

# 라우팅 모드에서 Firepower 위협 방어 인터페이스 구성

## 목차

---

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[관련 제품](#)

[배경 정보](#)

[구성](#)

[네트워크 다이어그램](#)

[라우티드 인터페이스 및 하위 인터페이스 구성](#)

[1단계. 논리적 인터페이스 구성](#)

[2단계. 물리적 인터페이스 구성](#)

[FTD 라우티드 인터페이스 작업](#)

[FTD 라우팅 인터페이스 개요](#)

[다음을 확인합니다.](#)

[FTD 라우팅 인터페이스에서 패킷 추적](#)

[관련 정보](#)

---

## 소개

이 문서에서는 FTD(Firepower Threat Defense) 어플라이언스에서 Inline Pair Interface의 컨피그레이션, 확인 및 작동에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

이 문서에 대한 특정 요구 사항은 없습니다.

### 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- ASA5512-X - FTD 코드 6.1.0.x
- FMC(firepower 관리 센터) - 코드 6.1.0.x

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.

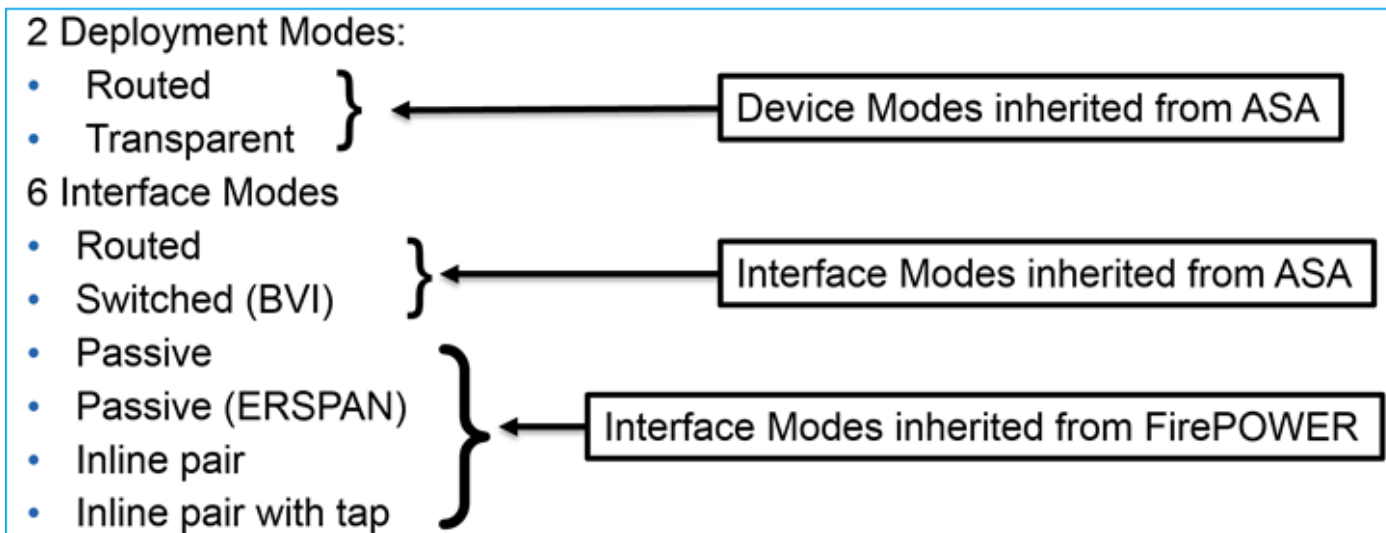
## 관련 제품

이 문서는 다음과 같은 하드웨어 및 소프트웨어 버전에서도 사용할 수 있습니다.

- ASA5506-X, ASA5506W-X, ASA5506H-X, ASA5508-X, ASA5516-X
- ASA5512-X, ASA5515-X, ASA5525-X, ASA5545-X, ASA5555-X
- FPR2100, FPR4100, FPR9300
- VMware(ESXi), Amazon Web Services(AWS), Kernel-based Virtual Machine(KVM)
- FTD 소프트웨어 코드 6.2.x 이상

## 배경 정보

FTD(Firepower Threat Defense)는 이 이미지에 표시된 대로 2개의 구축 모드와 6개의 인터페이스 모드를 제공합니다.



참고: 단일 FTD 어플라이언스에서 인터페이스 모드를 혼합할 수 있습니다.

