정책 기반 라우팅

이 장에서는 Management Center의 정책 기반 라우팅 페이지를 통해 정책 기반 라우팅(PBR)을 지원하도록 Threat Defense를 구성하는 방법에 대해 설명합니다. 다음 섹션에서는 PBR에 대한 정책 기반 라우팅, 지침, 및 PBR의 구성을 설명합니다.

정책 기반 라우팅 정보

기존 라우팅에서는 패킷이 대상 IP 주소에 따라 라우팅됩니다. 그러나 대상 기반 라우팅 시스템에서 특정 트래픽의 라우팅을 변경하기는 어렵습니다. PBR(정책 기반 라우팅)은 프로토콜을 라우팅하여 제공되는 기존 메커니즘을 확장하고 보완하여 라우팅에 추가적인 제어 기능을 제공합니다.

PBR을 통해 IP 우선순위를 설정할 수 있습니다. 또한 특정 트래픽(예: 비용이 많이 드는 링크를 통한 우선순위 트래픽)에 대해 경로를 지정할 수 있습니다. PBR을 사용하면 소스 포트, 대상 주소, 목적지 포트, 프로토콜, 애플리케이션 또는 이러한 개체의 조합과 같은 대상 네트워크 이외의 기준에 따라 라우팅을 정의할 수 있습니다.

PBR를 사용하여 애플리케이션. 이 라우팅 방법은 여러 디바이스가 대규모 네트워크 구축의 애플리케이션 및 데이터에 액세스하는 시나리오에 적용할 수 있습니다. 일반적으로 대규모 구축에는 경로 기반 VPN에서 암호화된 트래픽으로 허브에 대한 모든 네트워크 트래픽을 백홀하는 토폴로지가 있습니다. 이러한 토폴로지로 인해 패킷 레이턴시, 감소된 대역폭 및 패킷 삭제와 같은 문제가 발생하는 경우가 많습니다. 이러한 문제를 해결하려면 고비용의 복잡한 구축 및 관리가 필요합니다.

PBR 정책을 사용하면 지정된 애플리케이션에 대한 트래픽을 안전하게 분리할 수 있습니다. 애플리케이션에 직접 액세스할 수 있도록 Secure Firewall Management Center 사용자 인터페이스에서 PBR 정책을 구성할 수 있습니다.

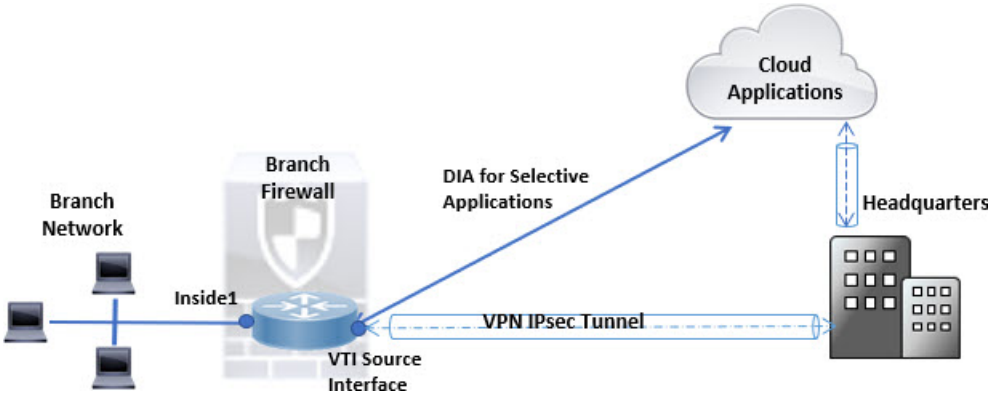
정책 기반 라우팅을 사용하는 이유

지점 간에 두 개의 링크가 있는 회사를 생각해 보십시오. 하나는 대역폭이 높고 지연 비용이 낮은 링크이고 또 다른 하나는 대역폭이 낮고 지연 시간이 길지만 비용이 낮은 링크입니다. 기존의 라우팅 프로토콜을 사용하는 동안에는 링크의 대역폭, 지연 또는 둘 모두(EIGRP 또는 OSPF 사용) 특성에서 얻은 메트릭 절약을 기반으로 하여 높은 대역폭 링크가 전송 트래픽의 전부는 아니더라도 대부분을 맡습니다. PBR을 활용하면 높은 대역폭/낮은 지연 링크를 통해 우선순위가 높은 트래픽을 라우팅하고 낮은 대역폭/높은 지연 링크를 통해 모든 기타 트래픽을 전송할 수 있습니다.

다음은 정책 기반 라우팅을 사용할 수 있는 몇 가지 시나리오입니다.

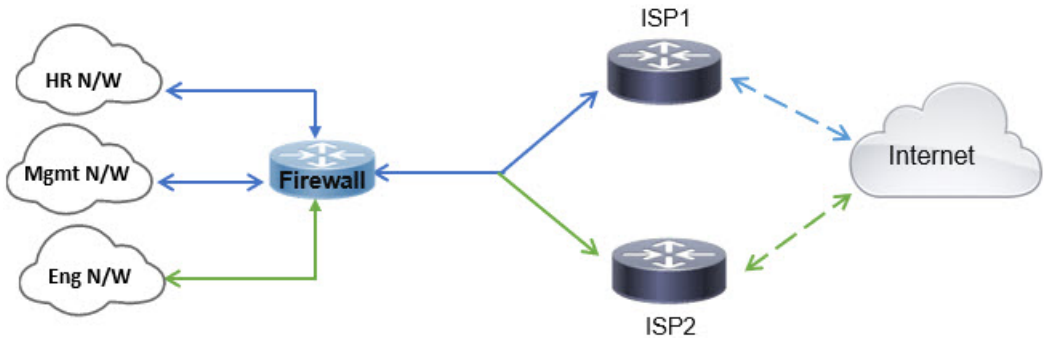
직접 인터넷 액세스

이 토폴로지에서는 브랜치 오피스에서 온 애플리케이션 트래픽을 본사에 연결하는 VPN 터널을 통과 하는 대신 인터넷으로 직접 라우팅할 수 있습니다. 브랜치 threat defense는 인터넷 종료 지점으로 구성되며 ACL에 정의된 애플리케이션 을 기반으로 트래픽을 식별하기 위해 인그레스 인터페이스(내부 *1*)에 PBR 정책이 적용됩니다. 따라서 트래픽은 이그레스 인터페이스를 통해 인터넷 또는 IPsec VPN 터널로 직접 전달됩니다.



동일 액세스 및 소스를 구분하는 라우팅

이 토폴로지에서 HR 및 관리 네트워크의 트래픽은 ISP1을 통해 구성될 수 있으며, Eng 네트워크의 트래픽은 ISP2를 통해 구성될 수 있습니다. 따라서 정책 기반 라우팅은 네트워크 관리자가 여기의 내용과 같이 동일 액세스 및 소스를 구분하는 라우팅을 제공하도록 지원합니다.



로드 공유

ECMP 로드 밸런싱에서 제공하는 동적인 로드 공유 기능 외에, 네트워크 관리자는 이제 트래픽 특성에 따라 여러 경로에서 트래픽을 분산시키기 위해 정책을 구현할 수 있습니다.

예를 들어, 동일 액세스 소스 구분 라우팅 시나리오에 설명되어 있는 토폴로지에서 관리자는 ISP1을 통한 HR 네트워크의 트래픽과 ISP2를 통한 Eng 네트워크 트래픽을 라우팅하여 부하를 공유하기 위해 정책 기반 라우팅을 구성할 수 있습니다.

