DIA(Direct Internet Access)를 사용하여 브랜치에서 인터넷으로 애플리케이션 트래픽 라우팅

이 장에서는 두 가지 활용 사례를 사용하여 DIA(Direct Internet Access)를 실제로 적용하는 방법을 살펴봅니다. 각 활용 사례에서는 시나리오, 네트워크 토폴로지, 모범 사례, 사전 요건에 대해 자세히 설명합니다. 또한 원활한 구현을 위한 포괄적인 엔드 투 엔드 절차를 제공합니다.

직접 인터넷 액세스

디지털 혁신은 기업이 운영하고, 커뮤니케이션하고, 고객과 상호 작용하는 방식을 혁신하고 있습니다. 이제는 협업 및 고객 경험을 개선하며 높은 대역폭 및 낮은 레이턴시 연결이 요구되는 새로운 애플리케이션 및 기술이 생성되었습니다.

기존 네트워크의 당면 과제

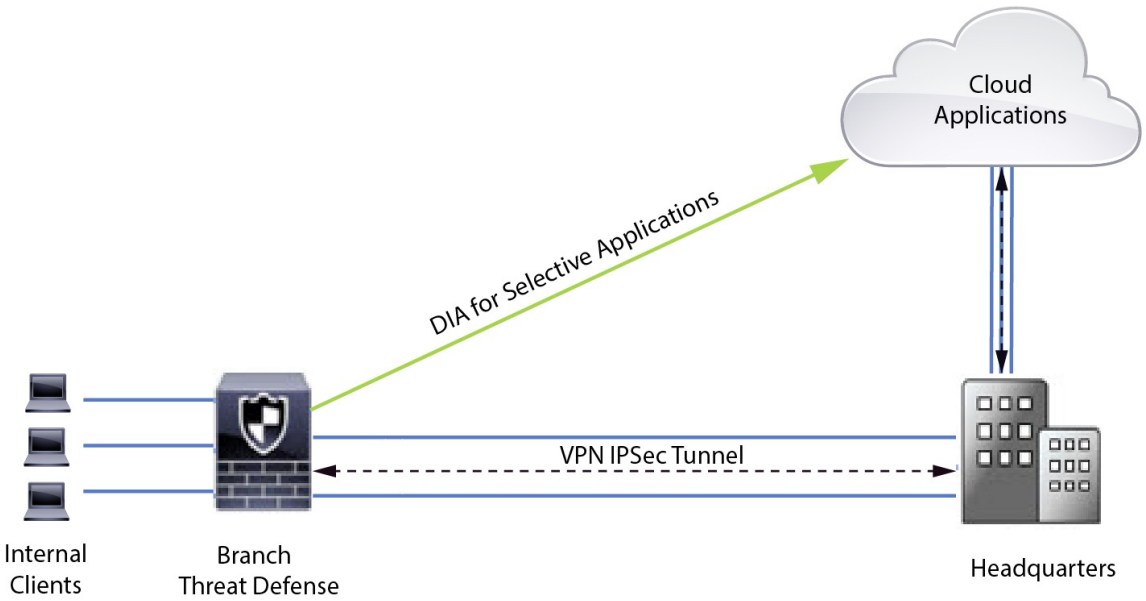
일반적으로 네트워크 구축은 중앙 사이트의 경계 방화벽을 활용하여 로컬 및 브랜치 사용자에 대한 보안 액세스를 제공합니다. 이 아키텍처는 원하는 연결성을 제공하지만, 모든 인터넷 트래픽을 VPN 터널을 통해 암호화된 트래픽으로 중앙 사이트에 전송하므로 패킷 레이턴시, 삭제 및 지터가 발생합니다. 또한, 네트워크는 높은 비용과 대역폭 사용률로 인해 구축 및 복잡한 네트워크 관리와 관련된 문제를 지속적으로 해결해야 합니다.

솔루션

이러한 문제를 해결하는 방법 중 하나는 DIA(직접 인터넷 액세스)를 사용하는 것입니다. DIA는 Cisco Secure Firewall의 브랜치 간소화 기능의 구성 요소입니다. DIA는 정책 기반 라우팅(PBR)을 사용합니다. DIA는 애플리케이션 인식 라우팅이라고도 합니다.

DIA 토폴로지에서는 브랜치 오피스의 애플리케이션 트래픽이 인터넷으로 직접 라우팅되므로 인터넷 바인딩 트래픽을 본사로 터널링하는 레이턴시를 우회합니다. Secure Firewall Threat Defense 브랜치는 인터넷 종료점을 포함하여 구성되어 있습니다. PBR 정책은 확장된 액세스 제어 목록에 정의된 애플리케이션을 기반으로 트래픽을 식별하기 위해 인그레스 인터페이스에 적용됩니다. 따라서 트래픽은 이그레스 인터페이스를 통해 인터넷으로 직접 전달됩니다.

그림 *1:* 특정 이그레스 인터페이스를 통한 직접 인터넷 액세스



정책 기반 라우팅을 사용하는 이유

PBR을 사용하여 지정된 애플리케이션에 대한 트래픽을 분류하고 안전하게 분할할 수 있습니다. 또한 특정 트래픽에 대한 경로를 지정할 수 있습니다. Secure Firewall Management Center 사용자 인터페이스에서 애플리케이션이 직접 액세스하도록 허용하는 PBR 정책을 구성할 수 있습니다.

PBR 및 경로 모니터링

일반적으로 PBR에서 트래픽은 구성된 우선순위 값(인터페이스 비용)에 따라 이그레스 인터페이스를 통해 전달됩니다. Secure Firewall Management Center 버전 7.2 이상 버전에서 PBR은 경로 모니터링을 사용하여 이그레스 인터페이스의 성과 측정(RTT, 지터, 패킷 손실 및 MOS)을 수집합니다. PBR은 메트릭을 사용하여 트래픽을 전달하기 위한 최적의 경로(이그레스 인터페이스)를 결정합니다. 경로 모니터링은 메트릭이 변경되면 모니터링되는 인터페이스에 대해 주기적으로 PBR에 알립니다. PBR은 경로 모니터링 데이터베이스에서 모니터링되는 인터페이스에 대한 최신 메트릭 값을 검색하고 데이터 경로를 업데이트합니다.

인터페이스에 대한 경로 모니터링을 활성화하고, 이그레스 인터페이스의 모니터링 유형을 구성한 후 메트릭 값을 사용하는 경로 모니터링을 활용하도록 애플리케이션 트래픽을 구성해야 합니다.

경로 모니터링에 대한 내용은 시나리오 2: 경로 모니터링을 사용한 직접 인터넷 액세스, 8 페이지의 내용을 참조하십시오.

이점

DIA 사용의 이점은 다음과 같습니다.

- 인터넷 속도 및 브랜치 오피스 사용자 환경을 개선합니다.
- 복잡성 감소로 네트워크 관리를 더 쉽고 저렴하게 할 수 있습니다.
- 대역폭 사용량을 줄이고 고가의 하드웨어가 필요하지 않으므로 비용 효율적입니다.
- 실시간 메트릭을 사용하는 동적 경로 선택합니다.
- 수동 개입 없이 최상의 이그레스 경로가 보장됩니다.
- 링크 상태 및 네트워크 상태에 대한 지속적인 모니터링.
- 민첩성 증가로 조직이 변화하는 비즈니스 요구에 빠르게 적응할 수 있습니다.

이 활용 사례가 귀사에 적합합니까?

이 활용 사례의 대상은 브랜치에서 직접 인터넷 바인딩 트래픽을 로컬로 분리할 수 있도록 각 원격 사이트 내에서 직접 인터넷 액세스를 구현하려는 네트워크 설계 엔지니어, 네트워크 운영 담당자, 보안 운영 담당자입니다.

직접 인터넷 액세스를 위한 구성 요소

브랜치 방화벽이 DIA에 사용하는 몇 가지 중요한 구성 요소는 다음과 같습니다.

