

# 관리에서 데이터 인터페이스로 FTD에 대한 관리자 액세스 구성

## 목차

---

### [소개](#)

#### [사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

#### [배경 정보](#)

#### [구성](#)

[인터페이스 마이그레이션 진행](#)

[플랫폼 설정에서 SSH 활성화](#)

#### [다음을 확인합니다.](#)

[FMC GUI\(Graphical User Interface\)에서 확인](#)

[FTD CLI\(Command Line Interface\)에서 확인](#)

#### [문제 해결](#)

[관리 연결 상태](#)

[작업 시나리오](#)

[비작업 시나리오](#)

[네트워크 정보 확인](#)

[관리자 상태 검증](#)

[네트워크 연결 확인](#)

[Management Center에 Ping하기](#)

[인터페이스 상태, 통계 및 패킷 수 확인](#)

[FTD에서 FMC에 연결하기 위한 경로 검증](#)

[Sftunnel 및 연결 통계 확인](#)

#### [관련 정보](#)

---

## 소개

이 문서에서는 FTD(Firepower Threat Defense)의 관리자 액세스를 관리에서 데이터 인터페이스로 수정하는 프로세스에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Firepower 위협 방어
- Firepower 관리 센터

## 사용되는 구성 요소

- Firepower Management Center Virtual 7.4.1
- Firepower Threat Defense Virtual 7.2.5

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

각 디바이스에는 FMC와의 통신을 위한 단일 전용 관리 인터페이스가 포함됩니다. 전용 관리 인터페이스 대신 관리를 위해 데이터 인터페이스를 사용하도록 디바이스를 선택적으로 구성할 수 있습니다. 외부 인터페이스에서 원격으로 Firepower 위협 방어를 관리하려는 경우 또는 별도의 관리 네트워크가 없는 경우 데이터 인터페이스의 FMC 액세스가 유용합니다. 이 변경은 FMC에서 관리하는 FTD의 FMC(Firepower 관리 센터)에서 수행해야 합니다.

데이터 인터페이스의 FMC 액세스에는 몇 가지 제한 사항이 있습니다.

- 하나의 물리적 데이터 인터페이스에서만 관리자 액세스를 활성화할 수 있습니다. 하위 인터페이스 또는 EtherChannel은 사용할 수 없습니다.
- 라우팅된 방화벽 모드만 해당, 라우팅된 인터페이스 사용
- PPPoE는 지원되지 않습니다. ISP에 PPPoE가 필요한 경우 Firepower Threat Defense와 WAN 모뎀 사이에 PPPoE를 지원하는 라우터를 두어야 합니다.
- 별도의 관리 및 이벤트 전용 인터페이스는 사용할 수 없습니다.

## 구성

### 인터페이스 마이그레이션 진행

---

참고: 변경을 진행하기 전에 FTD와 FMC의 최신 백업을 모두 사용하는 것이 좋습니다.

1. Devices(디바이스) > Device Management(디바이스 관리) 페이지로 이동하고 변경할 디바이스에 대해 Edit(수정)를 클릭합니다.

[Collapse All](#) [Download Device List Report](#)

<input type="checkbox"/>	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	Group	
<input type="checkbox"/>	▼ FMT Test (1)								
<input type="checkbox"/>	FTD-Test Snort 3 192.168.1.8 - Routed	FTDv for VMware	7.2.5	N/A	Essentials	Base-ACP	↺		Edit → ↗

2. Device(디바이스) > Management(관리) 섹션으로 이동하여 Manager Access Interface(관리자 액세스 인터페이스) 링크를 클릭합니다.

Management	
Remote Host Address:	192.168.1.8
Secondary Address:	
Status:	<span style="color: green;">✔</span>
Manager Access Interface:	 Management Interface

Manager Access Interface(관리자 액세스 인터페이스) 필드는 기존 관리 인터페이스를 표시합니다. 링크를 클릭하여 Manage device by 드롭다운 목록의 Data Interface 옵션인 새 인터페이스 유형을 선택하고 Save를 클릭합니다.