정책 기반 라우팅에 대한 지침 및 제한 사항

방화벽 모드 지침

PBR는 라우팅된 방화벽 모드에서만 지원됩니다.

디바이스 지침

- management center의 Policy Based Routing(정책 기반 라우팅) 페이지를 통한 PBR은 Secure Firewall Threat Defense 버전 7.1 이상의 디바이스에서만 지원됩니다. Secure Firewall Management Center 릴리스 7.1은 7.1 이전 Threat Defense버전을 지원하지만 Policy Based Routing(정책 기반 라우팅) 페이지를 사용하여 해당 디바이스에서 PBR를 활성화할 수 없습니다.
- FlexConfig는 7.1 이전 버전의 Threat Defense에 대해 management center에서 PBR를 구성하는 데 사용되었습니다. FlexConfig를 사용하여 모든 버전에서 PBR를 구성할 수 있습니다. 그러나 인그레스 인터페이스의 경우 FlexConfig 및 management center의 Policy Based Routing(정책 기반 라우팅) 페이지를 모두 사용하여 PBR를 구성할 수는 없습니다.
- 클러스터 디바이스에서 애플리케이션, 기반 PBR 정책 구성은 지원되지 않습니다.

인터페이스 지침

- 전역 가상 라우터에 속하는 라우팅 인터페이스 및 비 관리 전용 인터페이스만 인그레스 또는 이그레스 인터페이스로 구성할 수 있습니다.
- PBR은 사용자 정의 가상 라우터에서 지원되지 않습니다.
- 논리적 이름이 있는 인터페이스만 정책에서 정의할 수 있습니다.
- 고정 VTI는 이그레스 인터페이스로만 구성할 수 있습니다.
- 구성을 진행하기 전에 각 세션의 인그레스 및 이그레스 트래픽이 동일한 ISP 연결 인터페이스를 통과하는지 확인하여 비대칭 라우팅, 특히 NAT 및 VPN을 사용 중인 경우 예기치 않은 동작이 발생하지 않도록 해야 합니다.

IPv6 지원

PBR는 IPv6를 지원합니다.

애플리케이션 기반 **PBR** 및 **DNS** 구성

- 애플리케이션 기반 PBR은 애플리케이션 탐지에 DNS 스누핑을 사용합니다. DNS 요청이 일반 텍스트 형식으로 threat defense를 통과하는 경우에만 애플리케이션 탐지가 성공합니다. DNS 트래픽은 암호화되지 않습니다.
- 신뢰할 수 있는 DNS 서버를 구성해야 합니다.

DNS 서버 구성에 대한 자세한 내용은 DNS의 내용을 참조하십시오.

원시 트래픽에 적용되지 않는 **PBR** 정책

참고 원시 연결은 소스와 대상 간에 필요한 핸드셰이크를 완료하지 않은 연결입니다.

새 내부 인터페이스가 추가되고 고유한 주소 풀을 사용하여 새 VPN 정책이 생성되면 새 클라이언트 풀의 소스와 일치하는 외부 인터페이스에 PBR이 적용됩니다. 따라서 PBR은 클라이언트에서 새 인터페이스의 다음 홉으로 트래픽을 전송합니다. 그러나 새 내부 인터페이스 경로를 사용하여 클라이언트에 대한 연결을 아직 설정하지 않은 호스트의 반환 트래픽에는 PBR이 포함되지 않습니다. 따라서 호스트에서 VPN 클라이언트로의 반환 트래픽, 특히 유효한 경로가 없으므로 VPN 클라이언트 응답이 삭제됩니다. 내부 인터페이스에서 더 높은 메트릭으로 가중치 고정 경로를 구성해야 합니다.

추가 지침

- 경로 맵의 모든 기존 구성 제한사항 및 한계는 이후에 수행됩니다.
- 정책 일치 기준에 대한 ACL을 정의하는 동안 사전 정의된 애플리케이션 목록에서 여러 애플리케이션을 선택하여 ACE(Access Control Entry)를 구성할 수 있습니다. threat defense에서 사전 정의된 애플리케이션은 네트워크 서비스 개체로 저장되고 애플리케이션 그룹은 NSG(Network Service Group)로 저장됩니다. 최대 1,024개의 NSG를 생성할 수 있습니다. 애플리케이션 또는 네트워크 서비스 그룹이 첫 번째 패킷 분류를 통해 탐지됩니다. 현재는 사전 정의된 애플리케이션 목록을 추가하거나 수정할 수 없습니다.

경로 모니터링

경로 모니터링은 인터페이스에 구성된 경우 RTT(왕복 시간), 지터, MOS(평균 의견 점수) 및 인터페이스 당 패킷 손실과 같은 메트릭을 파생합니다. 이러한 메트릭은 PBR 트래픽 라우팅에 가장 적합한 경로를 결정하는 데 사용됩니다.

인터페이스의 메트릭은 ICMP 프로브 메시지를 사용하여 인터페이스의 기본 게이트웨이 또는 지정된 원격 피어에 동적으로 수집됩니다.

기본 모니터링 타이머

메트릭 수집 및 모니터링을 위해 다음 타이머가 사용됩니다.

- 인터페이스 모니터 평균 간격은 30초입니다. 이 간격은 프로브의 평균 빈도를 나타냅니다.
- 인터페이스 모니터 업데이트 간격은 30초입니다. 이 간격은 수집된 값의 평균이 계산되고 PBR에서 최적의 라우팅 경로를 결정하는 데 사용할 수 있는 빈도를 나타냅니다.
- ICMP의 인터페이스 모니터 프로브 간격은 1초입니다. 이 간격은 ICMP ping이 전송되는 빈도를 나타냅니다.

참고 이러한 타이머의 간격을 구성하거나 수정할 수 없습니다.

PBR 및 경로 모니터링

일반적으로 PBR에서 트래픽은 구성된 우선순위 값(인터페이스 비용)에 따라 이그레스 인터페이스를 통해 전달됩니다. Management Center 버전 7.2부터 PBR은 IP 기반 경로 모니터링을 사용하여 이그레스 인터페이스의 성능 메트릭(RTT, 지터, 패킷 손실 및 MOS)을 수집합니다. PBR은 메트릭을 사용하여 트래픽을 전달하기 위한 최적의 경로(이그레스 인터페이스)를 결정합니다. 경로 모니터링은 메트릭이 변경된 모니터링되는 인터페이스에 대해 주기적으로 PBR에 알립니다. PBR은 경로 모니터링 데이터베이스에서 모니터링되는 인터페이스에 대한 최신 메트릭 값을 검색하 고 데이터 경로를 업데이트합니다.

인터페이스에 대한 경로 모니터링을 활성화하고 모니터링 유형을 구성해야 합니다. PBR 정책 페이지에서는 경로 결정을 위해 원하는 메트릭을 지정할 수 있습니다. 정책 기반 라우팅 정책 구성, 6 페이지의 내용을 참조하십시오.의 내용을 참조하십시오.

경로 모니터링 설정 구성

PBR 정책은 트래픽에 가장 적합한 라우팅 경로를 식별하기 위해 인터페이스의 RTT(왕복 시간), 지터, MOS(평균 의견 점수) 및 패킷 손실과 같은 유연한 메트릭을 사용합니다. 경로 모니터링은 지정된 인터페이스에서 이러한 메트릭을 수집합니다. **Interfaces(**인터페이스**)** 페이지에서 메트릭 수집을 위해 ICMP 프로브을 전송하도록 경로 모니터링에 대한 설정을 사용하여 인터페이스를 구성할 수 있습니다.

Threat Defense 기능 기록**:**

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 threat defense 디바이스에 대한 **Edit(**수정**)** ( )를 클릭합니다. 기본적으로는 **Interfaces(**인터페이스**)** 페이지가 선택됩니다.

