Configuración y funcionamiento de las políticas de filtros previos de FTD

Contenido

Introducción

Este documento describe la configuración y el funcionamiento de las políticas de filtros previos de Firepower Threat Defence (FTD).

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- ASA5506X que ejecuta el código FTD 6.1.0-195
- FireSIGHT Management Center (FMC) que ejecuta 6.1.0-195
- Dos routers Cisco IOS® 3925 que ejecutan 15.2 imágenes

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Una política de prefiltro es una función introducida en la versión 6.1 y tiene tres objetivos principales:

1. Coincidir tráfico basado en encabezados internos y externos
2. Proporcione un control de acceso temprano que permite que un flujo omita por completo el motor Snort
3. Trabaje como marcador de posición para las entradas de control de acceso (ACE) que se migran desde la herramienta de migración de Adaptive Security Appliance (ASA).

Configurar

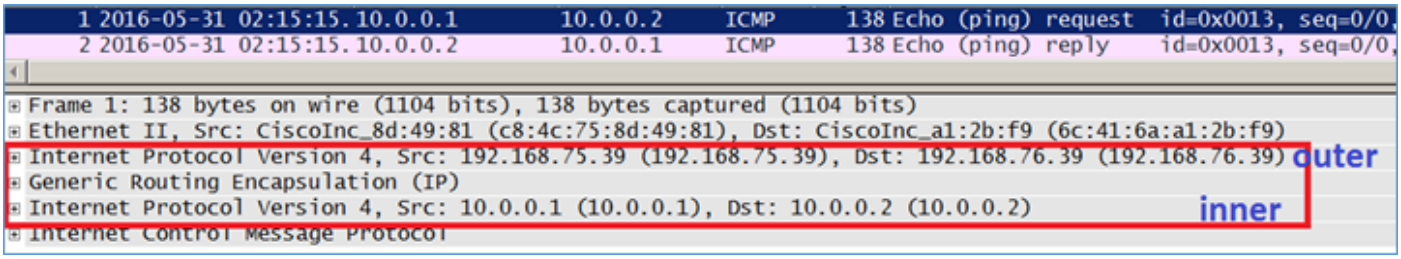
Caso práctico de directiva de prefiltro 1

Una política de prefiltro puede utilizar un tipo de regla de túnel que permite a FTD filtrar basándose en el tráfico tunelizado de encabezado IP interno y/o externo. En el momento en que se escribió este artículo, el tráfico tunelado se refiere a:

- Encapsulación de routing genérico (GRE)
- IP en IP
- IPv6 en IP
- Puerto Teredo 3544

Considere un túnel GRE como se muestra en la imagen.

Cuando hace ping de R1 a R2 con el uso de un túnel GRE, el tráfico pasa a través del firewall, como se muestra en la imagen.



Si el firewall es un dispositivo ASA, verifica el encabezado IP externo como se muestra en la imagen.

<#root>

ASA#

show conn

GRE OUTSIDE 192.168.76.39:0 INSIDE 192.168.75.39:0

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

Si el firewall es un dispositivo FirePOWER, comprueba el encabezado IP interno como se muestra en la imagen.

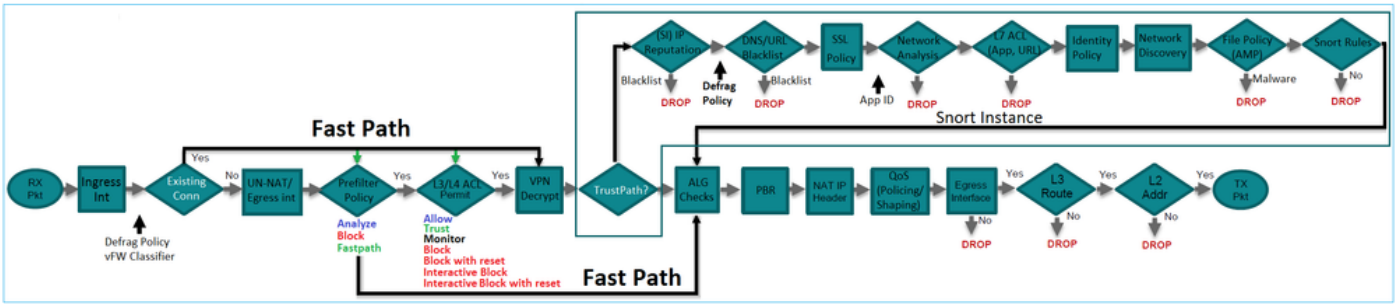
Con la política de filtro previo, un dispositivo FTD puede hacer coincidir el tráfico basado en encabezados internos y externos.

Punto principal:

Dispositivo	Cheques
ASA	IP externa
Snort	IP interna
FTD	Exterior (Prefiltro) + IP interior (política de control de acceso (ACP))

Caso práctico de directiva de filtro previo 2

Una política de filtro previo puede utilizar un tipo de regla de filtro previo que puede proporcionar control de acceso temprano y permitir que un flujo omita completamente el motor de Snort, como se muestra en la imagen.