## Manager Access Interface ?

i This is an advanced setting and need to be configured only if needed. See the [online help](#) for detailed steps.

Manage device by

Management Interface ▼

Management Interface

Data Interface

Close
Save

3. 이제 데이터 인터페이스에서 관리 액세스 활성화를 진행해야 합니다. Devices(디바이스) > Device Management(디바이스 관리) > Interfaces(인터페이스) > Edit Physical Interface(물리적 인터페이스 편집) > Manager Access(관리자 액세스)로 이동합니다.

## Edit Physical Interface



General IPv4 IPv6 Path Monitoring Hardware Configuration **Manager Access** Advanced

Enable management access

Available Networks



10.201.204.129  
192.168.1.0\_24  
any-ipv4  
any-ipv6  
CSM  
Data\_Store

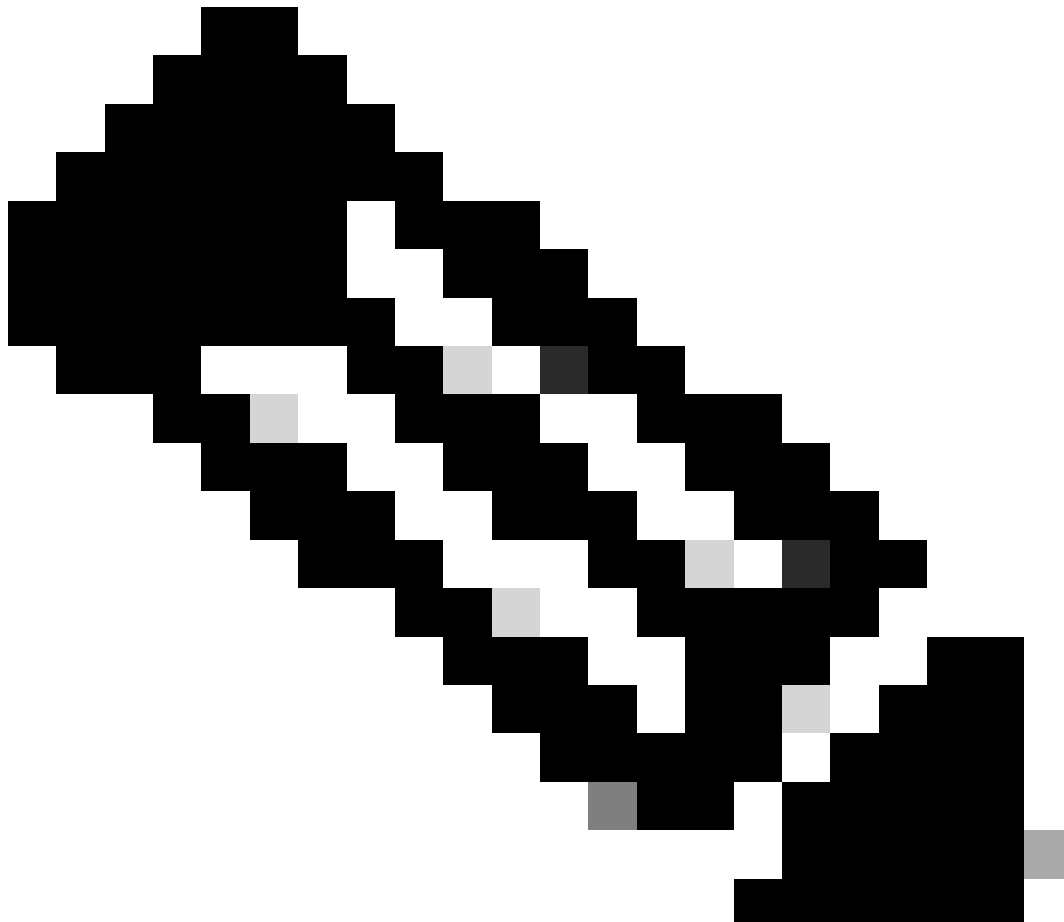
Add

Allowed Management Networks

any

Cancel

OK



---

참고: (선택 사항) 이중화를 위해 보조 인터페이스를 사용하는 경우 이중화를 위해 사용되는 인터페이스에서 관리 액세스를 활성화합니다.