단계 **2** 수정할 인터페이스의 **Edit(**수정**)** ( )을 클릭합니다.

단계 **3** **Path Monitoring(**경로 모니터링**)** 탭을 클릭합니다.

단계 **4** **Enable Path Monitoring(**경로 모니터링 활성화**)** 확인란을 클릭합니다.

단계 **5** **Monitoring Type(**모니터링 유형**)** 드롭다운 목록에서 관련 옵션을 선택합니다.

- **Auto(**자동**)** — ICMP 프로브를 인터페이스의 IPv4 기본 게이트웨이로 전송합니다. IPv4 게이트웨이가 없는 경우 경로 모니터링은 인터페이스의 IPv6 기본 게이트웨이로 프로브를 전송합니다.
- **Peer IPv4(**피어 **IPv4)** — 모니터링을 위해 ICMP 프로브를 지정된 피어 IPv4 주소(next-hop IP)로 전송합니다. 이 옵션을 선택하는 경우 **Peer IP To Monitor(**모니터링할 피어 **IP)** 필드에 IPv4 주소를 입력합니다.
- **Peer IPv6(**피어 **IPv6)** — 모니터링을 위해 ICMP 프로브를 지정된 피어 IPv6 주소(next-hop IP)로 전송합니다. 이 옵션을 선택하는 경우 **Peer IP To Monitor(**모니터링할 피어 **IP)** 필드에 IPv6 주소를 입력합니다.
- **Auto IPv4(**자동 **IPv4)** — ICMP 프로브를 인터페이스의 기본 IPv4 게이트웨이로 전송합니다.
- **Auto IPv6(**자동 **IPv6)** — 인터페이스의 기본 IPv6 게이트웨이로 ICMP 프로브를 전송합니다.

참고

- VTI 인터페이스에는 Auto(자동) 옵션을 사용할 수 없습니다. 피어 주소를 지정해야 합니다.
- 하나의 다음 홉만 대상으로 모니터링됩니다. 즉, 인터페이스를 모니터링할 피어 주소를 두 개 이상 지정할 수 없습니다.

단계 **6** **Ok(**확인**)**을 클릭하고 설정을 저장하려면 **Save(**저장**)**를 클릭합니다.

정책 기반 라우팅 정책 구성

인그레스 인터페이스, 일치 기준(확장된 액세스 제어 목록) 및 이그레스 인터페이스를 지정하여 Policy Based Routing(정책 기반 라우팅) 페이지에서 PBR 정책을 구성할 수 있습니다.

Threat Defense 기능 기록**:**

- 7.3 - PBR 루트 맵에 대한 다음 홉 구성.
- 7.2 - 경로 모니터링 기반의 PBR.
- 7.1 - 정책 기반 라우팅 도입.

시작하기 전에

이그레스 인터페이스에 대한 트래픽 전달 우선순위를 구성하기 위해 경로 모니터링 메트릭을 사용하려면 인터페이스에 대한 경로 모니터링 설정을 구성해야 합니다. 경로 모니터링 설정 구성, 5 페이지의 내용을 참조하십시오.

프로시저

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

단계 **2** **Routing(**라우팅**)**을 클릭합니다.

단계 **3** **Policy Based Routing(**정책 기반 라우팅**)**을 클릭합니다.

Policy Based Routing(정책 기반 라우팅) 페이지에 구성된 정책이 표시됩니다. 그리드에 인그레스 인터페이스 목록과 정책 기반 경로 액세스 목록 및 이그레스 인터페이스의 조합이 표시됩니다.

단계 **4** 정책을 구성하려면 **Add(**추가**)**를 클릭합니다.

단계 **5** **Add Policy Based Route(**정책 기반 경로 추가**)** 대화 상자의 드롭다운 목록에서 **Ingress Interface(**인그레스 인터페이스**)**를 선택합니다.

참고 논리적 이름이 있고 전역 가상 라우터에 속하는 인터페이스만 드롭다운에 나열됩니다.

단계 **6** 정책에서 일치 기준 및 전달 작업을 지정하려면 **Add(**추가**)**를 클릭합니다.

단계 **7** **Add Forwarding Actions(**전달 작업 추가**)** 대화 상자에서 다음을 수행합니다.

a) **Match ACL(ACL** 일치**)** 드롭다운에서 확장된 액세스 제어 목록 개체를 선택합니다. ACL 개체를 미리 정의하거나(확장 ACL 개체 설정 참조) **Add(**추가**)** (+) 아이콘을 클릭하여 개체를 생성할 수 있습니다. **New Extended Access List Object(**새 확장 액세스 목록 개체**)** 상자에 이름을 입력하고 **Add(**추가**)**를 클릭하여 **Add Extended Access List Entry(**확장 액세스 목록 항목 추가**)** 대화 상자를 엽니다. 여기서 PBR 정책에 대한 네트워크, 포트, 또는 애플리케이션 일치 기준을 정의할 수 있습니다.

참고 ACE에 애플리케이션 주소와 대상 주소를 모두 정의할 수는 없습니다.

수신 인터페이스에서 PBR을 선택적으로 적용하기 위해 ACE에서 차단 기준을 정의할 수 있습니다. 트래픽이 ACE의 차단 규칙과 일치하면 해당 트래픽은 라우팅 테이블을 기반으로 이그레스 인터페이스로 전달됩니다.

b) **Send To(**전송 대상**)** 드롭다운 목록에서:

- 구성된 인터페이스를 선택하려면 **Egress Interfaces(**이그레스 인터페이스**)**를 선택합니다.
- IPv4/IPv6 다음 홉 주소를 지정하려면 **IP Address(IP** 주소**)**를 선택합니다. 7.e, 8 페이지단계로 진행합니다.

c) **Egress Interfaces(**이그레스 인터페이스**)**를 선택한 경우 **Interface Ordering(**인터페이스 순서 지정**)** 드롭다운에서 관련 옵션을 선택합니다.

- **By Priority(**우선순위 기준**)** - 인터페이스의 우선순위에 따라 트래픽이 전달됩니다. 트래픽은 우선 순위 값이 가장 낮은 인터페이스로 라우팅됩니다. 인터페이스를 사용할 수 없는 경우 트래픽은 다음으로 낮은 우선순위 값을 가진 인터페이스로 전달됩니다. 예를 들어 *Gig0/1*, *Gig0/2*, and *Gig0/3*이 각각 우선 순위 값 *0,1* 및 *2*로 구성되어 있다고 가정합니다. 트래픽은 *Gig0/1*로 전달됩니다. *Gig0/1*을 사용할 수 없게 되면 트래픽이 *Gig0/2*로 전달됩니다.

참고 인터페이스의 우선순위를 구성하려면 Policy Based Routing(정책 기반 라우팅) 페이지에서 **Configure Interface Priority(**인터페이스 우선순위 구성**)**를 클릭합니다. 대화 상자에서 인터페이스에 대한 우선순위 번호를 입력하고 **Save(**저장**)**를 클릭합니다. Interface Settings(인터페이스 설정)에서 인터페이스의 우선순위를 구성할 수도 있습니다.

모든 인터페이스에 대해 우선순위 값이 동일한 경우 트래픽이 인터페이스 간에 균형을 이룹니다.

