게이트웨이 프로파일

게이트웨이 프로파일은 일반적으로 서로 다른 네트워크를 연결하고 네트워크 간 트래픽을 라우팅하는 디바이스를 통해 네트워크 게이트웨이의 설정과 연결됩니다. 프로파일은 네트워크 게이트웨이의 동작과 기능을 관리하는 데 사용되며, 따라서 네트워크의 여러 부분 간에 효율적이고 안전한 통신을 보장합니다. 이러한 프로파일은 일반적으로 다음과 같은 보호 방법에 적용됩니다.

- 라우팅 정책
- NAT(네트워크 주소 변환)
- VPN(Virtual Private Network) 설정
- QoS(Quality of Service)
- 인증 및 액세스 제어

이러한 프로파일은 일반적으로 Multicloud Defense 게이트웨이 또는 게이트웨이와 연결된 VPN 터널에 적용됩니다.

패킷 캡처 프로파일

PCAP(Packet Capture)는 네트워크를 통해 전송되는 데이터 패킷을 캡처하여 네트워크 트래픽을 상세하게 분석할 수 있습니다. 캡처된 패킷을 분석하여 네트워크 트래픽에서 악의적인 활동의 징후를 모니터링하는 데 PCAP를 사용할 수 있습니다. 보안 시스템은 잠재적인 위협을 실시간으로 탐지하고 대응할 수 있으며, 이를 통해 인시던트에 이르기까지의 일련의 이벤트를 재구성하고 공격의 출처와 성격을 파악할 수 있습니다. 이 정보는 타임라인을 진단하거나 연결성 문제, 레이턴시 및 패킷 손실과 같은 이벤트를 문제 해결하는 데 유용할 수 있습니다.

패킷 캡처 프로파일 생성

다음 절차에 따라 팩 캡처 프로파일을 생성합니다.

Procedure

단계 **1** 로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** 고유한 이름을 지정합니다.

단계 **4** (선택 사항) **Description(**설명**)**을 입력합니다. 이렇게 하면 유사한 이름의 다른 프로파일을 구분하는 데 도움이 될 수 있습니다.

단계 **5** **CSP** 어카운트를 지정합니다.

단계 **6** 클라우드 통신 사업자의 유형에 따라 스토리지 버킷의 매개변수를 결정할 수 있습니다. 클라우드 통신 사업자별 다음 요구 사항에 유의하십시오.

- **AWS** - S3 버킷.
- **Azure** - 스토리지 어카운트 이름, 블로그 컨테이너 및 스토리지 액세스 키.
- **GCP** - 스토리지 버킷.

단계 **7** **Save(**저장**)**를 클릭합니다.

What to do next

정책 규칙 집합에 프로파일을 연결합니다. 자세한 내용은 규칙 집합 및 규칙 집합 그룹를 참조하십시오.

로그 포워딩 프로파일

로그 포워딩 프로파일을 사용하면 게이트웨이, VPC 및 VNet 로그 컬렉션을 타사에 전송할 수 있습니다. Multicloud Defense과 선택한 타사 간의 통신에는 포워딩해야 하는 로그 유형 및 로그가 전송될 대상 서버 프로파일이 포함됩니다. 단일 프로파일을 사용하거나 여러 엔드포인트에 로그를 동시에 전송하는 프로파일 그룹을 사용할 수도 있습니다.

이 프로파일은 메트릭을 포함하지 않습니다. 로그 메트릭 포워딩에 대한 자세한 내용은 게이트웨이 메트릭 포워딩 프로파일, 4 페이지를 참조하십시오.

독립형 로그 포워딩 프로파일 생성

다음 절차에 따라 독립형 로그 포워딩할 프로파일을 생성합니다.

프로시저

단계 **1** 이벤트 목록을 확인하려면 **Infrastructure(**인프라**)** > **Profiles(**프로파일**)** > **Log Forwarding(**로그 포워딩**)**로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** 고유 **Profile Name(**프로파일 이름**)**을 입력합니다.

