Configuração e operação de políticas FTD Prefilter

Índice

[Introdução](#)
[Pré-requisitos](#)
[Requisitos](#)
[Componentes Utilizados](#)
[Informações de Apoio](#)
[Configurar](#)
[caso 1 do uso da política do PRE-filtro](#)
[caso 2 do uso da política do PRE-filtro](#)
[A tarefa 1. verifica a política do PRE-filtro do padrão](#)
[Verificação CLI (LINA)](#)
[Tráfego em túnel do bloco da tarefa 2. com etiqueta](#)
[Motor do Snort do desvio da tarefa 3. com regras de Prefilter do caminho rápido](#)
[Verificar](#)
[Troubleshooting](#)
[Informações Relacionadas](#)

Introdução

Este documento descreve a configuração e a operação de políticas do PRE-filtro da defesa da ameaça de FirePOWER (FTD).

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- ASA5506X que executa o código 6.1.0-195 FTD
- Centro de gerenciamento de FireSIGHT (FMC) essas corridas 6.1.0-195
- Dois 3925 Roteadores de Cisco IOS® que executa 15.2 imagens

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se sua rede está viva, assegure-se de que você compreenda o

impacto potencial do comando any.

Informações de Apoio

Uma política de Prefilter é uma característica introduzida na versão 6.1 e serve três propósitos principais:

1. Combine o tráfego baseado em interno e em cabeçalhos externos
2. Forneça o controle de acesso adiantado que permite que um fluxo contorneie o motor do Snort completamente
3. Trabalhe como um placeholder para as entradas de controle de acesso (ACE) que são migradas da ferramenta adaptável da migração da ferramenta de segurança (ASA).

Tempo da conclusão do laboratório: 30 minutos.

Configurar

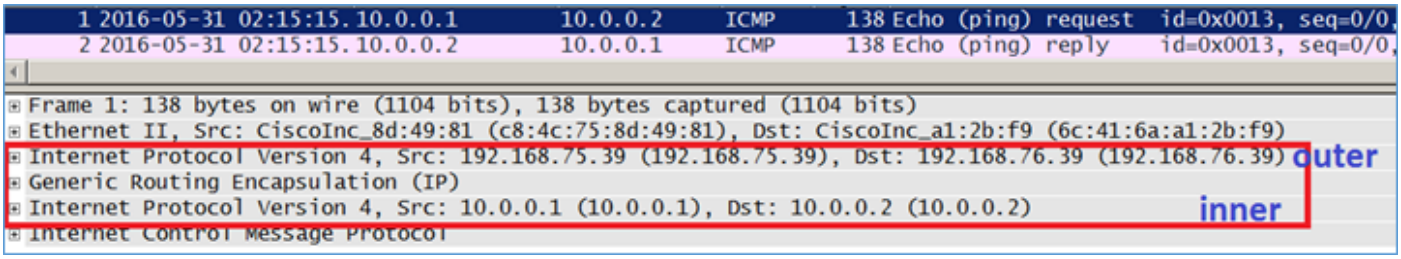
caso 1 do uso da política do PRE-filtro

Uma política do PRE-filtro pode usar um **tipo da regra do túnel** que permita que FTD filtre baseado em ambos internos e/ou no tráfego em túnel exterior do cabeçalho IP. Então este artigo foi escrito, o tráfego em túnel refere:

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

Considere um túnel GRE segundo as indicações da imagem aqui.

Quando você sibila do r1 ao R2 com o uso de um túnel GRE, o tráfego atravessa os olhares do Firewall segundo as indicações da imagem.



Se o Firewall é um **dispositivo ASA,** verifica o **cabeçalho IP exterior** segundo as indicações da imagem.


```
ASA# show conn
GRE OUTSIDE 192.168.76.39:0 INSIDE  192.168.75.39:0, idle 0:00:17, bytes 520, flags
```

Se o Firewall é um **dispositivo de FirePOWER,** verifica o **cabeçalho IP interno** segundo as indicações da imagem.

Com política do PRE-filtro, um dispositivo FTD pode combinar o tráfego baseado em interno e em cabeçalhos externos.

Ponto principal:

Dispositivo	Verificações
ASA	IP exterior
Snort	IP interno
FTD	Exterior (Prefilter) + IP interno (controle de acesso Policy(ACP))

caso 2 do uso da política do PRE-filtro

Uma política do PRE-filtro pode usar um **tipo da regra de Prefilter** que possa fornecer o controle de acesso adiantado e permitir que um fluxo contorneie o motor do Snort completamente segundo as indicações da imagem.

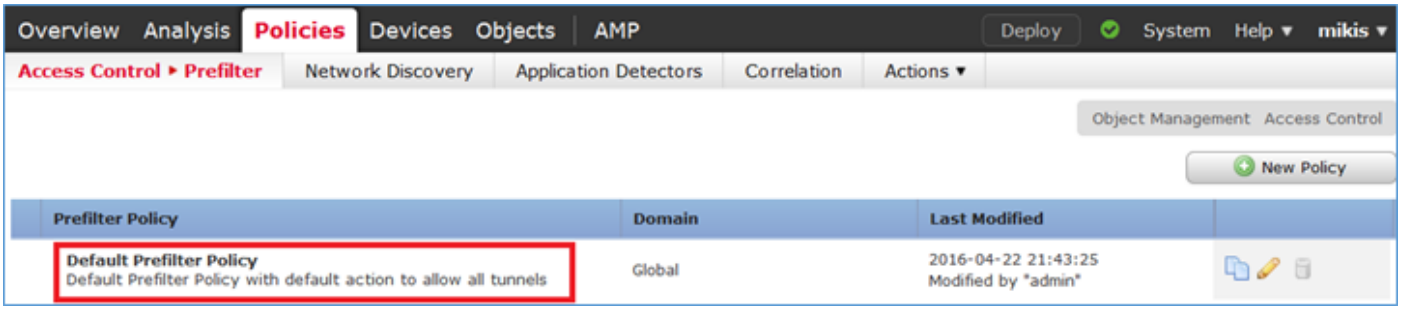
A tarefa 1. verifica a política do PRE-filtro do padrão

