Configuración y operación de las directivas FTD Prefilter

Contenido

Introducción

Este documento describe la configuración y la operación de las directivas del PRE-filtro de la defensa de la amenaza de FirePOWER (FTD).

Prerequisites

Requisitos

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 funciona con el código 6.1.0-195 FTD
- Centro de administración de FireSIGHT (FMC) esos funcionamientos 6.1.0-195
- Dos 3925 Routers de Cisco IOS® que funciona con 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 su red está viva, asegúrese de que usted entienda el impacto potencial del comando any.

Antecedentes

Una directiva de Prefilter es una característica introducida en la versión 6.1 y responde a tres propósitos principales:

1. Haga juego el tráfico basado en interno y los encabezados exteriores
2. Proporcione el control de acceso temprano que permite que un flujo desvíe el motor del Snort totalmente
3. Trabaje como placeholder para las entradas de control de acceso (ACE) que se emigran de la herramienta adaptante de la migración del dispositivo de seguridad (ASA).

Tiempo de la realización del laboratorio: 30 minutos.

Configurar

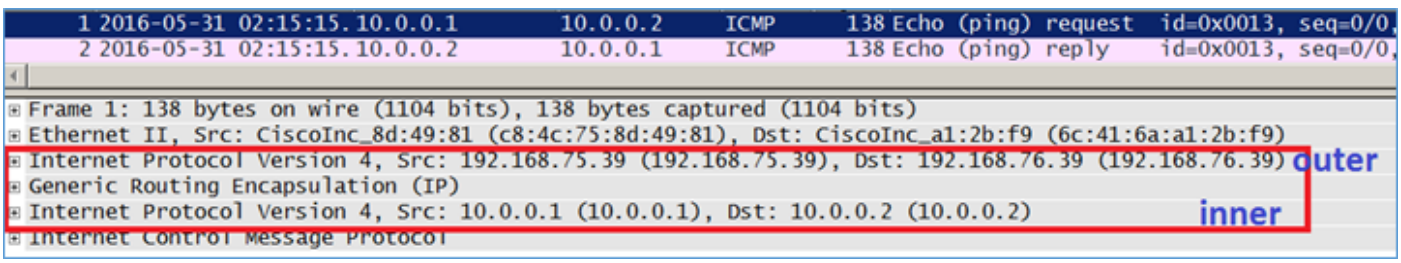
caso 1 del uso de la directiva del PRE-filtro

Una directiva del PRE-filtro puede utilizar un **tipo de la regla del túnel** que permita que FTD filtre basado en ambos interiores y/o el tráfico de túnel exterior del encabezado IP. Cuando este artículo fue escrito, el tráfico de túnel se refiere:

- Generic Routing Encapsulation (GRE)
- IP en IP
- IPv6-in-IP
- Puerto 3544 de Teredo

Considere un túnel GRE tal y como se muestra en de la imagen aquí.

Cuando usted hace ping del r1 al r2 con el uso de un túnel GRE, el tráfico pasa con las miradas del Firewall tal y como se muestra en de la imagen.



Si el Firewall es un **dispositivo ASA,** marca el **encabezado IP externo** tal y como se muestra en de la imagen.


```
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 de FirePOWER,** marca el **encabezado IP interno** tal y como se muestra en de la imagen.

Con la directiva del PRE-filtro, un dispositivo FTD puede hacer juego el tráfico basado en interno y los encabezados exteriores.

Punto principal:

Dispositivo	Controles
ASA	IP externo
Snort	IP interno
FTD	Externo (Prefilter) + IP interno (control de acceso Policy(ACP))

caso 2 del uso de la directiva del PRE-filtro

Una directiva del PRE-filtro puede utilizar un **tipo de la regla de Prefilter** que pueda proporcionar el control de acceso temprano y permitir que un flujo desvíe el motor del Snort totalmente tal y como se muestra en de la imagen.

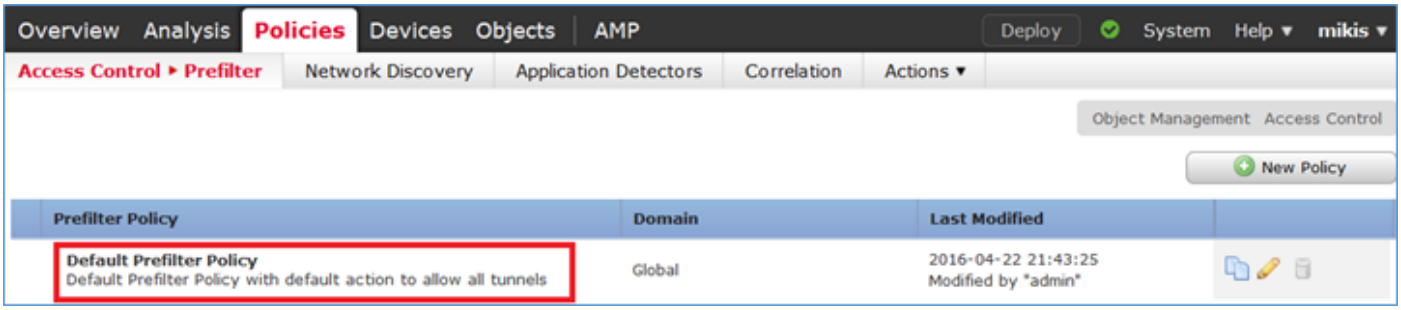
La tarea 1. verifica la directiva predeterminada del PRE-filtro

Requisito de la tarea:

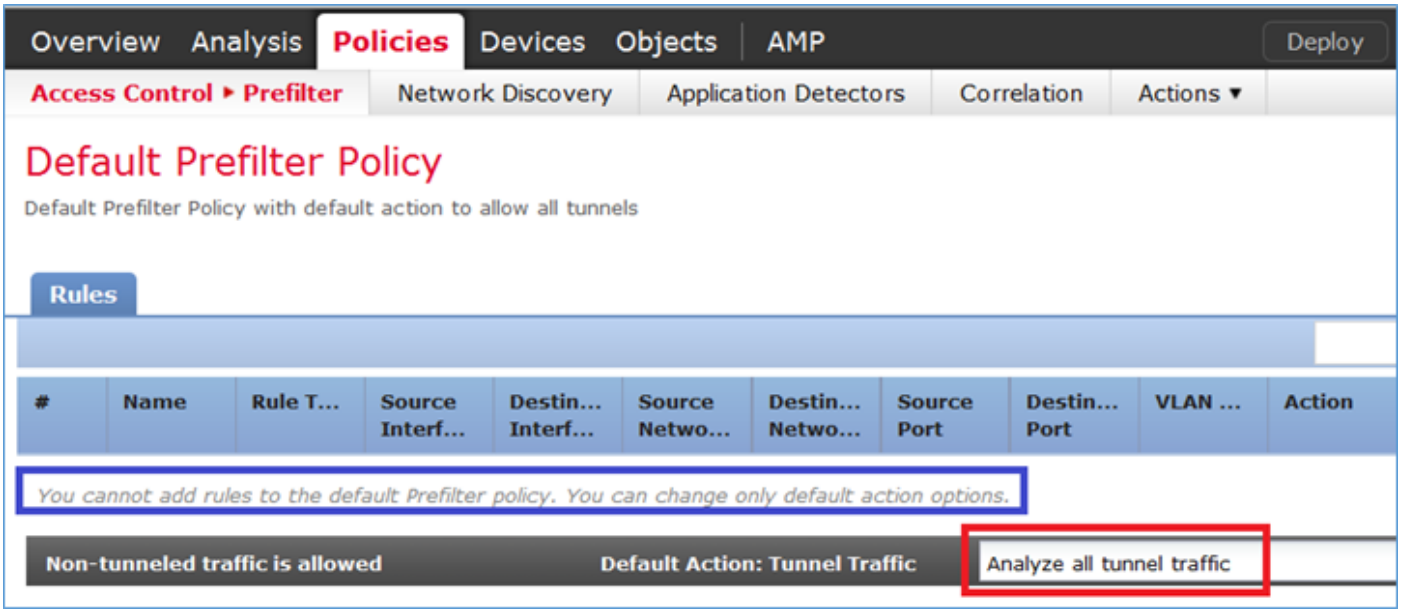
Verifique la directiva predeterminada de Prefilter

Solución:

Paso 1. Navegue a las **directivas > al control de acceso > a Prefilter**. Una directiva predeterminada de Prefilter existe ya tal y como se muestra en de la imagen.



Paso 2. Selecto **edite** para ver las configuraciones de la directiva tal y como se muestra en de la imagen.



Paso 3. La directiva del PRE-filtro se asocia ya a la directiva del control de acceso tal y como se muestra en de la imagen.

Verificación CLI (LINA)

las reglas del PRE-filtro se agregan encima de los ACL:

```
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
```

Tráfico de túnel del bloque de la tarea 2. con la etiqueta

Requisito de la tarea:

Tráfico del bloque ICMP que es túnel GRE interior tunneled.

Solución:

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


```
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)
```

```
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, usted puede utilizar una directiva del PRE-filtro para cumplir el requisito de la tarea. La lógica es como sigue:

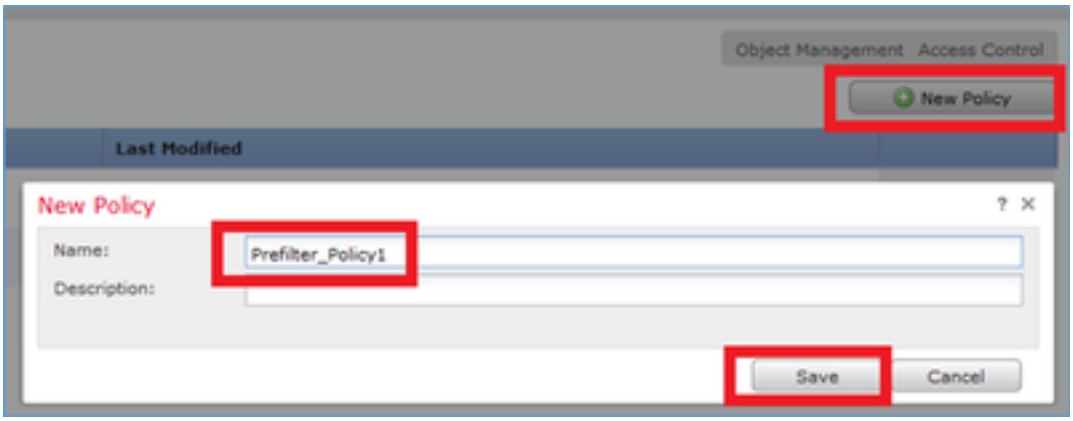
1. Usted marca todos los paquetes con etiqueta que se encapsulen dentro del GRE.
2. Usted crea una directiva del control de acceso que haga juego los paquetes con Tag y bloquee el ICMP.

Desde el punto de vista de la arquitectura, los paquetes se marcan contra las reglas del PRE-filtro

de LINA, después resoplan las reglas del PRE-filtro y el ACP y finalmente Snort da instrucciones a LINA para caer. El primer paquete lo hace a través del dispositivo FTD.

Paso 1. Defina una etiqueta para el tráfico de túnel.

Navegue a las **directivas > al control de acceso > a Prefilter** y cree una nueva directiva de Prefilter. Recuerde que la directiva predeterminada de Prefilter no se puede editar tal y como se muestra en de la imagen.

