가상 라우터

가상 라우터를 생성하여 인터페이스 하위 집합의 트래픽을 서로 분리할 수 있습니다.

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 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.

NAT 등의 보안 영역을 사용하지 않는 정책의 경우에는 단일 가상 라우터에 할당된 인터페이스를 소스 및 대상 인터페이스로 선택하여 가상 라우터에 해당하는 규칙을 작성할 수 있습니다. 별도의 두 가상 라우터에서 소스 및 대상 인터페이스를 선택하는 경우, 해당 규칙이 작동하도록 가상 라우터 간에 적절한 경로가 있는지 확인해야 합니다.

가상 라우터 간 라우팅

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 인터

페이스에 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.

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	가상 라우터는 이 모델에서 지원되지 않습니다.
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

디바이스 모델	최대 가상 라우터 수
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

가상 라우터 지침

디바이스 모델 지침

다음을 제외하고 모든 지원 디바이스 모델에서 가상 라우터를 구성할 수 있습니다.

- Firepower 1010
- ISA 3000

추가 지침

- 글로벌 가상 라우터에서만 다음 기능을 구성할 수 있습니다.
  - OSPFv3
  - RIP
  - EIGRP
  - IS-IS
  - BGPv6
  - 멀티캐스트 라우팅
  - 정책 기반 라우팅
  - VPN

- 각 가상 라우터에 대해 다음 기능을 개별적으로 구성할 수 있습니다.
  - 고정 경로 및 해당 SLA 모니터
  - OSPFv2
  - BGPv4
- 다음 기능은 원격 시스템을 통해 쿼리하거나 통신할 때 시스템에서 사용됩니다(from-the-box 트래픽). 이러한 기능에서는 글로벌 가상 라우터의 인터페이스만 사용합니다. 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 있으므로, VPN에 사용되는 외부 AAA 서버(예: Active Directory)는 글로벌 가상 라우터의 인터페이스를 통해 연결할 수 있어야 합니다.
  - Syslog 서버.
  - SNMP.
- NAT에서 다른 가상 라우터에 할당된 소스 및 대상 인터페이스를 지정하는 경우 NAT 규칙에서는 다른 가상 라우터를 통해 하나의 가상 라우터에서 트래픽을 전환합니다. NAT 규칙에서 인터페이스를 실수로 혼합하지 않았는지 확인합니다. 일반적으로 소스 및 대상 인터페이스가 사용되며 수동 NAT의 대상 변환에 대한 라우팅 테이블을 포함하여 해당 라우팅 테이블이 무시됩니다. 그러나 NAT 규칙에서 경로 조회를 수행해야 하는 경우에는 인바운드 인터페이스에 대해서만 VRF 테이블에서 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. 가상 라우터를 사용할 경우 NAT 규칙을 신중하게 테스트하여 정상적인 동작이 나오는지 확인하십시오. 필요한 경로 유출을 정의하는 것을 잊은 경우, 어떤 경우에는 해당 규칙은 일치하는 것으로 예상되는 모든 트래픽과 일치하지 않을 수 있으며 변환이 적용되지 않습니다.
- 가상 라우터 간 경로를 구성할 경우(예: 한 가상 라우터에서 두 번째 가상 라우터로 경로를 유출하는 경우), 시스템에서는 소스 가상 라우터에서 대상 인터페이스 조회를 수행합니다. 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.
- 예를 들어 가상 라우터 1에서 가상 라우터 2로의 가상 라우터 간 경로(누출된 경로)를 사용하는 경우 반환 트래픽을 허용하기 위해 가상 라우터 2에서 미러(역방향) 경로를 설정할 필요가 없습니다. 하지만 연결이 양방향에서 시작되도록 하려면 가상 라우터 1에서 2로, 그리고 가상 라우터 2에서 1로, 양방향으로 경로를 누출해야 합니다.

- 한 가상 라우터에서 다른 가상 라우터로 인터페이스를 이동할 경우, 해당 인터페이스에 대해 구성된 모든 기능이 유지됩니다. 컨피그레이션을 검토하여 새 가상 라우터의 컨텍스트 내에서 정적 경로, IP 주소, 기타 정책이 적합한지 확인합니다.
- 여러 가상 라우터에서 중복 어드레스 스페이스를 사용하는 경우 Cisco ISE(Identity Services Engine)에서 다운로드한 IP 주소 매핑에 대한 고정 SGT(보안 그룹 태그)에서 가상 라우터를 인식하지 않는다는 점에 유의하십시오. 가상 라우터마다 서로 다른 SGT 매핑을 생성해야 하는 경우 가상 라우터마다 별도의 ID 영역을 설정합니다. 각 가상 라우터에서 동일한 SGT 번호에 동일한 IP 주소를 매핑하려는 경우에는 이 작업이 필요하지 않습니다.
- 여러 가상 라우터에서 중복 어드레스 스페이스를 사용하는 경우 대시보드 데이터가 잘못될 수 있습니다. 동일한 IP 주소에 대한 연결이 집계되므로, 두 개 이상의 엔드포인트에서 공유되는 경우 특정 주소로 오고가는 트래픽이 더 많았던 것으로 표시됩니다. 별도의 ID 영역을 사용하여 ID 정책을 신중하게 구성하는 경우에는 사용자 기반 통계가 더 정확해야 합니다.
- 별도의 가상 라우터에서는 중복 DHCP 주소 풀을 사용할 수 없습니다.
- 전역 가상 라우터의 인터페이스에서만 DHCP 서버 자동 컨피그레이션을 사용할 수 있습니다. 자동 컨피그레이션은 사용자 정의 가상 라우터에 할당된 인터페이스에 대해 지원되지 않습니다.
- 전역 가상 라우터에서 새 라우터로 이동하는 등 인터페이스를 한 가상 라우터에서 다른 가상 라우터로 이동할 경우, 인터페이스를 통한 모든 기존 연결이 삭제됩니다.
- 보안 인텔리전스 정책에서는 가상 라우터를 인식하지 않습니다. IP 주소, URL 또는 DNS 이름을 차단 목록에 추가하면 해당 항목이 모든 가상 라우터에 대해 차단됩니다.

가상 라우터 관리

가상 라우터라고 하는 여러 VRF(가상 라우팅 및 포워딩) 인스턴스를 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.

기본적으로 가상 라우팅은 비활성화되어 있습니다. 전체 디바이스에서는 데이터(통과) 및 관리(to/from the box) 트래픽용으로 글로벌 라우팅 테이블의 단일 집합을 사용합니다.

가상 라우팅을 활성화할 경우 초기 라우팅 페이지는 시스템에 정의된 가상 라우터의 목록입니다. 가상 라우터를 활성화하지 않을 경우 초기 라우팅 페이지는 시스템에 정의된 고정 경로의 목록입니다.

글로벌 가상 라우터는 항상 있습니다. 글로벌 라우터에서는 개별 가상 라우터에 할당되지 않은 모든 인터페이스를 보유합니다.

프로시저

단계 **1** 디바이스를 클릭한 다음, **Routing(**라우팅**)** 요약의 링크를 클릭합니다.

단계 **2** 가상 라우터를 아직 활성화하지 않은 경우 **Add Multiple Virtual Routers(**여러 가상 라우터 추가**)** 링크를 클릭한 다음, **Create First Custom Virtual Router(**첫 번째 맞춤형 가상 라우터 생성**)**를 클릭합니다.

첫 번째 가상 라우터를 생성하는 것은 기본적으로 추가 가상 라우터를 생성하는 것과 동일합니다. 자세한 내용은 가상 라우터 생성 또는 인터페이스 할당 수정, 7 페이지의 내용을 참고하십시오.

단계 **3** 다음 중 하나를 수행합니다.