Exigência da tarefa:

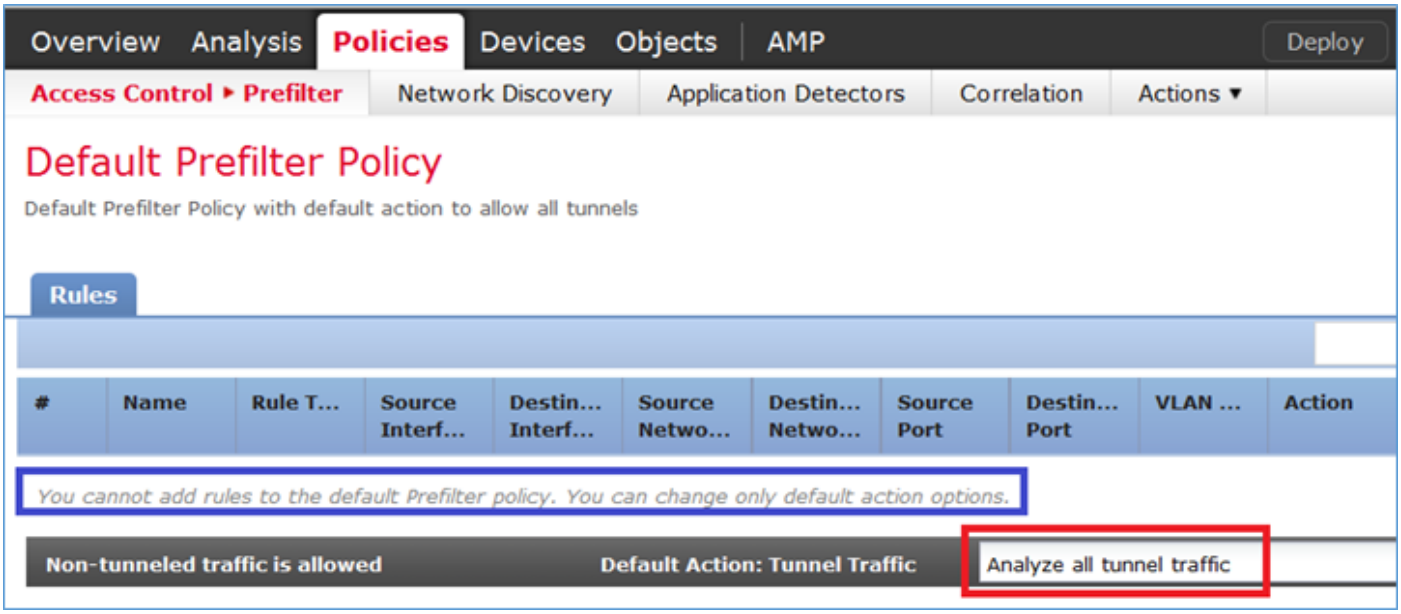
Verifique a política de Prefilter do padrão

Solução:

Etapa 1. Navegue às **políticas > ao controle de acesso > ao Prefilter**. Uma política de Prefilter do padrão já existe segundo as indicações da imagem.



Etapa 2. Seleto **edite** para ver os ajustes da política segundo as indicações da imagem.



Etapa 3. A política do PRE-filtro é anexada já à política do controle de acesso segundo as indicações da imagem.

Verificação CLI (LINA)

as regras do PRE-filtro são adicionadas sobre 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
```

Tráfego em túnel do bloco da tarefa 2. com etiqueta

Exigência da tarefa:

Tráfego do bloco ICMP que é escavado um túnel dentro do túnel GRE.

Solução:

Etapa 1. Se você aplica este o ACP, você pode ver que o tráfego do Internet Control Message Protocol (ICMP) está obstruído, nenhuma matéria se atravessa o túnel GRE ou não, segundo as indicações da imagem.