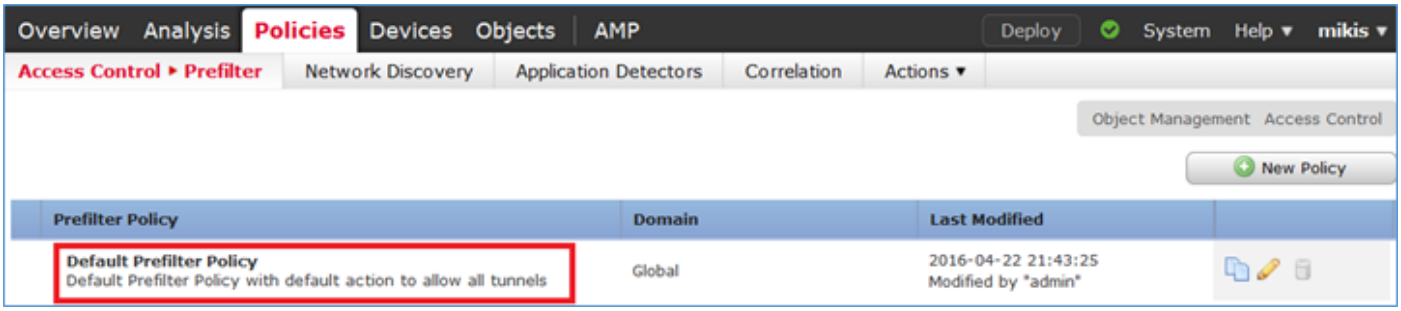
Tarea 1. Verificar política de prefiltro predeterminada

Tarea requerida:

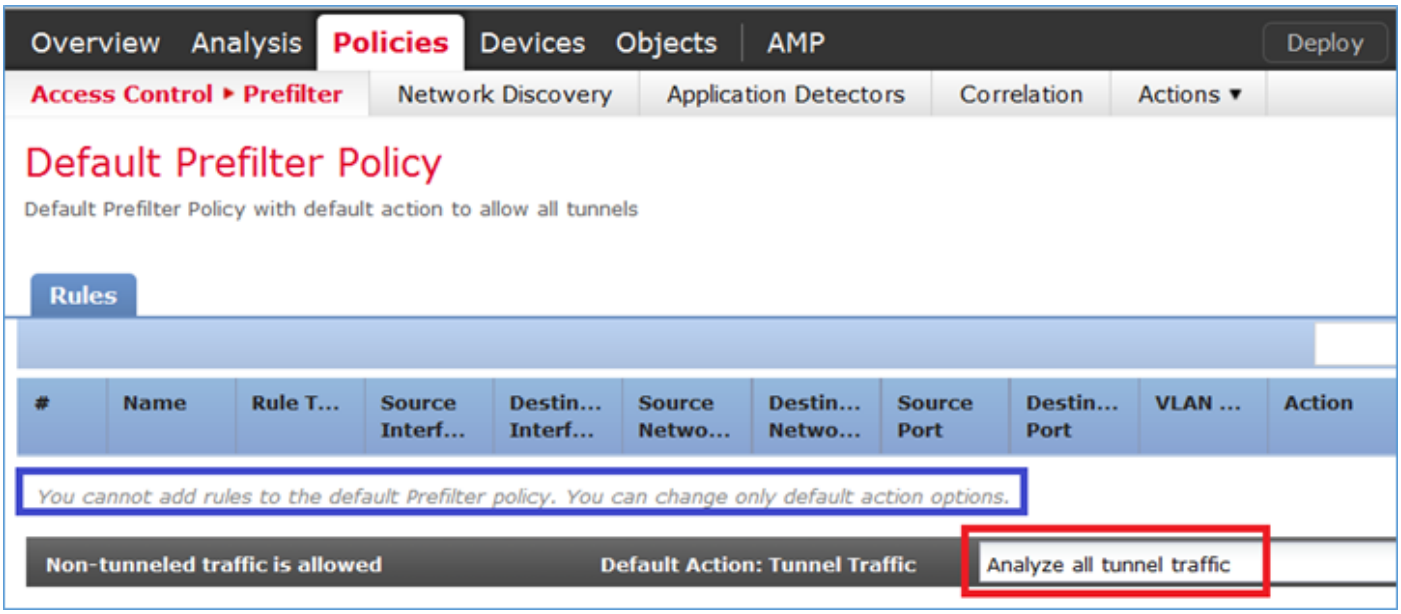
Verifique la política de filtro previo predeterminada

Solución:

Paso 1. Vaya a Políticas > Control de acceso > Prefiltro. Ya existe una política de prefiltro predeterminada, como se muestra en la imagen.



Paso 2. Elija Edit para ver la configuración de la política como se muestra en la imagen.



Paso 3. La política de filtro previo ya está asociada a la política de control de acceso, como se muestra en la imagen.

Verificación de CLI (LINA)

Las reglas de prefiltro se agregan sobre las 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
```

Tarea 2. Bloqueo del tráfico tunelizado con etiqueta

Tarea requerida:

Bloquee el tráfico ICMP que se tuneliza dentro del túnel GRE.

Solución:

Paso 1. Si aplica estos ACP, puede ver que el tráfico de Internet Control Message Protocol (ICMP) está bloqueado, independientemente de si pasa a través del túnel GRE o no, como se muestra en la imagen.

<#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)
```

