

FTD 사전 필터 정책 구성 및 운영

목차

- [소개](#)
 - [사전 요구 사항](#)
 - [요구 사항](#)
 - [사용되는 구성 요소](#)
 - [배경 정보](#)
 - [구성](#)
 - [사전 필터 정책 사용 사례 1](#)
 - [사전 필터 정책 사용 사례 2](#)
 - [작업 1. 기본 사전 필터 정책 확인](#)
 - [CLI\(LINA\) 확인](#)
-

소개

이 문서에서는 FTD(Firepower Threat Defense) 사전 필터 정책의 컨피그레이션 및 작업에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- FTD 코드 6.1.0-195를 실행하는 ASA5506X
- 6.1.0-195를 실행하는 FMC(FireSIGHT Management Center)
- 15.2 이미지를 실행하는 2개의 3925 Cisco IOS® 라우터

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

사전 필터 정책은 6.1 버전에 도입된 기능이며 세 가지 주요 목적을 제공합니다.

1. 내부 및 외부 헤더를 기준으로 트래픽 일치

- 2. 플로우가 Snort 엔진을 완전히 우회할 수 있는 조기 액세스 제어 기능 제공
- 3. ASA(Adaptive Security Appliance) 마이그레이션 툴에서 마이그레이션된 ACE(Access Control Entry)의 자리 표시자로 작동합니다.

구성

사전 필터 정책 사용 사례 1

사전 필터 정책은 FTD가 내부 및/또는 외부 IP 헤더 터널링 트래픽을 기반으로 필터링할 수 있도록 허용하는 터널 규칙 유형을 사용할 수 있습니다. 이 문서가 작성되었을 때 터널링된 트래픽은 다음을 나타냅니다.

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

이미지에 표시된 대로 GRE 터널을 고려하십시오.



GRE 터널을 사용하여 R1에서 R2로 ping할 때 트래픽이 방화벽을 통과하는 모습은 이미지에 표시된 것과 같습니다.

```

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) outer
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) inner
Internet Control Message Protocol

```

방화벽이 ASA 디바이스인 경우 이미지에 표시된 대로 외부 IP 헤더를 확인합니다.

L2 Header	Outer IP Header src=192.168.75.39 dst=192.168.76.39	GRE Header	Inner IP Header src=10.0.0.1 dst=10.0.0.2	L7
------------------	--	-------------------	--	-----------

ASA#

show conn

```
GRE OUTSIDE 192.168.76.39:0 INSIDE 192.168.75.39:0  
, idle 0:00:17, bytes 520, flags
```

방화벽이 Firepower 디바이스인 경우 이미지에 표시된 대로 내부 IP 헤더를 확인합니다.

L2 Header	Outer IP Header src= 192.168.75.39 dst= 192.168.76.39	GRE Header	Inner IP Header src= 10.0.0.1 dst= 10.0.0.2	L7
------------------	--	-------------------	--	-----------

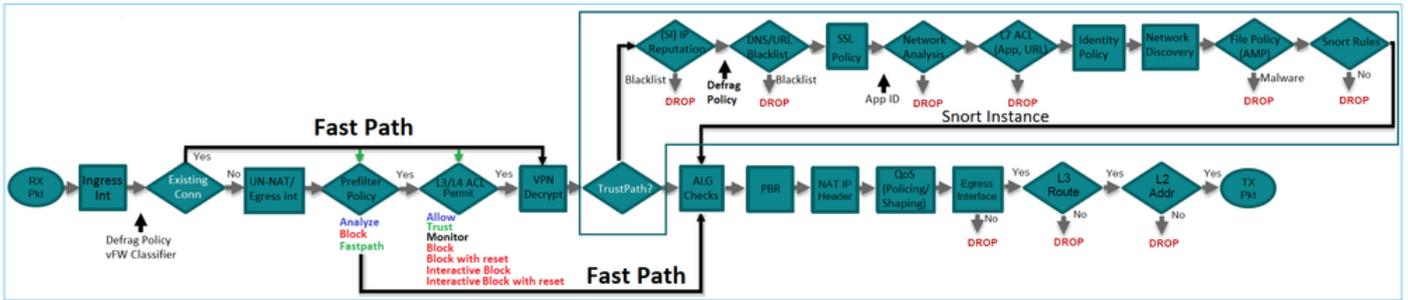
프리필터 정책을 사용하면 FTD 디바이스는 내부 및 외부 헤더를 기반으로 트래픽을 매칭할 수 있습니다.

요점:

디바이스	검사
ASA	외부 IP
Snort	내부 IP
FTD	외부(사전 필터) + 내부 IP(액세스 제어 정책(ACP))

사전 필터 정책 사용 사례 2

Pre-filter Policy(프리필터 정책)는 Pre-filter Rule Type(프리필터 규칙 유형)을 사용할 수 있습니다. 이 Rule Type(프리필터 규칙 유형)은 초기 액세스 제어를 제공하고 플로우가 이미지에 표시된 대로 Snort 엔진을 완전히 우회하도록 할 수 있습니다.