- 신뢰할 수 있는 **DNS** 서버 — DIA 기능의 애플리케이션 탐지는 DNS 스누핑을 사용하여 애플리케이션 또는 애플리케이션 그룹을 확인합니다. DNS 요청이 비인가 DNS 서버에 의해 확인되지 않고 원하는 DNS 서버에 고정되도록 하기 위해 관리 센터에서 위협 방어를 위해 신뢰할 수 있는 DNS 서버를 구성할 수 있습니다.
- 인터페이스 우선순위 - Cisco Secure Firewall은 인터페이스 우선순위를 사용하여 최적의 인터넷 경로를 결정합니다. 우선 순위는 낮을수록 트래픽을 인터넷으로 전송할 때 특정 ISP의 기본 설정을 결정합니다. 관리 센터에서 위협 방어의 인터페이스 우선순위를 구성할 수 있습니다.
- 네트워크 서비스 - 정책 기반 라우팅 내에서 사용되는 특정 애플리케이션과 관련된 개체입니다. 이 개체는 자동으로 생성됩니다.
- **NSG(Network Service Group)** - 네트워크 서비스 그룹은 방화벽에서 설정을 기반으로 경로를 결정하는 데 사용하는 애플리케이션 그룹입니다. 여러 네트워크 서비스 개체가 단일 NSG의 일부일 수 있습니다. 관리 센터는 정책 기반 라우팅을 위해 구성된 확장된 액세스 목록을 기반으로 NSG를 자동 생성합니다.

모범 사례

- Secure Firewall Threat Defense는 버전 7.1 이상을 실행해야 합니다.
- 애플리케이션 트래픽 흐름을 지원하기 위해 신뢰할 수 있는 DNS 서버를 통해 DNS 스누핑이 수행되도록 하려면 신뢰할 수 있는 DNS 서버를 구성해야 합니다.
- Threat Defense를 통과하는 DNS 요청은 DNS 스누핑을 통해 PBR 플로우를 지원하도록 암호화되지 않은 일반 텍스트 형식이어야 합니다.
- 애플리케이션 트래픽의 활성/활성 로드 밸런싱을 위해 ECMP 영역을 구성해야 합니다.
- ECMP는 라우팅 방화벽 모드에서만 지원되며, 디바이스는 최대 256개의 ECMP 영역을 가질 수 있습니다.
- 라우팅 인터페이스만 사용해야 합니다. 각 인터페이스는 단일 ECMP 영역에만 속해야 합니다.
- 인터페이스가 ECMP가 구성되는 가상 라우터에 속해 있는지 확인하십시오.
- ECMP 영역 설정에 사용된 인터페이스에는 인터페이스 설정 내에 논리적 이름이 정의되어 있어야 합니다.
- Secure Firewall Threat Defense에서 PBR에 대해 ECMP 영역당 8개의 인터페이스가 구성되어 있는지 확인합니다.
- PBR은 이 모드에서 지원되지 않으므로 Secure Firewall Threat Defense는 클러스터에 구축해서는 안 됩니다.
- PBR은 사용자 정의 가상 라우터에서 지원되지 않으므로 전역 가상 라우터에 대해 구성해야 합니다.
- PBR 내 인그레스 및 이그레스 인터페이스에 사용되는 인터페이스가 라우팅된 인터페이스 또는 관리 전용이 아닌 인터페이스이고, 전역 가상 라우터에 속해 있는지 확인합니다.

사전 요구 사항

- 디바이스 관리자를 사용하여 위협 방어 초기 구성 완료
- 매니지드 디바이스에 라이선스 할당
- 인터넷 액세스용 경로를 추가합니다. 고정 경로 추가를 참조하십시오.
- Threat Defense NAT 구성
- 기본 액세스 제어 정책 만들기

시나리오 1: 직접 인터넷 액세스

Bob은 어카운트 매니저이고 Ann은 헬프데스크 전문가입니다. 두 사람은 모두 대기업의 브랜치 오피스에서 근무합니다. 최근에는 Webex와 같은 웹 컨퍼런싱 툴 및 YouTube 같은 스트리밍 플랫폼을 사용하면서 레이턴시 문제를 경험하고 있습니다.

어떤 위험이 있습니까**?**

네트워크 레이턴시 및 네트워크 혼잡으로 인해 웹 컨퍼런싱 및 스트리밍 세션의 성능 및 사용자 경험이 감소합니다. 이는 브랜치 오피스 직원의 생산성과 효율성에 영향을 미쳐 전체 비즈니스 운영에 부정적인 영향을 미칠 수 있습니다.

PBR이 있는 **DIA**는 이 문제를 어떻게 해결합니까**?**

IT 관리자인 Alice는 네트워크의 레이턴시를 줄이기 위해 DIA와 함께 정책 기반 라우팅을 사용했습니다.

직접 인터넷 액세스를 사용하면 브랜치 오피스가 중앙 사이트나 데이터 센터를 통해 트래픽을 라우팅하지 않고 직접 인터넷에 액세스할 수 있습니다. 그 결과 브랜치 사용자에게 더욱 직접적이고 최적화된 인터넷 연결을 제공하여 레이턴시를 줄였습니다.

정책 기반 라우팅은 서로 다른 이그레스 인터페이스에서 Webex 트래픽과 YouTube 트래픽을 분리했습니다. 이를 통해 트래픽이 다른 경로를 통해 전달되어 단일 인터페이스에 대한 부담이 감소하고 애플리케이션 성능이 향상되었습니다.

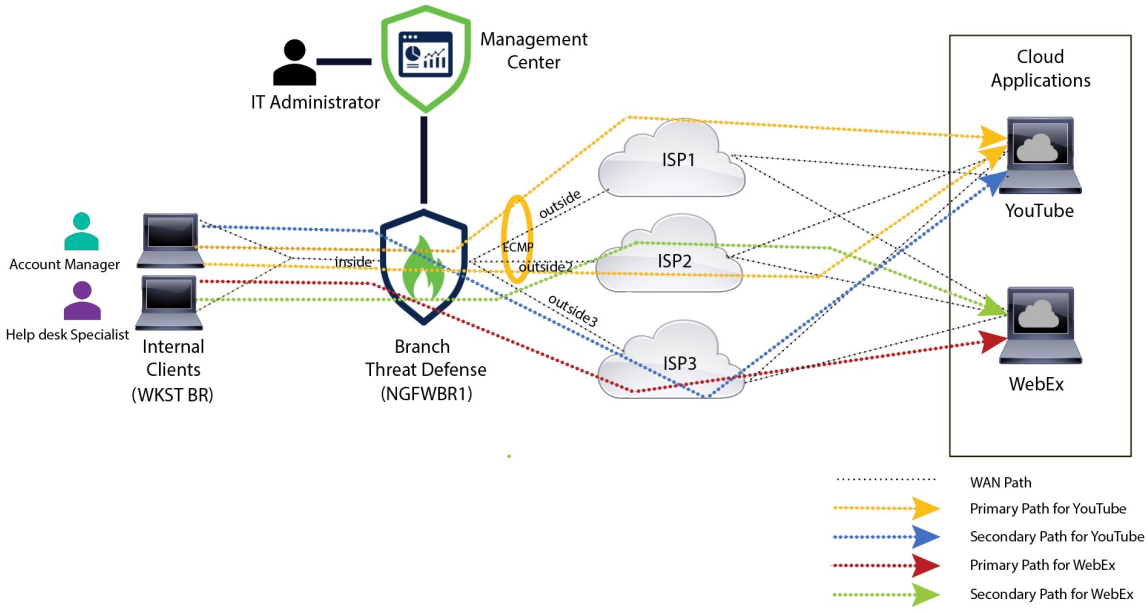
DIA용 네트워크 토폴로지

이 토폴로지에서 위협 방어 디바이스는 3개의 이그레스 인터페이스가 있는 브랜치 위치에 구축됩니다. 디바이스가 PBR을 사용하여 DIA에 대해 구성됩니다.

