FMC에서 관리 및 진단 인터페이스 병합 구성

목차

소개

이 문서에서는 FTD 7.4.0 버전 릴리스에 추가된 기능인 관리 및 진단 인터페이스의 병합을 구성하는 단계에 대해 설명합니다.

사전 요구 사항

Cisco에서는 다음 항목에 대한 지식이 있는 것을 권장합니다.

- Cisco FTD(Secure Firewall Threat Defense)
- Cisco FMC(Secure Firewall Manager Center)

배경 정보

7.3 이전 버전에서는 물리적 관리 인터페이스가 Lina(Diagnostic Logical Interface)와 Linux(Management Logical Interface) 간에 공유됩니다.

버전 7.4 이상에서는 간소화된 사용자 환경을 위해 Diagnostic 인터페이스가 Management와 병합됩니다.
7.4 이상을 사용하는 새 디바이스의 경우 레거시 진단 인터페이스를 사용할 수 없습니다. 병합된 관리 인터페이스만 사용할 수 있습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

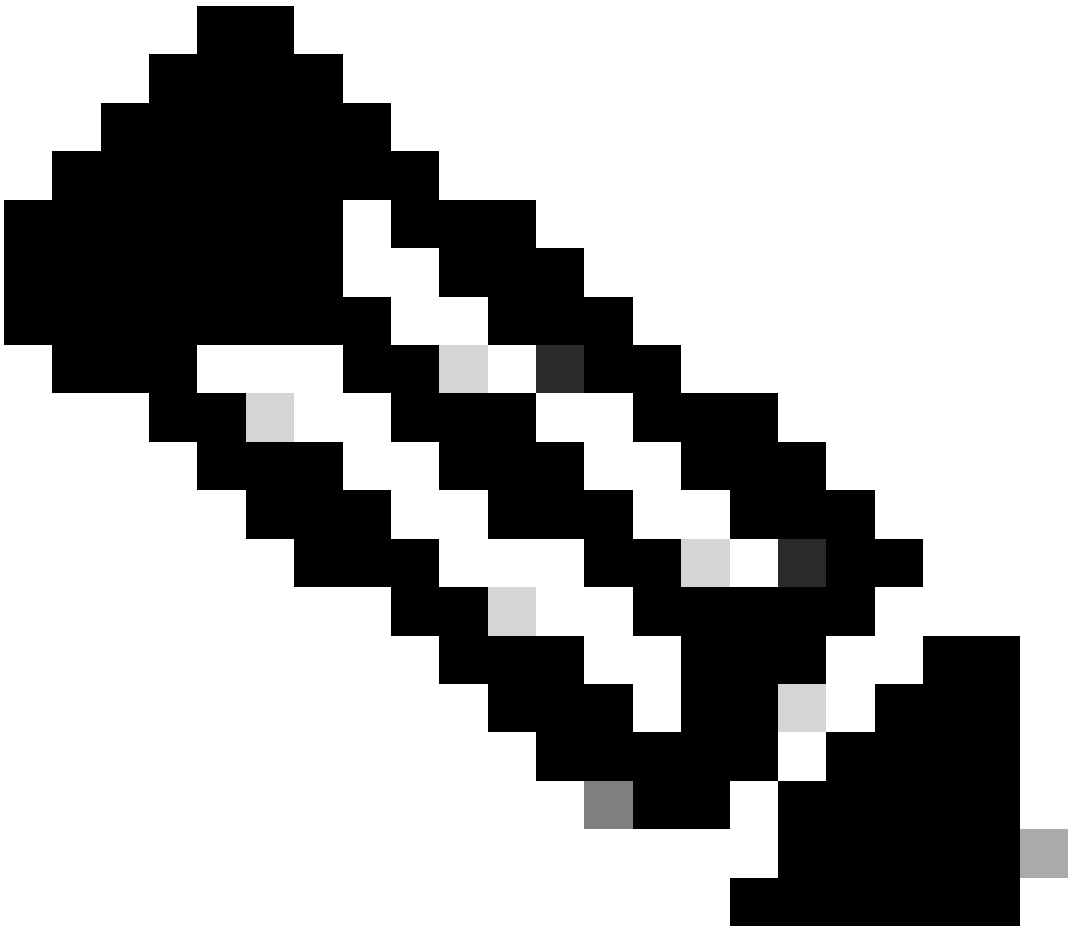
- Virtual Cisco FTD(Secure Firewall Threat Defense) 버전 7.4.2
- Virtual Cisco FMC(Secure Firewall Manager Center) 버전 7.4.2

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.

구성

7.4 이상으로 업그레이드하고 진단 인터페이스에 대한 컨피그레이션이 있는 경우, 인터페이스를 수동으로 병합하거나 별도의 진단 인터페이스를 계속 사용할 수 있습니다.

진단 인터페이스에 대한 컨피그레이션이 없는 경우 인터페이스 병합이 자동으로 수행됩니다.

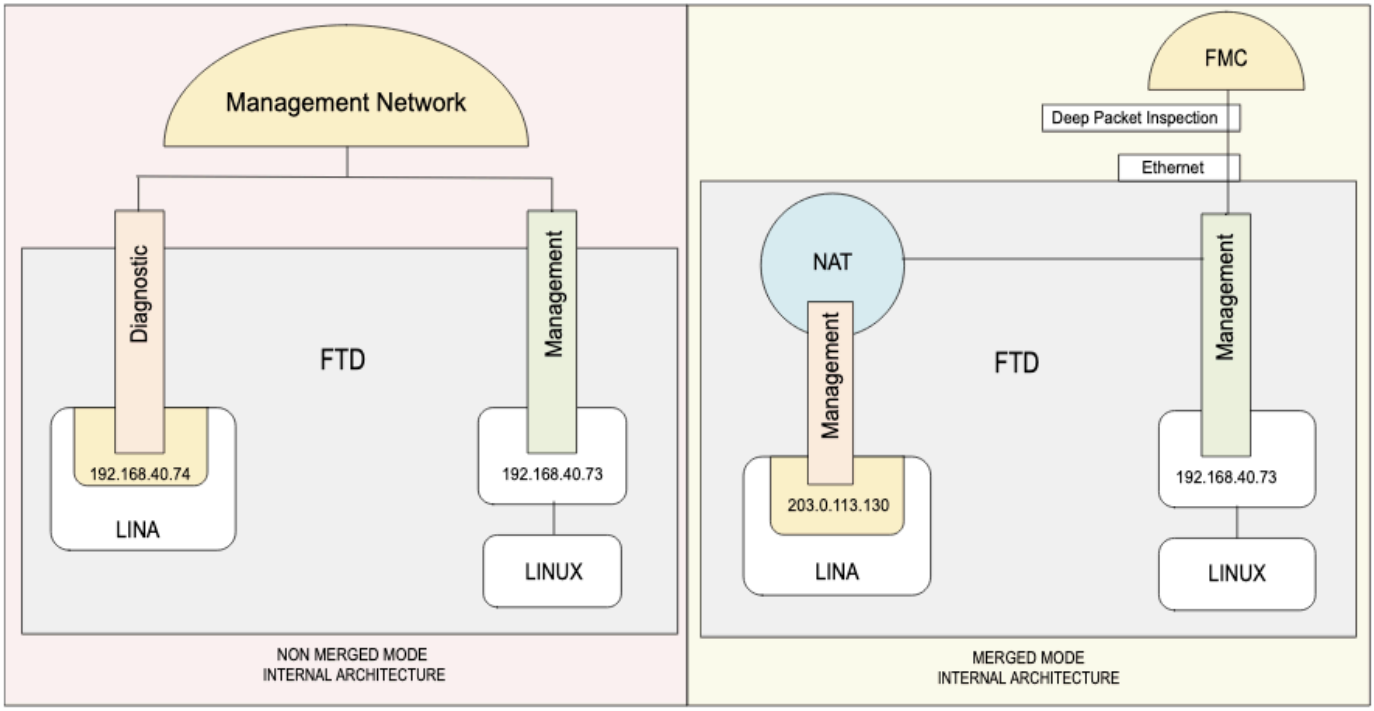


참고: 진단 인터페이스에 대한 지원은 이후 릴리스에서 제거될 예정이므로 가능한 한 빨리

인터페이스를 병합할 계획입니다.

FTD 내부 아키텍처 다이어그램

통합 관리 인터페이스 개요



Convergence Management Interface 전후의 내부 아키텍처 개요

왼쪽에는 Lina(Diagnostic Logical Interface) 및 Linux(Management Logical Interface)의 내부 아키텍처가 있습니다. 버전 7.3 이전.

오른쪽에는 단일 관리 인터페이스를 위한 내부 아키텍처가 있습니다. 관리 네트워크에 대한 Lina 액세스는 NAT 서비스를 사용합니다.

수렴 절차

컨피그레이션이 진단 인터페이스에 있는 경우, 업그레이드 후 인터페이스가 자동으로 병합되지 않으며 통합 절차를 수행해야 합니다.