단계 **4** (선택 사항) **Description(**설명**)**을 입력합니다. 이렇게 하면 유사한 이름의 다른 프로파일과 구분할 수 있습니다.

단계 **5** **Type(**유형**)** 드롭다운 메뉴를 확장하고 **Standalone(**독립형**)**을 선택합니다.

단계 **6** **Destination(**대상**)** 드롭다운 메뉴를 확장하고 로그를 전송할 타사 애플리케이션을 선택합니다.

단계 **7** 7단계에서 선택한 대상 유형에 따라 로그가 포워딩되는 최종 엔드포인트를 보호하라는 메시지가 표시되면 적절한 정보를 입력합니다. 대상 유형에 따라 모든 옵션을 사용할 수 있는 것은 아닙니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

정책 규칙 집합에 프로파일을 연결합니다. 자세한 내용은 규칙 집합 및 규칙 집합 그룹를 참조하십시오.

로그 포워딩 그룹 생성

다음 절차에 따라 그룹화된 메트릭 포워딩 프로파일을 생성합니다.

시작하기 전에

- 이 프로파일을 생성하기 전에 메트릭을 포워딩할 타사 애플리케이션이 하나 이상 있어야 합니다.
- 둘 이상의 독립형 메트릭 포워딩 프로파일이 이미 생성되어 있어야 합니다. 자세한 내용은 독립형 로그 포워딩 프로파일 생성, 2 페이지를 참조하십시오.

프로시저

단계 **1** 으로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** 고유 **Profile Name(**프로파일 이름**)**을 입력합니다.

단계 **4** (선택 사항) **Description(**설명**)**을 입력합니다. 이렇게 하면 유사한 이름의 다른 프로파일과 구분할 수 있습니다.

단계 **5** **Type(**유형**)** 드롭다운 메뉴를 확장하고 **Group(**그룹**)**을 선택합니다.

단계 **6** **Group Details(**그룹 세부 정보**)**에서 프로파일에 추가해야 하는 모든 새 행에 대해 **Add(**추가**)**를 클릭합니다.

단계 **7** 각 행에 대한 드롭다운 메뉴를 확장하여 그룹에 추가할 프로파일을 선택합니다. 저장하기 전에 언제든지 프로파일을 제거하려면, 해당 프로파일의 확인란을 선택하고 **Remove(**제거**)**를 선택합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

정책 규칙 집합에 프로파일을 연결합니다. 자세한 내용은 규칙 집합 및 규칙 집합 그룹를 참조하십시오.

게이트웨이 메트릭 포워딩 프로파일

이 프로파일은 데이터 모니터링 및 분석을 위해 Multicloud Defense 게이트웨이에 의해 생성된 게이트웨이 메트릭을 포워딩하는 데 사용됩니다. 메트릭은 게이트웨이에 의해 생성되지만 메트릭을 타사 분석 애플리케이션에 전달하는 Multicloud Defense 컨트롤러입니다. 이 포워딩 프로파일을 사용하면 Multicloud Defense에 로그인하지 않고도 게이트웨이 메트릭을 모니터링, 분석 및 구성할 수 있습니다. 이 정보를 사용하여 게이트웨이 환경의 성능 및 동작을 측정합니다. 또한 환경 문제 해결을 위해 이 정보를 활용합니다.

참고 Multicloud Defense 컨트롤러 버전 23.09부터는 DataDog만 타사 분석 애플리케이션으로 지원됩니다.

DataDog와 같이 사용 가능한 대부분의 분석 애플리케이션의 경우, 반드시 권한이 부여된 사용자여야 툴의 API 및 렌더링된 데이터에 액세스할 수 있습니다.

독립형 메트릭 포워딩 프로파일 생성

독립형 프로파일을 생성하고 타사에서 처리할 메트릭을 포워딩합니다.

시작하기 전에

이 프로파일을 생성하기 전에 메트릭을 포워딩할 타사 애플리케이션이 하나 이상 있어야 합니다.

