Multicloud Defense 게이트웨이 수정 사항 및 개선 사항(아카이브)

버전 24.06

버전 24.06-10-a1 2025년 3월 31일

핫픽스입니다.

수정 사항

이 핫픽스에는 다음과 같은 수정 사항이 포함되어 있습니다.

- 사후양자 암호화가 활성화된 브라우저 기반 클라이언트 트래픽을 처리할 때 간헐적으로 발생하는 데이터 경로 불안정을 수정합니다. 이러한 불안정성으로 인해 데이터 경로가 자가 복구가 수행됩니다. 이번 수정으로 데이터 경로 안정성이 보장되어 자가 복구가 필요하지 않습니다.
- 전달 정책이 TLS Client Hello 메시지로부터 SNI(Service Name Indication)를 검색할 수 없어 게이트웨이가 TCP RST와 함께 연결을 종료하는 문제를 수정합니다. 이는 2024년 4월에 사후양자 암호화로 전환하기 위해 Chrome에서 변경된 사항 때문에 발생합니다. 변경 사항으로 인해 클라이언트 Hello가 1415바이트보다 크기 때문에 정책에서 도메인과 일치하거나 필터링하는 데 사용하는 SNI를 검색할 수 없게 됩니다. 이번 수정으로 프록시가 1415바이트보다 큰 Client Hello 크기를 지원할 수 있습니다.

버전 24.06-10 2025년 3월 31일

수정 사항

이 릴리스에는 다음과 같은 수정 사항이 포함되어 있습니다.

- 정책의 작업이 거부로 설정된 트래픽 처리 시 CPU 사용률이 예상보다 높아지는 문제를 수정합니다.
- SMB 트래픽 처리 시 Multicloud Defense 게이트웨이 데이터 경로가 멈춘 상태가 될 수 있는 문제를 수정합니다. 이 현상이 발생하면 데이터 경로가 자가 복구됩니다. 이번 수정으로 데이터 경로가 해당 상태로 진입하지 않도록 하여 SMB 트래픽을 성공적으로 처리하도록 문제를 해결합니다.
- 특정 유형의 세션 동작에서 CPU 사용량이 누적될 수 있는 인그레스 게이트웨이 리버스 프록시 정책의 문제를 수정합니다. 성공적인 종단 간 세션이 설정되고 클라이언트와 서버가 통신한 후 각자가 해당 세션을 종료하지 않은 채 사라지면, 프록시는 결국 세션을 종료하지만 세션 할당을 완전히 정리하지는 않습니다. 이로 인해 시간이 지남에 따라 CPU 사용량이 누적됩니다. 세션 동작이 더 큰 볼륨으로 발생하면 CPU 사용량이 더 빠르게 증가할 수 있습니다. 이번 수정으로 세션 정리 기능을 개선하여 CPU 사용량이 시간이 지남에 따라 누적되지 않고 안정적으로 유지되도록 합니다.
- TCP 포워드 프록시 정책 사용 시 레거시 애플리케이션에 대한 완전한 종단 간 세션 설정 문제를 수정합니다. 레거시 애플리케이션의 예로는 SSHv1 및 데이터베이스 관리 트래픽(Oracle)이 포함될 수 있습니다. 이러한 유형의 애플리케이션에서는 TCP 연결이 수립된 후, 다음 패킷은 클라이언트가 아닌 서버로부터 도착합니다. TCP 포워드 프록시 정책에서 Multicloud Defense 게이트웨이는 먼저 프론트엔드 TCP 연결(클라이언트에서 게이트웨이로)을 설정하고, 다음 패킷이 서버가 아닌 클라이언트로부터 도착할 것으로 예상합니다. 패킷이 전혀 도착하지 않으므로 백엔드 TCP 연결(게이트웨이에서 서버로)이 절대 설정되지 않습니다. 이로 인해 종단 간 세션이 생성되지 않으며 애플리케이션 통신이 실패합니다.