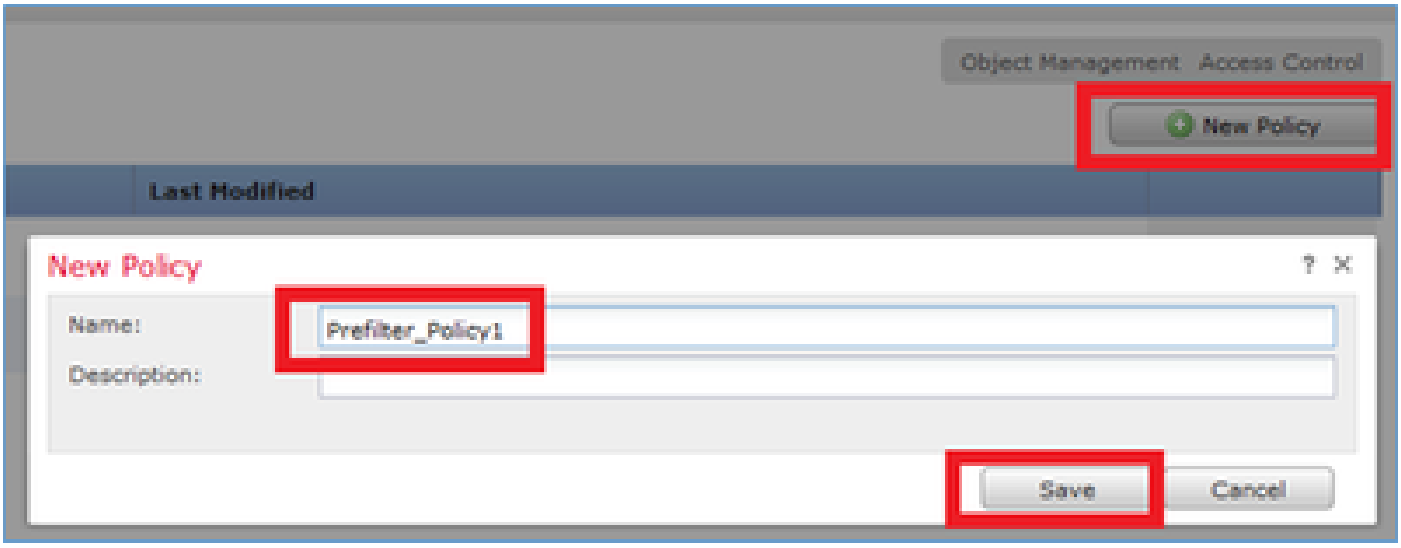
En este caso, puede utilizar una directiva de filtro previo para cumplir los requisitos de la tarea. La lógica es la siguiente:

1. Puede etiquetar todos los paquetes que están encapsulados dentro de GRE.
2. Cree una política de control de acceso que coincida con los paquetes etiquetados y bloquee el ICMP.

Desde el punto de vista de la arquitectura, los paquetes se comprueban con las reglas de prefiltro de LINA (LINA), a continuación, las reglas de prefiltro de Snort y ACP y, por último, Snort indica a LINA que descarte. El primer paquete pasa a través del dispositivo FTD.

Paso 1. Defina una etiqueta para el tráfico tunelizado.

Navegue hasta Políticas > Control de acceso > Prefiltro y cree una nueva Política de Prefiltro. Recuerde que la política de filtro previo predeterminada no se puede editar como se muestra en la imagen.

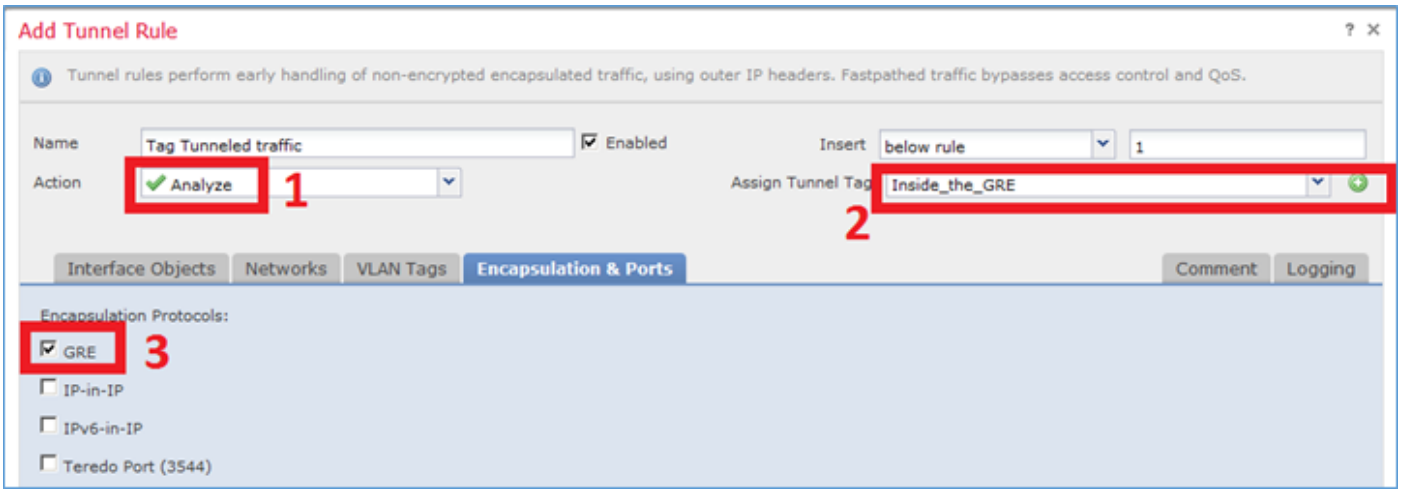


Dentro de la directiva de filtros previos, puede definir dos tipos de reglas:

1. Regla de túnel
2. Regla de filtro previo

Puede considerar estas dos funciones totalmente diferentes que se pueden configurar en una política de prefiltro.