프로시저

단계 **1** 이벤트 목록을 확인하려면 **Infrastructure(**인프라**)** > **Profiles(**프로파일**)** > **Metrics Forwarding(**메트릭 포워딩**)**로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** 고유한 프로파일 이름을 입력합니다.

단계 **4** (선택 사항) **Description(**설명**)**을 입력합니다. 이렇게 하면 유사한 이름의 다른 프로파일과 구분할 수 있습니다.

단계 **5** **Type(**유형**)** 드롭다운 메뉴를 확장하고 **Standalone(**독립형**)**을 선택합니다.

단계 **6** **Destination(**대상**)** 드롭다운 메뉴를 확장하고 메트릭을 처리하고 분석할 타사 애플리케이션을 선택합니다.

단계 **7** 메트릭의 엔드포인트 위치로 사용할 **Endpoint(**엔드포인트**)**를 입력합니다.

단계 **8** (선택 사항) 구성을 테스트하도록 이메일 메시지를 전송합니다. 메시지가 표시되면 텍스트 필드에 테스트 메시지의 내용을 입력하고 **Validate(**검증**)**를 클릭합니다. 테스트 메시지를 수신하지 않은 대상 7단계에서 대상 유형 및 구성을 확인합니다.

단계 **9** **Save(**저장**)**를 클릭합니다.

애널리틱스 애플리케이션으로 DataDog를 선택하는 경우, 엔드포인트는 기본적으로 HTTPS Webhook로 채워집니다. 이 항목이 기본값인 경우 프로파일을 저장하기 전에 수정할 수 있습니다.

다음에 수행할 작업

정책 규칙 집합에 프로파일을 연결합니다. 자세한 내용은 규칙 집합 및 규칙 집합 그룹를 참조하십시오.

그룹 메트릭 포워딩 프로파일 생성

이 프로세스에서는 프로파일을 생성한 다음 특정 게이트웨이에 할당합니다. 그룹 프로파일은 최대 5개의 독립형 메트릭 포워딩 프로파일을 결합한 다음 단일 게이트웨이에 할당할 수 있습니다. 다음 절차를 사용하여 그룹화된 메트릭 포워딩 프로파일을 생성합니다.

시작하기 전에

- 이 프로파일을 생성하기 전에 메트릭을 포워딩할 타사 애플리케이션이 하나 이상 있어야 합니다.
- 둘 이상의 독립형 메트릭 포워딩 프로파일이 이미 생성되어 있어야 합니다. 자세한 내용은 독립형 메트릭 포워딩 프로파일 생성, 4 페이지를 참조하십시오.

프로시저

단계 **1** Multicloud Defense 컨트롤러 웹 인터페이스에서 **Infrastructure(**인프라**)** > **Profiles(**프로파일**)** > **Metrics Forwarding(**메트릭 포워딩**)**로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** 고유 **Profile Name(**프로파일 이름**)**을 입력합니다.

단계 **4** (선택 사항) **Description(**설명**)**을 입력합니다. 이렇게 하면 유사한 이름의 프로파일을 구분하는 데 도움이 될 수 있습니다.

단계 **5** **Type(**유형**)** 드롭다운 메뉴를 확장하고 **Group(**그룹**)**을 선택합니다.

단계 **6** **Group Details(**그룹 세부 정보**)**에서 프로파일에 추가해야 하는 모든 새 행에 대해 **Add(**추가**)**를 클릭합니다.

단계 **7** 각 행에 대한 드롭다운 메뉴를 확장하여 그룹에 추가할 프로파일을 선택합니다. 저장하기 전에 언제든지 프로파일을 제거하려면, 해당 프로파일의 확인란을 선택하고 **Remove(**제거**)**를 선택합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

정책 규칙 집합에 프로파일을 연결합니다. 자세한 내용은 규칙 집합 및 규칙 집합 그룹를 참조하십시오.