  이번 수정으로 다음 두 가지 방법으로 문제를 해결합니다: (1) 게이트웨이 설정 활성화 및 (2) 트래픽을 처리하는 정책 규칙을 평가하여 도메인 평가(FQDN 일치, FQDN 필터링)가 구성되었는지 확인합니다. (1)과 (2)가 모두 구성된 경우, Multicloud Defense 게이트웨이는 트래픽이 TLS로 암호화될 것이라고 가정하며, 다음에 도착할 패킷은 클라이언트로부터의 TLS Hello 패킷이 될 것입니다. (1)만 구성된 경우, 게이트웨이는 트래픽이 TLS로 암호화되지 않았다고 가정하므로 클라이언트로부터 다음 패킷이 도착할 것을 기대하지 않고 즉시 백엔드 연결을 설정합니다. 다음에 도착하는 패킷은 클라이언트에서든 서버에서든, 해당 패킷을 처리하고 의도된 목적지로 전송하기 위한 완전한 종단 간 세션을 갖게 될 것입니다.

  (1)이 구성되지 않은 시나리오에서, 트래픽이 TLS로 암호화되어 있고 TLS Hello SNI로부터 도메인을 획득한 경우, 게이트웨이는 도메인 해상도를 수행하고 해상된 IP 중 하나를 백엔드 연결의 대상으로 사용합니다. (1)이 구성된 시나리오 또는 트래픽이 TLS로 암호화되지 않은 시나리오에서는 도메인을 획득할 수 없고 도메인 확인이 불가능하므로 프론트엔드 TCP 연결 대상 IP가 백엔드 TCP 연결 대상 IP로 사용됩니다.

  이 수정 사항을 적용하려면 게이트웨이 설정이 필요합니다. 이 문제가 발생한다고 생각되면, 해당 설정을 활성화하는 방법에 대한 평가 및 정보를 얻기 위해 시스코 지원팀에 문의하십시오. 향

후 릴리스에서는 규칙별로 이 동작을 구성할 수 있을 예정이므로, 이러한 유형의 트래픽을 세그먼트 하는 규칙을 생성할 수 있습니다. 여기서 위에서 설명한 변경 사항은 특정 트래픽에만 적용할 수 있습니다.

버전 24.06-09-a1 2025년 2월 14일

핫픽스입니다.

수정 사항

이 핫픽스에는 다음과 같은 수정 사항이 포함되어 있습니다.

- 사후양자 암호화가 활성화된 브라우저 기반 클라이언트 트래픽을 처리할 때 간헐적으로 발생하는 데이터 경로 불안정을 수정합니다. 이러한 불안정성으로 인해 데이터 경로가 자가 복구가 수행됩니다. 이번 수정으로 데이터 경로 안정성이 보장되어 자가 복구가 필요하지 않습니다.
- 전달 정책이 TLS Client Hello 메시지로부터 SNI(Service Name Indication)를 검색할 수 없어 게이트웨이가 TCP RST와 함께 연결을 종료하는 문제를 수정합니다. 이는 2024년 4월에 사후양자 암호화로 전환하기 위해 Chrome에서 변경된 사항 때문에 발생합니다. 변경 사항으로 인해 클라이언트 Hello가 1415바이트보다 크기 때문에 정책에서 도메인과 일치하거나 필터링하는 데 사용하는 SNI를 검색할 수 없게 됩니다. 이번 수정으로 프록시가 1415바이트보다 큰 Client Hello 크기를 지원할 수 있습니다.

버전 24.06-09 2025년 2월 14일

수정 사항

이 릴리스에는 다음과 같은 수정 사항이 포함됩니다.

- 브라우저 기반 클라이언트에서 양자 저항 암호화가 활성화된 경우 SNI 획득과 관련된 하위 문제점을 수정합니다. 사후양자 암호화 시나리오로 인해 TLS 헬로가 여러 패킷으로 분할됩니다. 첫 번째 패킷이 도착했지만 두 번째 패킷이 도착하지 않으면, 게이트웨이는 세션 정리 시 세션에 할당된 CPU를 절대 해제하지 않을 것이다. 이번 수정으로 CPU가 해제되고 시간이 지남에 따라 누적되지 않도록 보장합니다.