```
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)
```

Neste caso, você pode usar uma política do PRE-filtro para cumprir a exigência da tarefa. A lógica é como segue:

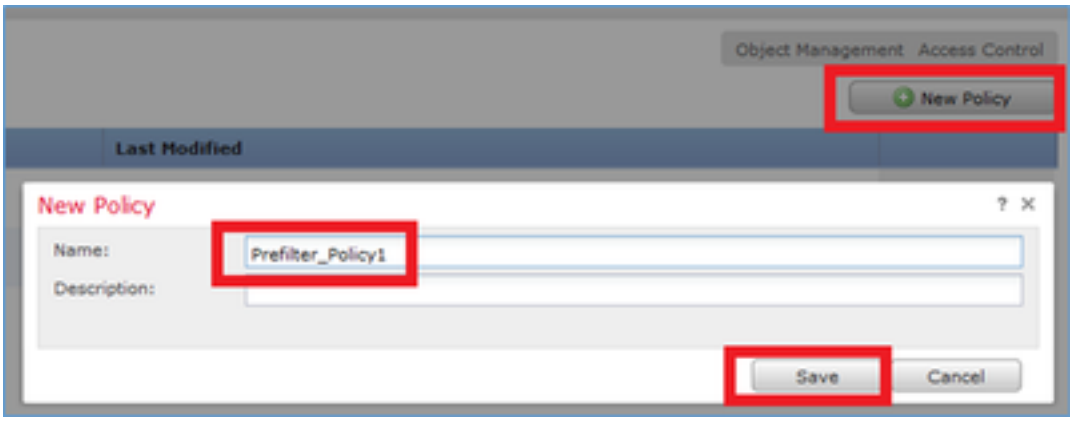
1. Você etiqueta todos os pacotes que são encapsulados dentro do GRE.
2. Você cria uma política do controle de acesso que combine os pacotes rotulados e obstrua o ICMP.

Do ponto de vista da arquitetura, os pacotes são verificados contra as regras do PRE-filtro de

LINA, a seguir roncam regras do PRE-filtro e o ACP e finalmente Snort instrui LINA deixar cair. O primeiro pacote fá-lo através do dispositivo FTD.

Etapa 1. Defina uma etiqueta para o tráfego em túnel.

Navegue às **políticas > ao controle de acesso > ao Prefilter** e crie uma política nova de Prefilter. Recorde que a política de Prefilter do padrão não pode ser editada segundo as indicações da imagem.

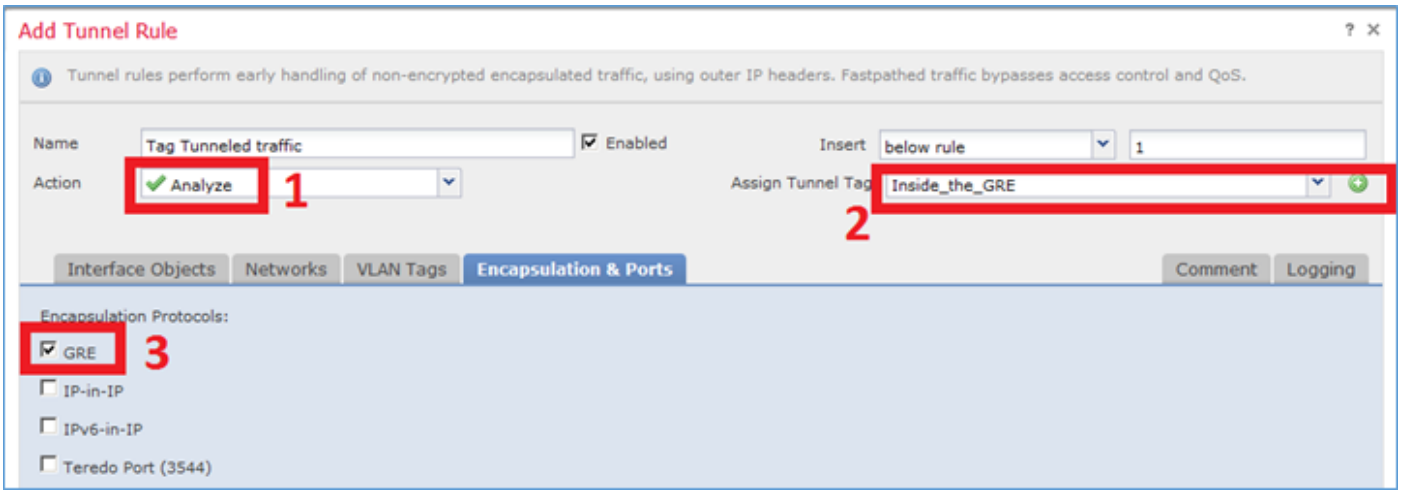


Dentro da política de Prefilter, você pode definir dois tipos de regras:

- Regra do túnel
- Regra de Prefilter

Você pode pensar destes dois como as características totalmente diferentes que podem ser configuradas em uma política de Prefilter.

Para esta tarefa, é necessário definir uma regra do túnel segundo as indicações da imagem.

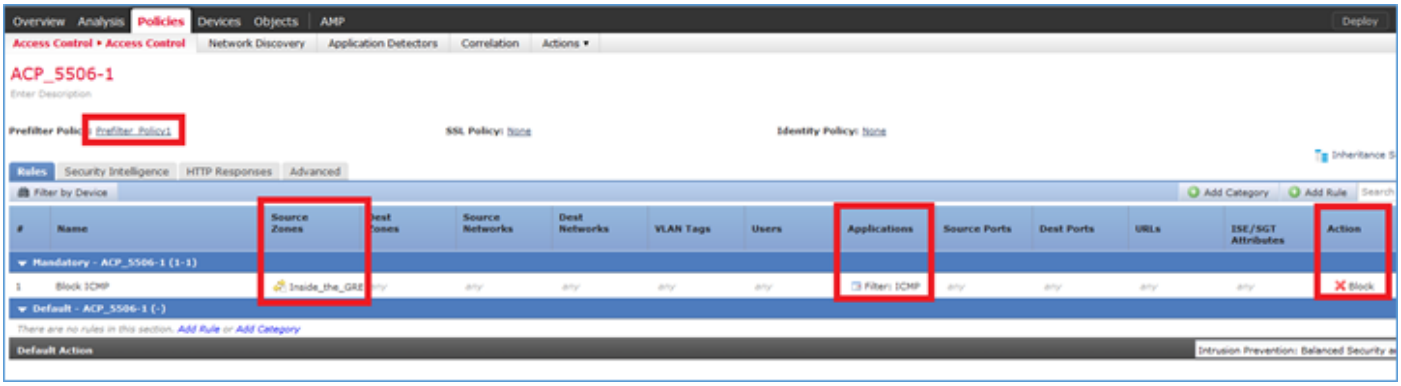


A propósito das ações:

Ação	Descrição
Analise	Após LINA, o fluxo é verificado pelo motor do Snort. Opcionalmente, uma etiqueta do tú pode ser atribuída ao tráfego em túnel.
Bloco	O fluxo é obstruído por LINA. O cabeçalho externo deve ser verificada.
Caminho rápido	O fluxo é segurado somente por LINA sem a necessidade de contratar o motor do Snor

Etapa 2. Defina a política do controle de acesso para o tráfego rotulado.

Embora não possa ser muito intuitivo no início, a etiqueta do túnel pode ser usada por uma regra da política do controle de acesso como uma **zona de origem**. Navegue às **políticas > ao controle de acesso** e crie uma regra que obstrua o ICMP para o tráfego rotulado segundo as indicações da imagem.



Note: A política nova de Prefilter é anexada à política do controle de acesso.

Verificação:

Permita a captação em LINA e em 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
```

Do r1, tente sibilar o valor-limite remoto do túnel GRE. O sibilo falha:

```
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)
```

A captação CLISH mostra que a primeira requisição de eco atravessou FTD e a resposta esteve obstruída:

```
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
```

A captação de LINA confirma esta:

```
> 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
```