- 모든 가상 라우터에 적용되는 글로벌 BGP 설정을 구성하려면 **BGP Global Settings(BGP** 글로벌 설정**)** 버튼을 클릭합니다. Smart CLI를 사용하여 이러한 설정을 구성합니다. 이 내용은 스마트 CLI 개체 구성에 설명되어 있습니다. 하나 이상의 가상 라우터에서 BGP를 구성하는 경우에만 글로벌 BGP 설정을 구성합니다.
- 새 가상 라우터를 생성하려면 테이블 위의 + 버튼을 클릭합니다.
- 가상 라우터의 라우팅 속성을 수정하려면, 예를 들어, 고정 경로를 생성하거나 라우팅 프로세스를 정의하려면 가상 라우터의 Action(작업) 셀에서 보기 아이콘( )을 클릭합니다.
- 가상 라우터의 이름, 설명 또는 인터페이스 할당을 수정하려면 가상 라우터의 Action(작업) 셀에서 보기 아이콘( )을 클릭한 다음, **Virtual Router Properties(**가상 라우터 속성**)** 탭을 선택합니다.
- 해당 내용을 볼 때 가상 라우터 간에 전환하려면, 가상 라우터 이름 옆의 아래쪽 화살표(라우팅 테이블 위)를 클릭하고 원하는 가상 라우터를 선택합니다. **Go Back to Virtual Routers(**가상 라우터로 돌아가기**)** 화살표( )를 클릭하여 목록 페이지로 돌아갈 수 있습니다.
- 가상 라우터를 삭제하려면 가상 라우터의 Action(작업) 셀에서 삭제 아이콘( )을 클릭하거나 가상 라우터의 콘텐츠를 볼 때 가상 라우터 이름 옆의 삭제 아이콘을 클릭합니다. 마지막 가상 라우터(글로벌 라우터 외에는 삭제할 수 없음)를 삭제하면 VRF가 비활성화됩니다.
- 가상 라우터에서 라우팅을 모니터링하려면 해당 가상 라우터의 테이블에서 **show** 명령 중 하나에 대한 링크를 클릭합니다. 명령을 클릭하면 CLI 콘솔이 열려 CLI 명령의 출력을 검사할 수 있습니다. 경로, OSPF 및 OSPF 네이버에 대한 정보를 표시할 수 있습니다. 명령 출력은 구축된 구성을 기반으로 합니다. 구축되지 않은 수정 작업과 관련된 내용은 표시되지 않습니다.

  가상 라우터를 볼 때 **Commands(**명령**)** 드롭다운 목록에서 해당 명령을 선택하여 이러한 명령을 실행할 수도 있습니다.

가상 라우터 생성 또는 인터페이스 할당 수정

가상 라우터에서 고정 경로 또는 라우팅 프로세스를 구성하려면 먼저 라우터를 생성하고 인터페이스를 할당해야 합니다.

시작하기 전에

Interface(인터페이스**)** 페이지로 이동하여 가상 라우터에 추가하려는 각 인터페이스에 이름이 있는지 확인합니다. 이름이 있는 경우에만 가상 라우터에 인터페이스를 추가할 수 있습니다.

프로시저

단계 **1** **Device(**디바이스**)** > **Routing(**라우팅**)**을 클릭합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 가상 라우터를 아직 생성하지 않은 경우 **Add Multiple Virtual Routers(**여러 가상 라우터 추가**)** 링크를 클릭한 다음, **Create First Custom Virtual Router(**첫 번째 맞춤형 가상 라우터 생성**)**를 클릭합니다.
- 새 가상 라우터를 하나 생성하려면 가상 라우터 목록 위의 **+** 버튼을 클릭합니다.
- 가상 라우터의 수정 아이콘( )을 클릭하여 해당 속성 및 인터페이스 목록을 수정합니다.
- 가상 라우터를 볼 때 **Virtual Router Properties(**가상 라우터 속성**)** 탭을 클릭하여 보고 있는 가상 라우터의 속성을 수정합니다.
- 가상 라우터를 볼 때 가상 라우터 이름 옆의 아래쪽 화살표를 클릭하고 **Create New Virtual Router(**새 가상 라우터 생성**)**를 클릭합니다.

단계 **3** 다음과 같이 가상 라우터의 속성을 구성합니다.

- **Name(**이름**)** - 가상 라우터의 이름입니다.
- **Description(**설명**)** - 가상 라우터의 설명(선택 사항)입니다.
- **Interfaces(**인터페이스**)** - **+**를 클릭하여 가상 라우터에 포함되어야 하는 각 인터페이스를 선택합니다. 인터페이스를 제거하려면 인터페이스 위에 마우스 커서를 올려 놓고 인터페이스 카드의 오른쪽에 있는 **X**를 클릭합니다. 물리적 인터페이스, 하위 인터페이스, 브리지 그룹, EtherChannel은 가상 라우터에 할당할 수 있지만 VLAN은 할당할 수 없습니다.

  다른 인터페이스에 대한 경로를 가상 라우팅 테이블로 의도적으로 유출하지 않는 한, 라우팅 테이블은 이러한 인터페이스로 제한됩니다.

  진단(Management X/Y) 인터페이스를 전역 가상 라우터에만 할당할 수 있습니다.

단계 **4** **OK(**확인**)** 또는 **Save(**저장**)**를 클릭합니다.

고정 경로 또는 라우팅 프로세스를 구성할 수 있는 이 가상 라우터의 보기로 이동하게 됩니다.

가상 라우터에서 고정 경로 및 라우팅 프로세스 구성

각 가상 라우터에는 자체 정적 경로 및 라우팅 프로세스가 있습니다. 이 둘은 다른 가상 라우터에 대해 정의된 경로 및 라우팅 프로세스와 별개로 작동합니다.

고정 경로를 구성할 때 가상 라우터 외부에 있는 대상 인터페이스를 선택할 수 있습니다. 그러면 대상 인터페이스가 포함된 가상 라우터로 경로가 유출됩니다. 더 많은 트래픽을 다른 가상 라우터로 전송하지 않도록 하려면 유출해야 하는 경로만 유출해야 합니다. 예를 들어 인터넷에 대한 경로가 하나 있는 경우, 인터넷으로 향하는 트래픽에 대해 각 가상 라우터에서 인터넷 연결 가상 라우터로 경로가 유출되어야 합니다.

프로시저

단계 **1** **Device(**디바이스**)** > **Routing(**라우팅**)**을 선택합니다.

단계 **2** 가상 라우터의 Action(작업) 셀에서 보기 아이콘( )을 클릭하여 엽니다.

단계 **3** 다음 중 하나를 수행합니다.

- 고정 경로를 구성하려면 **Static Routing(**고정 라우팅**)** 탭을 클릭한 다음, 경로를 생성하거나 수정합니다. 자세한 내용은 고정 경로 구성를 참조하십시오.
- BGP 라우팅 프로세스를 구성하려면 **BGP** 탭을 클릭한 다음, 프로세스를 정의하는 데 필요한 Smart CLI 개체를 생성합니다. 자세한 내용은 BGP(Border Gateway Protocol)를 참조하십시오.

  또한 모든 가상 라우터에 적용되는 BGP에 대한 글로벌 설정도 있습니다. 이러한 속성을 구성하려면 가상 라우터 목록 페이지로 돌아가서 **BGP Global Settings(BGP** 글로벌 설정**)** 버튼을 클릭해야 합니다.
- OSPF 라우팅 프로세스를 구성하려면 **OSPF** 탭을 클릭한 다음, 최대 2개의 프로세스를 정의하는 데 필요한 Smart CLI 개체 및 그와 연관된 인터페이스 구성을 생성합니다. 자세한 내용은 OSPF(Open Shortest Path First)를 참조하십시오.
- (전역 가상 라우터 전용) EIGRP 라우팅 프로세스를 구성하려면 **EIGRP** 탭을 클릭한 다음, 단일 프로세스를 정의하는 데 필요한 스마트 CLI 개체를 생성합니다. 자세한 내용은 EIGRP(Enhanced Interior Gateway Routing Protocol)를 참조하십시오.

가상 라우터 삭제

가상 라우터가 더 이상 필요하지 않은 경우에는 삭제할 수 있습니다. 글로벌 가상 라우터는 삭제할 수 없습니다.

가상 라우터를 삭제하면 가상 라우터 내에 구성된 모든 고정 경로 및 라우팅 프로세스도 삭제됩니다.

가상 라우터에 할당된 모든 인터페이스는 글로벌 라우터에 다시 할당됩니다.

프로시저

단계 **1** **Device(**디바이스**)** > **Routing(**라우팅**)**을 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 가상 라우터 목록에서 가상 라우터의 Action(작업) 열에 있는 삭제 아이콘()을 클릭합니다.
- 삭제할 가상 라우터를 볼 때 라우터 이름 옆의 삭제 아이콘()을 클릭합니다.

가상 라우터를 삭제할 것인지 확인해 달라는 메시지가 표시됩니다.

단계 **3** **OK(**확인**)**를 클릭하여 삭제를 확인합니다.