아래 그림에서 내부 클라이언트 또는 브랜치 워크스테이션은 **WKST BR** 레이블로 표시되고 브랜치 위협 방어는 **NGFWBR1** 레이블로 표시됩니다. **NGFWBR1**의 인그레스 인터페이스는 **inside**로 이름이 지정되고 이그레스 인터페이스는 **outside**, **outside2**, **outside3**으로 각각 지정됩니다.

outside 및 **outside2** 인터페이스 간의 로드 밸런싱은 ECMP 영역 및 정적 경로를 구성하여 수행합니다.

그림 *2:* 직접 인터넷 액세스 토폴로지

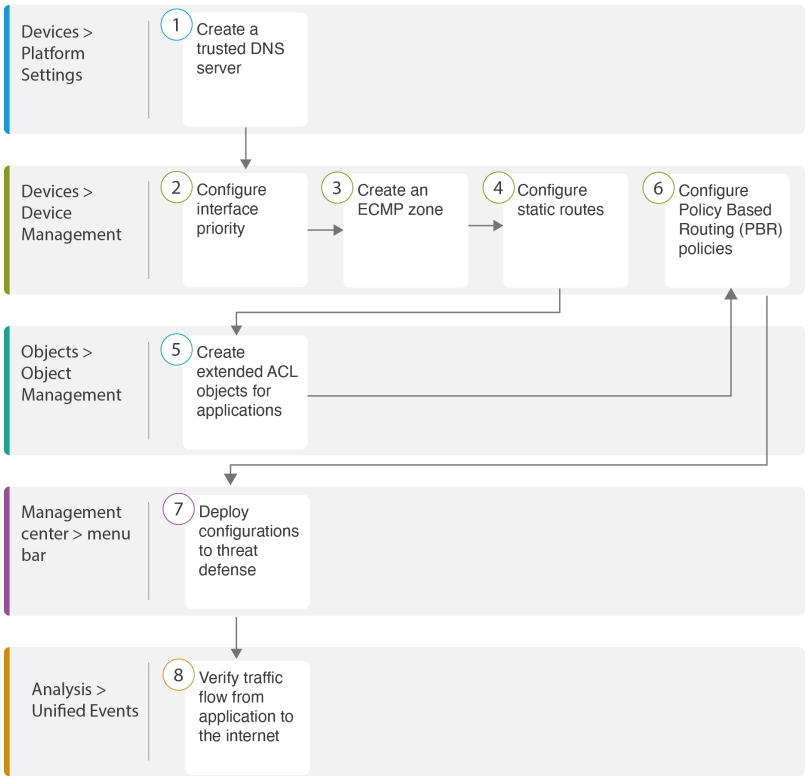


DIA를 사용하면 브랜치 방화벽 뒤에 있는 사용자가 다음에 액세스할 수 있습니다.

1. 2개의 이그레스 인터페이스(**outside** 및 **outside2**)를 사용하여 로드 밸런싱되는 소셜 미디어 애플리케이션 트래픽(예: **YouTube**). 두 인터페이스 모두에서 장애가 발생하면 트래픽은 세 번째 이그레스 인터페이스(**outside3**)로 폴백됩니다.
2. 협업 애플리케이션 트래픽(예: **WebEx**)은 **outside3** 인터페이스를 통해 전달되며 이 링크에 장애가 발생하면 트래픽은 **outside2** 인터페이스를 통해 전달됩니다.

DIA 구성을 위한 엔드 투 엔드 절차

다음 순서도에는 Secure Firewall Management Center에서 DIA 설정을 위한 워크플로우가 나와 있습니다.



단계	설명
1	(사전 요건) 신뢰할 수 있는 DNS 서버를 구성합니다. 신뢰할 수 있는 DNS 서버 구성, 11 페이지의 내용을 참조하십시오.
2	(사전 요건) 인터페이스 우선순위를 구성합니다. 인터페이스 우선순위 설정, 12 페이지의 내용을 참조하십시오.
3	(사전 요건) ECMP 영역을 생성합니다. ECMP 영역 생성, 12 페이지의 내용을 참조하십시오.
4	(사전 요건) 정적 경로를 구성합니다. 동일 비용 정적 경로 구성, 13 페이지의 내용을 참조하십시오.
5	애플리케이션의 확장 ACL 개체를 구성합니다. 확인 • YouTube의 확장 ACL 개체 구성, 14 페이지 • WebEx의 확장 ACL 개체 구성, 15 페이지
6	애플리케이션의 PBR 정책을 구성합니다. 확인 • YouTube용 정책 기반 라우팅 정책 구성, 15 페이지 • WebEx에 대한 정책 기반 라우팅 정책 구성, 16 페이지

단계	설명
7	구성을 위협 방어에 구축합니다. 컨피그레이션 구축, 19 페이지의 내용을 참조하십시오.
8	YouTube 및 WebEx 트래픽 흐름을 확인합니다. 애플리케이션 트래픽 흐름 확인, 19 페이지의 내용을 참조하십시오.

시나리오 2: 경로 모니터링을 사용한 직접 인터넷 액세스

Ann은 헬프데스크 전문가이며 대기업의 지사에서 근무합니다. Ann은 WebEx를 사용하는 동안 연결이 끊기고 지연이 발생하는 문제를 경험했습니다.

어떤 위험이 있습니까?

WebEx 미팅은 미팅 호스트와 참석자 간의 오디오 및 비디오 스트림을 포함한 실시간 데이터 전송을 사용합니다. 이 실시간 데이터는 네트워크 레이턴시 및 패킷 손실에 민감합니다. 네트워크에서 높은 패킷 손실이 발생하는 경우, 중단, 지연과 같은 오디오 및 비디오 품질 문제가 발생하여 미팅 경험에 부정적인 영향을 줄 수 있습니다.

경로 모니터링 기능이 있는 **PBR**이 문제를 어떻게 해결합니까?

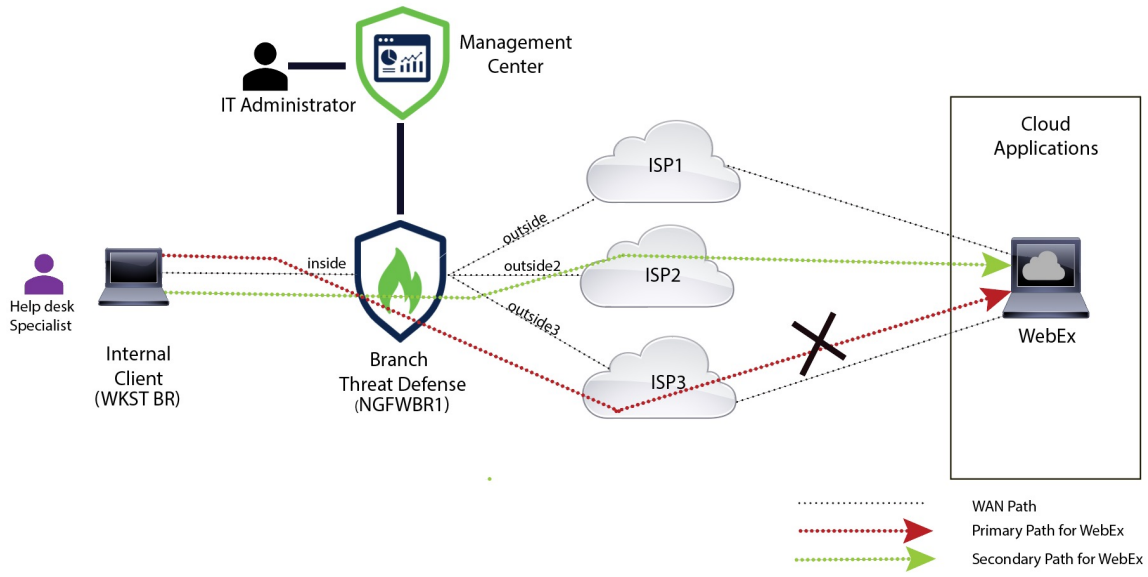
IT 관리자인 Grace는 경로 모니터링이 있는 정책 기반 라우팅을 사용하여 최소한의 패킷 손실로 이그레스 인터페이스를 통해 인터넷으로 WebEx 애플리케이션 트래픽을 조정하여 참석자에게 최상의 미팅 경험을 보장했습니다.