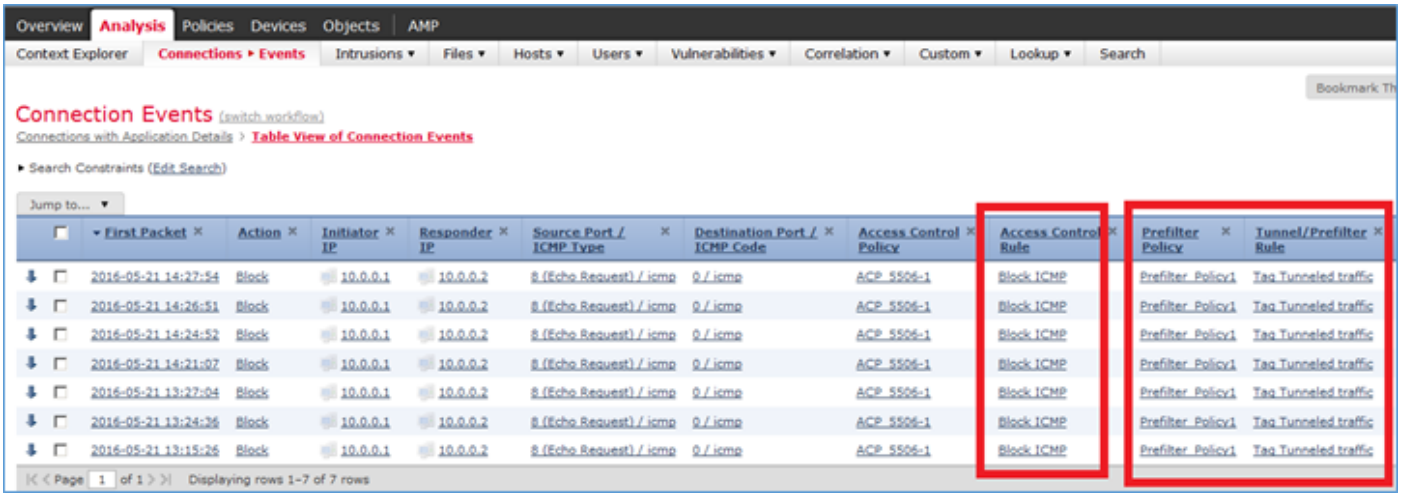
Permita CLISH Firewall-motor-debugam, contadores de queda claros de LINA ASP e fazem o mesmo teste. Os CLISH debugam mostram que para a requisição de eco você combinou a regra do prefilter e para a resposta de eco a regra ACP:

```
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
```

A gota ASP mostra que o Snort deixou cair os pacotes:

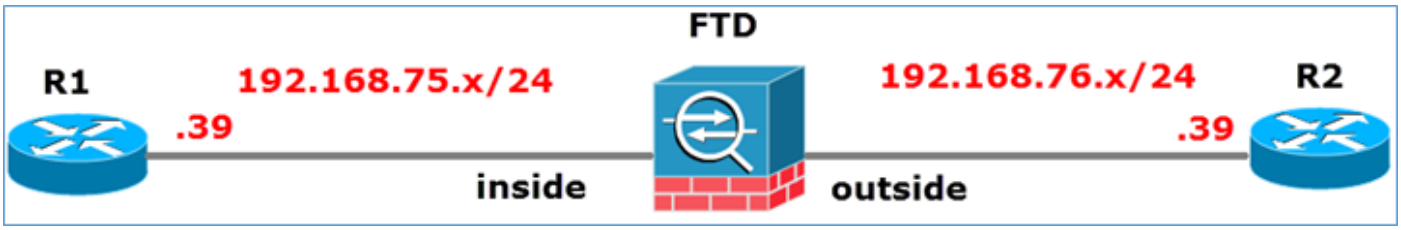
```
> show asp drop

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
```

Nos eventos de conexão, você pode ver a política de Prefilter e ordenar que você combinou segundo as indicações da imagem.



Motor do Snort do desvio da tarefa 3. com regras de Prefilter do caminho rápido

Diagrama de Rede

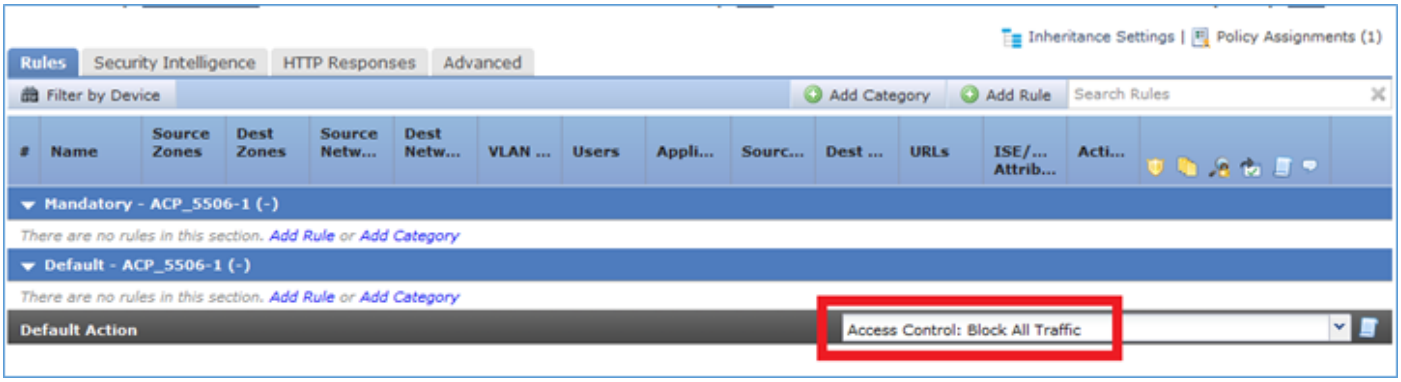


Exigência da tarefa:

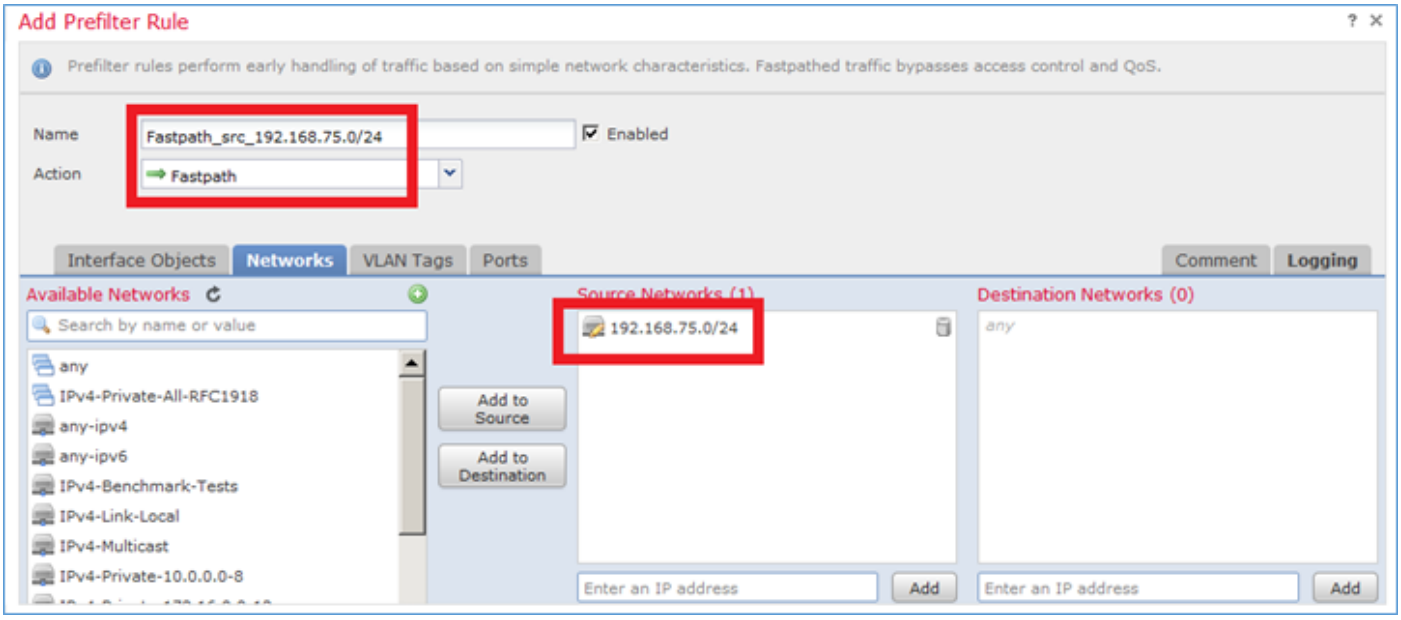
1. Remova as regras existentes da política do controle de acesso e adicionar uma regra da política do controle de acesso que obstrua todo o tráfego.
2. Configurar uma regra da política de Prefilter que contorneie o motor do Snort para o tráfego originado da rede 192.168.75.0/24.

Solução:

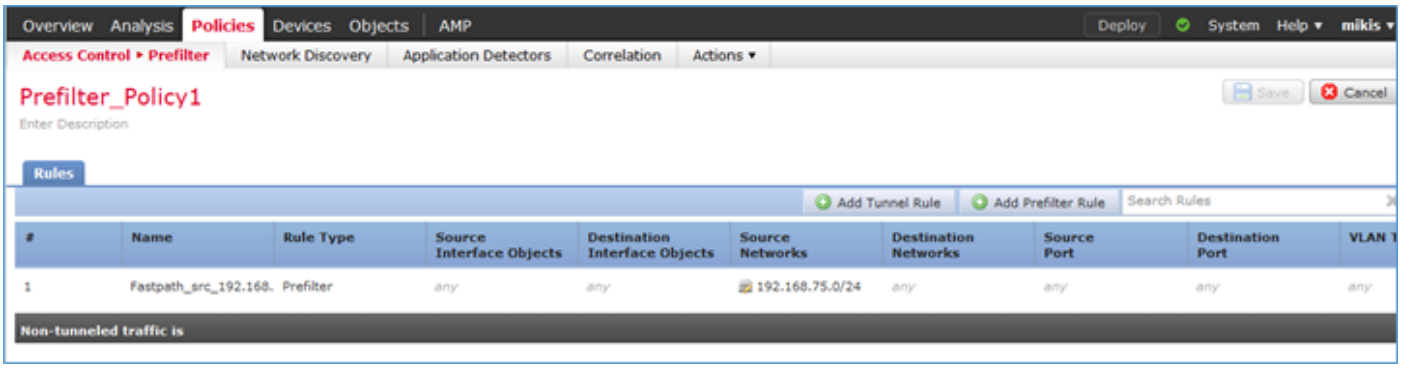
Etapa 1. A política do controle de acesso que obstrui todo o tráfego é segundo as indicações da imagem.



Etapa 2. Adicionar uma regra de Prefilter com **caminho rápido** como uma ação para a rede da fonte 192.168.75.0/24 segundo as indicações da imagem.



Etapa 3. O resultado é segundo as indicações da imagem.



Etapa 4. **Salvar** e **distribua**.