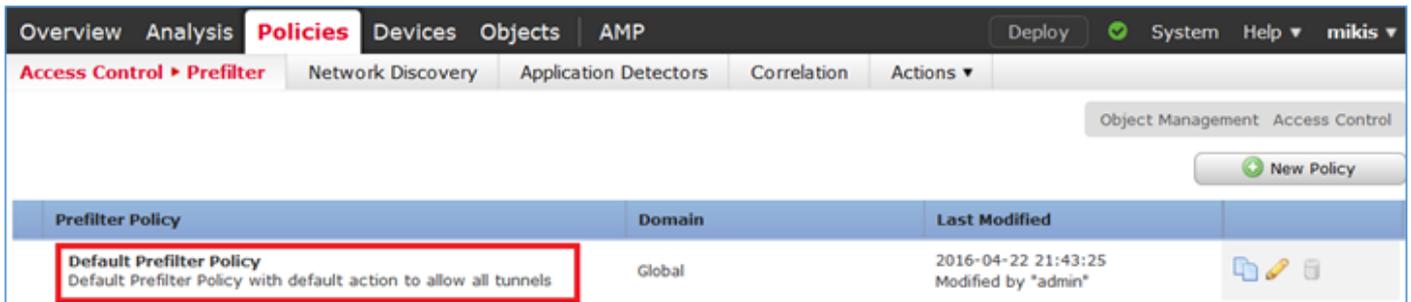
작업 1. 기본 사전 필터 정책 확인

작업 요구 사항:

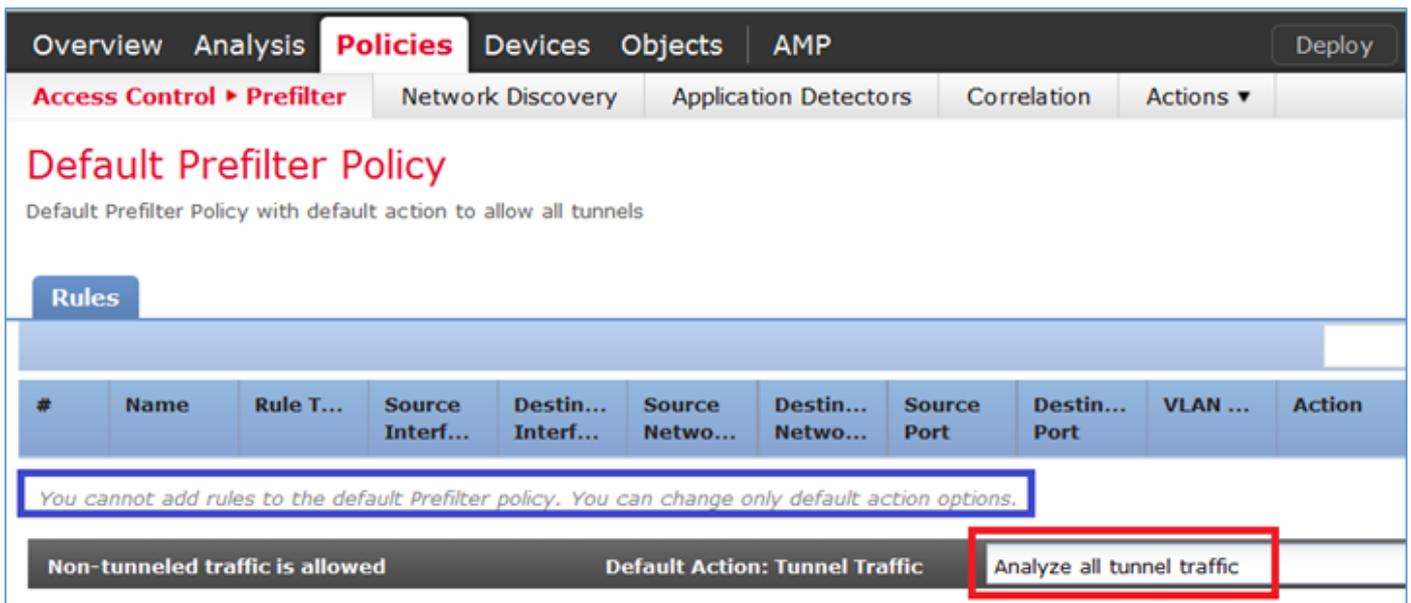
기본 사전 필터 정책 확인

해결책:

1단계. Policies(정책) > Access Control(액세스 제어) > Prefilter(사전 필터)로 이동합니다. 이미지에 표시된 대로 기본 사전 필터 정책이 이미 있습니다.



2단계. 이미지에 표시된 정책 설정을 보려면 Edit를 선택합니다.



3단계. 이미지에 표시된 대로 Prefilter Policy가 액세스 제어 정책에 이미 연결되어 있습니다.

Overview Analysis **Policies** Devices Objects AMP

Access Control ▶ Access Control Network Discovery Application D

ACP_5506-1

Enter Description

Prefilter Policy: [Default Prefilter Policy](#)

Rules Security Intelligence HTTP Responses **Advanced**

Prefilter Policy Settings

Prefilter Policy used before access control	Default Prefilter Policy
---	--------------------------

CLI(LINA) 확인

사전 필터 규칙이 ACL 위에 추가됩니다.

```
<#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
```

작업 2. 태그로 터널링된 트래픽 차단

작업 요구 사항:

GRE 터널 내에서 터널링되는 ICMP 트래픽을 차단합니다.