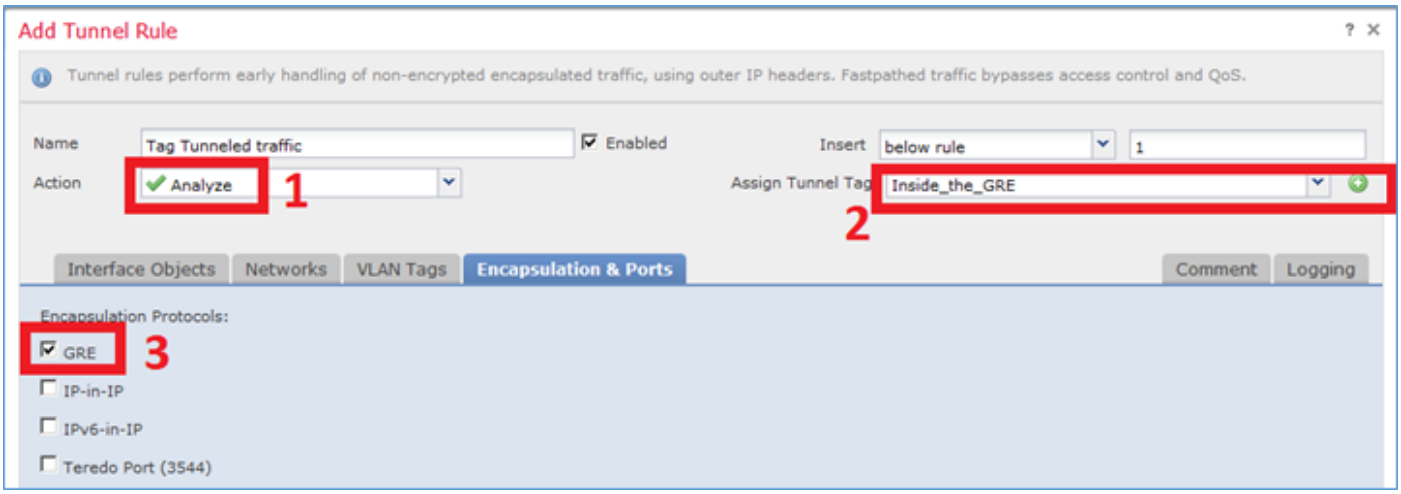


Dentro de la directiva de Prefilter, usted puede definir dos tipos de reglas:

- Regla del túnel
- Regla de Prefilter

Usted puede pensar de estos dos como características totalmente diversas que se puedan configurar en una directiva de Prefilter.

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

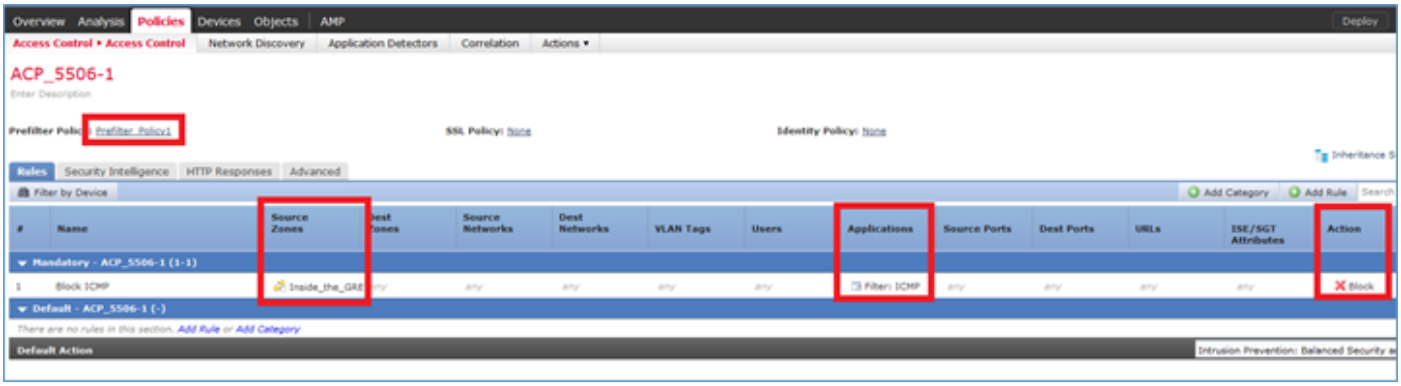


En lo que respecta a las acciones:

Acción	Descripción
Analice	Después de LINA, el flujo es marcado por el motor del Snort. Opcionalmente, una etiqu del túnel se puede asignar al tráfico de túnel.
Bloque	El flujo es bloqueado por LINA. El encabezado exterior debe ser marcado.
Fastpath	El flujo es manejado solamente por LINA sin la necesidad de dedicar el motor del Snort.

Paso 2. Defina la directiva del control de acceso para el tráfico con Tag.

Aunque pueda no ser muy intuitivo al principio, la etiqueta del túnel se puede utilizar por una regla de la directiva del control de acceso como **zona de origen**. Navegue a las **directivas > al control de acceso** y cree una regla que bloquee el ICMP para el tráfico con Tag tal y como se muestra en de la imagen.



Note: La nueva directiva de Prefilter se asocia a la directiva del control de acceso.

Verificación:

Captura del permiso en LINA y en CLISH:

```
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]
```

```
> 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
```

Del r1, intente hacer ping el punto final remoto del túnel GRE. El ping falla:

```
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 el primer pedido de eco pasó con FTD y la contestación fue bloqueada:

```
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 request, id 65, seq 0, length 80
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 reply, id 65, seq 0, length 80
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 request, id 65, seq 1, length 80
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 request, id 65, seq 2, length 80
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 request, id 65, seq 3, length 80
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 request, id 65, seq 4, length 80
```

La captura de LINA confirma esto:

```
> 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
```

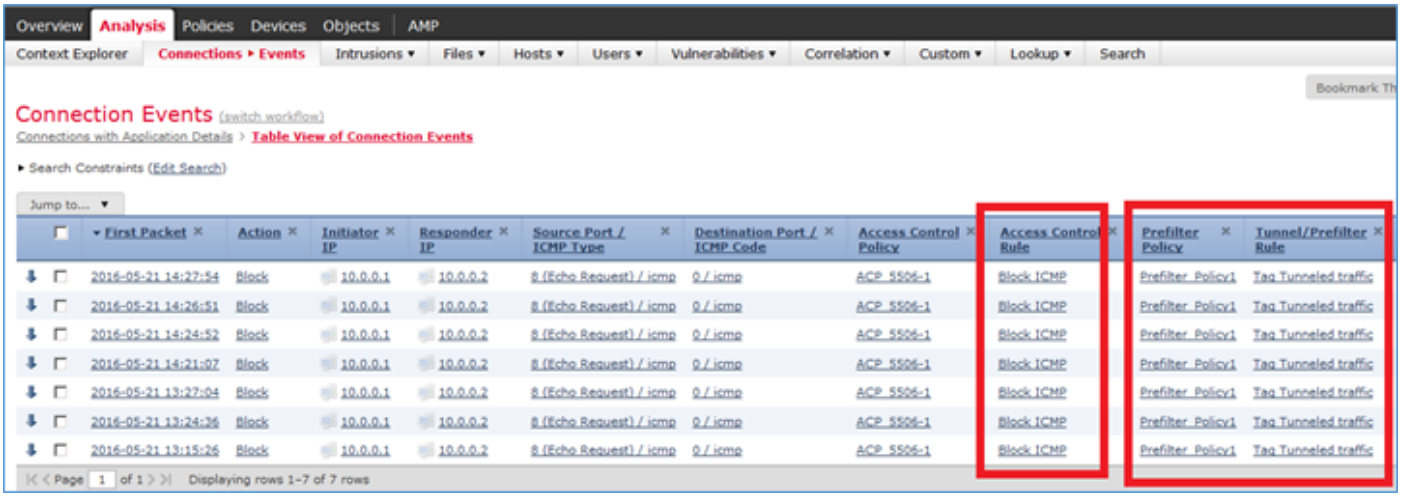
Habilite el Firewall-motor-debug CLISH, los contadores de caídas claros de LINA ASP y haga la misma prueba. El debug CLISH muestra que para el pedido de eco usted correspondió con la regla del prefilter y para la respuesta de eco la regla ACP:

```
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 using 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, geo 0 -> 0, vlan 0, sgt tag: 65535, svc 0, payload 0, client 0, misc 0, user 9999997,
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 using 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, geo 0 -> 0, vlan 0, sgt tag: 65535, svc 3501, payload 0, client 2000003501, misc 0, user
9999997, 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 descenso ASP muestra que el Snort cayó los paquetes:

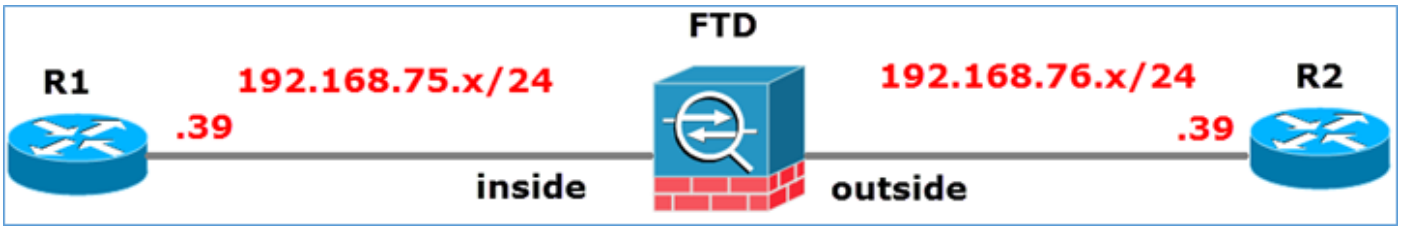
```
> show asp drop

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 los eventos de conexión, usted puede ver la directiva de Prefilter y gobernar que usted correspondió con tal y como se muestra en de la imagen.



Motor del Snort de puente de la tarea 3. con las reglas de Prefilter del fastpath

Diagrama de la red

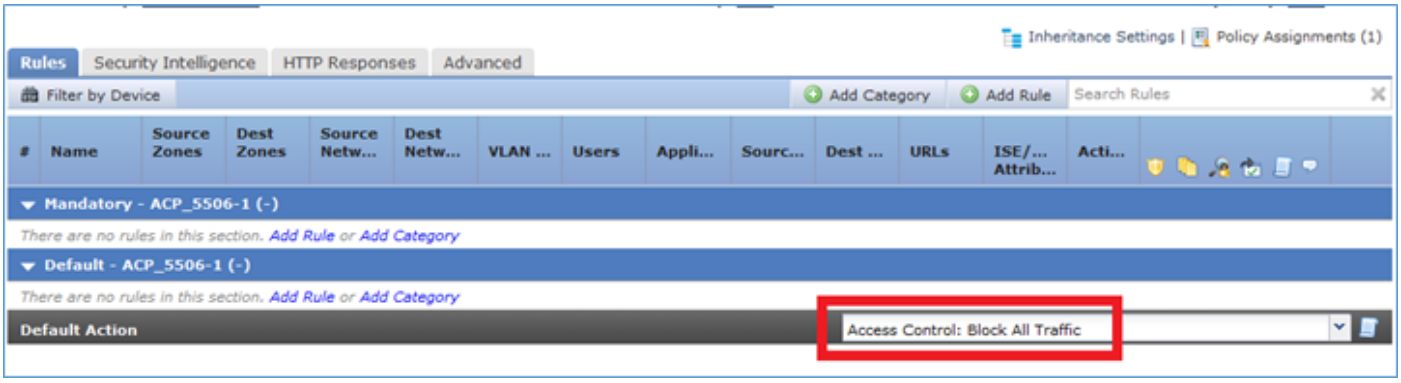


Requisito de la tarea:

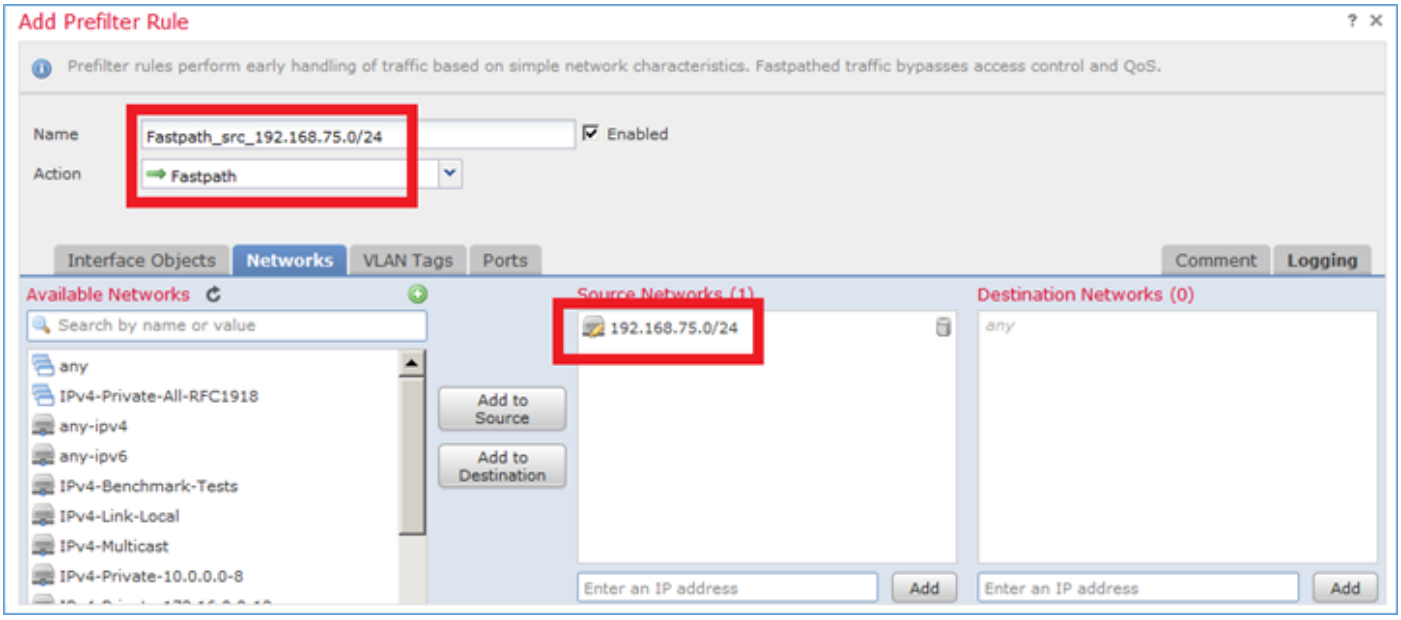
1. Quite las reglas existentes de la directiva del control de acceso y agregue una regla de la directiva del control de acceso que bloquee todo el tráfico.
2. Configure una regla de la directiva de Prefilter que desvíe el motor del Snort para el tráfico originado de la red 192.168.75.0/24.

Solución:

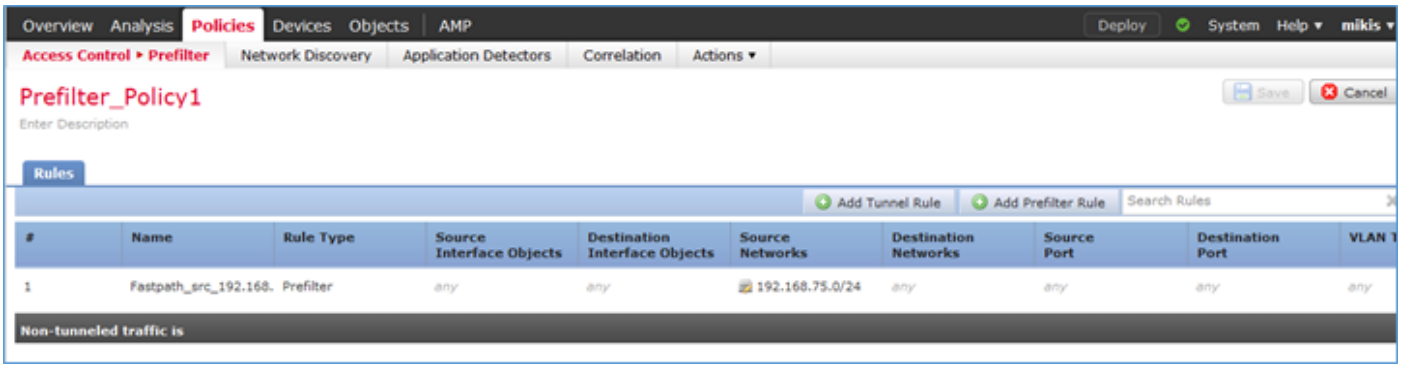
Paso 1. La directiva del control de acceso que bloquea todo el tráfico está tal y como se muestra en de la imagen.



Paso 2. Agregue una regla de Prefilter con el **fastpath** como acción para la red de origen 192.168.75.0/24 tal y como se muestra en de la imagen.



Paso 3. El resultado está tal y como se muestra en de la imagen.



Paso 4. **Salve** y **despliegue**.

Habilite la captura con la traza en ambas interfaces FTD:

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

Intente hacer ping del r1 (192.168.75.39) al r2 (192.168.76.39) con el FTD. El ping falla:

```
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)
```

Captura en las demostraciones de la interfaz interior:

```
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
```

Traza de las primeras demostraciones del paquete (pedido de eco) (puntos importantes resaltados):

Alerón

traza del paquete-número 1 de la captura CAPI de la demostración del firepower#

5 paquetes capturados

1: 23:35:07.281738 192.168.75.39 > 192.168.76.39: ICMP: pedido de eco

Fase: 1

Tipo: CAPTURA

Subtipo:

Resultado: PERMITA

Config:

Información adicional:

Lista de acceso MAC

Fase: 2

Tipo: LISTA DE ACCESO

Subtipo:

Resultado: PERMITA

Config:

Regla implícita

Información adicional:

Lista de acceso MAC

Fase: 3

Tipo: ROUTE-LOOKUP

Subtipo: Interfaz de egreso de la resolución

Resultado: PERMITA

Config:

Información adicional:

Next-Hop encontrado 192.168.76.39 usando el ifc de la salida afuera

Fase: 4

Tipo: LISTA DE ACCESO

Subtipo: registro

Resultado: PERMITA

Config:

acceso-grupo CSM_FW_ACL_ global

IP avanzado 192.168.75.0 255.255.255.0 de la confianza de la lista de acceso CSM_FW_ACL_ cualquier regla-identificación 268434448 registro de acontecimientos ambas

regla-identificación 268434448 de la observación de la lista de acceso CSM_FW_ACL_: DIRECTIVA PREFILTER: Prefilter_Policy1

regla-identificación 268434448 de la observación de la lista de acceso CSM_FW_ACL_: REGLA: Fastpath_src_192.168.75.0/24

Información adicional:

Fase: 5

Tipo: CONN-SETTINGS

Subtipo:

Resultado: PERMITA

Config:

class-default del clase-mapa

haga juego ningunos

global_policy del directiva-mapa

class class-default

fije las avanzado-opciones UM_STATIC_TCP_MAP de la conexión

global_policy de la servicio-directiva global

Información adicional:

Fase: 6

Tipo: NAT

Subtipo: por session

Resultado: PERMITA

Config:

Información adicional:

Fase: 7

Tipo: OPCIONES IP

Subtipo:

Resultado: PERMITA

Config:

Información adicional:

Fase: 8

Tipo: EXAMINE

Subtipo: NP-examine

Resultado: PERMITA

Config:

inspection_default del clase-mapa

 valor por defecto-examen-tráfico de la coincidencia

global_policy del directiva-mapa

 inspection_default de la clase

 examine el ICMP

global_policy de la servicio-directiva global

Información adicional:

Fase: 9

Tipo: EXAMINE

Subtipo: NP-examine

Resultado: PERMITA

Config:

Información adicional:

Fase: 10

Tipo: NAT

Subtipo: por session

Resultado: PERMITA

Config:

Información adicional:

Fase: 11

Tipo: OPCIONES IP

Subtipo:

Resultado: PERMITA

Config:

Información adicional:

Fase: 12

Tipo: FLOW-CREATION

Subtipo:

Resultado: PERMITA

Config:

Información adicional:

El nuevo flujo creado con la identificación 52, paquete envió al módulo siguiente

Fase: 13

Tipo: LISTA DE ACCESO

Subtipo: registro

Resultado: PERMITA

Config:

acceso-grupo CSM_FW_ACL_ global

IP avanzado 192.168.75.0 255.255.255.0 de la confianza de la lista de acceso CSM_FW_ACL_ cualquier regla-identificación 268434448 registro de acontecimientos ambas

regla-identificación 268434448 de la observación de la lista de acceso CSM_FW_ACL_: DIRECTIVA PREFILTER: Prefilter_Policy1

regla-identificación 268434448 de la observación de la lista de acceso CSM_FW_ACL_: REGLA: Fastpath_src_192.168.75.0/24

Información adicional:

Fase: 14

Tipo: CONN-SETTINGS

Subtipo:

Resultado: PERMITA

Config:

class-default del clase-mapa

haga juego ningunos

global_policy del directiva-mapa

class class-default

fije las avanzado-opciones UM_STATIC_TCP_MAP de la conexión

global_policy de la servicio-directiva global

Información adicional:

Fase: 15

Tipo: NAT

Subtipo: por session

Resultado: PERMITA

Config:

Información adicional:

Fase: 16

Tipo: OPCIONES IP

Subtipo:

Resultado: PERMITA

Config:

Información adicional:

Fase: 17

Tipo: ROUTE-LOOKUP

Subtipo: Interfaz de egreso de la resolución

Resultado: PERMITA

Config:

Información adicional:

Next-Hop encontrado 192.168.76.39 usando el ifc de la salida afuera

Fase: 18

Tipo: ADJACENCY-LOOKUP

Subtipo: Next-Hop y adyacencia

Resultado: PERMITA

Config:

Información adicional:

Active de la adyacencia

el MAC address 0004.deab.681b del Next-Hop golpea 140372416161507

Fase: 19

Tipo: CAPTURA

Subtipo:

Resultado: PERMITA

Config:

Información adicional:

Lista de acceso MAC

Resultado:

interfaz de entrada: fuera

entrada-estatus: en funcionamiento

entrada-línea-estatus: en funcionamiento

interfaz de salida: fuera

salida-estatus: en funcionamiento

salida-línea-estatus: en funcionamiento

Acción: permita

1 paquete mostrado

firepower#