- **Order(**순서**)** 기준 - 여기에 지정된 인터페이스의 순서에 따라 트래픽이 전달됩니다. 예를 들어 *Gig0/1*, *Gig0/2*, and *Gig0/3*이 *Gig0/2*, *Gig0/3*, *Gig0/1* 순서로 선택되었다고 가정해 보겠습니다. 트래픽은 우선 순위 값에 관계 없이 먼저 *Gig0/2*로 전달된 다음 *Gig0/3*으로 전달됩니다.
- **Minimal Jitter(**최소 지터**)** 기준 — 트래픽이 지터 값이 가장 낮은 인터페이스로 전달됩니다. 지터 값을 얻으려면 PBR에 대 한 인터페이스에서 경로 모니터링을 활성화해야 합니다.
- **Maximum Mean Opinion Score(**최대 평균 오피니언 점수**)** 기준 - 최대 MOS(평균 오피니언 점수)가 있는 인터페이스로 트래픽이 전달됩니다. MOS 값을 얻으려면 PBR에 대한 인터페이스에서 경로 모니터링을 활성화해야 합니다.
- **Minimum Round Trip Time(**최소 왕복 시간**)** 기준 — 트래픽이 RTT(최소 왕복 시간)가 있는 인터페이스로 전달됩니다. RTT 값을 가져오려면 PBR에 대한 인터페이스에서 경로 모니터링을 활성화해야 합니다.
- **Minimal Packet Loss(**최소 패킷 손실**)** 기준 — 트래픽이 패킷 손실이 최소인 인터페이스로 전달됩니다. 패킷 손실 값을 얻으려면 PBR에 대한 인터페이스에서 경로 모니터링을 활성화해야 합니다.

d) **Available Interfaces(**사용 가능한 인터페이스**)** 상자에 우선순위 값과 함께 모든 인터페이스가 나열됩니다. 인터페이스 목록에서 **Add(**추가**)** (⊕) 버튼을 클릭하여 선택한 이그레스 인터페이스에 추가합니다. 7.k, 9 페이지단계로 진행합니다.

e) **IP Address(IP** 주소**)**를 선택한 경우 **IPv4 Addresses(IPv4** 주소**)** 또는 **IPv6 Addresses(IPv6** 주소**)** 필드에 쉼표로 구분된 IP 주소를 입력합니다. 트래픽은 지정된 IP 주소의 순서에 따라 전달됩니다.

참고 여러 다음 홉 IP 주소가 제공되면 유효한 라우팅 가능한 다음 홉 IP 주소를 찾을 때까지 지정된 IP 주소의 시퀀스에 따라 트래픽이 전달됩니다. 구성된 다음 홉에는 직접 연결되어야 합니다.

f) **Don't Fragment(**조각화 금지**)** 드롭다운 목록에서 Yes(예), No(아니요) 또는 None(없음)을 선택합니다. DF(Don't Fragment) 플래그가 *Yes(*예*)*로 설정된 경우, 중간 라우터는 패킷의 조각화를 수행하지 않습니다.

g) 현재 인터페이스를 포워딩의 기본값으로 지정하려면 **Default Interface(**기본 인터페이스**)** 확인란을 선택합니다.

h) **IPv4 Settings(IPv4** 설정**)** 및 **IPv6 Settings(IPv6** 설정**)** 탭에서는 재귀 및 기본 설정을 지정할 수 있습니다.

참고 경로 맵의 경우 IPv4 또는 IPv6 다음 홉 설정만 지정할 수 있습니다.

- **Recursive(**재귀**)** - 루트 맵 구성은 지정된 다음 홉 주소 및 기본 다음 홉 주소가 직접 연결된 서브넷에서 발견되는 경우에만 적용됩니다. 그러나 다음 홉 주소를 직접 연결할 필요가 없는 경우 재귀 옵션을 사용할 수 있습니다. 여기에서 재귀 조회가 다음 홉 주소에서 수행되며 일치하는 트래픽이 라우터에서 라우터의 현재 라우팅 경로에 따라 경로 항목에서 사용하는 다음 홉에 전달됩니다.
- **Default(**기본값**)** - 일반 경로 조회가 트래픽과 일치하지 않으면 트래픽은 지정된 다음 홉 IP 주소로 전달됩니다.

i) 다음 홉 주소를 피어 주소로 사용하려면 **Peer Address(**피어 주소**)** 확인란을 선택합니다.

참고 기본 다음 홉 주소와 피어 주소를 모두 사용하여 경로 맵을 구성할 수는 없습니다.

j) IPv4 설정의 경우 **Verify Availability(**가용성 확인**)** 아래에서 경로 맵의 다음 IPv4 홉을 사용할 수 있는지 확인할 수 있습니다. **Add(**추가**)** (+) 버튼을 클릭하고 다음 홉 IP 주소 항목을 추가합니다.

- **IP Address(IP** 주소**)** — 다음 홉 IP 주소를 입력합니다.
- **Sequence(**시퀀스**)** — 일련 번호를 사용하여 순서대로 항목을 평가합니다. 중복된 시퀀스 번호가 입력되지 않았는지 확인합니다. 유효한 범위는 1 ~65535입니다.
- **Track(**추적**)** - 유효한 ID를 입력합니다. 유효한 범위는 1~255입니다.

k) **Save(**저장**)**를 클릭합니다.

단계 **8** 정책을 저장하려면 **Save** 및 **Deploy(**구축**)**를 클릭합니다.

---

threat defense는 ACL을 사용하여 트래픽을 일치시킨 다음 이 트래픽에서 라우팅 작업을 수행합니다. 일반적으로 트래픽이 일치하는 ACL을 지정하는 경로 맵을 구성한 다음 해당 트래픽에 대해 하나 이상의 작업을 지정합니다. 경로 모니터링을 사용하여 PBR은 이제 트래픽 라우팅에 가장 적합한 이그레스 인터페이스를 선택할 수 있습니다. 마지막으로, 모든 수신 트래픽에 PBR을 적용할 인터페이스에 경로 맵을 연결합니다.

경로 모니터링 대시보드 추가

경로 모니터링 메트릭을 보려면 디바이스의 상태 모니터링 페이지에 경로 모니터링 대시보드를 추가해야 합니다.

프로시저

단계 **1** **System(**시스템**)** > **Health(**상태**)** > **Monitor(**모니터**)**를 선택합니다.

단계 **2** 디바이스를 선택하고 **Add New Dashboard(**새 대시보드 추가**)**를 클릭합니다.

단계 **3** **Correlate Metrics(**상관 메트릭**)** 대화 상자의 드롭다운 목록에서 **Interface - Path Metrics(**인터페이스 - 경로 메트릭**)**를 선택합니다.

단계 **4** **Show Details(**세부 정보 표시**)** 링크를 클릭합니다. 여기에서 대시보드의 맞춤형 이름을 입력할 수 있습니다. 기본적으로 4개의 메트릭이 모두 선택되어 대시보드에서 포틀릿으로 표시됩니다. **Delete(**삭제**)** ( )를 클릭하여 제외할 수 있습니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