다양한 FTD 구축 및 인터페이스 모드에 대한 개괄적인 개요:

FTD 인터페이스 모드로 들어갑니다	FTD 구축 모드	설명	트래픽 삭제 가능

라우팅됨	라우팅됨	전체 LINA 엔진 및 Snort 엔진 검사	예
전환됨	투명	전체 LINA 엔진 및 Snort 엔진 검사	예
인라인 쌍	라우팅 또는 투명	부분 LINA 엔진 및 전체 Snort 엔진 검사	예
Tap가 있는 인라인 쌍	라우팅 또는 투명	부분 LINA 엔진 및 전체 Snort 엔진 검사	아니요
수동	라우팅 또는 투명	부분 LINA 엔진 및 전체 Snort 엔진 검사	아니요
수동(ERSPAN)	라우팅됨	부분 LINA 엔진 및 전체 Snort 엔진 검사	아니요

## 구성

### 네트워크 다이어그램



### 라우티드 인터페이스 및 하위 인터페이스 구성

다음 요구 사항에 따라 하위 인터페이스 G0/0.201 및 인터페이스 G0/1을 구성합니다.

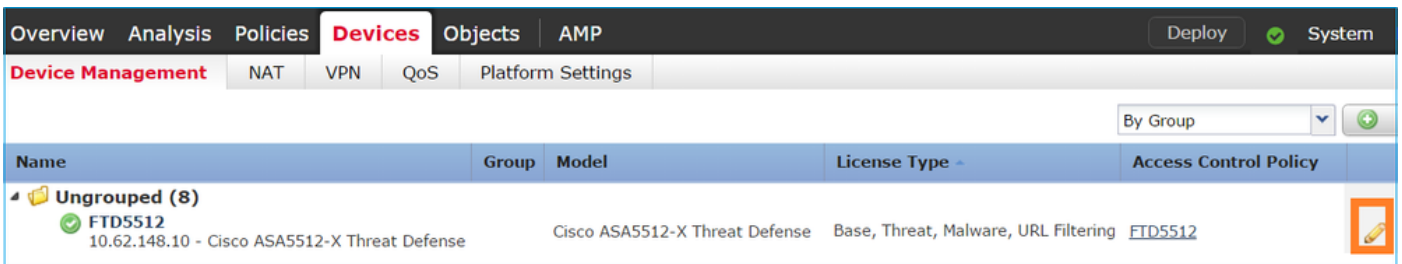
인터페이스	G0/0.201	G0/1
이름	내부	외부
보안 영역	내부 영역(_Z)	외부 영역(_Z)

설명	내부	외부
하위 인터페이스 ID	201	-
VLAN ID	201	-
IPv4	192.168.201.1/24	192.168.202.1/24
이중/속도	자동	자동

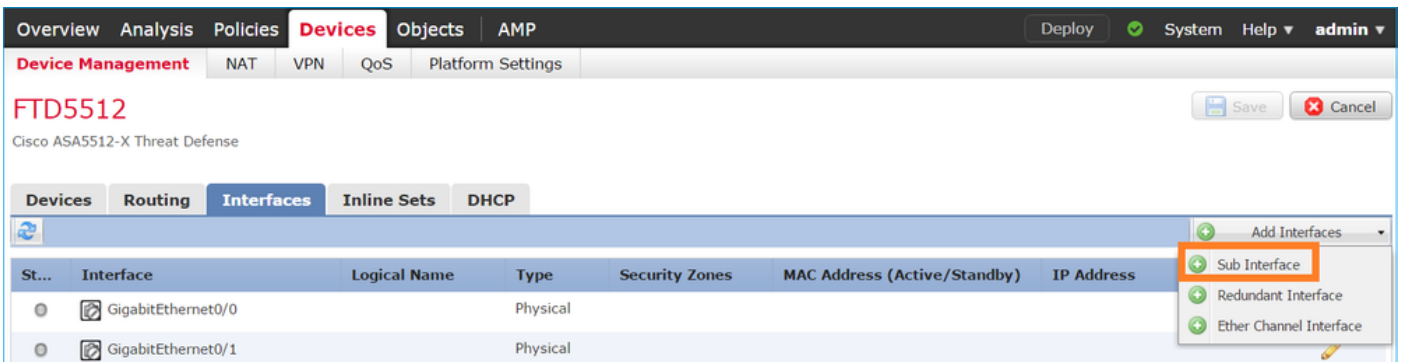
## 솔루션

### 1단계. 논리적 인터페이스 구성

Devices(디바이스) > Device Management(디바이스 관리)로 이동하여 적절한 디바이스를 선택하고 Edit(수정) 아이콘을 선택합니다.