가상 라우터의 예시

다음 주제에서는 가상 라우터 구현에 대한 예시를 제공합니다.

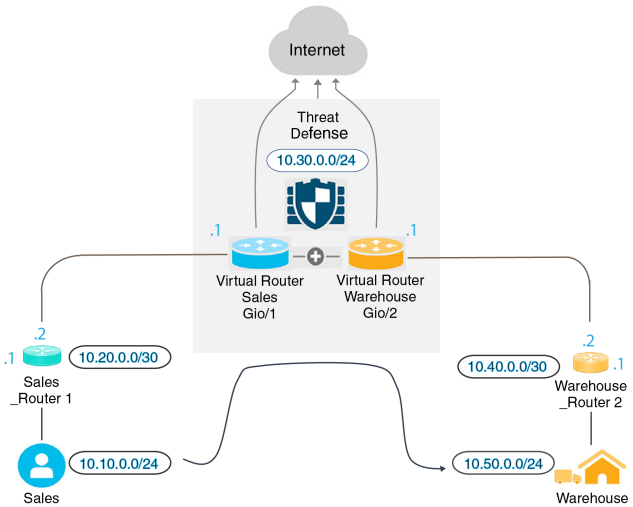
관련 항목

사이트 간 VPN을 통해 여러 가상 라우터의 네트워크에서 트래픽을 보호하는 방법
RA VPN 액세스를 다른 가상 라우터의 내부 네트워크에 허용하는 방법

여러 가상 라우터를 통해 원거리 서버로 라우팅하는 방법

가상 라우터를 사용할 경우, 한 가상 라우터에 있는 사용자가 별도의 가상 라우터를 통해서만 연결할 수 있는 서버에 액세스해야 하는 상황이 발생할 수 있습니다.

다음 사례를 고려하십시오. 영업 팀의 워크스테이션은 영업 가상 라우터에 연결되어 있습니다. 창고 서버는 창고 가상 라우터를 통해 연결되어 있습니다. 영업 팀이 IP 주소가 10.50.0.5/24인 창고 서버에서 정보를 조회해야 할 경우, 영업 가상 라우터의 경로를 창고 가상 라우터로 유출해야 합니다. 창고 가상 라우터는 창고 라우터 2 뒤에 멀티 홉 떨어진 창고 서버에 대한 경로도 있어야 합니다.



시작하기 전에

이 예시에서는 다음 항목을 이미 구성한 것으로 가정합니다.

- threat defense 디바이스에서 영업 가상 라우터와 창고 가상 라우터의 경우 GigabitEthernet 0/1은 영업에 할당되고, GigabitEthernet 0/2는 창고에 할당되었습니다.
- 영업 라우터 1에는 트래픽을 10.20.0.1/30 인터페이스에서 벗어나 10.50.0.5/24로 전송하는 정적 또는 동적 경로가 있습니다.

프로시저

단계 **1** 10.50.0.5/24 또는 10.50.0.0/24에 대한 네트워크 개체를 생성합니다. 또한, 게이트웨이 10.40.0.2/30에 대한 개체를 생성합니다.

경로를 창고 서버의 단일 IP 주소로 제한하려는 경우, 호스트 개체를 사용하여 10.50.0.5를 정의합니다. 또는 영업 팀이 창고에 있는 다른 시스템에 액세스해야 하는 경우, 10.50.0.0/24 네트워크에 대한 네트워크 개체를 생성합니다. 이 예시에서는 호스트 IP 주소에 대한 경로를 생성합니다.

a) 목차에서 **Objects(**개체**)**와 **Network(**네트워크**)**를 차례로 선택합니다.
b) +를 클릭한 다음 창고 서버에 대한 개체 속성을 입력합니다.

c) **OK(**확인**)**를 클릭합니다.
d) +를 클릭한 다음, 창고 네트워크로 연결되는 라우터 게이트웨이에 대한 개체 속성을 입력합니다.

e) **OK(**확인**)**를 클릭합니다.

단계 **2** 창고 가상 라우터에 있는 Gi0/2 인터페이스를 가리키는 영업 가상 라우터의 경로 유출을 정의합니다.

이 예시에서는 Gi0/1의 이름이 inside로 지정되고, Gi0/2가 inside-2로 지정되었습니다.

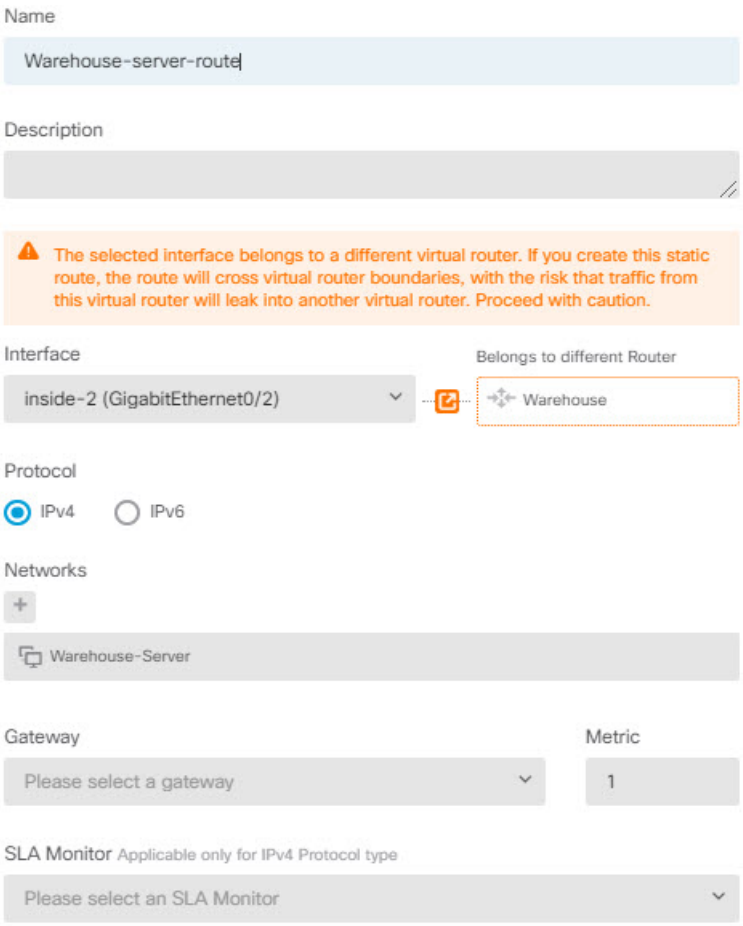
a) **Device(**디바이스**)**를 선택한 다음 **Routing(**라우팅**)** 요약에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

b) 가상 라우터 목록에서 영업 가상 라우터의 작업 열에 있는 보기 아이콘( )을 클릭합니다.

c) **Static Routing(**정적 라우팅**)** 탭에서 **+**를 클릭하고 다음과 같이 경로를 구성합니다.

- **Name(**이름**)** — 모든 이름을 지정할 수 있습니다(예: Warehouse-server-route).
- **Interface(**인터페이스**)** — **inside-2**를 선택합니다. 인터페이스가 다른 라우터에 있으며 경로 유출이 생성된다는 경고 메시지가 표시됩니다. 이는 사용자가 수행하려는 작업입니다.
- **Protocol(**프로토콜**)** — 이 예에서는 **IPv4**를 사용합니다. 또한 IPv6 주소를 사용하여 이 예시를 구현할 수 있습니다.
- **Networks(**네트워크**)** — Warehouse-Server 개체를 선택합니다.
- **Gateway(**게이트웨이**)** — 이 항목은 비워둡니다. 다른 가상 라우터로 경로를 유출할 경우에는 게이트웨이 주소를 선택하지 않습니다.

대화 상자가 다음과 비슷하게 표시됩니다.

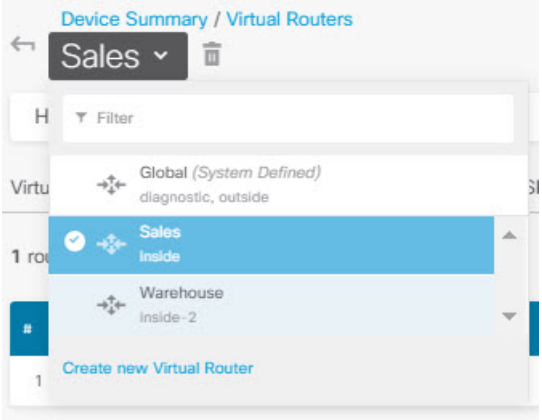


d) **OK(**확인**)**를 클릭합니다.