해결책:

1단계. 이러한 ACP를 적용하면 이미지에 표시된 것처럼 GRE 터널을 통과하든 통과하지 않든 상관 없이 ICMP(Internet Control Message Protocol) 트래픽이 차단되는 것을 볼 수 있습니다.



<#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)

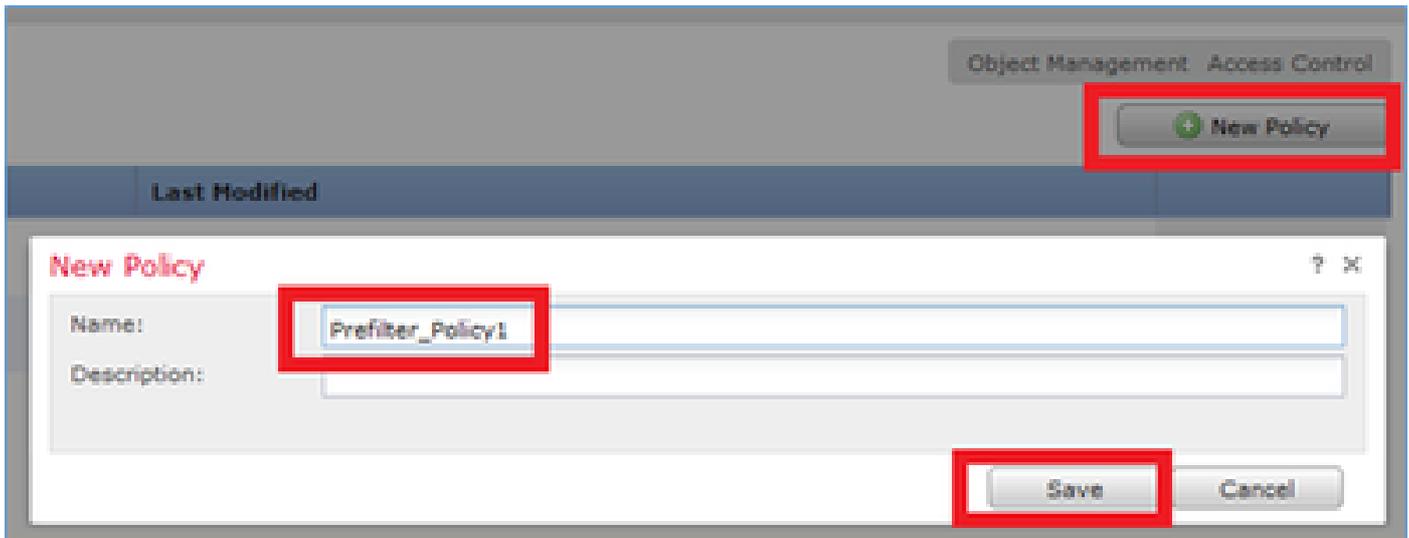
이 경우 사전 필터 정책을 사용하여 작업 요구 사항을 충족할 수 있습니다. 논리는 다음과 같습니다.

1. GRE 내에서 캡슐화된 모든 패킷에 태그를 지정합니다.
2. 태그가 지정된 패킷과 일치하고 ICMP를 차단하는 액세스 제어 정책을 생성합니다.

아키텍처 관점에서, 패킷은 LINA(Linux NetworkTively) 사전 필터 규칙, Snort 사전 필터 규칙 및 ACP를 기준으로 검사되고, 마지막으로 Snort가 LINA에 삭제를 지시합니다. 첫 번째 패킷은 FTD 디바이스를 통과합니다.

1단계. 터널링 트래픽에 대한 태그를 정의합니다.

Policies(정책) > Access Control(액세스 제어) > Prefilter(사전 필터)로 이동하고 새 사전 필터 정책을 생성합니다. 기본 사전 필터 정책은 이미지에 표시된 대로 편집할 수 없습니다.

