# 가상 라우터

이 장에서는 Secure Firewall Threat Defense 내 가상 라우터 그리고 가상 라우터 동작 방법의 기본 개념을 설명합니다.



# 가상 라우터 및 VRF(가상 라우팅 및 포워딩) 정보

여러 가상 라우터를 생성하여 인터페이스 그룹에 대해 별도의 라우팅 테이블을 유지 관리할 수 있습니다. 각 가상 라우터에는 자체 라우팅 테이블이 있으므로 디바이스를 통과하는 트래픽에서 명확하게 분리하는 기능을 제공할 수 있습니다.

따라서 공통 네트워킹 장비 집합을 통해 둘 이상의 개별 고객을 지원할 수 있습니다. 또한 가상 라우터를 사용하여 자체 네트워크의 요소를 더 쉽게 분리할 수 있습니다. 일반 목적의 기업 네트워크에서 개발 네트워크를 격리하는 경우를 예로 들 수 있습니다.

가상 라우터에서는 가상 라우팅 및 포워딩의 "light" 버전, 즉 VRF-Lite를 구현합니다. 이는 BGP용 멀티프로토콜 확장(MBGP)을 지원하지 않습니다.

가상 라우터를 생성하는 경우 라우터에 인터페이스를 할당합니다. 특정 인터페이스는 하나의 가상 라우터에만 할당할 수 있습니다. 그런 다음 고정 경로를 정의하고 각 가상 라우터에 대해 OSPF 또는 BGP와 같은 라우팅 프로토콜을 구성합니다. 또한 모든 참여 디바이스의 라우팅 테이블이 동일한 가상 라우터 라우팅 프로세스 및 테이블을 사용하도록 전체 네트워크에 대해 별도의 라우팅 프로세스를 구성합니다. 가상 라우터를 사용하면 동일한 물리적 네트워크를 통해 논리적으로 구분된 네트워크를 생성하여 각 가상 라우터를 통해 실행되는 트래픽의 프라이버시를 확보할 수 있습니다.

라우팅 테이블은 분리되어 있으므로 가상 라우터 전체에서 동일하거나 중복되는 어드레스 스페이스를 사용할 수 있습니다. 예를 들어, 2개의 개별 물리적 인터페이스에서 지원되는 2개의 개별 가상 라우터에 대해 192.168.1.0/24 어드레스 스페이스를 사용할 수 있습니다.

가상 라우터별로 별도의 관리 및 데이터 라우팅 테이블이 있습니다. 예를 들어, 가상 라우터에 관리 전용 인터페이스를 할당하는 경우 해당 인터페이스에 대한 라우팅 테이블은 가상 라우터에 할당된 데이터 인터페이스와는 별개입니다.

# 가상 라우터의 애플리케이션

가상 라우터를 사용하여 공유 리소스에서 네트워크를 격리하거나 공통 보안 정책으로 네트워크를 격리할 수 있습니다. 따라서 가상 라우터를 사용하면 다음을 달성할 수 있습니다.

- 각 고객 또는 다른 부서의 전용 라우팅 테이블을 통해 고객을 위한 트래픽 분리
- 여러 부서 또는 네트워크에 대한 공통 보안 정책 관리
- 다른 부서 또는 네트워크에 대한 공유 인터넷 액세스

# 전역 및 사용자 정의 가상 라우터

### 전역 가상 라우터

가상 라우팅 기능이 있는 디바이스의 경우 시스템은 기본적으로 전역 가상 라우터를 생성합니다. 시스템은 네트워크의 모든 인터페이스를 글로벌 가상 라우터에 할당합니다. 라우팅 인터페이스는 사용자 정의 가상 라우터 또는 전역 가상 라우터에 속할 수 있습니다. threat defense를 가상 라우터 기능이 있는 버전으로 업그레이드할 경우 기존의 모든 라우팅 구성이 전역 가상 라우터의 일부가 됩니다.

### 사용자 정의 가상 라우터

사용자 정의 가상 라우터는 사용자가 정의한 가상 라우터입니다. 디바이스에서 둘 이상의 가상 라우터를 생성할 수 있습니다. 그러나 언제든 하나의 사용자 정의 가상 라우터에만 인터페이스를 할당할 수 있습니다. 일부 디바이스 기능은 사용자 정의 가상 라우터에서 지원되지만 일부 기능은 전역 가상 라우터에서만 지원됩니다. 사용자 정의 가상 라우터는 경로 기반 사이트 간 VPN(정적 VTI)을 지원합니다.

### 지원되는 기능 및 모니터링 정책

글로벌 가상 라우터에서만 다음 기능을 구성할 수 있습니다.

- OSPFv3
- RIP
- EIGRP
- IS-IS
- 멀티캐스트 라우팅

- Policy Based Routing (PBR)

ISIS 및 PBR은 management center의 Flex 구성을 통해 지원됩니다(사전 정의된 FlexConfig 개체 참조). 이러한 기능을 위해 전역 가상 라우터의 인터페이스만 구성합니다.

DHCP 서버 자동 구성에서는 인터페이스에서 학습된 WINS/DNS 서버를 사용합니다. 이 인터페이스는 전역 가상 라우터 인터페이스만 될 수 있습니다.

각 사용자 정의 가상 라우터에 대해 다음 기능을 개별적으로 구성할 수 있습니다.

- 고정 경로 및 해당 SLA 모니터
- OSPFv2
- BGPv4/v6
- 통합 라우팅 및 브리징(IRB)
- SNMP

다음 기능은 원격 시스템을 통해 쿼리하거나 통신할 때 시스템에서 사용됩니다(from-the-box 트래픽). 이러한 기능에서는 글로벌 가상 라우터의 인터페이스만 사용합니다. 즉, 이 기능을 위해 인터페이스를 구성하는 경우 해당 인터페이스는 글로벌 가상 라우터에 속해야 합니다. 일반적으로 시스템에서는 자체 관리 목적으로 외부 서버에 연결하기 위해 경로를 조회해야 할 때마다 글로벌 가상 라우터에서 경로 조회를 수행합니다.

- 액세스 제어 규칙 또는 **ping** 명령의 이름을 확인할 때 사용되는 정규화된 이름을 확인하는 데 사용되는 DNS 서버입니다. DNS 서버에 대한 인터페이스로 **any**를 지정하면 시스템에서는 글로벌 가상 라우터의 인터페이스만 고려합니다.
- VPN과 함께 사용하는 경우 ID 영역 또는 AAA 서버입니다. 글로벌 가상 라우터의 인터페이스에서만 VPN을 구성할 수 있습니다. VPN에 사용되는 외부 AAA 서버(예: Active Directory)는 글로벌 가상 라우터의 인터페이스를 통해 연결할 수 있어야 합니다.
- Syslog 서버.

# 가상 라우터 인식 정책 구성

가상 라우터를 생성하면 해당 가상 라우터에 대한 라우팅 테이블이 전역 가상 라우터 또는 다른 모든 가상 라우터와 자동으로 분리됩니다. 그러나 보안 정책에서는 자동으로 가상 라우터를 인식하지 않습니다.

예를 들어 "any" 소스 또는 대상 보안 영역에 적용되는 액세스 제어 규칙을 작성하는 경우, 규칙은 모든 가상 라우터의 모든 인터페이스에 적용됩니다. 이는 실제로 원하는 것과 정확히 같을 수 있습니다. 예를 들어 모든 고객이 유해한 URL 카테고리의 동일한 목록에 대한 액세스를 차단하고자 할 수 있습니다.

그러나 가상 라우터 중 하나에만 정책을 적용해야 하는 경우에는 해당 단일 가상 라우터의 인터페이스만 포함하는 보안 영역을 생성해야 합니다. 그런 다음, 보안 정책의 소스 및 대상 기준에서 가상 라우터 제한 보안 영역을 사용합니다.

해당 멤버십이 단일 가상 라우터에 할당된 인터페이스로 제한되는 보안 영역을 사용하여 다음 정책에서 가상 라우터 인식 규칙을 작성할 수 있습니다.

- 액세스 제어 정책
- 침입 및 파일 정책
- SSL 암호 해독 정책
- ID 정책 및 사용자-IP 주소 매핑 가상 라우터에서 중복 어드레스 스페이스를 사용하는 경우 각 가상 라우터에 대해 별도의 영역을 생성하고 ID 정책 규칙에서 올바르게 적용해야 합니다.

가상 라우터에서 중복 어드레스 스페이스를 사용하는 경우 보안 영역을 사용하여 적절한 정책이 적용되도록 해야 합니다. 예를 들어, 두 개의 개별 가상 라우터에서 192.168.1.0/24 어드레스 스페이스를 사용하는 경우, 두 가상 라우터의 트래픽에 192.168.1.0/24 네트워크가 적용되도록 지정하는 액세스 제어 규칙이 적용됩니다. 원하는 결과가 아닌 경우, 가상 라우터 중 하나에 대해서만 소스/대상 보안 영역을 지정하여 규칙의 적용을 제한할 수 있습니다.

# 인터커넥트 가상 라우터

정적 및 동적 경로 유출

가상 라우터 간의 트래픽을 라우팅하는 디바이스를 구성할 수 있습니다. 이 경로 유출 프로세스는 정적 경로를 설정하여 수동으로 수행하거나 BGP 설정을 통해 동적으로 수행할 수 있습니다.

정적 경로 유출

가상 라우터 간의 트래픽을 라우팅하는 정적 경로를 구성할 수 있습니다.

예를 들어 전역 가상 라우터에 외부 인터페이스가 있는 경우, 각각의 다른 가상 라우터에서 정적 기본 경로를 설정하여 외부 인터페이스로 트래픽을 전송할 수 있습니다. 그런 다음, 지정된 가상 라우터 내에서 라우팅할 수 없는 모든 트래픽은 후속 라우팅을 위해 전역 라우터로 전송됩니다.

다른 가상 라우터로의 트래픽을 유출하고 있으므로 가상 라우터 간의 정적 경로를 경로 유출이라고 합니다. VR1 경로에서 VR2로 경로를 유출하는 경우 VR2에서 VR1로만 연결을 시작할 수 있습니다. VR1에서 VR2로의 트래픽을 전송하려면 역방향 경로를 구성해야 합니다. 다른 가상 라우터의 인터페이스에 대한 정적 경로를 생성할 경우 게이트웨이 주소를 지정하지 않아도 됩니다. 대상 인터페이스만 선택하면 됩니다.

가상 라우터 간 경로의 경우, 시스템에서는 소스 가상 라우터에서 대상 인터페이스를 조회합니다. 그런 다음, 대상 가상 라우터에서 다음 홉의 MAC 주소를 조회합니다. 따라서 대상 가상 라우터에는 대상 주소에 대해 선택된 인터페이스의 동적(학습한) 또는 정적 경로가 있어야 합니다.

서로 다른 가상 라우터에서 소스 및 대상 인터페이스를 사용하는 NAT 규칙을 구성하면 가상 라우터 간의 트래픽이 라우팅될 수도 있습니다. NAT에 대해 경로 조회를 수행하는 옵션을 선택하지 않을 경우, 대상 변환이 발생할 때마다 규칙에 따라 NAT 적용 주소가 있는 대상 인터페이스로 트래픽이 전송됩니다. 그러나 대상 가상 라우터에는 변환된 대상 IP 주소에 대한 경로가 있어야 next-hop 조회가 성공할 수 있습니다.

NAT 규칙에서 한 가상 라우터에서 다른 가상 라우터로 트래픽을 유출하여 올바른 라우팅이 보장되는 경우, 변환된 트래픽에 대해 이러한 가상 라우터 간에 정적 경로 유출을 구성하는 것을 권장합니다. 경로 유출이 없는 경우, 일치할 것으로 예상되는 트래픽과 규칙이 일치하지 않을 수도 있으며 변환이 적용되지 않을 수 있습니다.

가상 라우팅은 경로 유출의 연속 또는 체인을 지원하지 않습니다. 예를 들어 threat defense에 VR1, VR2 및 VR3 가상 라우터가 있다고 가정합니다. VR3는 네트워크 - 10.1.1.0/24에 직접 연결됩니다. 이제 VR2 및 VR2에서 인터페이스를 통한 네트워크 10.1.1.0/24의 VR1에서의 경로 유출을 구성하고 VR3를 통한 10.1.1.0/24에 대한 경로 유출을 정의한다고 가정합니다. 이 경로 유출 체인은 VR1에서 VR2로의 홉에 대한 트래픽을 허용하지 않으며 VR3에서 나갈 수 없습니다. 경로 유출이 발생하는 경우, 경로 조회는 먼저 입력 가상 라우터의 라우팅 테이블에서 이그레스 인터페이스를 확인한 후, 다음 홉 조회에 대한 가상 라우터의 라우팅 테이블 출력을 확인합니다. 두 조회 모두에서 이그레스 인터페이스가 일치해야 합니다. 이 예에서는, 이그레스 인터페이스가 동일하지 않으므로 트래픽이 통과하지 않습니다.

대상 네트워크가 업스트림(발신) VR의 직접 연결된 서브넷이 아닌 경우에는 정적 VRF 간 경로를 주의하여 사용합니다. 예를 들어 VR1 및 VR2의 두 VR을 가정합니다. VR1은 BGP 또는 동적 라우팅 프로토콜을 통해 외부 피어에서 기본 경로를 가져오는 발신 트래픽을 처리하고, VR2는 VR1을 다음 홉으로 사용하는 정적 VRF 간 기본 경로로 구성된 수신 트래픽을 처리합니다. VR1이 피어에서 기본 경로를 잃으면 VR2는 업스트림(발신) VR이 기본 경로를 손실했음을 탐지할 수 없으며 트래픽은 여전히 VR1로 전송되며, 이는 알림 없이 삭제됩니다. 이 시나리오에서는 BGP를 통해 동적 경로 누수를 사용하여 VR2를 구성하는 것이 좋습니다.

### **BGP**를 사용한 동적 경로 유출

경로 대상 확장 커뮤니티를 사용하여 소스 가상 라우터(예: VR1)에서 소스 BGP 테이블로 경로를 내보낸 다음 동일한 경로 대상 확장 커뮤니티를 소스 BGP 테이블에서 대상 가상 라우터(예: VR2)에서 사용하는 대상 BGP 테이블로 가져와서 가상 라우터 간 경로 유출을 구현할 수 있습니다. 경로를 필터링하는 데 경로 맵을 사용할 수 있습니다. 전역 가상 라우터의 경로는 사용자 정의 가상 라우터로 유출될 수 있으며, 그 반대의 경우도 마찬가지입니다. BGP 가상 라우터 간 경로 유출은 ipv4 및 ipv6 접두사를 모두 지원합니다.

BGP 경로 유출 구성에 대한 자세한 내용은 BGP 라우트 가져오기/내보내기 설정 구성 항목을 참조하십시오.

### **BGP** 경로 유출 지침

- 재귀에 필요한 모든 경로를 가져와서 인그레스 가상 라우터의 라우팅 테이블에 표시해야 합니다.
- ECMP는 가상 라우터별로 지원됩니다. 따라서 여러 가상 라우터에서 ECMP를 구성하지 마십시오. 서로 다른 가상 라우터에서 가져온 중복 접두사는 ECMP를 형성할 수 없습니다. 즉, 서로 다른 두 개의 가상 라우터에서 다른 가상 라우터(전역 가상 라우터 또는 사용자 정의 가상 라우터)로 주소가 중복되는 경로를 가져오려고 할 때 하나의 경로(BGP 최적 경로 알고리즘에 따라 전파되었던 첫 번째 경로)만 해당 가상 라우팅 테이블로 가져옵니다. 예를 들어, VR1에 연결된 네트워크 10.10.0.0/24가 BGP를 통해 전역 가상 라우터에 먼저 전파되고 나중에 동일한 주소 10.10.0.0/24의 다른 네트워크가 BGP를 통해 전역 가상 라우터에 전파되는 경우, 전역 가상 라우터로만 VR1 네트워크 경로를 가져옵니다.

- OSPFv3은 사용자 정의 가상 라우터에서 지원되지 않습니다. 따라서 OSPFv3 사용자 정의 가상 라우터를 전역 가상 라우터로 유출하도록 BGPv6을 구성하지 마십시오. 하지만 재배포를 통해 OSPFv3 전역 가상 라우터 경로를 사용자 정의 가상 라우터로 유출하도록 BGPv6을 구성할 수 있습니다.
- 경로 누수를 방지하기 위해 VTI 인터페이스, 보호된 내부 인터페이스(VTI에 대해 지원되는 경우 루프백 인터페이스)를 동일한 가상 라우터의 일부로 유지하는 것이 좋습니다.

# 중복된 IP 주소

가상 라우터는 독립적인 라우팅 테이블의 여러 인스턴스를 생성하므로 동일하거나 중복되는 IP 주소를 충돌 없이 사용할 수 있습니다. Threat Defense를 사용하면 동일한 네트워크를 둘 이상의 가상 라우터에 포함할 수 있습니다. 여기에는 인터페이스 또는 가상 라우터 레벨에서 적용할 여러 정책이 포함됩니다.

몇 가지 예외를 제외하면 라우팅 기능과 대부분의 NGFW 및 IPS 기능은 중복되는 IP 주소의 영향을 받지 않습니다. 다음 섹션에서는 IP 주소 중복과 관련된 제한 사항 및 이를 해결하기 위한 제안 또는 권장 사항에 대해 설명합니다.

### 중복 IP 주소의 제한 사항

여러 가상 라우터에서 중복 IP 주소를 사용하는 경우 정책을 적절하게 적용하려면 일부 기능에 대해 정책 또는 규칙을 수정해야 합니다. 이러한 기능을 사용하려면 기존 보안 영역을 분할하거나 필요에 따라 새 인터페이스 그룹을 사용하여 더 구체적인 인터페이스를 사용해야 합니다.

다음 기능은 IP 주소가 겹치는 올바른 기능을 위해 수정이 필요합니다.

- 네트워크 맵 - 일부 중복 IP 세그먼트를 제외하도록 네트워크 검색 정책을 수정하여 매핑되는 중복 IP 주소가 없는지 확인합니다.
- ID 정책 - ID 피드 소스는 가상 라우터를 구분할 수 없습니다. 이 제한 사항을 극복하기 위해 중복 주소 공간 또는 가상 라우터를 서로 다른 영역에 매핑합니다.

다음 기능의 경우, 중복 IP 세그먼트에 서로 다른 정책이 적용되도록 특정 인터페이스에 규칙을 적용해야 합니다.

- 액세스 정책
- 사전 필터 정책
- QoS/속도 제한
- SSL 정책

### 중복 IP 주소로 지원되지 않는 기능

- AC 정책의 ISE SGT 기반 규칙 - Cisco ISE(Identity Services Engine)에서 다운로드한 IP 주소 매핑에 대한 고정 SGT(보안 그룹 태그)에서 가상 라우터를 인식하지 않습니다. 가상 라우터마다 서로 다른 SGT 매핑을 생성해야 하는 경우 가상 라우터마다 별도의 ISE 시스템을 설정합니다. 각

가상 라우터에서 동일한 SGT 번호에 동일한 IP 주소를 매핑하려는 경우에는 이 작업이 필요하지 않습니다.

- 가상 라우터에서는 중복 DHCP 서버 풀이 지원되지 않습니다.
- 이벤트 및 분석 - 대부분의 management center 분석은 네트워크 맵 및 ID 매핑에 따라 달라지며, 동일한 IP 주소가 두 개의 서로 다른 엔드 호스트에 속하는 경우 이를 구분할 수 없습니다. 따라서 이러한 분석은 동일한 디바이스에 있지만 서로 다른 가상 라우터에 중복 IP 세그먼트가 있는 경우에는 정확하지 않습니다.

# 사용자 정의 가상 라우터에서 SNMP 구성

이제 관리 인터페이스 및 전역 가상 라우터 데이터 인터페이스에서 SNMP를 지원할 수있을뿐 아니라 Secure Firewall Threat Defense에서 사용자 정의 가상 라우터에서 SNMP 호스트를 구성할 수 있습니다.

사용자 정의 가상 라우터에서 SNMP 호스트를 구성하는 과정은 다음과 같습니다.

1. 디바이스 인터페이스를 구성합니다.
2. 가상 라우터 생성
3. 가상 라우터 인터페이스에서 SNMP 호스트를 구성합니다.

참고 SNMP는 가상 라우터를 인식하지 않습니다. 따라서 사용자 정의 가상 라우터에서 SNMP 서버를 구성하는 동안 네트워크 주소가 중복된 IP 주소가 아닌지 확인하십시오.

4. 구성을 Secure Firewall Threat Defense에 구축합니다. 성공적인 구축에서는 SNMP 라우터 및 SNMP 트랩이 가상 라우터 인터페이스를 통해 네트워크 관리 스테이션으로 전송됩니다.

# 디바이스 모델별 최대 가상 라우터 수

생성할 수 있는 최대 가상 라우터 수는 디바이스 모델에 따라 다릅니다. 다음 표에는 최대 한도가 나와 있습니다. 글로벌 가상 라우터를 포함하지 않는 해당 플랫폼에 대해 최대 사용자 정의 가상 라우터 수를 표시하는 **show vrf counters** 명령을 입력하여 시스템을 두 번 확인할 수 있습니다. 아래 표의 숫자에는 사용자 및 글로벌 라우터가 포함되어 있습니다. Firepower 4100/9300의 경우 이러한 숫자는 네이티브 모드에 적용됩니다.

Firepower 4100/9300 등의 다중 인스턴스 기능을 지원하는 플랫폼의 경우 최대 가상 라우터를 디바이스의 코어 수만큼 분할한 다음 가장 근접한 정수로 내림하여 인스턴스에 할당된 코어 수를 곱하여 컨테이너 인스턴스 당 최대 가상 라우터 수를 결정합니다. 예를 들어 플랫폼에서 최대 100개의 가상 라우터를 지원하고 70 코어를 보유한 경우, 각 코어는 최대 1.43개의 가상 라우터(내림됨)를 지원합니다. 따라서 6개의 코어에 할당된 인스턴스는 8.58 가상 라우터를 지원하며, 이 라우터는 8개로 내림되며, 10개의 코어가 할당된 인스턴스는 14.3 가상 라우터(내림함, 14)를 지원합니다.

| 디바이스 모델 | 최대 가상 라우터 수 |
|---|---|
| Firepower 1010 | 5 |
| Firepower 1120 | 5 |
| Firepower 1140 | 10 |
| Firepower 1150 | 10 |
| Firepower 2110 | 10 |
| Firepower 2120 | 20 |
| Firepower 2130 | 30 |
| Firepower 2140 | 40 |
| Secure Firewall 3105 | 10 |
| Secure Firewall 3110 | 15 |
| Secure Firewall 3120 | 25 |
| Secure Firewall 3130 | 50 |
| Secure Firewall 3140 | 100 |
| Firepower 4112 | 60 |
| Firepower 4115 | 80 |
| Firepower 4125 | 100 |
| Firepower 4145 | 100 |
| Firepower 9300 Appliance, 모든 모델 | 100 |
| Threat Defense Virtual, 모든 플랫폼 | 30 |
| ISA 3000 | 10 |

관련 항목

컨테이너 인스턴스의 요구 사항 및 사전 요구 사항

# 가상 라우터를 위한 요구 사항 및 사전 요건

모델 지원

Threat Defense

지원되는 도메인

모든

사용자 역할

관리자

네트워크 관리자

보안 승인자

# 가상 라우터 대한 지침 및 제한 사항

방화벽 모드 지침

가상 라우터는 라우팅 방화벽 모드에서만 지원됩니다.