버전 24.06-08-a1 2025년 1월 16일

핫픽스입니다.

수정 사항

이 핫픽스에는 다음과 같은 수정 사항이 포함되어 있습니다.

- 전달 정책이 TLS Client Hello 메시지로부터 SNI(Service Name Indication)를 검색할 수 없어 게이트웨이가 TCP RST와 함께 연결을 종료하는 문제를 수정합니다. 이는 2024년 4월에 사후양자 암호화로 전환하기 위해 Chrome에서 변경된 사항 때문에 발생합니다. 변경 사항으로 인해 클라이

언트 Hello가 1415바이트보다 크기 때문에 정책에서 도메인과 일치하거나 필터링하는 데 사용하는 SNI를 검색할 수 없게 됩니다. 이번 수정으로 프록시가 1415바이트보다 큰 Client Hello 크기를 지원할 수 있습니다.

버전 24.06-08 2024년 1월 16일

개선 사항

이 릴리스에는 다음과 같은 개선 사항이 포함되어 있습니다.

- 암호화 프로파일의 일부로 구성할 수 있으며 TLS 협상을 위한 포워드 프록시 또는 리버스 프록시 정책에서 사용할 수 있는 추가 암호화 모음을 포함합니다.
- Nginx 추적을 켜고 끌 수 있는 고급 문제 해결 설정을 제공합니다. 이전 버전에서는 Nginx 추적 기능을 고급 디버깅 설정을 통해서만 활성화할 수 있었으며, 이 설정은 Nginx 추적 정보보다 훨씬 더 많은 내용을 캡처했습니다. 이 설정에서는 활성화 시 Nginx 추적 정보만 수집됩니다. 해당 설정은 시스코 지원팀 또는 시스코 엔지니어링 팀에 의해서만 활성화될 수 있으며, 프록시 문제 해결이 필요한 경우에 활성화하도록 의도되었습니다. 추적 데이터가 수집되면 진단 번들에 포함된 Multicloud Defense 컨트롤러로 전송됩니다.

수정 사항

이 릴리스에는 다음과 같은 수정 사항이 포함됩니다.

- 그룹 주소 개체 제외 목록에서 제외된 주소 개체에 지정된 IP/CIDR이 Multicloud Defense 게이트웨이 정책에 제대로 적용되지 않던 문제를 수정합니다. 이를 통해 포함된 주소 개체와 제외된 주소 개체 모두 적절한 트래픽 매칭에 적용됩니다.

버전 24.06-07-a1 2024년 12월 18일

이 릴리스는 핫픽스입니다.

수정 사항

이 핫픽스에는 다음과 같은 수정 사항이 포함되어 있습니다.

- 전달 정책이 TLS Client Hello 메시지로부터 SNI(Service Name Indication)를 검색할 수 없어 게이트웨이가 TCP RST와 함께 연결을 종료하는 문제를 수정합니다. 이는 2024년 4월에 사후양자 암호화로 전환하기 위해 Chrome에서 변경된 사항 때문에 발생합니다. 변경 사항으로 인해 클라이언트 Hello가 1415바이트보다 크기 때문에 정책에서 도메인과 일치하거나 필터링하는 데 사용하는 SNI를 검색할 수 없게 됩니다. 이번 수정으로 프록시가 1415바이트보다 큰 Client Hello 크기를 지원할 수 있습니다.

버전 24.06-07 2024년 12월 18일

수정 사항

이 릴리스에는 다음과 같은 수정 사항이 포함되어 있습니다.