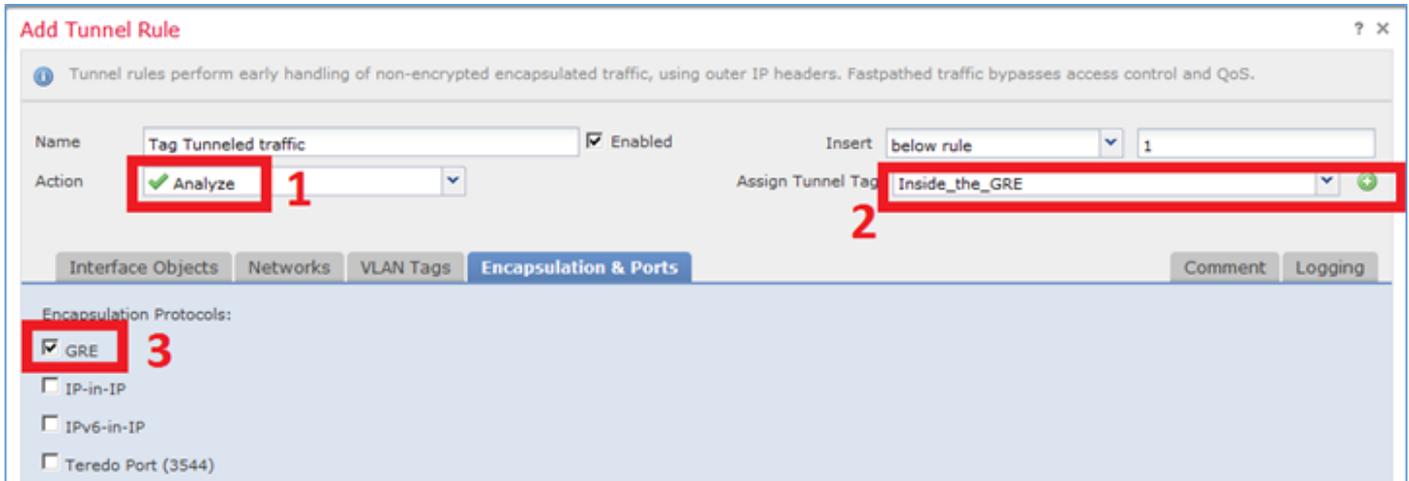


사전 필터 정책 내에서 두 가지 유형의 규칙을 정의할 수 있습니다.

1. 터널 규칙
2. 사전 필터 규칙

이 두 기능은 사전 필터 정책에서 구성할 수 있는 완전히 다른 기능이라고 생각할 수 있습니다.

이 작업을 위해 이미지에 표시된 대로 터널 규칙을 정의해야 합니다.



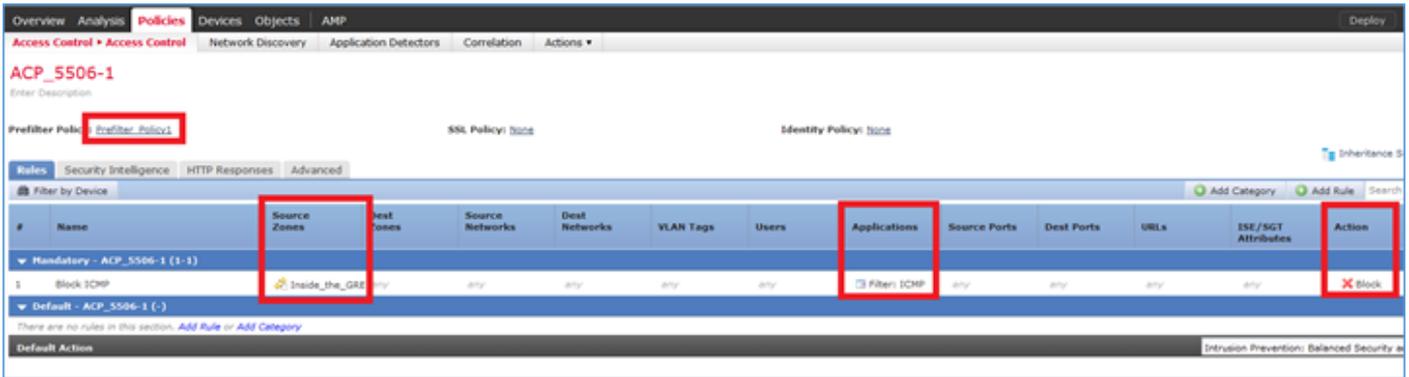
작업과 관련하여:

작업	설명
분석	LINA 이후에는 Snort Engine에서 플로우를 확인합니다. 선택적으로 터널 태그를 터널링된 트래픽에 할당할 수 있습니다.

차단	LINA에 의해 흐름이 차단되었습니다. 외부 헤더를 검사합니다.
빠른 경로	Snort 엔진을 사용할 필요 없이 LINA에서만 플로우를 처리합니다.

2단계. 태그가 지정된 트래픽에 대한 액세스 제어 정책을 정의합니다.

처음에는 매우 직관적일 수는 없지만 액세스 제어 정책 규칙에서 터널 태그를 소스 영역으로 사용할 수 있습니다. Policies(정책) > Access Control(액세스 제어)로 이동하고 이미지에 표시된 대로 태그 처리된 트래픽에 대해 ICMP를 차단하는 규칙을 생성합니다.



 참고: 새 사전 필터 정책이 액세스 제어 정책에 연결됩니다.

확인:

LINA 및 CLISH에서 캡처를 활성화합니다.

```
<#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

R1에서 원격 GRE 터널 엔드포인트에 ping을 시도합니다. Ping이 실패합니다.

<#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 캡처는 첫 번째 에코 요청이 FTD를 거쳤으며 응답이 차단되었음을 보여줍니다.

<#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 캡처는 다음을 확인합니다.

<#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
```

CLISH firewall-engine-debug를 활성화하고 LINA ASP 삭제 카운터를 지우고 동일한 테스트를 수행합니다. CLISH 디버그는 Echo-Request에 대해 프리필터 규칙과 일치했으며 Echo-Reply에 대해 ACP 규칙을 매칭했음을 보여줍니다.

```
<#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, 0
```

```
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, 0
```

```
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 삭제는 Snort가 패킷을 삭제했음을 보여줍니다.