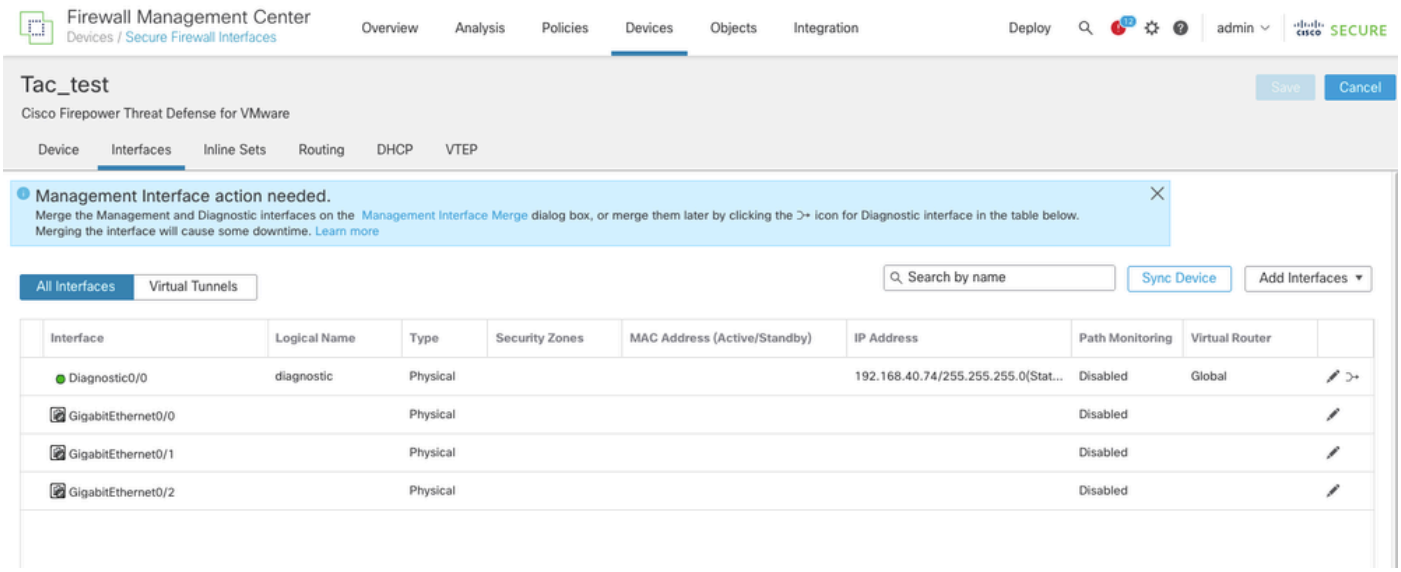
이 절차에서는 컨피그레이션 변경 사항을 승인해야 하며, 경우에 따라 수동으로 컨피그레이션을 수정해야 합니다.

디바이스의 현재 모드를 보려면 FTD CLI Client에서 show management-interface converge 명령을 입력합니다

```
> show management-interface convergence
no management-interface convergence
```

그러면 관리 인터페이스가 병합되지 않은 것입니다.

1단계.
FMC UI에서 Devices(디바이스) > Device Management(디바이스 관리)로 이동하고 편집할 FTD를 선택합니다. Interfaces(인터페이스) 탭으로 바로 열립니다.

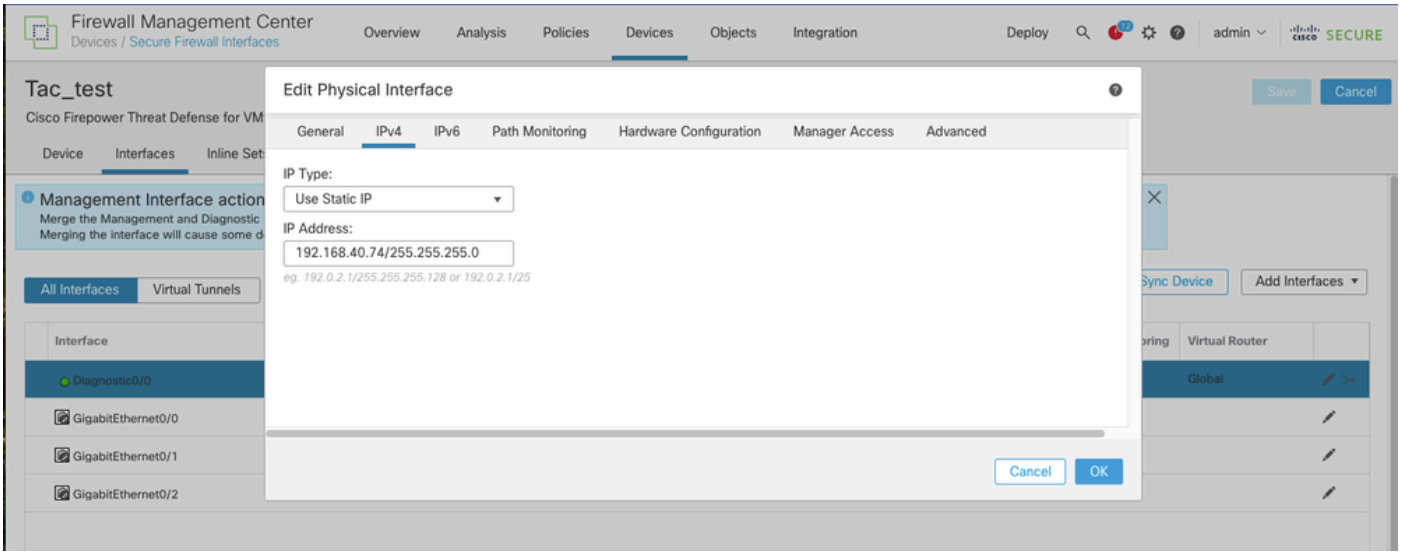


소프트웨어 버전 7.4.2로 디바이스를 업그레이드한 후 진단 및 관리 인터페이스를 병합하기 위해 필요한 작업

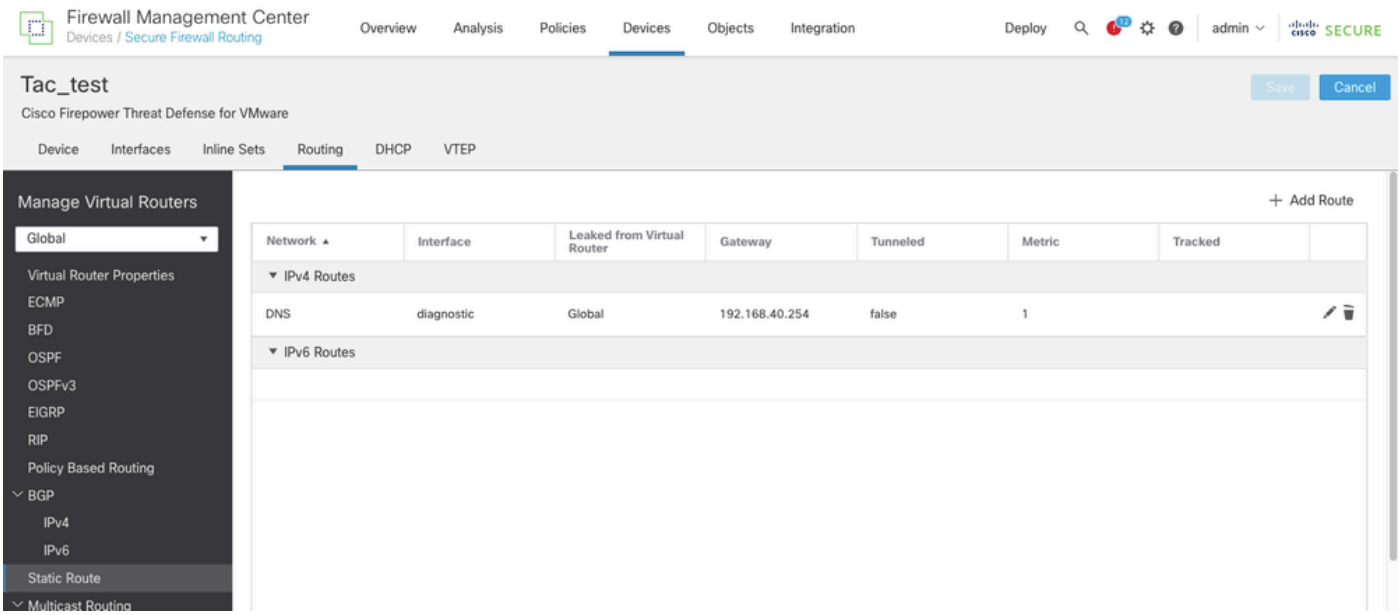
2단계.

진단 인터페이스에서 모든 컨피그레이션을 제거합니다. Diagnostic 인터페이스에 병합을 계속할 구성이 없어야 합니다.

예를 들어, 이 진단 인터페이스에는 다음이 있습니다. IP 주소 및 고정 경로.