네트워크 토폴로지-DIA(경로 모니터링 포함)

이 토폴로지에서 위협 방어 디바이스는 3개의 이그레스 인터페이스가 있는 브랜치 위치에 구축됩니다. 디바이스가 정책 기반 라우팅을 사용하는 직접 인터넷 액세스용으로 구성되어 있습니다.

아래 그림에서 내부 클라이언트 또는 브랜치 워크스테이션은 **WKST BR** 레이블로 표시되고 브랜치 위협 방어는 **NGFWBR1** 레이블로 표시됩니다. **NGFWBR1**의 인그레스 인터페이스는 **inside**로 이름이 지정되고 이그레스 인터페이스는 **outside**, **outside2**, **outside3**으로 각각 지정됩니다.

그림 ***3:*** 직접 인터넷 액세스 토폴로지*(경로 모니터링 사용)*



outside2 및 **outside3** 이그레스 인터페이스는 경로 모니터링을 통해 활성화됩니다. WebEx용 PBR 정책은 최소한의 패킷 손실로 트래픽이 이그레스 인터페이스로 라우팅되도록 구성됩니다.

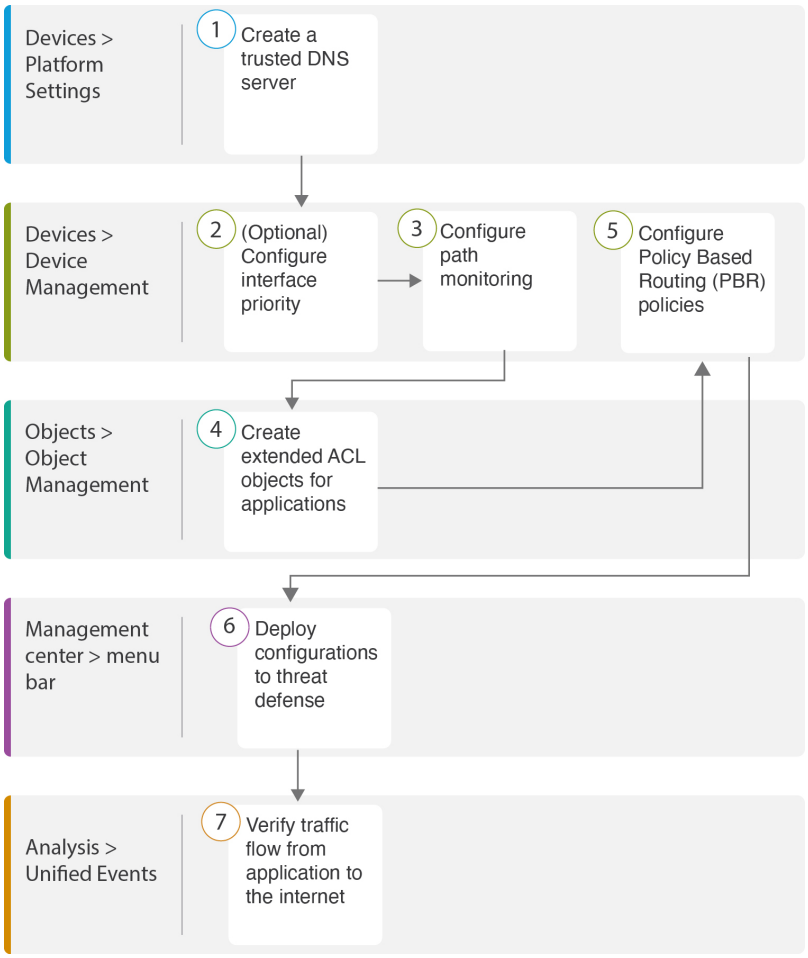
이 시나리오에서는 경로 모니터링을 검증하기 위해 업스트림 디바이스의 액세스 제어 목록을 통해 인터넷으로 이동하는 **outside3** 인터페이스에서 소싱되는 아웃바운드 트래픽을 제한하거나 Firewall Management Center에서 Secure Firewall Threat Defense에 대한 **outside3** 인터페이스를 종료하여 패킷 손실을 유발할 수 있습니다.

참고 인터페이스를 종료하는 것은 네트워크를 방해하므로 프로덕션 네트워크에서 시도해서는 안 됩니다.

패킷 손실의 결과로 **outside3** 인터페이스와 연결된 링크가 중단됩니다. 협업 애플리케이션 트래픽은 **outside3** 인터페이스 대신 **outside2** 인터페이스를 통해 전달됩니다.

경로 모니터링을 통해 **DIA**를 구성하기 위한 엔드 투 엔드 절차

다음 순서도에는 Secure Firewall Management Center에서 경로 모니터링을 사용하여 DIA를 설정하는 워크플로우가 나와 있습니다.



단계	설명
1	(사전 요건) 신뢰할 수 있는 DNS 서버를 구성합니다. 신뢰할 수 있는 DNS 서버 구성, 11 페이지의 내용을 참조하십시오.
2	[사전 요건 (선택 사항)] 인터페이스 우선순위를 구성합니다. 인터페이스 우선순위 설정, 12 페이지의 내용을 참조하십시오.
3	경로 모니터링을 구성합니다. 경로 모니터링 설정 구성, 13 페이지의 내용을 참조하십시오.
4	애플리케이션의 확장 ACL 개체를 구성합니다. WebEx의 확장 ACL 개체 구성, 15 페이지의 내용을 참조하십시오.
5	애플리케이션에 대한 PBR 정책을 구성합니다. Webex용 경로 모니터링을 사용하여 정책 기반 라우팅 정책 구성, 17 페이지의 내용을 참조하십시오.
6	구성을 위협 방어에 구축합니다. 컨피그레이션 구축, 19 페이지의 내용을 참조하십시오.

단계	설명
7	WebEx 트래픽 흐름을 확인합니다. 애플리케이션 트래픽 흐름 확인, 19 페이지의 내용을 참조하십시오.

신뢰할 수 있는 DNS 서버 구성

직접 인터넷 액세스 기능의 애플리케이션 탐지는 DNS 스누핑을 사용하여 애플리케이션 또는 애플리케이션 그룹을 탐지하기 위해 애플리케이션 도메인을 IP에 매핑합니다. DNS 요청이 비인가 DNS 서버에 의해 확인되지 않고 실제로 원하는 DNS 서버에 잠기도록 Cisco Secure Firewall Management Center를 사용하여 Cisco Secure Firewall Threat Defense에 신뢰할 수 있는 DNS 서버를 구성할 수 있습니다. 따라서 방화벽은 신뢰할 수 있는 DNS 서버로 이동하는 트래픽만 스누핑합니다. 신뢰할 수 있는 DNS 서버를 구성하는 것 외에도 DNS 서버 그룹, DHCP 풀, DHCP 릴레이 및 DHCP 클라이언트에 이미 구성된 서버를 신뢰할 수 있는 DNS 서버로 포함할 수 있습니다.

Trusted DNS Servers(신뢰할 수 있는 DNS 서버) 탭을 사용하여 DNS 스누핑에 대해 신뢰할 수 있는 DNS 서비스를 구성할 수 있습니다.

참고 애플리케이션 기반 PBR의 경우 신뢰할 수 있는 DNS 서버를 구성해야 합니다. 또한 도메인을 확인하여 애플리케이션을 탐지할 수 있도록 DNS 트래픽이 일반 텍스트 형식(암호화된 DNS는 지원하지 않음)으로 위협 방어를 통과하는지 확인해야 합니다.

시작하기 전에

- 하나 이상의 DNS 서버 그룹을 만들었는지 확인합니다. 자세한 내용은 DNS 서버 그룹 개체 생성을 참조하십시오.
- DNS 서버에 연결할 인터페이스 개체를 생성했는지 확인합니다.
- 관리 디바이스에 DNS 서버에 액세스하기 위한 적절한 정적 또는 동적 경로가 있는지 확인합니다.

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 위협 방어 정책을 편집합니다.

단계 **2** **Edit(**수정**)** (✎) 아이콘을 클릭합니다.

단계 **3** **DNS**를 클릭합니다.