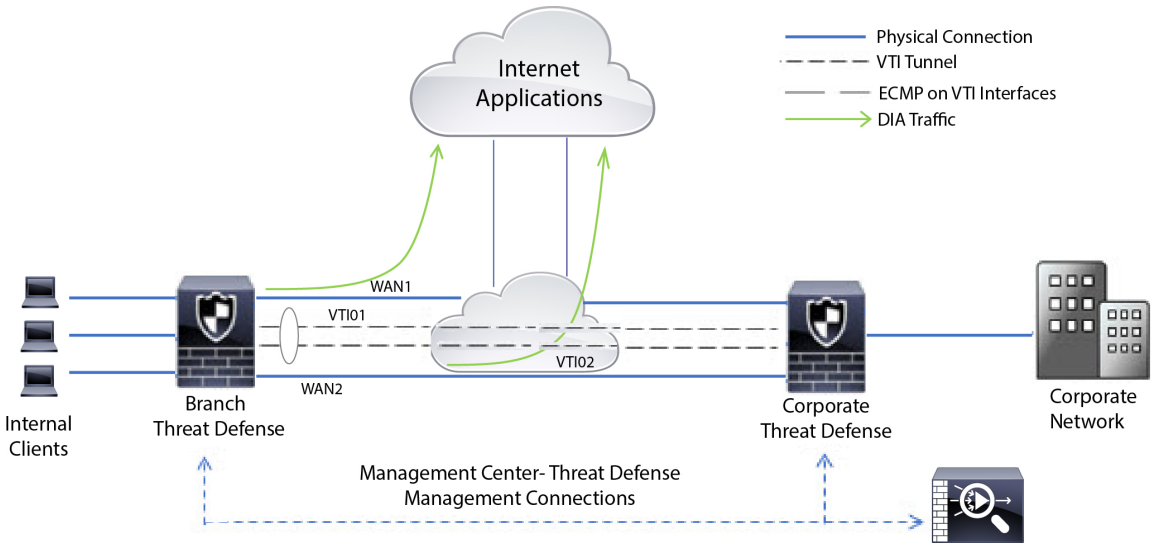
정책 기반 라우팅 컨피그레이션 예

모든 브랜치 네트워크 트래픽이 회사 네트워크의 경로 기반 VPN을 통과하고 필요한 경우 엑스트라넷으로 분기하는 일반적인 회사 네트워크 시나리오를 고려해 보십시오. 기업 네트워크를 통해 일상적인 작업을 처리하는 웹 기반 애플리케이션에 액세스하면 막대한 네트워크 확장 및 유지 보수 비용이 발생합니다. 이 예에서는 직접 인터넷 액세스를 위한 PBR 구성 절차를 보여줍니다.

다음 그림에는 기업 네트워크의 토폴로지가 나와 있습니다. 브랜치 네트워크는 경로 기반 VPN을 통해 기업 네트워크에 연결됩니다. 일반적으로 회사 threat defense는 브랜치 오피스의 내부 및 외부 트래픽을 모두 처리하도록 구성됩니다. PBR 정책을 사용하면 특정 트래픽을 가상 터널 대신 WAN 네트워크로 라우팅하는 정책으로 브랜치 threat defense가 구성됩니다. 나머지 트래픽은 평소와 같이 경로 기반 VPN을 통해 흐릅니다.

이 예에서는 로드 밸런싱을 위해 ECMP 영역을 사용하여 WAN 및 VTI 인터페이스를 구성하는 방법도 보여줍니다.

그림 ***1: Management Center***의 브랜치 ***Threat Defense***에서 정책 기반 라우팅 구성



시작하기 전에

이 예에서는 management center의 브랜치 threat defense에 대해 WAN 및 VTI 인터페이스를 이미 구성했다고 가정합니다.

프로시저

단계 **1** 브랜치 threat defense에 대한 정책 기반 라우팅을 구성하고 인그레스 인터페이스를 선택합니다.

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

b) **Routing(**라우팅**)** > **Policy Based Routing(**정책 기반 라우팅**)**을 선택하고 **Policy Based Routing(**정책 기반 라우팅**)** 페이지에서 **Add(**추가**)**를 클릭합니다.

c) **Add Policy Based Route(**정책 기반 경로 추가**)** 대화 상자의 **Ingress Interface(**인그레스 인터페이스**)** 드롭다운 목록에서 *Inside 1(*내부 *1)* 및 *Inside 2(*내부 *2)*를 선택합니다.

단계 **2** 일치 기준을 지정합니다.

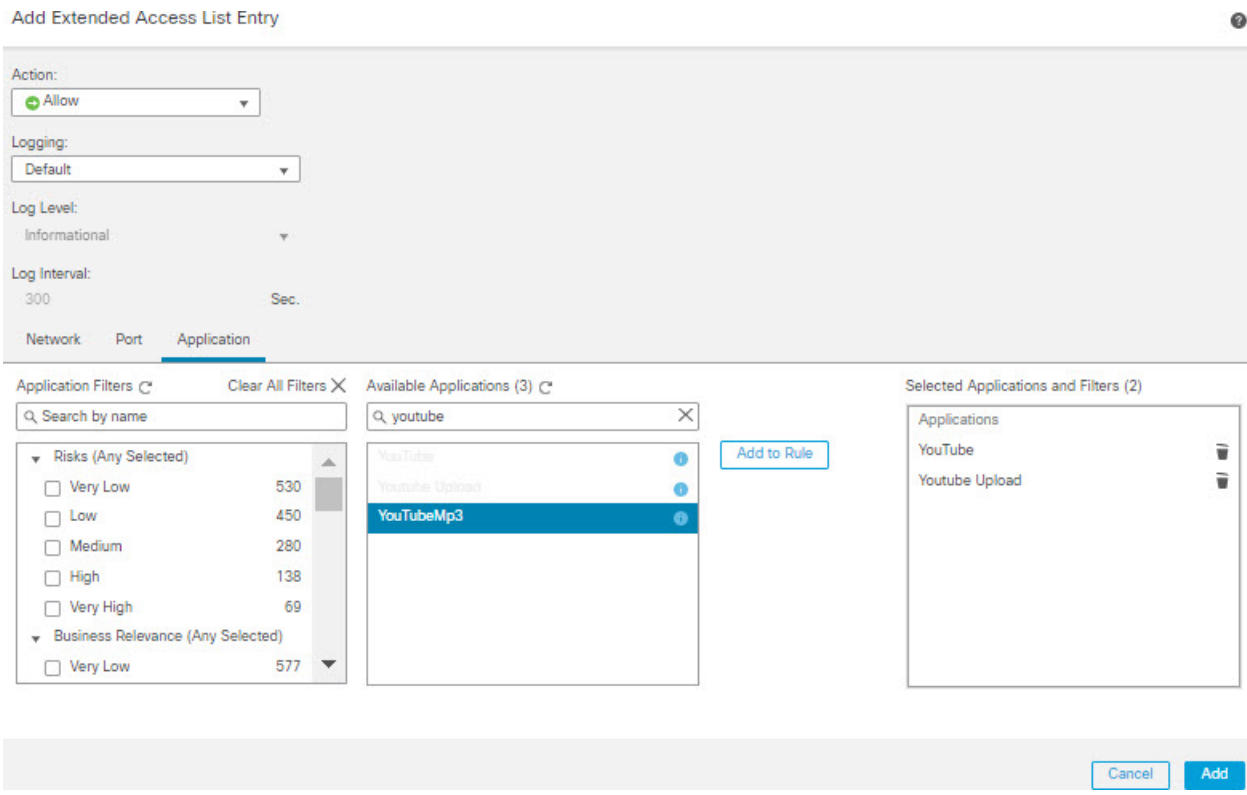
a) **Add(**추가**)**를 클릭합니다.

b) 일치 기준을 정의하려면 **Add(**추가**)** (+) 버튼을 클릭합니다.

c) **New Extended Access List Object(**새 확장 액세스 목록 개체**)**에서 ACL의 이름(예: *DIA-FTD-Branch*)을 입력하고 **Add(**추가**)**를 클릭합니다.