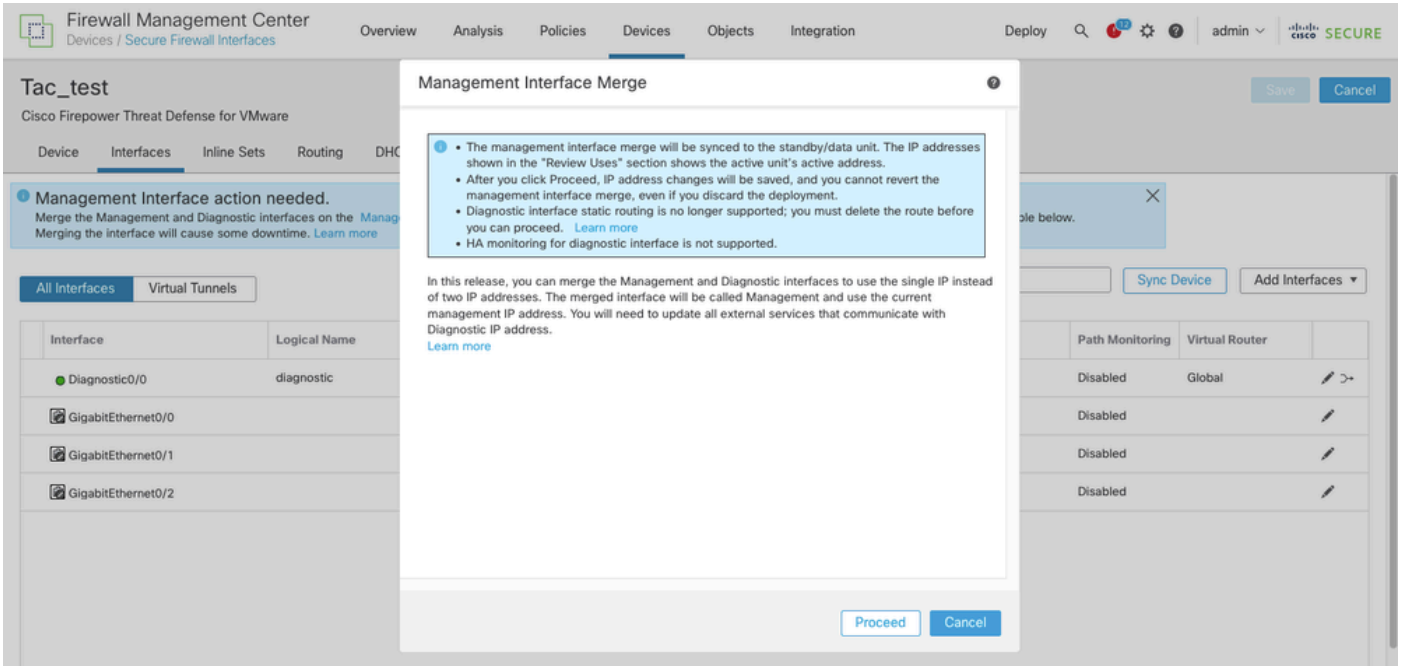
진단 인터페이스 IP 주소 제거



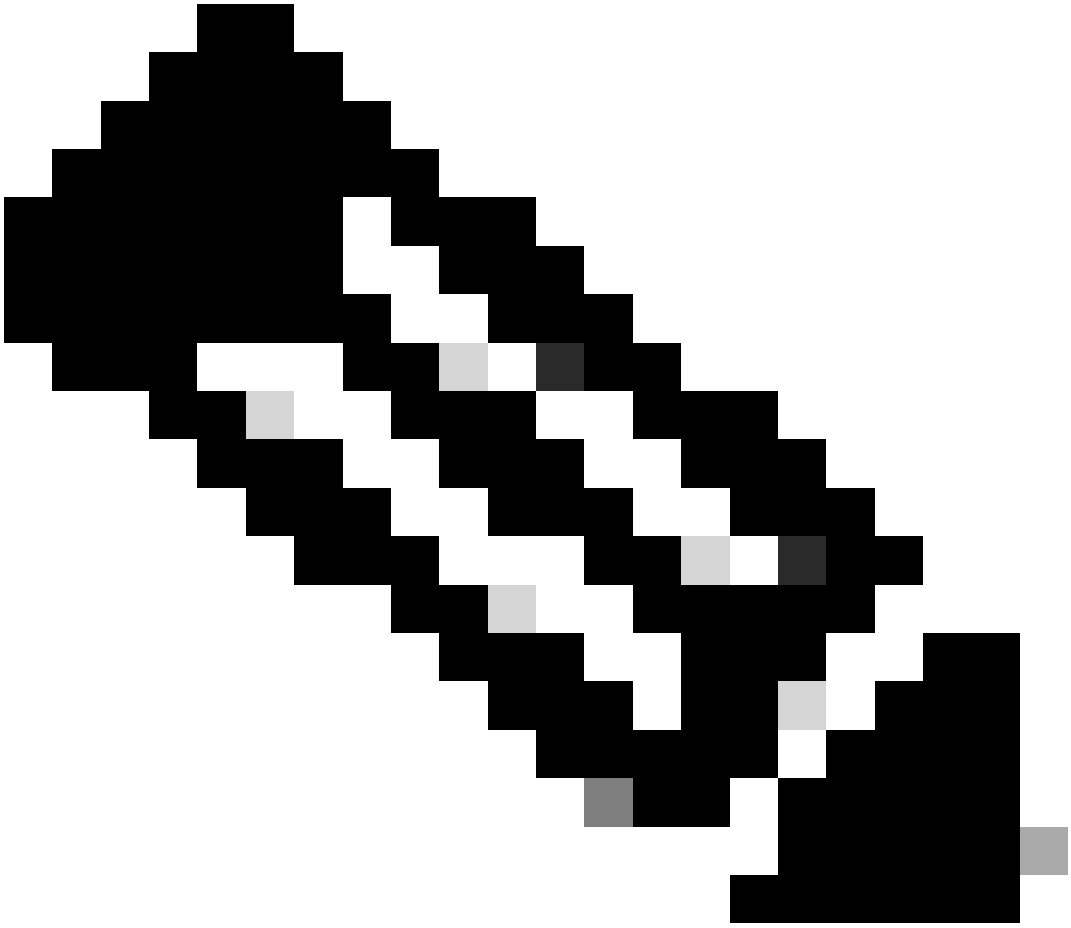
진단 인터페이스에서 고정 경로 구성

3단계.

Management Interface Merge action needed(관리 인터페이스 병합 작업 필요) 영역이나 Diagnostic(진단) 인터페이스에서 Edit(수정) 아이콘(연필) 옆에 있는 Merge(병합) 아이콘을 클릭합니다.

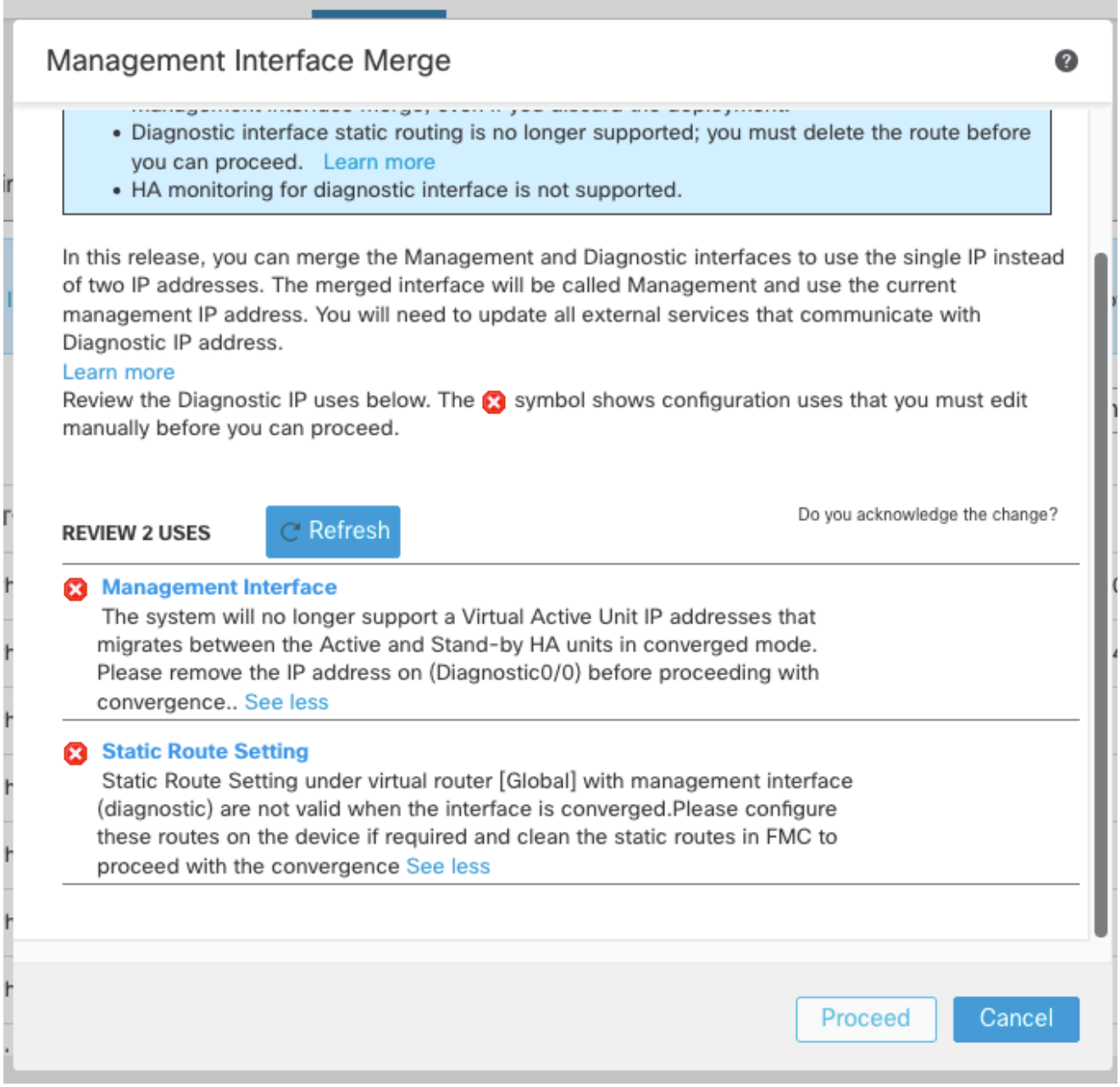


계속하기 전에 관리 인터페이스 병합 정보



참고: 고가용성 쌍 및 클러스터의 경우 활성/제어 유닛에서 이 작업을 수행합니다. 병합된 컨피그레이션은 대기/데이터 유닛에 자동으로 복제됩니다.