Para esta tarea, es necesario definir una regla de túnel como se muestra en la imagen.

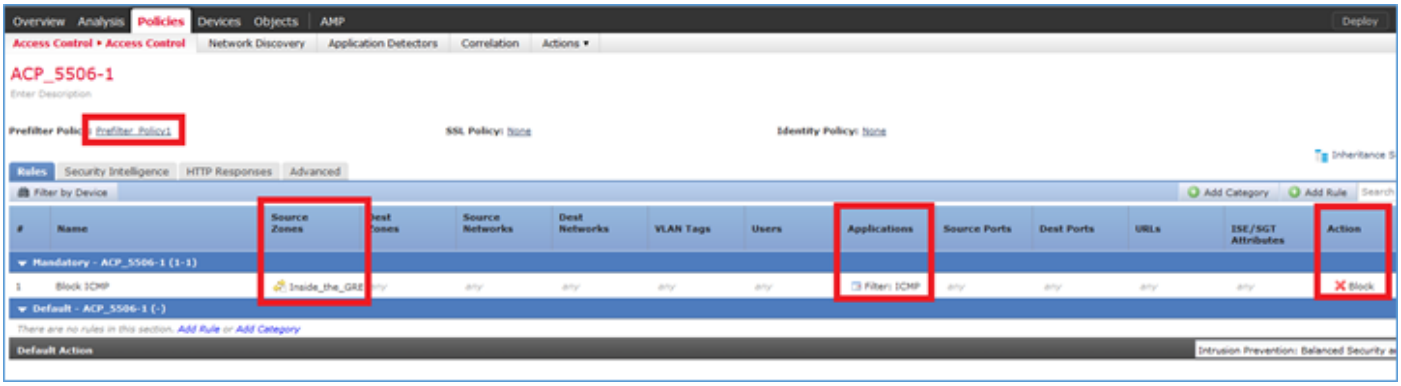


Por lo que se refiere a las acciones:

Acción	Descripción
Analizar	Después de LINA, el flujo es verificado por Snort Engine. Opcionalmente, se puede asignar una etiqueta de túnel al tráfico tunelizado.
Bloqueo	LINA bloquea el flujo. El encabezado externo debe ser verificado.
Trayectoria rápida	El flujo lo gestiona sólo LINA sin necesidad de acoplar el motor Snort.

Paso 2. Defina la política de control de acceso para el tráfico etiquetado.

Aunque no puede ser muy intuitivo al principio, la etiqueta de túnel puede ser utilizada por una regla de política de control de acceso como zona de origen. Navegue hasta Políticas > Control de acceso y cree una Regla que bloquee el ICMP para el tráfico etiquetado como se muestra en la imagen.



Nota: La nueva política de filtro previo se adjunta a la política de control de acceso.

Verificación:

Habilite la captura en LINA y en 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
```

Desde R1, intente hacer ping al extremo del túnel GRE remoto. El ping falla:

<#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)
```

La captura CLISH muestra que la primera solicitud de eco pasó a través de FTD y la respuesta se bloqueó:

<#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 captura LINA confirma lo siguiente:

```
<#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
```

Habilite CLISH firewall-engine-debug, borre los contadores de caídas de LINA ASP y realice la misma prueba. La depuración CLISH muestra que para la solicitud de eco coincidió con la regla de prefiltro y para la regla de respuesta de eco la regla ACP:

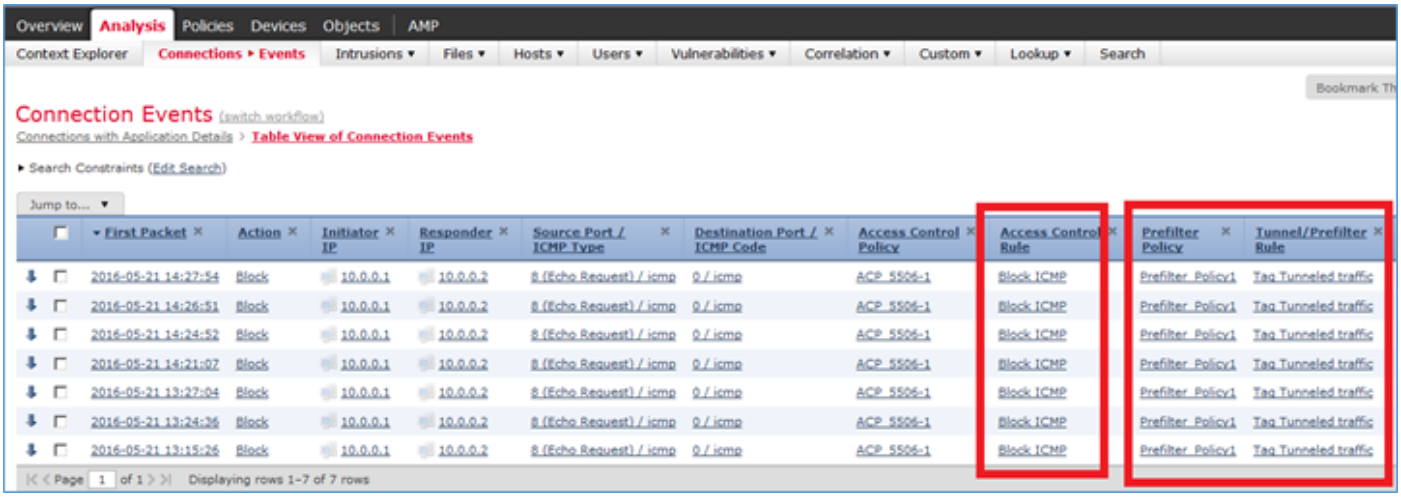
```
<#root>

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
```