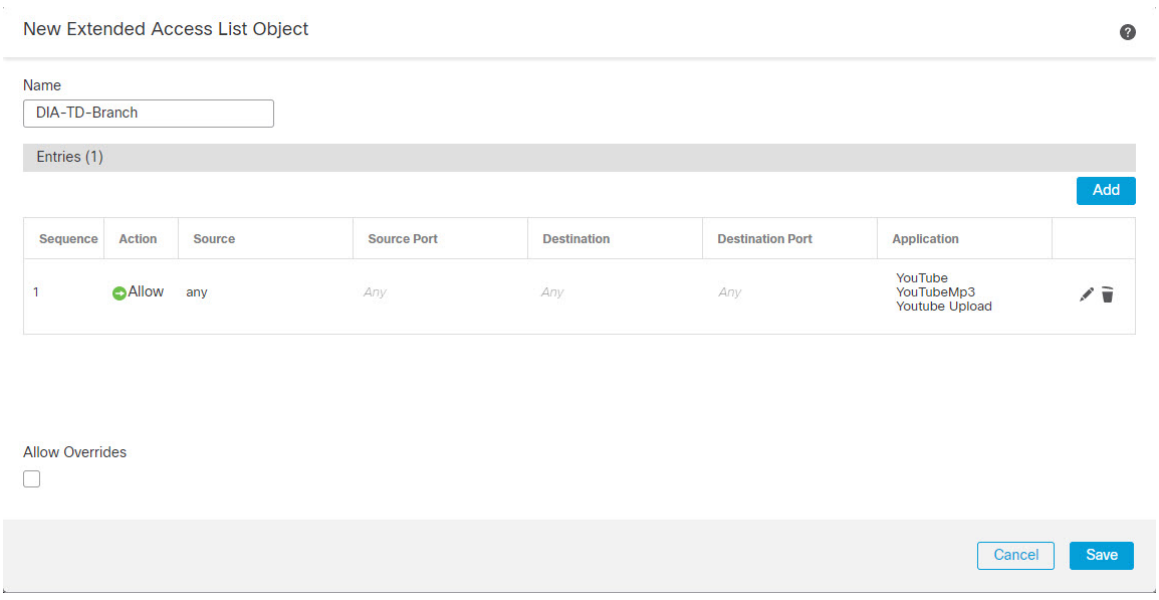
d) **Add Extended Access List Entry(**확장 액세스 목록 항목 추가**)** 대화 상자의 **Application(**애플리케이션**)** 탭에서 필요한 웹 기반 애플리케이션을 선택합니다.

그림 ***2: Applications(***애플리케이션***)*** 탭



threat defense에서 ACL의 애플리케이션 그룹은 네트워크 서비스 그룹으로 구성되고 각 애플리케이션은 네트워크 서비스 개체로 구성됩니다.

그림 ***3:*** 확장된 ***ACL***



e) **Save(**저장**)**를 클릭합니다.

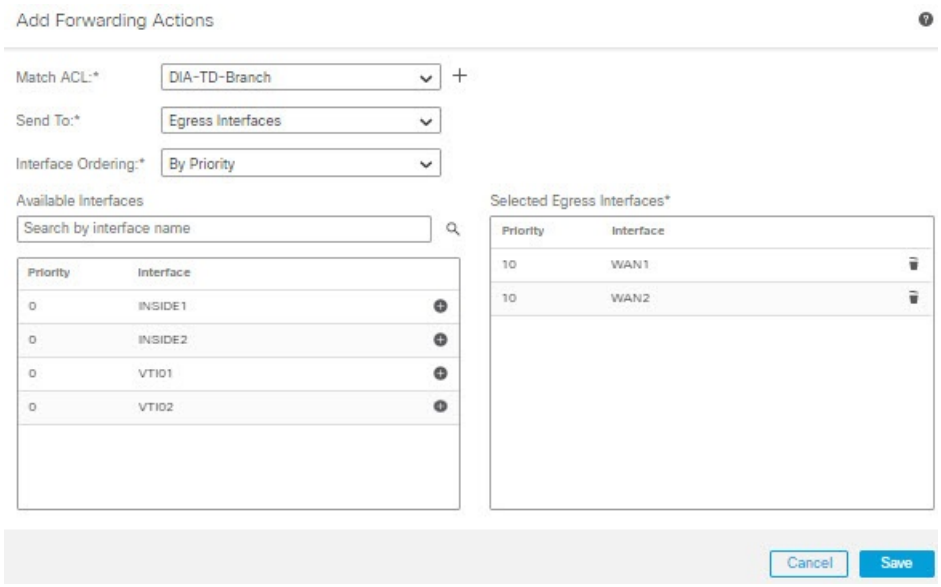
f) **Match ACL(ACL** 일치**)** 드롭다운 목록에서 *DIA-FTD-Branch*를 선택합니다.

단계 **3** 이그레스 인터페이스를 지정합니다.

a) **Send To(**전송 대상**)** 및 **Interface Ordering(**인터페이스 순서 지정**)** 드롭다운 목록에서 각각 Egress Interfaces(이그레스 인터페이스) 및 By Priority(우선 순위 기준)를 선택합니다.

b) **Available Interfaces(**사용 가능한 인터페이스**)**아래에서 각 인터페이스 이름 옆에 있는 ⊕ 버튼을 클릭하여 *WAN1*및 *WAN2*를 추가합니다.

그림 ***4:*** 정책 기반 라우팅 구성



c) **Save(**저장**)**를 클릭합니다.

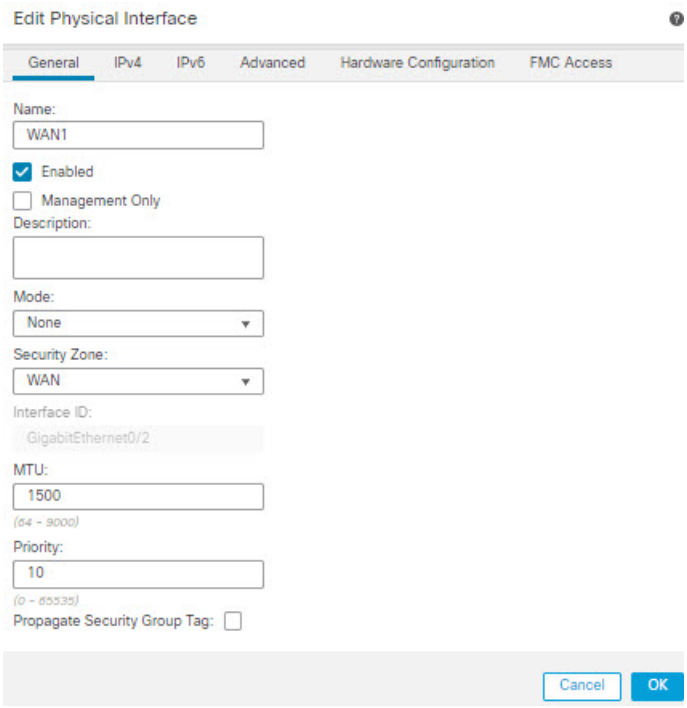
단계 **4** 인터페이스 우선순위 구성:

Edit Physical Interface(물리적 인터페이스 편집**)** 페이지 또는 **Policy Based Routing(**정책 기반 라우팅**)** 페이지(**Configure Interface Priority(**인터페이스 우선순위 구성**)**)에서 인터페이스에 대한 우선순위 값을 설정할 수 있습니다. 이 예에서는 Edit Physical Interface(물리적 인터페이스 편집) 방법에 대해 설명합니다.

a) **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 브랜치 threat defense를 편집합니다.

b) 인터페이스의 우선순위를 설정합니다. 인터페이스에 대해 **Edit(**편집**)**를 클릭하고 우선순위 값을 입력합니다.