Add Interfaces > Sub Interface를 선택합니다.



요구 사항에 따라 하위 인터페이스 설정을 구성합니다.

## Add Sub Interface

Name:   Enabled  Management Only

Security Zone:  ▼

Description:

### General

IPv4

IPv6

Advanced

MTU:  (64 - 9198)

Interface \*:  ▼  Enabled

Sub-Interface ID \*:  (1 - 4294967295)

VLAN ID:  (1 - 4094)

인터페이스 IP 설정:

## Add Sub Interface

Name:   Enabled  Management Only

Security Zone:  ▼

Description:

General

**IPv4**

IPv6

Advanced

IP Type:  ▼

IP Address:  eg. 1.1.1.1/255.255.255.228

물리적 인터페이스(GigabitEthernet0/0)에서 Duplex 및 Speed 설정을 지정합니다.

General	IPv4	IPv6	Advanced	<b>Hardware Configuration</b>
Duplex:	auto <input type="button" value="v"/>			
Speed:	auto <input type="button" value="v"/>			

물리적 인터페이스를 활성화합니다(이 경우 G0/0).

### Edit Physical Interface

Mode:	None <input type="button" value="v"/>		
Name:	<input type="text"/>	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Management Only
Security Zone:	<input type="text"/> <input type="button" value="v"/>		
Description:	<input type="text"/>		

<b>General</b>	IPv4	IPv6	Advanced	Hardware Configuration
MTU:	1500		(64 - 9198)	
Interface ID:	GigabitEthernet0/0			

2단계. 물리적 인터페이스 구성

요구 사항에 따라 GigabitEthernet0/1 물리적 인터페이스를 수정합니다.

## Edit Physical Interface

Mode:  ▼

Name:   Enabled  Management Only

Security Zone:  ▼

Description:

General **IPv4** IPv6 Advanced Hardware Configuration

IP Type:  ▼

IP Address:  eg. 1.1.1.1/255.255.255.228

- 라우팅된 인터페이스의 경우 모드는 None입니다.
- Name은 ASA 인터페이스 nameif와 같습니다
- FTD에서 모든 인터페이스의 보안 수준 = 0
- 동일한 보안 트래픽은 FTD에 적용되지 않습니다. FTD 인터페이스(간)와 (인트라) 간의 트래픽은 기본적으로 허용됩니다

저장과 배포를 선택합니다.

확인

FMC GUI에서:

St...	Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
●	GigabitEthernet0/0		Physical			
●	GigabitEthernet0/1	OUTSIDE	Physical	OUTSIDE_ZONE		192.168.202.1/24(Static)
○	GigabitEthernet0/2		Physical			
○	GigabitEthernet0/3		Physical			
○	GigabitEthernet0/4		Physical			
○	GigabitEthernet0/5		Physical			
●	Diagnostics0/0		Physical			
●	GigabitEthernet0/0.201	INSIDE	SubInterf...	INSIDE_ZONE		192.168.201.1/24(Static)

FTD CLI에서 다음을 수행합니다.

<#root>

>

show interface ip brief

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	unassigned	YES	unset	up	up
GigabitEthernet0/0.201	192.168.201.1	YES	manual	up	up
GigabitEthernet0/1	192.168.202.1	YES	manual	up	up
GigabitEthernet0/2	unassigned	YES	unset	administratively down	down
GigabitEthernet0/3	unassigned	YES	unset	administratively down	down
GigabitEthernet0/4	unassigned	YES	unset	administratively down	down
GigabitEthernet0/5	unassigned	YES	unset	administratively down	down
Internal-Control0/0	127.0.1.1	YES	unset	up	up
Internal-Data0/0	unassigned	YES	unset	up	up
Internal-Data0/1	unassigned	YES	unset	up	up
Internal-Data0/2	169.254.1.1	YES	unset	up	up
Management0/0	unassigned	YES	unset	up	up

<#root>

>

show ip

System IP Addresses:

Interface	Name	IP address	Subnet mask	Method
GigabitEthernet0/0.201	INSIDE	192.168.201.1	255.255.255.0	manual
GigabitEthernet0/1	OUTSIDE	192.168.202.1	255.255.255.0	manual

Current IP Addresses:

Interface	Name	IP address	Subnet mask	Method
GigabitEthernet0/0.201	INSIDE	192.168.201.1	255.255.255.0	manual
GigabitEthernet0/1	OUTSIDE	192.168.202.1	255.255.255.0	manual

FMC GUI 및 FTD CLI 상관관계:

The image shows a correlation between the FMC GUI and the FTD CLI. On the left, the 'Edit Sub Interface' GUI for the 'INSIDE' interface is shown. The 'Name' field is 'INSIDE', 'Security Zone' is 'INSIDE\_ZONE', and 'Description' is 'INTERNAL'. Under the 'IPv4' tab, 'IP Type' is 'Use Static IP' and 'IP Address' is '192.168.201.1/24'. On the right, the FTD CLI configuration for 'interface GigabitEthernet0/0.201' is shown, with arrows pointing from the GUI fields to the corresponding CLI commands: 'description INTERNAL', 'nameif INSIDE', and 'ip address 192.168.201.1 255.255.255.0'.

```

> show running-config interface g0/0.201
!
interface GigabitEthernet0/0.201
  description INTERNAL
  vlan 201
  nameif INSIDE
  cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
  security-level 0
  ip address 192.168.201.1 255.255.255.0

```

<#root>

>



```
show interface g0/0.201
```

```
Interface GigabitEthernet0/0.201
```

```
"
```

```
INSIDE
```

```
",
```

```
is up, line protocol is up
```

```
Hardware is i82574L rev00, BW 1000 Mbps, DLY 10 usec
```

```
VLAN identifier 201
```

```
Description: INTERNAL
```

```
MAC address a89d.21ce.fdea, MTU 1500
```

```
IP address 192.168.201.1, subnet mask 255.255.255.0
```

```
Traffic Statistics for "INSIDE":
```

```
1 packets input, 28 bytes
```

```
1 packets output, 28 bytes
```

```
0 packets dropped
```

```
>
```

```
show interface g0/1
```

```
Interface GigabitEthernet0/1 "OUTSIDE", is up, line protocol is up
```

```
Hardware is i82574L rev00, BW 1000 Mbps, DLY 10 usec
```

```
Auto-Duplex(Full-duplex), Auto-Speed(1000 Mbps)
```

```
Input flow control is unsupported, output flow control is off
```

```
Description: EXTERNAL
```

```
MAC address a89d.21ce.fde7, MTU 1500
```

```
IP address 192.168.202.1, subnet mask 255.255.255.0
```

```
0 packets input, 0 bytes, 0 no buffer
```

```
Received 0 broadcasts, 0 runts, 0 giants
```

```
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
```

```
0 pause input, 0 resume input
```

```
0 L2 decode drops
```

```
1 packets output, 64 bytes, 0 underruns
```

```
0 pause output, 0 resume output
```

```
0 output errors, 0 collisions, 12 interface resets
```

```
0 late collisions, 0 deferred
```

```
0 input reset drops, 0 output reset drops
```

```
input queue (blocks free curr/low): hardware (511/511)
```

```
output queue (blocks free curr/low): hardware (511/511)
```

```
Traffic Statistics for "OUTSIDE":
```

```
0 packets input, 0 bytes
```

```
0 packets output, 0 bytes
```

```
0 packets dropped
```

```
1 minute input rate 0 pkts/sec, 0 bytes/sec
```

1 minute output rate 0 pkts/sec, 0 bytes/sec  
 1 minute drop rate, 0 pkts/sec  
 5 minute input rate 0 pkts/sec, 0 bytes/sec  
 5 minute output rate 0 pkts/sec, 0 bytes/sec  
 5 minute drop rate, 0 pkts/sec