(미리 보기 전용) 네트워크 패킷 브로커 프로파일

네트워크 패킷 브로커(NPB) 프로파일은 네트워크 트래픽을 관리하고 전달하는 방법을 정의하는 네트워크 패킷 브로커 디바이스 내에 있는 구성 모음입니다. 트래픽은 IP 주소, 프로토콜, 포트 및 애플리케이션 유형과 같은 다양한 기준에 따라 필터링됩니다. 프로파일은 다양한 모니터링, 보안 및 성능 관리 툴에 대한 네트워크 트래픽의 플로우를 최적화하는 데 사용되는 특수 디바이스입니다.

네트워크 패킷 브로커 프로파일 생성

다음 절차에 따라 네트워크 패킷 브로커(NPB) 프로파일을 생성합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Profiles(**프로파일**)** > **Network Packet Broker(**네트워크 패킷 브로커**)**로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** 고유한 이름을 제공합니다.

단계 **4** (선택 사항) **Description(**설명**)**을 입력합니다. 이렇게 하면 유사한 이름의 다른 프로파일을 구분하는 데 도움이 될 수 있습니다.

단계 **5** **Destinations(**대상**)**에서 드롭다운 메뉴를 확장하고 NPB 프로파일에서 일치하는 트래픽을 보낼 기본 대상을 선택합니다.

단계 **6** 형식을 정의하여 네트워크 데이터를 효과적으로 캡처, 저장 및 분석하여 네트워크 관리 및 문제 해결 기능을 개선합니다. **Capture Format(**캡처 형식**)** 드롭다운 메뉴를 확장하고 다음 형식 중 하나를 선택합니다.

- **None(**없음**)** - 리소스가 제한되어 있거나 여러 형식을 사용하는 매우 동적 환경에서 작업하는 경우 이 옵션을 선택합니다. 나중에 이 필드를 변경하려는 경우에도 이 옵션을 선택할 수 있습니다.
- **VXLAN** - 가상 확장 LAN은 캡처 형식 자체가 아니라 네트워크 가상화 기술입니다. 레이어 3 인프라를 통해 레이어 2 네트워크를 확장하여 가상화된 네트워크 오버레이를 생성할 수 있도록 하며 UDP 패킷 내에 이더넷 프레임을 포함하여 IP 네트워크를 통해 전송할 수 있도록 합니다.
- **Netflow(**넷플로우**)** - PCAP와 같은 형식으로 원시 패킷을 캡처하는 대신 지정된 컬렉터 또는 분석 툴로 플로우 레코드를 내보내도록 환경이 구성된 경우 이 옵션을 선택합니다.
- **ERSPAN** - 네트워크를 통해 소스에서 대상으로 트래픽을 미러링하려면 이 프로토콜을 선택하고, 미러링된 트래픽을 GRE 패킷에 포함시킨 다음 레이어 3 네트워크를 통해 전송되는 방식으로 기존 SPAN(Switched Port

Analyzer)의 기능을 확장합니다. 이는 중앙 위치에서 네트워크 트래픽을 모니터링해야 하는 환경에 이상적입니다.

단계 **7** **Slicing(**슬라이싱**)** 드롭다운 메뉴를 확장하고 전체 패킷 대신 각 네트워크 패킷의 섹션화 및 캡처 방법을 선택합니다. 이를 구성하려는 경우 다음 옵션도 구성해야 합니다.

Offset value(오프셋 값**) -** 이 필드는 각 패킷의 시작 부분부터 데이터 캡처를 시작하기 전에 건너뛰는 바이트 수를 구성할 수 있습니다. 이는 기본값 **4**로 설정됩니다.

Strip Encrypted Payload(암호화된 페이로드 제거**) -** 캡처 또는 분석 중에 패킷 데이터 페이로드의 암호화된 부분을 제거하려면 이 옵션을 선택합니다. 이 옵션을 활성화하면 프라이버시를 존중하고 리소스 사용을 최적화하면서 메타데이터 및 네트워크 동작에 집중할 수 있습니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

정책 규칙 집합에 프로파일을 연결합니다. 자세한 내용은 규칙 집합 및 규칙 집합 그룹를 참조하십시오.

