設定和操作FTD預過濾器原則

目錄

簡介

必要條件

- 需求
- 採用元件

背景資訊

設定

- 預過濾器策略使用案例1
- 預過濾器策略使用案例2

任務1.驗證預設PreFilter策略

- CLI(LINA)驗證

簡介

本檔案介紹Firepower威脅防禦(FTD)預過濾器策略的設定和操作。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 執行FTD代碼6.1.0-195的ASA5506X
- 運行6.1.0-195的FireSIGHT管理中心(FMC)
- 兩台運行15.2映像的3925 Cisco IOS®路由器

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

預過濾器策略是6.1版中引入的一項功能，主要有三個用途：

1. 根據內部報頭和外部報頭匹配流量
2. 提供早期訪問控制，允許流量完全繞過Snort引擎
3. 充當從自適應安全裝置(ASA)遷移工具遷移的訪問控制項目(ACE)的佔位符。

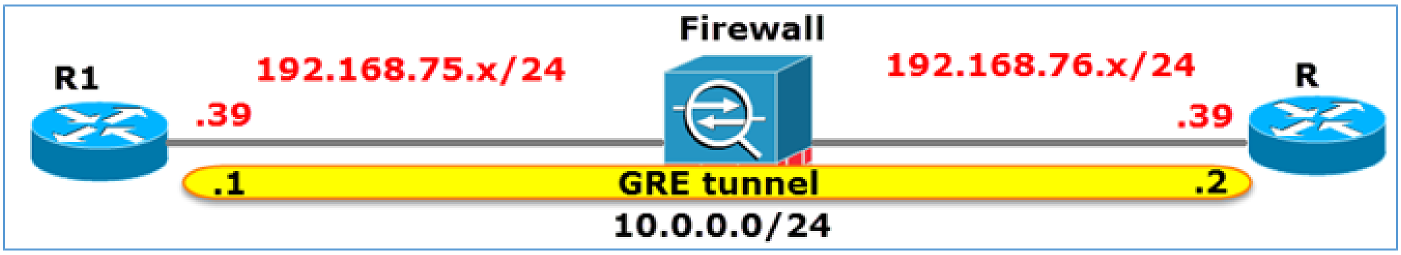
設定

預過濾器策略使用案例1

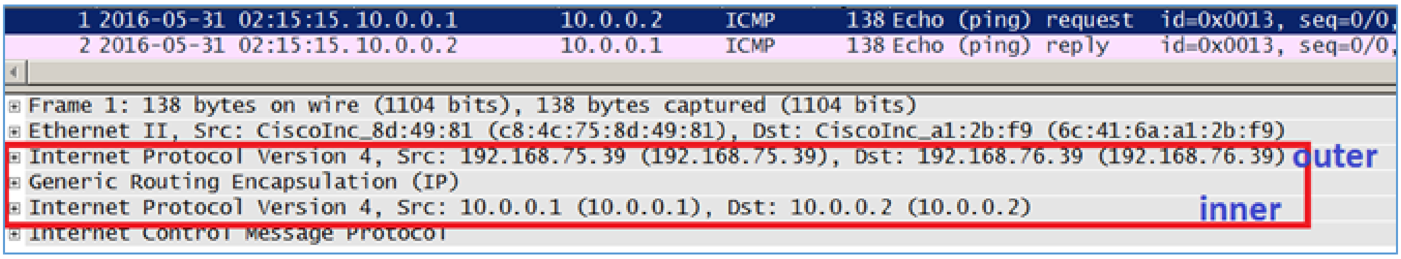
預過濾器策略可以使用允許FTD根據內部和/或外部IP標頭通道流量的通道規則型別。在撰寫本文時，隧道流量是指：

- 通用路由封裝(GRE)
- IP-in-IP
- IPv6-in-IP
- Teredo 連接埠 3544

請考慮GRE通道，如圖所示。

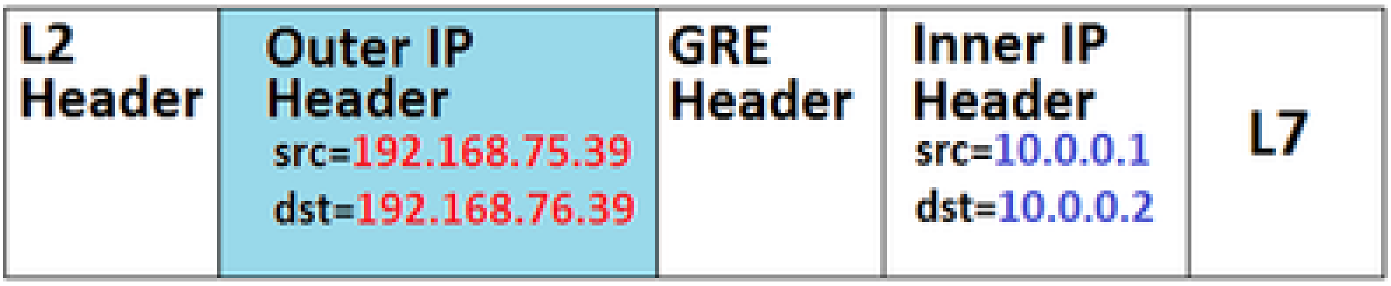


使用GRE通道從R1 ping R2時，流量會通過防火牆，如下圖所示。



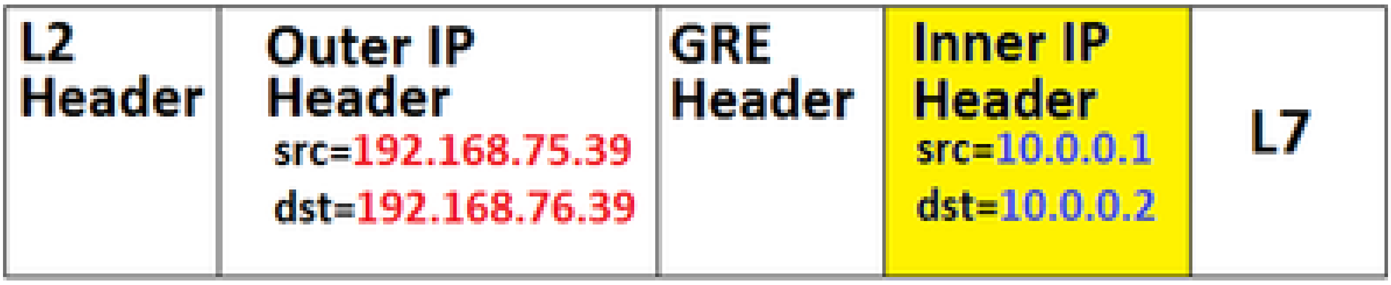
```
1 2016-05-31 02:15:15.10.0.0.1        10.0.0.2    ICMP    138 Echo (ping) request   id=0x0013, seq=0/0,
2 2016-05-31 02:15:15.10.0.0.2        10.0.0.1    ICMP    138 Echo (ping) reply     id=0x0013, seq=0/0,

⊞ Frame 1: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits)
⊞ Ethernet II, Src: CiscoInc_8d:49:81 (c8:4c:75:8d:49:81), Dst: CiscoInc_a1:2b:f9 (6c:41:6a:a1:2b:f9)
⊞ Internet Protocol Version 4, Src: 192.168.75.39 (192.168.75.39), Dst: 192.168.76.39 (192.168.76.39)
⊞ Generic Routing Encapsulation (IP)
⊞ Internet Protocol Version 4, Src: 10.0.0.1 (10.0.0.1), Dst: 10.0.0.2 (10.0.0.2)
⊞ Internet Control Message Protocol
```