```
<#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
```

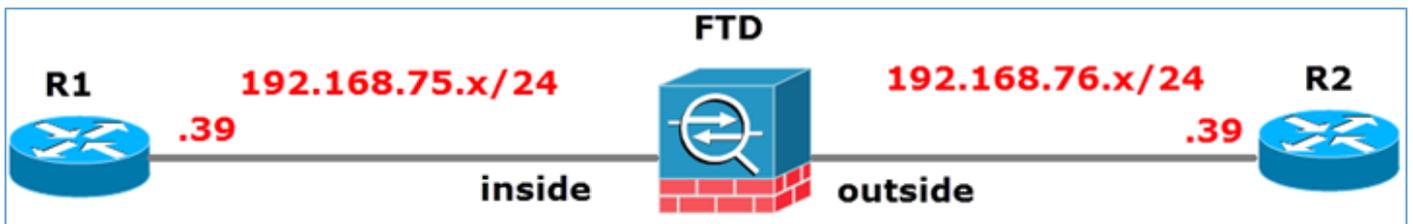
Connection Events(연결 이벤트)에서는 이미지에 표시된 대로 매치한 Prefilter Policy and Rule(프

리필터 정책 및 규칙)을 볼 수 있습니다.

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 Tunnelled 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 Tunnelled 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 Tunnelled 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 Tunnelled 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 Tunnelled traffic
2016-05-21 13:24:26	Block	10.0.0.1	10.0.0.2	8 (Echo Request) / icmp	0 / icmp	ACP_5506-1	Block ICMP	Prefilter_Policy1	Tag Tunnelled 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 Tunnelled traffic

작업 3. Fastpath Prefilter 규칙으로 Snort 엔진 우회

네트워크 다이어그램



작업 요구 사항:

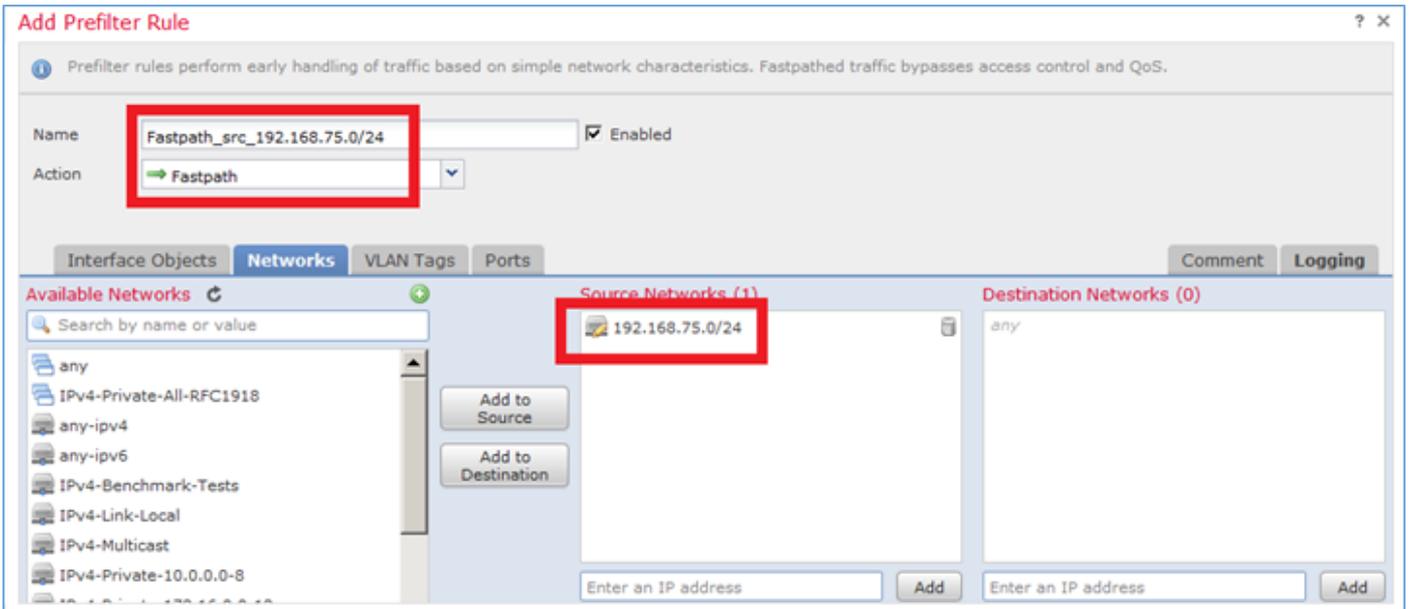
1. 현재 액세스 제어 정책 규칙을 제거하고 모든 트래픽을 차단하는 액세스 제어 정책 규칙을 추가합니다.
2. 192.168.75.0/24 네트워크에서 소싱된 트래픽에 대해 Snort Engine을 우회하는 Prefilter Policy 규칙을 구성합니다.

해결책:

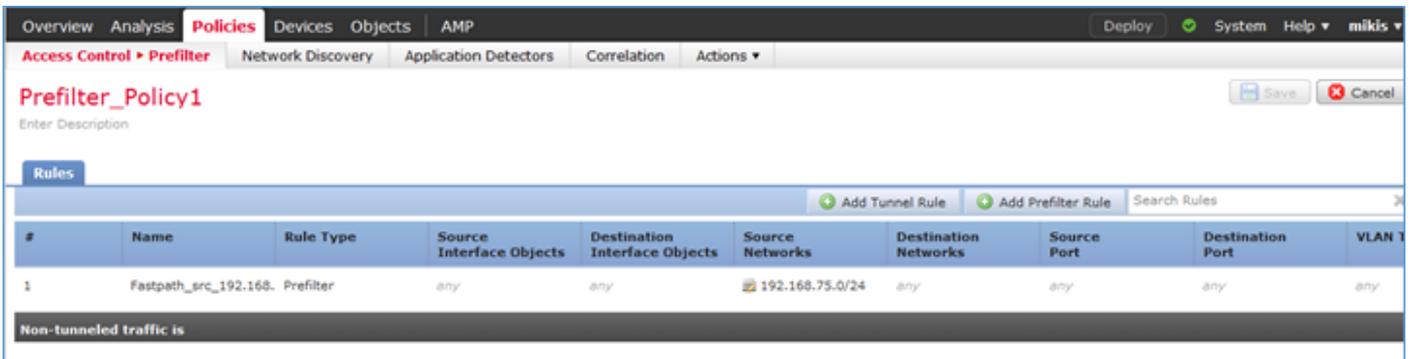
1단계. 모든 트래픽을 차단하는 액세스 제어 정책은 그림과 같습니다.

#	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													

2단계. 이미지에 표시된 대로 소스 네트워크 192.168.75.0/24에 대한 작업으로 Fastpath가 있는 Prefilter Rule을 추가합니다.



3단계. 결과는 이미지에 표시된 것과 같습니다.



4단계. 저장 및 구축.

두 FTD 인터페이스에서 추적을 사용하여 캡처를 활성화합니다.