단계 **4** 신뢰할 수 있는 DNS 서버를 구성하려면 **Trusted DNS Servers(**신뢰할 수 있는 **DNS** 서버**)** 탭을 클릭합니다.

단계 **5** 기존 호스트 개체에서 **DNS_Server**를 선택하려면 **Available Host Objects(**사용 가능한 호스트 개체**)**에서 검색 필드를 사용하여 해당 호스트를 검색하고 **Add(**추가**)**를 클릭하여 **Selected DNS Servers(**선택한 **DNS** 서버**)** 목록에 포함합니다.

참고 **DNS_Server**는 이 예에 구성된 DNS 서버입니다.

단계 **6** **Save(**저장**)**를 클릭합니다. 추가된 DNS 서버가 **Trusted DNS Servers(**신뢰할 수 있는 **DNS** 서버**)** 페이지에 표시됩니다.

단계 **7** **NGFWBR1**이 **Selected Devices(**선택한 디바이스**)** 목록에 이미 있는지 확인하려면 **Policy Assignments(**정책 할당**)**를 클릭합니다.

단계 **8** **OK(**확인**)**를 클릭하여 변경 사항을 확인합니다.

단계 **9** 플랫폼 설정에 대한 변경 사항을 기록하려면 **Save(**저장**)**를 클릭합니다.

인터페이스 우선순위 설정

Cisco Secure Firewall Threat Defense는 인터페이스 우선순위를 사용하여 최적의 인터넷 경로를 결정합니다. 우선순위의 범위는 0~65535이며, 트래픽을 인터넷으로 전송할 때 특정 ISP의 우선순위를 결정합니다. 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 outside2 및 outside3가 우선 순위 값 10과 20으로 각각 설정되어 있다고 가정합니다. 트래픽은 outside2로 전달됩니다. outside2를 사용할 수 없게 되면 트래픽은 outside3으로 전달됩니다.

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 위협 방어 디바이스(**NGFWBR1**)를 편집합니다.

단계 **2** NGFWBR1의 인터페이스 보기에서 **Routing(**라우팅**)** 탭을 클릭합니다.

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

단계 **4** **Configure Interface Priority(**인터페이스 우선순위 구성**)**를 클릭합니다.

단계 **5** 대화 상자에서 인터페이스에 대한 우선순위 번호를 입력합니다.

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

단계 **6** **Save(**저장**)**를 클릭합니다.

ECMP 영역 생성

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 위협 방어 디바이스(**NGFWBR1**)를 편집합니다.

단계 **2** NGFWBR1의 인터페이스 보기에서 **Routing(**라우팅**)** 탭을 클릭합니다.

단계 **3** **ECMP**를 클릭합니다.

단계 **4** **Add(**추가**)**를 클릭합니다.

단계 **5** **Add ECMP(ECMP** 추가**)** 상자에 ECMP 영역의 이름인 **ECMP-WAN**을 입력합니다.

단계 **6** 인터페이스를 연결하려면 **Available Interface(**사용 가능한 인터페이스**)** 상자에서 인터페이스를 선택하고 **Add(**추가**)**를 클릭합니다.

단계 **7** **OK(**확인**)**를 클릭합니다.

이제 ECMP 페이지에 새로 생성된 ECMP 영역이 표시됩니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

동일 비용 정적 경로 구성

전역 및 사용자 정의 가상 라우터의 인터페이스를 디바이스의 ECMP 영역에 할당할 수 있습니다.

시작하기 전에

- 인터페이스에 대해 동일 비용 고정 경로를 구성하려면 이를 ECMP 영역과 연결해야 합니다. ECMP 영역 생성, 12 페이지의 내용을 참조하십시오.
- 인터페이스를 ECMP 영역과 연결하지 않고는 대상 및 메트릭이 동일한 인터페이스에 대해 정적 경로를 정의할 수 없습니다.

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** 페이지에서 위협 방어 디바이스(**NGFWBR1**)를 편집합니다.

단계 **2** 라우팅 탭을 클릭합니다.

단계 **3** 드롭다운 목록에서 인터페이스가 ECMP 영역과 연결된 가상 라우터를 선택합니다.

단계 **4** 인터페이스에 대해 동일 비용 고정 경로를 구성하려면 **Static Route(**고정 경로**)**를 클릭합니다.

단계 **5** **Add Route(**경로 추가**)**를 클릭하여 새 경로를 추가하거나 기존 경로에 대해 **Edit(**수정**)** ( )를 클릭합니다.

단계 **6** **Interface(**인터페이스**)** 드롭다운에서 가상 라우터 및 ECMP 영역에 속한 인터페이스를 선택합니다.

단계 **7** **Available Networks(**사용 가능한 네트워크**)** 상자에서 대상 네트워크를 선택하고 **Add(**추가**)**를 클릭합니다.

단계 **8** 네트워크의 게이트웨이를 입력합니다.

단계 **9** 메트릭 값을 입력합니다. 1~254 범위의 숫자일 수 있습니다.

단계 **10** 설정을 저장하려면 **Save(**저장**)**를 클릭합니다.

단계 **11** 동일 비용 고정 라우팅을 구성하려면 동일한 대상 네트워크 및 메트릭 값을 사용하여 동일한 ECMP 영역에서 다른 인터페이스에 대한 고정 경로를 구성하는 단계를 반복합니다. 다른 게이트웨이를 제공해야 합니다.

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 프로브를 전송하도록 경로 모니터링에 대한 설정을 사용하여 인터페이스를 구성할 수 있습니다.

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 위협 방어 디바이스(**NGFWBR1**)에 대한 **Edit(**수정**)** ( )를 클릭합니다.

단계 **2** 편집할 인터페이스의 **Edit(**수정**)** ( )을 클릭합니다(외부).

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

단계 **4** **Enable IP based Path Monitoring(IP** 기반 경로 모니터링 활성화**)** 확인란을 선택합니다.

단계 **5** **Monitoring Type(**모니터링 유형**)** 드롭다운 목록에서 관련 옵션을 선택합니다. 이 예시에서는 기본값인 인터페이스에서 기본 경로의 다음 홉**(**자동**)**을 사용합니다.

단계 **6** **Ok(**확인**)**를 클릭합니다.

단계 **7** **outside2** 및 **outside3** 인터페이스에 대해 2 ~ 8단계를 반복합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

YouTube의 확장 ACL 개체 구성

YouTube 트래픽이 정책 기반 라우팅을 사용하여 다른 이그레스 인터페이스에서 인터넷으로 향하도록 조정되도록 액세스 목록이 구성됩니다.

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택하고 목차에서 **Access Lists(**액세스 목록**)** > **Extended(**확장**)**를 선택합니다.

단계 **2** **Add Extended Access List(**확장된 액세스 목록 추가**)**를 클릭하여 소셜 미디어 트래픽에 대한 확장된 액세스 목록을 생성합니다.

단계 **3** Extended ACL Object(확장된 ACL 개체) 대화 상자에서 개체의 이름(**DIA_SocialMedia**)을 입력합니다.

단계 **4** **Add(**추가**)**를 클릭하여 새 확장된 액세스 목록을 생성합니다.

단계 **5** 다음 액세스 제어 속성을 구성합니다.

1. 작업을 선택하여 트래픽 조건을 허용(일치)합니다.
2. **Application(**애플리케이션**)** 탭을 클릭하고 **Available Applications(**사용 가능한 애플리케이션**)** 목록에서 **YouTube**를 검색합니다.
3. **YouTube**를 선택하고 **Add to Rule(**규칙에 추가**)**을 클릭합니다.
4. 개체에 해당 항목을 추가하려면 **Add(**추가**)**를 클릭합니다.
5. **Save(**저장**)**를 클릭합니다.

WebEx의 확장 ACL 개체 구성

WebEx 트래픽이 정책 기반 라우팅을 사용하여 다른 이그레스 인터페이스에서 인터넷으로 향하도록 조정되도록 액세스 목록이 구성됩니다.

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택하고 목차에서 **Access Lists(**액세스 목록**)** > **Extended(**확장**)**를 선택합니다.