>

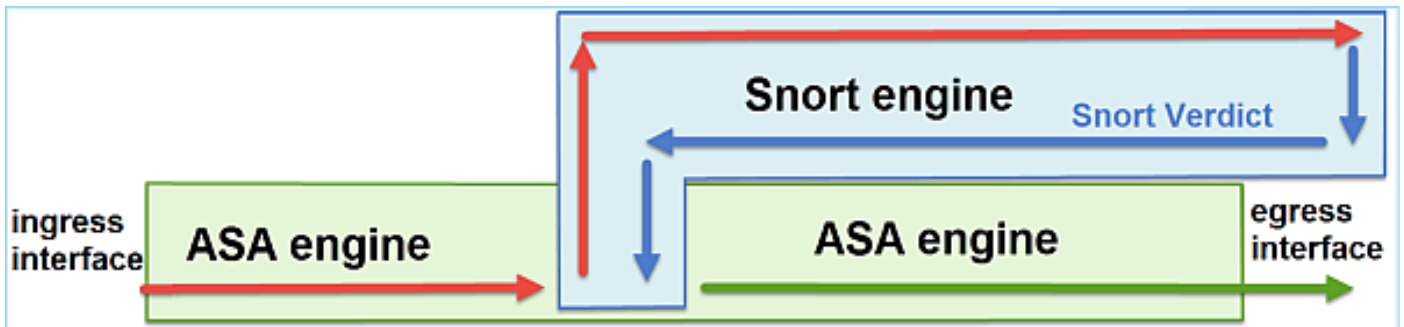
## FTD 라우티드 인터페이스 작업

라우티드 인터페이스가 사용 중일 때 FTD 패킷 흐름을 확인합니다.

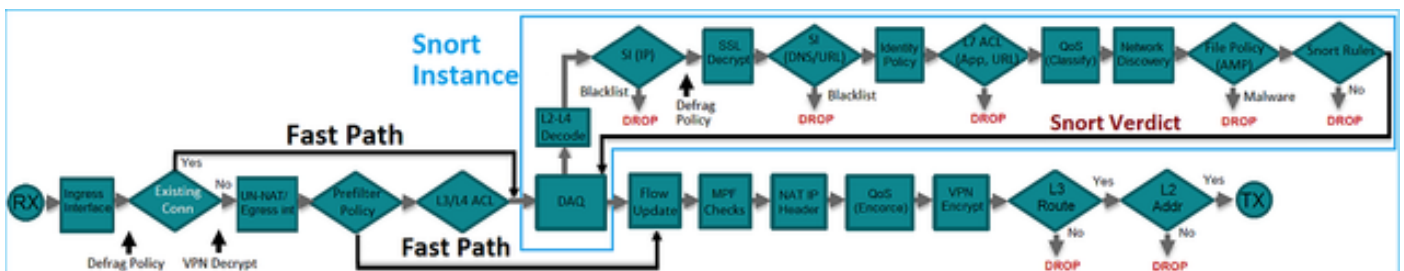
### 솔루션

#### FTD 아키텍처 개요

FTD 데이터 플레인에 대한 개괄적인 개요:



이 그림은 각 엔진에서 발생하는 몇 가지 검사를 보여줍니다.



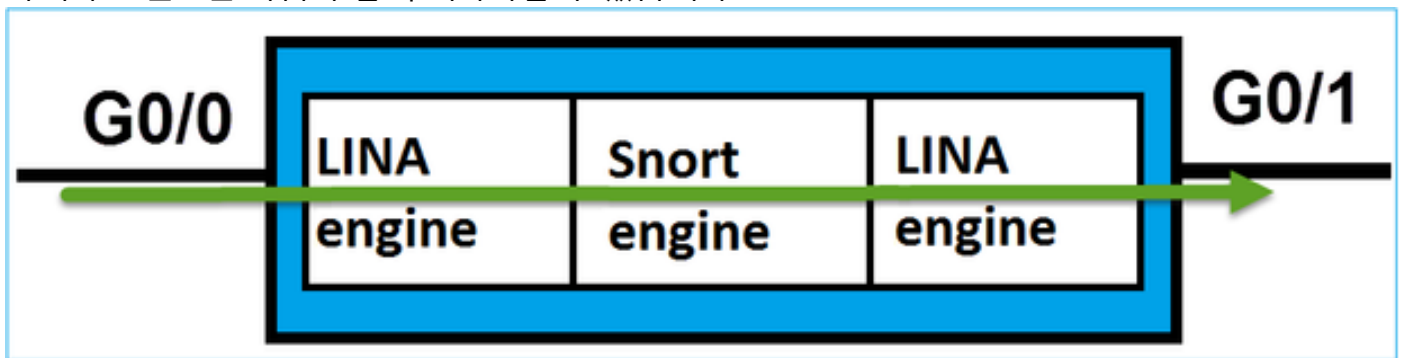
### 핵심 사항

- 하단 검사는 FTD LINA 엔진 데이터 경로에 해당합니다
- 파란색 상자 안의 체크는 FTD Snort 엔진 인스턴스에 해당합니다

### FTD 라우팅 인터페이스 개요

- 라우팅된 구축에서만 사용 가능
- 기존 L3 방화벽 구축
- 하나 이상의 물리적 또는 논리적(VLAN) 라우팅 가능 인터페이스
- NAT 또는 동적 라우팅 프로토콜과 같은 기능을 구성할 수 있습니다.
- 패킷은 경로 조회를 기반으로 전달되며 다음 홉은 ARP 조회를 기반으로 확인됩니다
- 실제 트래픽 삭제 가능
- 전체 LINA 엔진 검사와 전체 Snort 엔진 검사 적용

마지막 포인트는 다음과 같이 시각화할 수 있습니다.