(선택 사항) 인터페이스에 DHCP를 사용하는 경우 Devices(디바이스) > Device Management(디바이스 관리) > DHCP > DDNS 대화 상자에서 웹 유형 DDNS 메서드를 활성화합니다.

(선택 사항) 플랫폼 설정 정책에서 DNS를 구성하고 Devices(디바이스) > Platform Settings(플랫폼 설정) > DNS에서 이 디바이스에 적용합니다.

---

4. 위협 방어가 데이터 인터페이스를 통해 관리 센터에 라우팅될 수 있는지 확인합니다. 필요한 경우 Devices(디바이스) > Device Management(디바이스 관리) > Routing(라우팅) > Static Route(고정 경로)에서 고정 경로를 추가합니다.

1. 추가하는 고정 경로의 유형에 따라 IPv4 또는 IPv6을 클릭합니다.
2. 이 고정 경로가 적용되는 인터페이스를 선택합니다.
3. Available Network(사용 가능한 네트워크) 목록에서 목적지 네트워크를 선택합니다.
4. Gateway or IPv6 Gateway(게이트웨이 또는 IPv6 게이트웨이) 필드에 이 경로의 다음 홉인 게이트웨이 라우터를 입력하거나 선택합니다.

(선택 사항) 경로 가용성을 모니터링하려면 Route Tracking(경로 추적) 필드에 모니터링 정책을 정의하는 SLA(Service Level Agreement) Monitor 개체의 이름을 입력하거나 선택합니다.

## Add Static Route Configuration



Type:  IPv4  IPv6

Interface\*



(Interface starting with this icon  signifies it is available for route leak)

Available Network  +

Add

Selected Network



Gateway\*

+



Metric:

(1 - 254)

Tunneled:  (Used only for default Route)

Route Tracking:

+

Cancel

OK

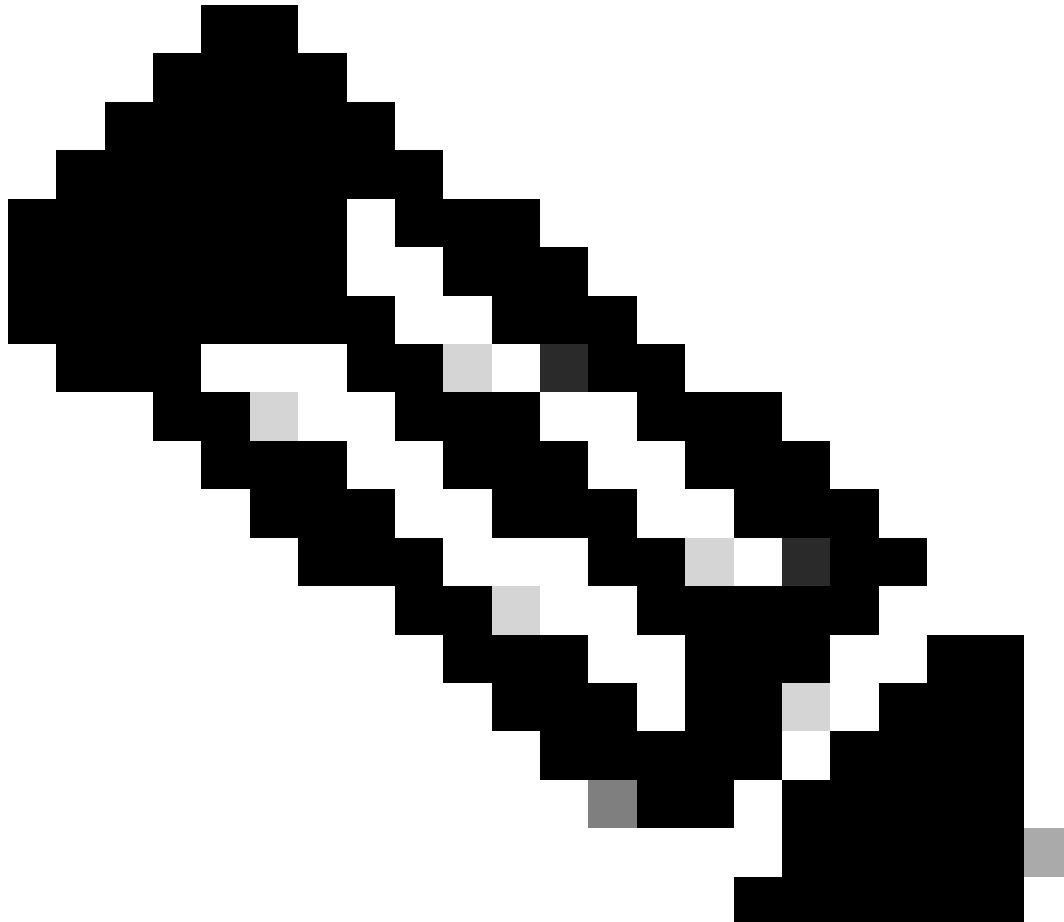
5. 구성 변경 사항을 배포합니다. 이제 컨피그레이션 변경 사항이 현재 관리 인터페이스를 통해 구축됩니다.