如果防火牆是ASA裝置，則會檢查外部IP報頭，如下圖所示。



```
<#root>

ASA#

show conn

GRE OUTSIDE 192.168.76.39:0 INSIDE  192.168.75.39:0

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

如果防火牆是FirePOWER裝置，它會檢查內部IP報頭，如下圖所示。



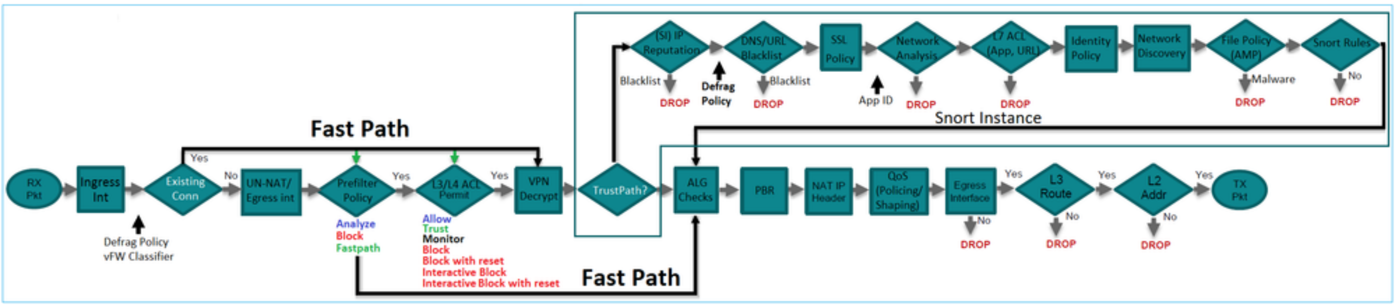
使用預過濾器策略，FTD裝置可以基於內部標頭和外部標頭來匹配流量。

要點：

裝置	支票
ASA	外部IP
Snort	內部IP
FTD	外部（預過濾器）+內部IP(存取控制原則(ACP))

預過濾器策略使用案例2

預過濾器策略可以使用預過濾器規則型別，該規則型別可以提供早期訪問控制並允許流完全繞過Snort引擎，如圖所示。



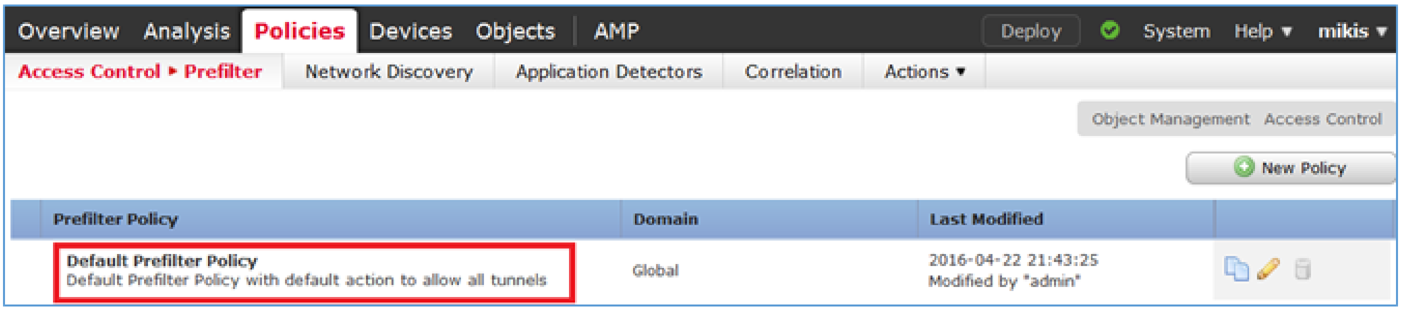
任務1.驗證預設PreFilter策略

工作需求：

驗證預設預過濾器策略

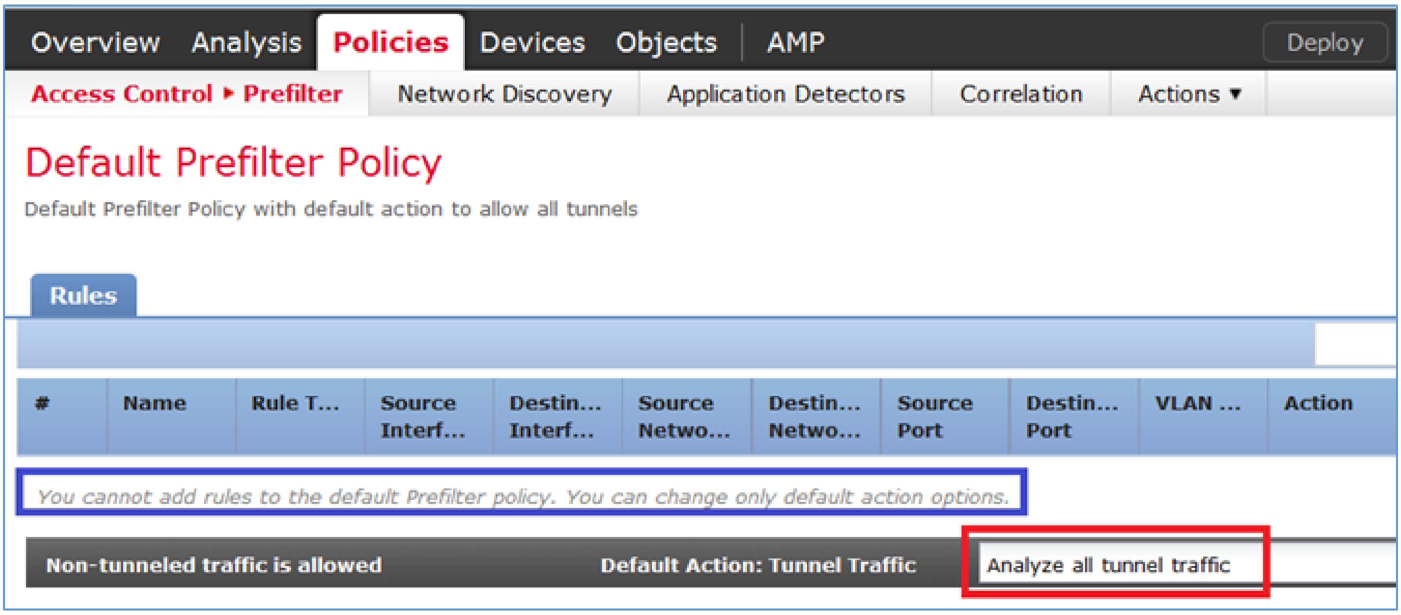
解決方案：

步驟 1.導覽至Policies > Access Control > Prefilter。預設預過濾器策略已存在，如圖所示。



Prefilter Policy	Domain	Last Modified
Default Prefilter Policy Default Prefilter Policy with default action to allow all tunnels	Global	2016-04-22 21:43:25 Modified by "admin"

步驟 2.選擇Edit以檢視策略設定，如下圖所示。



Default Prefilter Policy

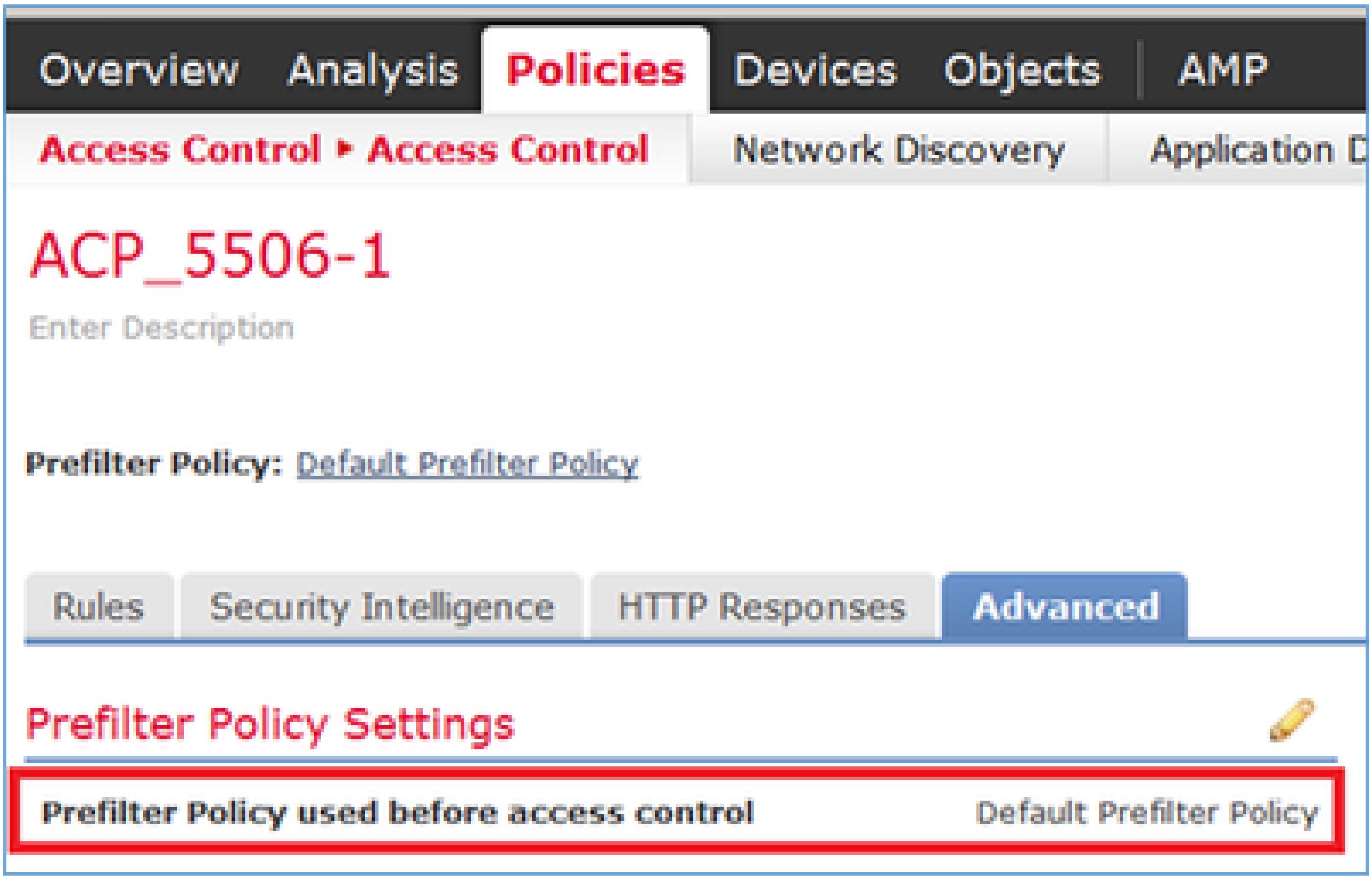
Default Prefilter Policy with default action to allow all tunnels

#	Name	Rule T...	Source Interf...	Destin... Interf...	Source Netwo...	Destin... Netwo...	Source Port	Destin... Port	VLAN ...	Action

You cannot add rules to the default Prefilter policy. You can change only default action options.

Non-tunneled traffic is allowed   Default Action: Tunnel Traffic   Analyze all tunnel traffic

步驟 3.預過濾器策略已附加到訪問控制策略，如圖所示。



ACP_5506-1

Enter Description

Prefilter Policy: Default Prefilter Policy

Prefilter Policy Settings

Prefilter Policy used before access control   Default Prefilter Policy

CLI(LINA)驗證

預過濾器規則新增到ACL的頂部：

<#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
```