단계 **3** 창고 가상 라우터에서 창고 라우터 2 게이트웨이를 가리키는 경로를 정의합니다.

또는, 창고 라우터 2에서 경로를 동적으로 검색하는 라우팅 프로토콜을 구성하여 이 작업을 수행할 수 있습니다. 이 예에서는 정적 경로를 정의합니다.

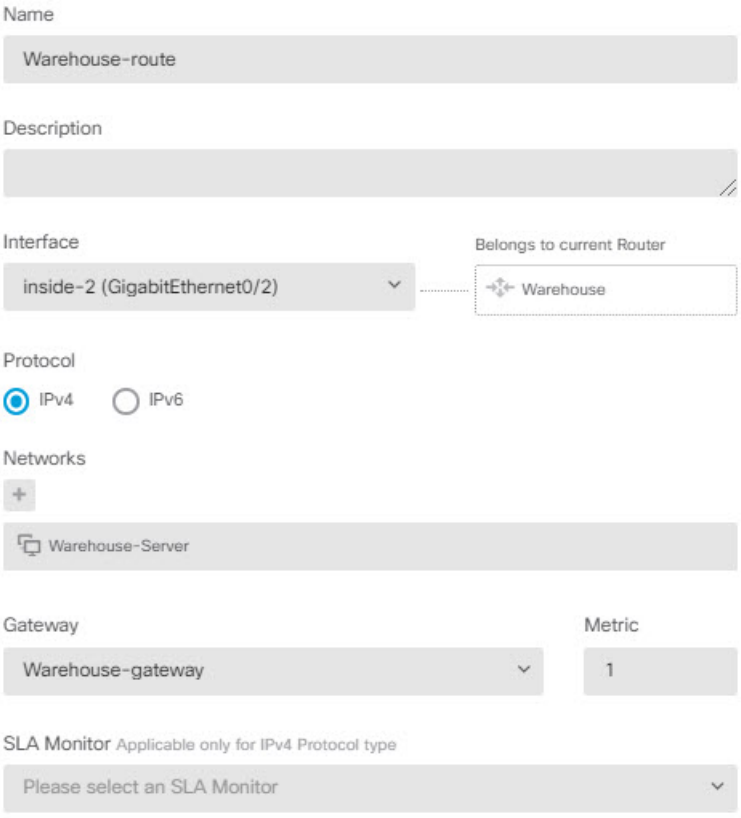
a) 현재 Sales(영업)라고 표시된 가상 라우터 드롭다운 목록에서 창고 가상 라우터를 선택하여 라우터를 전환합니다.



b) **Static Routing(**정적 라우팅**)** 탭에서 **+**를 클릭하고 다음과 같이 경로를 구성합니다.

- **Name(**이름**)** — 모든 이름을 지정할 수 있습니다(예: Warehouse-route).
- **Interface(**인터페이스**)** — **inside-2**를 선택합니다.
- **Protocol(**프로토콜**)** — **IPv4**를 선택합니다.
- **Networks(**네트워크**)** — Warehouse-Server 개체를 선택합니다.
- **Gateway(**게이트웨이**)** — Warehouse-gateway 개체를 선택합니다.

대화 상자가 다음과 비슷하게 표시됩니다.

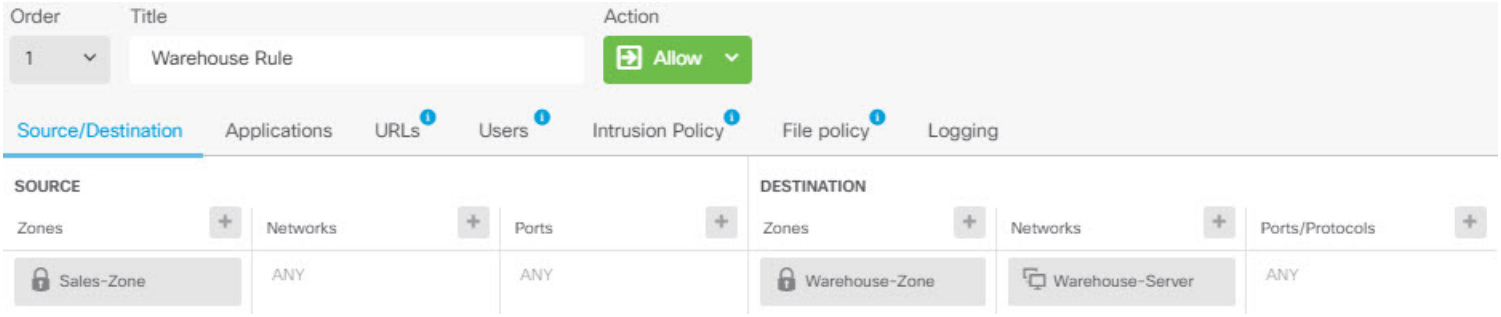


c) **OK(**확인**)**를 클릭합니다.

단계 **4** 창고 서버에 대한 액세스를 허용하는 액세스 제어 규칙이 있는지 확인합니다.

가장 단순한 규칙을 사용할 경우, 영업 가상 라우터에 있는 소스 인터페이스의 트래픽을 대상 Warehouse-Server 네트워크 개체에 대한 창고 가상 라우터에 있는 대상 인터페이스로 전송할 수 있습니다. 적절하다고 판단될 경우 침입 검사를 트래픽에 적용할 수 있습니다.

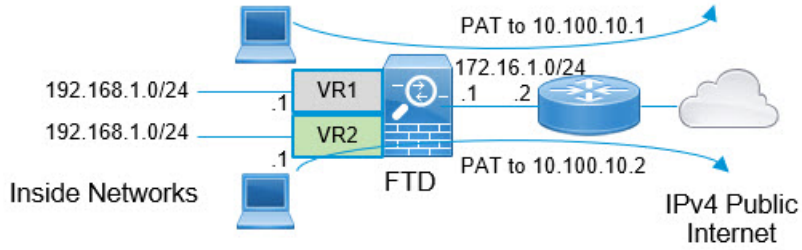
예를 들어 영업 가상 라우터에 있는 인터페이스가 Sales-Zone 보안 영역에 있을 경우, 창고 가상 라우터에 있는 해당 인터페이스는 Warehouse-Zone 보안 영역에 존재하며 액세스 제어 규칙은 다음과 유사합니다.



중복된 어드레스 스페이스가 있는 여러 가상 라우터에 인터넷 액세스를 제공하는 방법

가상 라우터를 사용할 경우, 별도의 라우터에 상주하는 인터페이스에 대해 동일한 네트워크 주소를 사용할 수 있습니다. 예를 들어 내부 및 내부-2 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. 그러나 이러한 별도의 가상 라우터에서 라우팅되는 IP 주소가 동일하므로, 반환 트래픽이 올바른 대상으로 이동하도록 하려면 가상 라우터에서 나가는 트래픽을 신중하게 처리해야 합니다.

예를 들어 동일한 어드레스 스페이스를 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 가상 라우터 1의 소스 주소를 10.100.10.1로 변환하고, 가상 라우터 2의 소스 주소를 10.100.10.2로 변환할 수 있습니다. 아래 그림에는 이러한 설정이 나와 있습니다. 여기서 인터넷 연결 외부 인터페이스는 전역 라우터의 일부입니다. 소스 인터페이스를 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 이 예는 각 가상 라우터에 단일 인터페이스가 포함된 단순화된 예입니다. "내부" 가상 라우터에 둘 이상의 인터페이스가 있을 경우 각 "내부" 인터페이스에 대해 NAT 규칙을 생성해야 합니다. 중복된 어드레스 스페이스를 사용하지 않는 가상 라우터 내에 일부 인터페이스가 있는 경우에도 NAT 규칙의 소스 인터페이스를 명시적으로 식별하면 문제를 더 쉽게 해결할 수 있으며, 인터넷에 바인딩된 가상 라우터에서 나가는 트래픽을 더 명확하게 분리할 수 있습니다.

프로시저

단계 **1** 가상 라우터 1(VR1)에 대한 내부 인터페이스를 구성합니다.