6. FTD CLI에서 정적 IP 주소를 사용하도록 관리 인터페이스를 설정하고 데이터 인터페이스로 게이트웨이를 설정합니다.

- `configure network {ipv4 | ipv6} manual ip_address netmask data-interfaces`

```
>  
>  
> configure network ipv4 manual IP_ADDRESS 192.168.1.8 NETMASK 255.255.255.0 GATEWAY data-interfaces  
Setting IPv4 network configuration...  
Interface eth0 speed is set to '10000baseT/Full'  
Network settings changed.
```

---

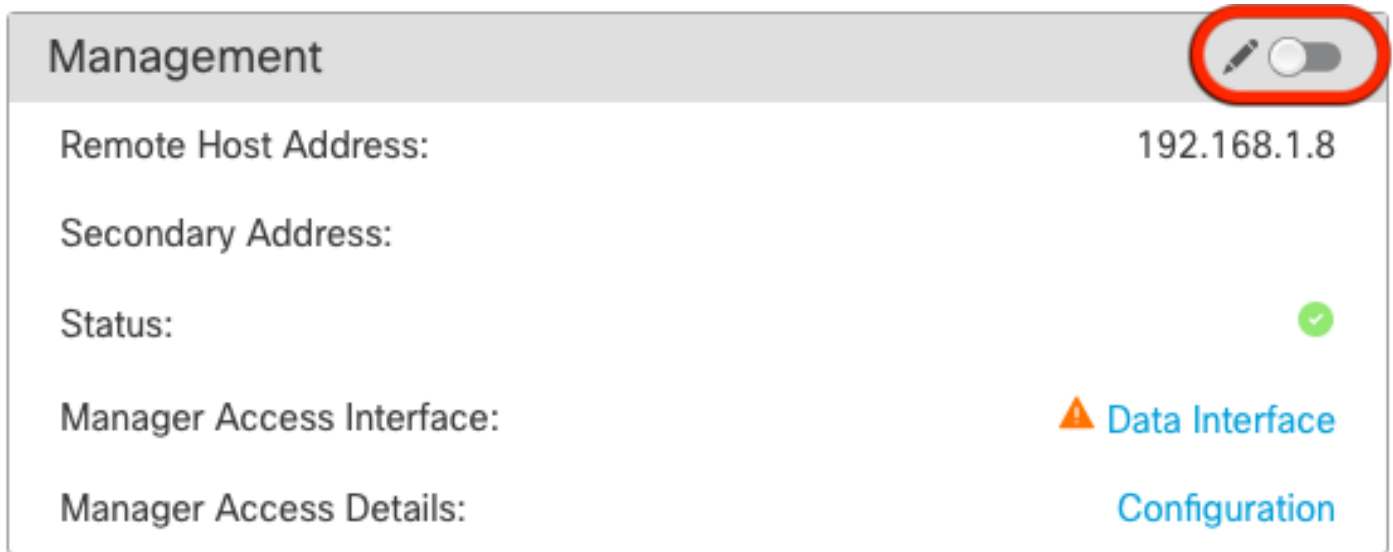


**참고:** 관리 인터페이스를 사용할 계획은 없지만 고정 IP 주소를 설정해야 합니다. 예를 들어 게이트웨이를 데이터 인터페이스로 설정할 수 있도록 개인 주소. 이 관리는 tap\_nlp 인터페이스를 사용하여 관리 트래픽을 데이터 인터페이스로 전달하는 데 사용됩니다.