네트워크 타임 프로토콜

네트워크 타임 프로토콜은 전화 모뎀, 라디오 및 위성을 통해 컴퓨터 시계를 서로 동기화하고 국제 표준에 맞게 동기화합니다. 프로파일로서, 특히 분산 시스템 내에서 동기화된 시간은 작업을 조정하고 분산 프로세스가 원활하게 협력하도록 보장하는 데 필수적입니다. 네트워크 관리 작업(예: 모니터링 및 문제 해결)에서는 여러 디바이스 간에 일관된 시간이 이상적입니다. 서로 다른 디바이스의 로그를 정확하게 상호 연결할 수 있으며 네트워크의 원활하고 안전한 운영을 보장합니다.

프로파일 생성

다음 절차에 따라 NTP 프로파일을 생성합니다.

Procedure

단계 **1** 로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** 고유한 이름을 지정합니다.

단계 **4** (선택 사항) **Description(**설명**)**을 입력합니다. 이렇게 하면 유사한 이름의 다른 프로파일을 구분하는 데 도움이 될 수 있습니다.

단계 **5** NTP 서버 목록을 지정합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

What to do next

정책 규칙 집합에 프로파일을 연결합니다. 자세한 내용은 규칙 집합 및 규칙 집합 그룹를 참조하십시오.

IPSec 프로파일

가상 터널 인터페이스에 IPSec(Internet Protocol Security) 프로파일을 사용하면 원격 액세스를 위한 보호를 제공해야 하는 경우 구성 프로세스를 간소화할 수 있습니다. IPSec 프로파일에는 두 사이트 간 VPN 피어 간의 안전한 논리적 통신 경로를 보장하는 데 필요한 필수 보안 프로토콜 및 알고리즘이 포함되어 있습니다. VPN은 네트워크-네트워크, 호스트-네트워크, 호스트-호스트 통신에 IPsec 터널에 의존하므로 터널을 생성할 때 필수 구성 요소입니다. IPsec 프로파일을 사용하면 추가 보안 및 암호화 보호를 위해 IKE 및 IPSEC 매개 변수를 한 곳에서 구성할 수 있습니다.

사이트 간 터널 구성에 IPSec 프로파일을 포함하도록 선택하면, 해당 프로파일은 네트워크 상의 지점 간을 이동하는 데이터를 암호화하고 인증함으로써 강력한 네트워크 보안을 제공하며, 사이트 간, 클라이언트-사이트 간, 클라이언트 간 터널과 호환되는 유연성을 갖추고 있습니다.

IPSec 프로파일 생성

다음 절차에 따라 Multicloud Defense 컨트롤러 대시보드에서 IPSec 프로파일을 생성합니다.

프로시저

단계 **1** 으로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** 고유 **Profile Name(**프로파일 이름**)**을 입력합니다.

단계 **4** (선택 사항) **Description(**설명**)**을 입력합니다. 이렇게 하면 유사한 이름의 다른 프로파일과 구분할 수 있습니다.

단계 **5** 프롬프트가 표시되면 적절한 IKE 정보를 입력합니다.

a) **DH Group(DH** 그룹**)** - DH(Diffie-Hellman) 그룹은 키 교환 프로세스에 사용되는 키의 강도를 결정합니다. 드롭다운 메뉴를 확장하여 프로파일에 적절한 그룹을 선택합니다.

b) **Authentication(**인증**)** - 이 터널에 대해 원하는 인증 유형을 선택하려면 드롭다운 메뉴를 확장합니다.

c) **Encryption(**암호화**)** - 가로채기된 스택에는 암호화 및 암호 해독이 필요합니다. 드롭다운 메뉴를 확장하여 암호화 방법을 선택합니다.

d) **Hash(**해시**)** - SHA1은 160비트 다이제스트를 생성하는 단방향 해싱 알고리즘입니다. 드롭다운 메뉴를 사용하여 적절한 옵션을 선택합니다.

e) **Key Lifetime(**키 수명**)** - 키가 지속되는 시간 값을 초 단위로 입력합니다. 사용 가능한 값은 60초 ~ 86400초입니다.

f) **IKE Version(IKE** 버전**)** - IKE(Internet Key Exchange)는 IP 패킷의 강력한 인증 및 암호화를 제공하는 IPSec 프로토콜 제품군의 보안 연결을 설정하는 데 사용되는 프로토콜입니다. 드롭다운 메뉴를 사용하여 IKE 버전 1 또는 버전 2를 선택합니다. 버전 간에는 상당한 차이점이 있으므로 환경에 가장 적합한 버전을 선택해야 합니다.