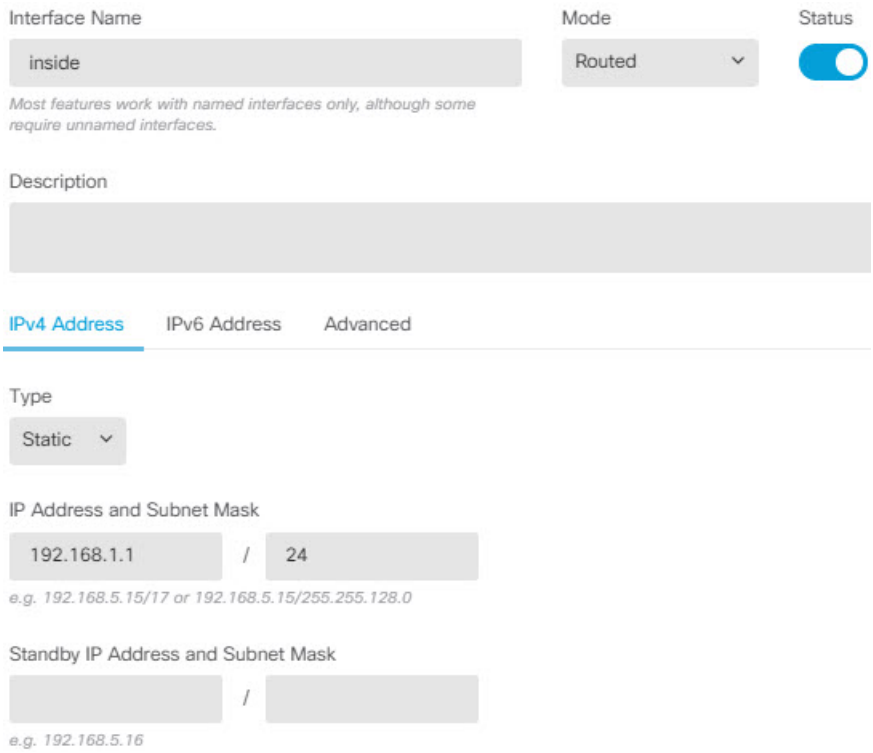
a) 디바이스를 클릭한 다음, **Interfaces(**인터페이스**)** 요약에서 **View All Interfaces(**모든 인터페이스 보기**)**를 클릭합니다.

b) VR1에 할당할 인터페이스에 대한 Action(작업) 열에서 수정 아이콘( )을 클릭합니다.

c) 다음 속성을 하나 이상 구성합니다.

- **Name(**이름**)** — 이 예에서는 **inside**로 지정합니다.

- **Mode(모드) - Routed(라우팅)**를 선택합니다.
- **Status(상태)** — 인터페이스를 활성화합니다.
- **IPv4 Address(IPv4 주소) > Type(유형)— Static(고정)**을 선택합니다.
- **IPv4 Address and Subnet Mask(IPv4 주소 및 서브넷 마스크)** — 192.168.1.1/24를 입력합니다.



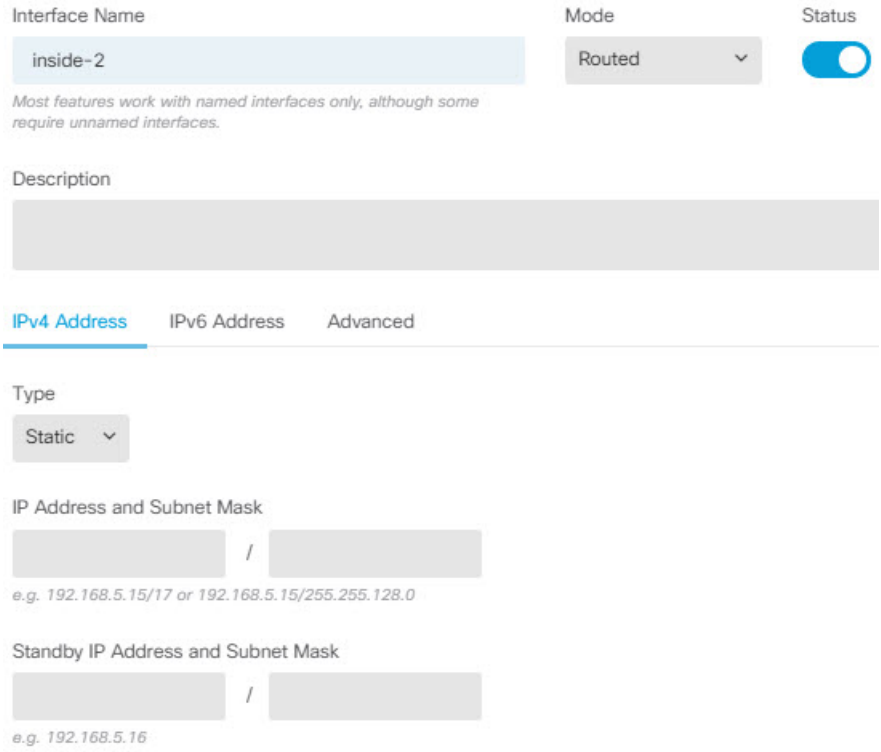
d) **OK(확인)**를 클릭합니다.

단계 **2** 가상 라우터 2(VR2)에 대한 inside-2 인터페이스를 구성하되, IP 주소는 지정하지 않습니다.

a) Interfaces(인터페이스) 목록 페이지에서 VR2에 할당할 인터페이스에 대한 Action(작업) 열에서 수정 아이콘( )을 클릭합니다.

b) 다음 속성을 하나 이상 구성합니다.

- **Name(이름)** — 이 예에서는 **inside-2**로 지정합니다.
- **Mode(모드) - Routed(라우팅)**를 선택합니다.
- **Status(상태)** — 인터페이스를 활성화합니다.
- **IPv4 Address(IPv4 주소) > Type(유형)— Static(고정)**을 선택합니다.
- **IPv4 Address and Subnet Mask(IPv4 주소 및 서브넷 마스크)** — 이 필드는 비워둡니다. 이 단계에서 내부 인터페이스와 동일한 주소를 구성하려고 할 경우, 시스템에 오류 메시지가 표시되며 기능 이외의 컨피그레이션을 생성할 수 없습니다. 동일한 라우터 내에서는 서로 다른 인터페이스를 통해 동일한 어드레스 스페이스로 라우팅할 수 없습니다.



c) **OK(**확인**)**를 클릭합니다.

단계 **3** 외부 인터페이스에 대한 정적 기본 경로 유출을 포함하여, 가상 라우터 VR1을 구성합니다.

a) **Device(**디바이스**)**를 선택한 다음 **Routing(**라우팅**)** 요약에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

b) Routing(라우팅) 페이지의 상단에서 **Add Multiple Virtual Routers(**여러 가상 라우터 추가**)**를 클릭합니다.

c) 설명 패널의 오른쪽 하단에서 **Create First Custom Virtual Router(**첫 번째 맞춤형 가상 라우터 생성)를 클릭합니다.

d) 가상 라우터 VR1에 대한 속성을 입력합니다.

- **Name(**이름**)** — VR1 또는 선택한 다른 이름을 입력합니다.
- **Interfaces(**인터페이스**)** — **+**를 클릭하고 **inside**를 선택한 후 **OK(**확인**)**를 클릭합니다.

e) **OK(**확인**)**를 클릭합니다.