인터페이스 지침

- 인터페이스를 하나의 가상 라우터에만 할당할 수 있습니다.
- 가상 라우터에 할당되는 인터페이스 수에는 제한이 없습니다.
- 논리적 이름 과 VTI를 가진 라우팅된 인터페이스만 사용자 정의 가상 라우터에 할당할 수 있습니다.
- 가상 라우터 인터페이스를 비 라우팅 모드로 변경하려면 가상 라우터에서 인터페이스를 제거한 다음 해당 모드를 변경합니다.
- 전역 가상 라우터 또는 다른 사용자 정의 가상 라우터에서 가상 라우터에 인터페이스를 할당할 수 있습니다.
- 다음 인터페이스는 사용자 정의 가상 라우터에 할당할 수 없습니다.
  - 진단 인터페이스.
  - EtherChannel의 멤버.
  - 이중 인터페이스의 멤버.
  - BVI의 멤버.
- VTI는 경로 기반 VPN입니다. 따라서 터널이 설정되면 암호화에 VTI를 사용하는 트래픽이 라우팅을 통해 제어되어야 합니다. 고정 라우팅 및 BGP, OSPFv2/v3 또는 EIGRP를 사용하는 동적 라우팅이 지원됩니다.
- 정책 기반 사이트 간 또는 원격 액세스 VPN에서는 사용자 정의 가상 라우터에 속하는 인터페이스를 사용할 수 없습니다.

- 이동 중인 인터페이스 또는 가상 라우터를 삭제하는 경로가 소스 또는 대상 가상 라우터 테이블에 있는 경우, 인터페이스 이동 또는 가상 라우터 삭제 전에 경로를 제거합니다.
- 각 가상 라우터에 대해 별도의 라우팅 테이블이 유지되므로, 인터페이스가 하나의 가상 라우터에서 다른 가상 라우터로 이동하면(전역 또는 사용자 정의) 시스템은 인터페이스에 설정된 IP 주소를 일시적으로 제거합니다. 인터페이스의 모든 기존 연결이 종료됩니다. 그러므로 가상 라우터 간에 인터페이스를 이동하면 네트워크 트래픽에 막대한 영향을 미치게 됩니다. 따라서 인터페이스를 이동하기 전에 예방 조치를 취해야 합니다.

전역 가상 라우터 지침

- 이름이 지정되고 다른 가상 라우터의 일부가 아닌 인터페이스는 전역 가상 라우터의 일부입니다.
- 전역 가상 라우터에서 라우팅 인터페이스를 제거할 수 없습니다.
- 전역 가상 라우터는 수정할 수 없습니다.
- 일반적으로 인터페이스를 설정한 후 등록을 취소하고 동일하거나 다른 management center에 다시 등록하면 디바이스에서 인터페이스 설정을 다시 가져옵니다. 가상 라우터를 지원할 경우, 제한 사항이 있습니다. 전역 가상 라우터 인터페이스의 IP 주소만 유지됩니다.

클러스터링 지침

- 인터페이스 장애로 인해 제어 유닛 링크에 장애가 발생하는 경우, 유닛은 전역 라우팅 테이블에서 인터페이스의 모든 유출 경로를 제거하고 클러스터의 다른 유닛에 비활성 연결 및 고정 경로를 전파합니다. 그러면 다른 유닛의 라우팅 테이블에서 이러한 누수 경로가 제거됩니다. 이러한 제거는 다른 유닛이 새 제어 유닛이 되기 전에 수행되며, 여기에는 약 500밀리초가 소요됩니다. 다른 유닛이 새 제어 유닛이 되면 이러한 경로를 학습하고 BGP 수렴을 통해 라우팅 테이블에 다시 추가합니다. 따라서 수렴 시간(약 1분)까지 라우팅 이벤트가 발생하는 데 누수 경로를 사용할 수 없습니다.
- 클러스터에서 제어 역할 변경이 발생하면 BGP를 통해 확인된 누수 경로가 최적의 ECMP 경로로 업데이트됩니다. 그러나 최적이 아닌 ECMP 경로는 BGP 재통합 타이머가 210초 경과한 후에만 클러스터 라우팅 테이블에서 제거됩니다. 따라서 BGP 재통합 타이머가 경과할 때까지 이전의 가장 적합하지 않은 ECMP 경로는 라우팅 이벤트에 대한 기본 경로로 유지됩니다.

추가 지침

- 가상 라우터에 대한 BGP를 구성하는 동안 동일한 가상 라우터 내에서 서로 다른 프로토콜에 속하는 경로를 재배포할 수 있습니다. 예를 들어 OSPF VR2 경로는 BGP VR1로 가져올 수 없습니다. OSPF VR2를 BGP VR2로만 재배포한 다음 BGP VR2와 BGP VR1 간에 경로 누수를 구성할 수 있습니다.
- IPv6 ACL을 사용하여 루트 맵의 경로를 필터링할 수 없습니다. 접두사 목록만 지원됩니다.

- 보안 인텔리전스 정책 - 보안 인텔리전스 정책에서는 가상 라우터를 인식하지 않습니다. IP 주소, URL 또는 DNS 이름을 차단 목록에 추가하면 해당 항목이 모든 가상 라우터에 대해 차단됩니다. 이 제한 사항은 보안 영역이 있는 인터페이스에 적용됩니다.
- NAT 규칙 - NAT 규칙에서 인터페이스를 혼합하지 마십시오. 가상 라우팅에서 지정된 소스 및 대상 인터페이스 개체(인터페이스 그룹 또는 보안 영역)에 서로 다른 가상 라우터에 속하는 인터페이스가 있는 경우, NAT 규칙에서는 다른 가상 라우터를 통해 하나의 가상 라우터에서 트래픽을 전환합니다. NAT는 인바운드 인터페이스에 대해서만 가상 라우터 테이블에서 경로 조회를 수행합니다. 필요한 경우 소스 가상 라우터에서 대상 인터페이스에 대한 고정 경로를 정의합니다. 인터페이스를 **any**로 둘 경우, 가상 라우터 멤버십에 관계없이 규칙이 모든 인터페이스에 적용됩니다.
- DHCP 릴레이 - DHCP 릴레이에 대한 가상 라우터 상호 연결은 지원되지 않습니다. 예를 들어, DHCP 릴레이 클라이언트가 VR1 인터페이스에서 활성화되고 DHCP 릴레이 서버가 VR2 인터페이스에서 활성화된 경우 DHCP 요청은 VR2 인터페이스 외부로 전달되지 않습니다.
- 삭제된 가상 라우터 재생성 -10초 이내에 삭제된 가상 라우터를 재생성하면 가상 라우터 삭제가 진행 중이라는 오류 메시지가 나타납니다. 삭제된 가상 라우터를 연속으로 재생성하려면 새 가상 라우터에 다른 이름을 사용합니다.

# Management Center 웹 인터페이스 - 라우팅 페이지에 대한 수정 사항

threat defense 6.6 이전 디바이스 및 소수의 디바이스 모델은 가상 라우팅 기능을 지원하지 않습니다. management center 웹 인터페이스는 이러한 비 지원 디바이스에 대해 management center 6.5 또는 이전 버전과 동일한 라우팅 페이지를 표시합니다. 가상 라우팅이 지원되는 디바이스 및 플랫폼을 확인하려면 디바이스 모델별 최대 가상 라우터 수을 참조하십시오.

지원되는 디바이스의 라우팅 페이지에서 가상 라우터를 구성할 수 있습니다.

1. **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**로 이동하여 가상 라우터 인식 디바이스를 편집합니다.
2. **Routing(**라우팅**)**을 클릭하여 가상 라우터 페이지에 입장합니다.

가상 라우팅을 사용하는 디바이스의 경우 Routing(라우팅) 페이지의 왼쪽 창에는 다음이 표시됩니다.

- **Manage Virtual Routers(**가상 라우터 관리**)**-가상 라우터를 생성하고 관리할 수 있습니다.
- List of virtual routing protocols(가상 라우팅 프로토콜 목록)-가상 라우터에 대해 구성할 수있는 라우팅 프로토콜을 나열합니다.
- **Settings(**설정**)** - 모든 가상 라우터에 적용 가능한 BGP 일반 설정을 구성할 수 있습니다. 다른 BGP 설정을 정의하려면 **Enable BGP(BGP** 활성화**)** 확인란을 선택합니다. 가상 라우터에 대한 다른 BGP 설정을 구성하려면 가상 라우팅 프로토콜에서 **BGP**로 이동합니다.

# 가상 라우터 관리

Virtual Routers(가상 라우터) 창에서 **Manage Virtual Routers(**가상 라우터 관리**)**를 클릭하면 Manage Virtual Routers(가상 라우터 관리) 페이지가 나타납니다. 이 페이지에는 디바이스 및 연결된 인터페이스의 기존 가상 라우터가 표시됩니다. 이 페이지에서 디바이스에 **Add Virtual Router(**가상 라우터 추가**)**( )할 수 있습니다. 사용자 정의 가상 라우터를 **Edit(**수정**)** ( )하거나 **Delete(**삭제**)** ( )할 수도 있습니다. 전역 가상 라우터는 편집하거나 제거할 수 없습니다. 전역 가상 라우터의 세부 사항만 **View(**보기**)** ( ) 수 있습니다.

# 가상 라우터 생성

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 threat defense 디바이스를 편집합니다.

단계 **2** **Routing(**라우팅**)**을 클릭합니다.

단계 **3** **Manage Virtual Routers(**가상 라우터 관리**)**를 클릭합니다.

단계 **4** **Add Virtual Router(**가상 라우터 추가**)**( ) 버튼을 클릭합니다.

단계 **5** Add Virtual Router(가상 라우터 추가) 상자에 가상 라우터의 이름과 설명을 입력합니다.

참고 10초 이내에 삭제된 가상 라우터를 생성하는 경우 가상 라우터 삭제가 진행 중이라는 오류 메시지가 표시됩니다. 삭제된 가상 라우터를 연속으로 생성하려면 새 가상 라우터에 다른 이름을 사용합니다.

단계 **6** **Ok(**확인**)**를 클릭합니다.

Routing(라우팅) 페이지가 나타나고 새로 생성된 가상 라우터 페이지가 표시됩니다.

다음에 수행할 작업

- 가상 라우터 구성.

# 가상 라우터 구성

| 스마트 라이선스 | 기본 라이선스 | 지원되는 장치 | 지원되는 도메인 | 액세스 |
|---|---|---|---|---|
| 모두 | 해당 없음 | Threat defense 및 Threat Defense Virtual | 모두 | 관리자/네트워크 관리자/보안 승인자 |

사용자 정의 가상 라우터에 인터페이스를 할당하고 디바이스에 대한 라우팅 정책을 설정할 수 있습니다. 글로벌 가상 라우터의 인터페이스를 수동으로 추가하거나 제거할 수는 없지만, 디바이스 인터페이스에 대한 라우팅 정책을 설정할 수 있습니다.

시작하기 전에

- 사용자 정의 가상 라우터에 대한 라우팅 정책을 구성하려면 라우터를 추가합니다. 가상 라우터 생성, 12 페이지의 내용을 참조하십시오.
- 비가상 라우팅 가능 디바이스의 모든 라우팅 구성 설정은 전역 가상 라우터에도 사용할 수 있습니다. 설정에 대한 자세한 내용은 라우팅 설정을 참조하십시오.
- 사용자 정의 가상 라우터에는 제한된 라우팅 프로토콜만 지원됩니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** 페이지에서 가상 라우터 지원 디바이스를 편집합니다. **Routing(**라우팅**)**으로 이동합니다. 라우팅 페이지 수정에 대해서는 Management Center 웹 인터페이스 - 라우팅 페이지에 대한 수정 사항, 11 페이지의 내용을 참조하십시오.

단계 **2** 드롭다운 목록에서 원하는 가상 라우터를 선택합니다.

단계 **3** **Virtual Router Properties(**가상 라우터 속성**)** 페이지에서 설명을 수정할 수 있습니다.

단계 **4** 인터페이스를 추가하려면 **Available Interface(**사용 가능한 인터페이스**)** 상자에서 인터페이스를 선택하고 **Add(**추가**)**를 클릭합니다.

다음 사항에 유의하십시오.

- **Available Interface(**사용 가능한 인터페이스**)** 상자 아래에는 논리적 이름이 있는 인터페이스만 나열됩니다. **Interface(**인터페이스**)**에서 논리적 이름을 제공하고 인터페이스를 편집할 수 있습니다. 설정이 적용되려면 변경 사항을 저장해야 합니다.
- 전역 가상 라우터의 인터페이스만 할당이 가능합니다. 즉, **Available Interfaces(**사용 가능한 인터페이스**)** 상자에는 다른 사용자 정의 가상 라우터에 할당되지 않은 인터페이스만 나열됩니다. 물리적 인터페이스, 하위 인터페이스, 이중 인터페이스, 브리지 그룹, VTI, EtherChannel은 가상 라우터에 할당할 수 있지만 그 멤버 인터페이스에는 할당할 수 없습니다. 멤버 인터페이스는 이름을 지정할 수 없으므로 가상 라우팅에서 사용할 수 없습니다.

  진단 인터페이스는 전역 가상 라우터에만 할당할 수 있습니다.

단계 **5** 설정을 저장하려면 **Save(**저장**)**를 클릭합니다.

단계 **6** 가상 라우터에 대한 라우팅 정책을 설정하려면 각 이름을 클릭하여 해당하는 설정 페이지를 엽니다.

- **OSPF** - 사용자 정의 가상 라우터에서는 OSPFv2만 지원됩니다. OSPFv2에 대한 다른 모든 설정은 비 가상 라우터 인식 인터페이스에 적용됩니다. 단, **Interface(**인터페이스**)**에서는 설정한 가상 라우터의 인터페이스만 선택할 수 있습니다. 전역 가상 라우터에 대해 OSPFv3 및 OSPFv2 라우팅 정책을 정의할 수 있습니다. OSPF 설정에 대한 자세한 내용은 OSPF의 내용을 참조하십시오.

- **RIP** - 전역 가상 라우터에 대해서만 RIP 라우팅 정책을 설정할 수 있습니다. RIP 설정에 대한 자세한 내용은 RIP의 내용을 참조하십시오.
- **BGP** - 이 페이지는 **Settings(**설정**)**에서 구성한 BGP 일반 설정을 표시합니다.
  - 이 페이지에서는 라우터 ID 설정을 제외한 일반 설정을 수정할 수 없습니다. 이 페이지에서 **Settings(**설정**)** 페이지에 정의된 라우터 ID 설정을 수정하여 재정의할 수 있습니다.
  - 다른 BGP IPv4 또는 IPv6 설정을 구성하려면 **BGP** 페이지의 **General Settings(**일반 설정**)**에서 BGP 옵션을 활성화해야 합니다.
  - IPv4 및 IPv6 주소군 모두에 대한 BGP 구성이 전역 라우터 및 사용자 정의 가상 라우터에 대해 지원됩니다.

  BGP 설정 구성에 대한 자세한 내용은 BGP의 내용을 참조하십시오.
- 정적 경로 - 이 설정을 사용하여 특정 대상 네트워크에 대해 트래픽을 보낼 위치를 정의합니다. 이 설정을 통해 가상 라우터 간 정적 경로를 생성할 수도 있습니다. 사용자 정의 또는 글로벌 가상 라우터의 인터페이스를 사용하여 연결된 경로 또는 정적 경로 유출을 생성할 수 있습니다. **FMC**는 인터페이스가 다른 가상 라우터에 속해 있음을 나타내기 위해 인터페이스에 접두사를 지정하여 경로 유출에 사용할 수 있습니다. 경로 유출이 성공하려면 다음 홉 게이트웨이를 지정하지 마십시오.

  정적 경로 테이블은 **Leaked from Virtual Router(**가상 라우터에서 유출된 경로**)** 열에서 경로 유출에 사용되는 인터페이스가 있는 가상 라우터를 표시합니다. 경로 유출이 아닌 경우, 열이 N/A(해당 없음)로 표시됩니다.

  정적 경로가 속한 가상 라우터에 관계없이 Null0 인터페이스는 정적 경로가 속한 동일한 가상 라우터의 인터페이스와 함께 나열됩니다.

  정적 경로 설정에 대한 자세한 내용은 고정 경로 및 기본 경로의 내용을 참조하십시오.
- 멀티캐스트 - 전역 가상 라우터에 대해서만 멀티캐스트 라우팅 정책을 설정할 수 있습니다. 멀티캐스트 설정에 대한 자세한 내용은 멀티캐스트의 내용을 참조하십시오.

단계 **7** 설정을 저장하려면 **Save(**저장**)**를 클릭합니다.

---

다음에 수행할 작업

- 가상 라우터 수정
- 가상 라우터 제거

# 가상 라우터 수정

가상 라우터의 설명 및 기타 라우팅 정책을 수정할 수 있습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 threat defense 디바이스를 편집합니다.

단계 **2** **Routing(**라우팅**)**을 클릭합니다.

단계 **3** **Manage Virtual Routers(**가상 라우터 관리**)**를 클릭합니다.

가상 라우터 페이지에 할당된 인터페이스와 함께 모든 가상 라우터가 표시됩니다.

단계 **4** 가상 라우터를 수정하려면 원하는 가상 라우터에 해당하는 **Edit(**수정**)** ( )을 클릭합니다.

참고 글로벌 가상 라우터의 일반 설정은 수정할 수 없습니다. 따라서 글로벌 라우터에서는 편집을 사용할 수 없습니다. 대신 설정을 볼 수 있는 **View(**보기**)** ( )이 제공됩니다.

단계 **5** 변경 사항을 저장하려면 **Save(**저장**)**을 클릭합니다.

다음에 수행할 작업

- 가상 라우터 제거

# 가상 라우터 제거

시작하기 전에

- 글로벌 가상 라우터는 삭제할 수 없습니다. 따라서 글로벌 가상 라우터에서는 삭제 옵션을 사용할 수 없습니다.
- 한 번에 여러 가상 라우터를 제거할 수 있습니다.
- 삭제된 가상 라우터의 모든 라우팅 정책도 삭제됩니다.
- 삭제된 가상 라우터의 모든 인터페이스는 글로벌 가상 라우터로 이동합니다.
- IP 이동, 경로 충돌 등 인터페이스 이동에 제한이 있는 경우, 충돌을 해결한 후에만 라우터를 제거할 수 있습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 threat defense 디바이스를 편집합니다.

단계 **2** **Routing(**라우팅**)**을 클릭합니다.

단계 **3** **Manage Virtual Routers(**가상 라우터 관리**)**를 클릭합니다.

매핑된 인터페이스와 함께 모든 가상 라우터가 가상 라우터 페이지에 표시됩니다.

단계 **4** 가상 라우터를 제거하려면 원하는 가상 라우터에 해당하는 **Delete(**삭제**)** ( )을 클릭합니다.

단계 **5** 여러 라우터를 제거하려면 CTRL 키를 누른 상태에서 삭제할 가상 라우터를 클릭합니다. 마우스 오른쪽 버튼을 클릭하고 **Delete(**삭제**)**를 클릭합니다.

단계 **6** 변경 사항을 저장하려면 **Save(**저장**)**을 클릭합니다.

# 가상 라우터 모니터링

가상 라우터를 모니터링하고 문제해결을 수행하려면 디바이스 CLI에 로그인하여 다음 명령을 사용합니다.

- **show vrf**: 가상 라우터 및 관련 인터페이스의 세부 정보를 표시합니다.
- **show route vrf** <*vrf_name*>: 가상 라우터의 라우팅 세부 정보를 표시합니다.
- **show run router bgp all**: 모든 가상 라우터의 BGP 라우팅 세부 정보를 표시합니다.
- **show run router bgp vrf** <*vrf_name*>: 가상 라우터의 BGP 라우팅 세부 정보를 표시합니다.

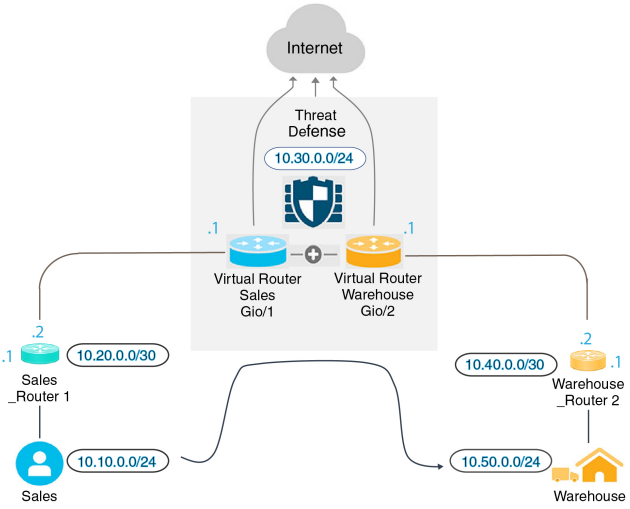
# 가상 라우터의 구성 예시

## 가상 라우터를 통해 원거리 서버로 라우팅하는 방법

가상 라우팅에서 여러 가상 라우터를 생성하여 인터페이스 그룹에 대해 별도의 라우팅 테이블을 유지 관리할 수 있으므로 네트워크 분리를 달성할 수 있습니다. 일부 시나리오에서는 별도의 가상 라우터를 통해서만 연결할 수 있는 서버에 액세스해야 할 수 있습니다. 이 예에서는 여러 홉이 있는 호스트에 연결하기 위해 가상 라우터를 상호 연결하는 절차를 제공합니다.

의류 회사 영업 부서 직원이 공장 유닛의 창고 관리 부서에서 보관 중인 재고를 조회하려는 경우를 예로 들어 보겠습니다. 가상 라우팅 환경에서는 영업 부서에서 대상(창고 관리 부서)까지 가상 라우터 간에 멀티 홉의 경로 유출을 사용해야 합니다. 이 경로 유출은 멀티 홉 경로 유출을 추가하여 수행됩니다. 이 경우 영업 가상 라우터(소스)에 있는 정적 경로에서 창고 가상 라우터의 인터페이스(대상)까지의 정적 경로를 구성합니다. 대상 네트워크가 떨어져 있으므로(멀티 홉), 창고 가상 라우터를 또한 대상 네트워크(일명 10.50.0.0/24)까지의 경로를 통해 구성해야 합니다.

그림 *1: 2*개의 가상 라우터 인터커넥트 - 예




시작하기 전에

이 예에서는 10.20.0.1/30 인터페이스에서 10.50.0.5/24로의 트래픽을 라우팅하기 위해 이미 Sales_Router1를 구성한 것으로 가정합니다.

프로시저

단계 **1** 영업 가상 라우터에 할당할 디바이스의 내부 인터페이스(Gi0/1)를 구성합니다.

a) **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Interfaces(**인터페이스**)**를 선택합니다.

b) Gi0/1 인터페이스를 수정합니다:

- 이름 - 이 예의 경우 VR-Sales입니다.
- 활성화 확인란을 선택합니다.
- **IPV4**에서 **IP** 유형의 경우 **Use Static IP(**정적 **IP** 사용**)**를 선택합니다.
- **IP** 주소 - 10.30.0.1/24를 입력합니다.

c) **Ok(**확인**)**를 클릭합니다.

d) **Save(**저장**)**를 클릭합니다.