Permita a captação com traço em ambas as relações FTD:

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

Tente sibilar do r1 (192.168.75.39) a R2 (192.168.76.39) com o FTD. O sibilo falha:

```
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)
```

Captação nas mostras da interface interna:

```
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
```

Traço de primeiras mostras do pacote (requisição de eco) (pontos importantes destacados):

Desmancha prazeres
traço do pacote-número 1 da captação CAPI da mostra do firepower#

pacotes 5 capturados

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

Fase: 1

Digite: CAPTAÇÃO

Subtipo:

Resultado: RESERVE

Configuração:

Informações adicionais:

Lista de acessos MAC

Fase: 2

Digite: LISTA DE ACESSO

Subtipo:

Resultado: RESERVE

Configuração:

Regra implícita

Informações adicionais:

Lista de acessos MAC

Fase: 3

Digite: ROUTE-LOOKUP

Subtipo: Interface de saída da resolução

Resultado: RESERVE

Configuração:

Informações adicionais:

salto seguinte encontrado 192.168.76.39 usando o ifc da saída fora

Fase: 4

Digite: LISTA DE ACESSO

Subtipo: log

Resultado: RESERVE

Configuração:

acesso-grupo CSM_FW_ACL_ global

confiança avançada IP 192.168.75.0 255.255.255.0 da lista de acesso CSM_FW_ACL_ algum regra-identificação 268434448 log de eventos ambos

regra-identificação 268434448 da observação da lista de acesso CSM_FW_ACL_: POLÍTICA PREFILTER: Prefilter_Policy1

regra-identificação 268434448 da observação da lista de acesso CSM_FW_ACL_: REGRA: Fastpath_src_192.168.75.0/24

Informações adicionais:

Fase: 5

Digite: CONN-SETTINGS

Subtipo:

Resultado: RESERVE

Configuração:

class-default do mapa de classe

 combine alguns

policy-map global_policy

 class class-default

 ajuste as avançado-opções UM_STATIC_TCP_MAP da conexão

service-policy global_policy global

Informações adicionais:

Fase: 6

Digite: NAT

Subtipo: por sessão

Resultado: RESERVE

Configuração:

Informações adicionais:

Fase: 7

Digite: OPÇÕES IP

Subtipo:

Resultado: RESERVE

Configuração:

Informações adicionais:

Fase: 8

Digite: INSPECIONE

Subtipo: NP-inspecione

Resultado: RESERVE

Configuração:

inspection_default do mapa de classe

 padrão-inspeção-tráfego do fósforo

policy-map global_policy

 inspection_default da classe

 inspecione o ICMP

service-policy global_policy global

Informações adicionais:

Fase: 9

Digite: INSPECIONE

Subtipo: NP-inspecione

Resultado: RESERVE

Configuração:

Informações adicionais:

Fase: 10

Digite: NAT

Subtipo: por sessão

Resultado: RESERVE

Configuração:

Informações adicionais:

Fase: 11

Digite: OPÇÕES IP

Subtipo:

Resultado: RESERVE

Configuração:

Informações adicionais:

Fase: 12

Digite: FLOW-CREATION

Subtipo:

Resultado: RESERVE

Configuração:

Informações adicionais:

O fluxo novo criado com a identificação 52, pacote despachou ao módulo seguinte

Fase: 13

Digite: LISTA DE ACESSO

Subtipo: log

Resultado: RESERVE

Configuração:

acesso-grupo CSM_FW_ACL_ global

confiança avançada IP 192.168.75.0 255.255.255.0 da lista de acesso CSM_FW_ACL_ algum regra-identificação 268434448 log de eventos ambos

regra-identificação 268434448 da observação da lista de acesso CSM_FW_ACL_: POLÍTICA PREFILTER: Prefilter_Policy1

regra-identificação 268434448 da observação da lista de acesso CSM_FW_ACL_: REGRA: Fastpath_src_192.168.75.0/24

Informações adicionais:

Fase: 14

Digite: CONN-SETTINGS

Subtipo:

Resultado: RESERVE

Configuração:

class-default do mapa de classe

 combine alguns

policy-map global_policy

 class class-default

 ajuste as avançado-opções UM_STATIC_TCP_MAP da conexão

service-policy global_policy global

Informações adicionais:

Fase: 15

Digite: NAT

Subtipo: por sessão

Resultado: RESERVE

Configuração:

Informações adicionais:

Fase: 16

Digite: OPÇÕES IP

Subtipo:

Resultado: RESERVE

Configuração:

Informações adicionais:

Fase: 17

Digite: ROUTE-LOOKUP

Subtipo: Interface de saída da resolução

Resultado: RESERVE

Configuração:

Informações adicionais:

salto seguinte encontrado 192.168.76.39 usando o ifc da saída fora

Fase: 18

Digite: ADJACENCY-LOOKUP

Subtipo: salto seguinte e adjacência

Resultado: RESERVE

Configuração:

Informações adicionais:

Active da adjacência

o MAC address 0004.deab.681b do salto seguinte bate 140372416161507

Fase: 19

Digite: CAPTAÇÃO

Subtipo:

Resultado: RESERVE

Configuração:

Informações adicionais:

Lista de acessos MAC

Resultado:

interface de entrada: externa

entrada-estado: up

entrada-linha-estado: up

interface de saída: externa

saída-estado: up

saída-linha-estado: up

Ação: reserve

1 pacote mostrado

firepower#

os pacotes do traço 5 do pacote-número 1 da captação CAPI da mostra do firepower# capturaram 1: 23:35:07.281738 192.168.75.39 > 192.168.76.39: ICMP: fase da requisição de eco: 1 tipo: Subtipo da CAPTAÇÃO: Resultado: PERMITA a configuração: Informações adicionais: Fase da lista de acessos MAC: Tipo 2: Subtipo da LISTA DE ACESSO: Resultado: PERMITA a configuração: Informação adicional implícita da regra: Fase da lista de acessos MAC: Tipo 3: Subtipo ROUTE-LOOKUP: Resultado da interface de saída da resolução: PERMITA a configuração: Informações adicionais: salto seguinte encontrado 192.168.76.39 usando o ifc da saída fora da fase: Tipo 4: Subtipo da LISTA DE ACESSO: resultado do log: PERMITA a configuração: a lista de acesso global CSM_FW_ACL_ do acesso-grupo CSM_FW_ACL_ avançou a confiança IP 192.168.75.0 255.255.255.0 todo o log de eventos regra-identificação 268434448 ambos os a regra-identificação 268434448 da observação da lista de acesso CSM_FW_ACL_: POLÍTICA PREFILTER: Prefilter_Policy1 regra-identificação 268434448 da observação da lista de acesso CSM_FW_ACL_: REGRA: Informação adicional Fastpath_src_192.168.75.0/24: Fase: Tipo 5: Subtipo CONN-SETTINGS: Resultado: PERMITA a configuração: fósforo do class-default do mapa de classe alguma informação adicional global do global_policy da serviço-política das avançado-opções UM_STATIC_TCP_MAP da conexão do grupo de class class-default do global_policy do mapa de política: Fase: Tipo 6: Subtipo NAT: por sessão resultado: PERMITA a configuração: Informações adicionais: Fase: Tipo 7: Subtipo das OPÇÕES IP: Resultado: PERMITA a configuração: Informações adicionais: Fase: Tipo 8: INSPECIONE o subtipo: NP-inspecione o resultado: PERMITA a configuração: o inspection_default da classe do global_policy do mapa de política do padrão-inspeção-tráfego do fósforo do inspection_default do mapa de classe inspeciona a informação adicional global do global_policy da serviço-política ICMP: Fase: Tipo 9: INSPECIONE o subtipo: NP-inspecione o resultado: PERMITA a configuração: Informações adicionais: Fase: Tipo 10: Subtipo NAT: por sessão resultado: PERMITA a configuração: Informações adicionais: Fase: Tipo 11: Subtipo das OPÇÕES IP: Resultado: PERMITA a configuração: Informações adicionais: Fase: Tipo 12: Subtipo FLOW-CREATION: Resultado: PERMITA a configuração: Informações adicionais: O fluxo novo criado com a identificação 52, pacote despachou à próxima fase do módulo: Tipo 13: Subtipo da LISTA DE ACESSO: resultado do log: PERMITA a configuração: a lista de acesso global CSM_FW_ACL_ do acesso-grupo CSM_FW_ACL_ avançou a confiança IP 192.168.75.0 255.255.255.0 todo o log de eventos regra-identificação 268434448 ambos os a regra-identificação 268434448 da observação da lista de acesso CSM_FW_ACL_: POLÍTICA PREFILTER: Prefilter_Policy1 regra-identificação 268434448 da observação da lista de acesso CSM_FW_ACL_: REGRA: Informação adicional Fastpath_src_192.168.75.0/24: Fase: Tipo 14: Subtipo CONN-SETTINGS: Resultado: PERMITA a configuração: fósforo do class-default do mapa de classe alguma informação adicional global do global_policy da serviço-política das avançado-opções UM_STATIC_TCP_MAP da conexão do grupo de class class-default do global_policy do mapa de política: Fase: Tipo 15: Subtipo NAT:

por sessão resultado: PERMITA a configuração: Informações adicionais: Fase: Tipo 16: Subtipo das OPÇÕES IP: Resultado: PERMITA a configuração: Informações adicionais: Fase: Tipo 17: Subtipo ROUTE-LOOKUP: Resultado da interface de saída da resolução: PERMITA a configuração: Informações adicionais: salto seguinte encontrado 192.168.76.39 usando o ifc da saída fora da fase: Tipo 18: Subtipo ADJACENCY-LOOKUP: salto seguinte e resultado da adjacência: PERMITA a configuração: Informações adicionais: o MAC address ativo 0004.deab.681b do salto seguinte da adjacência bate a fase 140372416161507: Tipo 19: Subtipo da CAPTAÇÃO: Resultado: PERMITA a configuração: Informações adicionais: Resultado da lista de acessos MAC: interface de entrada: entrada-estado exterior: acima do entrada-linha-estado: acima da interface de saída: saída-estado exterior: acima do saída-linha-estado: acima da ação: permita 1 firepower# mostrado pacote

Capture nas mostras da interface externa:

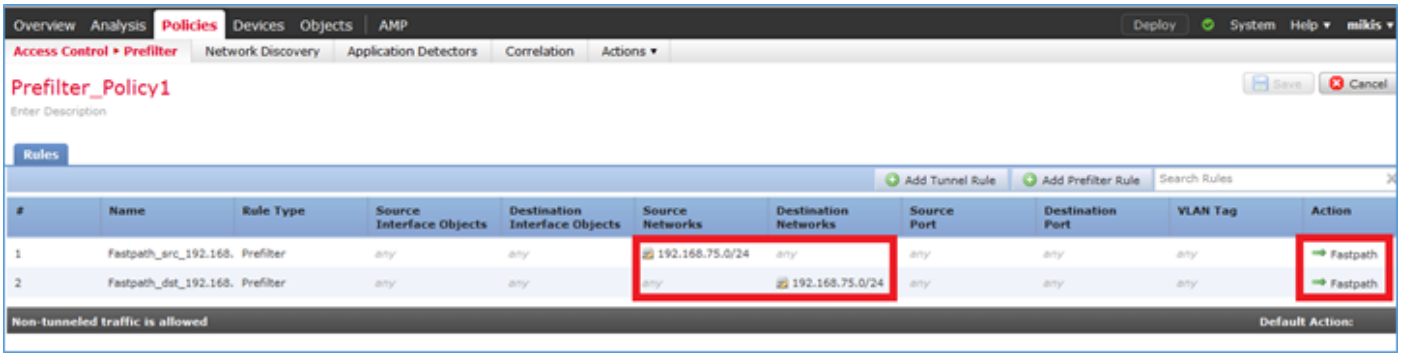
```
firepower# show capture CAPO

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
```