El descarte de ASP muestra que Snort descartó los paquetes:

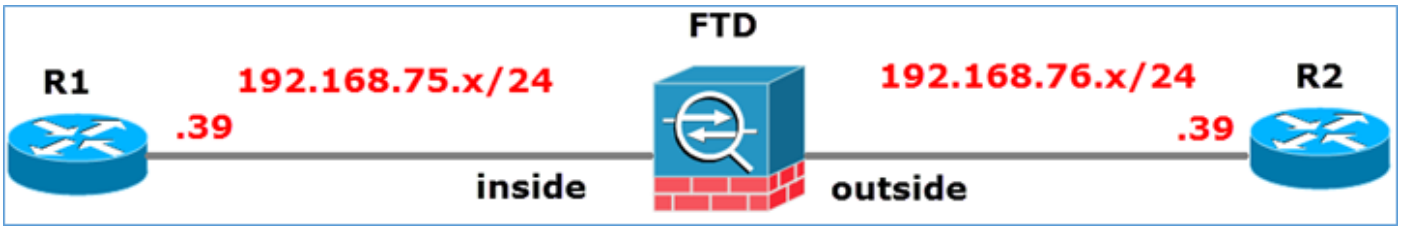
```
<#root>
>
show asp drop

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
```

En Connection Events (Eventos de conexión), puede ver la regla y directiva de filtro previo que coincidió, como se muestra en la imagen.



Tarea 3. Omitir motor Snort con reglas de filtro previo de ruta rápida

Diagrama de la red

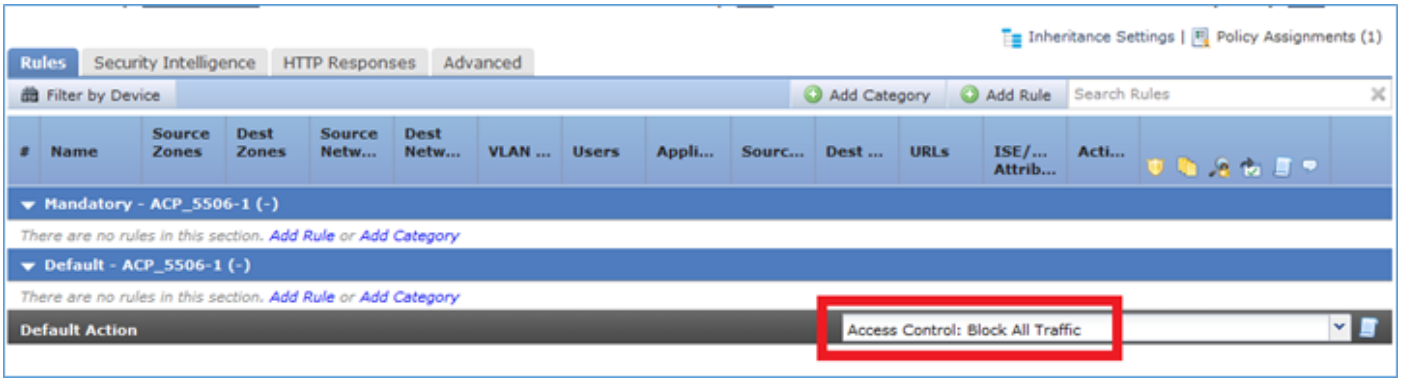


Tarea requerida:

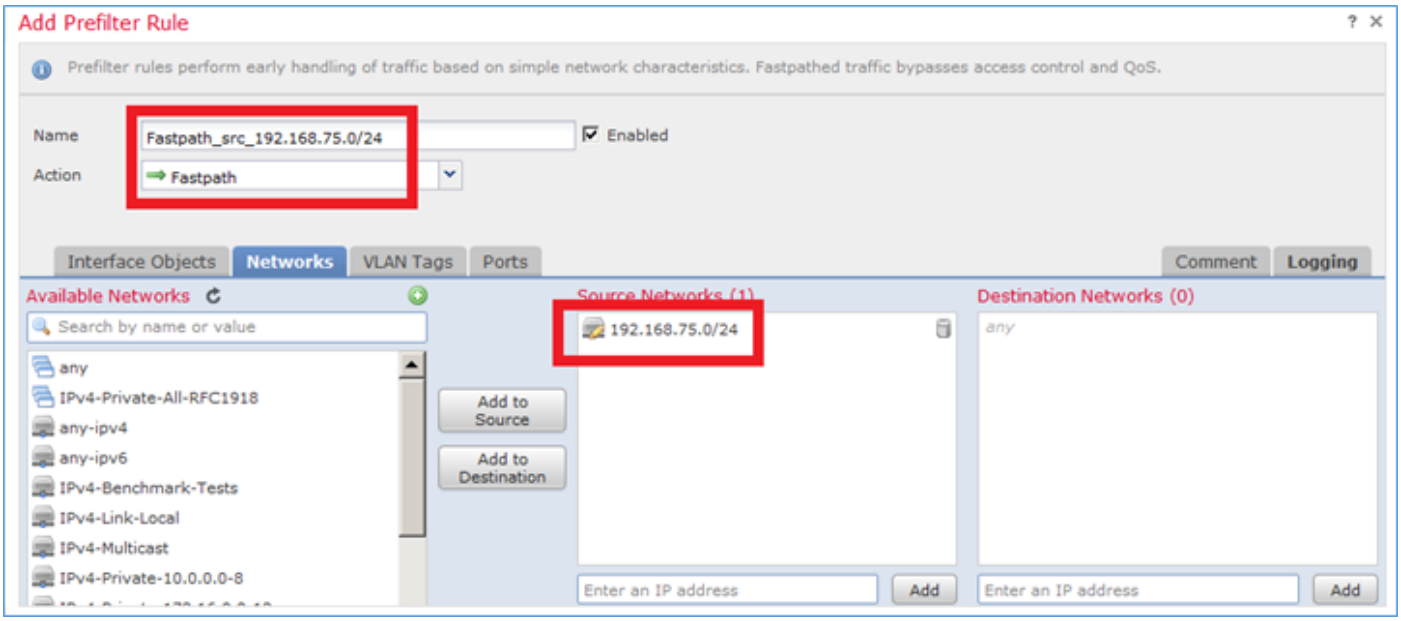
1. Quite las reglas actuales de la directiva de control de acceso y agregue una regla de directiva de control de acceso que bloquee todo el tráfico.
2. Configure una regla de directiva de filtro previo que omita el motor Snort para el tráfico originado en la red 192.168.75.0/24.