단계 **2** 창고 가상 라우터에 할당할 디바이스의 내부 인터페이스(Gi0/2)를 구성합니다:

a) **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Interfaces(**인터페이스**)**를 선택합니다.

b) Gi0/2 인터페이스를 수정합니다:

- 이름 - 이 예의 경우 VR-Warehouse입니다.
- 활성화 확인란을 선택합니다.

- **IPV4**에서 **IP** 유형의 경우 **Use Static IP(**정적 **IP** 사용**)**를 선택합니다.
- **IP** 주소 - 공백으로 둡니다. 아직 사용자 정의 가상 라우터를 생성하지 않았으므로 동일한 IP 주소(10.30.0.1/24)의 인터페이스를 구성할 수 없습니다.

c) **Ok(**확인**)**를 클릭합니다.
d) **Save(**저장**)**를 클릭합니다.

단계 **3** 영업 및 창고 가상 라우터를 생성하고 해당 인터페이스를 할당합니다:

a) **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 threat defense 디바이스를 편집합니다.
b) **Routing(**라우팅**)** > **Manage Virtual Routers(**가상 라우터 관리**)**를 선택합니다.
c) **Add Virtual Router(**가상 라우터 추가**)**를 클릭하고 Sales(영업)를 생성합니다.
d) **Add Virtual Router(**가상 라우터 추가**)**를 클릭하고 Warehouse(창고)를 생성합니다.
e) **Virtual Router Properties(**가상 라우터 속성**)**의 가상 라우터 드롭다운에서 Sales(영업)를 선택하고 VR-Sales를 **Selected Interface(**선택된 인터페이스**)**로 추가하고 저장합니다.
f) **Virtual Router Properties(**가상 라우터 속성**)**의 가상 라우터 드롭다운에서 Warehouse(창고)를 선택하고 VR-Warehouse를 **Selected Interface(**선택된 인터페이스**)**로 추가하고 저장합니다.

단계 **4** VR-Warehouse 인터페이스 컨피그레이션을 다시 확인합니다:

a) **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Interfaces(**인터페이스**)**를 선택합니다.
b) VR-Warehouse 인터페이스에 대해 **Edit(**편집**)**를 클릭합니다. IP 주소를 10.30.0.1/24로 지정합니다. 이제 시스템에서 VR-Sales의 동일한 IP 주소로 구성할 수 있습니다. 왜냐하면 인터페이스는 두 개의 서로 다른 가상 라우터에 별도로 할당되기 때문입니다.
c) **Ok(**확인**)**를 클릭합니다.
d) **Save(**저장**)**를 클릭합니다.

단계 **5** 창고 서버용 네트워크 개체 생성-10.50.0.0/24 및 창고 게이트웨이에 대한 네트워크 개체 생성 -10.40.0.2/30:

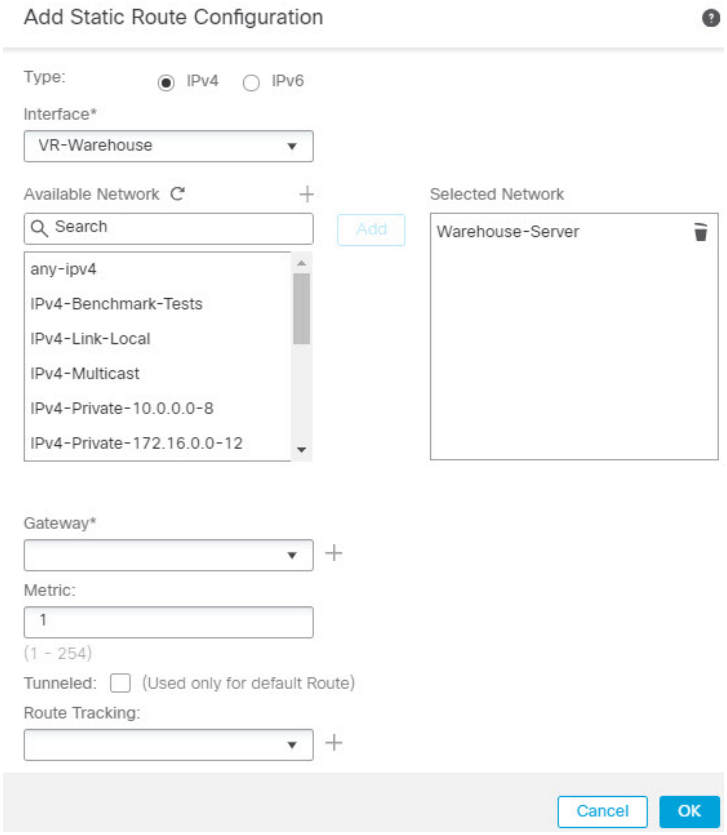
a) **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택합니다.
b) **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 선택합니다.
   - 이름-이 예시로는 Warehouse-Server가 있습니다.
   - 네트워크-Network(네트워크)를 클릭하고 10.50.0.0/24를 입력합니다.

c) **Save(**저장**)**를 클릭합니다.
d) **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 선택합니다.
   - 이름-이 예시로는 Warehouse-Gateway가 있습니다.
   - 네트워크)-Host를 클릭하고 10.40.0.2를 입력합니다.

e) **Save(**저장**)**를 클릭합니다.

단계 **6** VR-Warehouse 인터페이스를 가리키는 영업의 경로 유출을 정의합니다.

a) **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 threat defense 디바이스를 편집합니다.
b) **Routing(**라우팅**)**을 선택합니다.
c) 드롭다운에서 영업 가상 라우터를 선택한 다음 **Static Route(**정적 경로**)**를 클릭합니다.
d) **Add Route(**경로 추가**)**를 클릭합니다. **Add Static Route Configuration(**정적 경로 구성 추가**)**에서 다음을 지정합니다.
   - 인터페이스-VR-Warehouse를 선택합니다.
   - 네트워크 — Warehouse-Server 개체를 선택합니다.
   - 게이트웨이 — 이 항목은 비워둡니다. 다른 가상 라우터로 경로를 유출할 경우에는 게이트웨이를 선택하지 마십시오.

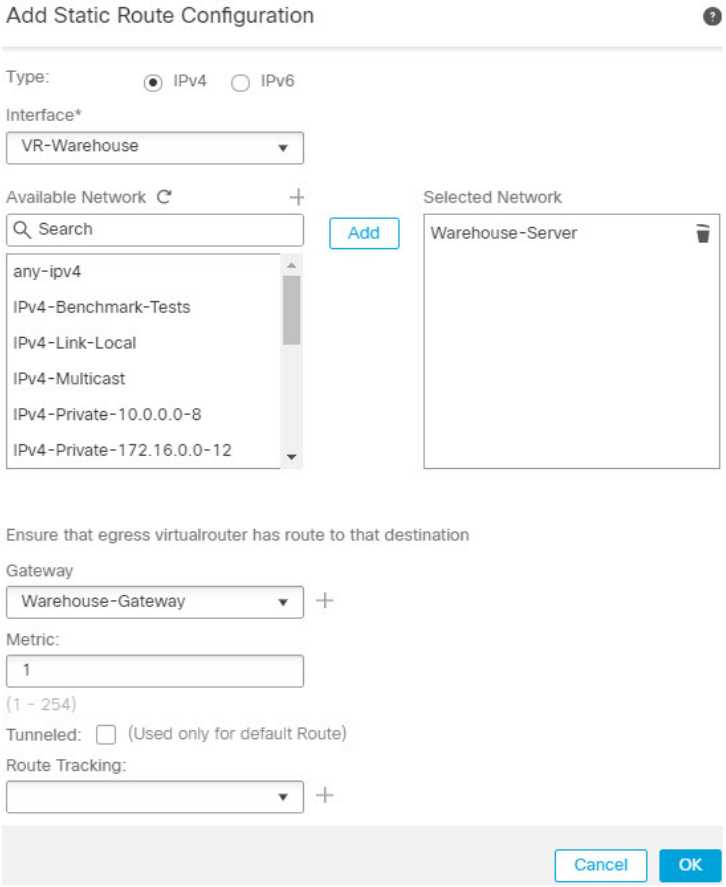



e) **Ok(**확인**)**를 클릭합니다.
f) **Save(**저장**)**를 클릭합니다.

단계 **7** 창고 가상 라우터에서 창고 라우터 2 게이트웨이를 가리키는 경로를 정의합니다:

a) 드롭다운에서 창고 가상 라우터를 선택한 다음 **Static Route(**정적 경로**)**를 클릭합니다.
b) **Add Route(**경로 추가**)**를 클릭합니다. **Add Static Route Configuration(**정적 경로 구성 추가**)**에서 다음을 지정합니다.
   - 인터페이스-VR-Warehouse를 선택합니다.

- 네트워크 — Warehouse-Server 개체를 선택합니다.
- 게이트웨이 — Warehouse-Gateway 개체를 선택합니다.



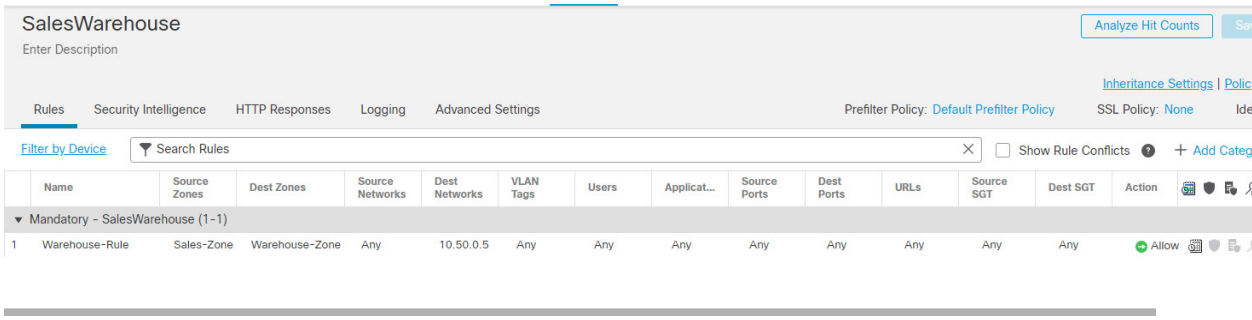

c) **Ok(**확인**)**를 클릭합니다.

d) **Save(**저장**)**를 클릭합니다.

단계 **8** 창고 서버에 대한 액세스를 허용하는 액세스 컨트롤 규칙을 구성합니다. 액세스 컨트롤 규칙을 생성하려면 보안 영역을 생성해야 합니다. **Object(**개체**)** > **Object Management(**개체 관리**)** > **Interface(**인터페이스**)**를 사용합니다. **Add(**추가**)** > **Security Zone(**보안 영역**)**을 선택하고 VR-Sales와 VR-Warehouse에 대한 보안 영역을 생성합니다. Warehouse-Server 네트워크 개체의 경우, Warehouse-Server 인터페이스 그룹**(Add(**추가**)** > **Interface Group(**인터페이스 그룹**)** 선택)을 생성합니다.

단계 **9** 정책 > 액세스 컨트롤을 선택하고 액세스 컨트롤 규칙을 구성하여 영업 가상 라우터에 있는 소스 인터페이스의 트래픽을 대상 Warehouse-Server 네트워크 개체에 대한 창고 가상 라우터에 있는 대상 인터페이스로 전송할 수 있습니다.

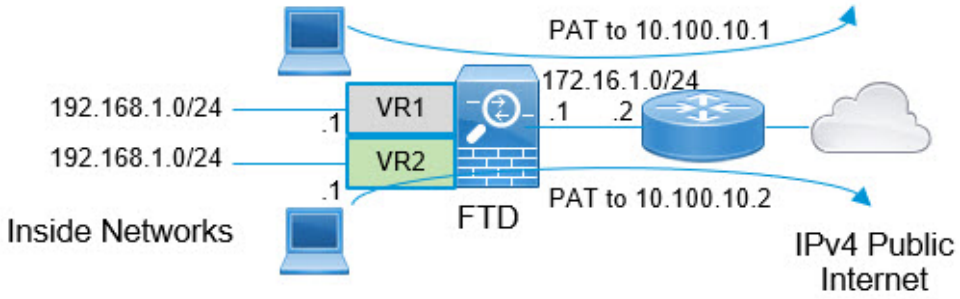
예를 들어 영업 가상 라우터에 있는 인터페이스가 Sales-Zone 보안 영역에 있을 경우, 창고 가상 라우터에 있는 해당 인터페이스는 Warehouse-Zone 보안 영역에 존재하며 액세스 제어 규칙은 다음과 유사합니다.




# 중복된 주소 공간에 인터넷 액세스를 제공하는 방법

가상 라우터를 사용할 경우, 별도의 라우터에 상주하는 인터페이스에 대해 동일한 네트워크 주소를 사용할 수 있습니다. 그러나 이러한 별도의 가상 라우터에서 라우팅되는 IP 주소는 동일하므로 개별 NAT/PAT 풀이 있는 각 인터페이스에 NAT/PAT 규칙을 적용하여 반환 트래픽이 올바른 대상으로 전달되도록 합니다. 이 예에서는 중복 주소 공간을 관리하기 위해 가상 라우터 및 NAT/PAT 규칙을 구성하는 절차를 제공합니다.

예를 들어 FTD에서 vr1-inside 및 vr2-inside 인터페이스를 정의하여 두 인터페이스가 모두 192.168.1.1/24라는 IP 주소를 사용하도록 하고 192.168.1.0/24 네트워크의 해당 세그먼트에서 엔드포인트를 관리할 수 있습니다. 동일한 주소 공간을 사용하는 두 개의 가상 라우터에서 인터넷 액세스를 허용하려면, 각 가상 라우터 내의 인터페이스에 개별적으로 NAT 규칙을 적용해야 합니다. 이 경우 별도의 NAT 또는 PAT 풀을 사용하는 것이 좋습니다. PAT를 사용하여 VR1의 소스 주소를 10.100.10.1로 변환하고, VR2의 소스 주소를 10.100.10.2로 변환할 수 있습니다. 아래 그림에는 이러한 설정이 나와 있습니다. 여기서 인터넷 연결 외부 인터페이스는 전역 라우터의 일부입니다. 소스 인터페이스(vr1-inside 및 vr2-inside)를 명시적으로 선택한 상태에서 NAT/PAT 규칙을 정의해야 합니다. 왜냐하면 "any"를 소스 인터페이스로 사용할 경우 2개의 서로 다른 인터페이스에 동일한 IP 주소가 존재할 수 있으므로, 시스템에서 올바른 소스를 식별하는 것이 불가능하기 때문입니다.




참고 중복된 주소 공간을 사용하지 않는 가상 라우터 내에 일부 인터페이스가 있는 경우에도 NAT 규칙을 소스 인터페이스로 정의하면 문제 해결을 더 쉽게 하고, 인터넷에 바인딩된 가상 라우터에서 나가는 트래픽을 더 명확하게 분리할 수 있습니다.

프로시저

단계 **1** VR1에 대한 디바이스의 내부 인터페이스를 구성합니다.

a) **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Interfaces(**인터페이스**)**를 선택합니다.

b) VR1에 할당할 인터페이스를 수정합니다.

- **Name(**이름**)** - 이 예에서는 vr1-inside입니다.
- 활성화 확인란을 선택합니다.
- **IPV4**에서 **IP** 유형의 경우 **Use Static IP(**정적 **IP** 사용**)**를 선택합니다.
- **IP Address(IP** 주소**)**-192.168.1.1/24를 입력합니다.

c) **Ok(**확인**)**를 클릭합니다.

d) **Save(**저장**)**를 클릭합니다.

단계 **2** VR2에 대한 디바이스의 내부 인터페이스를 구성합니다.

a) **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Interfaces(**인터페이스**)**를 선택합니다.

b) VR2에 할당할 인터페이스를 수정합니다.

- **Name(**이름**)** - 이 예에서는 vr2-inside입니다.
- 활성화 확인란을 선택합니다.
- **IPV4**에서 **IP** 유형의 경우 **Use Static IP(**정적 **IP** 사용**)**를 선택합니다.
- **IP** 주소 - 공백으로 둡니다. 아직 사용자 정의 가상 라우터를 생성하지 않았으므로 동일한 IP 주소의 인터페이스를 구성할 수 없습니다.

c) **Ok(**확인**)**를 클릭합니다.

d) **Save(**저장**)**를 클릭합니다.

단계 **3** 외부 인터페이스에 대한 정적 기본 경로 유출과 VR1을 구성합니다.

a) **Device(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스를 수정합니다.

b) **Routing(**라우팅**)** > **Manage Virtual Routers(**가상 라우터 관리**)**를 선택합니다. **Add Virtual Router(**가상 라우터 추가**)**를 클릭하고 VR1을 생성합니다.

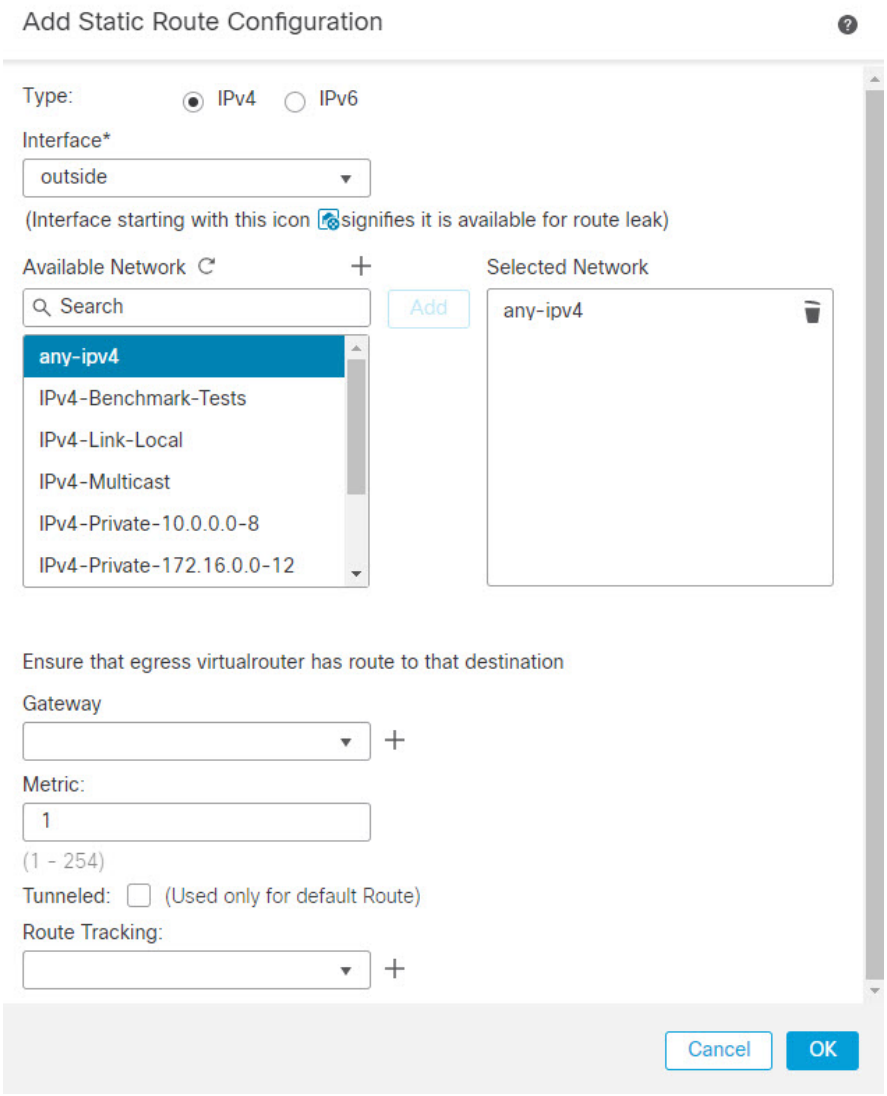
c) VR1의 경우 **Virtual Router Properties(**가상 라우터 속성**)**에서 vr1-inside를 할당하고 저장합니다.

d) **Static Route(**정적 경로**)**를 클릭합니다.

e) **Add Route(**경로 추가**)**를 클릭합니다. **Add Static Route Configuration(**정적 경로 구성 추가**)**에서 다음을 지정합니다.

- **Interface(**인터페이스**)** - 전역 라우터의 외부 인터페이스를 선택합니다.
- **Networks(**네트워크**)** — any-ipv4 개체를 선택합니다. 이 네트워크가 VR1 내에서 라우팅될 수 없는 모든 트래픽에 대한 기본 경로가 됩니다.

- **Gateway(**게이트웨이**)** — 이 항목은 비워둡니다. 다른 가상 라우터로 경로를 유출할 경우에는 게이트웨이를 제공하지 마십시오.




f) **Ok(**확인**)**를 클릭합니다.

g) **Save(**저장**)**를 클릭합니다.

단계 **4** 외부 인터페이스에 대한 정적 기본 경로 유출과 VR2을 구성합니다.

a) **Device(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스를 수정합니다.

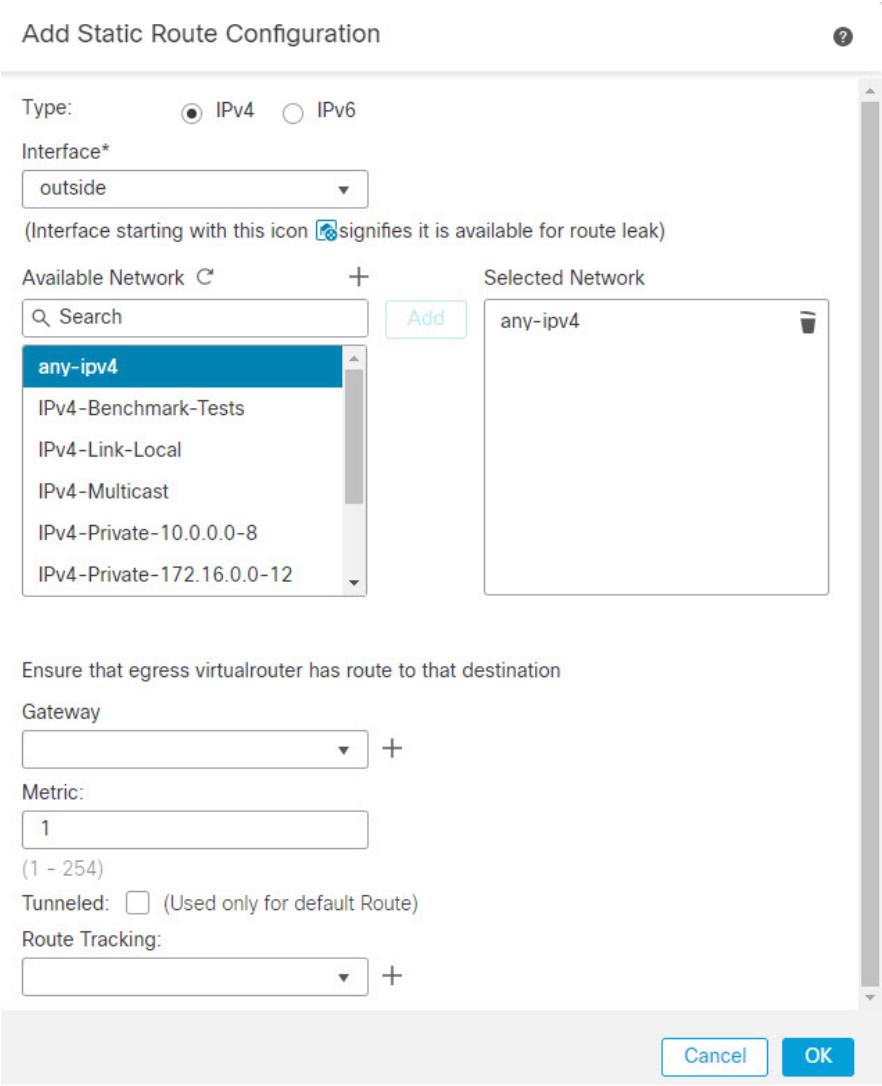
b) **Routing(**라우팅**)** > **Manage Virtual Routers(**가상 라우터 관리**)**를 선택합니다. **Add Virtual Router(**가상 라우터 추가**)**를 클릭하고 VR2를 생성합니다.

c) VR2의 경우 **Virtual Router Properties(**가상 라우터 속성**)**에서 vr2-inside를 할당하고 저장합니다.

d) **Static Route(**정적 경로**)**를 클릭합니다.

e) **Add Route(**경로 추가**)**를 클릭합니다. **Add Static Route Configuration(**정적 경로 구성 추가**)**에서 다음을 지정합니다.