```
<#root>
```

```
firepower#
```

```
capture CAPI int inside trace match icmp any any
```

```
firepower#
```

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

FTD를 통해 R1(192.168.75.39)에서 R2(192.168.76.39)로 ping을 시도합니다. Ping 실패:

```
<#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)

내부 인터페이스의 캡처는 다음을 보여줍니다.

<#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
```

첫 번째 패킷의 추적(echo-request)은 (강조된 중요 사항):

[스포일러](#) (읽으려면 강조 표시)

firepower# show capture CAPI packet-number 1 trace

캡처된 패킷 5개

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

단계: 1

유형: CAPTURE

하위 유형:

결과: 허용

설정:

추가 정보:

MAC 액세스 목록

단계: 2

유형: 액세스 목록

하위 유형:

결과: 허용

설정:

암시적 규칙

추가 정보:

MAC 액세스 목록

단계: 3

유형: 경로 조회

하위 유형: 이그레스 인터페이스 확인

결과: 허용

설정:

추가 정보:

next-hop 192.168.76.39에서 외부 이그레스(egress) ifc 사용

단계: 4

유형: 액세스 목록

하위 유형: 로그

결과: 허용

설정:

액세스 그룹 CSM_FW_ACL_ 전역

access-list CSM_FW_ACL_ advanced trust ip 192.168.75.0 255.255.255.0 규칙 ID 268434448 이벤트 로그 모두

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

추가 정보:

단계: 5

유형: CONN-SETTINGS

하위 유형:

결과: 허용

설정:

class-map class-default

모두 일치

정책 맵 global_policy

class-default

연결 고급 옵션 설정 UM_STATIC_TCP_MAP

서비스 정책 전역 정책 전역

추가 정보:

단계: 6

유형: NAT

하위 유형: 세션당

결과: 허용

설정:

추가 정보:

단계: 7

유형: IP-OPTIONS

하위 유형:

결과: 허용

설정:

추가 정보:

단계: 8

유형: INSPECT

하위 유형: np-inspect

결과: 허용

설정:

class-map inspection_default

기본 검사 트래픽 일치

정책 맵 global_policy

class inspection_default

icmp 검사

서비스 정책 전역 정책 전역

추가 정보:

단계: 9

유형: INSPECT

하위 유형: np-inspect

결과: 허용

설정:

추가 정보:

단계: 10

유형: NAT

하위 유형: 세션당

결과: 허용

설정:

추가 정보:

단계: 11

유형: IP-OPTIONS

하위 유형:

결과: 허용

설정:

추가 정보:

단계: 12

유형: 플로우 생성

하위 유형:

결과: 허용

설정:

추가 정보:

ID 52로 생성된 새 플로우, 다음 모듈로 전달되는 패킷

단계: 13

유형: 액세스 목록

하위 유형: 로그

결과: 허용

설정:

액세스 그룹 CSM_FW_ACL_ 전역

access-list CSM_FW_ACL_ advanced trust ip 192.168.75.0 255.255.255.0 규칙 ID 268434448 이벤트 로그 모두

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

추가 정보:

단계: 14

유형: CONN-SETTINGS

하위 유형:

결과: 허용

설정:

class-map class-default

모두 일치

정책 맵 global_policy

class-default

연결 고급 옵션 설정 UM_STATIC_TCP_MAP

서비스 정책 전역 정책 전역

추가 정보:

단계: 15

유형: NAT

하위 유형: 세션당

결과: 허용

설정:

추가 정보:

단계: 16

유형: IP-OPTIONS

하위 유형:

결과: 허용

설정:

추가 정보:

단계: 17

유형: 경로 조회

하위 유형: 이그레스 인터페이스 확인

결과: 허용

설정:

추가 정보:

next-hop 192.168.76.39에서 외부 이그레스(egress) ifc 사용

단계: 18

유형: ADJACENCY-LOOKUP

하위 유형: 다음 홉 및 인접성

결과: 허용

설정:

추가 정보:

인접성 활성화

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

단계: 19

유형: CAPTURE

하위 유형:

결과: 허용

설정:

추가 정보:

MAC 액세스 목록

결과:

입력 인터페이스: 외부

입력 상태: up

입력 라인 상태: up

출력 인터페이스: 외부

출력 상태: up

출력 라인 상태: up

작업: 허용

1개 패킷 표시

firepower 번호