Solución:

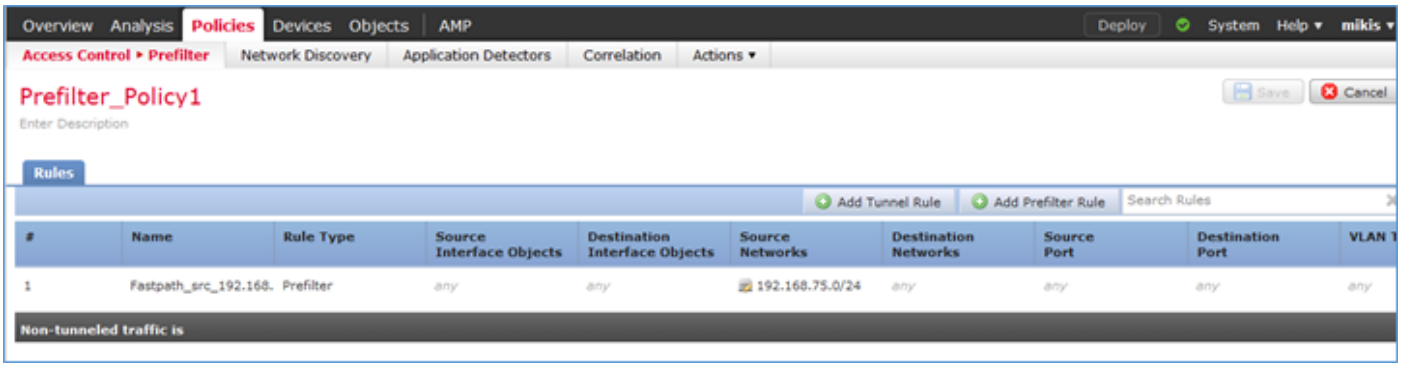
Paso 1. La política de control de acceso que bloquea todo el tráfico es como se muestra en la imagen.



Paso 2. Agregue una regla de filtro previo con ruta rápida como acción para la red de origen 192.168.75.0/24, como se muestra en la imagen.



Paso 3. El resultado es como se muestra en la imagen.



Paso 4. Guardar e implementar.

Habilite la captura con seguimiento en ambas interfaces FTD:

<#root>

```
firepower#

capture CAPI int inside trace match icmp any any

firepower#

capture CAPO int outsid trace match icmp any any
```

Intente hacer ping desde R1 (192.168.75.39) a R2 (192.168.76.39) a través del FTD. El ping falla:

<#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 captura en la interfaz interior muestra:

<#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
```

El seguimiento del primer paquete (petición de eco) muestra (puntos importantes resaltados):

Deflector (Destaque para leer)

firepower# show capture CAPI packet-number 1 trace

5 paquetes capturados

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

Fase: 1

Tipo: CAPTURA

Subtipo:

Resultado: PERMITIR

Config:

Información adicional:

Lista de acceso MAC

Fase: 2

Tipo: ACCESS-LIST

Subtipo:

Resultado: PERMITIR

Config:

Regla implícita

Información adicional:

Lista de acceso MAC

Fase: 3

Tipo: ROUTE-LOOKUP

Subtipo: Resolver interfaz de salida

Resultado: PERMITIR

Config:

Información adicional:

found next-hop 192.168.76.39 uses egress ifc outside

Fase: 4

Tipo: ACCESS-LIST

Subtipo: registro

Resultado: PERMITIR

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

Información adicional:

Fase: 5

Tipo: CONN-SETTINGS

Subtipo:

Resultado: PERMITIR

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

Información adicional:

Fase: 6

Tipo: NAT

Subtipo: por sesión

Resultado: PERMITIR

Config:

Información adicional:

Fase: 7

Tipo: IP-OPTIONS

Subtipo:

Resultado: PERMITIR

Config:

Información adicional:

Fase: 8

Tipo: INSPECCIONAR

Subtipo: np-inspect

Resultado: PERMITIR

Config:

class-map inspection_default

 match default-inspection-traffic

policy-map global_policy

 class inspection_default

  inspeccionar icmp

service-policy global_policy global

Información adicional:

Fase: 9

Tipo: INSPECCIONAR

Subtipo: np-inspect

Resultado: PERMITIR

Config:

Información adicional:

Fase: 10

Tipo: NAT

Subtipo: por sesión

Resultado: PERMITIR

Config:

Información adicional:

Fase: 11

Tipo: IP-OPTIONS

Subtipo:

Resultado: PERMITIR

Config:

Información adicional:

Fase: 12

Tipo: CREACIÓN DE FLUJO

Subtipo:

Resultado: PERMITIR

Config:

Información adicional:

Nuevo flujo creado con id 52, paquete enviado al siguiente módulo

Fase: 13

Tipo: ACCESS-LIST

Subtipo: registro

Resultado: PERMITIR

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

Información adicional:

Fase: 14

Tipo: CONN-SETTINGS

Subtipo:

Resultado: PERMITIR

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

Información adicional:

Fase: 15

Tipo: NAT

Subtipo: por sesión

Resultado: PERMITIR

Config:

Información adicional:

Fase: 16

Tipo: IP-OPTIONS

Subtipo:

Resultado: PERMITIR

Config:

Información adicional:

Fase: 17

Tipo: ROUTE-LOOKUP

Subtipo: Resolver interfaz de salida

Resultado: PERMITIR

Config:

Información adicional:

found next-hop 192.168.76.39 uses egress ifc outside

Fase: 18

Tipo: BÚSQUEDA DE ADYACENCIA

Subtipo: next-hop y adyacencia

Resultado: PERMITIR

Config:

Información adicional:

adyacencia activa

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

Fase: 19

Tipo: CAPTURA

Subtipo:

Resultado: PERMITIR

Config:

Información adicional:

Lista de acceso MAC

Resultado:

input-interface: outside

input-status: up

input-line-status: up

interfaz de salida: externa

output-status: up

output-line-status: up

Acción: permitir

Se muestra 1 paquete

firepower#

firepower# show capture CAPI packet-number 1 trace 5 packets capturados 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 Config: Result: ALLOW: Implicit Rule Additional Information: MAC Access list Phase: 3 Type: ROUTE-LOOO Subtipo KUP: Resolver interfaz de salida Resultado: PERMITIR configuración: Información adicional: encontrado next-hop 192.168.76.39 utiliza ifc de salida fuera Fase: 4 Tipo: ACCESS-LIST Subtipo: log Resultado: PERMITIR configuración: 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 Información adicional: Phase: 5 Type: CONN-SETTINGS Subtype: Result: 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 Información adicional: Phase: 6 Type: NAT Tipo: por sesión Resultado: ALLOW Config: Información adicional: Fase: 7 Tipo: IP-OPTIONS Subtipo: Resultado: ALLOW Config: Información adicional: Fase: 8 Tipo: INSPECT Subtipo: np-inspect Resultado: ALLOW Config: class-map inspection_default match default-inspection-traffic policy-map global_policy class inspection_default inspect icmp service-policy global_policy global Información adicional: Fase: 9 Tipo: INSPECT Subtipo: np-Config Resultado: ALLOW: Información adicional: Fase: 10 Tipo: NAT Subtipo: por sesión Resultado: ALLOW Configuración W: Información Adicional: Fase: 11 Tipo: IP-OPTIONS Subtipo: Resultado: PERMITIR Configuración: Información Adicional: Fase: 12 Tipo: FLUJO-CREACIÓN Subtipo: Resultado: PERMITIR Configuración: Información Adicional: Nuevo flujo creado con ID 52, paquete enviado al siguiente módulo Fase: 13 Tipo: ACCESS-LIST Subtipo: log Resultado: PERMITIR Configuración: access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ advanced trust ip 192.168.78.768.78.75.0 25.0 55.255.255.0 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 Información adicional: Phase: 14 Type: CONN-SETTINGS Subtype Config: ALLOW: class-map class-default match any policy-map global_policy class-default set conexión avanzada 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: ADJACID ENCY-LOOKUP Subtipo: next-hop y adyacencia Resultado: ALLOW Config: Información adicional: adyacencia MAC next-hop activo address 0004.deab.681b hits 140372416161507 Fase: 19 Tipo: CAPTURE Subtipo: Resultado: ALLOW Config: Información adicional: MAC Access list Resultado: input-interface: outside input-status: up input-line-status: up output-interface: outside output-status: up output-line-status: up Acción: allow 1 packet show firepower#

La captura en la interfaz externa muestra:

<#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
```

El seguimiento del paquete de retorno muestra que coincide con el flujo actual (52), pero está bloqueado por la 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