- **Interface(**인터페이스**)** - 전역 라우터의 외부 인터페이스를 선택합니다.
- **Networks(**네트워크**)** — any-ipv4 개체를 선택합니다. 이 네트워크가 VR2 내에서 라우팅될 수 없는 모든 트래픽에 대한 기본 경로가 됩니다.
- **Gateway(**게이트웨이**)** — 이 항목은 비워둡니다. 다른 가상 라우터로 경로를 유출할 경우에는 게이트웨이를 선택하지 마십시오.



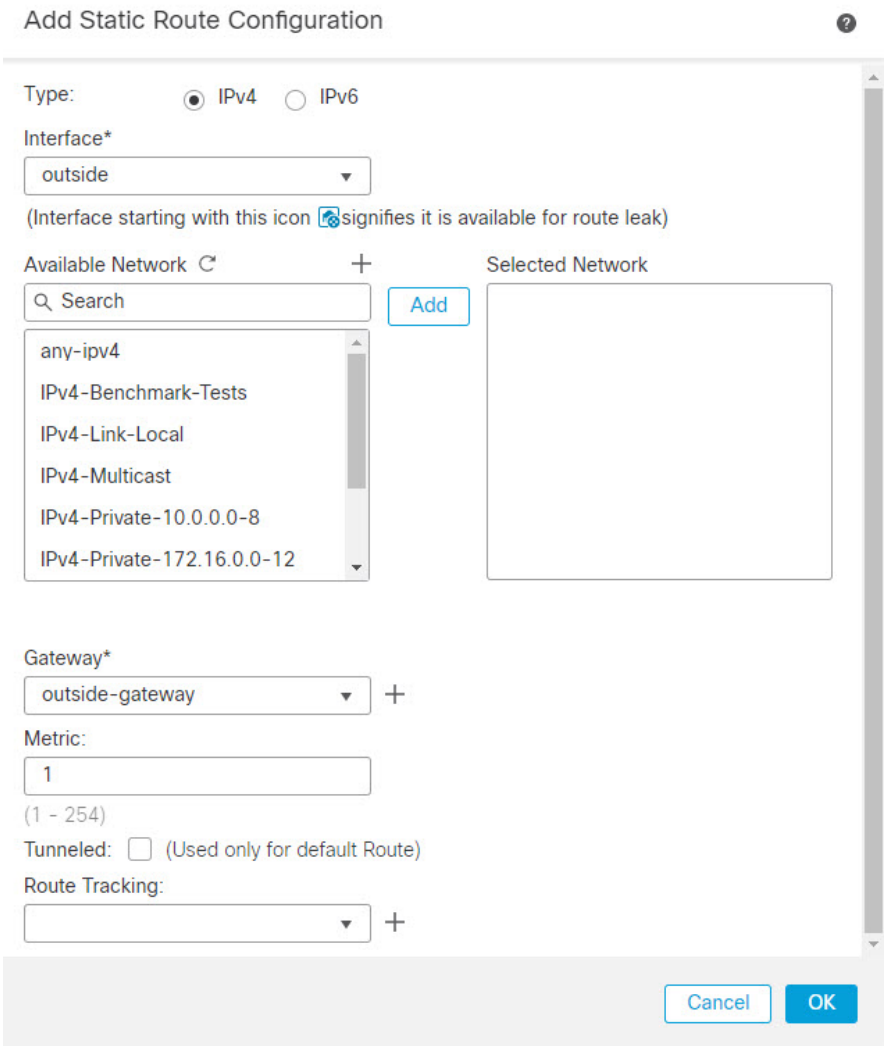

f) **Ok(**확인**)**를 클릭합니다.

g) **Save(**저장**)**를 클릭합니다.

단계 **5** 전역 라우터의 외부 인터페이스에서 IPv4 고정 기본 경로(즉, 172.16.1.2)를 구성합니다.

a) **Device(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스를 수정합니다.
b) **Routing(**라우팅**)**을 선택하고 전역 라우터 속성을 수정합니다.
c) **Static Route(**정적 경로**)**를 클릭합니다.
d) **Add Route(**경로 추가**)**를 클릭합니다. **Add Static Route Configuration(**정적 경로 구성 추가**)**에서 다음을 지정합니다.

- **Interface(**인터페이스**)** - 전역 라우터의 외부 인터페이스를 선택합니다.
- **Networks(**네트워크**)** — any-ipv4 개체를 선택합니다. 이 경로가 모든 IPv4 트래픽에 대한 기본 경로가 됩니다.
- **Gateway(**게이트웨이**)**-이미 생성된 경우 드롭 다운에서 호스트 이름을 선택합니다. 개체가 아직 생성되지 않았다면 **Add(**추가**)**를 클릭한 다음 외부 인터페이스에서 네트워크 링크의 다른 끝에 있는 게이트웨이의 IP 주소(이 예에서는 172.16.1.2)에 대한 호스트 개체를 정의합니다. 개체를 생성한 후 게이트웨이 필드에서 해당 개체를 선택합니다.



e) **Ok(**확인**)**를 클릭합니다.
f) **Save(**저장**)**를 클릭합니다.

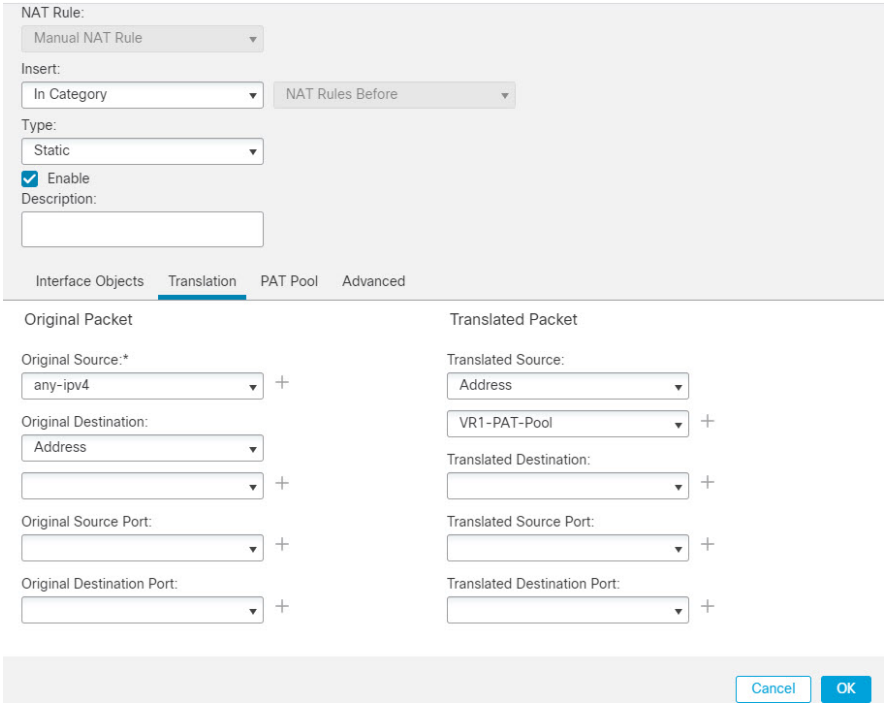
단계 **6** vr2-inside 인터페이스 구성을 다시 확인합니다.

a) **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Interfaces(**인터페이스**)**를 선택합니다.
b) vr2-inside 인터페이스에 대해 **Edit(**편집**)**를 클릭합니다. IP 주소를 192.168.1.1/24로 지정합니다. 이제 시스템에서 vr1-inside의 동일한 IP 주소로 구성할 수 있습니다. 왜냐하면 인터페이스는 두 개의 서로 다른 가상 라우터에 별도로 할당되기 때문입니다.
c) **Ok(**확인**)**를 클릭합니다.
d) **Save(**저장**)**를 클릭합니다.

단계 **7** VR1의 외부 트래픽이 10.100.10.1로 향하도록 PAT inside에 대한 NAT 규칙을 생성합니다.

a) **Devices(**디바이스**)** > **NAT**를 선택합니다.
b) **New Policy(**새 정책**)** > **Threat Defense NAT**를 클릭합니다.
c) NAT 정책 이름으로 InsideOutsideNATRule을 입력하고 FTD 디바이스를 선택합니다. **Save(**저장**)**를 클릭합니다.
d) InsideOutsideNATRule 페이지에서 **Add Rule(**규칙 추가**)**을 클릭하고 다음을 정의합니다.

- **NAT Rule(NAT** 규칙**)** - Manual NAT Rule(수동 NAT 규칙)을 선택합니다.
- **Type(**유형**)** - Dynamic(동적)을 선택합니다.
- **Insert(**삽입**)**-동적 NAT 규칙이 있는 경우 위의 내용을 입력합니다.
- **Enable(**활성화**)**을 클릭합니다.
- **Interface Objects(**인터페이스 개체**)**에서 vr1-interface object(vr1-인터페이스 개체)를 선택하고 **Add to Source(**소스에 추가**)** 를 클릭합니다(개체를 사용할 수없는 경우, **Object(**개체**)** > **Object Management(**개체 관리**)** > **Interface(**인터페이스**)**에서 하나를 생성). outside(외부)를 **Add to Destination(**대상에 추가**)**로 선택합니다.
- **Translation(**변환)에서 **Original Source(**원본 소스**)**로 any-ipv4를 선택합니다. **Translated Source(**변환된 소스**)**에서 **Add(**추가**)**를 클릭하고 호스트 개체 VR1-PAT-Pool을 10.100.10.1로 정의합니다. 아래 그림과 같이 VR1-PAT-Pool을 선택합니다.




e) **Ok(**확인**)**를 클릭합니다.

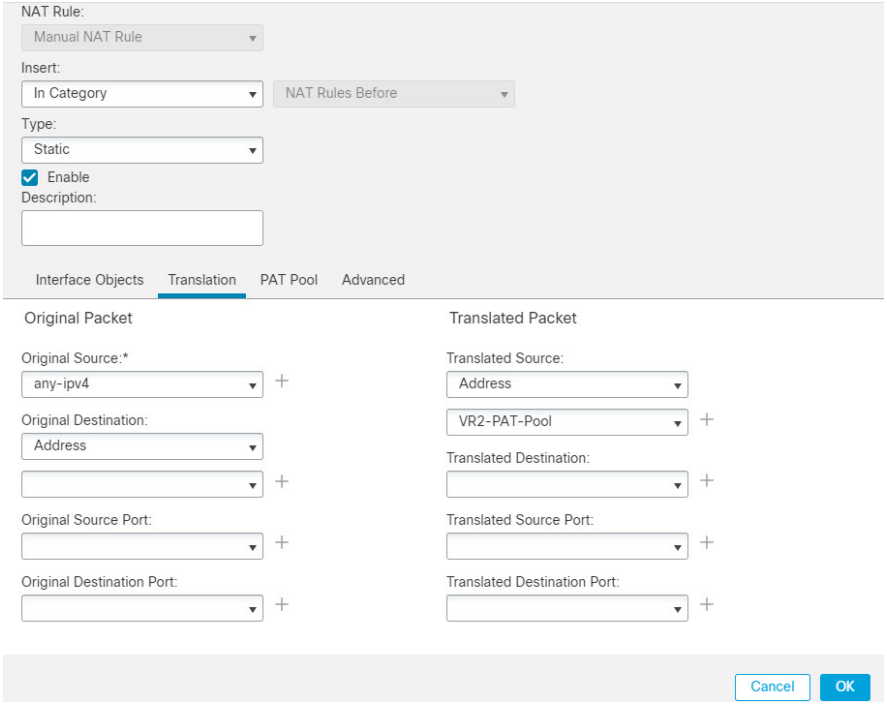
f) **Save(**저장**)**를 클릭합니다.

단계 **8** VR2의 외부 트래픽이 10.100.10.2로 향하도록 PAT inside에 대한 NAT 규칙을 추가합니다.

a) **Devices(**디바이스**) > NAT**를 선택합니다.

b) InsideOutsideNATRule을 수정하여 VR2 NAT 규칙을 정의합니다.

- **NAT Rule(NAT** 규칙**)** - Manual NAT Rule(수동 NAT 규칙)을 선택합니다.
- **Type(**유형**)** - Dynamic(동적)을 선택합니다.
- **Insert(**삽입**)**-동적 NAT 규칙이 있는 경우 위의 내용을 입력합니다.
- **Enable(**활성화**)**을 클릭합니다.
- **Interface Objects(**인터페이스 개체**)**에서 vr2-interface object(vr2-인터페이스 개체)를 선택하고 **Add to Source(**소스에 추가**)**를 클릭합니다(개체를 사용할 수없는 경우, **Object(**개체**) > Object Management(**개체 관리**) > Interface(**인터페이스**)**에서 하나를 생성). outside(외부)를 **Add to Destination(**대상에 추가**)**로 선택합니다.
- **Translation(**변환)에서 **Original Source(**원본 소스**)**로 any-ipv4를 선택합니다. **Translated Source(**변환된 소스**)**에서 **Add(**추가**)**를 클릭하고 호스트 개체 VR2-PAT-Pool을 10.100.10.2로 정의합니다. 아래 그림과 같이 VR2-PAT-Pool을 선택합니다.



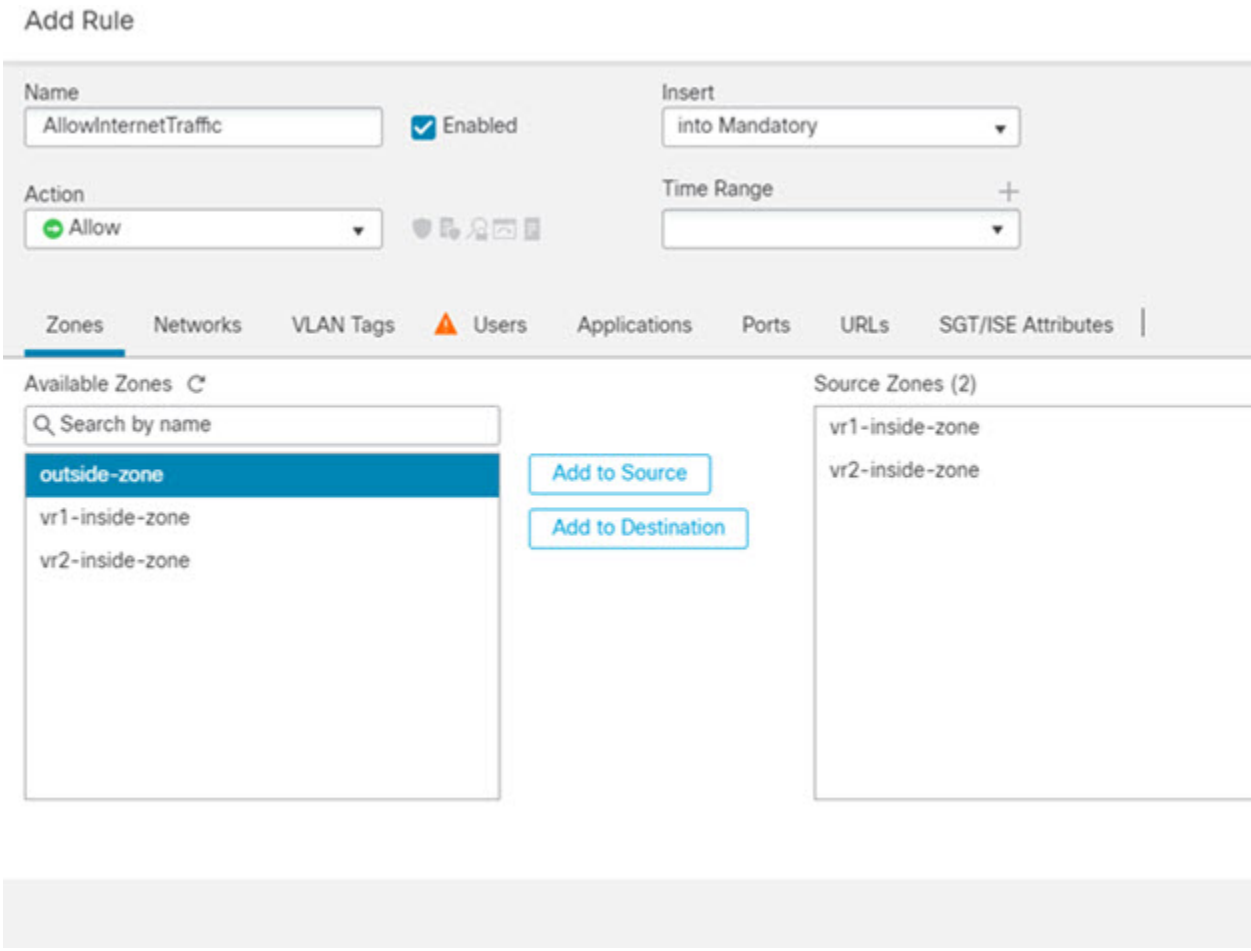

c) **Ok(**확인**)**를 클릭합니다.

d) **Save(**저장**)**를 클릭합니다.

단계 **9** vr1-inside 및 vr2-inside 인터페이스에서 외부 인터페이스로 향하는 트래픽을 허용하는 액세스 제어 정책을 구성하려면 보안 영역을 생성해야 합니다. **Object(**개체**)** > **Object Management(**개체 관리**)** > **Interface(**인터페이스**)**를 사용합니다. **Add(**추가**)** > **Security Zone(**보안 영역**)**을 선택하고 vr1-inside, vr2-inside 및 외부 인터페이스에 대한 보안 영역을 생성합니다.

단계 **10** **Policies(**정책**)** > **Access Control(**액세스 제어**)**을 선택하고, 트래픽이 vr1-inside-zone 및 vr2- inside-zone에서 outside_zone으로 향하도록 허용하는 액세스 제어 규칙을 구성합니다.

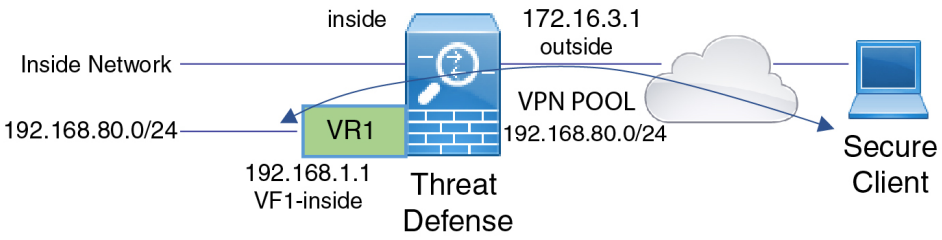
인터페이스의 이름을 딴 영역을 생성한다고 가정할 경우, 모든 트래픽이 인터넷으로 흐르도록 허용하는 기본 규칙은 다음과 같습니다. 이 액세스 제어 정책에 다른 매개 변수를 적용할 수 있습니다.




# RA VPN 액세스를 가상 라우터의 내부 네트워크에 허용하는 방법

가상 라우팅이 활성화된 디바이스에서는 RA VPN이 전역 가상 라우터 인터페이스에서만 지원됩니다. 이 예에서는 Secure Client 사용자가 사용자 정의 가상 라우터 네트워크에 연결할 수 있는 절차를 제공합니다.

다음 예에서 RA VPN 사용자(Secure Client)는 172.16.3.1의 threat defense 외부 인터페이스에 연결되며 192.168.80.0/24 풀 내에 IP 주소가 지정됩니다. 사용자는 전역 가상 라우터의 내부 네트워크에 액세스할 수 있습니다. 사용자 정의 가상 라우터 VR1(192.168.1.0/24)의 네트워크를 통한 트래픽 흐름을 허용하려면 전역 및 VR1에서 고정 경로를 구성하여 경로를 유출합니다.




시작하기 전에

이 예에서는 RA VPN을 이미 구성하고 가상 라우터를 정의했으며 적절한 가상 라우터에 인터페이스를 구성 및 할당한 것으로 가정합니다.

프로시저

단계 **1** 전역 가상 라우터에서 사용자 정의 VR1으로의 경로 유출을 설정합니다.

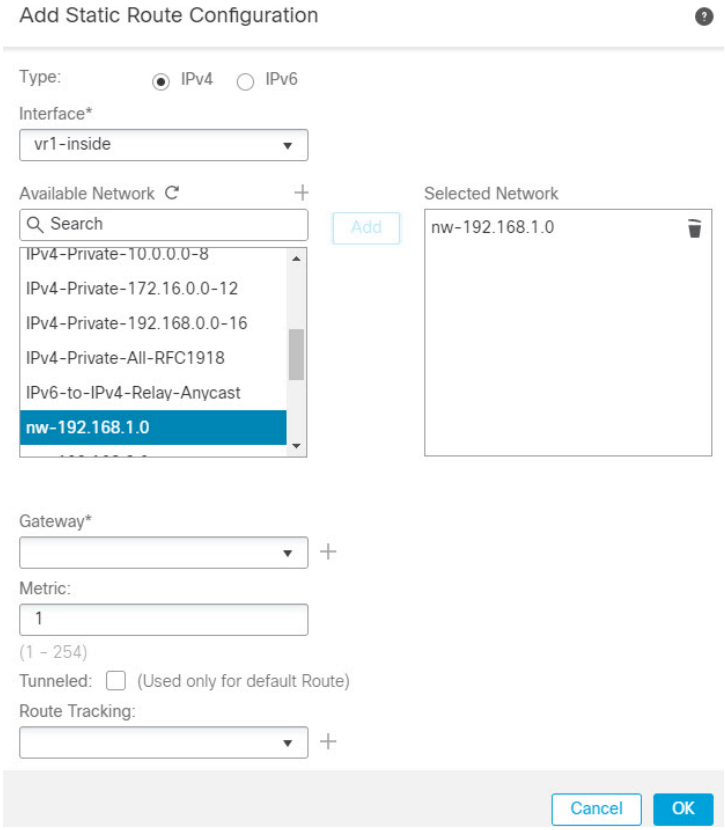
a) **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 threat defense 디바이스를 편집합니다.

b) **Routing(**라우팅**)**을 클릭합니다. 기본적으로 Global routing properties(전역 라우팅 속성) 페이지가 나타납니다.

c) **Static Route(**정적 경로**)**를 클릭합니다.

d) **Add Route(**경로 추가**)**를 클릭합니다. **Add Static Route Configuration(**정적 경로 구성 추가**)**에서 다음을 지정합니다.