los paquetes de la traza 5 del paquete-número 1 de la captura CAPI de la demostración del firepower# capturaron 1: 23:35:07.281738 192.168.75.39 > 192.168.76.39: ICMP: fase del pedido de eco: 1 tipo: Subtipo de la CAPTURA: Resultado: PERMITA los Config: Información adicional: Fase de la lista de acceso MAC: Tipo 2: Subtipo de la LISTA DE ACCESO: Resultado: PERMITA los Config: Información adicional implícita de la regla: Fase de la lista de acceso MAC: Tipo 3: Subtipo ROUTE-LOOKUP: Resultado de la interfaz de egreso de la resolución: PERMITA los Config: Información adicional: Next-Hop encontrado 192.168.76.39 usando el ifc de la salida fuera de la fase: Tipo 4: Subtipo de la LISTA DE ACCESO: resultado del registro: PERMITA los Config: la lista de acceso global CSM_FW_ACL_ del acceso-grupo CSM_FW_ACL_ avanzó el IP 192.168.75.0 255.255.255.0 de la confianza cualquier registro de acontecimientos regla-identificación 268434448 ambos la regla-identificación 268434448 de la observación de la lista de acceso CSM_FW_ACL_: DIRECTIVA PREFILTER: Prefilter_Policy1 regla-identificación 268434448 de la observación de la lista de acceso CSM_FW_ACL_: REGLA: Información adicional Fastpath_src_192.168.75.0/24: Fase: Tipo 5: Subtipo CONN-SETTINGS: Resultado: PERMITA los Config: coincidencia del class-default del clase-mapa cualquier información adicional global del global_policy de la servicio-directiva de las avanzado-opciones UM_STATIC_TCP_MAP de la conexión del conjunto de class class-default del global_policy del directiva-mapa: Fase: Tipo 6: Subtipo NAT: resultado del por session: PERMITA los Config: Información adicional: Fase: Tipo 7: Subtipo de las OPCIONES IP: Resultado: PERMITA los Config: Información adicional: Fase: Tipo 8: EXAMINE el subtipo: NP-examine el resultado: PERMITA los Config: el inspection_default de la clase del global_policy del directiva-mapa del valor por defecto-examen-tráfico de la coincidencia del inspection_default del clase-mapa examina la información adicional global del global_policy de la servicio-directiva ICMP: Fase: Tipo 9: EXAMINE el subtipo: NP-examine el resultado: PERMITA los Config: Información adicional: Fase: Tipo 10: Subtipo NAT: resultado del por session: PERMITA los Config: Información adicional: Fase: Tipo 11: Subtipo de las OPCIONES IP: Resultado: PERMITA los Config: Información adicional: Fase: Tipo 12: Subtipo FLOW-CREATION: Resultado: PERMITA los Config: Información adicional: El nuevo flujo creado con la identificación 52, paquete envió a la fase próxima del módulo: Tipo 13: Subtipo de la LISTA DE ACCESO: resultado del registro: PERMITA los Config: la lista de acceso global CSM_FW_ACL_ del acceso-grupo CSM_FW_ACL_ avanzó el IP 192.168.75.0 255.255.255.0 de la confianza cualquier registro de acontecimientos regla-identificación 268434448 ambos la regla-identificación 268434448 de la observación de la lista de acceso CSM_FW_ACL_: DIRECTIVA PREFILTER: Prefilter_Policy1 regla-identificación 268434448 de la observación de la lista de acceso CSM_FW_ACL_: REGLA: Información adicional Fastpath_src_192.168.75.0/24: Fase: Tipo 14: Subtipo CONN-SETTINGS: Resultado:

PERMITA los Config: coincidencia del class-default del clase-mapa cualquier información adicional global del global_policy de la servicio-directiva de las avanzado-opciones UM_STATIC_TCP_MAP de la conexión del conjunto de class class-default del global_policy del directiva-mapa: Fase: Tipo 15: Subtipo NAT: resultado del por session: PERMITA los Config: Información adicional: Fase: Tipo 16: Subtipo de las OPCIONES IP: Resultado: PERMITA los Config: Información adicional: Fase: Tipo 17: Subtipo ROUTE-LOOKUP: Resultado de la interfaz de egreso de la resolución: PERMITA los Config: Información adicional: Next-Hop encontrado 192.168.76.39 usando el ifc de la salida fuera de la fase: Tipo 18: Subtipo ADJACENCY-LOOKUP: Next-Hop y resultado de la adyacencia: PERMITA los Config: Información adicional: el MAC address activo 0004.deab.681b del Next-Hop de la adyacencia golpea la fase 140372416161507: Tipo 19: Subtipo de la CAPTURA: Resultado: PERMITA los Config: Información adicional: Resultado de la lista de acceso MAC: interfaz de entrada: entrada-estatus exterior: encima del entrada-línea-estatus: encima de la interfaz de salida: salida-estatus exterior: encima del salida-línea-estatus: encima de la acción: permita 1 firepower# mostrado paquete Capture en las demostraciones de la interfaz exterior:

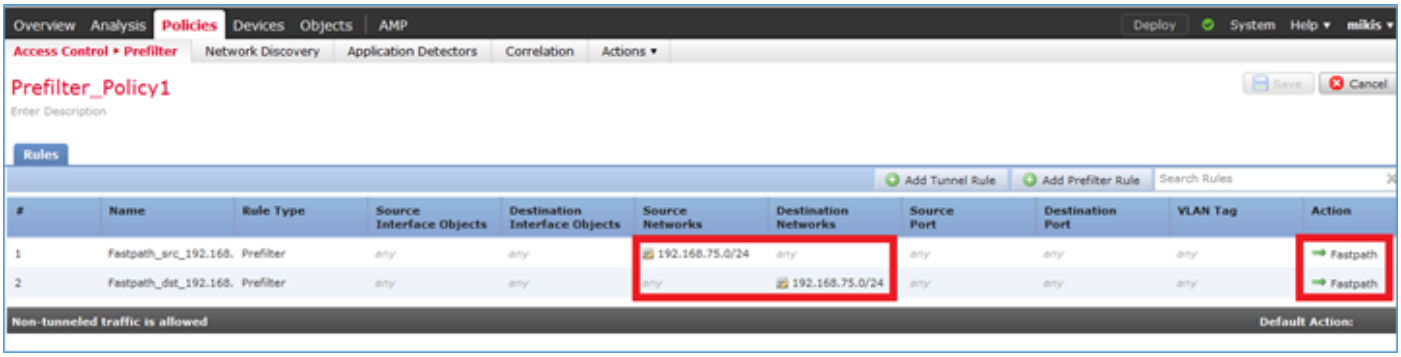
```
firepower# show capture CAPO