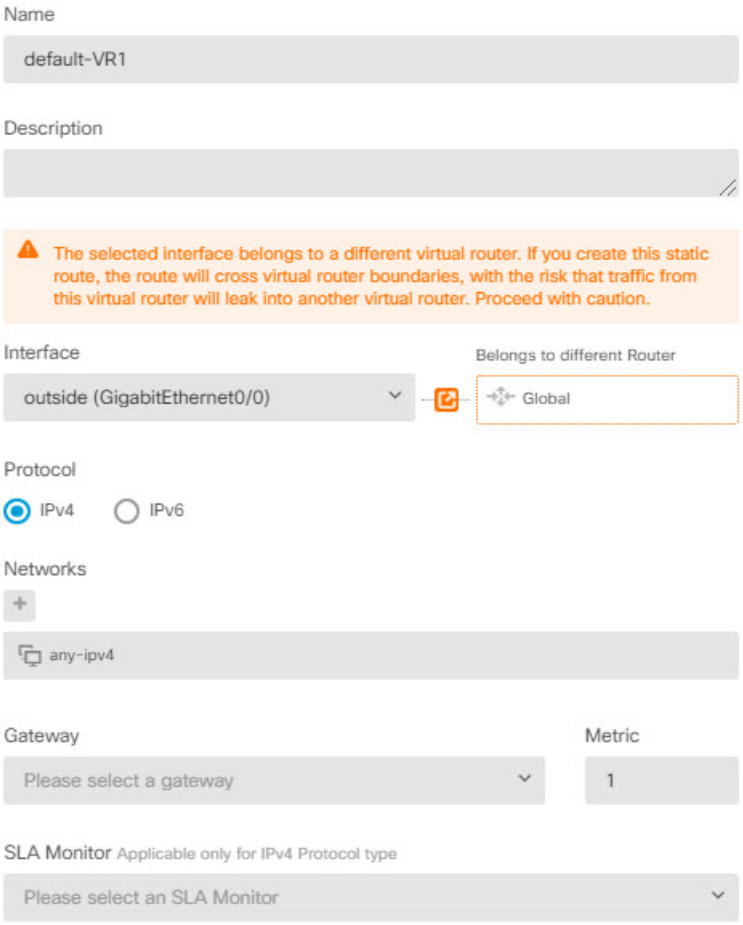
대화 상자가 닫히고 가상 라우터의 목록이 표시됩니다.

f) 가상 라우터 목록에서 VR1 가상 라우터의 작업 열에 있는 보기 아이콘( )을 클릭합니다.

g) **Static Routing(**정적 라우팅**)** 탭에서 **+**를 클릭하고 다음과 같이 경로를 구성합니다.

- **Name(**이름**)** — 어떤 이름이든 가능합니다(예: **default-VR1**).
- **Interface(**인터페이스**)** — **outside**를 선택합니다. 인터페이스가 다른 라우터에 있으며 경로 유출이 생성된다는 경고 메시지가 표시됩니다. 이는 사용자가 수행하려는 작업입니다.
- **Protocol(**프로토콜**)** — 이 예에서는 **IPv4**를 사용합니다.
- **Networks(**네트워크**)** — **any-ipv4** 개체를 선택합니다. 이 경로가 VR1 내에서 라우팅될 수 없는 모든 트래픽에 대한 기본 경로가 됩니다.
- **Gateway(**게이트웨이**)** — 이 항목은 비워둡니다. 다른 가상 라우터로 경로를 유출할 경우에는 게이트웨이 주소를 선택하지 않습니다.

대화 상자가 다음과 비슷하게 표시됩니다.



h) **OK(**확인**)**를 클릭합니다.

단계 **4** 외부 인터페이스에 대한 정적 기본 경로 유출을 포함하여, 가상 라우터 VR2를 구성합니다.

a) VR1이 표시되어 있는 경우, 뒤로 버튼(⮌)을 클릭하여 가상 라우터 목록으로 돌아갑니다.

b) 목록 위쪽에 있는 +를 클릭합니다.

c) 가상 라우터 VR2에 대한 속성을 입력합니다.

- **Name(**이름**)** — VR2 또는 선택한 다른 이름을 입력합니다.
- **Interfaces(**인터페이스**)** — +를 클릭하고 **inside-2**를 선택한 후 **OK(**확인**)**를 클릭합니다.

d) **OK(**확인**)**를 클릭합니다.

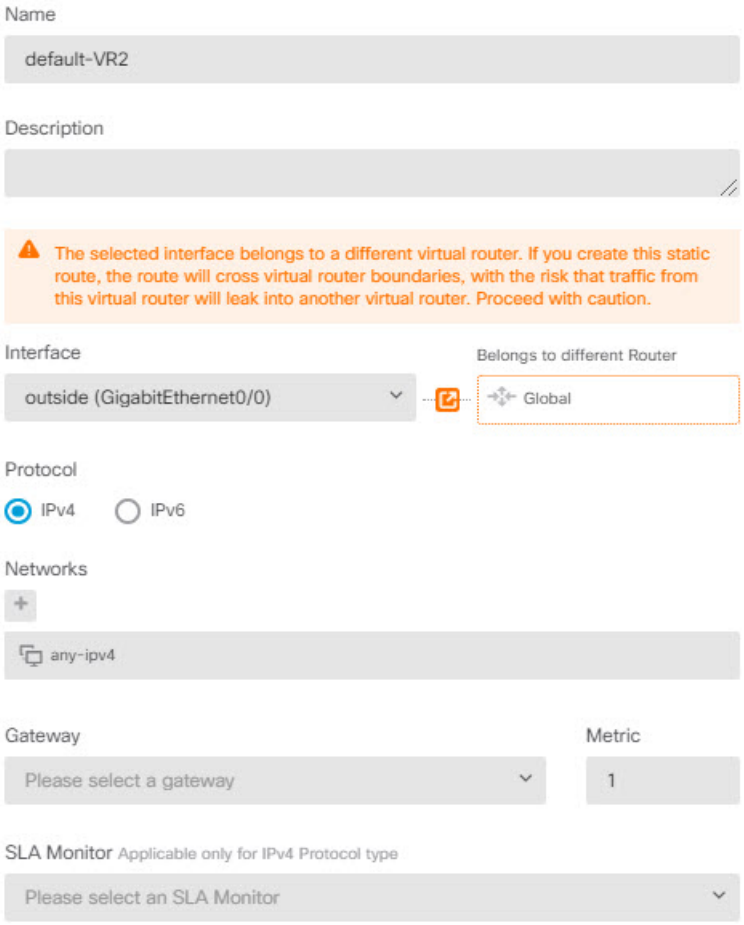
대화 상자가 닫히고 가상 라우터의 목록이 표시됩니다.

e) 가상 라우터 목록에서 VR2 가상 라우터의 작업 열에 있는 보기 아이콘( )을 클릭합니다.

f) **Static Routing(**정적 라우팅**)** 탭에서 **+**를 클릭하고 다음과 같이 경로를 구성합니다.

- **Name(**이름**)** — 어떤 이름이든 가능합니다(예: **default-VR2**).
- **Interface(**인터페이스**)** — **outside**를 선택합니다. 인터페이스가 다른 라우터에 있으며 경로 유출이 생성된다는 경고 메시지가 표시됩니다. 이는 사용자가 수행하려는 작업입니다.
- **Protocol(**프로토콜**)** — 이 예에서는 **IPv4**를 사용합니다.
- **Networks(**네트워크**)** — **any-ipv4** 개체를 선택합니다. 이 경로가 VR2 내에서 라우팅될 수 없는 모든 트래픽에 대한 기본 경로가 됩니다.
- **Gateway(**게이트웨이**)** — 이 항목은 비워둡니다. 다른 가상 라우터로 경로를 유출할 경우에는 게이트웨이 주소를 선택하지 않습니다.

대화 상자가 다음과 비슷하게 표시됩니다.

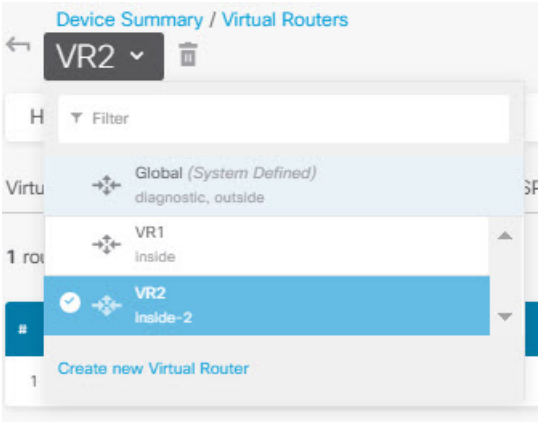


g) **OK(**확인**)**를 클릭합니다.

단계 **5** 외부 인터페이스에 대한 기본 경로를 전역 라우터에 생성합니다.

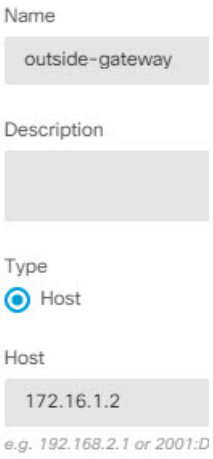
이 경로의 목적은 두 가지 가상 라우터에서 전역 라우터의 외부 인터페이스로 유출되는 트래픽에 올바른 게이트웨이를 할당하기 위한 것입니다.

a) VR2가 표시되면, 페이지 상단에 있는 VR2 이름을 클릭하여 가상 라우터 목록을 열고 전역 라우터를 선택합니다.