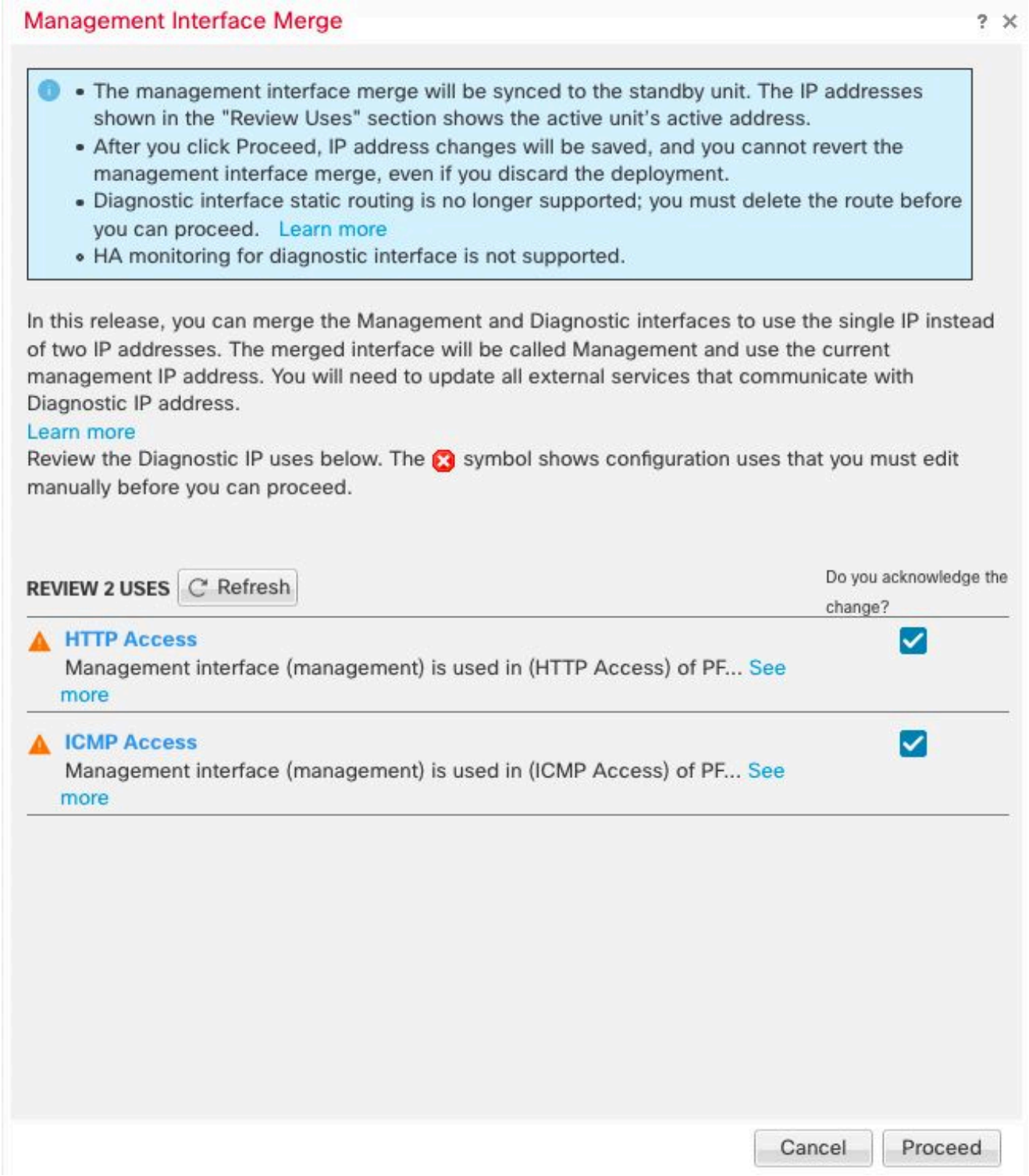
- 수동 변경 또는 제거가 필요한 경우 경고 아이콘이 나타날 수 있습니다.



병합하기 전에 제거해야 하는 구성에 대한 경고 예시

그렇다면: 대화 상자를 취소하고 컨피그레이션 제거 또는 재컨피그레이션을 진행한 다음 Management Interface Merge 대화 상자를 다시 엽니다.

- 디바이스에서 작동할 플랫폼 설정은 주의 아이콘으로 표시되며 확인이 필요합니다.



편집해야 하는 플랫폼 설정 컨피그레이션의 경고 예

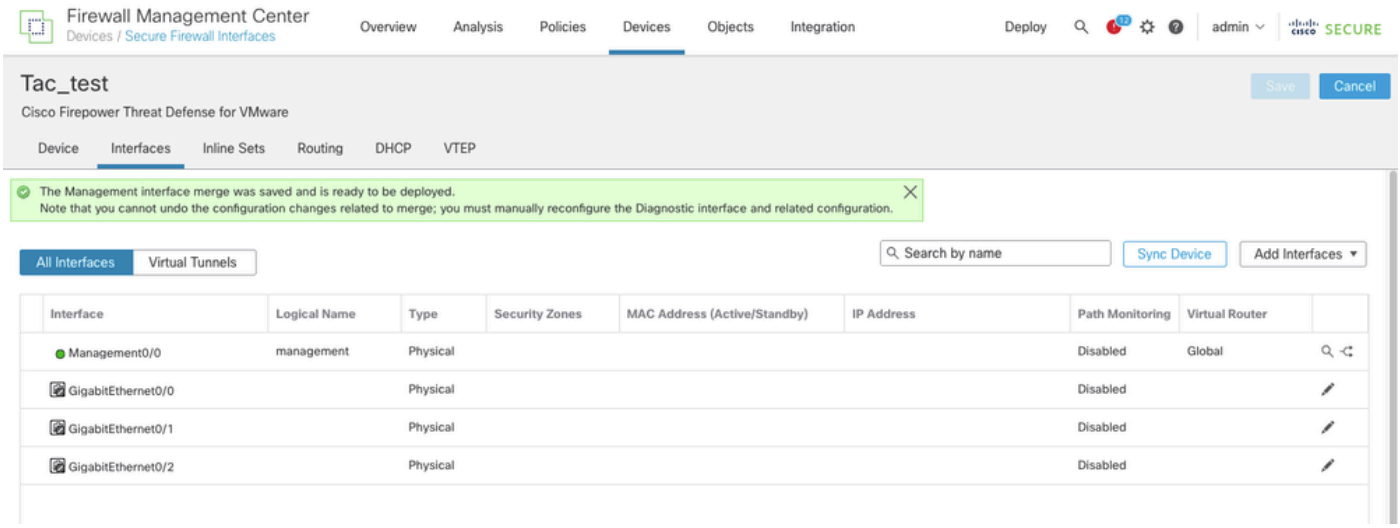
- Do you acknowledge the change?(변경 사항을 승인합니까?)의 상자를 클릭합니다. 열을 클릭한 다음 Proceed(진행)를 클릭합니다.

4단계.

컨피그레이션이 병합되면 성공의 배너가 표시됩니다.
"관리 인터페이스 병합이 저장되었으며 배포할 준비가 되었습니다.

병합과 관련된 컨피그레이션 변경 사항은 실행 취소할 수 없습니다. 진단 인터페이스 및 관련 컨피그레이션을 수동으로 다시 구성해야 합니다."

병합된 새 컨피그레이션을 구축합니다.



관리 인터페이스 병합이 저장되었으며 배포할 준비가 되었습니다.

관리 인터페이스는 읽기 전용이지만 Interfaces 페이지에 표시됩니다.

구축 후에는 관리 인터페이스의 컨버전스 절차가 완료됩니다.

5단계. 선택 사항

진단 인터페이스와 통신하는 외부 서비스가 있는 경우 컨버전스 모드에서 관리 경로 대체가 제거되었으므로 해당 컨피그레이션을 변경하여 관리 인터페이스 IP 주소를 사용해야 합니다.

예를 들면 다음과 같습니다.

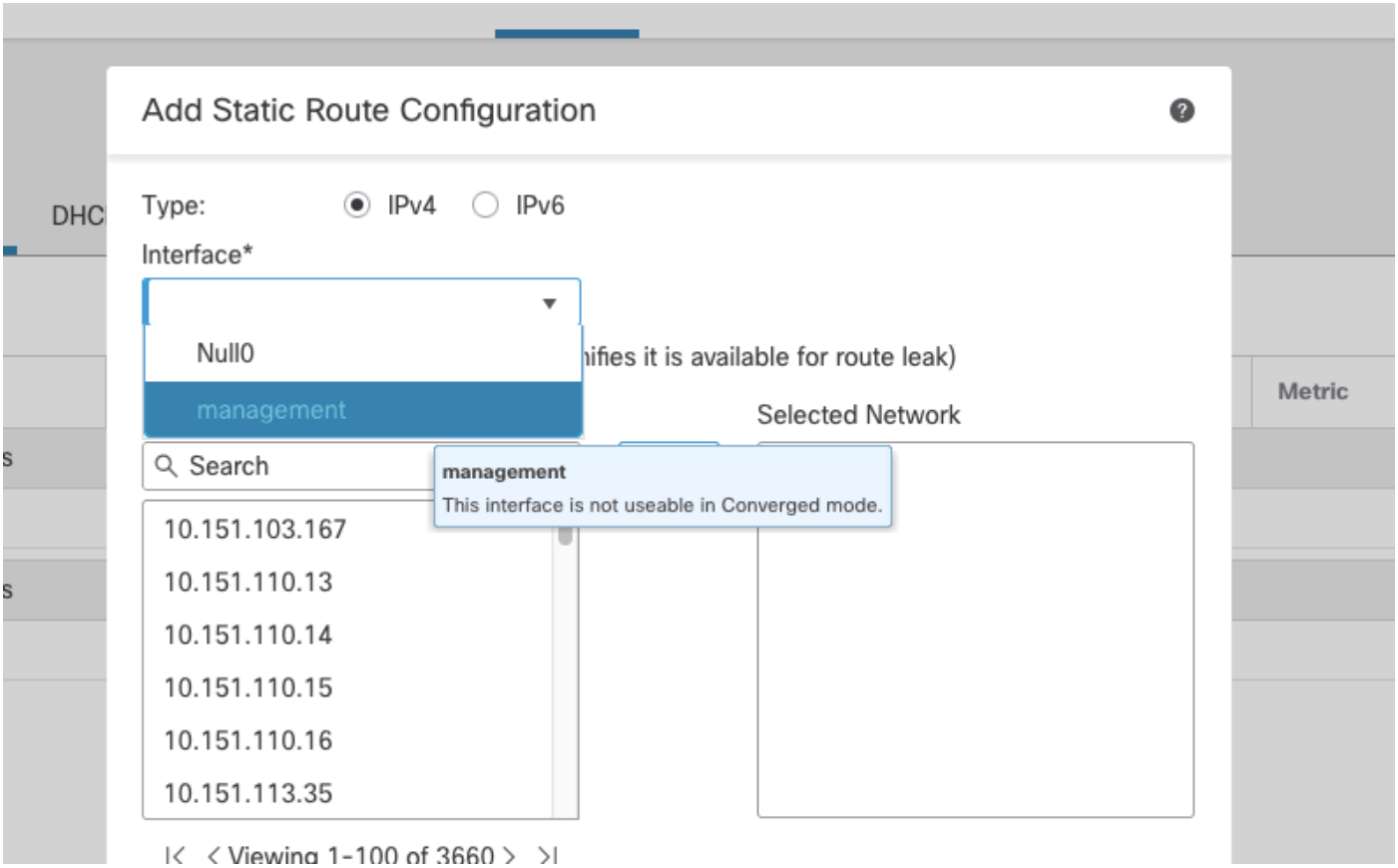
- SNMP 클라이언트
- RADIUS 서버
- 관리 네트워크를 통해 DNS 서버에 연결할 수 있으려면 사용자가 명시적으로 "Enable DNS Lookup via diagnostic/Management Interface also"를 선택해야 합니다. 예외가 DNS 조회 및 ICMP(ping 및 traceroute)에 대해 설정되었으므로 Platform Settings(플랫폼 설정) > DNS 컨피그레이션에서 다음을 수행합니다. 이러한 경우 위협 방어는 데이터를 사용한 다음 경로를 찾을 수 없는 경우 자동으로 관리로 돌아갑니다.