- **Interface(**인터페이스**)** - VR1 내부 인터페이스를 선택합니다.
- **Network(**네트워크**)** - VR1 가상 라우터 네트워크 개체를 선택합니다. **Add Object(**개체 추가**)** 옵션을 사용하여 생성할 수 있습니다.
- **Gateway(**게이트웨이**)** — 이 항목은 비워둡니다. 다른 가상 라우터로 경로를 유출할 경우에는 게이트웨이를 선택하지 마십시오.




경로 누출을 사용하면 VPN 풀에서 Secure Client 할당 IP 주소로 VR1 가상 라우터에서 192.168.1.0/24 네트워크에 액세스할 수 있습니다.

e) **Ok(**확인**)**를 클릭합니다.

단계 **2** VR1에서 전역 가상 라우터로의 경로 유출을 설정합니다.

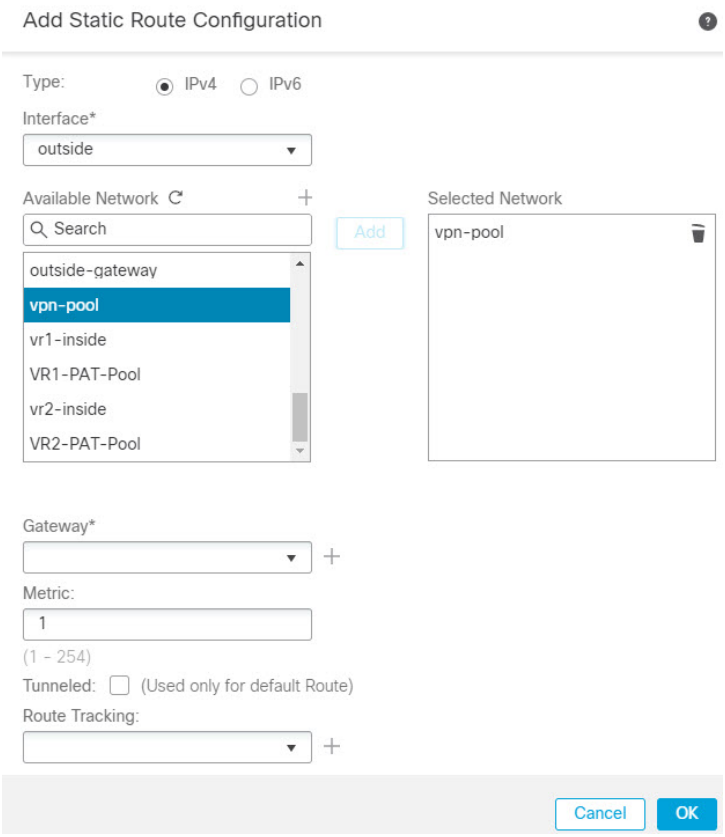
a) **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 threat defense 디바이스를 편집합니다.

b) **Routing(**라우팅**)**을 클릭하고 드롭다운에서 VR1을 선택합니다.

c) **Static Route(**정적 경로**)**를 클릭합니다.

d) **Add Route(**경로 추가**)**를 클릭합니다. **Add Static Route Configuration(**정적 경로 구성 추가**)**에서 다음을 지정합니다.

- **Interface(**인터페이스**)** - 전역 라우터의 외부 인터페이스를 선택합니다.
- **Network(**네트워크**)** - 전역 가상 라우터 네트워크 개체를 선택합니다.
- **Gateway(**게이트웨이**)** — 이 항목은 비워둡니다. 다른 가상 라우터로 경로를 유출할 경우에는 게이트웨이를 선택하지 마십시오.




구성된 정적 경로를 사용하면 192.168.1.0/24 네트워크(VR1)의 엔드포인트가 VPN 풀에서 Secure Client 할당 IP 주소에 대한 연결을 시작할 수 있습니다.

e) **Ok(**확인**)**를 클릭합니다.

---

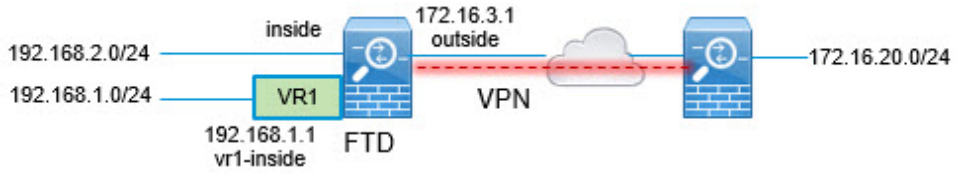
다음에 수행할 작업

RA VPN 주소 풀과 사용자 정의 가상 라우터의 IP 주소가 중복되는 경우 IP 주소에서 고정 NAT 규칙을 또한 사용하여 적절한 라우팅을 활성화해야 합니다. 또는 중복이 없도록 RA VPN 주소 풀을 변경할 수 있습니다.

# 사이트 간 VPN을 통해 여러 가상 라우터의 네트워크에서 트래픽을 보호하는 방법

가상 라우팅이 활성화된 디바이스에서는 사이트 간 VPN이 전역 가상 라우터 인터페이스에서만 지원됩니다. 사용자 정의 가상 라우터에 속한 인터페이스에서는 설정할 수 없습니다. 이 예에서는 사이트 간 VPN을 통해 사용자 정의 가상 라우터 내에서 호스팅되는 네트워크와의 연결을 보호할 수 있는 절차를 제공합니다. 또한 이러한 사용자 정의 가상 라우팅 네트워크를 포함하도록 사이트 간 VPN 연결을 업데이트해야 합니다.

지사 네트워크와 회사 본사 네트워크 사이에 사이트 간 VPN이 설정된 시나리오를 살펴보겠습니다. 가상 라우터가 있는 지사 사무실의 FTD입니다. 이 경우, 사이트 간 VPN은 172.16.3.1의 지사 외부 인터페이스에 정의됩니다. 내부 인터페이스는 전역 가상 라우터의 일부이므로 이 VPN에는 추가 설정 없이 내부 네트워크 192.168.2.0/24가 포함됩니다. 그러나 VR1 가상 라우터의 일부인 192.168.1.0/24 네트워크에 사이트 간 VPN 서비스를 제공하려면 전역 및 VR1에 정적 경로를 설정하여 경로를 유출하고 VR1 네트워크를 사이트 간 VPN 설정에 추가해야 합니다.




시작하기 전에

이 예에서는 192.168.2.0/24 로컬 네트워크와 172.16.20.0/24 외부 네트워트 간의 사이트 간 VPN을 이미 구성하고 가상 라우터를 정의했으며 적절한 가상 라우터에 인터페이스를 구성 및 할당한 것으로 가정합니다.

프로시저

단계 **1** 전역 가상 라우터에서 사용자 정의 VR1으로의 경로 유출을 설정합니다.

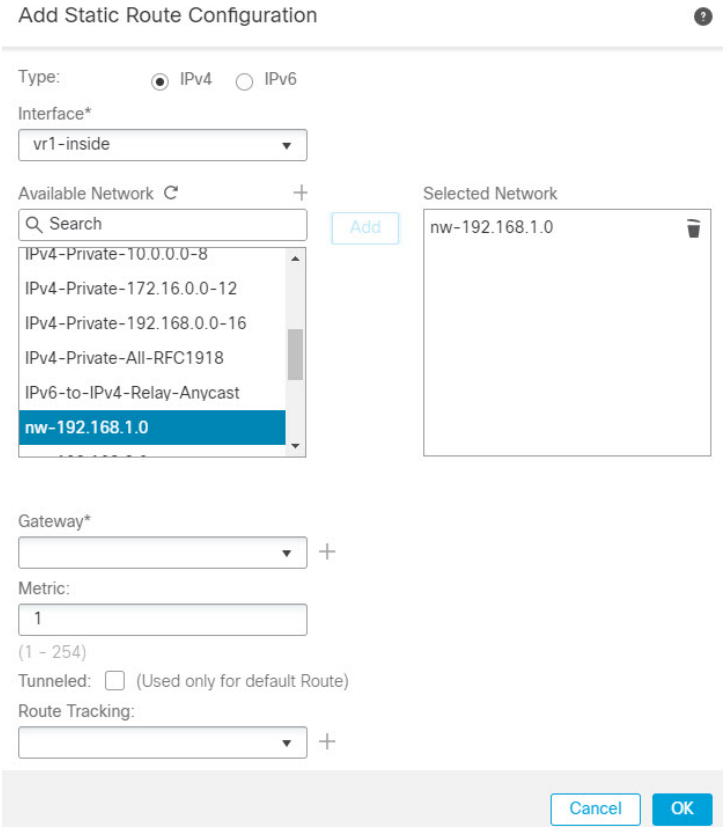
a) **Device(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스를 수정합니다.

b) **Routing(**라우팅**)**을 클릭합니다. 기본적으로 Global routing properties(전역 라우팅 속성) 페이지가 나타납니다.

c) **Static Route(**정적 경로**)**를 클릭합니다.

d) **Add Route(**경로 추가**)**를 클릭합니다. **Add Static Route Configuration(**정적 경로 구성 추가**)**에서 다음을 지정합니다.

- **Interface(**인터페이스**)** - VR1 내부 인터페이스를 선택합니다.
- **Network(**네트워크**)** - VR1 가상 라우터 네트워크 개체를 선택합니다. **Add Object(**개체 추가**)** 옵션을 사용하여 생성할 수 있습니다.
- 게이트웨이 — 이 항목은 비워둡니다. 다른 가상 라우터로 경로를 유출할 경우에는 게이트웨이를 선택하지 마십시오.




이 경로 유출은 사이트 간 VPN의 외부(원격) 끝에서 보호하는 엔드포인트를 VR1 가상 라우터의 192.168.1.0/24 네트워크에 액세스하는 데 사용할 수 있습니다.

e) **Ok(**확인**)**를 클릭합니다.

단계 **2** VR1에서 전역 가상 라우터로의 경로 유출을 설정합니다.

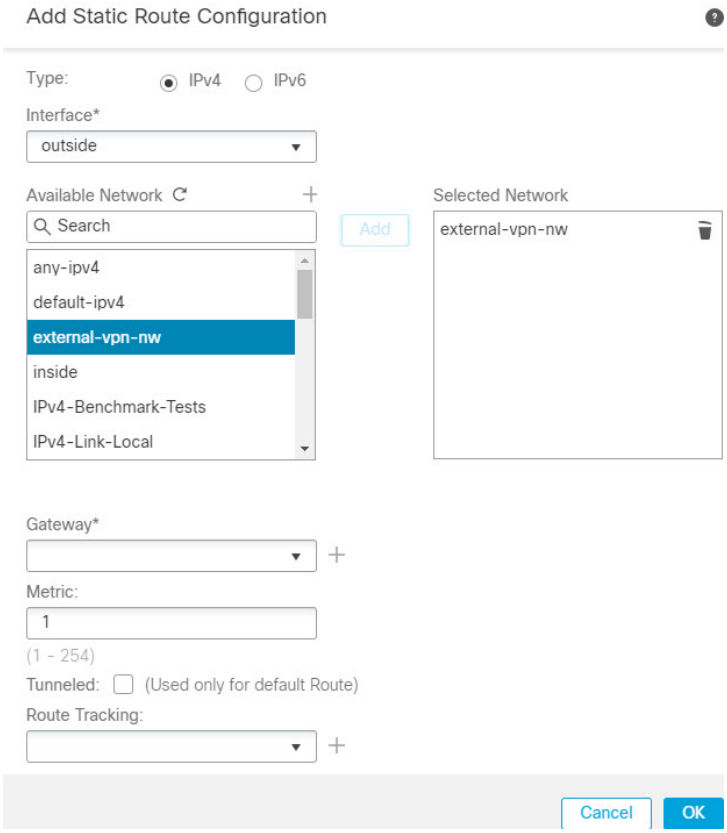
a) **Device(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스를 수정합니다.

b) **Routing(**라우팅**)**을 클릭하고 드롭다운에서 VR1을 선택합니다.

c) **Static Route(**정적 경로**)**를 클릭합니다.

d) **Add Route(**경로 추가**)**를 클릭합니다. **Add Static Route Configuration(**정적 경로 구성 추가**)**에서 다음을 지정합니다.

- **Interface(**인터페이스**)** - 전역 라우터의 외부 인터페이스를 선택합니다.
- **Network(**네트워크**)** - 전역 가상 라우터 네트워크 개체를 선택합니다.
- 게이트웨이 — 이 항목은 비워둡니다. 다른 가상 라우터로 경로를 유출할 경우에는 게이트웨이를 선택하지 마십시오.




이 정적 경로를 사용하면 192.168.1.0/24 네트워크(VR1)의 엔드포인트에서 사이트 간 VPN 터널을 통과하는 연결을 시작할 수 있습니다. 이 예에서는 원격 엔드포인트에서 172.16.20.0/24 네트워크를 보호하고 있습니다.

e) **Ok(**확인**)**를 클릭합니다.

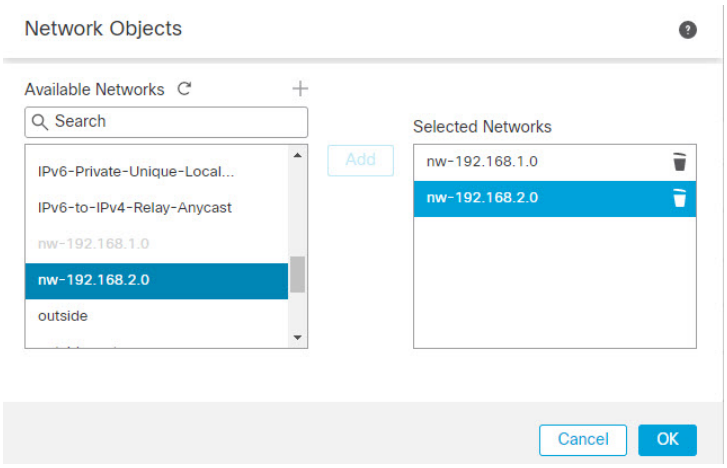
단계 **3** 사이트 간 VPN 연결 프로파일에 192.168.1.0/24 네트워크를 추가합니다.

a) **Devices(**디바이스**)** > **VPN** > **Site To Site(**사이트 간**)**를 선택하고 VPN 토폴로지를 편집합니다.

b) **Endpoints(**엔드포인트**)**에서 노드 A 엔드포인트를 편집합니다.

c) **Edit Endpoint(**엔드포인트 편집**)**의 **Protected Networks(**보호되는 네트워크**)** 필드에서 **Add New Network Object(**새 네트워크 개체 추가**)**를 클릭합니다.

d) 192.168.1.0 네트워크로 VR1 네트워크 개체를 추가합니다.

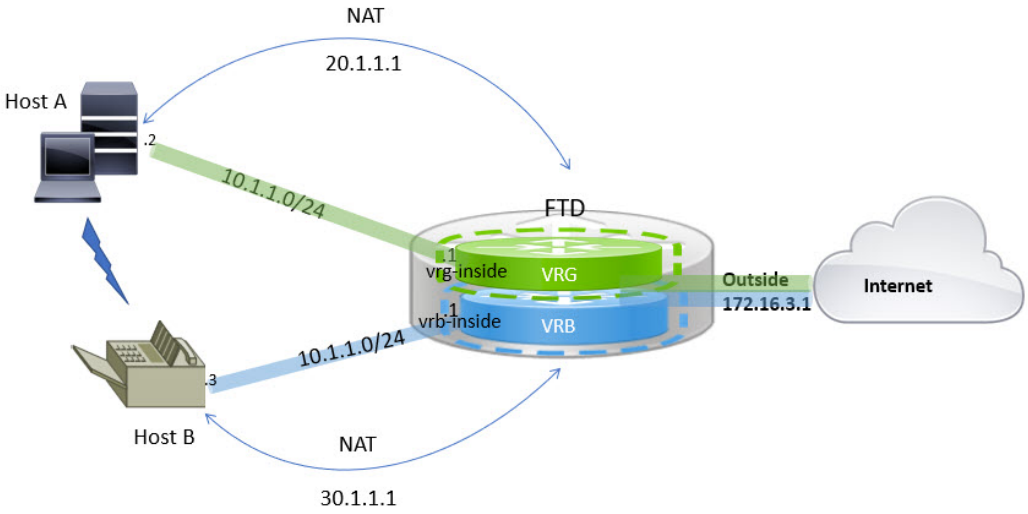



e) **OK(**확인**)**를 클릭하여 설정을 저장합니다.

# 가상 라우팅에서 두 개의 중복되는 네트워크 호스트 간에 트래픽을 라우팅하는 방법

동일한 네트워크 주소를 가진 가상 라우터에서 호스트를 구성할 수 있습니다. 호스트가 통신하려는 경우 NAT를 2회 구성할 수 있습니다. 이 예에서는 중복 네트워크 호스트를 관리하기 위해 NAT 규칙을 구성하는 절차를 제공합니다.

다음 예에서 호스트 A와 호스트 B의 두 호스트는 서로 다른 가상 라우터에 속합니다. VRG(인터페이스 vrg-inside), VRB(인터페이스 vrb-inside)는 각각 동일한 서브넷 10.1.1.0/24입니다. 두 호스트가 모두 통신할 수 있도록 VRG-Host 인터페이스 개체는 매핑된 NAT 주소 20.1.1.1을 사용하고, VRB-Host 인터페이스 개체는 매핑된 NAT 주소 30.1.1.1을 사용하는 NAT 정책을 생성합니다. 따라서 호스트 A는 30.1.1.1을 사용하여 호스트 B와 통신합니다. 호스트 B는 20.1.1.1을 사용하여 호스트 A에 연결합니다.



시작하기 전에

이 예시에서는 다음 항목을 이미 구성한 것으로 가정합니다.

- vrg-inside 및 vrb-inside 인터페이스는 가상 라우터(각각 VRG 및 VRB) 및 동일한 서브넷 주소(예: 10.1.1.0/24)로 구성된 vrg-inside 및 vrb-inside 인터페이스와 연결됩니다.
- 인터페이스 영역 VRG-Inf, VRB-Inf는 각각 vrg-inside 및 vrb-inside 인터페이스로 생성됩니다.
- vRG-inside를 기본 게이트웨이로 사용하는 VRG의 호스트 A. vrb-inside를 기본 게이트웨이로 사용하는 VRB의 호스트 B

프로시저

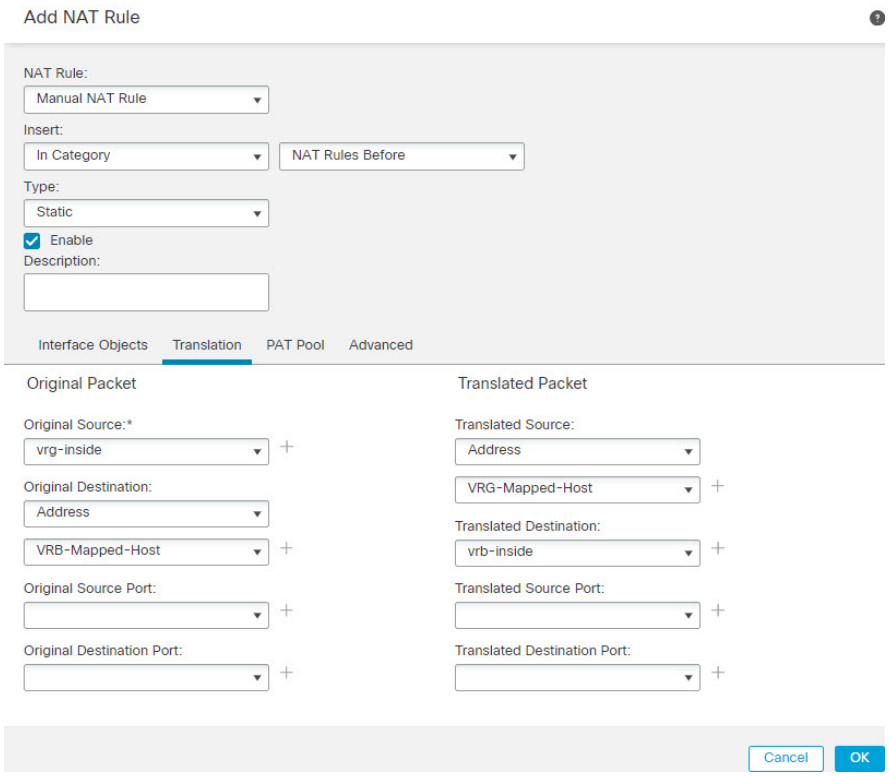
단계 **1** 호스트 A에서 호스트 B로의 트래픽을 처리할 NAT 규칙을 생성합니다. **Devices(**디바이스**)** > **NAT**를 선택합니다.

단계 **2** **New Policy(**새 정책**)** > **Threat Defense NAT**를 클릭합니다.

단계 **3** NAT 정책 이름을 입력하고 FTD 디바이스를 선택합니다. **Save(**저장**)**를 클릭합니다.

단계 **4** NAT 페이지에서 **Add Rule(**규칙 추가**)**을 클릭하고 다음을 정의합니다.

- **NAT Rule(NAT** 규칙**)** - Manual NAT Rule(수동 NAT 규칙)을 선택합니다.
- 유형 - Static(고정)을 선택합니다.
- **Insert (**삽입**)** - NAT 규칙이 있는 경우 Above(위에)를 선택합니다.
- **Enable(**활성화**)**을 클릭합니다.
- **Interface Objects(**인터페이스 개체**)**에서 VRG-Inf object(VRG-Inf 개체)를 선택하고 **Add to Source(**소스에 추가**)**를 클릭하고(개체를 사용할 수없는 경우, **Object(**개체**)** > **Object Management(**개체 관리**)** > **Interface(**인터페이스**)**에서 하나를 생성) VRB-Inf object(VRB-Inf 개체)를 선택하고 **Add to Destination(**대상에 추가**)**을 클릭합니다.
- **Translation(**변환**)**에서 다음을 선택합니다.
  - **Original Source(**원본 소스**)**: vrg-inside를 선택합니다.
  - **Original Destination(**원본 대상**)**에서 **Add(**추가**)**를 클릭하고 30.1.1.1로 개체 VRB-Mapped-Host를 정의합니다. VRB-Mapped-Host를 선택합니다.
  - **Translated Source(**변환된 소스**)**에서 **Add(**추가**)**를 클릭하고 20.1.1.1로 개체 VRG-Mapped-Host를 정의합니다. VRG-Mapped-Host를 선택합니다.
  - **Translated Destination(**변환된 대상**)**에서 다음 그림과 같이 vrb-inside를 선택합니다.