그림 ***5:*** 인터페이스 우선순위 설정



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

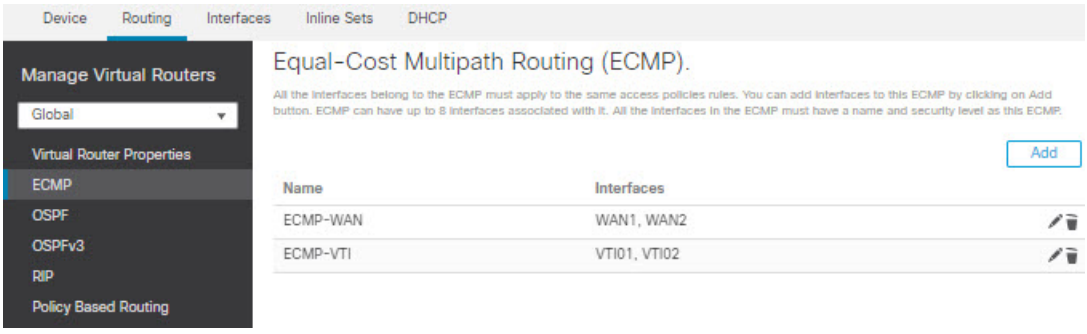
단계 **5** 로드 밸런싱을 위한 ECMP 영역을 생성합니다.

a) **Routing(**라우팅**)** 페이지에서 **ECMP**를 클릭합니다.

b) 인터페이스를 ECMP 영역에 연결하려면 **Add(**추가**)**를 클릭합니다.

c) *WAN1* 및 *WAN 2*를 선택하고 ECMP 영역(*ECMP-WAN*)을 생성합니다. 마찬가지로, *VTI01* 및 *VTI02*를 추가하고 ECMP 영역(*ECMP-VTI*)을 생성합니다.

그림 ***6: ECMP*** 영역과 인터페이스 연결

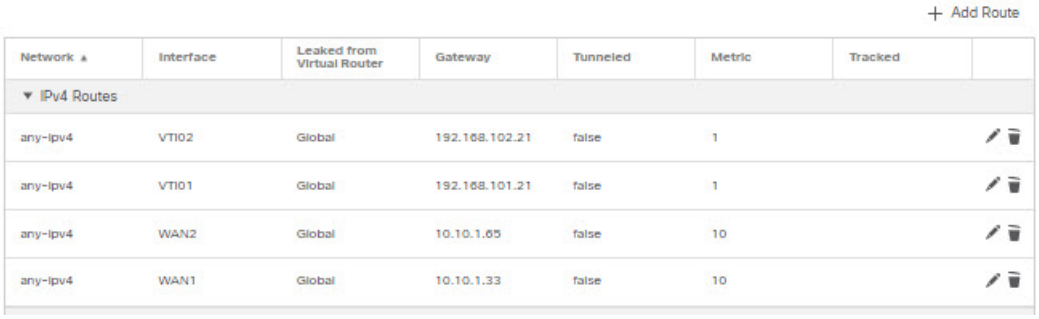


단계 **6** 로드 밸런싱을 위해 영역 인터페이스에 대한 고정 경로를 구성합니다.

a) **Routing(**라우팅**)** 페이지에서 **Static Route(**고정 경로**)**를 클릭합니다.

b) **Add(**추가**)**를 클릭하고 *WAN1*, *WAN2*, *VTI01* 및 *VTI02*에 대한 고정 경로를 지정합니다. 동일한 ECMP 영역에 속한 인터페이스에 대해 동일한 메트릭 값을 지정해야 합니다(단계 5).

그림 ***7: ECMP*** 영역 인터페이스에 대한 고정 경로 구성



참고 영역 인터페이스의 대상 주소와 메트릭은 동일하지만 게이트웨이 주소는 서로 다른지 확인합니다.

단계 **7** 인터넷에 대한 트래픽의 보안 흐름을 보장하기 위해 브랜치 threat defense의 WAN 개체에서 신뢰할 수 있는 DNS를 구성합니다.

a) **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 브랜치 threat defense에서 DNS 정책을 생성합니다.

b) 신뢰할 수 있는 DNS를 지정하려면 정책을 편집하고 **DNS**를 클릭합니다.

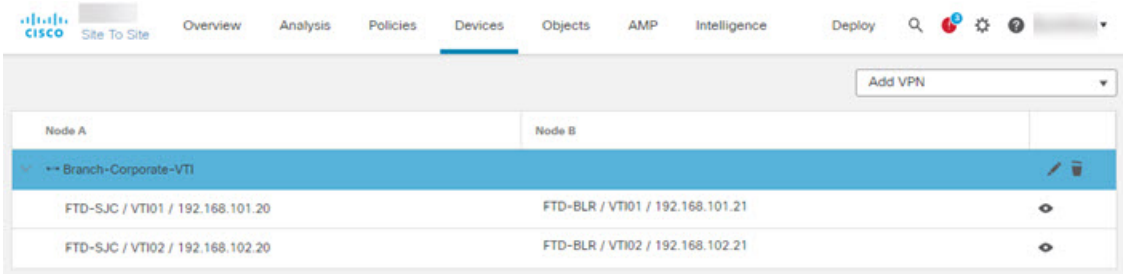
c) WAN 개체에서 사용할 DNS 확인에 대한 DNS 서버를 지정하려면 **DNS Settings(DNS** 설정**)** 탭에서 DNS 서버 그룹 세부 정보를 제공하고 인터페이스 개체에서 WAN을 선택합니다.

d) **Trusted DNS Servers(**신뢰할 수 있는 **DNS** 서버**)** 탭을 사용하여 DNS 확인을 위해 신뢰할 수 있는 특정 DNS 서버를 제공합니다.

단계 **8** **Save(**저장**)**하고 **Deploy(**구축**)**합니다.

네트워크 *INSIDE1* 또는 *INSIDE2* 내부 브랜치의 *YouTube* 관련 액세스 요청은 *DIA-FTD*-브랜치 ACL과 일치하므로 *WAN1* 또는 *WAN2*로 라우팅됩니다. *google.com*과 같은 다른 요청은 사이트 간 VPN 설정에 구성된 대로 *VTI01* 또는 *VTI02*를 통해 라우팅됩니다.

그림 ***8:*** 사이트 간 ***VPN*** 설정



ECMP가 구성되면 네트워크 트래픽이 원활하게 균형을 유지합니다.

경로 모니터링을 사용하는 PBR에 대한 구성 예

이 예에서는 유연한 메트릭을 사용하여 다음 애플리케이션에 대한 경로 모니터링을 사용하는 PBR의 구성을 자세히 설명합니다.

- 지터가 있는 오디오 또는 비디오 민감한 애플리케이션(예: WebEx Meetings).
- RTT를 사용하는 클라우드 기반 애플리케이션(예: Office365)
- 패킷 손실을 사용하는 네트워크 기반 액세스 제어(특정 소스 및 대상 포함).

시작하기 전에

1. 이 예에서는 사용자가 PBR에 대한 기본 구성 단계를 알고 있다고 가정합니다.
2. 논리적 이름으로 인그레스 및 이그레스 인터페이스를 구성했습니다. 이 예에서 인그레스 인터페이스의 이름은 *Inside1*이고, 이그레스 인터페이스의 이름은 *ISP01*, *ISP02* 및 *ISP03*입니다.

프로시저

단계 **1** 인터페이스 *ISP01*, *ISP02* 및 *ISP03*의 경로 모니터링 구성:

이그레스 인터페이스에서 메트릭 수집의 경우, 해당 인터페이스에서 경로 모니터링을 활성화하고 구성해야 합니다.

a) **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 threat defense를 편집합니다.
b) **Interfaces(**인터페이스**)** 탭에서 인터페이스를 수정합니다(이 예에서는 *ISP01*).
c) **Path Monitoring(**경로 모니터링**)** 탭을 클릭하고 **Enable Path Monitoring(**경로 모니터링 활성화**)** 확인란을 선택한 다음 모니터링 유형을 지정합니다(경로 모니터링 설정 구성, 5 페이지 참조).
d) **Ok(**확인**)**를 클릭하고 **Save(**저장**)**를 클릭합니다.
e) 동일한 단계를 반복하고 *ISP02* 및 *ISP03*에 대한 경로 모니터링 설정을 구성합니다.