관리 인터페이스에 대한 고정 경로 사용은 FTD CLI Client(Linux)를 통해서만 구성할 수 있습니다

Lina 관리 포트 기본 경로는 모든 프레임을 Linux 모듈로 전송합니다.

```
> configure network static-routes ipv4 add management ?
  IP address AAA.BBB.CCC.DDD where each part is in the range 0-255  destination address
```

FMC UI에서 관리 인터페이스는 선택을 위해 회색으로 비활성화됩니다.



병합이 완료된 후에는 고정 경로에서 관리 인터페이스를 선택할 수 없습니다.

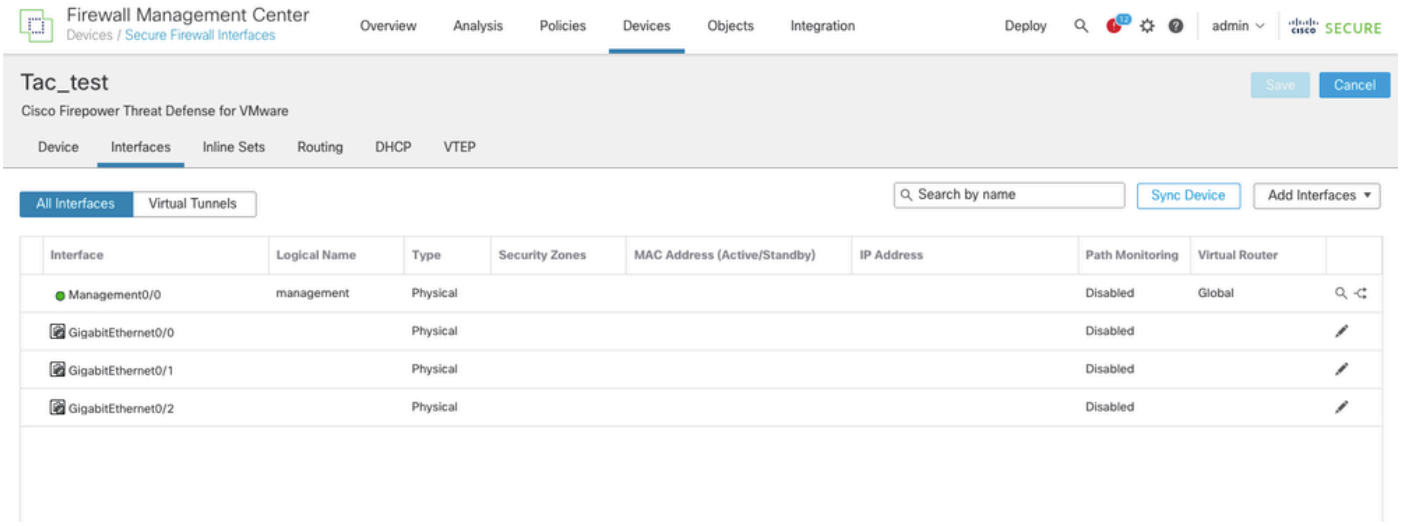
다음을 확인합니다.

관리 인터페이스에서 병합 후 예상되는 변경 사항

- 명령을 실행하여 FTD CLI Client에서 컨버전스 모드를 확인합니다

```
> show management-interface convergence
management-interface convergence
```

- FMC UI에서 인터페이스 이름은 Management0/0, 논리적 이름은 management로 변경됩니다.



관리 인터페이스 이름 및 논리 이름에 대한 병합 확인

- FTD CLI Client에서 새 IP 주소는 Lina for Management 인터페이스에 자동으로 구성됩니다. NAT는 내부 구현으로 사용됩니다. 내부 개인 IPv4 주소 203.0.113.130 및 IPv6 주소 fd00:0:1:1::2가 할당된 것입니다(둘 다 변경될 수 있음).
  이러한 IP는 공용 Linux 커널 FTD IPv4 및 IPv6 주소에 NAT되므로 더 이상 Lina에 공용 IP가 필요하지 않습니다.

  전문가 모드에서 "ifconfig"는 Linux용 내부 IPv4(203.0.113.129) 및 IPv6(fd00:0:1:1::1) 주소를 표시합니다.

```
FTD CLI Clish:
> show interface management
Interface Management0/0 "management", is up, line protocol is up
  Hardware is en_vtun rev00, DLY 10 usec
        Input flow control is unsupported, output flow control is unsupported
        MAC address 0050.56b3.f75d, MTU 1500
        IP address 203.0.113.130, subnet mask 255.255.255.248

Expert mode on Linux:
root@ftd01:/home/admin# ifconfig
...
tap5: flags=4419



         mtu 1500
        inet 203.0.113.129  netmask 255.255.255.248  broadcast 203.0.113.135
        inet6 fe80::8403:9ff:fefb:6d16  prefixlen 64  scopeid 0x20


        inet6 fd00:0:1:1::1  prefixlen 123  scopeid 0x0
```

문제 해결 - 사례 연구

이 연구 사례에서 가상 FTD의 진단 인터페이스는 7.4.2로 업그레이드하기 전에 DNS 조회의 외부 서비스에 연결하기 위한 별도의 IP 주소를 구성했습니다.

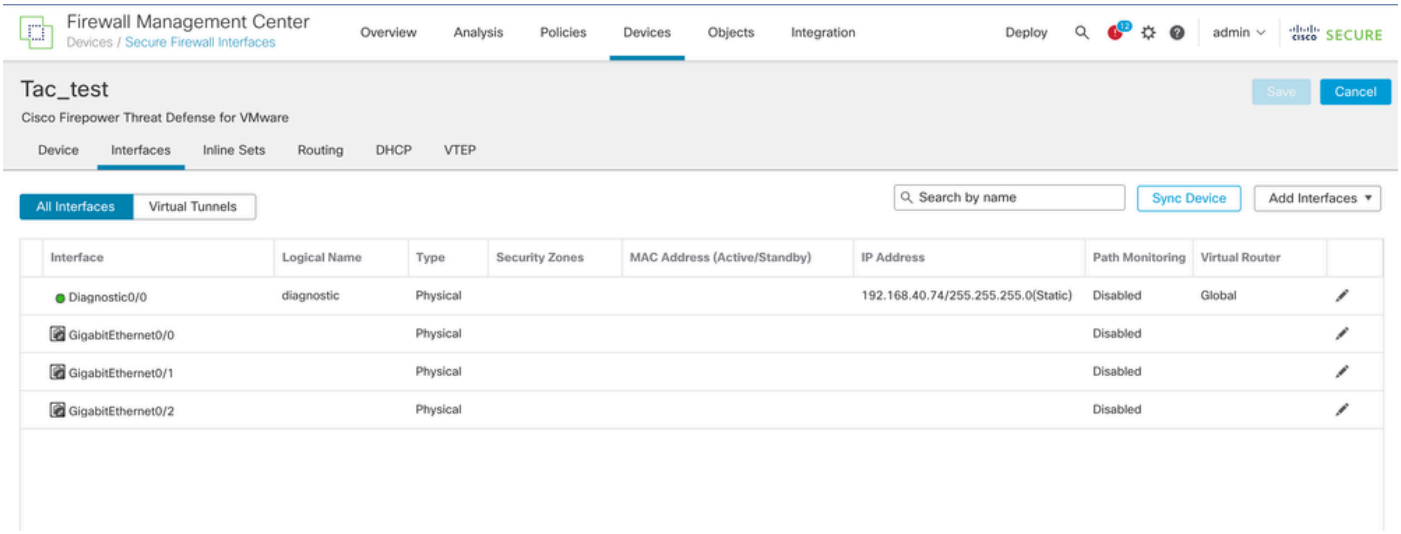
7.4.2로 업그레이드한 후에는 통합이 필요하며, 병합 전후에 FMC UI, FTD CLI Lina 및 Linux의 컨피그레이션이 이와 같습니다.

또한 FTD CLI Lina 및 Linux에 트래픽 캡처가 있어 논리적 진단 인터페이스를 사용하여 관리 인터페이스를 사용하도록 이동하는 트래픽을 보여줍니다.