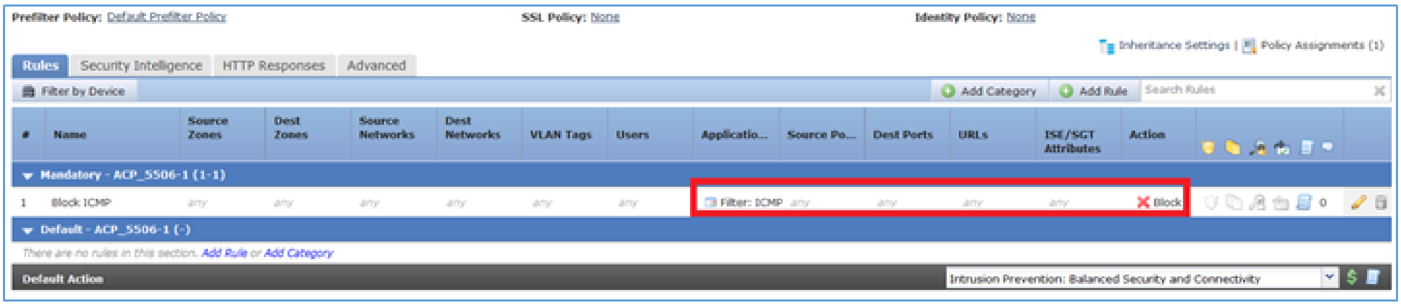
任務2.使用標籤阻止隧道流量

工作需求：

封鎖在GRE通道中通道傳輸的ICMP流量。

解決方案：

步驟 1.如果套用這些ACP，您可以看到網際網路控制訊息通訊協定(ICMP)流量無論是否通過GRE通道都會遭到封鎖，如圖所示。



Prefilter Policy: Default Prefilter Policy   SSL Policy: None   Identity Policy: None

Inheritance Settings | Policy Assignments (1)

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicatio...	Source Po...	Dest Ports	URLs	ISE/SGT Attributes	Action	
▼ Mandatory - ACP_5506-1 (1-1)														
1	Block ICMP	any	any	any	any	any	any	Filter: ICMP	any	any	any	any	✖ Block	0
▼ Default - ACP_5506-1 (-)														
There are no rules in this section. Add Rule or Add Category														