단계 **6** 프롬프트가 표시되면 적절한 IPsec 정보를 입력합니다.

a) **Authentication(**인증**)** - 드롭다운 메뉴를 확장하여 인증 방법으로 None(없음), SHA256, SHA 또는 Null을 선택합니다.

b) **Encryption(**암호화**)** - 드롭다운을 확장하고 키 유형(AES GCM 256, AES GCM 192 또는 AES GCM)을 선택합니다. 이렇게 하면 연결된 디바이스 간 고유 키 교환이 생성되므로 각 디바이스에서 다른 디바이스의 메시지를 암호 해독할 수 있습니다.

c) **Mode(**모드**)** - 드롭다운 메뉴를 확장하여 IPSec 정책 인증 프로토콜을 선택합니다. 둘 이상 선택할 수 있습니다.

다음에 수행할 작업

정책 규칙 집합에 프로파일을 연결합니다. 자세한 내용은 규칙 집합 및 규칙 집합 그룹를 참조하십시오.

BGP 프로파일

BGP(Border Gateway Protocol)는 IETF(Internet Engineering Task Force) 표준이며 모든 라우팅 프로토콜 중에서 가장 확장성이 뛰어납니다. BGP는 글로벌 인터넷 및 통신 사업자 프라이빗 네트워크의 라우팅 프로토콜입니다. BGP를 사용하면 VPN 게이트웨이와 BGP 인접한 라우터가 커넥터의 양쪽에 있는 게이트웨이에 관련 게이트웨이 또는 라우터의 가용성을 알리는 경로를 교환할 수 있습니다.

다른 플랫폼 또는 디바이스에 대한 사이트 간 VPN 터널 연결을 설정하는 경우 BGP 프로파일을 생성하고 게이트웨이에 추가 해야 합니다. BGP 프로파일을 사용하여 구축하면 네트워크와 클라우드 통신 사업자 간에 BGP를 포함한 동적 라우팅을 사용하는 게이트웨이가 구축됩니다.

BGP 인접한 라우터 및 경로 선택

BGP 프로파일은 "neighbors" 속성을 활용합니다. 인접한 라우터는 BGP 세션이 설정된 다른 BGP 라우터를 나타냅니다. BGP 프로파일에서 인접한 라우터를 설정하는 목적은 자율 시스템(AS) 간 또는 단일 AS 내에서 라우팅 정보를 쉽게 교환할 수 있도록 하는 것입니다.

중요 BGP 프로파일에 하나 이상의 네이버를 추가하는 것을 강력히 권장합니다.

BGP 프로파일의 인접한 라우터 섹션에서 **Route Map In(**입력 경로 맵**)** 또는 **Route Map Out(**출력 경로 맵**)**을 선택할 수 있습니다. 경로 맵은 해당 경로 맵에서 식별된 내용을 기반으로 알리거나(아웃바운드) 수락(인바운드)하는 메커니즘을 제공합니다.

경로 맵 입력**(in)**을 허용하면 다음 작업이 활성화됩니다.

- **Incoming Route Filtering(**수신 경로 필터링**):** BGP 인접한 라우터에서 어떤 경로를 수락할지 제어합니다. 원치 않는 경로를 필터링하여 관련 경로만 고려되도록 라우팅 테이블을 최적화합니다.
- **Attribute Modification(**속성 수정**)**: 로컬 기본 설정 또는 메트릭과 같은 수신 경로의 속성을 조정하여 네트워크 내의 경로 선택 프로세스에 영향을 미칩니다. 이렇게 하면 구축된 네트워크 정책을 기반으로 특정 경로의 우선 순위를 다른 경로보다 우선시하는 데 도움이 됩니다.
- **Security and Policy Compliance(**보안 및 정책 컴플라이언스**)**: 보안을 강화하고 정책 컴플라이언스를 보장하기 위해 네트워크 정책을 준수하지 않는 경로의 수락을 방지합니다.