```

168.75.0/24 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: echo request phase: 1 type: CAPTURE 하
위 유형: 결과: ALLOW Config: 추가 정보: MAC Access list Phase: 2 Type: ACCESS-LIST 하위 유
형: 결과: ALLOW Config: Implicit Rule 추가 정보: MAC Access List Phase: 3 Type: ROUTE-
LOOKUP 하위 유형: Resolve Egress Interface 결과: ALLOW Additional Information: found next-
hop922.61 8.76.39에서 이그레스 ifc를 사용합니다. 단계: 4 유형: ACCESS-LIST 하위 유형: 로그
결과: 허용 구성: 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_
rule-id remark 268434448: PREFILTER 정책: Prefilter_Policy1 access-list CSM_FW_ACL_ remark
rule-id 268434448: 규칙: Fastpath_src_192.2 추가 정보: 5단계 유형: CONN-SETTINGS 하위 유형:
결과: ALLOW 구성: class-map class-default match any policy-map global_policy class-default set
connection advanced-options UM_STATIC_TCP_MAP service-policy global_policy 추가 정보: 6단
계 유형: NAT 하위 유형: 세션당 결과: ALLOW 구성: 추가 정보: 7단계: IP-OPTIONS 하위 유형: 결
과: ALLOW 구성: 추가 정보: 8단계: INSPECT 하위 유형: np-inspect 결과: ALLOW 구성: class-
map inspection_default match default-inspection-traffic policy-map global_policy class_default
inspect icmp service-global_policy 추가 정보: 9단계 유형: INSPECT 하위 유형: np-inspect 결과:
ALLOW 구성: 추가 정보: 10단계 유형: NAT 하위 유형: 세션당 결과: ALLOW 구성: 추가 정보: 11단

```

계 유형: IP-OPTIONS 하위 유형: 결과: ALLOW 구성: 추가 정보: 12단계 유형: FLOW-CREATION
하위 유형: 결과: ALLOW 구성: 추가 정보: id 52로 생성된 새 흐름, 다음 모듈로 전달된 패킷 단계:
13단계: ACCESS-LIST 하위 유형: 로그 결과: ALLOW 구성: access-group CSM_FW_ACL global
access-list CSM_CSM fw_ACL_ advanced trust ip 192.168.75.0 255.255.0 any rule-id 268434448
event-log both access-list CSM_FW_ACL_ remark rule-id 268434448: PREFILTER 정책:
Prefilter_Policy1 access-list CSM_FW_ACL_ remark rule-id 268434448: 규칙:
Fastpath_src_192.168.75.0/24 추가 정보: 단계: 14 유형: CONN-SETTINGS 하위 유형: 결과:
ALLOW 구성: class-map class-default match any policy-map global_policy class-default set
connection advanced-options UM_STATIC_TCP map service-policy global_policy 전역 추가 정보:
단계: 15 유형: NAT 하위 유형: 세션당 결과: 허용 구성: 추가 정보: 단계: 16 유형: IP-OPTIONS 하
위 유형: 결과: 허용 구성: 추가 정보: 단계: 17 유형: ROUTE-LOOKUP 하위 유형: 이그레스 인터페
이스 확인 결과: 허용 구성: 추가 정보: 발견 next-hop 192.168.76.39에서 이그레스 ifc 외부 단계: 18
유형: ADJACENCY-LOOKUP 하위 유형: next-hop 및 adjacency 결과: 허용 구성: 추가 정보:
adjacency Active next-mac 주소 0 004.deab.681b 적중 140372416161507 단계: 19 유형: 캡처 하
위 유형: 결과: 허용 구성: 추가 정보: MAC 액세스 목록 결과: 입력 인터페이스: 외부 입력 상태: 위
입력 라인 상태: 위 출력 인터페이스: 외부 출력 상태: 위 출력 라인 상태: 위 작업: firepower 번호 포
시 패킷 1개 허용

외부 인터페이스의 캡처 기능은 다음과 같습니다.

```
<#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
```

반환 패킷의 추적은 현재 흐름(52)과 일치하지만 ACL에 의해 차단됨을 나타냅니다.

```
<#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

5단계. 반환 트래픽에 대한 프리필터 규칙을 하나 더 추가합니다. 결과는 이미지에 표시된 것과 같습니다.

#	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	Prefilter	any	any	192.168.75.0/24	any	any	any	any	Fastpath
2	Fastpath_dst_192.168. Prefilter	Prefilter	any	any	any	192.168.75.0/24	any	any	any	Fastpath

이제 표시되는 반환 패킷을 추적합니다(중요 포인트가 강조 표시됨).