Default Action: Intrusion Prevention: Balanced Security and Connectivity

<#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)
```

在這種情況下，您可以使用預過濾器策略來滿足任務要求。其邏輯如下：

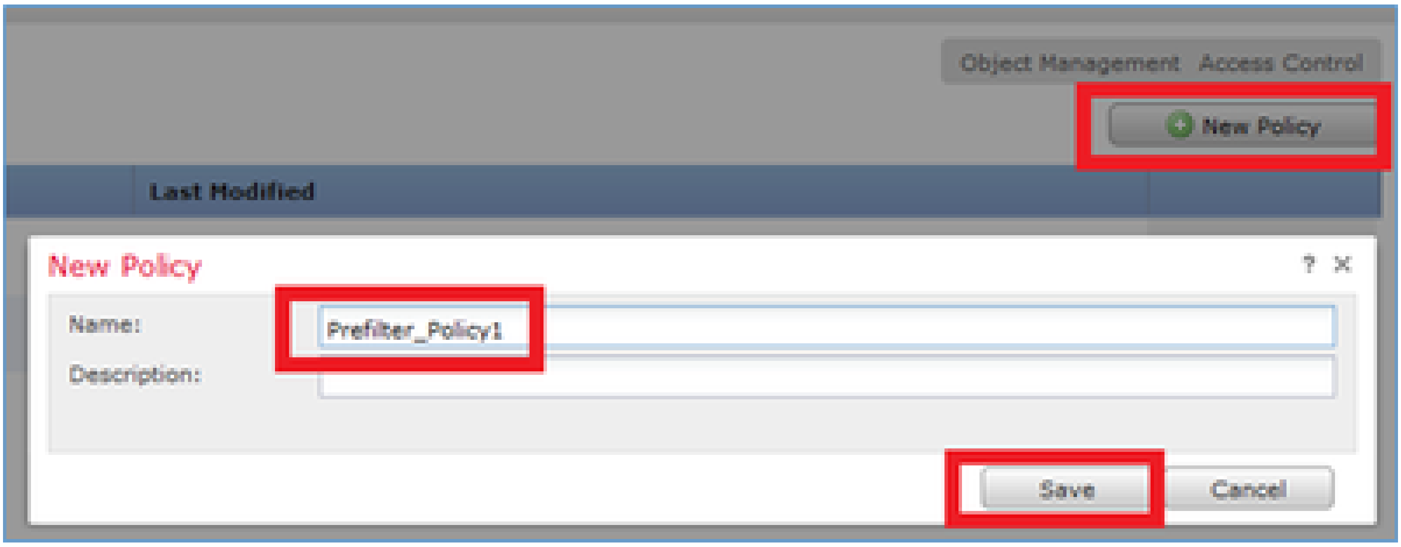
1. 您可以標籤封裝在GRE中的所有資料包。
2. 建立與標籤的資料包匹配並阻止ICMP的訪問控制策略。

從架構的角度來看，會根據LINUX NAelly(LINA)預過濾器規則檢查封包，然後是Snort預過濾器規則和ACP，最後是Snort指示LINA捨棄。第一個封包會通過FTD裝置。

步驟 1.定義隧道流量的標籤。

導覽至Policies > Access Control > Prefilter，然後建立新的預過濾器策略。請記住，不能編輯預設

預過濾器策略，如下圖所示。



New Policy

Name: Prefilter_Policy1

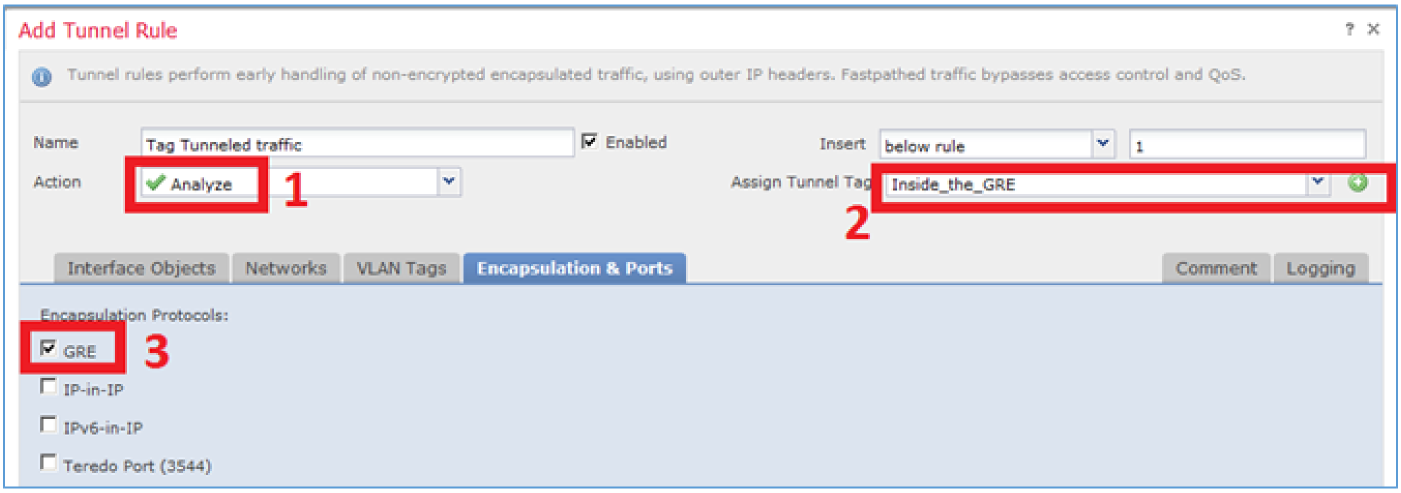
Description:

在預過濾器策略中，可以定義兩種型別的規則：

1. 通道規則
2. 預過濾器規則

可以將這兩個功能視為可在預過濾器策略中配置的完全不同的功能。

對於此任務，必須定義隧道規則，如下圖所示。


Add Tunnel Rule

Tunnel rules perform early handling of non-encrypted encapsulated traffic, using outer IP headers. Fastpathed traffic bypasses access control and QoS.

Name: Tag Tunneled traffic

☑ Enabled

Insert: below rule, 1

Action: Analyze

Assign Tunnel Tag: Inside_the_GRE

Encapsulation Protocols:

☑ GRE
□ IP-in-IP
□ IPv6-in-IP
□ Teredo Port (3544)

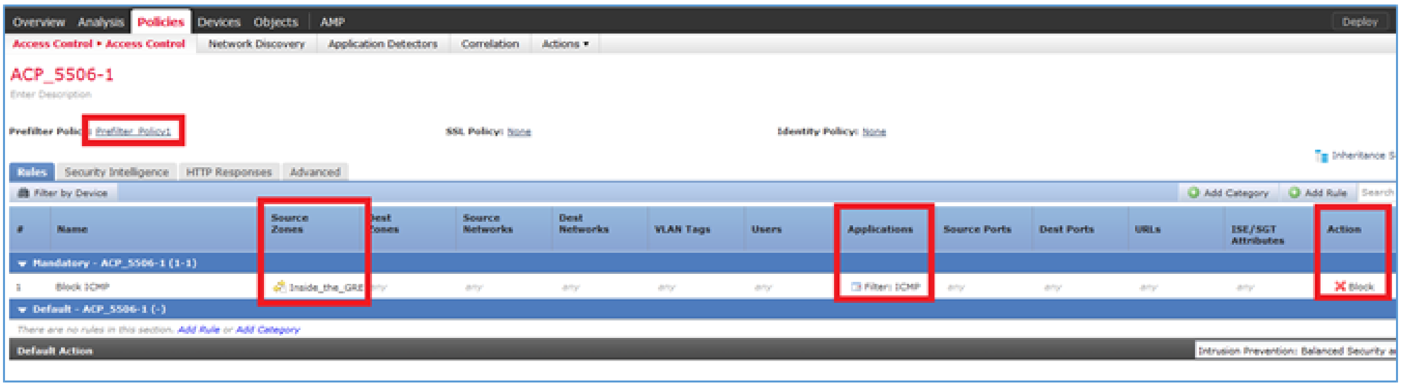
關於操作：

動作	說明
分析	在LINA後，Snort引擎會檢查流量。或者，可以為隧道流量分配隧道標籤。
封鎖	此流量被LINA封鎖。將檢查外部報頭。

快速路徑	流量僅由LINA處理，不需要使用Snort引擎。

步驟 2.為標籤的流量定義訪問控制策略。

雖然一開始不能非常直觀，但隧道標籤可以由訪問控制策略規則用作源區域。導覽至Policies > Access Control，然後建立一個規則，阻擋已標籤流量的ICMP，如下圖所示。



ACP_5506-1

Enter Description

Prefilter Policy: Prefilter_Policy1 SSL Policy: None Identity Policy: None

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applications	Source Ports	Dest Ports	URLs	ISE/SGT Attributes	Action
▾ Mandatory - ACP_5506-1 (1-1)													
1	Block ICMP	Inside_the_GRE	any	any	any	any	any	Filter: ICMP	any	any	any	any	✕ Block
▾ Default - ACP_5506-1 (-)													
There are no rules in this section. Add Rule or Add Category													
Default Action													Intrusion Prevention: Balanced Security a

注意：新的預過濾器策略已附加到訪問控制策略。

驗證：

在LINA和CLISH上啟用擷取：

<#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
```