단계 **2** **Add Extended Access List(**확장된 액세스 목록 추가**)**를 클릭하여 협업 트래픽에 대한 확장된 액세스 목록을 생성합니다.

단계 **3** Extended ACL Object(확장된 ACL 개체) 대화 상자에서 개체의 이름(**DIA_Collaboration**)을 입력합니다.

단계 **4** **Add(**추가**)**를 클릭하여 새 확장된 액세스 목록을 생성합니다.

단계 **5** 다음 액세스 제어 속성을 구성합니다.

1. 작업을 선택하여 트래픽 조건을 허용(일치)합니다.
2. **Application(**애플리케이션**)** 탭을 클릭하고 **Available Applications(**사용 가능한 애플리케이션**)** 목록에서 **Webex**를 검색합니다.
3. **Webex**를 선택하고 **Add to Rule(**규칙에 추가**)**을 클릭합니다.
4. 개체에 해당 항목을 추가하려면 **Add(**추가**)**를 클릭합니다.
5. **Save(**저장**)**를 클릭합니다.

YouTube용 정책 기반 라우팅 정책 구성

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

YouTube 트래픽은 **outside** 및 **outside2** 인터페이스 간에 로드 밸런싱되고 두 링크 모두 실패하면 **outside3**으로 폴백됩니다.

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 위협 방어 디바이스(**NGFWBR1**)를 편집합니다.

단계 **2** NGFWBR1의 인터페이스 보기에서 **Routing(**라우팅**)** 탭을 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 **Ingress Interface(**인그레스 인터페이스**)** 드롭다운 목록에서 **inside**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 **DIA_SocialMedia**를 선택합니다.

b) 구성된 인터페이스를 선택하려면 **Send To(**전송 대상**)** 드롭다운 목록에서 **Egress Interfaces(**이그레스 인터페이스**)**를 선택합니다.

c) **Interface Ordering(**인터페이스 순서 지정**)** 드롭다운 목록에서 **By Priority(**우선순위별**)**를 선택합니다.

트래픽은 우선 순위 값이 가장 낮은 인터페이스로 라우팅됩니다. 인터페이스를 사용할 수 없는 경우 트래픽은 다음으로 낮은 우선순위 값을 가진 인터페이스로 전달됩니다. 예를 들어 outside2 및 outside3가 우선 순위 값 10과 20으로 각각 설정되어 있다고 가정합니다. 트래픽은 outside2로 전달됩니다. outside2를 사용할 수 없게 되면 트래픽은 outside3으로 전달됩니다.

d) **Available Interfaces(**사용 가능한 인터페이스**)** 상자에 우선순위 값과 함께 모든 인터페이스가 나열됩니다. **Add(**추가**)** (+) 아이콘을 클릭하여 선택한 이그레스 인터페이스를 추가합니다.

이 시나리오의 경우:

1. Available Interfaces(사용 가능한 인터페이스)에서 **outside** 및 **outside2** 인터페이스에 인접한 **Add(**추가**)** (+) 아이콘을 클릭하여 이를 **Selected Egress Interfaces(**선택한 이그레스 인터페이스**)**로 이동합니다.

2. 그런 다음 **outside3** 인터페이스 옆의 **Add(**추가**)** (+) 아이콘을 클릭하여 이를 **Selected Egress Interfaces(**선택한 이그레스 인터페이스**)**로 이동합니다.

e) **Save(**저장**)**를 클릭하여 일치 기준에 대한 변경 사항을 기록합니다.

f) 구성을 검토하고 **Save(**저장**)**를 클릭하여 정책 기반 라우팅에 대한 모든 구성 변경 사항을 씁니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

WebEx에 대한 정책 기반 라우팅 정책 구성

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

WebEx 애플리케이션 트래픽은 **outside3**으로 라우팅되고 기본 링크가 실패하면 **outside2**로 폴백됩니다.

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 위협 방어 디바이스(**NGFWBR1**)를 편집합니다.

단계 **2** NGFWBR1의 인터페이스 보기에서 **Routing(**라우팅**)** 탭을 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 편집하려면 **Edit(**수정**)** (✎) 아이콘을 클릭합니다.

단계 **5** 정책에서 일치 기준 및 전달 작업을 지정하려면 **Add(**추가**)**를 클릭합니다.

단계 **6** **Add Forwarding Actions(**전달 작업 추가**)** 대화 상자에서 다음을 수행합니다.

a) **Match ACL(ACL** 일치**)** 드롭다운에서 **DIA_Coloperation**을 선택합니다.

b) 구성된 인터페이스를 선택하려면 **Send To(**전송 대상**)** 드롭다운 목록에서 **Egress Interfaces(**이그레스 인터페이스**)**를 선택합니다.

c) **Interface Ordering(**인터페이스 순서 지정**)** 드롭다운 목록에서 **Order(**순서**)**를 선택합니다.

여기에 지정된 인터페이스의 순서에 따라 트래픽이 전달됩니다.

d) **Available Interfaces(**사용 가능한 인터페이스**)** 상자에 우선순위 값과 함께 모든 인터페이스가 나열됩니다. **Add(**추가**)** (+) 아이콘을 클릭하여 선택한 이그레스 인터페이스를 추가합니다.

이 시나리오의 경우:

1. Available Interfaces(사용 가능한 인터페이스)에서 **outside3** 인터페이스 옆의 **Add(**추가**)** (+) 아이콘을 클릭하여 이를 **Selected Egress Interfaces(**선택한 이그레스 인터페이스**)**로 이동합니다.
2. 그런 다음 **outside2** 인터페이스에 인접한 **Add(**추가**)** (+) 아이콘을 클릭하여 **Selected Egress Interfaces(**선택한 이그레스 인터페이스**)**로 이동합니다.

e) **Save(**저장**)**를 클릭하여 일치 기준에 대한 변경 사항을 기록합니다.

f) 구성을 검토하고 **Save(**저장**)**를 클릭하여 정책 기반 라우팅에 대한 모든 구성 변경 사항을 씁니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

Webex용 경로 모니터링을 사용하여 정책 기반 라우팅 정책 구성

Policy Based Routing(정책 기반 라우팅) 페이지에서 경로 모니터링을 사용하여 PBR 정책을 구성할 수 있습니다. 이 예에서 WebEx 애플리케이션 트래픽은 트래픽 손실이 가장 적은 인터페이스에 전달됩니다.

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, 13 페이지의 내용을 참조하십시오.

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 위협 방어 디바이스(**NGFWBR1**)를 편집합니다.

단계 **2** NGFWBR1의 인터페이스 보기에서 **Routing(**라우팅**)** 탭을 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 **Ingress Interface(**인그레스 인터페이스**)** 드롭다운 목록에서 **inside**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 **DIA_Coloperation**을 선택합니다.

b) 구성된 인터페이스를 선택하려면 **Send To(**전송 대상**)** 드롭다운 목록에서 **Egress Interfaces(**이그레스 인터페이스**)**를 선택합니다.

c) **Interface Ordering(**인터페이스 순서 지정**)** 드롭다운 목록에서 **Minimal Packet Loss(**최소 패킷 손실**)**를 선택합니다.

트래픽이 패킷 손실이 최소인 인터페이스로 전달됩니다.

d) **Available Interfaces(**사용 가능한 인터페이스**)** 상자에 모든 인터페이스가 나열됩니다. 인터페이스 목록에서 **Add(**추가**)** (+) 아이콘을 클릭하여 선택한 이그레스 인터페이스를 추가합니다.

이 시나리오의 경우:

1. Available Interfaces(사용 가능한 인터페이스)에서 **outside3** 인터페이스 옆의 **Add(**추가**)** (+) 아이콘을 클릭하여 이를 **Selected Egress Interfaces(**선택한 이그레스 인터페이스**)**로 이동합니다.
2. 그런 다음 **outside2** 인터페이스에 인접한 **Add(**추가**)** (+) 아이콘을 클릭하여 **Selected Egress Interfaces(**선택한 이그레스 인터페이스**)**로 이동합니다.

e) **Save(**저장**)**를 클릭하여 일치 기준에 대한 변경 사항을 기록합니다.

f) 구성을 검토하고 **Save(**저장**)**를 클릭하여 정책 기반 라우팅에 대한 모든 구성 변경 사항을 씁니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

컨피그레이션 구축

모든 구성을 완료한 후 매니지드 디바이스에 구축합니다.