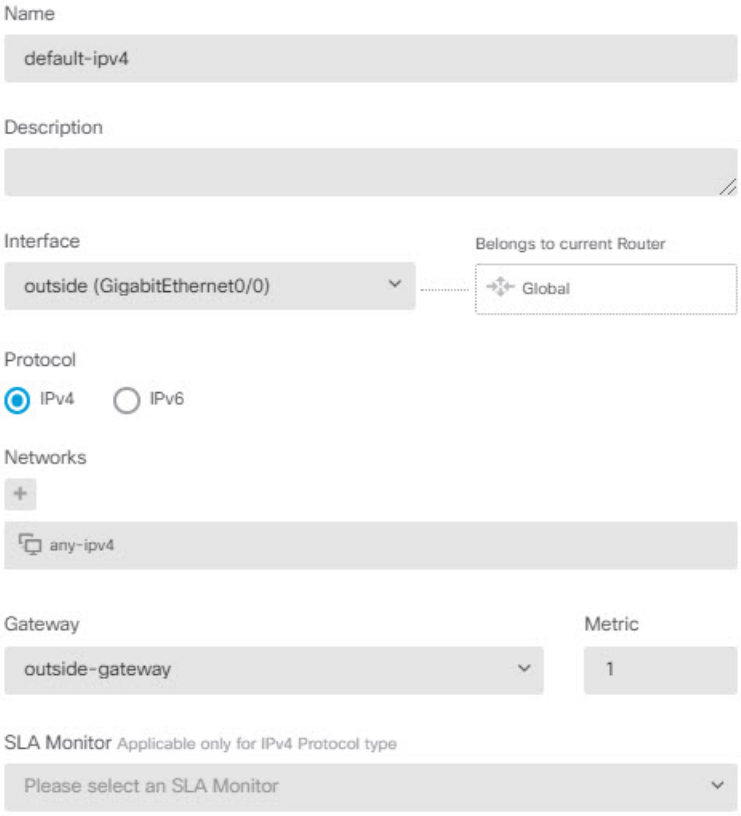


b) 전역 라우터에 대한 Static Routing(정적 라우팅) 탭에서 +를 클릭하고 다음과 같이 경로를 구성합니다.

- **Name(**이름**)** — 어떤 이름이든 가능합니다(예: default-ipv4).
- **Interface(**인터페이스**)** — **outside**를 선택합니다.
- **Protocol(**프로토콜**)** — 이 예에서는 **IPv4**를 사용합니다.
- **Networks(**네트워크**)** — **any-ipv4** 개체를 선택합니다. 이 경로가 모든 IPv4 트래픽에 대한 기본 경로가 됩니다.
- **Gateway(**게이트웨이**)** — 개체가 기존에 없다고 가정한 상태에서 **Create New Network Object(**새 네트워크 개체 생성**)**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, 정적 경로의 Gateway(게이트웨이) 필드에서 해당 개체를 선택합니다.



대화 상자가 다음과 비슷하게 표시됩니다.



c) **OK(**확인**)**를 클릭합니다.

단계 **6** **Interfaces(**인터페이스**)** 페이지로 돌아가 IP 주소를 inside-2에 추가합니다.

a) 디바이스를 클릭한 다음, **Interfaces(**인터페이스**)** 요약에서 **View All Interfaces(**모든 인터페이스 보기**)**를 클릭합니다.

b) VR2에 할당한 inside-2 인터페이스에 대한 Action(작업) 열에서 수정 아이콘( )을 클릭합니다.

c) **IPv4 Address(IPv4** 주소**)** 탭에 192.168.1.1/24를 IP 주소 및 서브넷 마스크로 입력합니다.

d) **OK(**확인**)**를 클릭합니다.

inside 및 inside-2 인터페이스가 현재 별도의 가상 라우터에 있으므로 이번에는 중복 IP 주소에 대한 오류가 발생하지 않습니다.

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

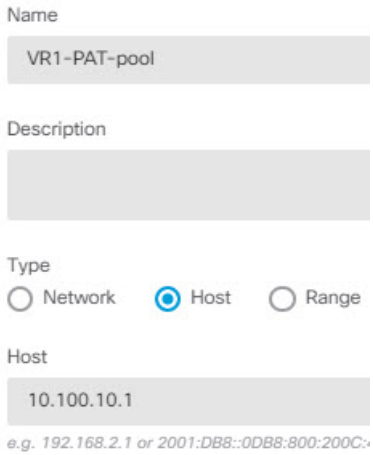
a) **Policies(**정책**)**를 선택한 다음 **NAT**를 클릭합니다.

b) 내부-외부 인터페이스에 InsideOutsideNatRule이라는 이름의 수동 NAT 규칙이 이미 있는 경우, 인터페이스 PAT를 적용하고 해당 규칙에 대해 수정 아이콘( )을 클릭합니다. 그렇지 않을 경우, **+**를 클릭하여 새 규칙을 생성합니다.

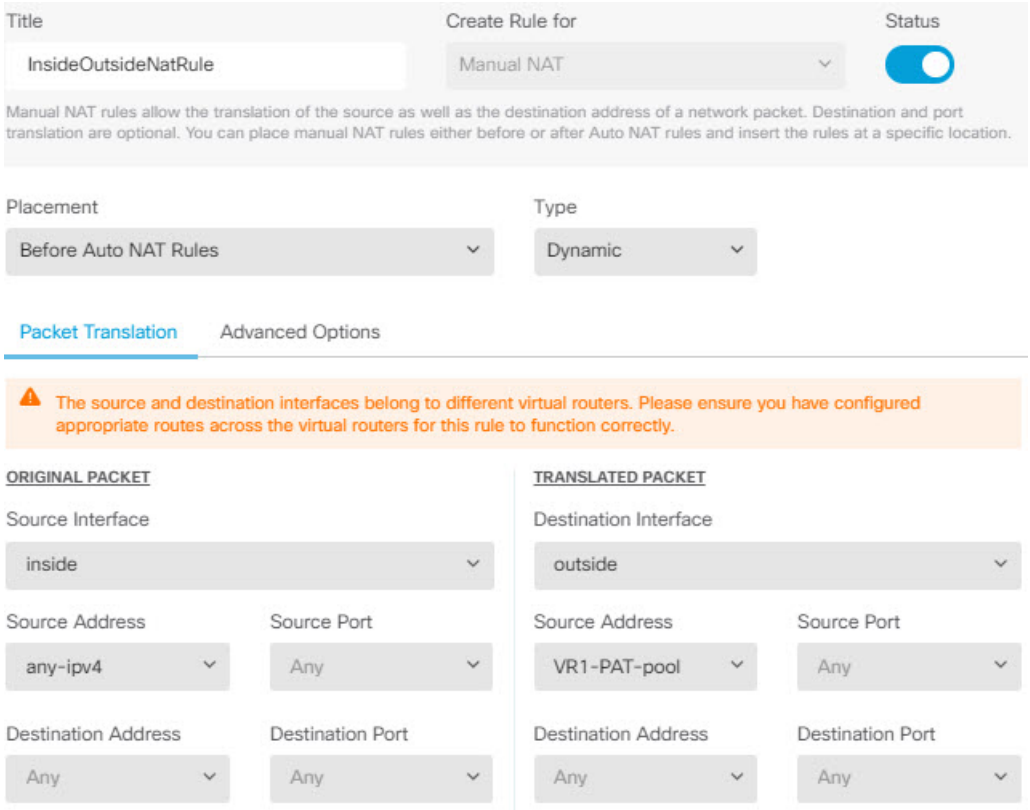
기존 규칙을 수정할 경우, 소스 및 대상 인터페이스가 서로 다른 가상 라우터에 있으며 경로를 정의해야 한다는 경고 메시지가 나타납니다. 이는 절차의 앞 단계에서 수행한 작업입니다.

c) 기존 규칙을 수정한다고 가정할 경우, **Translated Packet(**변환된 패킷**)** > **Source Address(**소스 주소**)**에서 드롭다운 화살표를 클릭하고, **Create New Network(**새 네트워크 생성**)**를 클릭합니다(10.100.10.1을 정의하는 호스트 개체가 기존에 없다고 가정).

d) PAT 주소에 대한 호스트 네트워크 개체를 구성합니다. 개체는 다음과 비슷해야 합니다.



e) 새 개체를 **Translated Packet(**변환된 패킷**)** > **Source Address(**소스 주소**)**로 선택합니다. NAT 규칙이 다음과 유사하게 표시됩니다.