從R1，嘗試ping遠端GRE隧道端點。ping失敗：

<#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)
```

CLISH擷取顯示第一個回應要求已通過FTD，且回覆已封鎖：

<#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
```

LINA擷取會確認這點：

<#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
```

啟用CLISH firewall-engine-debug，清除LINA ASP丟棄計數器並執行相同的測試。CLISH調試顯示

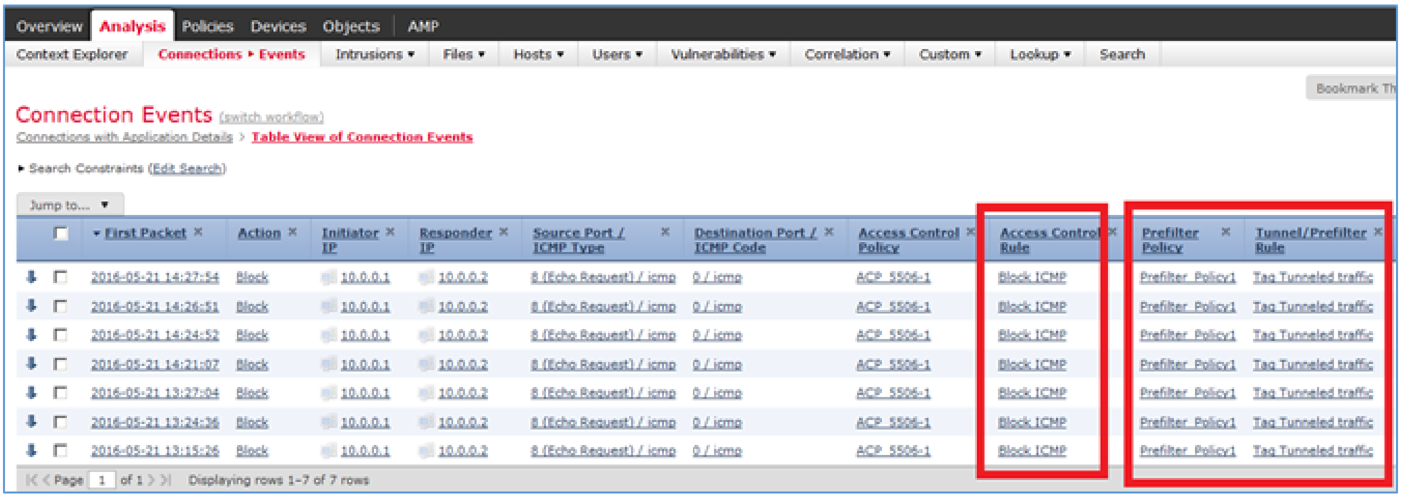
，對於Echo-Request，您匹配了預過濾器規則，對於Echo-Reply，則顯示ACP規則：

```
<#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
```

ASP捨棄顯示Snort捨棄了封包：