단계 **1** 관리 센터 메뉴 바에서 **Deploy(**구축**)**를 클릭합니다.

단계 **2** 구성 변경 사항을 구축할 NGFWBR1 옆의 확인란을 선택합니다.

단계 **3** **Deploy(**구축**)**를 클릭합니다.

단계 **4** 구축할 변경 사항에서 오류나 경고를 식별하면 시스템은 **Validation Messages(**검증 메시지**)** 또는 **Validation Warnings(**검증 경고**)** 창에 이를 표시합니다. 전체 세부 정보를 보려면 Validation Errors(검증 오류) 또는 Validation Warnings(검증 경고) 링크를 클릭합니다.

다음 옵션을 이용할 수 있습니다.

- Proceed with Deploy(구축 계속) - 경고 조건을 해결하지 않고 구축을 계속합니다. 오류가 식별되는 경우 계속 진행할 수 없습니다.
- Close(닫기) -구축하지 않고 종료합니다. 오류 및 경고 조건을 해결하고 컨피그레이션을 재구축합니다.

애플리케이션 트래픽 흐름 확인

단계 **1** 관리 센터 인터페이스에서 **Analysis(**분석**) - Unified Events(**통합 이벤트**)**를 선택합니다.

단계 **2** **Web Application(**웹 애플리케이션**)** 및 **Egress Interface(**이그레스 인터페이스**)**를 선택하고 **Apply(**적용**)**를 클릭하여 열 선택기를 사용하여 열을 맞춤화합니다.

단계 **3** 쉽게 확인할 수 있도록 열 순서를 변경합니다.

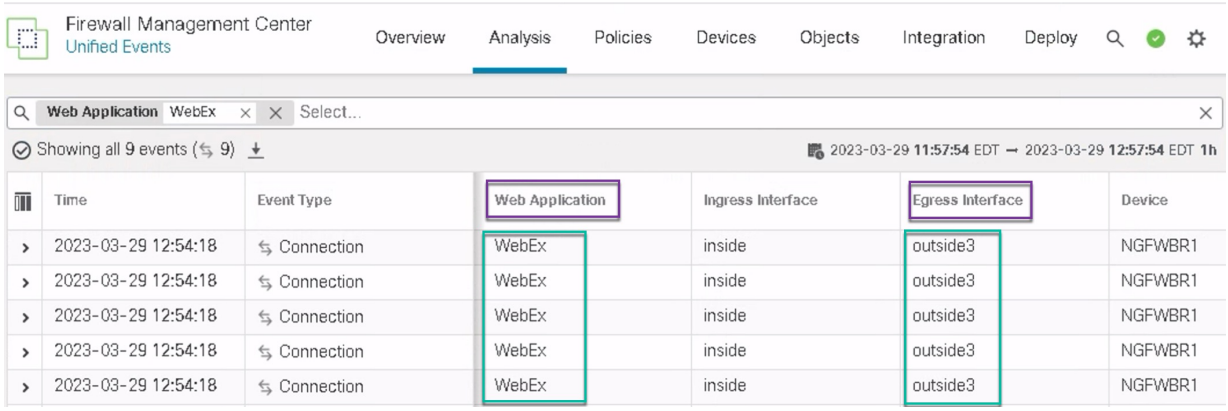
단계 **4** **Web Application(**웹 애플리케이션**)** 필터 내에서 **WebEx** 이름을 입력하고 **Apply(**적용**)**를 클릭합니다.

단계 **5** **Web Application(**웹 애플리케이션**)** 필터 내에서 **YouTube** 이름을 입력하고 **Apply(**적용**)**를 클릭합니다.

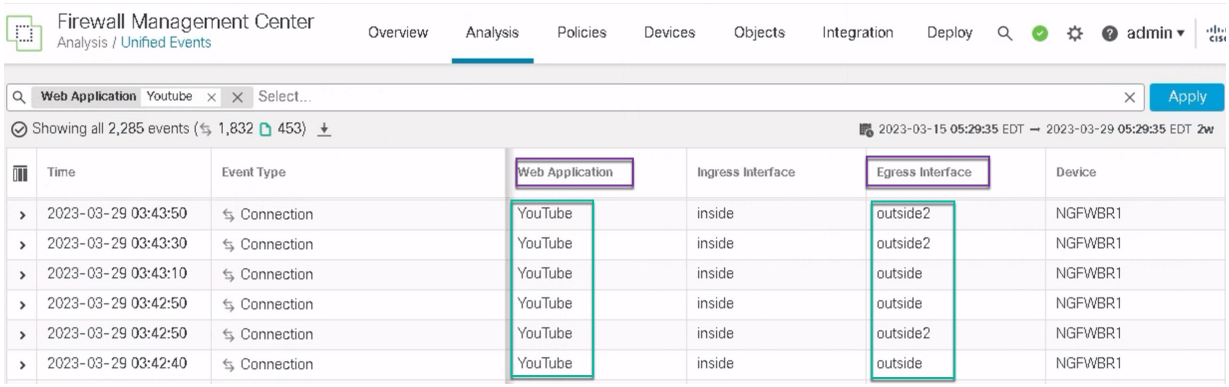
단계 **6** Secure Firewall 뒤에 있는 호스트에서 **YouTube** 및 **WebEx** 애플리케이션에 대한 트래픽을 시작합니다. 이 시나리오에서는 Google Chrome 브라우저를 실행하고 https://youtube.com으로 이동한 다음 브랜치 워크스테이션 **WKST BR1**의 다른 탭에 있는 https://webex.com으로 이동합니다.

단계 **7** 관리 센터에서 두 애플리케이션의 트래픽 흐름을 확인합니다.

1. DIA의 경우:
   - **WebEx** 애플리케이션 트래픽은 아래 그림에 표시된 것과 같이 설정에 따라 **outside3** 인터페이스를 통해 전송됩니다.

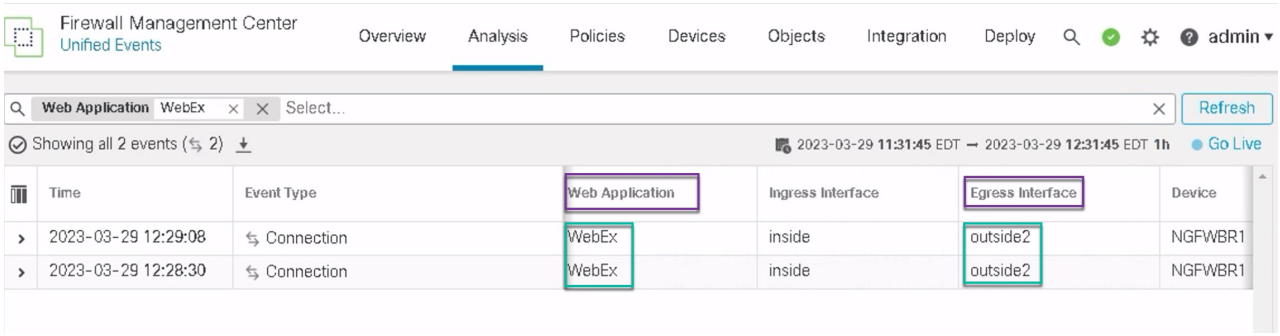


- **YouTube** 애플리케이션 트래픽은 아래 그림에 표시된 설정에 따라 **outside** 및 **outside2** 인터페이스 사이에서 로드 밸런싱됩니다.



2. 경로 모니터링을 사용하는 DIA의 경우:

   아래 그림에서 볼 수 있듯이 **outside3** 인터페이스에서 패킷 손실이 있으므로 **WebEx** 애플리케이션 트래픽은 **outside2** 인터페이스를 통해 전송됩니다.