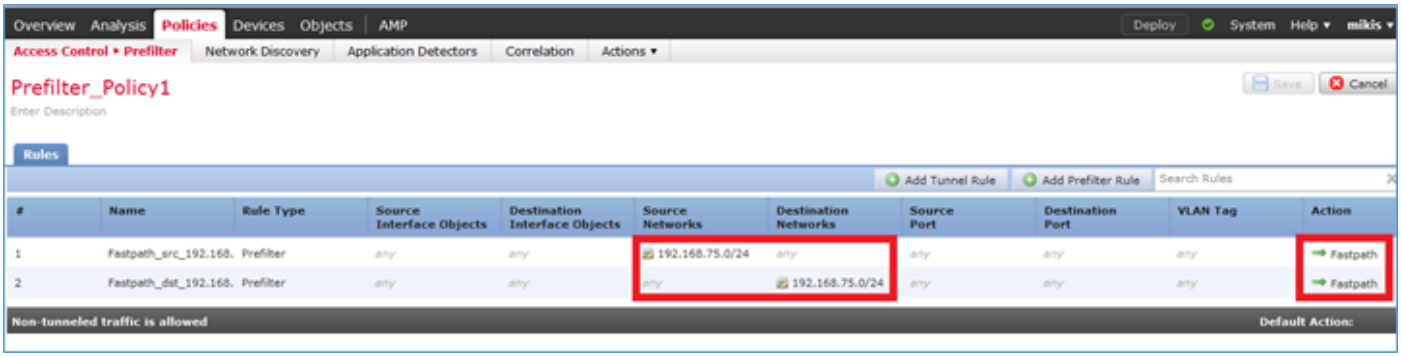
```
Subtype: log
```

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

Paso 5. Agregue una regla de filtro previo más para el tráfico de retorno. El resultado es como se muestra en la imagen.



A continuación, realice un seguimiento del paquete de retorno que aparece (puntos importantes resaltados):

Deflector (Destaque para leer)

firepower# show capture CAPO packet-number 2 trace

10 paquetes capturados

2: 00:01:38.873123 192.168.76.39 > 192.168.75.39: icmp: respuesta de eco

Fase: 1

Tipo: CAPTURA

Subtipo:

Resultado: PERMITIR

Config:

Información adicional:

Lista de acceso MAC

Fase: 2

Tipo: ACCESS-LIST

Subtipo:

Resultado: PERMITIR

Config:

Regla implícita

Información adicional:

Lista de acceso MAC

Fase: 3

Tipo: FLOW-LOOKUP

Subtipo:

Resultado: PERMITIR

Config:

Información adicional:

Flujo encontrado con id. 62, utiliza el flujo actual

Fase: 4

Tipo: ACCESS-LIST

Subtipo: registro

Resultado: PERMITIR

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

Información adicional:

Fase: 5

Tipo: CONN-SETTINGS

Subtipo:

Resultado: PERMITIR

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

Información adicional:

Fase: 6

Tipo: NAT

Subtipo: por sesión

Resultado: PERMITIR

Config:

Información adicional:

Fase: 7

Tipo: IP-OPTIONS

Subtipo:

Resultado: PERMITIR

Config:

Información adicional:

Fase: 8

Tipo: ROUTE-LOOKUP

Subtipo: Resolver interfaz de salida

Resultado: PERMITIR

Config:

Información adicional:

found next-hop 192.168.75.39 uses egress ifc inside

Fase: 9

Tipo: BÚSQUEDA DE ADYACENCIA

Subtipo: next-hop y adyacencia

Resultado: PERMITIR

Config:

Información adicional:

adyacencia activa

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

Fase: 10

Tipo: CAPTURA

Subtipo:

Resultado: PERMITIR

Config:

Información adicional:

Lista de acceso MAC

Resultado:

input-interface: inside

input-status: up

input-line-status: up

interfaz de salida: interior

output-status: up

output-line-status: up

Acción: permitir

firepower# show capture CAPO packet-number 2 trace 10 packets capture 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 Rule Additional Information: MAC Access list Phase: 3 Type: FLOW-LIST LOOKUP Subtipo: Resultado: ALLOW Config: Información adicional: Flujo encontrado con id. 62, utiliza el flujo actual Fase: 4 Tipo: ACCESS-LIST Subtipo: log Resultado: 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 TER POLICY: Prefilter_Policy1 access-list CSM_FW_ACL_ remark rule-id 268434450: RULE: Fastpath_dst_192.168.75.0/24 Información adicional: Phase: 5 Type: CONN-SETTINGS Subtype: Result: 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 Información adicional: Phase: 6 Type: NAT Subtype: per-session Result: ALLOW Config: Additional Information: 7 Type: IP -OPTIONS Subtipo: Resultado: PERMITIR configuración: Información adicional: Fase: 8 Tipo: ROUTE-LOOKUP Subtipo: Resolver interfaz de salida Resultado: PERMITIR configuración: Información adicional: encontrado next-hop 192.168.75.39 utiliza ifc de salida dentro de Fase: 9 Tipo: ADJACENCY-LOOKUP Subtipo: next-hop y adyacencia Resultado: PERMITIR configuración: Información adicional: adyacencia MAC de siguiente salto activo dirección c84c.758d.498881 hits 140376711128802 Fase: 10 Tipo: CAPTURE Subtipo: Resultado: ALLOW Configuración: Información adicional: MAC Lista de acceso Resultado: input-interface: inside input-status: up input-line-status: up output-interface: inside output-status: up output-line-status: up Acción: allow

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

La verificación se ha explicado en las respectivas secciones de tareas.

Troubleshoot

Actualmente no hay información específica disponible para resolver problemas de esta configuración.

Información Relacionada

- Todas las versiones de la guía de configuración de Cisco Firepower Management Center se pueden encontrar aquí:

Navegación por la documentación de Cisco Secure Firewall Threat Defence

- Cisco Global Technical Assistance Center (TAC) recomienda encarecidamente esta guía visual para obtener un conocimiento práctico en profundidad de las tecnologías de seguridad de última generación de Cisco Firepower, que incluye las mencionadas en este artículo:

Cisco Firepower Threat Defence (FTD)

- Para todas las notas técnicas sobre configuración y resolución de problemas:

Cisco Secure Firewall Management Center

- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).