```
<#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
```

在連線事件中，您可以看到您匹配的Prefilter策略和規則，如下圖所示。



Connection Events (switch workflow)

Connections with Application Details > Table View of Connection Events

▸ Search Constraints (Edit Search)

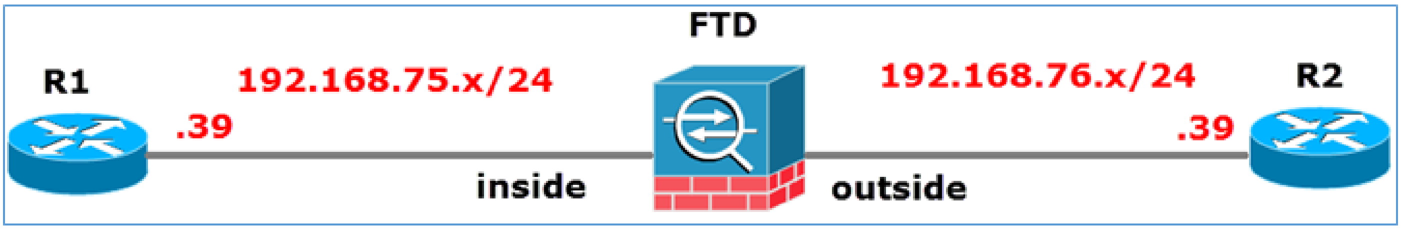
Jump to... ▾

	□	First Packet	Action	Initiator IP	Responder IP	Source Port / ICMP Type	Destination Port / ICMP Code	Access Control Policy	Access Control Rule	Prefilter Policy	Tunnel/Prefilter Rule
⬇	□	2016-05-21 14:27:54	Block	10.0.0.1	10.0.0.2	8 (Echo Request) / icmp	0 / icmp	ACP_5506-1	Block ICMP	Prefilter_Policy1	Tag Tunneled traffic
⬇	□	2016-05-21 14:26:51	Block	10.0.0.1	10.0.0.2	8 (Echo Request) / icmp	0 / icmp	ACP_5506-1	Block ICMP	Prefilter_Policy1	Tag Tunneled traffic
⬇	□	2016-05-21 14:24:52	Block	10.0.0.1	10.0.0.2	8 (Echo Request) / icmp	0 / icmp	ACP_5506-1	Block ICMP	Prefilter_Policy1	Tag Tunneled traffic
⬇	□	2016-05-21 14:21:07	Block	10.0.0.1	10.0.0.2	8 (Echo Request) / icmp	0 / icmp	ACP_5506-1	Block ICMP	Prefilter_Policy1	Tag Tunneled traffic
⬇	□	2016-05-21 13:27:04	Block	10.0.0.1	10.0.0.2	8 (Echo Request) / icmp	0 / icmp	ACP_5506-1	Block ICMP	Prefilter_Policy1	Tag Tunneled traffic
⬇	□	2016-05-21 13:24:36	Block	10.0.0.1	10.0.0.2	8 (Echo Request) / icmp	0 / icmp	ACP_5506-1	Block ICMP	Prefilter_Policy1	Tag Tunneled traffic
⬇	□	2016-05-21 13:15:26	Block	10.0.0.1	10.0.0.2	8 (Echo Request) / icmp	0 / icmp	ACP_5506-1	Block ICMP	Prefilter_Policy1	Tag Tunneled traffic

|< < Page 1 of 1 > >| Displaying rows 1-7 of 7 rows

任務3.含Fastpath預過濾器規則的旁路Snort引擎

網路圖表

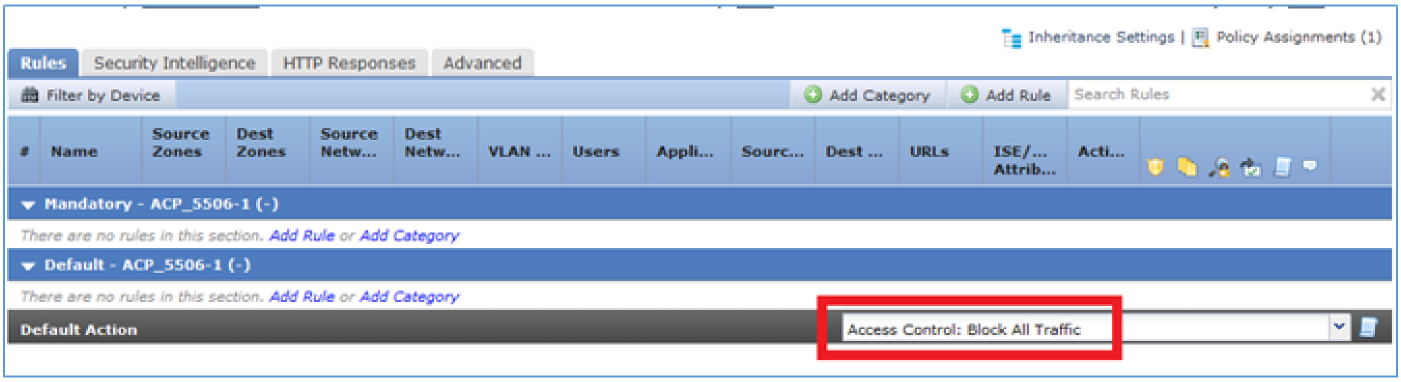


工作需求：

1. 刪除當前的訪問控制策略規則並新增阻止所有流量的訪問控制策略規則。
2. 為源自192.168.75.0/24網路的流量配置繞過Snort引擎的預過濾器策略規則。

解決方案：

步驟 1.阻止所有流量的訪問控制策略如下圖所示。



#	Name	Source Zones	Dest Zones	Source Netw...	Dest Netw...	VLAN ...	Users	Appli...	Sourc...	Dest ...	URLs	ISE/... Attrib...	Acti...

▾ Mandatory - ACP_5506-1 (-)

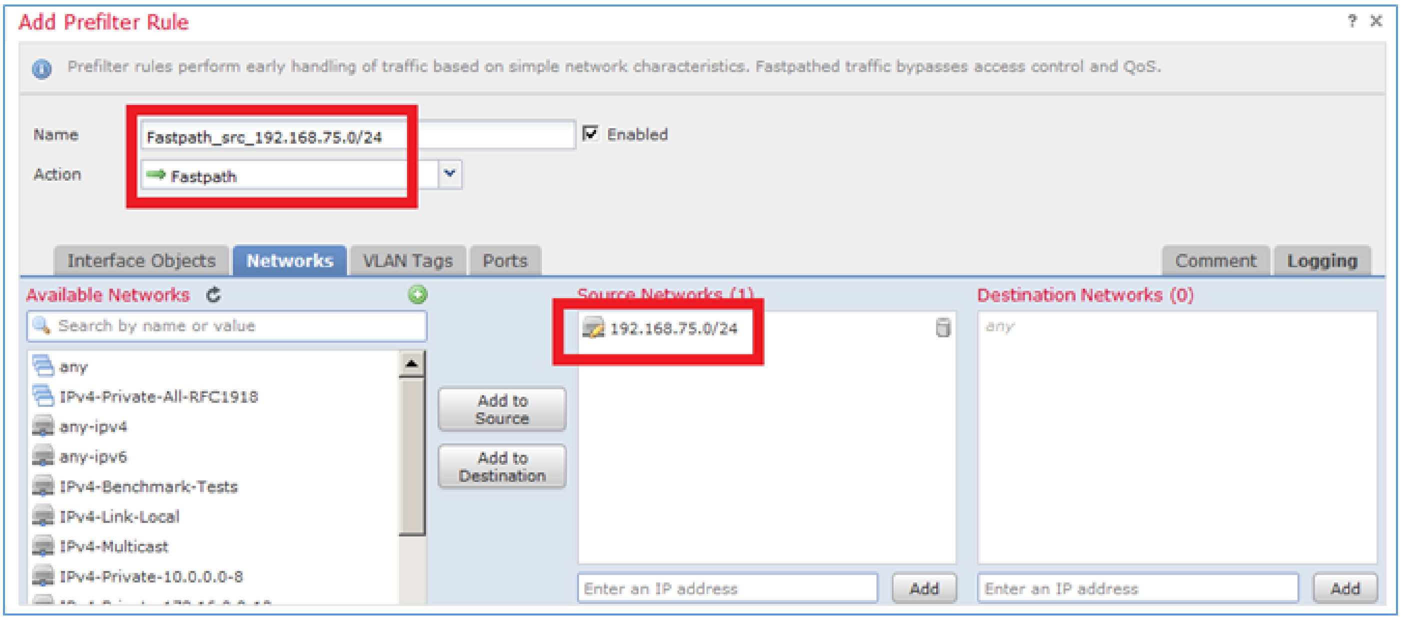
There are no rules in this section. Add Rule or Add Category

▾ Default - ACP_5506-1 (-)

There are no rules in this section. Add Rule or Add Category

Default Action: Access Control: Block All Traffic

步驟 2.為來源網路192.168.75.0/24新增一個以Fastpath作為動作的預過濾器規則，如下圖所示。


Add Prefilter Rule

Prefilter rules perform early handling of traffic based on simple network characteristics. Fastpathed traffic bypasses access control and QoS.

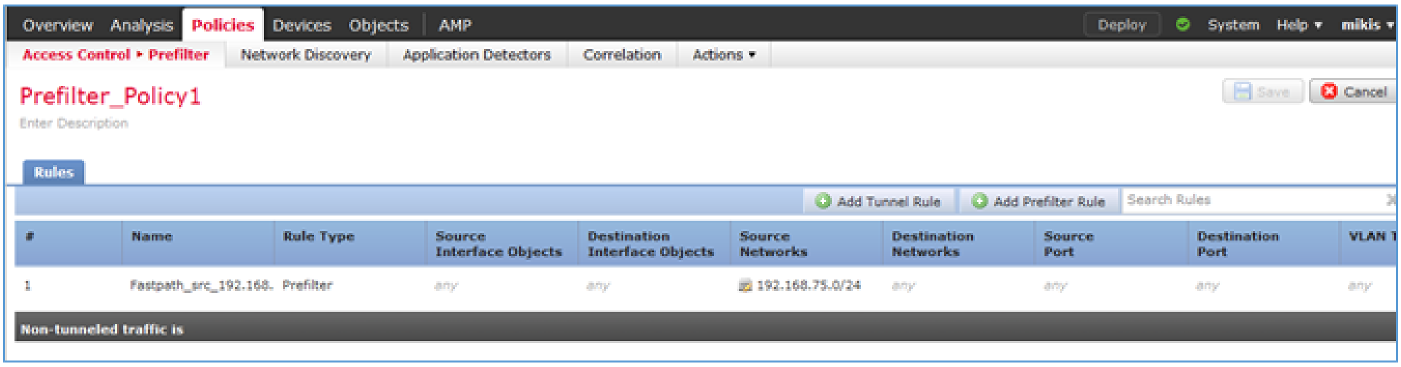
Name: Fastpath_src_192.168.75.0/24 ☑ Enabled

Action: Fastpath

Source Networks (1): 192.168.75.0/24

Destination Networks (0): any

步驟 3.結果如下圖所示。



Prefilter_Policy1

Enter Description

#	Name	Rule Type	Source Interface Objects	Destination Interface Objects	Source Networks	Destination Networks	Source Port	Destination Port	VLAN T
1	Fastpath_src_192.168.	Prefilter	any	any	192.168.75.0/24	any	any	any	any

Non-tunneled traffic is

步驟 4.儲存和部署。

在兩個FTD介面上啟用含有追蹤軌跡的擷取：

<#root>

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

嘗試通過FTD從R1(192.168.75.39)對R2(192.168.76.39)執行ping。Ping失敗：

<#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)
```