다음을 확인합니다.

FTD 라우팅 인터페이스에서 패킷 추적

네트워크 다이어그램



적용된 정책을 보려면 다음 매개변수와 함께 packet-tracer를 사용합니다.

입력 인터페이스	내부
----------	----

프로토콜/서비스	TCP 포트 80
소스 IP	192.168.201.100
대상 IP	192.168.202.100

### 솔루션

라우티드 인터페이스가 사용될 경우, 기존 ASA 라우티드 인터페이스와 유사한 방식으로 패킷이 처리됩니다. LINA 엔진 데이터 경로에서 경로 조회, MPF(Modular Policy Framework), NAT, ARP 조회 등이 발생하는지 확인합니다. 또한 액세스 제어 정책에 필요한 경우, Snort 엔진(Snort 인스턴스 중 하나)에서 패킷을 검사하며, 여기에서 판정이 생성되어 LINA 엔진으로 돌아갑니다.

<#root>

>

```
packet-tracer input INSIDE tcp 192.168.201.100 11111 192.168.202.100 80
```

Phase: 1

Type: ROUTE-LOOKUP

Subtype: Resolve Egress Interface

Result: ALLOW

Config:

Additional Information:

```
found next-hop 192.168.202.100 using egress ifc OUTSIDE
```

Phase: 2

Type: ACCESS-LIST

Subtype: log

Result: ALLOW

Config:

```
access-group CSM_FW_ACL_ global
```

```
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268437505
access-list CSM_FW_ACL_ remark rule-id 268437505: ACCESS POLICY: FTD5512 - Default/1
access-list CSM_FW_ACL_ remark rule-id 268437505: L4 RULE: DEFAULT ACTION RULE
```

**Additional Information:**

This packet will be sent to snort for additional processing where a verdict will be reached

Phase: 3

Type: 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:**

Phase: 4

Type: NAT

Subtype: per-session  
Result: ALLOW  
Config:  
Additional Information:

Phase: 5  
Type: IP-OPTIONS  
Subtype:  
Result: ALLOW  
Config:  
Additional Information:

Phase: 6  
Type: NAT  
Subtype: per-session  
Result: ALLOW  
Config:  
Additional Information:

Phase: 7  
Type: IP-OPTIONS  
Subtype:  
Result: ALLOW  
Config:  
Additional Information:

Phase: 8  
Type: FLOW-CREATION  
Subtype:  
Result: ALLOW  
Config:  
Additional Information:  
New flow created with id 11336, packet dispatched to next module

Result:

input-interface: INSIDE


input-status: up  
input-line-status: up

output-interface: OUTSIDE

output-status: up  
output-line-status: up  
Action: allow

>

---

 참고: 4단계에서는 패킷이 UM\_STATIC\_TCP\_MAP이라는 TCP 맵에 대해 점검됩니다. FTD의 기본 TCP 맵입니다.

---

<#root>

firepower#

show run all tcp-map

!

```
tcp-map UM_STATIC_TCP_MAP
  no check-retransmission
  no checksum-verification
  exceed-mss allow
  queue-limit 0 timeout 4
  reserved-bits allow
  syn-data allow
```

```
synack-data drop
invalid-ack drop
seq-past-window drop
tcp-options range 6 7 allow
tcp-options range 9 18 allow
tcp-options range 20 255 allow
tcp-options selective-ack allow
tcp-options timestamp allow
tcp-options window-scale allow
tcp-options mss allow
tcp-options md5 clear
ttl-evasion-protection
urgent-flag allow
window-variation allow-connection
!
>
```

## 관련 정보

- [firepower 디바이스 관리자용 Cisco Firepower Threat Defense 컨피그레이션 가이드, 버전 6.1](#)
- [ASA 55xx-X 디바이스에 Firepower Threat Defense 설치 및 업그레이드](#)
- [Cisco Secure Firewall 위협 방어](#)
- [Cisco 기술 지원 및 다운로드](#)

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.