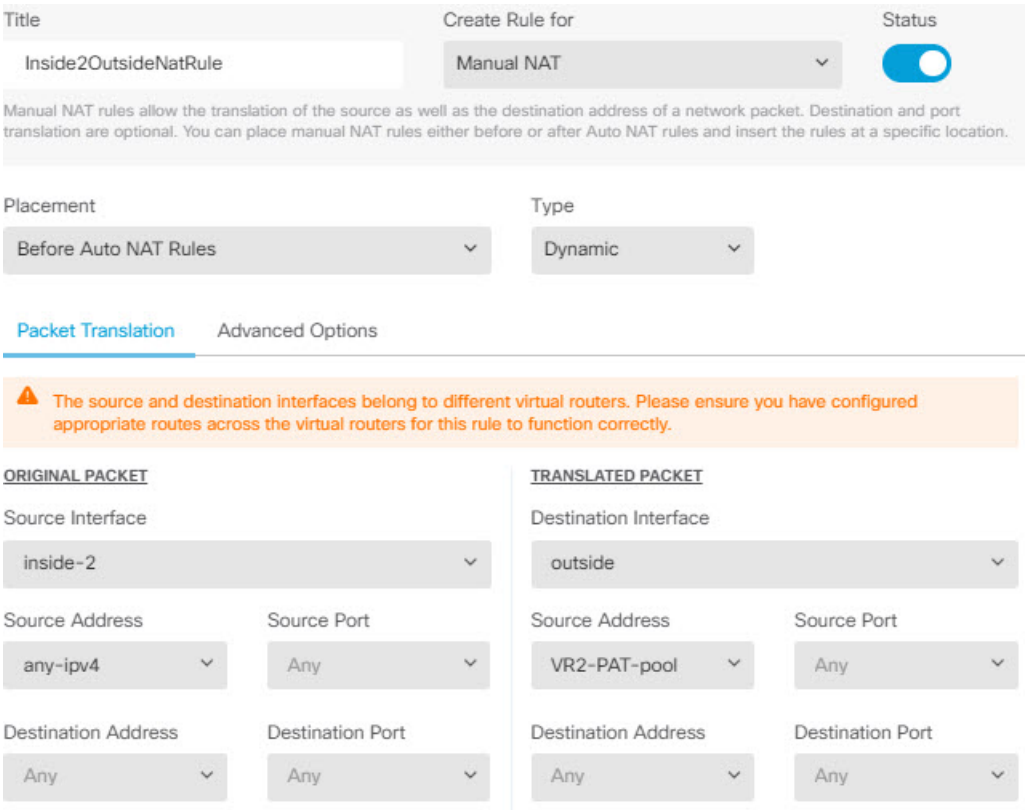
f) **OK(**확인**)**를 클릭합니다.

단계 **8** 외부 트래픽이 10.100.10.2로 향하도록 PAT inside-2에 대한 NAT 규칙을 생성합니다.

이 규칙은 다음과 같은 예외를 제외하고 VR1에 대한 규칙과 동일하게 표시됩니다.

- **Name(**이름**)** — 이는 고유해야 합니다(예: Inside2OutsideNatRule).
- **Original Packet(**원본 패킷**)** > **Source Interface(**소스 인터페이스**)** — inside-2를 선택합니다.
- **Translated Packet(**변환된 패킷**)** > **Source Address(**소스 주소**)** — 10.100.10.2에 대한 새 호스트 네트워크 개체를 생성합니다.

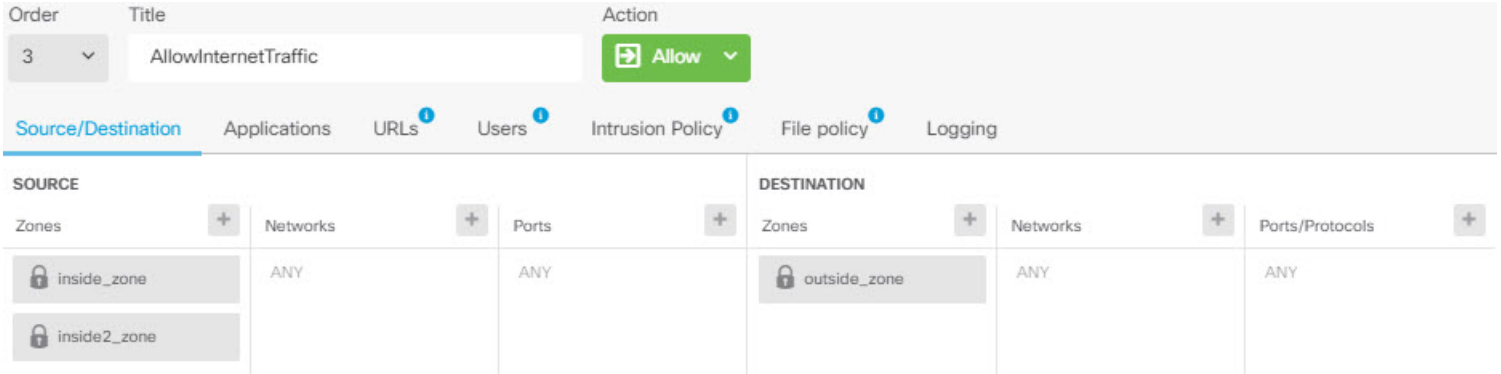
규칙이 다음과 유사하게 표시됩니다.



단계 **9** **Policies(**정책**)** > **Access Control(**액세스 제어**)**을 선택하고, 트래픽이 inside_zone 및 inside2_zone에서 outside_zone으로 향하도록 허용하는 액세스 제어 규칙을 구성합니다.

마지막으로, inside 및 inside-2 인터페이스에서 외부 인터페이스로 향하는 트래픽을 허용하는 액세스 제어 정책을 구성해야 합니다. 액세스 제어 규칙은 보안 영역을 사용해야 하므로, 이러한 각 인터페이스에 대한 영역을 생성해야 합니다. 또는 inside 및 inside-2 양쪽을 모두 보유하는 단일 영역을 생성할 수도 있지만, 이러한 라우터에서 트래픽을 처리하는 방식을 차별화하는 추가 규칙을 이 정책 또는 다른 정책에서 생성할 가능성이 높습니다.

인터페이스의 이름을 딴 영역을 생성한다고 가정할 경우, 모든 트래픽이 인터넷으로 흐르도록 허용하는 기본 규칙은 다음과 같습니다. 적합하다고 생각되는 경우 침입 정책을 이 규칙에 적용할 수 있습니다. 원치 않는 트래픽을 차단하는 추가 규칙(예: URL 필터링을 구현하는 경우)을 정의할 수 있습니다.



가상 라우터 모니터링

가상 라우터를 모니터링하고 트러블슈팅하려면 CLI 콘솔을 열거나 디바이스 CLI에 로그인하여 다음 명령을 사용합니다. Routing(라우팅) 페이지의 **Commands(명령)** 메뉴에서 이러한 명령 중 일부를 선택할 수도 있습니다.

- **show vrf** 시스템에 정의된 가상 라우터에 대한 정보를 표시합니다.
- **show ospf** [**vrf** *name* | **all**]

  가상 라우터의 OSPF 프로세스에 대한 정보를 표시합니다. 가상 라우터를 지정하여 해당 가상 라우터의 프로세스에 대한 정보만 볼 수도 있고, 옵션을 생략하여 모든 가상 라우터의 VRF에 대한 정보를 볼 수도 있습니다. **show ospf ?**를 사용하여 추가 옵션 목록을 확인합니다.
- **show bgp** [**vrf** *name* | **all**]

  가상 라우터의 OSPF 프로세스에 대한 정보를 표시합니다. 가상 라우터를 지정하여 해당 가상 라우터의 프로세스에 대한 정보만 볼 수도 있고, 옵션을 생략하여 모든 가상 라우터의 VRF에 대한 정보를 볼 수도 있습니다. **show bgp ?**를 사용하여 추가 옵션 목록을 확인합니다.
- **show eigrp** *option*

  EIGRP 프로세스에 대한 정보를 표시합니다. **show eigrp ?**를 사용하여 사용 가능한 옵션을 확인합니다.