內部介面上的捕獲顯示：

<#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
```

第一個封包(echo-request)的追蹤軌跡顯示（重要點突出顯示）：

擾流器（突出顯示讀取）

firepower# show capture CAPI packet-number 1 trace

5 packets captured

1:23:35:07.281738 192.168.75.39 > 192.168.76.39:icmp：回應請求

階段：1

型別：CAPTURE

Subtype:

Result: ALLOW

Config:

Additional Information:

MAC Access list

階段：2

型別：ACCESS-LIST

```
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list
階段：3
型別：ROUTE-LOOKUP
Subtype：解析輸出介面
Result: ALLOW
Config:
Additional Information:
發現下一跳192.168.76.39使用輸出ifc outside
階段：4
型別：ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced trust ip 192.168.75.0 255.255.255.0 any rule-id 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
Additional Information:
階段：5
型別：CONN-SETTINGS
Subtype:
```

```
Result: ALLOW
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
Additional Information:
階段：6
型別：NAT
Subtype：每個會話
Result: ALLOW
Config:
Additional Information:
階段：7
型別：IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
階段：8
型別：INSPECT
Subtype:np-inspect
Result: ALLOW
Config:
class-map inspection_default
```

```
 match default-inspection-traffic
policy-map global_policy
 class inspection_default
  inspect icmp
service-policy global_policy global
Additional Information:
階段：9
型別：INSPECT
Subtype:np-inspect
Result: ALLOW
Config:
Additional Information:
階段：10
型別：NAT
Subtype：每個會話
Result: ALLOW
Config:
Additional Information:
階段：11
型別：IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
階段：12
型別：流建立
Subtype:
```

```
Result: ALLOW
Config:
Additional Information:
使用ID 52建立的新流，將資料包分派到下一個模組
階段：13
型別：ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced trust ip 192.168.75.0 255.255.255.0 any rule-id 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
Additional Information:
階段：14
型別：CONN-SETTINGS
Subtype:
Result: ALLOW
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
Additional Information:
```

```
階段：15
型別：NAT
Subtype：每個會話
Result: ALLOW
Config:
Additional Information:
階段：16
型別：IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
階段：17
型別：ROUTE-LOOKUP
Subtype：解析輸出介面
Result: ALLOW
Config:
Additional Information:
發現下一跳192.168.76.39使用輸出ifc outside
階段：18
型別：ADJACENCY-LOOKUP
Subtype：下一跳和鄰接關係
Result: ALLOW
Config:
Additional Information:
活動鄰接關係
下一跳mac address 0004.deab.681b hits 140372416161507
```

```
階段：19

型別：CAPTURE

Subtype:

Result: ALLOW

Config:

Additional Information:

MAC Access list

Result:

input-interface:outside

input-status:up

input-line-status: up

output-interface: outside

output-status: up

output-line-status: up

Action: allow

1 packet shown

firepower#
```

firepower# show capture CAPI packet-number 1 trace 5 packets captured 1: 23:35:07.281738 192.168.75.39 > 192.168.76.39: icmp：回應請求階段： 1型別：CAPTURE子型別：結果：允許配置：其他資訊：MAC訪問清單階段： 2型別：訪問清單子型別：結果：允許配置：隱式規則其他資訊：MAC訪問清單階段： 3型別： ROUTE-LOOKUP子型別：解析出口介面結果：允許配置：其他資訊：發現下一跳192.168.76.39使用輸出ifc超出階段：4型別：ACCESS-LIST子型別：日誌結果：允許配置：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其他資訊：階段： 5型別：CONN-SETTINGS子型別：結果： ALLOW Config: class-map class-default match any policy-map global_policy class-default set connection advanced-options UM_STATIC_SERVICE_MAP -policy global_policy全域性附加資訊：階段：6型別：NAT子型別：每會話結果：ALLOW配置：附加資訊：階段：7型別：IP-OPTIONS子型別：結果：ALLOW配置：附加資訊：階段：8型別：INSPECT子型別：np-inspect結果：ALLOW配置：class-map inspection_default match default-inspection-traffic policy-map global_policy類inspection_default icmp service-policy global_policy附加資訊：階段：9型別：INSPECT子型別：np-inspect結果：允許config：其他資訊：階段：10型別：NAT子型別：每會話結果：ALLOW配置：其他資訊：階段：11型別：IP-OPTIONS子型別：結果

：ALLOW配置：其他資訊：階段：12型別：FLOW-CREATION子型別：結果：ALLOW配置：其他資訊：使用ID 52建立的新流，將資料包傳送到下一個模組階段：13型別：ACCESS-LIST子型別：日誌結果：ALLOW配置：訪問組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_src_11191.168.75.0/24其它資訊： 4型別：CONN-SETTINGS子型別：結果：ALLOW配置：class-map class-default match any policy-map global_policy class-default set connection advanced-options UM_STATIC_TCP_MAP服務 — policy global_policy全域性附加資訊：階段：15型別：NAT子型別：每個會話結果：ALLOW配置：附加資訊：階段：16型別：IP — 選項子型別：結果：ALLOW配置：附加資訊：階段：17型別：ROUTE-LOOKUP subtype：解析出口介面結果：ALLOW Config：其他資訊：found next-hop 192.168.76.39使用出口ifc outside Phase: 18型別：ADJACENCY-LOOKUP子型別：next-hop and adjacency結果：ALLOW Config：其他資訊：adjacency活動下一跳mac地址004.deab.681b hits 140372416161507 Phase: 19型別：CAPTURE子型別：結果：ALLOW Config：其他資訊： MAC訪問清單結果：input-interface:outside input-status:up input-line-status:up output-interface:outside output-status:up output-line-status:up操作：allow 1 packet shown firepower#

外部介面上的捕獲顯示：

<#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
```