- 새로운 Talos 규칙 집합과 관련된 문제를 수정합니다. 규칙 집합 변경 시 새 규칙 집합을 게이트웨이에 적용하는 데 문제가 발생할 수 있었습니다. 게이트웨이가 정책 규칙 집합 상태 "업데이트 중..." 상태에서 중단됩니다. 해당 문제는 새로운 Talos 규칙 집합이 게시되기 전에 발견되었습니다. 이번 업데이트로 문제가 해결되어 새 Talos 규칙 집합을 성공적으로 적용할 수 있습니다.
- 데이터 경로가 일시적으로 중단되어 상태 체크를 비롯한 트래픽 처리에 문제가 발생할 수 있는 문제를 수정합니다. 이 경우 게이트웨이는 정상과 비정상 사이를 반복해서 오가며, 이를 연속적으로 출력되는 시스템 로그 메시지에서 확인할 수 있습니다. 이러한 중단 상태는 일반적으로 컨트롤러가 해당 인스턴스를 교체 대상으로 표시할 만큼 오래 지속되지는 않습니다.
- 특정 UDP 세션 동작으로 인해 발생하는, 결과적으로 데이터 경로가 재시작될 수 있는 UDP 연결 풀 유출 관련 문제를 수정합니다. 데이터 경로가 재시작되면 인스턴스는 재시작 기간 동안 비정상 상태가 됩니다. 비정상 기간이 오래 지속되면 컨트롤러는 인스턴스를 교체 대상으로 표시합니다.

버전 24.06-06-a1 2024년 11월 28일

이 릴리스는 핫픽스입니다.

수정 사항

이 핫픽스에는 다음과 같은 수정 사항이 포함되어 있습니다.

- 전달 정책이 TLS Client Hello 메시지로부터 SNI(Service Name Indication)를 검색할 수 없어 게이트웨이가 TCP RST와 함께 연결을 종료하는 문제를 수정합니다. 이는 2024년 4월에 사후양자 암호화로 전환하기 위해 Chrome에서 변경된 사항 때문에 발생합니다. 변경 사항으로 인해 클라이언트 Hello가 1415바이트보다 크기 때문에 정책에서 도메인과 일치하거나 필터링하는 데 사용하는 SNI를 검색할 수 없게 됩니다. 이번 수정으로 프록시가 1415바이트보다 큰 Client Hello 크기를 지원할 수 있습니다.

버전 24.06-06 2024년 11월 26일

수정 사항

이 릴리스에는 다음과 같은 수정 사항이 포함됩니다.

- Azure 인그레스 게이트웨이가 새 게이트웨이 인스턴스가 활성화될 때 충돌할 수 있는 문제를 수정합니다.

버전 24.06-05 2024년 11월 22일

개선 사항

이 릴리스에는 다음과 같은 개선 사항이 포함되어 있습니다.

- FIPS(FedRAMP) 및 비 FIPS(상용) 환경을 모두 수용하기 위해 FIPS Teleport 에이전트를 게이트웨이에 통합합니다. 텔레포트는 기본적으로 비활성화되어 있습니다. 고급 문제 해결을 위해 시스코 지원팀과 협력하는 경우에만 고객이 활성화할 수 있습니다.

수정 사항

이 릴리스에는 다음과 같은 수정 사항이 포함되어 있습니다.

- 인그레스 게이트웨이에서 처리하는 트래픽으로 인해 CPU 과부하가 발생하여 불필요한 스케일 아웃이 발생할 수 있는 문제를 수정합니다. 높은 CPU는 암호화되지 않은 HTTP 프록시 사용하여 연결을 처음에 처리하는 정책에서 HTTP 리디렉션으로 인해 암호화된 TCP 프록시로 이동하기 때문에 발생합니다.
- 트래픽을 적절한 정책 규칙과 일치시키려고 할 때 이그레스 게이트웨이 포워드 프록시 정책이 중단될 수 있는 문제를 수정합니다.
- 일부 장시간 활성 상태인 연결이 제대로 활성 재설정(TCP RST 전송)되지 않는 문제를 수정합니다.
- 인그레스 게이트웨이 역방향 프록시 정책에서 멀웨어가 탐지될 때 발생하던 게이트웨이 충돌을 수정합니다.
- UDP 세션이 정상적으로 제대로 집계되지 않아 관련된 활성 연결 및 연결율 통계가 잘못 기록되던 문제를 수정합니다.

