

Abilitare CLISH firewall-engine-debug, cancellare i contatori di rilascio ASP LINA ed eseguire lo stesso test. Il debug CLISH mostra che per la richiesta echo è stata trovata una corrispondenza con la regola di prefiltro e per la regola Echo-Reply è stata trovata la corrispondenza con la regola ACP:

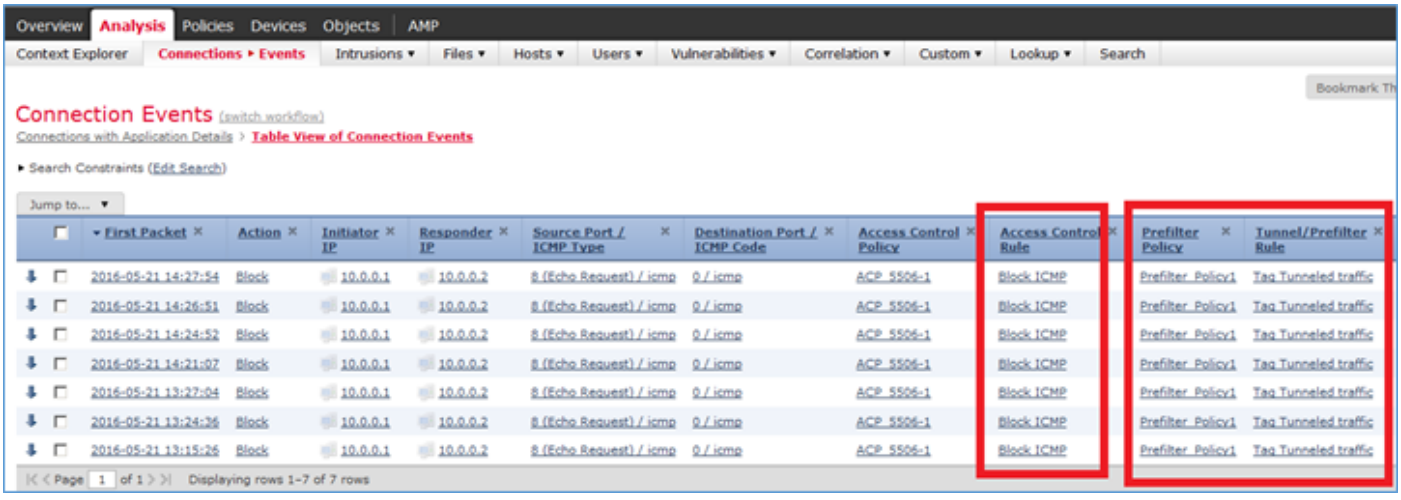
```
<#root>

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
```

Il drop ASP mostra che Snort ha scartato i pacchetti:

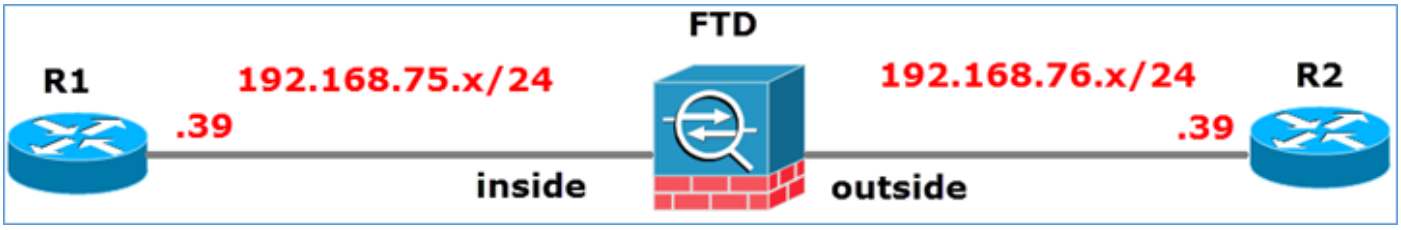
```
<#root>

>

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 Eventi connessione è possibile visualizzare il criterio di filtro e la regola corrispondenti, come illustrato nell'immagine.



Attività 3. Ignora motore di snort con regole di prefiltro Fastpath

Esempio di rete

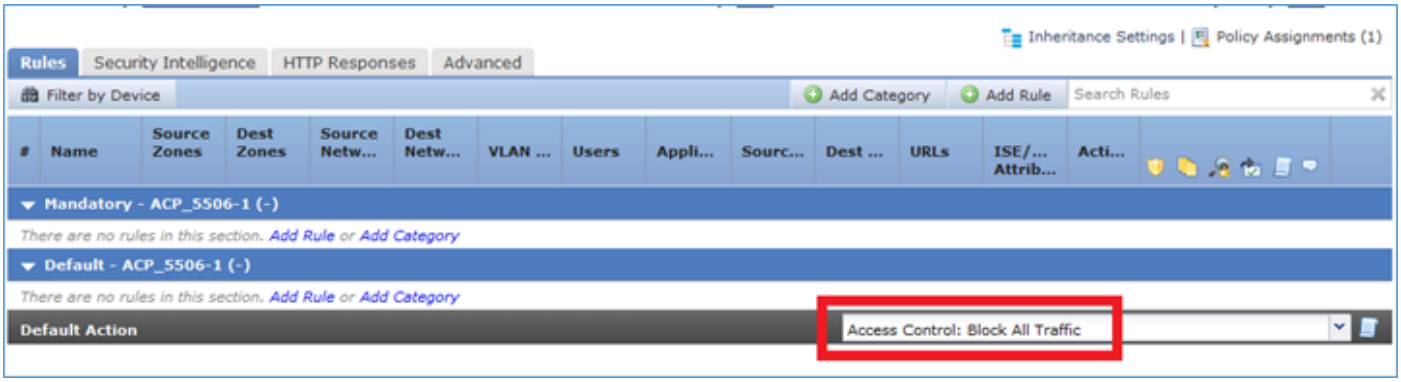


Attività richiesta:

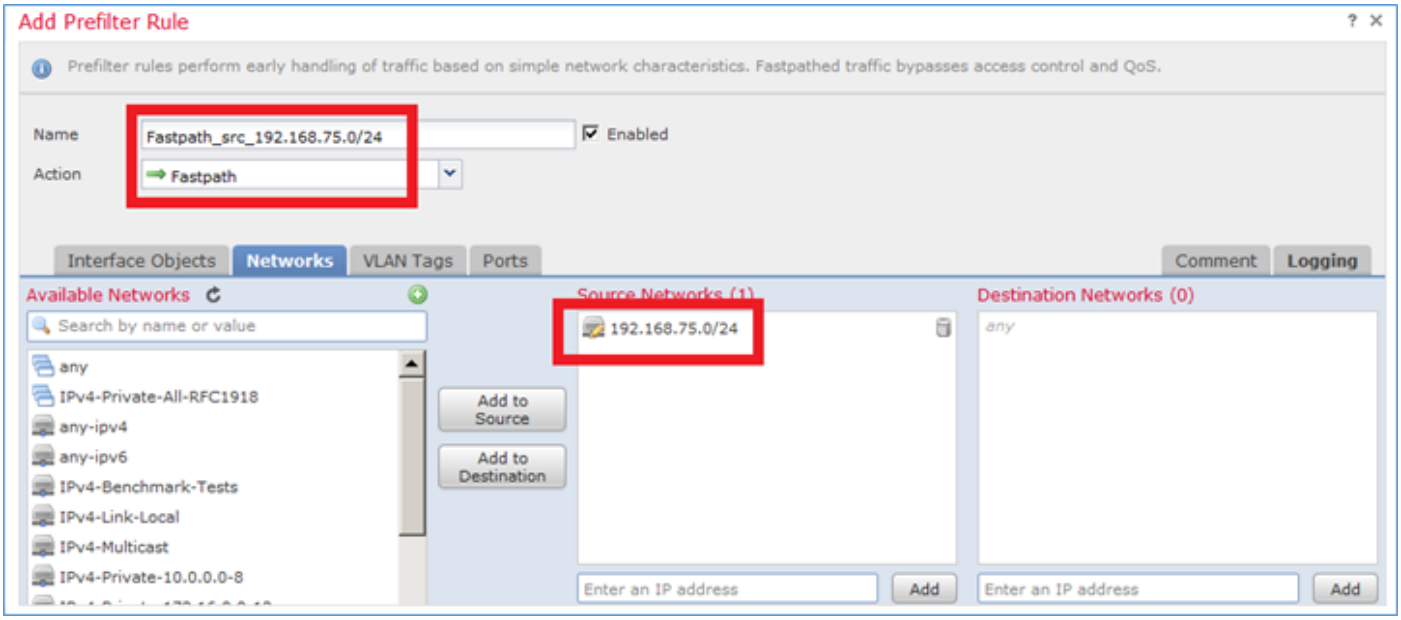
1. Rimuovere le regole dei criteri di controllo di accesso correnti e aggiungere una regola dei criteri di controllo di accesso che blocchi tutto il traffico.
2. Configurare una regola dei criteri di prefiltro che ignori il motore di snort per il traffico proveniente dalla rete 192.168.75.0/24.