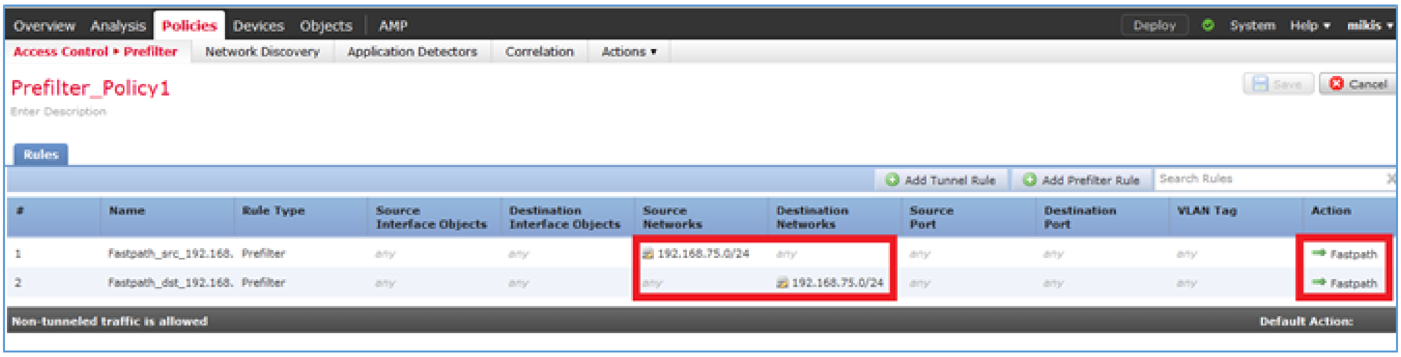
返回封包的追蹤軌跡顯示它與目前流量(52)相符，但遭到ACL封鎖：

<#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
```

步驟 5.為返回流量新增另一個預過濾器規則。結果如下圖所示。



Prefilter_Policy1

#	Name	Rule Type	Source Interface Objects	Destination Interface Objects	Source Networks	Destination Networks	Source Port	Destination Port	VLAN Tag	Action
1	Fastpath_src_192.168.	Prefilter	any	any	192.168.75.0/24	any	any	any	any	Fastpath
2	Fastpath_dst_192.168.	Prefilter	any	any	any	192.168.75.0/24	any	any	any	Fastpath

Non-tunneled traffic is allowed

Default Action:

現在跟蹤您看到的返回資料包（重要點突出顯示）：

擾流器 （突出顯示讀取）

firepower# show capture CAPO packet-number 2 trace

10 packets captured

2: 00:01:38.873123 192.168.76.39 > 192.168.75.39: icmp：回應回覆

階段：1

型別：CAPTURE

Subtype:

Result: ALLOW

Config:

Additional Information:

MAC Access list

階段：2

型別：ACCESS-LIST

Subtype:

Result: ALLOW

Config:

Implicit Rule

Additional Information:

MAC Access list

階段：3

```
型別：FLOW-LOOKUP
Subtype:
Result: ALLOW
Config:
Additional Information:
找到ID為62的流，使用當前流
階段：4
型別：ACCESS-LIST
Subtype: log
Result: 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 POLICY: Prefilter_Policy1
access-list CSM_FW_ACL_ remark rule-id 268434450: RULE: Fastpath_dst_192.168.75.0/24
Additional Information:
階段：5
型別：CONN-SETTINGS
Subtype:
Result: ALLOW
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
Additional Information:
階段：6
型別：NAT
Subtype：每個會話
Result: ALLOW
Config:
Additional Information:
階段：7
型別：IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
階段：8
型別：ROUTE-LOOKUP
Subtype：解析輸出介面
Result: ALLOW
Config:
Additional Information:
發現下一跳192.168.75.39在內部使用輸出ifc
階段：9
型別：ADJACENCY-LOOKUP
Subtype：下一跳和鄰接關係
Result: ALLOW
Config:
Additional Information:
```

活動鄰接關係

下一跳mac address c84c.758d.4981 hits 140376711128802

階段：10

型別：CAPTURE

Subtype:

Result: ALLOW

Config:

Additional Information:

MAC Access list

Result:

input-interface:inside

input-status:up

input-line-status: up

output-interface:inside

output-status: up

output-line-status: up

Action: allow

firepower# show capture CAPO packet-number 2 trace 10 packets captured 2: 00:01:38.873123 192.168.76.39 > 192.168.75.39: icmp：回應應答階段： 1型別：CAPTURE子型別：結果：允許配置：其他資訊：MAC訪問清單階段： 2型別：ACCESS-LIST子型別：結果：允許配置：隱式規則其他資訊：MAC訪問清單階段： 3 :FLOW-LOOKUP子型別：結果：允許配置：其他資訊：找到ID為62的流，使用當前流階段：4型別：ACCESS-LIST子型別：日誌結果：允許配置：access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ advanced trust ip any 192.168.75.0 255.255.0 rule-id 268434450 event-log both access-list CSM_FW acl_ remark rule-id 268434450: PREFILTER POLICY: Prefilter_Policy1 access-list CSM_FW_ACL_ remark rule-id 268434450: RULE: Fastpath_dst_192.168.75.0/24其他資訊：階段： 5型別： CONN-SETTINGS子型別：結果：ALLOW Config: class-map class-default match any policy-map global_policy class-default set connection advanced-options UM_STATIC_TCP_MAPservice-policy global其他資訊：階段： 6子型別： NAT型別：每會話結果：ALLOW配置：其他資訊：階段：7型別：IP-OPTIONS子型別：結果：ALLOW配置：其他資訊：階段：8型別：ROUTE-LOOKUP子型別：解析出口介面結果：ALLOW配置：其他資訊：發現下一跳192.168.75.39在階段：9型別中使用出口ifc:ADJACENCY-LOOKUP子型別：next-hop和鄰接結果：ALLOW配置：其他資訊資訊：鄰接活動下一跳mac地址c84c.758d.4981命中140376711128802階段： 10型別： CAPTURE子型別：結果：允許配置：其他資訊： MAC訪問清單結果：input-interface:inside input-status: up input-line-status: up output-interface: inside output-status: up output-line-status: up操作： allow

驗證

使用本節內容，確認您的組態是否正常運作。

在各自的任務部分中解釋了驗證過程。

疑難排解

目前尚無特定資訊可用於排解此組態的疑難問題。

相關資訊

- 所有版本的Cisco Firepower Management Center配置指南都可以在以下位置找到：

導航思科安全防火牆威脅防禦文檔

- 思科全球技術協助中心(TAC)強烈建議使用以下視覺指南，以瞭解有關Cisco Firepower下一代安全技術的深入實用知識，其中包括本文中提到的內容：

Cisco Firepower威脅防禦(FTD)

- 有關所有配置和故障排除技術說明：

思科安全防火牆管理中心

- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。