---



7. Management Center에서 관리를 비활성화하고 Edit(편집)를 클릭하여 Remote Host Address IP address(원격 호스트 주소 IP 주소)를 업데이트한 다음 Devices(디바이스) > Device Management(디바이스 관리) > Device(디바이스) > Management(관리) 섹션에서 위협 방어를 위한 Secondary Address(선택 사항)Secondary Address(보조 주소)를 업데이트하고 연결을 활성화합니다.



The screenshot shows a 'Management' configuration panel. At the top right, there is a red circle around an edit icon (a pencil) and a toggle switch. Below this, the configuration items are listed:

- Remote Host Address: 192.168.1.8
- Secondary Address:
- Status: 
- Manager Access Interface:  Data Interface
- Manager Access Details: Configuration

플랫폼 설정에서 SSH 활성화

플랫폼 설정 정책에서 데이터 인터페이스에 대해 SSH를 활성화하고, Devices(디바이스) > Platform Settings(플랫폼 설정) > SSH Access(SSH 액세스)에서 이 디바이스에 적용합니다.Add(추가)를 클릭합니다.

- SSH 연결을 허용할 호스트 또는 네트워크.
- SSH 연결을 허용할 인터페이스를 포함하는 영역을 추가합니다. 영역에 없는 인터페이스의 경우 Selected Zones /Interfaces(선택한 영역/인터페이스) 목록에 인터페이스 이름을 입력하고 Add(추가)를 클릭할 수 있습니다.
- OK(확인)를 클릭합니다. 변경 사항을 배포합니다.

## Add Secure Shell Configuration



IP Address\*

+



Available Zones/Interfaces

C

- DMZ
- Inside
- outside

Add



Selected Zones/Interfaces

Interface Name

Add

Cancel

OK



**참고:** SSH는 데이터 인터페이스에서 기본적으로 활성화되어 있지 않으므로 SSH를 사용하여 위협 방어를 관리하려면 명시적으로 허용해야 합니다.

---

다음을 확인합니다.

데이터 인터페이스를 통해 관리 연결이 설정되었는지 확인합니다.

FMC GUI(Graphical User Interface)에서 확인

관리 센터에서 **Devices(디바이스) > Device Management(디바이스 관리) > Device(디바이스) > Management(관리) > Manager Access(관리자 액세스) - Configuration Details(컨피그레이션 세부사항) > Connection Status(연결 상태)** 페이지에서 관리 연결 상태

를 확인합니다.

The screenshot shows a 'Management' interface with a toggle switch in the top right corner. The interface displays the following information:

- Remote Host Address: 192.168.1.30
- Secondary Address:
- Status: **Connected** (indicated by a green arrow and a green checkmark icon)
- Manager Access Interface: [Data Interface](#)
- Manager Access Details: [Configuration](#)

FTD CLI(Command Line Interface)에서 확인

threat defenseCLI에서 관리 연결 상태를 보려면 sftunnel-status-brief 명령을 입력합니다.

```
>
> sftunnel-status-brief

PEER:192.168.1.2
Peer channel Channel-A is valid type (CONTROL), using 'tap_nlp', connected to '192.168.1.2' via '169.254.1.2'
Peer channel Channel-B is valid type (EVENT), using 'tap_nlp', connected to '192.168.1.2' via '169.254.1.2'
Registration: Completed.
IPv4 Connection to peer '192.168.1.2' Start Time: Tue Jul 16 22:23:54 2024 UTC
Heartbeat Send Time: Tue Jul 16 22:39:52 2024 UTC
Heartbeat Received Time: Tue Jul 16 22:39:52 2024 UTC
Last disconnect time : Tue Jul 16 22:17:42 2024 UTC
Last disconnect reason : Both control and event channel connections with peer went down
```

상태는 내부 tap\_nlp 인터페이스를 보여주는 데이터 인터페이스에 대한 성공적인 연결을 보여줍니다.