[스포일러](#) (읽으려면 강조 표시)

```
firepower# show capture CAPO packet-number 2 trace
```

캡처된 패킷 10개

```
2: 00:1:38.873123 192.168.76.39 > 192.168.75.39: icmp: echo reply
```

단계: 1

유형: CAPTURE

하위 유형:

결과: 허용

설정:

추가 정보:

MAC 액세스 목록

단계: 2

유형: 액세스 목록

하위 유형:

결과: 허용

설정:

암시적 규칙

추가 정보:

MAC 액세스 목록

단계: 3

유형: FLOW-LOOKUP

하위 유형:

결과: 허용

설정:

추가 정보:

ID가 62인 흐름을 찾았습니다. 현재 흐름을 사용합니다.

단계: 4

유형: 액세스 목록

하위 유형: 로그

결과: 허용

설정:

액세스 그룹 CSM_FW_ACL_ 전역

```
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
```

추가 정보:

단계: 5

유형: CONN-SETTINGS

하위 유형:

결과: 허용

설정:

```
class-map class-default
```

모두 일치

```
정책 맵 global_policy
```

```
class-default
```

```
연결 고급 옵션 설정 UM_STATIC_TCP_MAP
```

서비스 정책 전역 정책 전역

추가 정보:

단계: 6

유형: NAT

하위 유형: 세션당

결과: 허용

설정:

추가 정보:

단계: 7

유형: IP-OPTIONS

하위 유형:

결과: 허용

설정:

추가 정보:

단계: 8

유형: 경로 조회

하위 유형: 이그레스 인터페이스 확인

결과: 허용

설정:

추가 정보:

next-hop 192.168.75.39에서 내부 이그레스 ifc 사용

단계: 9

유형: ADJACENCY-LOOKUP

하위 유형: 다음 홉 및 인접성

결과: 허용

설정:

추가 정보:

인접성 활성화

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

단계: 10

유형: CAPTURE

하위 유형:

결과: 허용

설정:

추가 정보:

MAC 액세스 목록

결과:

입력 인터페이스: 내부

입력 상태: up

입력 라인 상태: up

출력 인터페이스: 내부

출력 상태: up

출력 라인 상태: up

작업: 허용

```
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: echo reply phase: 1 유형: CAPTURE 하위 유형: 결과:
ALLOW 구성: 추가 정보: MAC 액세스 목록 단계: 2 유형: ACCESS-LIST 하위 유형: 결과: ALLOW
구성: 암시적 규칙 추가 정보: MAC 액세스 목록 단계: 3 유형: FLOW-LOOKUP 하위 유형: 결과:
ALLOW 구성: 추가 정보: Found flow with id62, uses current flow 단계: 유형: ACCESS-LIST 하위
유형: 로그 결과: ALLOW 구성: 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 정책: Prefilter_Policy1 access-list
CSM_FW_ACL_ remark rule-id 268434450: 규칙: Fastpath_dst_dst_192.168.75.0/24 추가 정보:
5단계 유형: CONN-SETTINGS 결과: ALLOW Config: class-map class-default match any policy-
map global_policy class-default set connection advanced-options UM_STATIC_TCP_MAP service-
policy global_policy global 추가 정보: 단계: 6 유형: NAT 하위 유형: 세션당 결과: ALLOW Config:
추가 정보: 단계: 7 유형: IP-OPTIONS 하위 유형: 결과: ALLOW Config: 추가 정보: 단계: 8 유형:
ROUTE-LOOKUP 하위 유형: 이그레스 인터페이스 해결 결과: ALLOW Config: 추가 정보: found
next-hop 192.168.75.39 uses egress ifc inside 단계: 유형: ADJACENCY-9 조회 하위 유형: next-
hop 및 adjacency 결과: 허용 구성: 추가 정보: adjacency 활성화 next-hop mac 주소 c84c.758d.4981
hits 140376711128802 단계: 10 유형: 캡처 하위 유형: 결과: 허용 구성: 추가 정보: MAC 액세스 목록
```

록 결과: 입력-인터페이스: 내부 입력-상태: up input-line-status: up output-interface: inside output-status: up output-line-status: up 작업: allow

다음을 확인합니다.

구성이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

각 작업 섹션에서 검증에 대해 설명했습니다.

문제 해결

현재 이 구성의 문제를 해결하는 데 사용할 수 있는 특정 정보가 없습니다.

관련 정보

- 모든 버전의 Cisco Firepower Management Center 컨피그레이션 가이드는 여기에서 찾을 수 있습니다.

[Cisco Secure Firewall Threat Defense 설명서 탐색](#)

- Cisco Global Technical Assistance Center(TAC)는 이 문서에 언급된 기술을 포함하여 Cisco Firepower Next Generation Security 기술에 대한 심층적인 실무 지식을 얻기 위해 이 시각적 가이드를 적극 권장합니다.

[Cisco FTD\(Firepower 위협 방어\)](#)

- 모든 컨피그레이션 및 문제 해결 TechNotes:

[Cisco Secure Firewall 관리 센터](#)

- [기술 지원 및 문서 - Cisco Systems](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.