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 traza del paquete de devolución muestra que está correspondiendo con el flujo existente (52), pero es bloqueada por el ACL:

```
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, using existing 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 más regla del prefilter para el tráfico de retorno. El resultado está tal y como se muestra en de la imagen.



Ahora localice el paquete de devolución que usted ve (los puntos importantes resaltados):

Alerón

traza del paquete-número 2 de la CEJA de la captura de la demostración del firepower#

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: PERMITA

Config:

Información adicional:

Lista de acceso MAC

Fase: 2

Tipo: LISTA DE ACCESO

Subtipo:

Resultado: PERMITA

Config:

Regla implícita

Información adicional:

Lista de acceso MAC

Fase: 3

Tipo: FLOW-LOOKUP

Subtipo:

Resultado: PERMITA

Config:

Información adicional:

Flujo encontrado con la identificación 62, usando el flujo existente

Fase: 4

Tipo: LISTA DE ACCESO

Subtipo: registro

Resultado: PERMITA

Config:

acceso-grupo CSM_FW_ACL_ global

IP avanzado de la confianza de la lista de acceso CSM_FW_ACL_ cualquier registro de acontecimientos ambos regla-identificación 268434450 de 192.168.75.0 255.255.255.0

regla-identificación 268434450 de la observación de la lista de acceso CSM_FW_ACL_:
DIRECTIVA PREFILTER: Prefilter_Policy1

regla-identificación 268434450 de la observación de la lista de acceso CSM_FW_ACL_: REGLA:

Fastpath_dst_192.168.75.0/24

Información adicional:

Fase: 5

Tipo: CONN-SETTINGS

Subtipo:

Resultado: PERMITA

Config:

class-default del clase-mapa

 haga juego ningunos

global_policy del directiva-mapa

 class class-default

 fije las avanzado-opciones UM_STATIC_TCP_MAP de la conexión

global_policy de la servicio-directiva global

Información adicional:

Fase: 6

Tipo: NAT

Subtipo: por session

Resultado: PERMITA

Config:

Información adicional:

Fase: 7

Tipo: OPCIONES IP

Subtipo:

Resultado: PERMITA

Config:

Información adicional:

Fase: 8

Tipo: ROUTE-LOOKUP

Subtipo: Interfaz de egreso de la resolución

Resultado: PERMITA

Config:

Información adicional:

Next-Hop encontrado 192.168.75.39 usando el ifc de la salida dentro

Fase: 9

Tipo: ADJACENCY-LOOKUP

Subtipo: Next-Hop y adyacencia

Resultado: PERMITA

Config:

Información adicional:

Active de la adyacencia

el MAC address c84c.758d.4981 del Next-Hop golpea 140376711128802

Fase: 10

Tipo: CAPTURA

Subtipo:

Resultado: PERMITA

Config:

Información adicional:

Lista de acceso MAC

Resultado:

interfaz de entrada: dentro

entrada-estatus: en funcionamiento

entrada-línea-estatus: en funcionamiento

interfaz de salida: dentro

salida-estatus: en funcionamiento

salida-línea-estatus: en funcionamiento

Acción: permita

los paquetes de la traza 10 del paquete-número 2 de la CEJA de la captura de la demostración del firepower# capturaron 2: 00:01:38.873123 192.168.76.39 > 192.168.75.39: ICMP: fase de la Respuesta de eco: 1 tipo: Subtipo de la CAPTURA: Resultado: PERMITA los Config: Información adicional: Fase de la lista de acceso MAC: Tipo 2: Subtipo de la LISTA DE ACCESO: Resultado: PERMITA los Config: Información adicional implícita de la regla: Fase de la lista de acceso MAC: Tipo 3: Subtipo FLOW-LOOKUP: Resultado: PERMITA los Config: Información adicional: Flujo encontrado con la identificación 62, usando la fase de flujo existente: Tipo 4: Subtipo de la LISTA DE ACCESO: resultado del registro: PERMITA los Config: la lista de acceso global CSM_FW_ACL_ del acceso-grupo CSM_FW_ACL_ avanzó el IP de la confianza cualquier registro de acontecimientos regla-identificación 268434450 de 192.168.75.0 255.255.255.0 ambos la regla-identificación 268434450 de la observación de la lista de acceso CSM_FW_ACL_: DIRECTIVA PREFILTER: Prefilter_Policy1 regla-identificación 268434450 de la observación de la lista de acceso CSM_FW_ACL_: REGLA: Información adicional Fastpath_dst_192.168.75.0/24: Fase: Tipo 5: Subtipo CONN-SETTINGS: Resultado: PERMITA los Config: coincidencia del class-default del clase-mapa cualquier información adicional global del global_policy de la servicio-directiva de las avanzado-opciones UM_STATIC_TCP_MAP de la conexión del conjunto de class class-default del global_policy del directiva-mapa: Fase: Tipo 6: Subtipo NAT: resultado del por session: PERMITA los Config: Información adicional: Fase: Tipo 7: Subtipo de las OPCIONES IP: Resultado: PERMITA los Config: Información adicional: Fase: Tipo 8: Subtipo ROUTE-LOOKUP: Resultado de la interfaz de egreso de la resolución: PERMITA los Config: Información adicional: Next-Hop encontrado 192.168.75.39 usando el ifc de la salida dentro de la fase: Tipo 9: Subtipo ADJACENCY-LOOKUP: Next-Hop y resultado de la adyacencia: PERMITA los Config: Información adicional: el MAC address activo c84c.758d.4981 del Next-Hop de la adyacencia golpea la fase 140376711128802: Tipo 10: Subtipo de la CAPTURA: Resultado: PERMITA los Config: Información adicional: Resultado de la lista de acceso MAC: interfaz de entrada: entrada-estatus interior: encima del entrada-línea-estatus: encima de la interfaz de salida: salida-estatus interior: encima del salida-línea-estatus: encima de la acción: permita

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

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

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Todas las versiones de la guía de configuración del centro de administración de Cisco FirePOWER se pueden encontrar aquí:

https://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html#id_47280

- El Centro de Asistencia Técnica (TAC) global de Cisco recomienda fuertemente esta guía

visual para el conocimiento práctico profundizado en las tecnologías de seguridad de la última generación de Cisco FirePOWER, incluyendo las que está mencionadas en este artículo: http://www.ciscopress.com/title/9781587144806

- Para toda la configuración y notas técnicas de Troubleshooting: https://www.cisco.com/c/en/us/support/security/defense-center/tsd-products-support-series-home.html

- Soporte Técnico y Documentación - Cisco Systems