Soluzione:

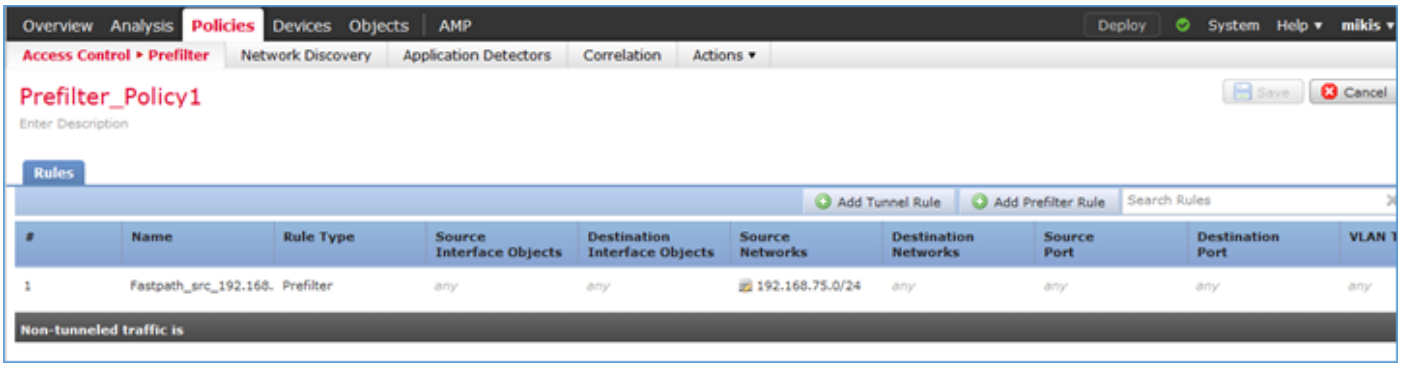
Passaggio 1. I criteri di controllo dell'accesso che bloccano tutto il traffico sono quelli mostrati nell'immagine.



Passaggio 2. Aggiungere una regola di prefiltro con Fastpath come azione per la rete di origine 192.168.75.0/24, come mostrato nell'immagine.



Passaggio 3. Il risultato è quello mostrato nell'immagine.



Passaggio 4. Salvataggio e distribuzione.

Abilita acquisizione con traccia su entrambe le interfacce FTD:

<#root>

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

Provare a eseguire il ping tra R1 (192.168.75.39) e R2 (192.168.76.39) tramite FTD. Ping non riuscito:

<#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)
```