정책 기반 라우팅 모니터링 및 문제 해결

구축 후 다음 CLI를 사용하여 Secure Firewall Threat Defense에서 정책 기반 라우팅과 관련된 문제를 모니터링하고 해결합니다.

방법	**CLI** 명령
Secure Firewall Threat Defense Lina CLI에 로그인하는 방법	**system support diagnostic-cli**
구축 중에 관리 센터에서 위협 방어로 푸시된 사전 정의된 네트워크 서비스 개체를 보는 방법	• **show object network-service** • **show object network-service detail**
설정된 애플리케이션과 관련된 특정 NSG(네트워크 서비스 개체) 보는 방법	• **show object id YouTube** • **show object id WebEx**
Secure Firewall로 푸시된 네트워크 서비스 그룹(NSG)을 확인하는 방법	**show run object-group network-service**
정책 기반 라우팅에 연결된 경로 맵을 보는 방법	**show run route-map**
인터페이스 이름 및 인터페이스 우선순위와 같은 인터페이스 구성 세부 정보를 확인하는 방법	**show run interface**
신뢰할 수 있는 DNS 서버 설정을 확인하는 방법	**show dns**
트래픽이 사용된 경로를 확인하는 방법	**debug policy-route** 중요 debug 명령은 트래픽에 따라 자세한 정보가 표시될 수 있으므로 프로덕션 환경에서 신중하게 실행합니다.
경로 디버깅을 중지하는 방법	**undebug all**

사전 정의된 네트워크 서비스 개체를 보려면 다음 명령을 사용합니다.

```
ngfwbr1# show object network-service
object network-service "ADrive" dynamic
 description Online file storage and backup.
 app-id 17
 domain adrive.com (bid=0) ip (hitcnt=0)
object network-service "Amazon" dynamic
 description Online retailer of books and most other goods.
 app-id 24
 domain amazon.com (bid=0) ip (hitcnt=0)
 domain amazon.jobs (bid=0) ip (hitcnt=0)
 domain amazon.in (bid=0) ip (hitcnt=0)
.
.
.
```

```
output snipped
.
.
.
object network-service "Logitech" dynamic
 description Company develops Computer peripherals and accessories.
 app-id 4671
 domain logitech.com (bid=0) ip (hitcnt=0)
object network-service "Lenovo" dynamic
 description Company manufactures/markets computers, software and related services.
 app-id 4672
 domain lenovo.com (bid=0) ip (hitcnt=0)
 domain lenovo.com.cn (bid=0) ip (hitcnt=0)
 domain lenovomm.com (bid=0) ip (hitcnt=0)
ngfwbr1#
```

YouTube 및 WebEx와 같은 특정 네트워크 서비스 개체를 보려면 다음 명령을 사용합니다.

```
ngfwbr1# show object id YouTube
object network-service "YouTube" dynamic
 description A video-sharing website on which users can upload, share, and view videos.
 app-id 929
 domain youtubei.googleapis.com (bid=592729) ip (hitcnt=0)
 domain yt3.ggpht.com (bid=709809) ip (hitcnt=102)
 domain youtube.com (bid=830871) ip (hitcnt=101)
 domain ytimg.com (bid=1035543) ip (hitcnt=93)
 domain googlevideo.com (bid=1148165) ip (hitcnt=466)
 domain youtu.be (bid=1247981) ip (hitcnt=0)
ngfwbr1# show object id WebEx
object network-service "WebEx" dynamic
 description Cisco's online meeting and web conferencing application.
 app-id 905
 domain files-prod-us-east-2.webexcontent.com (bid=182837) ip (hitcnt=0)
 domain webex.com (bid=290507) ip (hitcnt=30)
 domain avatar-prod-us-east-2.webexcontent.com (bid=452667) ip (hitcnt=0)
ngfwbr1#
```

NSG가 Threat Defense로 푸시되었는지 확인하려면 다음 명령을 사용합니다.

```
ngfwbr1# show run object-group network-service
object-group network-service FMC_NSG_292057776181
 network-service-member "WebEx"
object-group network-service FMC_NSG_292057776200
 network-service-member "YouTube"
ngfwbr1#
```

PBR과 연결된 경로 맵을 확인하려면 다음 명령을 사용합니다.

```
ngfwbr1# show run route-map
!
route-map FMC_GENERATED_PBR_1678091359817 permit 5
 match ip address DIA_Collaboration
 set interface outside3 outside2

!
route-map FMC_GENERATED_PBR_1678091359817 permit 10
 match ip address DIA_SocialMedia
 set adaptive-interface cost outside outside2 outside3
!
ngfwbr1#
```

인터페이스 설정 및 인터페이스 우선순위 세부정보를 확인하려면 다음 명령을 사용합니다.

```
ngfwbr1# show run interface
!
```

```
interface GigabitEthernet0/0
 nameif outside
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
 security-level 0
  zone-member ECMP-WAN
 ip address 198.18.128.81 255.255.192.0
 policy-route cost 10
!
interface GigabitEthernet0/1
 nameif inside
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
 security-level 0
 ip address 198.19.11.4 255.255.255.0
 policy-route route-map FMC_GENERATED_PBR_1678091359817
!
interface GigabitEthernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/3
 nameif outside2
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
 security-level 0
 zone-member ECMP-WAN
 ip address 198.19.40.4 255.255.255.0
 policy-route cost 10
!
interface GigabitEthernet0/4
 nameif outside3
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
 security-level 0
 ip address 198.19.30.4 255.255.255.0
 policy-route cost 20
!
interface Management0/0
 management-only
 nameif diagnostic
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
 security-level 0
 no ip address
ngfwbr1#
```

신뢰할 수 있는 DNS 설정을 확인하려면 다음 명령을 사용합니다.

```
ngfwbr1# show dns

DNS Trusted Source enabled for DHCP Server Configured
DNS Trusted Source enabled for DHCP Client Learned
DNS Trusted Source enabled for DHCP Relay Learned
DNS Trusted Source enabled for DNS Server Configured
DNS Trusted Source not enabled for Trust-any
DNS Trusted Source: Type: IPs : Interface : Idle/Timeout (sec)
```

```
    DNS Server Configured: 198.19.10.100: <ifc-not-specified> : N/A
Trusted Source Configured: 198.19.10.100: <ifc-not-specified> : N/A
DNS snooping IP cache: 0 in use, 37 most used
Address                                 Idle(sec) Timeout(sec) Hit-count          Branch(es)
ngfwbr1#
```

정책 경로를 디버깅하려면 다음 명령을 사용합니다.

```
ngfwbr1# debug policy-route
debug policy-route  enabled at level 1
ngfwbr1# pbr: policy based route lookup called for 198.19.11.225/58119 to 198.19.10.100/53
 proto 17 sub_proto 0 received on interface inside, NSGs, nsg_id=none
pbr: no route policy found; skip to normal route lookup
.
output-snipped
.
pbr: policy based route lookup called for 198.19.11.225/61482 to 63.140.48.151/443 proto 6
 sub_proto 0 received on interface inside
                                                                , NSGs, nsg_id=1
pbr: First matching rule from ACL(2)
pbr: route map FMC_GENERATED_PBR_1678091359817, sequence 5, permit; proceed with policy
routing
pbr: evaluating interface outside3
pbr: policy based routing applied; egress_ifc = outside3 : next_hop = 198.19.30.63

ngfwbr1#
```

위의 디버그 예는 WebEx 트래픽에 대한 것입니다. PBR이 outside2 인터페이스에 대한 라우팅 경로를 변경하기 전에 트래픽은 outside3 인터페이스를 통해 라우팅됩니다.

디버그 프로세스를 중지하려면 다음 명령을 사용합니다.

```
ngfwbr1# undebug all
```

추가 리소스

리소스	URL
Secure Firewall Threat Defense 릴리스 노트	https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-release-notes-list.html
모든 신규 및 지원 중단된 기능	http://www.cisco.com/go/whatsnew-fmc
Cisco.com의 보안 방화벽	http://www.cisco.com/go/firewall
유튜브의 Secure Firewall	https://www.youtube.com/cisco-netsec
Secure Firewall 기초	https://secure.cisco.com/secure-firewall