버전 24.06-04 2024년 10월 25일

수정 사항

이 릴리스에는 다음과 같은 수정 사항이 포함됩니다.

- 백엔드 연결이 응답하지 않아 트래픽 처리에 지연이 발생하는 프록시 시나리오에서 게이트웨이가 불필요하게 CPU를 소모하는 문제를 수정합니다.

버전 24.06-03 2024년 10월 20일

개선 사항

이 릴리스에는 다음과 같은 개선 사항이 포함되어 있습니다.

- FedRamp 환경에 구축된 게이트웨이 사용에 필요한 BoringCrypto를 지원하는 향상된 게이트웨이 이미지를 제공합니다. 이는 Multicloud Defense가 FedRamp 컴플라이언스를 위한 지속적인 노력입니다.
- Teleport를 통해 게이트웨이에 SSH 세션이 설정될 때 표시될 사용자 지정 배너 지원을 추가합니다.

수정 사항

이 릴리스에는 다음과 같은 수정 사항이 포함되어 있습니다.

- Kyber 암호화 모음을 포함하는 TLS 세션으로 인해 CPU 사용량이 증가하여 트래픽 처리가 불가능해지는 문제를 수정합니다.
- 게이트웨이 인스턴스가 교체될 때 연결 소모 시간이 적용되지 않던 문제를 수정했습니다.
- 정책 변경 또는 게이트웨이 인스턴스 교체 중에 프록시 세션이 종료될 때 게이트웨이 데이터 경로가 자가 복구될 수 있는 안정성 문제를 수정합니다.
- 진단 번들 생성이 실패할 수 있는 문제를 수정합니다.
- 프록시 정책이 TLS Client Hello 메시지로부터 SNI(Service Name Indication)를 검색하지 못해, TCP RST를 사용하여 연결을 종료하는 문제를 수정합니다. 이는 2024년 4월에 사후양자 암호화로 전환하기 위해 Chrome에서 변경된 사항 때문에 발생합니다. 이 변경 사항을 적용하면 Client Hello가 1415바이트보다 커집니다. 이에 따라 프록시에서 발급할 인증서를 결정하는 데 사용되는 SNI(Server Name Indication)를 검색할 수 없게 됩니다. 이번 수정으로 프록시 정책이 1415바이트보다 큰 Client Hello 크기를 지원할 수 있습니다.
- FQDN 기반 주소 개체에 사용된 도메인의 DNS 변경 사항이 게이트웨이 데이터패스 에이전트에는 수신되지만 데이터패스 워커에는 적용되지 않는 문제를 수정합니다. 이로 인해 DNS 변경 사항이 주소 개체의 동적 특성에 적용되지 않아 정상적인 트래픽 처리에 영향을 미칠 수 있습니다.
- 기본 구성과 다르게 설정된 해독 프로파일이 게이트웨이에 제대로 적용되지 않아 클라이언트와 게이트웨이 간 암호 모음 불일치로 TLS 협상 실패가 발생하는 문제를 수정합니다.
- 게이트웨이 SSH 세션에서 사용되는 게이트웨이 측 암호화 모음이 잠재적으로 더 취약한 암호화 모음으로 표시될 수 있는 문제를 수정합니다. 이번 수정으로 가장 안전한 GCM 기반 암호 모음만 지원합니다.
- 다양한 안정성 문제를 수정합니다.

버전 24.06-02-a2 2024년 10월 2일

이 릴리스는 핫픽스입니다.

수정 사항

이 핫픽스에는 다음과 같은 수정 사항이 포함되어 있습니다.

- 새로운 게이트웨이 이미지가 구축될 때 Multicloud Defense 게이트웨이이 일시적으로 충돌하는 문제를 수정합니다.
- Multicloud Defense 게이트웨이는 이제 게이트웨이 인스턴스를 종료할 때 Multicloud Defense 컨트롤러에 구성된 배수 시간 값을 준수합니다.