그러나 경로 맵 출력**(out)**을 허용하면 다음 작업이 활성화됩니다.

- **Outgoing Route Filtering(**발신 경로 필터링**)**: BGP 인접한 라우터에 광고할 경로를 제어합니다. 이렇게 하면 외부 피어에 대한 네트워크의 가시성을 관리하는 데 도움이 되며 특정 내부 경로의 알림을 방지할 수 있습니다.
- **Attribute Setting(**속성 설정**)**: 경로 속성을 인접한 라우터로 전송하기 전에 수정합니다.
- **Traffic Engineering(**트래픽 엔지니어링**)**: 기본 경로를 통해 트래픽을 안내하기 위해 AS 경로 길이와 같은 경로 속성을 조정하여 인바운드 트래픽 경로에 영향을 미칩니다.

BGP는 같은 경로에 대해 서로 다른 소스로부터 여러 공지를 수신할 수 있습니다. BGP는 최적의 경로로 하나의 경로만 선택합니다. 이 경로가 선택된 경우 BGP는 선택된 경로를 IP 라우팅 테이블에 놓고 인접한 라우터에 전파합니다. BGP는 제시된 순서대로 다음 기준에 따라 목적지에 대한 경로를 선택합니다.

- 경로가 접근할 수 없는 next hop을 지정하면 업데이트를 삭제합니다.
- 가중치가 가장 높은 경로가 우선합니다.
- 가중치가 동일한 경우 로컬 우선이 가장 높은 경로가 우선합니다.
- 로컬 우선이 동일한 경우 이 라우터에서 실행 중인 BGP에서 발생한 경로가 우선합니다.
- 경로가 시작되지 않은 경우 AS_path가 가장 짧은 경로가 우선합니다.
- 모든 경로의 AS_path 길이가 같은 경우 발신지 유형이 가장 낮은 경로(IGP가 EGP보다 낮고 EGP가 incomplete보다 낮은 경로)가 우선합니다.
- 발신지 코드가 동일한 경우 MED 속성이 가장 낮은 경로가 우선합니다.
- MED가 같은 경로의 경우 내부 경로보다 외부 경로가 우선합니다.
- 그래도 경로가 동일한 경우 가장 가까운 IGP 인접한 라우터를 통한 경로가 우선합니다.
- 두 경로 모두 외부인 경우 먼저 수신된 경로가 우선합니다(오래된 경로).
- BGP 라우터 ID가 지정한 대로 IP 주소가 가장 낮은 경로가 우선합니다.
- 여러 경로의 발신자 또는 라우터 ID가 동일할 경우 클러스터 목록 길이가 가장 짧은 경로가 우선합니다.
- 가장 낮은 인접한 라우터 주소에서 시작하는 경로가 우선합니다.

BGP 프로파일 생성

다음 절차에 따라 Multicloud Defense 컨트롤러 대시보드에서 BGP 프로파일을 생성합니다.

시작하기 전에

참고 BGP 프로파일을 생성할 때 트래픽에 대해 프로파일을 활성화해야 하며, BGP 프로파일에서와 같이 터널 에서 사용되는 동일한 값을 가져야 합니다.

프로시저

단계 **1** 로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** 생성 창의 **General Settings(**일반 설정**)** 탭에서 고유한 **Profile Name(**프로파일 이름**)**을 입력합니다.

단계 **4** (선택 사항) **Description(**설명**)**을 입력합니다. 이렇게 하면 유사한 이름의 다른 프로파일과 구분할 수 있습니다.