단계 **2** 조직 threat defense의 브랜치에 대한 정책 기반 라우팅을 구성하고 인그레스 인터페이스를 선택합니다.

a) **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 threat defense 디바이스를 편집합니다.
b) **Routing(**라우팅**)** > **Policy Based Routing(**정책 기반 라우팅**)**을 선택하고 **Policy Based Routing(**정책 기반 라우팅**)** 페이지에서 **Add(**추가**)**를 클릭합니다.
c) **Add Policy Based Route(**정책 기반 경로 추가**)** 대화 상자의 **Ingress Interface(**인그레스 인터페이스**)** 드롭다운 목록에서 *Inside 1(*내부 *1)*을 선택합니다.

단계 **3** 일치 기준을 지정합니다.

a) **Add(**추가**)**를 클릭합니다.
b) 일치 기준을 정의하려면 **Add(**추가**)** (+) 버튼을 클릭합니다.

c) **New Extended Access List Object(**새 확장 액세스 목록 개체**)**에서 ACL의 이름(예: *PBR-WebEx*)을 입력하고 **Add(**추가**)**를 클릭합니다.

d) **Add Extended Access List Entry(**확장 액세스 목록 항목 추가**)** 대화 상자의 **Application(**애플리케이션**)** 탭에서 필요한 웹 기반 애플리케이션(예: WebEx Meetings)을 선택합니다.

기억 threat defense에서 ACL의 애플리케이션 그룹은 네트워크 서비스 그룹으로 구성되고 각 애플리케이션은 네트워크 서비스 개체로 구성됩니다.

e) **Save(**저장**)**를 클릭합니다.

f) **Match ACL(ACL** 일치**)** 드롭다운 목록에서 *PBR-WebEx*를 선택합니다.

단계 **4** 이그레스 인터페이스를 지정합니다.

a) **Send To(**전송 대상**)** 드롭다운 목록에서 Egress Interfaces(이그레스 인터페이스)를 선택합니다.

b) **Interface Ordering(**인터페이스 순서 지정**)** 드롭다운 목록에서 By Minimum Jitter(최소 지터 기준)를 선택합니다.

c) **Available Interfaces(**사용 가능한 인터페이스**)** 아래에서 각 인터페이스 이름에 대한 **Right Arrow(**오른쪽 화살표**)** (>) 버튼을 클릭하여 *ISP01*, *ISP02* 및 *ISP03*을 추가합니다.

d) **Save(**저장**)**를 클릭합니다.

단계 **5** 2단계와 3단계를 반복하여 동일한 인터페이스(*Inside1*)에 대해 PBR을 생성하여 Office365 및 네트워크 기반 액세스 제어 트래픽을 라우팅합니다.

a) 일치 기준 개체(예: *PBR-Office365*)를 생성하고 **Application(**애플리케이션**)** 탭에서 Office365 애플리케이션을 선택합니다.

b) **Interface Ordering(**인터페이스 순서**)** 드롭다운 목록에서 By Minimum Roundtrip Time(최소 라운드트립 시간 기준)을 선택합니다.

c) 이그레스 인터페이스 *ISP01*, *ISP02* 및 *ISP03*을 지정하고 **Save(**저장**)**를 클릭합니다.

d) 이제 일치 기준 개체(예: *PBR-networks*)를 생성하고 **Network(**네트워크**)** 탭에서 소스 및 대상 인터페이스를 지정합니다.

e) **Interface Ordering(**인터페이스 순서 지정**)** 드롭다운 목록에서 By Minimum Packet Loss(최소 패킷 손실 기준)를 선택합니다.

f) 이그레스 인터페이스 *ISP01*, *ISP02* 및 *ISP03*을 지정하고 **Save(**저장**)**를 클릭합니다.

단계 **6** **Save(**저장**)**하고 **Deploy(**구축**)**합니다.

단계 **7** 경로 모니터링 메트릭을 보려면 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 추가 (⋮)에서 **Health Monitor(**상태 모니터**)**를 클릭합니다. 디바이스의 인터페이스에 대한 메트릭 세부 정보를 보려면 경로 메트릭 대시보드를 추가해야 합니다. 자세한 내용은 경로 모니터링 대시보드 추가 , 9 페이지를 참조하십시오.

WebEx, Office365 및 네트워크 기반 ACL 트래픽은 *ISP01*, *ISP02* 및 *ISP03*에서 수집된 메트릭 값에서 파생된 최적의 경로를 통해 전달됩니다.

Secure Firewall Threat Defense의 정책 기반 라우팅 내역

기능	버전	세부 사항
듀얼 WAN/ISP 위협 방어 관리 지원	7.3	듀얼 WAN 지원 위협 방어에서 단일 데이터 인터페이스가 관리 센터와 통신하도록 구성되었습니다. 이제 기본 데이터 인터페이스에 장애가 발생해도 통신 채널이 유지되도록 보조 데이터 인터페이스를 구성할 수 있습니다. 관리 센터는 우선순위 및 SLA 메트릭을 기반으로 SF 터널 트래픽을 *tapnlp*(내부) 인터페이스에서 사용 가능한 데이터 인터페이스 중 하나로 라우팅하도록 PBR을 자동 구성합니다. 신규/수정된 화면 없음. 그러나 구축 검증이 추가되었습니다.
PBR 경로 맵에 대한 다음 홉 설정	7.3	패킷 전달 작업을 활성화하는 동안 PBR 경로 맵에 대한 다음 홉을 구성할 수 있습니다. 신규/수정된 화면: 이그레스 인터페이스 구성을 위한 Add/Edit Forwarding Actions(전달 작업 추가/수정) 페이지의 새 필드: **Device Management(**디바이스 관리**)** > **Routing(**라우팅**)** > **Policy Based Routing(**정책 기반 라우팅**)** > **Add Forwarding Actions(**전달 작업 추가**)** 페이지.
PBR 및 경로 모니터링	7.2	PBR은 경로 모니터링을 사용하여 이그레스 인터페이스의 성능 메트릭(RTT, 지터, 패킷 손실 및 MOS)을 수집합니다. 인터페이스에 대한 경로 모니터링을 활성화하고 모니터링 유형을 구성해야 합니다. 경로 결정을 위해 원하는 메트릭으로 PBR 정책을 구성할 수 있습니다. 신규/수정된 화면: 경로 모니터링 활성화를 위한 Interfaces(인터페이스) 페이지의 새 탭: **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Edit Interfaces(**인터페이스 편집**)** > **Path Monitoring(**경로 모니터링**)** 탭
Policy Based Routing (PBR)	7.1	애플리케이션을 기반으로 네트워크 트래픽을 분류하기 위해 management center를 통한 정책 기반 라우팅이 도입되었습니다. PBR 정책을 정의하고 인그레스 인터페이스에서 구성할 수 있습니다. 일치 기준 및 이그레스 인터페이스를 지정할 수 있습니다. ACL 목록과 일치하는 네트워크 트래픽은 정책에 구성된 우선순위 또는 순서에 따라 이그레스 인터페이스를 통해 전달됩니다. 신규/수정된 화면: 정책 기반 라우팅 정책을 구성하기 위한 새 정책 페이지: **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Routing(**라우팅**)** > **Policy Based Routing(**정책 기반 라우팅**)** 페이지 지원되는 플랫폼: threat defense