La funzione Capture sull'interfaccia interna mostra:

<#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
```

La traccia del primo pacchetto (richiesta echo) mostra (punti importanti evidenziati):

Spoiler (Evidenziato da leggere)

firepower# show capture CAPI packet-number 1 trace

5 pacchetti acquisiti

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

Fase 1

Tipo: ACQUISIZIONE

Sottotipo:

Risultato: ALLOW

Config:

Ulteriori informazioni:

Elenco accessi MAC

Fase: 2

Tipo: ACCESS-LIST

Sottotipo:

Risultato: ALLOW

Config:

Regola implicita

Ulteriori informazioni:

Elenco accessi MAC

Fase: 3

Tipo: RICERCA ROUTE

Sottotipo: Interfaccia Resolve Egress

Risultato: ALLOW

Config:

Ulteriori informazioni:

found next-hop 192.168.76.39 utilizza ifc in uscita

Fase: 4

Tipo: ACCESS-LIST

Sottotipo: log

Risultato: ALLOW

Config:

access-group CSM_FW_ACL_ globale

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_ note rule-id 268434448: CRITERIO PREFILTRO: Criterio_Prefiltro1

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

Ulteriori informazioni:

Fase: 5

Tipo: CONN-SETTINGS

Sottotipo:

Risultato: ALLOW

Config:

class-map class-default

 qualsiasi

policy-map criteri_globali

 class-default

  imposta connessione opzioni avanzate UM_STATIC_TCP_MAP

criteri-servizio globali_criteri_globali

Ulteriori informazioni:

Fase: 6

Tipo: NAT

Sottotipo: per sessione

Risultato: ALLOW

Config:

Ulteriori informazioni:

Fase: 7

Tipo: OPZIONI IP

Sottotipo:

Risultato: ALLOW

Config:

Ulteriori informazioni:

Fase 8

Tipo: INSPECT

Sottotipo: np-inspect

Risultato: ALLOW

Config:

class-map_inspection_default

 associare traffico-ispezione-predefinito

policy-map criteri_globali

 ispezione classe_default

  ispezionare icmp

criteri-servizio globali_criteri_globali

Ulteriori informazioni:

Fase 9

Tipo: INSPECT

Sottotipo: np-inspect

Risultato: ALLOW

Config:

Ulteriori informazioni:

Fase: 10

Tipo: NAT

Sottotipo: per sessione

Risultato: ALLOW

Config:

Ulteriori informazioni:

Fase: 11

Tipo: OPZIONI IP

Sottotipo:

Risultato: ALLOW

Config:

Ulteriori informazioni:

Fase: 12

Tipo: CREAZIONE FLUSSO

Sottotipo:

Risultato: ALLOW

Config:

Ulteriori informazioni:

Nuovo flusso creato con ID 52, pacchetto inviato al modulo successivo

Fase: 13

Tipo: ACCESS-LIST

Sottotipo: log

Risultato: ALLOW

Config:

access-group CSM_FW_ACL_ globale

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_ note rule-id 268434448: CRITERIO PREFILTRO: Criterio_Prefiltro1

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

Ulteriori informazioni:

Fase: 14

Tipo: CONN-SETTINGS

Sottotipo:

Risultato: ALLOW

Config:

class-map class-default

 qualsiasi

policy-map criteri_globali

 class-default

  imposta connessione opzioni avanzate UM_STATIC_TCP_MAP

criteri-servizio globali_criteri_globali

Ulteriori informazioni:

Fase: 15

Tipo: NAT

Sottotipo: per sessione

Risultato: ALLOW

Config:

Ulteriori informazioni:

Fase: 16

Tipo: OPZIONI IP

Sottotipo:

Risultato: ALLOW

Config:

Ulteriori informazioni:

Fase: 17

Tipo: RICERCA ROUTE

Sottotipo: Interfaccia Resolve Egress

Risultato: ALLOW

Config:

Ulteriori informazioni:

found next-hop 192.168.76.39 utilizza ifc in uscita

Fase: 18

Tipo: ADIACENZA-RICERCA

Sottotipo: next-hop e adiacenza

Risultato: ALLOW

Config:

Ulteriori informazioni:

adiacenza attiva

next-hop indirizzo mac 0004.deab.681b hit 140372416161507

Fase: 19

Tipo: ACQUISIZIONE

Sottotipo:

Risultato: ALLOW

Config:

Ulteriori informazioni:

Elenco accessi MAC

Risultato:

interfaccia di ingresso: esterna

input-status: attivo

stato della linea di ingresso: su

interfaccia di uscita: esterna

stato-output: attivo

output-line-status: attivo

Azione: consenti

1 pacchetto visualizzato

firepower#

firepower# show capture CAPI numero-pacchetto 1 trace 5 pacchetti acquisiti 1: 23:35:07.281738 192.168.75.39 > 192.168.76.39: icmp: richiesta echo Fase: 1 Tipo: Acquisisci Sottotipo: Risultato: ALLOW Config: Informazioni aggiuntive: MAC Access list Fase: 2 Tipo: ACCESS-LIST Sottotipo: Risultato: ALLOW Config: Implicit Rule Informazioni aggiuntive: MAC Access list Fase: 3 Tipo: ROUTE Sottotipo OKUP: Risultato interfaccia di uscita risoluzione: ALLOW Config: Informazioni aggiuntive: trovato hop successivo 192.168.76.39 utilizza ifc in uscita Fase: 4 Tipo: ACCESS-LIST Sottotipo: log Risultato: 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 268434 48 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 Ulteriori informazioni: Phase: 5 Type: CONN-SETTINGS Subtype: Result: ALLOW Config: class-map class-default match any policy-map global_policy class options-default set connection UM_STATIC_TCP_MAP criterio-servizio global_policy global Ulteriori informazioni: Fase: 6 Tipo: NAT Sottotipo: per sessione Risultato: ALLOW Config: Informazioni aggiuntive: Fase: 7 Tipo: IP-OPTIONS Sottotipo: Risultato: ALLOW Config: Informazioni aggiuntive: Fase: 8 Tipo: INSPECT Sottotipo: np-inspect Risultato: ALLOW Config: class-map selection_default-match default-traffic-policy-map classe ispezione_default icmp service-policy global_policy global_policy global Informazioni aggiuntive: Fase: 9 Tipo: INSPECT Sottotipo: np-inspect Risultato: ALLOW Config: Additional Information Fase: 10 Tipo: NAT Sottotipo: per sessione Risultato: ALLOW Configurazione: Informazioni aggiuntive: Fase: 11 Tipo: IP-OPTIONS Sottotipo: Risultato: ALLOW Configurazione: Informazioni aggiuntive: Fase: 12 Tipo: FLOW-CREATION Sottotipo: Risultato: ALLOW Configurazione: Informazioni aggiuntive: Nuovo flusso creato con ID 52, pacchetto inviato al modulo successivo Fase: 13 Tipo: ACCESS-LIST Sottotipo: log Risultato: ALLOW Configurazione: access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ advanced trust ip 192.16 8.75.0 255.255.255.0 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 Ulteriori informazioni: Fase: 14 Tipo: CONN-SETTINGS Sottotipo: Risultato: 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 informazioni aggiuntive: Fase: 15 Tipo: NAT Sottotipo: per sessione Risultato: ALLOW Config: Informazioni aggiuntive: Fase: 16 Tipo: IP-OPTIONS Sottotipo: Risultato: ALLOW Config: Informazioni aggiuntive: Fase: 17 Tipo: ROUTE-LOOKUP Sottotipo: Resolve Egress Interface

Risultato: ALLOW Config: Informazioni aggiuntive: found next-hop 1 92.168.76.39 utilizza ifc in uscita Fase: 18 Tipo: ADIACENZA-CERCA Sottotipo: hop successivo e adiacenza Risultato: CONSENTI Configurazione: Informazioni aggiuntive: adiacenza Indirizzo MAC hop successivo attivo 0004.deab.681b riscontri 140372416161507 Fase: 19 Tipo: ACQUISISCI Sottotipo: Risultato: CONSENTI Configurazione: Informazioni aggiuntive: MAC Access list Result: input-interface stato-input-esterno: attivo stato-linea-input: attivo interfaccia-output: esterno stato-output: attivo stato-linea-output: attivo Azione: consenti 1 pacchetto mostrato firepower#

L'acquisizione sull'interfaccia esterna mostra:

<#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
```