### 문제 해결

관리 센터에서 Devices(디바이스) > Device Management(디바이스 관리) > Device(디바이스) > Management(관리) > Manager Access(관리자 액세스) - Configuration Details(컨피그레이션 세부사항) > Connection Status(연결 상태) 페이지에서 관리 연결 상태를 확인합니다.

threat defenseCLI에서 관리 연결 상태를 보려면 sftunnel-status-brief 명령을 입력합니다. 또한 sftunnel-status를 사용하여 더 자세한 정보를 볼 수 있습니다.

관리 연결 상태

작업 시나리오

> sftunnel-status-brief

```
PEER:192.168.1.2
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '192.168.1.2' via '192.168.1.8'
Peer channel Channel-B is valid type (EVENT), using 'tap_nlp', connected to '192.168.1.2' via '169.254.1.2'
Registration: Completed.
IPv4 Connection to peer '192.168.1.2' Start Time: Wed Jul 17 06:21:15 2024 UTC
Heartbeat Send Time: Wed Jul 17 17:15:20 2024 UTC
Heartbeat Received Time: Wed Jul 17 17:16:55 2024 UTC
Last disconnect time : Wed Jul 17 06:21:12 2024 UTC
Last disconnect reason : Process shutdown due to stop request from PM
```

## 비작업 시나리오

> sftunnel-status-brief

```
PEER:192.168.1.2
Registration: Completed.
Connection to peer '192.168.1.2' Attempted at Wed Jul 17 17:20:26 2024 UTC
Last disconnect time : Wed Jul 17 17:20:26 2024 UTC
Last disconnect reason : Both control and event channel connections with peer went down
```

## 네트워크 정보 확인

Threat defenseCLI에서 Management 및 Manager 액세스 데이터 인터페이스 네트워크 설정을 확인합니다.

> show network

```
> show network
===== [ System Information ] =====
Hostname                : ftdcdo.breakstuff.com
Domains                 : breakstuff.com
DNS Servers             : 192.168.1.103
DNS from router        : enabled
Management port        : 8305
IPv4 Default route
  Gateway               : data-interfaces
IPv6 Default route
  Gateway               : data-interfaces

===== [ eth0 ] =====
State                   : Enabled
Link                    : Up
Channels                : Management & Events
Mode                    : Non-Autonegotiation
MDI/MDIX                : Auto/MDIX
MTU                     : 1500
MAC Address             : 00:0C:29:54:D4:47
----- [ IPv4 ] -----
Configuration          : Manual
Address                : 192.168.1.8
Netmask                : 255.255.255.0
Gateway                : 192.168.1.1
----- [ IPv6 ] -----
Configuration          : Disabled

===== [ Proxy Information ] =====
State                   : Disabled
Authentication         : Disabled

===== [ System Information - Data Interfaces ] =====
DNS Servers            :
Interfaces             : GigabitEthernet0/0

===== [ GigabitEthernet0/0 ] =====
State                   : Enabled
Link                    : Up
Name                    : Outside
MTU                     : 1500
MAC Address            : 00:0C:29:54:D4:5B
```

---

참고: 이 명령은 관리 연결의 현재 상태를 표시하지 않습니다.

---

## 네트워크 연결 확인

### Management Center에 Ping하기

threat defenseCLI에서 명령을 사용하여 데이터 인터페이스에서 관리 센터를 ping합니다.