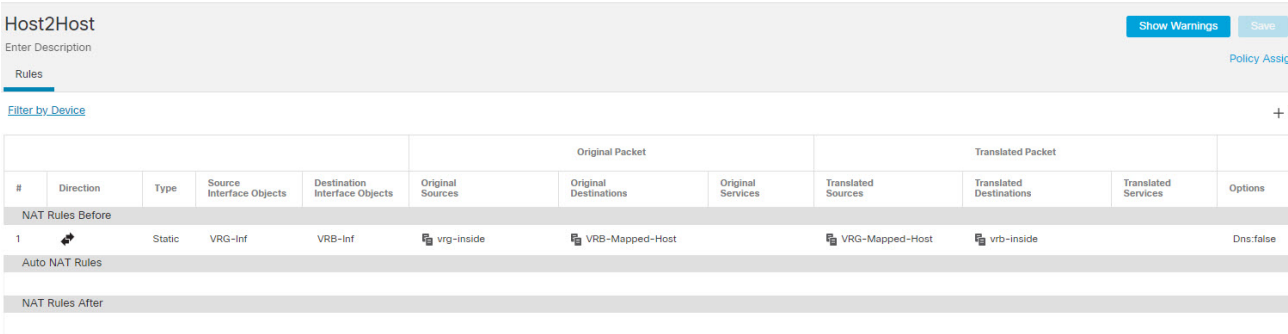

FTD 디바이스에서 **show nat detail** 명령을 실행하면 다음과 유사한 출력이 표시됩니다.

```
firepower(config-service-object-group)# show nat detail
Manual NAT Policies (Section 1)
1 (2001) to (3001) source static vrg-inside VRG-MAPPED-HOST destination static VRB-MAPPED-HOST
 vrb-inside
translate_hits = 0, untranslate_hits = 0
Source - Origin: 10.1.1.1/24, Translated: 20.1.1.1/24
Destination - Origin: 30.1.1.1/24, Translated: 10.1.1.1/24
```

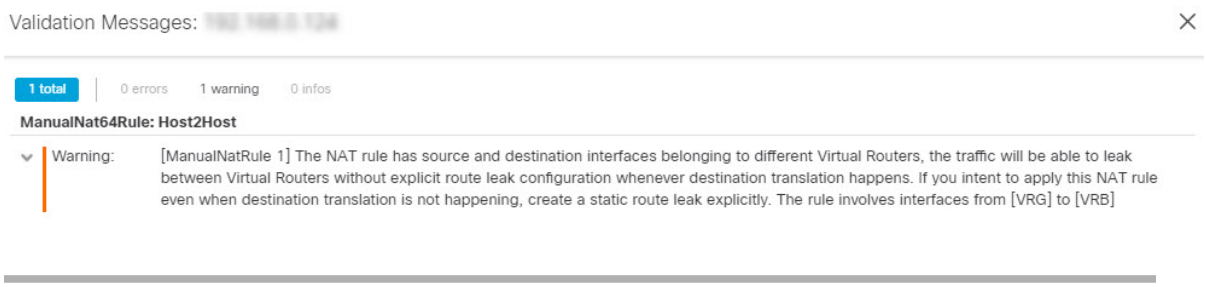
단계 **5** **Ok(**확인**)**를 클릭합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

NAT 규칙은 다음과 같습니다.




구성을 구축할 때 경고 메시지가 나타납니다.

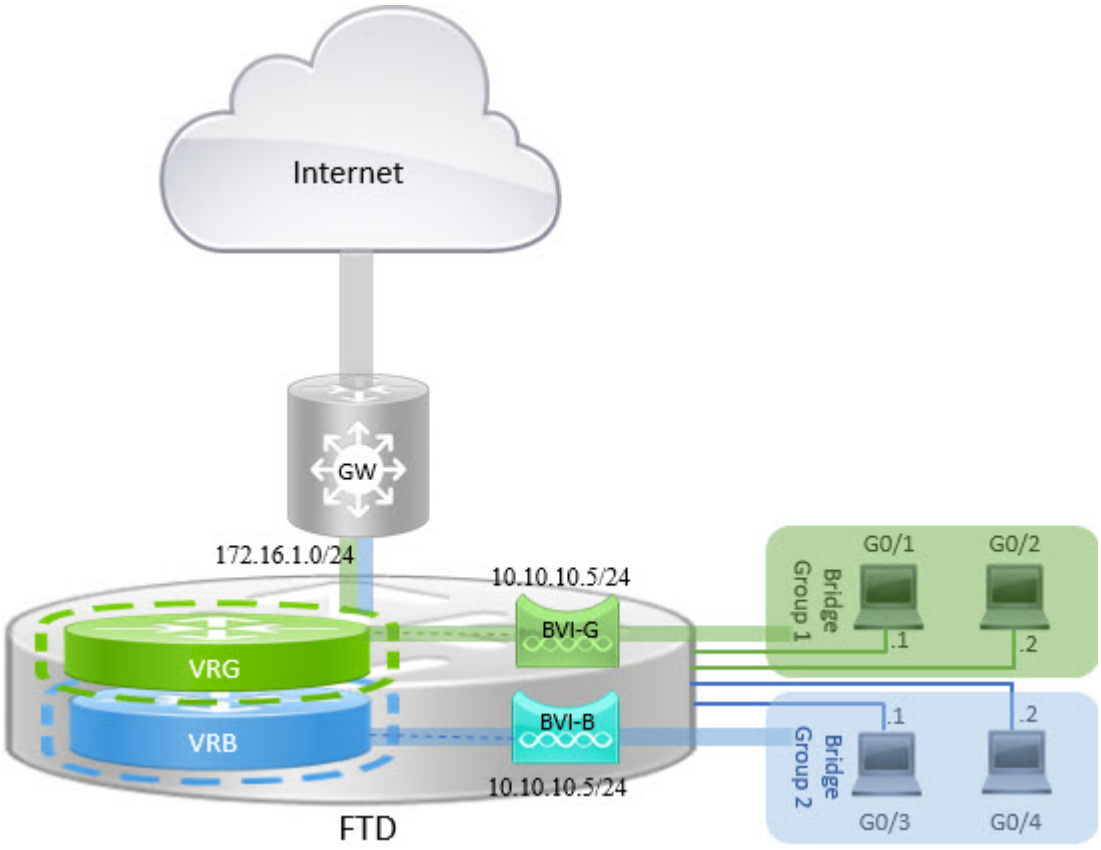



# BVI 인터페이스를 사용하여 라우팅 방화벽 모드에서 중복 세그먼트를 관리하는 방법

여러 중복 네트워크 간에 투명하게 단일 FTD를 구축하거나 동일한 네트워크의 호스트 간에 방화벽을 구축할 수 있습니다. 이 구축을 수행하려면 가상 라우터별로 BVI를 설정합니다. 가상 라우터에서 BVI를 설정하는 절차는 여기에 설명되어 있습니다.

BVI는 일반적인 라우팅 인터페이스처럼 작동하는 라우터 내의 가상 인터페이스입니다. 브리징은 지원하지 않지만, 라우터 내에서 라우팅된 인터페이스와 비교 가능한 브리지 그룹을 나타냅니다. 이러한 브리지된 인터페이스를 오가는 모든 패킷은 BVI 인터페이스를 통과합니다. BVI의 인터페이스 번호는 가상 인터페이스가 나타내는 브리지 그룹의 번호입니다.

다음 예에서 BVI-G는 VRG에 설정되고, 브리지 그룹 1은 인터페이스 G0/1 및 G0/2에 대한 라우팅 인터페이스입니다. 마찬가지로, BVI-B는 VRB에서 설정되며, 브리지 그룹 2는 인터페이스 G0/3 및 G0/4의 라우팅 인터페이스입니다. 두 BVI 모두 동일한 IP 서브넷 주소(예: 10.10.10.5/24)를 가집니다. 가상 라우터 때문에 네트워크가 공유 리소스에서 격리됩니다.



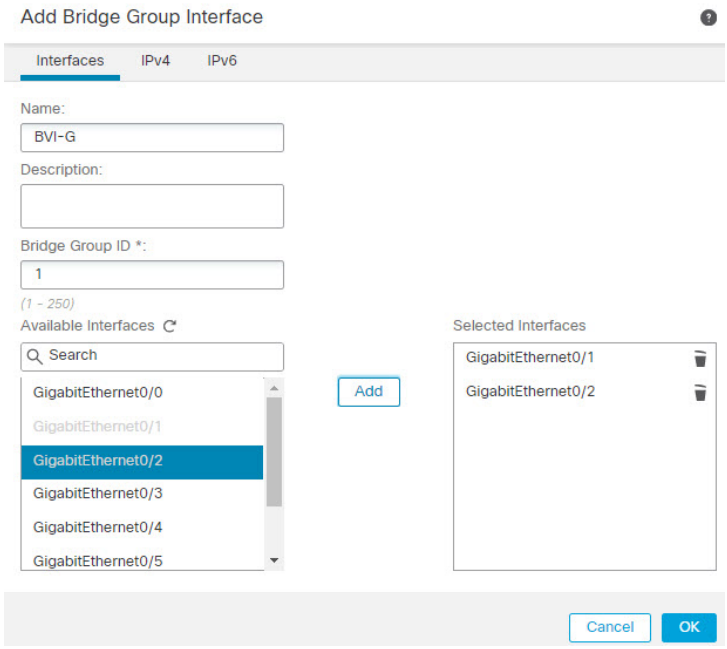

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택합니다. 필요한 디바이스를 편집합니다.

단계 **2** **Interfaces(**인터페이스**)**에서 **Add Interfaces(**인터페이스 추가**)** > **Bridge Group Interface(**브리지 그룹 인터페이스**)**를 선택합니다.

a) 다음 BVI-G 세부 사항을 입력합니다.

- **Name(**이름**)** - 이 예에서는 BVI-G입니다.
- **Bridge Group ID(**브리지 그룹 **ID)** - 이 예에서는 1입니다.
- **Available Interface(**사용 가능한 인터페이스**)** - 인터페이스를 선택합니다.
- **IPV4**에서 **IP** 유형의 경우 **Use Static IP(**정적 **IP** 사용**)**를 선택합니다.
- **IP Address(IP** 주소**)** - 10.10.10.5/24를 입력합니다.

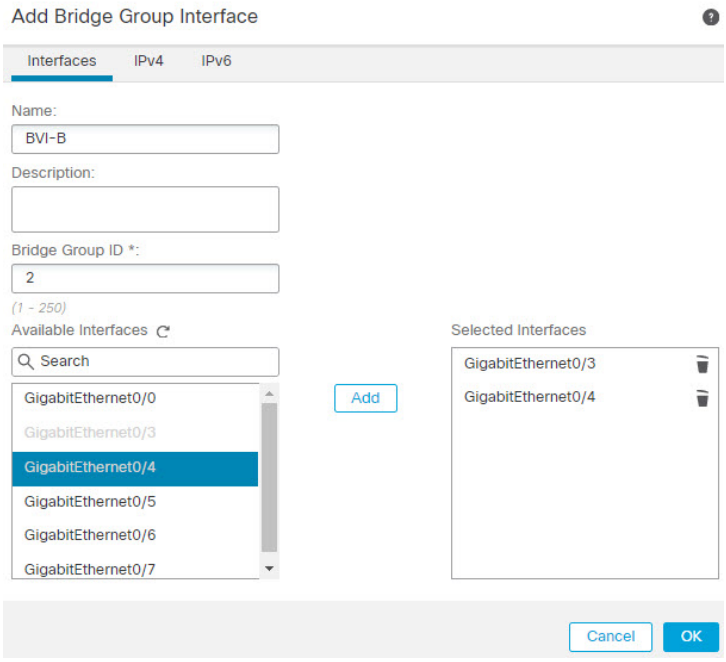



b) **Ok(**확인**)**를 클릭합니다.

c) **Save(**저장**)**를 클릭합니다.

a) 다음 BVI-B 세부 정보를 입력합니다.

- **Name(**이름**)** - 이 예에서는 BVI-B입니다.
- **Bridge Group ID(**브리지 그룹 **ID)** - 이 예에서는 2입니다.
- **Available Interface(**사용 가능한 인터페이스**)** - 하위 인터페이스를 선택합니다.
- **IPV4**에서 **IP** 유형의 경우 **Use Static IP(**정적 **IP** 사용**)**를 선택합니다.
- **IP Address(IP** 주소**)** - 시스템에서 두 인터페이스의 IP 주소 중복을 허용하지 않으므로 이 필드를 비워 두십시오. 브리지 그룹을 다시 방문하여 가상 라우터 아래에 정렬한 후 동일한 IP 주소를 제공할 수 있습니다.




b) **Ok(**확인**)**를 클릭합니다.

c) **Save(**저장**)**를 클릭합니다.

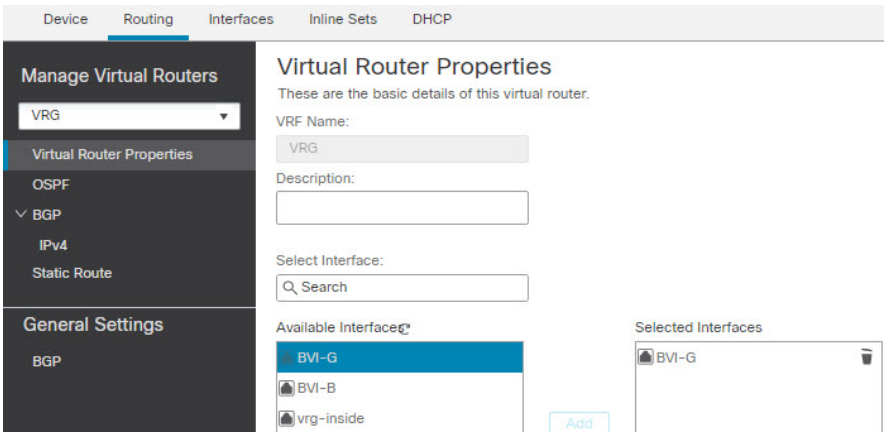
단계 **3** VRG라고 하는 가상 라우터를 생성하고 네트워크로 BVI-G를 선택합니다.

a) **Devices(**디바이스**) > Device Management(**디바이스 관리**)**를 선택합니다.

b) 디바이스를 편집하고 **Routing(**라우팅**) > Manage Virtual Routers(**가상 라우터 관리**)**를 선택합니다.

c) **Add Virtual Router(**가상 라우터 추가**)**를 클릭합니다. 가상 라우터의 이름을 입력하고 **Ok(**확인**)**를 클릭합니다.

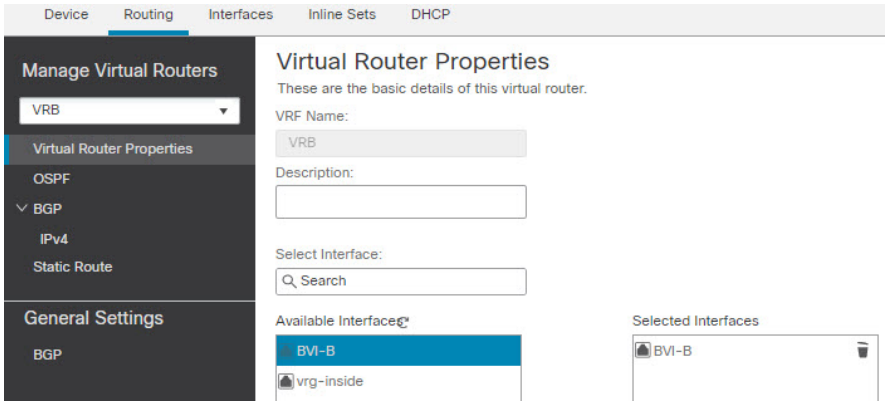
d) **Virtual Routing Properties(**가상 라우터 속성**)**에서 **BVI-G**를 선택하고 **Add(**추가**)**를 클릭합니다.




e) **Save(**저장**)**를 클릭합니다.

단계 **4** 가상 라우터를 생성하고(VRB라고 함) 네트워크로 BVI-B를 선택합니다.

a) **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택합니다.
b) 디바이스를 편집하고 **Routing(**라우팅**)** > **Manage Virtual Routers(**가상 라우터 관리**)**를 선택합니다.
c) **Add Virtual Router(**가상 라우터 추가**)**를 클릭합니다. 가상 라우터의 이름을 입력하고 **Ok(**확인**)**를 클릭합니다.
d) **Virtual Routing Properties(**가상 라우터 속성**)**에서 **BVI-B**를 선택하고 **Add(**추가**)**를 클릭합니다.




e) **Save(**저장**)**를 클릭합니다.

단계 **5** BVI-B 설정을 다시 살펴봅니다.

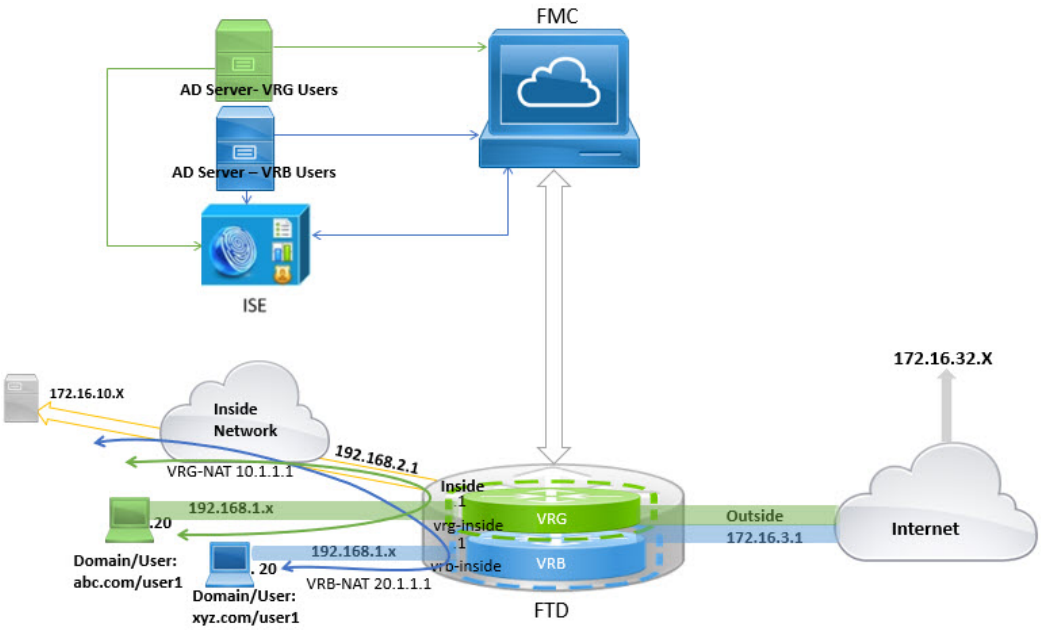
a) **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Interfaces(**인터페이스**)**를 선택합니다.
b) BVI-B 인터페이스에 대해 **Edit(**편집**)**을 클릭합니다. IP 주소를 10.10.10.5/24로 지정합니다. 인터페이스가 두 개의 서로 다른 가상 라우터에 별도로 할당되므로 이제 시스템에서 동일한 BVI-G IP 주소로 설정할 수 있습니다.
c) **Ok(**확인**)**를 클릭합니다.
d) **Save(**저장**)**를 클릭합니다.

BVI 간 통신을 활성화하려면 외부 라우터를 기본 게이트웨이로 사용합니다. 이 예와 같이 중복되는 BVI 시나리오에서는 NAT 외부 라우터를 게이트웨이로 두 번 사용하여 BVI 간 트래픽을 설정합니다. 브리지 그룹 멤버에 대해 NAT를 구성할 때는 멤버 인터페이스를 지정합니다. BVI(브리지 그룹 인터페이스) 자체에 대해서는 NAT를 구성할 수 없습니다. 브리지 그룹 멤버 인터페이스 간에 NAT를 수행할 때는 실제 및 매핑된 주소를 지정해야 합니다. 인터페이스로 "임의"를 지정할 수는 없습니다.

# 중복되는 네트워크로 사용자 인증을 구성하는 방법

가상 라우팅에서는 중복 IP 및 중복 사용자로 여러 가상 라우터를 구성할 수 있습니다. 이 예에서 VRG 및 VRB는 IP가 192.168.1.1/24로 중복되는 가상 라우터입니다. 서로 다른 두 도메인의 사용자가 네트워크 IP 192.168.1.20과 중복됩니다. VRG 및 VRB 사용자가 공유 서버 172.16.10.X에 액세스하는 경우 전역 가상 라우터로 라우트를 유출합니다. 소스 NAT를 사용하여 중복 IP를 처리합니다. VRG 및 VRB 사용자의 액세스를 제어하려면 FMC에서 사용자 인증을 설정해야 합니다. FMC는 영역, 활성 디렉토리, ID 소스, ID 규칙 및 정책을 사용하여 사용자 ID를 인증합니다. FTD는 사용자 인증에서 직접 역할

을 수행하지 않으므로 사용자 액세스는 액세스 제어 정책을 통해서만 관리됩니다. 중복되는 사용자의 트래픽을 제어하려면 ID 정책 및 규칙을 사용하여 액세스 제어 정책을 생성합니다.




시작하기 전에

이 예시에서는 사용자에게 다음 항목이 이미 있는 것으로 가정합니다.

- VRG 및 VRB 사용자용 AD 서버 2개
- AD 서버가 2개가 추가된 ISE.

프로시저

---

단계 **1** VRG에 대해 디바이스의 내부 인터페이스를 구성합니다.

a) **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Interfaces(**인터페이스**)**를 선택합니다.

b) VRG에 할당할 인터페이스를 편집합니다.

- **Name(**이름**)** - 이 예에서는 VRG-inside입니다.
- 활성화 확인란을 선택합니다.
- **IPV4**에서 **IP** 유형의 경우 **Use Static IP(**정적 **IP** 사용**)**를 선택합니다.
- **IP Address(IP** 주소**)**-192.168.1.1/24를 입력합니다.

c) **Ok(**확인**)**를 클릭합니다.

d) **Save(**저장**)**를 클릭합니다.

단계 **2** VRB에 대해 디바이스의 내부 인터페이스를 구성합니다.

a) **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Interfaces(**인터페이스**)**를 선택합니다.

b) VRB에 할당할 인터페이스를 편집합니다.

- **Name(**이름**)** - 이 예에서는 VRB-inside입니다.
- 활성화 확인란을 선택합니다.
- **IPV4**에서 **IP** 유형의 경우 **Use Static IP(**정적 **IP** 사용**)**를 선택합니다.
- **IP** 주소 - 공백으로 둡니다. 아직 사용자 정의 가상 라우터를 생성하지 않았으므로 동일한 IP 주소(10.30.0.1/24)의 인터페이스를 구성하는 것을 시스템에서 허용하지 않습니다.

c) **Ok(**확인**)**를 클릭합니다.