La traccia del pacchetto restituito mostra che corrisponde al flusso corrente (52), ma è bloccato dall'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

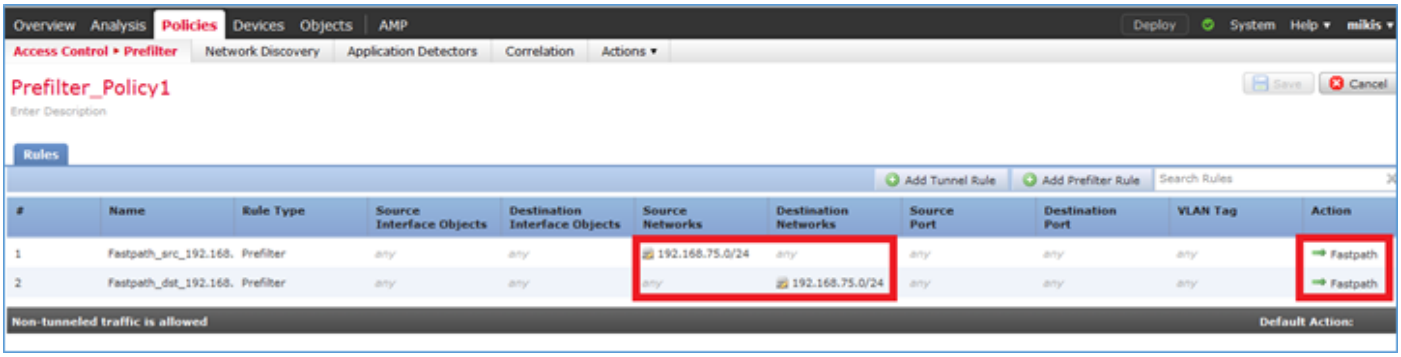
```
Subtype: log
```

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

Passaggio 5. Aggiungere un'altra regola di prefiltro per il traffico di ritorno. Il risultato è quello mostrato nell'immagine.



Tracciare il pacchetto di ritorno visualizzato (punti importanti evidenziati):

Spoiler (Evidenziato da leggere)

firepower# show capture CAPO packet-number 2 trace

10 pacchetti acquisiti

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

Fase 1

Tipo: ACQUISIZIONE

Sottotipo:

Risultato: ALLOW

Config:

Ulteriori informazioni:

Elenco accessi MAC

Fase: 2

Tipo: ACCESS-LIST

Sottotipo:

Risultato: ALLOW

Config:

Regola implicita

Ulteriori informazioni:

Elenco accessi MAC

Fase: 3

Tipo: RICERCA FLUSSO

Sottotipo:

Risultato: ALLOW

Config:

Ulteriori informazioni:

Trovato flusso con ID 62, utilizza il flusso corrente

Fase: 4

Tipo: ACCESS-LIST

Sottotipo: log

Risultato: ALLOW

Config:

access-group CSM_FW_ACL_ globale

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_ note rule-id 268434450: CRITERIO PREFILTRO: Criterio_Prefiltro1

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

Ulteriori informazioni:

Fase: 5

Tipo: CONN-SETTINGS

Sottotipo:

Risultato: ALLOW

Config:

class-map class-default

 qualsiasi

policy-map criteri_globali

 class-default

  imposta connessione opzioni avanzate UM_STATIC_TCP_MAP

criteri-servizio globali_criteri_globali

Ulteriori informazioni:

Fase: 6

Tipo: NAT

Sottotipo: per sessione

Risultato: ALLOW

Config:

Ulteriori informazioni:

Fase: 7

Tipo: OPZIONI IP

Sottotipo:

Risultato: ALLOW

Config:

Ulteriori informazioni:

Fase 8

Tipo: RICERCA ROUTE

Sottotipo: Interfaccia Resolve Egress

Risultato: ALLOW

Config:

Ulteriori informazioni:

found next-hop 192.168.75.39 utilizza ifc in uscita all'interno

Fase 9

Tipo: ADIACENZA-RICERCA

Sottotipo: next-hop e adiacenza

Risultato: ALLOW

Config:

Ulteriori informazioni:

adiacenza attiva

indirizzo mac next-hop c84c.758d.4981 trovato 140376711128802

Fase: 10

Tipo: ACQUISIZIONE

Sottotipo:

Risultato: ALLOW

Config:

Ulteriori informazioni:

Elenco accessi MAC

Risultato:

interfaccia di ingresso: interna

input-status: attivo

stato della linea di ingresso: su

interfaccia-uscita: interna

stato-output: attivo

output-line-status: attivo

Azione: consenti

firepower# show capture CAPO numero-pacchetto 2 trace 10 pacchetti acquisiti 2: 00:01:38.873123 192.168.76.39 > 192.168.75.39: icmp: echo risposta Fase: 1 Tipo: ACQUISISCI Sottotipo: Risultato: ALLOW Config: Informazioni aggiuntive: MAC Access list Fase: 2 Tipo: ACCESS-LIST Sottotipo: Risultato: ALLOW Config: Implicit Regola Informazioni aggiuntive: MAC Access list Fase: 3 Tipo: Sottotipo RICERCA: Risultato: ALLOW Config: Informazioni aggiuntive: Flusso trovato con ID 62, utilizza il flusso corrente Fase: 4 Tipo: ACCESS-LIST Sottotipo: log Risultato: 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 mark rule-id 268434450: PREFILTER POLICY: Prefilter_Policy1 access-list CSM_FW_ACL_ remark rule-id 268434450: RULE: Fastpath_dst_192.168.75.0/24 Ulteriori informazioni: fase: 5 Tipo: CONN-SETTINGS Sottotipo: Risultato: ALLOW Config: class-map class-default match any policy-map global_class-default set connection advanced-options UM_STATIC_TCP_MAP service-policy global_policy global_informazioni aggiuntive: fase: Tipo: NAT Sottotipo: per sessione Risultato: ALLOW Config: Informazioni aggiuntive: Fase: 7 Tipo: IP-OPTIONS Sottotipo: Risultato: ALLOW Config: Informazioni aggiuntive: Fase: 8 Tipo: ROUTE-LOOKUP Sottotipo: Resolve Egress Interface Risultato: ALLOW Config: Informazioni aggiuntive: found next-hop 192.168.75.39 uses exit ifc inside Phase: 9 Tipo: ADJACENCY-LOOKUP Sottotipo: next-hop e adjacency Risultato: ALLOW Config: Additional Information: adjacency Active-hop indirizzo mac c841.758d.4981 hit 140376711128802 fase: 10 tipo: CATTURA sottotipo: risultato: ALLOW Config: informazioni aggiuntive: MAC Access list Risultato: input-interface: inside input-status: up input-line-status: up output-interface: inside output-status: up output-line-status: up Azione: allow

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

La verifica è stata illustrata nelle sezioni corrispondenti delle attività.

Risoluzione dei problemi

Non sono attualmente disponibili informazioni specifiche per risolvere i problemi relativi a questa configurazione.

Informazioni correlate

- Tutte le versioni della guida alla configurazione di Cisco Firepower Management Center sono disponibili qui:

Navigazione nella documentazione di Cisco Secure Firewall Threat Defense

- Cisco Global Technical Assistance Center (TAC) consiglia vivamente questa guida visiva per una conoscenza pratica e approfondita delle tecnologie di sicurezza di nuova generazione di Cisco Firepower, incluse quelle menzionate in questo articolo:

Cisco Firepower Threat Defense (FTD)

- Note tecniche sulla configurazione e la risoluzione dei problemi:

Cisco Secure Firewall Management Center

- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).