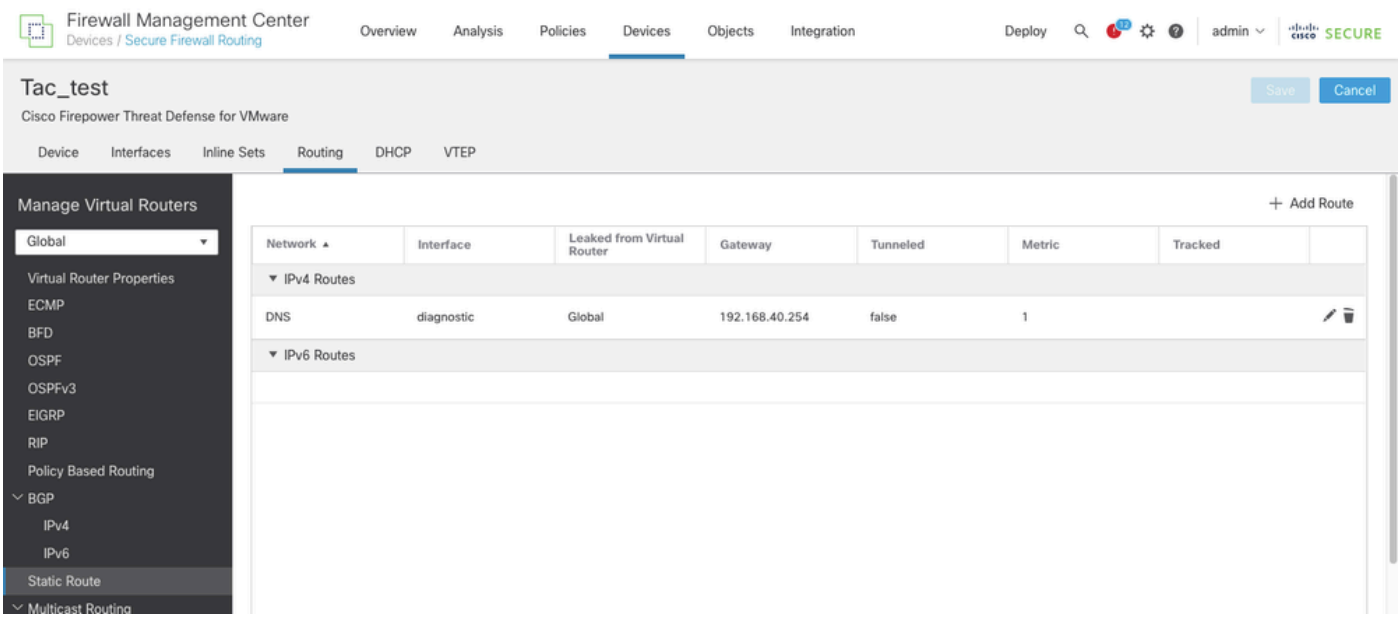
컨버전스 컨피그레이션 전

진단 인터페이스에는 DNS 조회를 위한 별도의 IP 및 고정 경로가 있습니다. 이 방식은 FTD에서 Lina에서 Linux로의 논리적 인터페이스를 모두 사용하여 작동합니다.

FMC UI 컨피그레이션

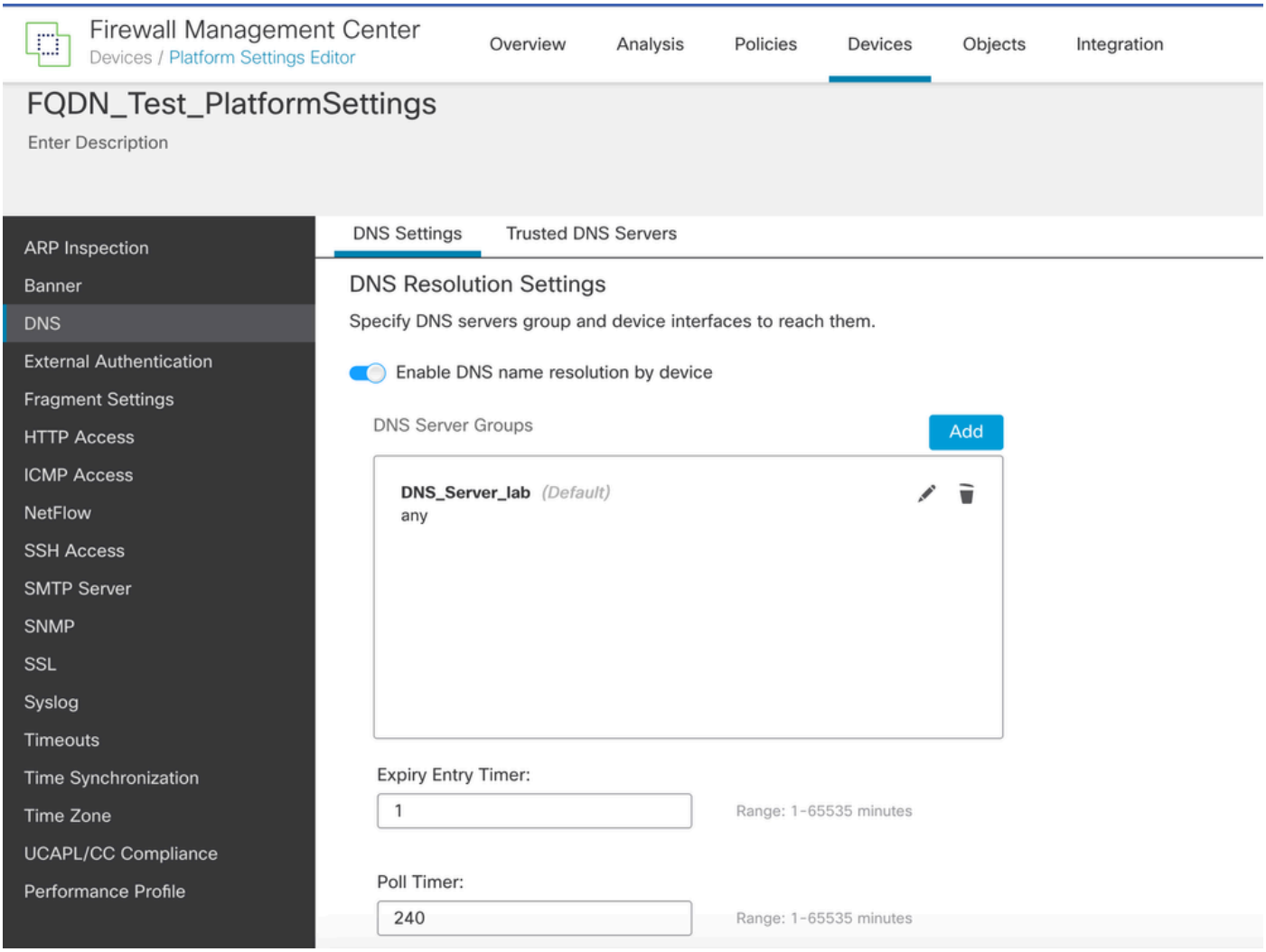


병합 전 진단 인터페이스 컨피그레이션

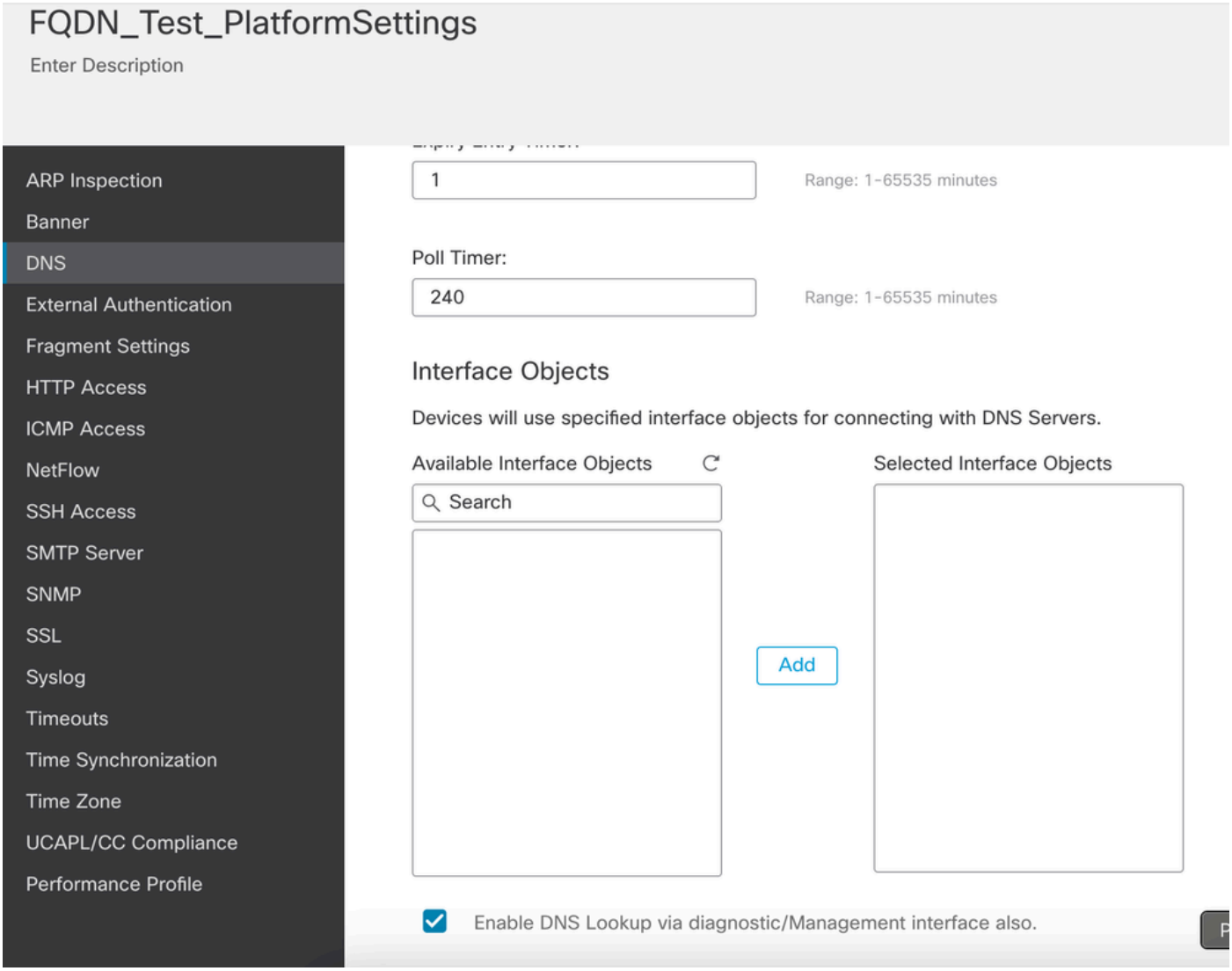


DNS 구성

Devices(디바이스) > Platform Settings(플랫폼 설정)에서 정책을 선택한 다음 DNS 탭을 선택합니다.