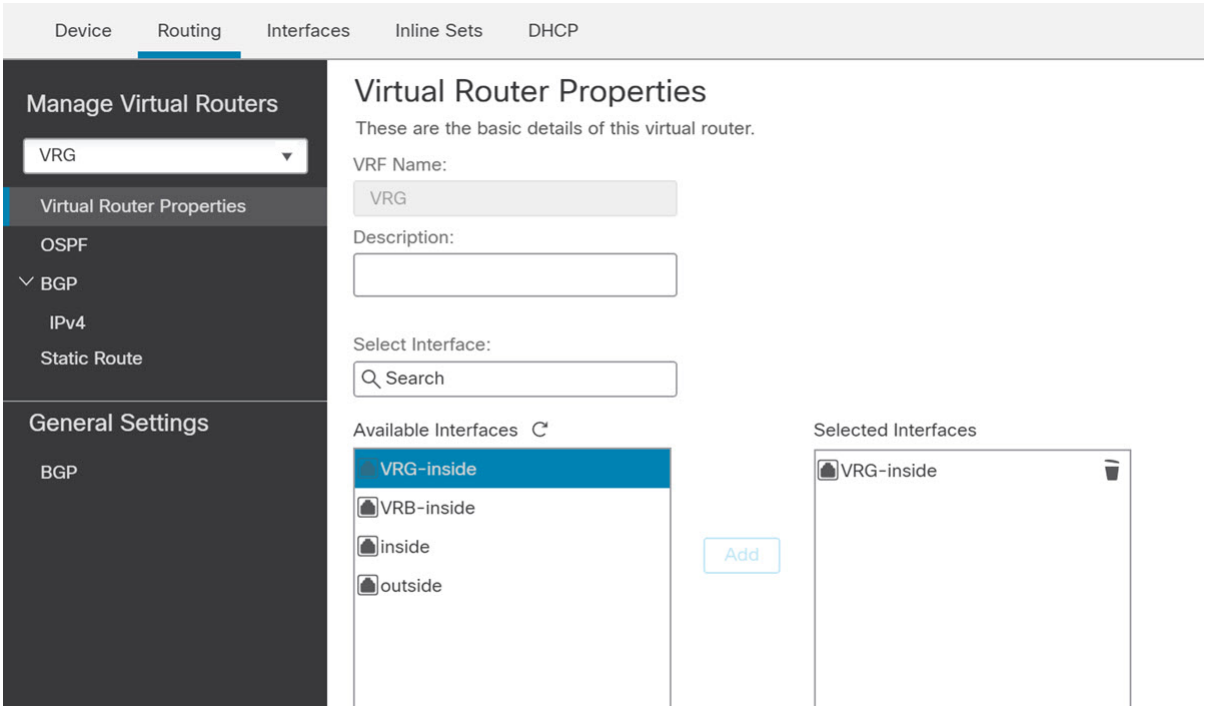
d) **Save(**저장**)**를 클릭합니다.

단계 **3** VRG 사용자가 공통 서버 172.16.10.1에 액세스할 수 있도록 전역 라우터의 내부 인터페이스에 대한 VRG 및 고정 기본 경로 유출을 구성합니다.

a) **Device(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스를 수정합니다.

b) **Routing(**라우팅**)** > **Manage Virtual Routers(**가상 라우터 관리**)**를 선택합니다. **Add Virtual Router(**가상 라우터 추가**)**를 클릭하고 VRG를 생성합니다.

c) VRG의 경우 **Virtual Router Properties(**가상 라우터 속성**)**에서 VRG-inside를 할당하고 저장합니다.




d) **Static Route(**정적 경로**)**를 클릭합니다.

e) **Add Route(**경로 추가**)**를 클릭합니다. **Add Static Route Configuration(**정적 경로 구성 추가**)**에서 다음을 지정합니다.

- **Interface(**인터페이스**)** - 전역 라우터의 내부 인터페이스를 선택합니다.
- **Networks(**네트워크**)** — any-ipv4 개체를 선택합니다.
- **Gateway(**게이트웨이**)** — 이 항목은 비워둡니다. 다른 가상 라우터로 라우트를 유출할 경우에는 게이트웨이를 선택하지 마십시오.

f) **Ok(**확인**)**를 클릭합니다.

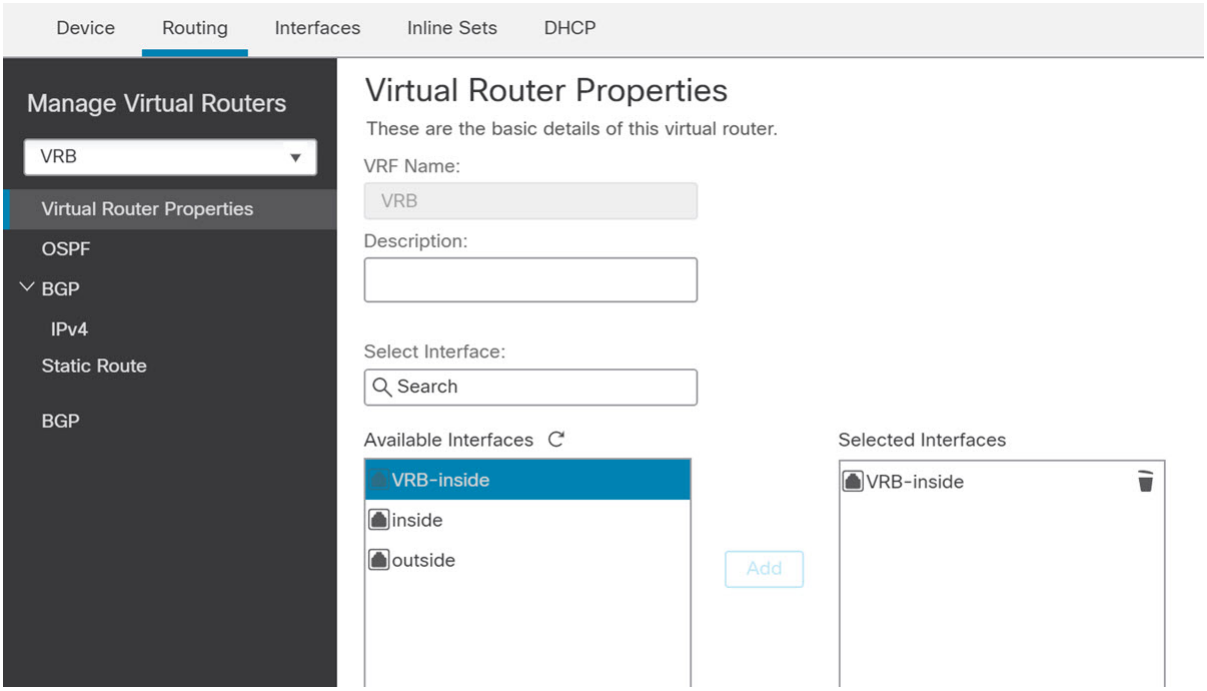
g) **Save(**저장**)**를 클릭합니다.

단계 **4** VRB 사용자가 공유 서버 172.16.10.x에 액세스할 수 있도록 전역 라우터의 내부 인터페이스에 대한 고정 기본 경로 유출을 구성합니다.

a) **Device(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스를 수정합니다.

b) **Routing(**라우팅**)** > **Manage Virtual Routers(**가상 라우터 관리**)**를 선택합니다. **Add Virtual Router(**가상 라우터 추가**)**를 클릭하고 VRB를 생성합니다.

c) VRB의 경우 **Virtual Router Properties(**가상 라우터 속성**)**에서 VRB-inside를 할당하고 저장합니다.




d) **Static Route(**정적 경로**)**를 클릭합니다.

e) **Add Route(**경로 추가**)**를 클릭합니다. **Add Static Route Configuration(**정적 경로 구성 추가**)**에서 다음을 지정합니다.

- **Interface(**인터페이스**)** - 전역 라우터의 내부 인터페이스를 선택합니다.
- **Networks(**네트워크**)** — any-ipv4 개체를 선택합니다.

- **Gateway(**게이트웨이**)** — 이 항목은 비워둡니다. 다른 가상 라우터로 라우트를 유출할 경우에는 게이트웨이를 선택하지 마십시오.

f) **Ok(**확인**)**를 클릭합니다.

g) **Save(**저장**)**를 클릭합니다.

단계 **5** VRB-inside 인터페이스 구성을 다시 확인합니다:

a) **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Interfaces(**인터페이스**)**를 선택합니다.

b) VRB-inside 인터페이스에 대해 **Edit(**편집**)**를 클릭합니다. IP 주소를 192.168.1.1/24로 지정합니다. 이제 시스템에서 VRG-inside의 동일한 IP 주소로 구성할 수 있습니다. 왜냐하면 인터페이스는 두 개의 서로 다른 가상 라우터에 별도로 할당되기 때문입니다.

c) **Ok(**확인**)**를 클릭합니다.

d) **Save(**저장**)**를 클릭합니다.

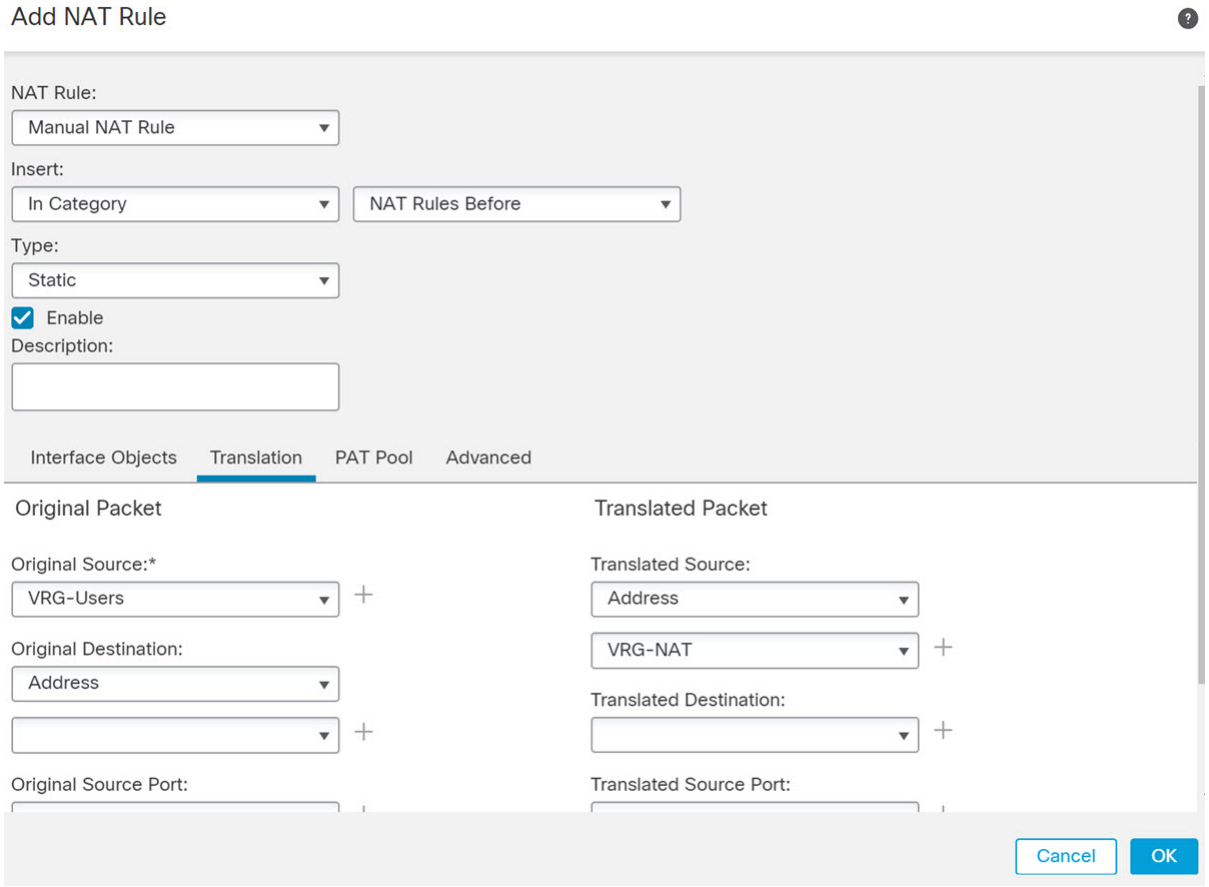
단계 **6** 소스 개체 VRG 및 VRB에 대한 NAT 규칙을 추가합니다. **Devices(**디바이스**)** > **NAT**를 클릭합니다.

단계 **7** **New Policy(**새 정책**)** > **Threat Defense NAT**를 클릭합니다.

단계 **8** NAT 정책 이름을 입력하고 FTD 디바이스를 선택합니다. **Save(**저장**)**를 클릭합니다.

단계 **9** NAT 페이지에서 **Add Rule(**규칙 추가**)**을 클릭하고 VRG에 대해 다음 소스 NAT를 정의합니다.

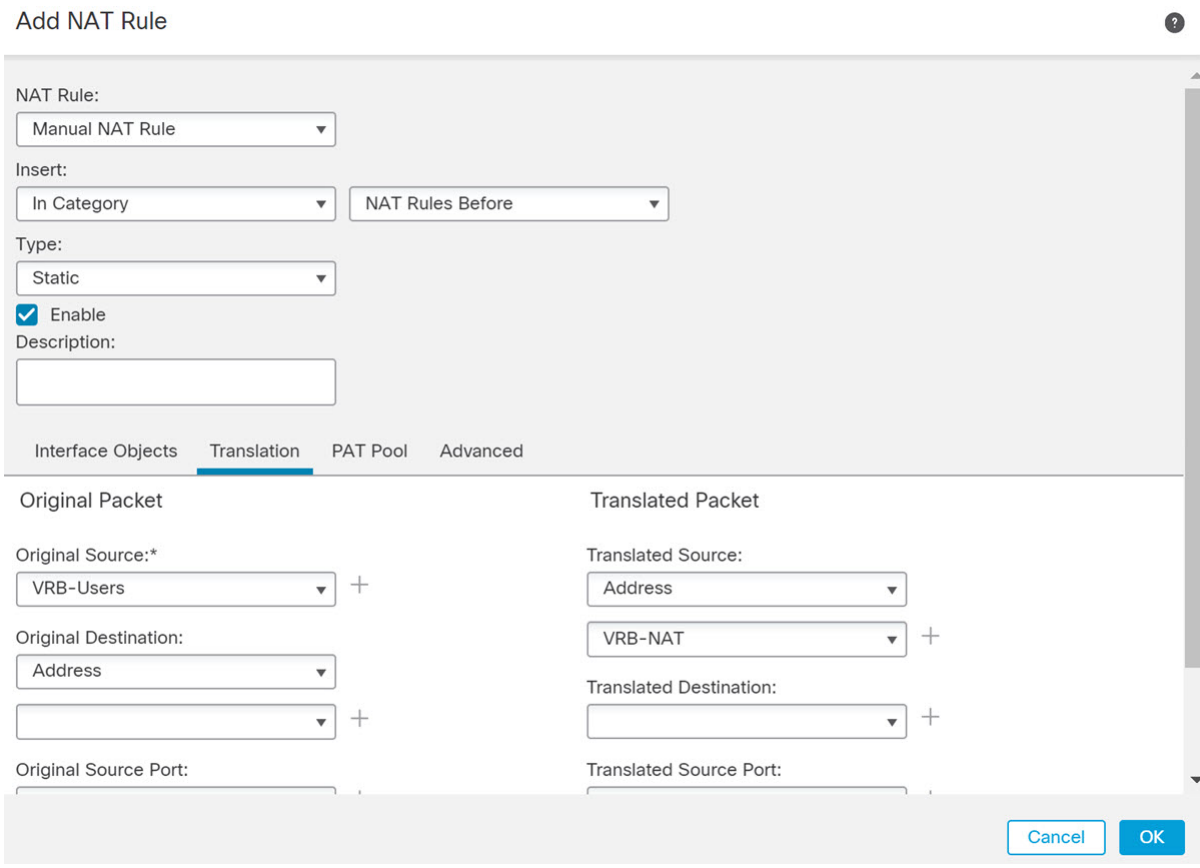
- **NAT Rule(NAT** 규칙**)** - Manual NAT Rule(수동 NAT 규칙)을 선택합니다.
- 유형 - Static(고정)을 선택합니다.
- **Insert (**삽입**)** - NAT 규칙이 있는 경우 Above(위에)를 선택합니다.
- **Enable(**활성화**)**을 클릭합니다.
- **Interface Objects(**인터페이스 개체**)**에서 VRG-Inside object(VRG-Inf 개체)를 선택하고 **Add to Source(**소스에 추가**)**를 클릭하고(개체를 사용할 수없는 경우, **Object(**개체**)** > **Object Management(**개체 관리**)** > **Interface(**인터페이스**)**에서 하나를 생성) Global-Inside object(VRB-Inf 개체)를 선택하고 **Add to Destination(**대상에 추가**)**을 클릭합니다.
- **Translation(**변환**)**에서 다음을 선택합니다.
  - **Original Source(**원본 소스**)**에서 VRG-Users를 선택합니다.
  - **Translated Source(**변환된 소스**)**에서 **Add(**추가**)**를 클릭하고 10.1.1.1로 개체 VRG-NAT를 정의합니다. 다음 그림과 같이 VRG-NAT를 선택합니다.




단계 **10** **Ok(**확인**)**를 클릭합니다.

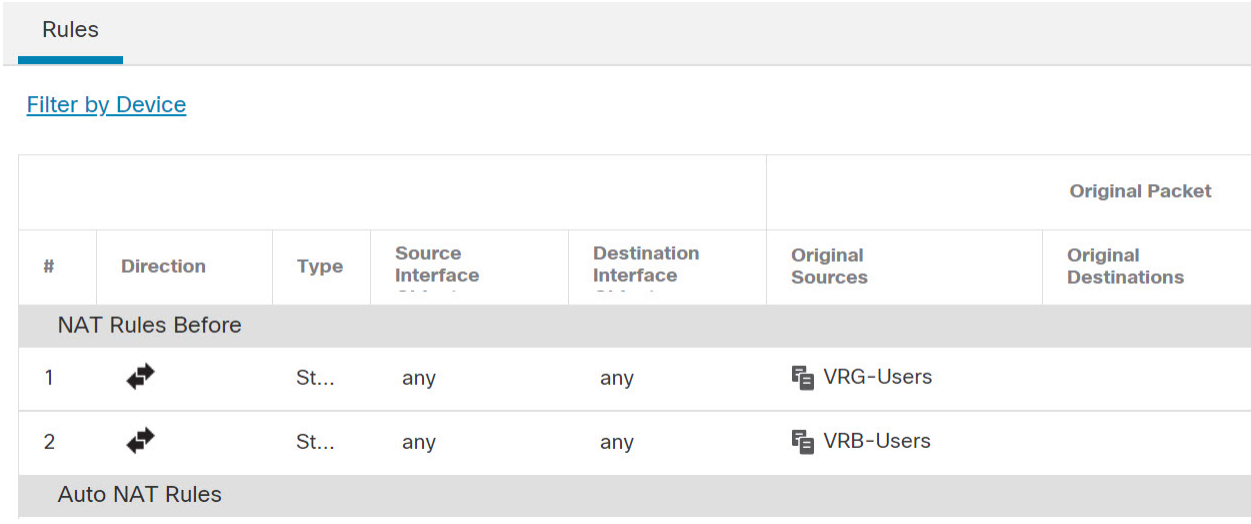
단계 **11** NAT 페이지에서 **Add Rule(**규칙 추가**)**을 클릭하고 VRB에 대해 다음 소스 NAT를 정의합니다.

- **NAT Rule(NAT** 규칙**)** - Manual NAT Rule(수동 NAT 규칙)을 선택합니다.
- 유형 - Static(고정)을 선택합니다.
- **Insert (**삽입**)** - NAT 규칙이 있는 경우 Above(위에)를 선택합니다.
- **Enable(**활성화**)**을 클릭합니다.
- **Interface Objects(**인터페이스 개체**)**에서 VRB-Inside object(VRB-Inside 개체)를 선택하고 **Add to Source(**소스에 추가**)**를 클릭하고(개체를 사용할 수없는 경우, **Object(**개체**)** > **Object Management(**개체 관리**)** > **Interface(**인터페이스**)**에서 하나를 생성) Global-Inside object(VRB-Inf 개체)를 선택하고 **Add to Destination(**대상에 추가**)**을 클릭합니다.
- **Translation(**변환**)**에서 다음을 선택합니다.
  - **Original Source(**원본 소스**)**에서 VRB-Users를 선택합니다.
  - **Translated Source(**변환된 소스**)**에서 **Add(**추가**)**를 클릭하고 20.1.1.1로 개체 VRB-NAT를 정의합니다. 다음 그림과 같이 VRB-NAT를 선택합니다.




단계 **12** **Save(**저장**)**를 클릭합니다.

NAT 규칙은 다음과 같습니다.




단계 **13** 각 VRG 및 VRB 사용자에 대해 FMC에 고유한 AD 서버 2개를 추가합니다. **System(**시스템**)** > **Integration(**통합**)** > **Realms(**영역**)**을 선택합니다.

단계 **14** **New Realm(**새 영역**)**을 클릭하고 필드를 완료합니다. 필드에 대한 자세한 내용은 영역 필드의 내용을 참조하십시오.

단계 **15** VRG 및 VRB 사용자의 액세스를 제어하려면 활성 디렉토리 2개를 정의합니다. 영역 디렉터리 및 동기화 필드 및 Active Directory 영역 및 영역 디렉터리 생성의 내용을 참조하십시오.

단계 **16** FMC에 ISE 추가—**System(**시스템**)** > **Integration(**통합**)** > **Identity Sources(ID** 소스**)**를 선택합니다.

단계 **17** **Identity Services Engine(ID** 서비스 엔진**)**을 클릭하고 필드를 완료합니다. 필드에 대한 자세한 내용은 영역을 사용해 사용자 제어에 대한 ISE/ISE-PIC를 설정하는 방법의 내용을 참조하십시오.

단계 **18** ID 정책 및 규칙을 생성한 다음 VRG 및 VRB에서 중복되는 사용자의 액세스를 제어하기 위한 액세스 제어 정책을 정의합니다.

# BGP를 사용하여 가상 라우터를 상호 연결하는 방법

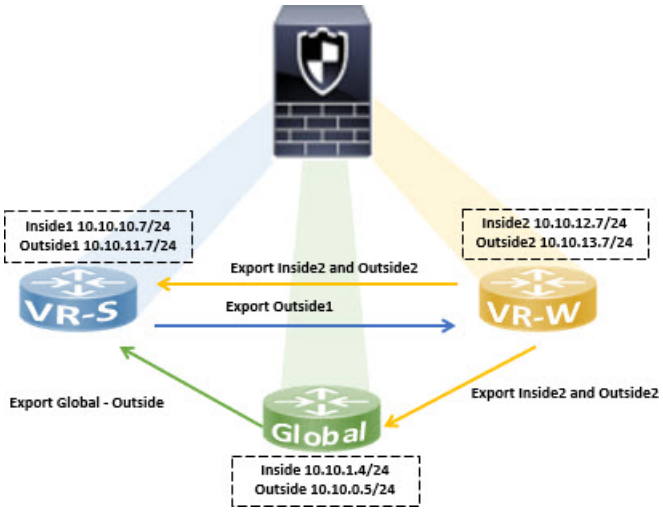
이제 가상 라우터(전역 및 사용자 정의 가상 라우터) 간에 경로를 유출하도록 디바이스에서 BGP 설정을 구성할 수 있습니다. 소스 가상 라우터의 경로 대상을 BGP 테이블로 내보내고, 이 테이블을 대상 가상 라우터로 가져옵니다. 경로 맵은 전역 가상 경로를 사용자 정의 가상 라우터와 공유하거나 그 반대로 공유하는 데 사용됩니다. BGP 테이블에 대한 경로의 모든 가져오기 또는 내보내기는 전역 가상 경로를 포함하여 사용자 정의 가상 라우터에서 구성됩니다.