> **fmc\_ip ping**

```
> ping 192.168.1.2
Please use 'CTRL+C' to cancel/abort...
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

threat defenseCLI에서 명령을 사용하여 관리 센터를 Management 인터페이스에서 ping합니다. 이 인터페이스는 백플레인을 통해 데이터 인터페이스로 라우팅합니다.

> 시스템 **fmc\_ip ping**

```
> ping system 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_seq=1 ttl=64 time=0.340 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=64 time=0.291 ms
64 bytes from 192.168.1.2: icmp_seq=3 ttl=64 time=0.333 ms
64 bytes from 192.168.1.2: icmp_seq=4 ttl=64 time=0.282 ms
^C
--- 192.168.1.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 132ms
rtt min/avg/max/mdev = 0.282/0.311/0.340/0.030 ms
```

### 인터페이스 상태, 통계 및 패킷 수 확인

threat defenseCLI에서 내부 백플레인 인터페이스인 nlp\_int\_tap에 대한 정보를 참조하십시오.

> 인터페이스 세부사항 표시

```
Interface Internal-Data0/1 "nlp_int_tap", is up, line protocol is up
Hardware is en_vtun rev00, BW Unknown Speed-Capability, DLY 1000 usec
(Full-duplex), (1000 Mbps)
Input flow control is unsupported, output flow control is unsupported
MAC address 0000.0100.0001, MTU 1500
IP address 169.254.1.1, subnet mask 255.255.255.248
311553 packets input, 41414494 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
232599 packets output, 165049822 bytes, 0 underruns
0 pause output, 0 resume output
0 output errors, 0 collisions, 0 interface resets
0 late collisions, 0 deferred
0 input reset drops, 0 output reset drops
input queue (blocks free curr/low): hardware (0/0)
output queue (blocks free curr/low): hardware (0/0)
Traffic Statistics for "nlp_int_tap":
  311553 packets input, 37052752 bytes
  232599 packets output, 161793436 bytes
  167463 packets dropped
  1 minute input rate 0 pkts/sec, 3 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, 3 bytes/sec
  5 minute output rate 0 pkts/sec, 0 bytes/sec
  5 minute drop rate, 0 pkts/sec
Control Point Interface States:
  Interface number is 14
  Interface config status is active
  Interface state is active
```

FTD에서 FMC에 연결하기 위한 경로 검증

threat defenseCLI에서 기본 경로(S\*)가 추가되었고 관리 인터페이스(nlp\_int\_tap)에 대한 내부 NAT 규칙이 있는지 확인합니다.

> 경로 표시



```
> show route
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, + - replicated route
SI - Static InterVRF, BI - BGP InterVRF
```

```
Gateway of last resort is not set
```

```
C      192.168.1.0 255.255.255.0 is directly connected, Outside
L      192.168.1.30 255.255.255.255 is directly connected, Outside
```

```
> nat 표시
```

```
> show nat
Manual NAT Policies Implicit (Section 0)
1 (nlp_int_tap) to (Outside) source static nlp_server__sftunnel_0.0.0.0_intf3 interface destination static 0_0.0.0.0_5 0_0.0.0.0_5 service tcp 8305 8305
  translate_hits = 5, untranslate_hits = 6
2 (nlp_int_tap) to (Outside) source static nlp_server__sftunnel::_intf3 interface ipv6 destination static 0::_6 0::_6 service tcp 8305 8305
  translate_hits = 0, untranslate_hits = 0
3 (nlp_int_tap) to (Outside) source dynamic nlp_client_0_intf3 interface
  translate_hits = 10, untranslate_hits = 0
4 (nlp_int_tap) to (Outside) source dynamic nlp_client_0_ipv6_intf3 interface ipv6
  translate_hits = 0, untranslate_hits = 0
```

Sftunnel 및 연결 통계 확인

```
> show running-config sftunnel
```

```
> show running-config sftunnel
sftunnel interface Outside
sftunnel port 8305
```



**경고:** 관리자 액세스 권한을 변경하는 과정에서 FTD에서 관리자를 삭제하거나 FMC에서 FTD를 등록 취소/강제 삭제하지 마십시오.

---

#### 관련 정보

- [DNS over Platform 설정 구성](#)
- [FMC를 통해 FTD\(HTTPS 및 SSH\)에 대한 관리 액세스 구성](#)

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.