플랫폼 설정의 DNS 컨피그레이션



Enable DNS Lookup via diagnostic/Management interface(진단/관리 인터페이스를 통한 DNS 조회 활성화)에 대해 선택된 확인란

FTD Lina를 통한 진단 인터페이스 컨피그레이션

```
interface Management0/0
 management-only
 nameif diagnostic
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
 security-level 0
 ip address 192.168.40.74 255.255.255.0

ftd01# sh ip
System IP Addresses:
Interface                Name                IP address      Subnet mask     Method
Management0/0            diagnostic          192.168.40.74   255.255.255.0   manual
Current IP Addresses:
Interface                Name                IP address      Subnet mask     Method
Management0/0            diagnostic          192.168.40.74   255.255.255.0   manual

ftd01# sh route management-only
Routing Table: mgmt-only
```

```
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

S        10.10.10.10 255.255.255.255 [1/0] via 192.168.40.254, diagnostic
C        192.168.40.0 255.255.255.0 is directly connected, diagnostic
L        192.168.40.74 255.255.255.255 is directly connected, diagnostic
```

FTD CLI Lina의 DNS 컨피그레이션

```
ftd01# sh run dns
dns domain-lookup diagnostic
DNS server-group DNS_Server_lab
    retries 5
    timeout 15
    name-server 10.10.10.10 diagnostic
    domain-name test.lab
DNS server-group DefaultDNS
dns-group DNS_Server_lab
```

DNS 서버 10.10.10.10으로 이동하는 DNS 트래픽에 대한 진단 인터페이스에서 캡처

```
ftd01# sh cap
capture diag type raw-data trace detail interface diagnostic [Capturing - 340 bytes]
  match udp any host 10.10.10.10 eq domain

ftd01# sh cap diag

5 packets captured

   1: 00:15:39.660442       192.168.40.74.59939 > 10.10.10.10.53:  udp 27
   2: 00:15:54.661953       192.168.40.74.59939 > 10.10.10.10.53:  udp 27
   3: 00:16:09.661739       192.168.40.74.59939 > 10.10.10.10.53:  udp 27
   4: 00:16:24.667674       192.168.40.74.59939 > 10.10.10.10.53:  udp 27
   5: 00:16:39.684946       192.168.40.74.59939 > 10.10.10.10.53:  udp 27
5 packets shown
ftd01#
```

Linux expert 모드에서 캡처하여 진단 인터페이스에서 관리 인터페이스의 DNS 조회 트래픽의 올바른 흐름을 확인합니다.

```
root@ftd01:/home/admin# tcpdump -i br1 port 53
```

```
HS_PACKET_BUFFER_SIZE is set to 4.
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on br1, link-type EN10MB (Ethernet), capture size 262144 bytes
04:58:14.648941 IP 192.168.40.74.49171 > 10.10.10.10.domain: 5655+ AAAA? cisco.com. (27)
04:58:29.656317 IP 192.168.40.74.11606 > 10.10.10.10.domain: 26905+ A? cisco.com. (27)
04:58:44.686568 IP 192.168.40.74.11606 > 10.10.10.10.domain: 24324+ A? cisco.com. (27)
04:58:59.704586 IP 192.168.40.74.11606 > 10.10.10.10.domain: 35592+ A? cisco.com. (27)
04:59:14.742685 IP 192.168.40.74.11606 > 10.10.10.10.domain: 40993+ A? cisco.com. (27)
04:59:29.763690 IP 192.168.40.74.11606 > 10.10.10.10.domain: 62225+ A? cisco.com. (27)
04:59:44.796484 IP 192.168.40.74.11606 > 10.10.10.10.domain: 25350+ A? cisco.com. (27)
```

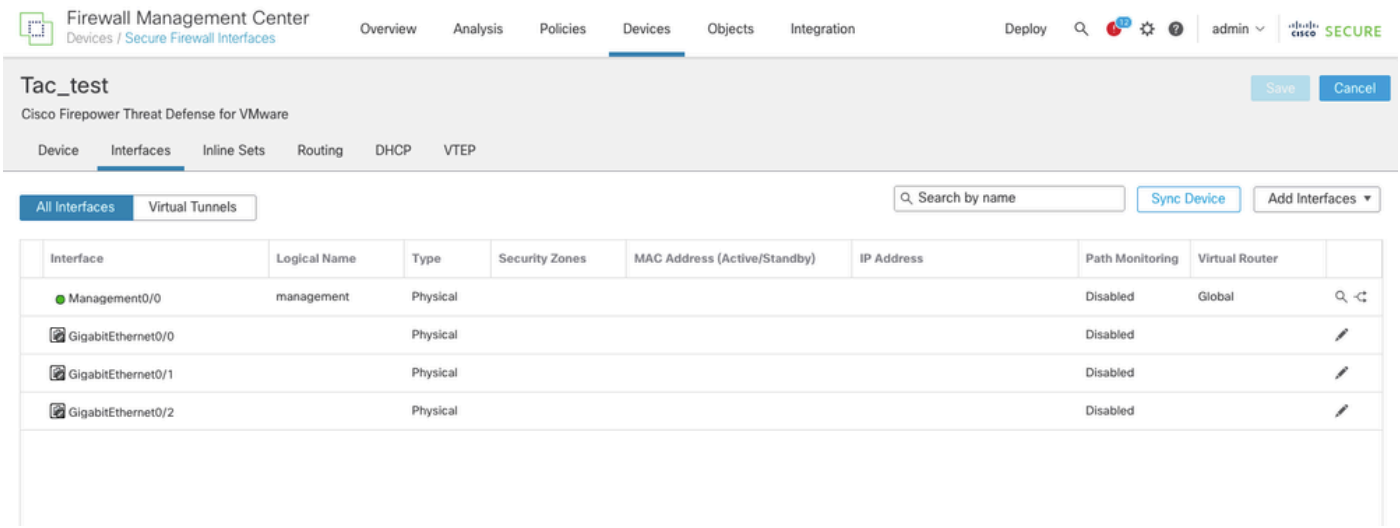
컨버전스 컨피그레이션 후

컨버전스 절차에서도 언급했듯이 병합을 수행하려면 진단 인터페이스의 모든 컨피그레이션을 제거해야 합니다.

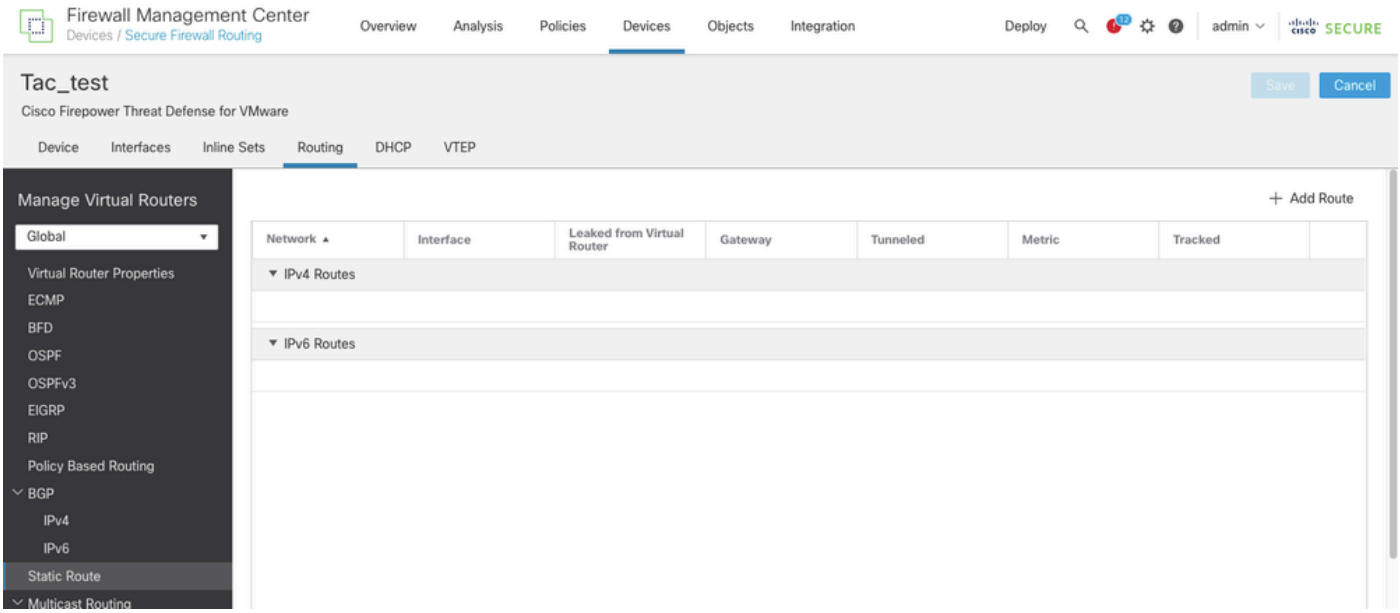
병합이 완료되면 FMC 및 FTD CLI에 대한 정보가 표시됩니다.

FMC UI를 통한 관리 인터페이스 컨피그레이션

Devices(디바이스) > Device Management(디바이스 관리)에서 FTD를 선택합니다. Interfaces(인터페이스) 탭으로 바로 열립니다.