공장의 방화벽 디바이스가 다음 가상 라우터 및 인터페이스로 구성되어 있다고 가정합니다.

- 전역 가상 라우터는 내부(10.10.1.4/24) 및 외부(10.10.0.5/24)로 구성됩니다.
- VR-S(영업) 가상 라우터는 Inside1(10.10.10.7/24) 및 Outside1(10.10.11.7/24)로 구성됩니다.
- VR-W(창고) 가상 라우터는 Inside2(10.10.12.7/24) 및 Outside2(10.10.13.7/24)로 구성됩니다.

창고(VR-W)의 경로를 영업(VR-S) 및 글로벌로 유출하고 VR-S의 외부 인터페이스 경로를 VR-W로 유출 하려는 경우를 가정해 보겠습니다. 마찬가지로, 전역 라우터의 외부 인터페이스 경로를 영업(VR-S)으로 유출하려고 합니다. 이 예에서는 라우터를 상호 연결 하기 위한 BGP 구성 절차를 보여줍니다.

그림 *2: BGP* 설정을 사용하여 가상 라우터 상호 연결




시작하기 전에

- 가상 라우터 생성.
- BGP를 활성화하고 각 가상 라우터에 대해 연결된 경로를 재배포할 수 있도록 BGP를 구성합니다.

프로시저

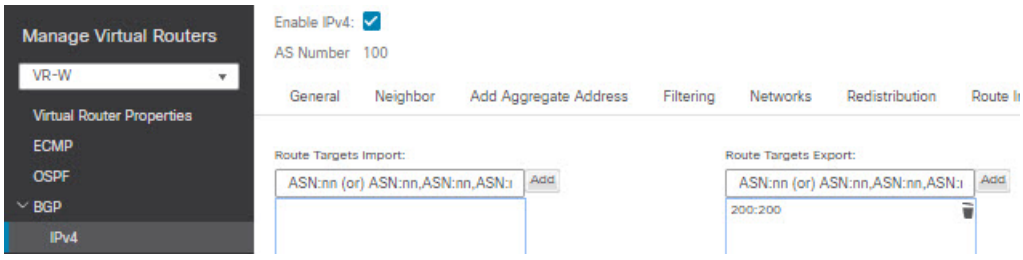
단계 **1** VR-W가 경로 대상으로 태그가 지정된 경로를 VR-S로 내보내도록 구성합니다.

a) **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 디바이스를 편집한 다음 **Routing(**라우팅**)** 탭을 클릭합니다.

b) 가상 라우터 드롭다운에서 VR-W를 선택합니다.

c) **BGP** > **IPv4** > **Route Import/Export(**경로 가져오기 내보내기**)**를 클릭합니다.

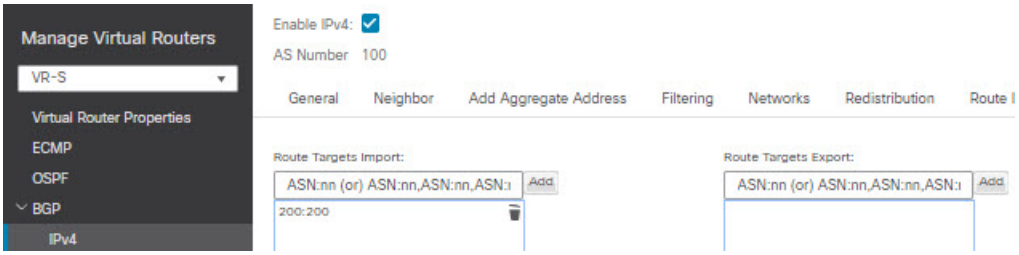
d) VR-W 경로를 VR-S로 유출하려면 경로 대상을 사용하여 경로에 태그를 지정하여 VR-W 경로를 경로 대상이 표시된 BGP 테이블로 내보내도록 합니다. **Route Targets Export(**경로 대상 내보내기**)** 필드에 *200:200*과 같은 값을 입력합니다. **Add(**추가**)**를 클릭합니다.




e) 가상 라우터 드롭다운에서 VR-S를 선택합니다.

f) **BGP** > **IPv4** > **Route Import/Export(**경로 가져오기 내보내기**)**를 클릭합니다.

g) VR-W에서 유출된 경로를 수신하려면 (피어 또는 재배포된) BGP 테이블의 경로 대상으로 표시된 VR-W 경로를 가져오도록 Import Route Target (경로 대상 가져오기)을 구성합니다. **Route Targets Import(**경로 대상 가져오기**)** 필드에 VR-W, *200:200*에 대해 구성한 것과 동일한 경로 대상 값을 입력합니다. **Add(**추가**)**를 클릭합니다.



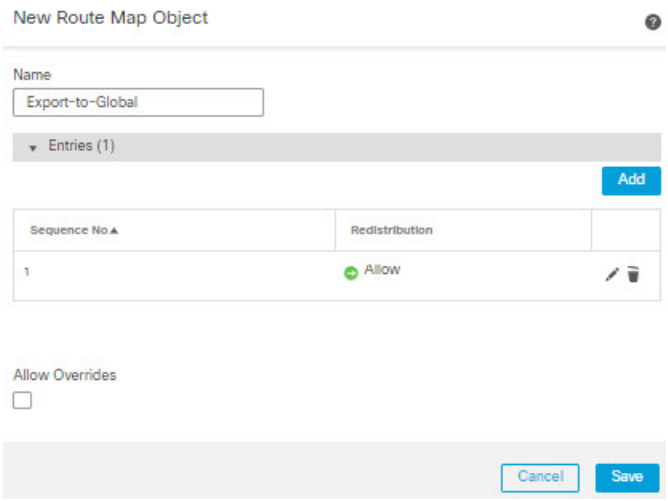

참고 VR-W에서 경로를 유출하도록 조건을 설정하려면 경로 맵 개체에서 일치 기준을 지정하고 **User Virtual Router Export Route Map(**사용자 가상 라우터 내보내기 경로 맵**)**에서 이를 선택할 수 있습니다. 마찬가지로, BGP 테이블에서 VR-S로 가져올 경로를 조건화하려는 경우 **User Virtual Router Import Route Map(**사용자 가상 라우터 가져오기 경로 맵**)**을 사용할 수 있습니다. 이 절차는 3단계에서 설명합니다.

단계 **2** 전역 가상 라우터로 경로를 내보내도록 VR-W를 구성합니다.

a) VR-W 경로를 전역 라우팅 테이블로 내보낼 수 있는 경로 맵을 생성해야 합니다. **Objects(**개체**)** > **Object Management(**개체 관리**)** > **Route Map(**경로 맵**)**을 선택합니다.

b) **Add Route Map(**경로 맵 추가**)**을 클릭하고 이름을 지정한 다음 *Export-to-Global(*글로벌로 내보내기*)*을 지정한 다음 **Add(**추가**)**를 클릭합니다.

c) **Sequence Number(**시퀀스 번호**)**(예: 1)를 지정하고 **Redistribution(**재배포**)** 드롭다운 목록에서 Allow(허용)를 선택합니다.

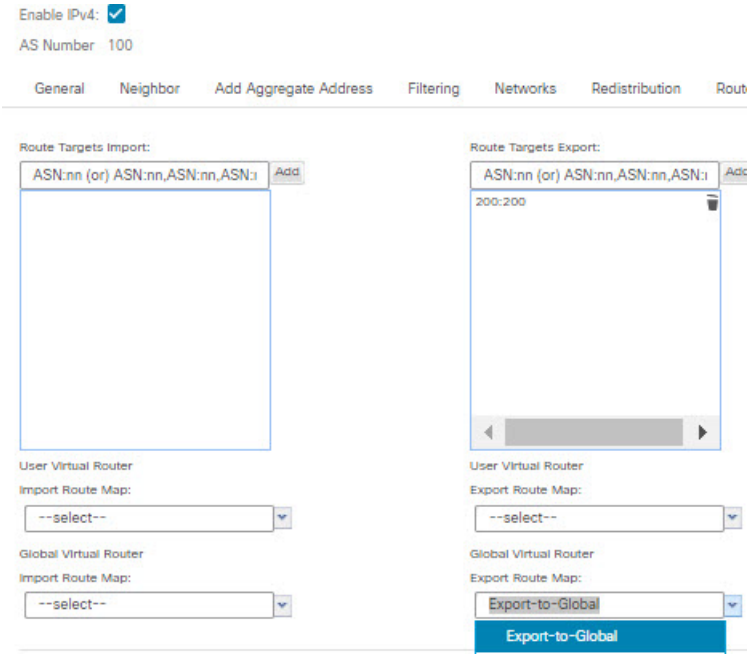



d) **Save(**저장**)**를 클릭합니다.

이 예에서는 모든 VR-W 경로가 전역 라우팅 테이블로 유출됩니다. 따라서 경로 맵에 대해 일치 기준이 구성되지 않습니다.

e) 디바이스의 **Routing(**라우팅**)** 탭으로 이동하여 VR-W를 선택합니다. **BGP** > **IPv4** > **Route Import/Export(BGP IPv4** 경로 가져오기/내보내기**)**를 클릭합니다.

f) **Global Virtual Router Export Route Map(**전역 가상 라우터 내보내기 경로 맵**)** 드롭다운 목록에서 Export-to-Global(전역으로 내보내기)을 선택합니다.




단계 **3** VR-S의 Outside1 경로만 VR-W로 유출하려면 다음을 수행합니다.

a) 가상 라우터 드롭다운에서 VR-S를 선택합니다.

b) **BGP** > **IPv4** > **Route Import/Export(**경로 가져오기 내보내기**)**를 클릭합니다.

c) VR-S 경로를 VR-W로 유출하려면 경로 대상을 사용하여 경로에 태그를 지정하여 VR-S 경로를 경로 대상이 표시된 BGP 테이블로 내보내도록 합니다. **Route Targets Export(**경로 대상 내보내기**)** 필드에 *100:100*과 같은 값을 입력합니다. **Add(**추가**)**를 클릭합니다.

d) 가상 라우터 드롭다운에서 VR-W를 선택하고 **BGP** > **IPv4** > **Route Import/Export(BGP IPv4** 경로 가져오기/내보내기**)**를 선택합니다.

e) VR-S에서 유출된 경로를 수신하려면 (피어 또는 재배포된) BGP 테이블의 경로 대상으로 표시된 VR-S 경로를 가져오도록 Import Route Target (경로 대상 가져오기)을 구성합니다. **Route Targets Import(**경로 대상 가져오기**)** 필드에 VR-S 경로 대상 값 *100:100*을 입력합니다. **Add(**추가**)**를 클릭합니다.

f) 이제 VR-S의 Outside1 경로만 VR-W로 유출되도록 조건을 설정해야 합니다. **Objects(**개체**)** > **Object Management(**개체 관리**)** > **Prefix List(**접두사 목록**)** > **IPv4 Prefix List(IPv4** 접두사 목록**)**를 선택합니다.

g) **Add IPv4 Prefix List(IPv4** 접두사 목록 추가**)**를 클릭하고 이름을 *VRS-Outside1-Only*로 지정한 후 **Add(**추가**)**를 클릭합니다.

h) **Sequence Number(**시퀀스 번호**)**(예: 1)를 지정하고 **Redistribution(**재배포**)** 드롭다운 목록에서 Allow(허용)를 선택합니다.

i) VR-S Outside1 인터페이스의 IP 주소(처음 2개의 옥텟)를 입력합니다.

j) **Save(**저장**)**를 클릭합니다.

k) 접두사 목록이 있는 match 절을 사용하여 경로 맵을 생성합니다. **Route Map(**경로 맵**)**을 클릭합니다. **Add Route Map(**경로 맵 추가**)**을 클릭하고 *Import-from-VRS*라는 이름을 지정한 다음 **Add(**추가**)**를 클릭합니다.

l) **Sequence Number(**시퀀스 번호**)**(예: 1)를 지정하고 **Redistribution(**재배포**)** 드롭다운 목록에서 Allow(허용)를 선택합니다.

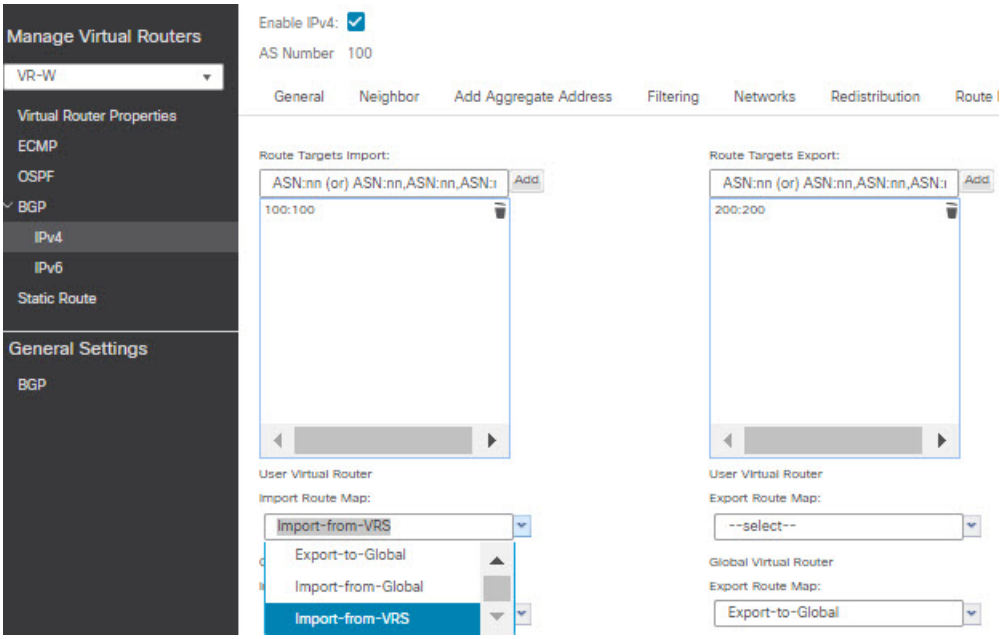
m) **Match Clause(**일치 절**)** 탭에서 **IPv4**를 클릭합니다. **Address(**주소**)** 탭에서 **Prefix List(**접두사 목록**)**를 클릭합니다.

n) **Available IPv4 Prefix List(**사용 가능한 **IPv4** 접두사 목록**)**에서 VRS-Outside1-Only를 선택하고 **Add(**추가**)**를 클릭합니다.

o) **Save(**저장**)**를 클릭합니다.

p) 디바이스의 **Routing(**라우팅**)** 탭으로 이동하여 VR-W를 선택합니다. **BGP** > **IPv4** > **Route Import/Export(BGP IPv4** 경로 가져오기/내보내기**)**를 클릭합니다.

q) **Global Virtual Router Import Route Map(**전역 가상 라우터 경로 맵 가져오기**)** 드롭다운 목록에서 Import-from-VRS를 선택합니다.




단계 **4** 전역 가상 라우터의 외부 경로를 가져오도록 VR-S를 구성합니다.

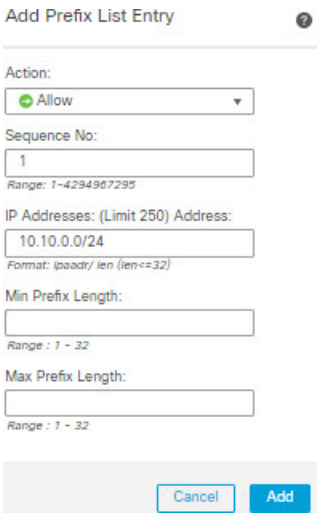
참고 전역 가상 라우터에서 경로를 유출하려면 소스 또는 대상 사용자 정의 가상 라우터를 각각 구성해야 합니다. 따라서 이 예에서 VR-S는 전역 가상 라우터의 외부 인터페이스에서 경로를 가져오는 대상 라우터입니다.

a) **Objects(**개체**)** > **Object Management(**개체 관리**)** > **Prefix List(**접두사 목록**)** > **IPv4 Prefix List(IPv4** 접두사 목록**)**를 선택합니다.

b) **Add IPv4 Prefix List(IPv4** 접두사 목록 추가**)**를 클릭하고 이름을 *Global-Outside-Only*로 지정한 다음 **Add(**추가**)**를 클릭합니다.

c) **Sequence Number(**시퀀스 번호**)**(예: 1)를 지정하고 **Redistribution(**재배포**)** 드롭다운 목록에서 Allow(허용)를 선택합니다.

d) Global Outside 인터페이스의 IP 주소(처음 두 옥텟)를 입력합니다.



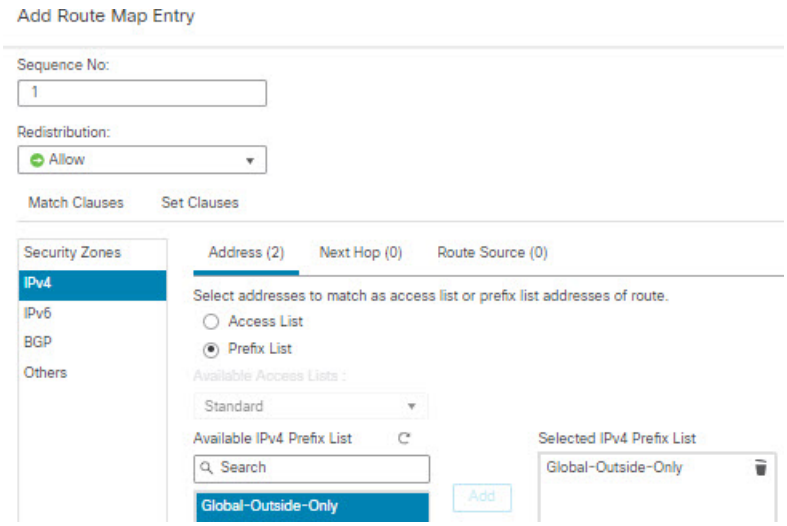

e) **Save(**저장**)**를 클릭합니다.

f) **Route Map(**경로 맵**)**을 클릭합니다. **Add Route Map(**경로 맵 추가**)**을 클릭하고 이름을 *Import-from-Global*로 지정한 다음 **Add(**추가**)**를 클릭합니다.

g) **Sequence Number(**시퀀스 번호**)**(예: 1)를 지정하고 **Redistribution(**재배포**)** 드롭다운 목록에서 Allow(허용)를 선택합니다.

h) **Match Clause(**일치 절**)** 탭에서 **IPv4**를 클릭합니다. **Address(**주소**)** 탭에서 **Prefix List(**접두사 목록**)**를 클릭합니다.

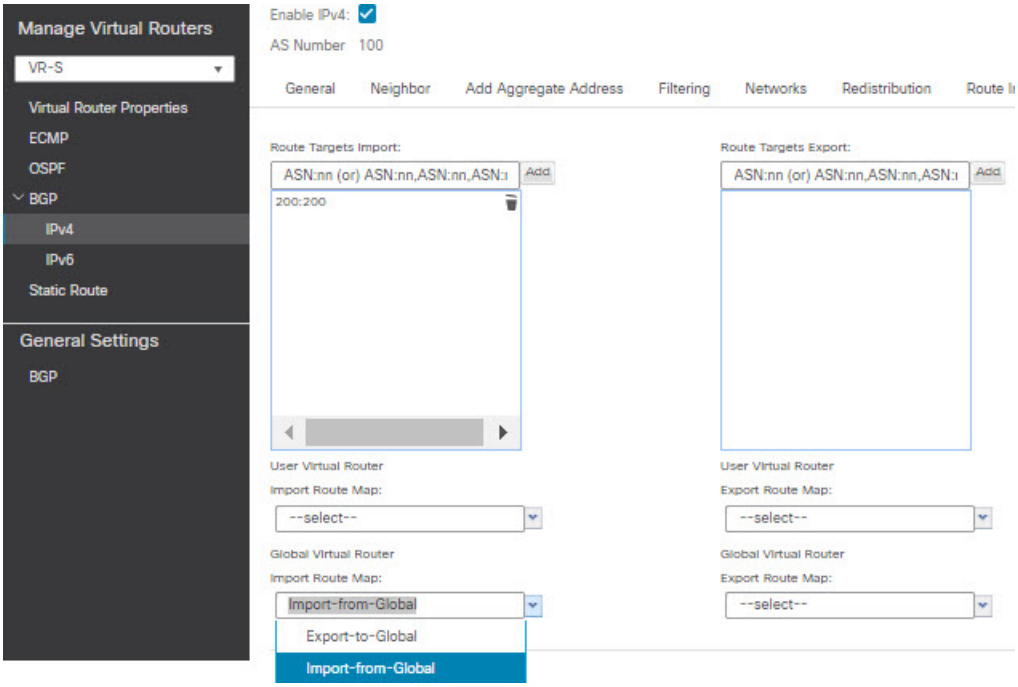
i) **Available IPv4 Prefix List(**사용 가능한 **IPv4** 접두사 목록**)** 아래에서 Global-Outside-Only를 선택하고 **Add(**추가**)**를 클릭합니다.




j) **Save(**저장**)**를 클릭합니다.

k) 디바이스의 **Routing(**라우팅**)** 탭으로 이동하여 VR-S를 선택합니다. **BGP** > **IPv4** > **Route Import/Export(BGP IPv4** 경로 가져오기/내보내기**)**를 클릭합니다.

l) **Global Virtual Router Import Route Map(**전역 가상 라우터 경로 맵 가져오기**)** 드롭다운 목록에서 Import-from-Global을 선택합니다.




단계 **5** **Save(**저장**)**하고 **Deploy(**구축**)**합니다.

# 가상 라우터 기록

| 기능 | 버전 | 세부 사항 |
|---|---|---|
| ISA 3000에 대한 가상 라우터 지원 | 7.0 | ISA 3000 디바이스에서 최대 10개의 가상 라우터를 설정할 수 있습니다.<br>신규/수정된 화면: 없음 |
| Snort 3 지원 디바이스용 가상 라우터 | 7.0 | Snort3 지원 디바이스는 이제 가상 라우터 기능을 지원합니다. 따라서 Snort3 엔진으로 전환하기 전에 가상 라우터에서 Snort 2 디바이스를 제거할 필요가 없습니다.<br>신규/수정된 화면: 없음 |
| 사용자 정의 가상 라우터에서 SNMP 지원 | 7.0 | Secure Firewall Threat Defense에서는 이제 사용자 정의 가상 라우터에서 SNMP 구성을 지원합니다.<br>신규/수정된 화면: 없음 |

| 기능 | 버전 | 세부 사항 |
| --- | --- | --- |
| 가상 라우터 대량 제거 | 6.7 | Secure Firewall Threat Defense에서 한 번에 여러 가상 라우터를 제거할 수 있습니다.<br>신규/수정된 화면: **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Routing(**라우팅**)** > **Manage Virtual Routers(**가상 라우터 관리**)** 페이지. |
| Secure Firewall Threat Defense의 가상 라우터 | 6.6 | Secure Firewall Threat Defense의 가상 라우터가 도입되었습니다.<br>신규/수정된 화면: **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Routing(**라우팅**)** 페이지에서 가상 라우터를 생성하고 Threat Defense 인터페이스를 가상 라우터에 할당할 수 있습니다.<br>지원되는 플랫폼: Secure Firewall Threat Defense |