단계 **5** **LocalAS** 값을 입력합니다. 이 값은 BGP4 디바이스가 상주하는 로컬 자율 시스템(AS)을 나타냅니다.

단계 **6** 전환하려면 창 상단의 **Neighbors(**인접한 라우터**)** 탭을 클릭합니다. 인접한 라우터 및 이 구성이 환경을 위해 수행할 수 있는 작업에 대한 자세한 내용은 BGP 인접한 라우터 및 경로 선택, 9 페이지을 참조하십시오.

단계 **7** **Add Neighbors(**인접한 라우터 추가**)**를 클릭합니다.

단계 **8** **Neighbor 1(**인접한 라우터 **1)** 공간을 확장합니다.

단계 **9** **IP** 주소 텍스트 상자에 단일 주소 또는 IP 주소 범위와 BGP 피어 그룹을 수동으로 입력합니다. 여러 주소를 추가하는 경우에는 공백으로 각 주소를 구분합니다.

단계 **10** **Autonomous System(**자동 시스템**)** - 인접한 라우터가 상주하는 위치에 대한 LocalAS를 입력합니다.

단계 **11** **Route Map In(**입력 경로 맵**)** - 인터페이스에서 인바운드 방향으로 일치하는 모든 트래픽에 루트 맵을 적용하려면 이 옵션을 활성화합니다. **Route Map Out(**출력 경로 맵**)** - 인터페이스에서 아웃바운드 방향으로 일치하는 모든 트래픽에 루트 맵을 적용하려면 이 옵션을 활성화합니다. 환경에 적합한 옵션을 선택한 후 다음 정보를 입력합니다.

a) **Local Preference(**로컬 환경 설정**)** - 기본적으로 이 값은 "100"입니다. 선택적으로, 0~4,294,967,295 사이의 32비트 무부호 정수 값을 입력합니다. 자율 시스템 내에서 더 선호되는 경로를 나타내는 더 높은 로컬 선호도 값에 유의하십시오.

로컬 기본 설정은 동일한 자율 시스템(iBGP) 내의 BGP 라우터 간에만 교환되며 외부에 알림(eBGP)되지 않습니다.

b) **AS Path Prepend(AS** 경로 앞에**)** - 이 값을 입력합니다. 둘 이상의 값을 입력하는 경우 각 값을 공백으로 구분합니다. 이 값은 경로의 AS 경로 특성을 인공적으로 늘려 경로 선택 프로세스에 영향을 미칩니다. 인바운드 트래픽에 이것을 포함하는 것은 일반적이지 않지만, 수신 경로에 추가 AS 번호를 추가하면 라우팅 트래픽을 위한 경로를 선택할 때 이러한 경로가 내부 BGP 스피커에 덜 선호될 수 있습니다.

c) **Add(**추가**)**를 클릭하여 IP 주소 또는 네트워크를 포함하고 IP 주소, 쉼표로 구분된 IP 주소의 범위 또는 IP와 넷마스크 모두로 구성된 네트워크를 입력합니다. BGP 세션 내에서 또는 외부로 허용할 경로 또는 네트워크입니다. 아무 때나 **Remove(**제거**)**를 클릭하여 인접한 라우터에서 IP 주소를 제거할 수 있습니다.

단계 **12** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

BGP 프로파일을 Multicloud Defense 게이트웨이에 추가합니다. 새 게이트웨이를 생성 하거나 새 프로파일을 포함하도록 기존 게이트웨이를 편집할 수 있습니다.

번역에 관하여
Cisco는 일부 지역에서 본 콘텐츠의 현지 언어 번역을 제공할 수 있습니다. 이러한 번역은 정보 제공의 목적으로만 제공되며, 불일치가 있는 경우 본 콘텐츠의 영어 버전이 우선합니다.

번역에 관하여
Cisco는 일부 지역에서 본 콘텐츠의 현지 언어 번역을 제공할 수 있습니다. 이러한 번역은 정보 제공의 목적으로만 제공되며, 불일치가 있는 경우 본 콘텐츠의 영어 버전이 우선합니다.