병합 후의 관리 인터페이스

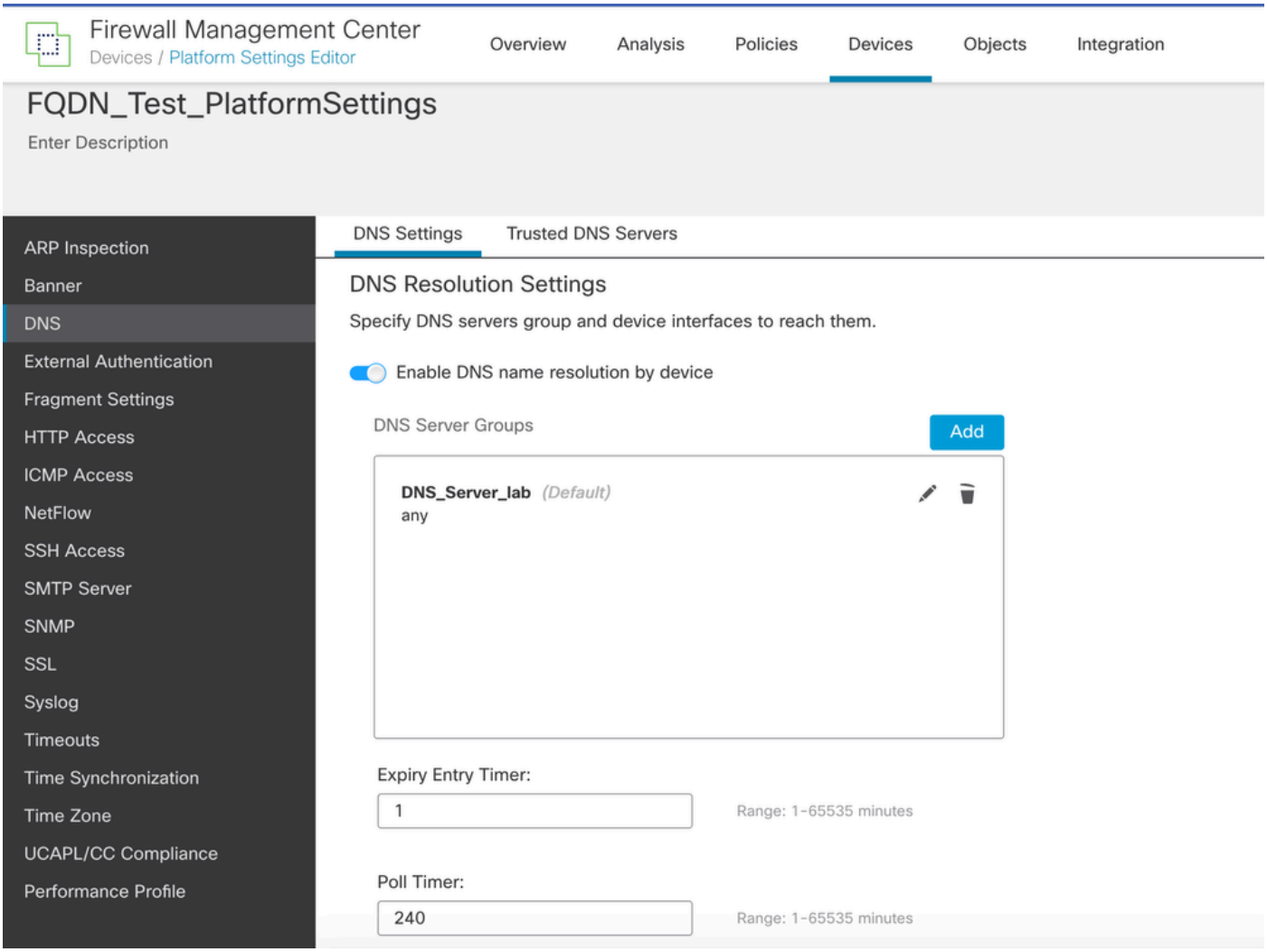


DNS 서버에 대한 고정 경로가 추가되지 않았습니다.

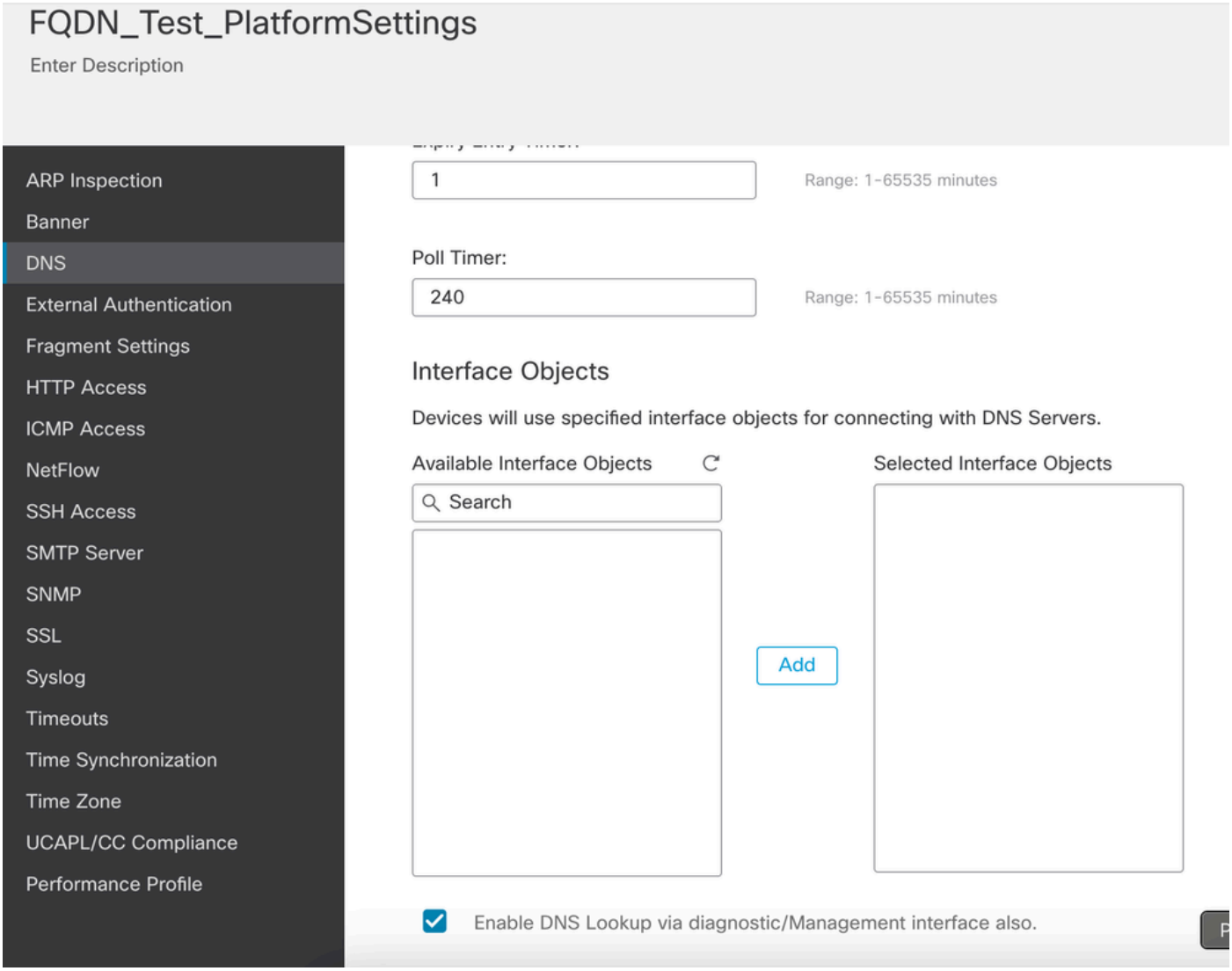
DNS 컨피그레이션은 플랫폼 설정에서 동일하게 유지해야 합니다.

Devices(디바이스) > Platform Settings(플랫폼 설정)에서 정책을 선택한 다음 DNS 탭을 선택합니다.

고정 경로를 추가할 필요 없이 DNS 조회가 관리 인터페이스로 계속 전송되려면 "진단/관리 인터페이스를 통한 DNS 조회 기능도 활성화하십시오." 은(는) 선택된 상태를 유지해야 합니다.



플랫폼 설정의 DNS 컨피그레이션



진단/관리 인터페이스를 통한 DNS 조회 활성화 옵션도 동일하게 유지해야 합니다

FTD CLI의 컨피그레이션

```
> show interface management
Interface Management0/0 "management", is up, line protocol is up
  Hardware is en_vtun rev00, DLY 10 usec
        Input flow control is unsupported, output flow control is unsupported
        MAC address 0050.56b3.f75d, MTU 1500
        IP address 203.0.113.130, subnet mask 255.255.255.248

> show interface ip brief
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0         unassigned      YES unset  administratively down up
GigabitEthernet0/1         unassigned      YES unset  administratively down up
GigabitEthernet0/2         unassigned      YES unset  administratively down up
Internal-Control0/0        127.0.1.1       YES unset  up                    up
Internal-Control0/1        unassigned      YES unset  up                    up
Internal-Data0/0           unassigned      YES unset  down                  up
Internal-Data0/0           unassigned      YES unset  up                    up
Internal-Data0/1           169.254.1.1     YES unset  up                    up
Internal-Data0/2           unassigned      YES unset  up                    up
Management0/0              203.0.113.130   YES unset  up                    up
```

```
ftd01# sh route management-only


Routing Table: mgmt-only
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
```

LINA 측의 FTD CLI에서 DNS 컨피그레이션

```
ftd01# sh run dns
dns domain-lookup management
DNS server-group DNS_Server_lab
    retries 5
    timeout 15
    name-server 10.10.10.10 management
    domain-name test.lab
DNS server-group DefaultDNS
dns-group DNS_Server_lab
```

Linux expert 모드에서 캡처하여 관리 인터페이스에서 DNS 조회 트래픽의 올바른 흐름을 확인합니다.

```
root@ftd01:/home/admin# tcpdump -i br1 port 53
HS_PACKET_BUFFER_SIZE is set to 4.
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on br1, link-type EN10MB (Ethernet), capture size 262144 bytes
20:20:33.623146 IP ftd01.60310 > 10.10.10.10.domain: 61954+ A? cisco.com. (27)
20:20:33.623533 IP ftd01.33417 > umbrella.domain: 20595+ PTR? 10.10.10.10.in-addr.arpa. (42)
20:20:48.660172 IP ftd01.60310 > 10.10.10.10.domain: 41252+ A? cisco.com. (27)
20:20:52.638426 IP ftd01.39304 > umbrella.domain: 20595+ PTR? 10.10.10.10.in-addr.arpa. (42)
20:21:09.669133 IP ftd01.47150 > umbrella.domain: 39343+ AAAA? ftd01. (23)
20:21:09.669305 IP ftd01.50173 > umbrella.domain: 57694+ AAAA? ftd01. (23)
20:21:11.659352 IP ftd01.48092 > umbrella.domain: 46478+ PTR? opendns.in-addr.arpa. (45)
20:21:14.673992 IP ftd01.58547 > umbrella.domain: 57694+ AAAA? ftd01. (23)
20:21:18.673371 IP ftd01.47607 > umbrella.domain: 39343+ AAAA? ftd01. (23)
20:21:18.695507 IP ftd01.60310 > 10.10.10.10.domain: 29973+ A? cisco.com. (27)
```

이러한 증거로 Linux를 통해 관리 인터페이스에 고정 경로가 추가되지 않은 경우에도 DNS 조회가 계속 작동함을 확인할 수 있습니다.

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.