O traço do pacote de informação de retorno mostra que está combinando o fluxo existente (52), mas é obstruído pelo 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
```

Etapa 5. Adicionar uma mais regra do prefilter para o tráfego de retorno. O resultado é segundo as indicações da imagem.



Siga agora o pacote de informação de retorno que você vê (os pontos importantes destacados):

Desmancha prazeres
traço do pacote-número 2 do CAPO da captação da mostra do firepower#

pacotes 10 capturados

2: 00:01:38.873123 192.168.76.39 > 192.168.75.39: ICMP: resposta de eco

Fase: 1

Digite: CAPTAÇÃO

Subtipo:

Resultado: RESERVE

Configuração:

Informações adicionais:

Lista de acessos MAC

Fase: 2

Digite: LISTA DE ACESSO

Subtipo:

Resultado: RESERVE

Configuração:

Regra implícita

Informações adicionais:

Lista de acessos MAC

Fase: 3

Digite: FLOW-LOOKUP

Subtipo:

Resultado: RESERVE

Configuração:

Informações adicionais:

Fluxo encontrado com identificação 62, usando o fluxo existente

Fase: 4

Digite: LISTA DE ACESSO

Subtipo: log

Resultado: RESERVE

Configuração:

acesso-grupo CSM_FW_ACL_ global

confiança avançada IP da lista de acesso CSM_FW_ACL_ algum log de eventos ambos regra-identificação 268434450 de 192.168.75.0 255.255.255.0

regra-identificação 268434450 da observação da lista de acesso CSM_FW_ACL_: POLÍTICA PREFILTER: Prefilter_Policy1

regra-identificação 268434450 da observação da lista de acesso CSM_FW_ACL_: REGRA: Fastpath_dst_192.168.75.0/24

Informações adicionais:

Fase: 5

Digite: CONN-SETTINGS

Subtipo:

Resultado: RESERVE

Configuração:

class-default do mapa de classe

 combine alguns

policy-map global_policy

 class class-default

 ajuste as avançado-opções UM_STATIC_TCP_MAP da conexão

service-policy global_policy global

Informações adicionais:

Fase: 6

Digite: NAT

Subtipo: por sessão

Resultado: RESERVE

Configuração:

Informações adicionais:

Fase: 7

Digite: OPÇÕES IP

Subtipo:

Resultado: RESERVE

Configuração:

Informações adicionais:

Fase: 8

Digite: ROUTE-LOOKUP

Subtipo: Interface de saída da resolução

Resultado: RESERVE

Configuração:

Informações adicionais:

salto seguinte encontrado 192.168.75.39 usando o ifc da saída para dentro

Fase: 9

Digite: ADJACENCY-LOOKUP

Subtipo: salto seguinte e adjacência

Resultado: RESERVE

Configuração:

Informações adicionais:

Active da adjacência

o MAC address c84c.758d.4981 do salto seguinte bate 140376711128802

Fase: 10

Digite: CAPTAÇÃO

Subtipo:

Resultado: RESERVE

Configuração:

Informações adicionais:

Lista de acessos MAC

Resultado:

interface de entrada: interna

entrada-estado: up

entrada-linha-estado: up

interface de saída: interna

saída-estado: up

saída-linha-estado: up

Ação: reserve

os pacotes do traço 10 do pacote-número 2 do CAPO da captação da mostra do firepower# capturaram 2: 00:01:38.873123 192.168.76.39 > 192.168.75.39: ICMP: fase da resposta de eco: 1 tipo: Subtipo da CAPTAÇÃO: Resultado: PERMITA a configuração: Informações adicionais: Fase da lista de acessos MAC: Tipo 2: Subtipo da LISTA DE ACESSO: Resultado: PERMITA a configuração: Informação adicional implícita da regra: Fase da lista de acessos MAC: Tipo 3: Subtipo FLOW-LOOKUP: Resultado: PERMITA a configuração: Informações adicionais: Fluxo encontrado com identificação 62, usando a fase de fluxo existente: Tipo 4: Subtipo da LISTA DE ACESSO: resultado do log: PERMITA a configuração: a lista de acesso global CSM_FW_ACL_ do acesso-grupo CSM_FW_ACL_ avançou a confiança IP todo o log de eventos regra-identificação 268434450 de 192.168.75.0 255.255.255.0 ambos os a regra-identificação 268434450 da observação da lista de acesso CSM_FW_ACL_: POLÍTICA PREFILTER: Prefilter_Policy1 regra-identificação 268434450 da observação da lista de acesso CSM_FW_ACL_: REGRA: Informação adicional Fastpath_dst_192.168.75.0/24: Fase: Tipo 5: Subtipo CONN-SETTINGS: Resultado: PERMITA a configuração: fósforo do class-default do mapa de classe alguma informação adicional global do global_policy da serviço-política das avançado-opções UM_STATIC_TCP_MAP da conexão do grupo de class class-default do global_policy do mapa de política: Fase: Tipo 6: Subtipo NAT: por sessão resultado: PERMITA a configuração: Informações adicionais: Fase: Tipo 7: Subtipo das OPÇÕES IP: Resultado: PERMITA a configuração: Informações adicionais: Fase: Tipo 8: Subtipo ROUTE-LOOKUP: Resultado da interface de saída da resolução: PERMITA a configuração: Informações adicionais: salto seguinte encontrado 192.168.75.39 usando o ifc da saída dentro da fase: Tipo 9: Subtipo ADJACENCY-LOOKUP: salto seguinte e resultado da adjacência: PERMITA a configuração: Informações adicionais: o MAC address ativo c84c.758d.4981 do salto seguinte da adjacência bate a fase 140376711128802: Tipo 10: Subtipo da CAPTAÇÃO: Resultado: PERMITA a configuração: Informações adicionais: Resultado da lista de acessos MAC: interface de entrada: entrada-estado interno: acima do entrada-linha-estado: acima da interface de saída: saída-estado interno: acima do saída-linha-estado: acima da ação: reserve

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A verificação foi explicada nas seções respectivas das tarefas.

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- Todas as versões do manual de configuração do centro de gerenciamento de Cisco FirePOWER podem ser encontradas aqui:

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

- O centro de assistência técnica (TAC) global de Cisco recomenda fortemente este guia visual para o conhecimento prático detalhado em tecnologias de segurança da próxima geração de

Cisco FirePOWER, incluindo esses mencionados neste artigo:
http://www.ciscopress.com/title/9781587144806

- Para toda a configuração e TechNotes do Troubleshooting:
https://www.cisco.com/c/en/us/support/security/defense-center/tsd-products-support-series-home.html

- Suporte Técnico e Documentação - Cisco Systems