버전 24.06-02 2024년 9월 18일

개선 사항

이 릴리스에는 다음과 같은 개선 사항이 포함되어 있습니다.

- FedRAMP CIS 레벨-2 강화 기준을 수용하기 위한 게이트웨이의 지속적인 개선.

수정 사항

이 릴리스에는 다음과 같은 수정 사항이 포함되어 있습니다.

- 정책 규칙 세트에 비어 있는 FQDN/URL 필터링 프로파일이 할당될 경우 게이트웨이가 자가 복구되는 문제를 수정합니다.
- 도메인을 6-튜플로 일치 조건으로 사용하는 것과 관련된 거부 규칙 작업 문제를 수정합니다. 첫 번째 규칙 일치가 6-튜플 일치(할당된 FQDN 일치 프로파일 포함)이고 작업 동작이 거부로 설정되어 있는 경우, 거부 작업은 5-튜플 일치를 기준으로 적용하며, 일치 판단 시 도메인은 고려하지 않습니다. 이번 수정으로 규칙과 해당 작업을 평가할 때 6-튜플이 모두 고려됩니다. 트래픽이 6-튜플 일치에 기반한 규칙과 일치하지 않으면 후속 규칙에 대한 일치를 구체화하고 일치하는 규칙의 구성에 따라 작업을 수행합니다.
- 정책 업데이트가 적용된 후 Azure 인그레스 게이트웨이가 상태 확인 보류 상태에서 멈추는 문제를 수정합니다. 이 문제에는 새 게이트웨이 구축도 포함되어 있습니다.
- 도메인을 6-튜플로 일치 조건으로 사용하는 것과 관련된 허용 규칙 작업 문제를 수정합니다. 첫 번째 규칙 일치가 6-튜플 일치(할당된 FQDN 일치 프로파일 포함)인 경우, 정책 작업은 허용으로 설정되고 첫 번째 규칙의 5-튜플 일치와 일치하는 후속 규칙이 없으면 모든 도메인에 적용됩니다. 허용되며 도메인이 거부됩니다. 이번 수정으로 규칙에서 일치하는 도메인만 허용되고, 일치하지 않는 다른 모든 도메인은 거부됩니다.
- 해독 기반 전달 프록시(TLS, HTTPS, WebsocketS)를 사용하는 이그레스 정책 규칙 집합이 처음에 5-튜플과 일치하고 SNI에서 도메인 검색하지만 6-튜플을 기반으로 일치 구체화를 수행하지 않는 문제를 수정합니다. TLS 오류가 발생합니다. 이번 수정으로 6-튜플 일치 구체화가 발생하여 적절한 해독 규칙으로 트래픽을 성공적으로 처리할 수 있도록 합니다.
- TLS 오류가 발생한 세션에서 SNI를 트래픽 요약 > 이벤트로 기록하지 않던 문제를 수정합니다.
- 해독된 전체 포워드 프록시 세션마다 여러 SNI 이벤트가 기록되는 문제를 수정합니다.
- 주소 그룹 크기가 초과되어 크기를 초과하는 모든 IP/CIDR이 주소 그룹에 포함되지 않는 문제를 수정합니다. 주소 그룹 크기가 20k IP/CIDR로 증가했습니다.

- 게이트웨이의 GeoIP 제한이 초과된 경우 시스템 로그 메시지를 추가합니다.
- 캐시에 URL이 없는 경우 URL 필터링 범주 검색을 시도할 때 시간 초과가 발생하면 URL 필터링 범주 일치에 대해 잘못된 작업이 수행되는 문제를 수정합니다.
- URL 필터링 프로파일을 설정할 수 있는 관리자 액세스 권한이 있는 사용자가 맞춤형 URL 응답을 사용하여 JavaScript를 삽입할 수 없도록 합니다. 이번 수정으로 맞춤형 URL 응답에서 HTML 인코딩을 적용합니다.

버전 24.06-01 2024년 7월 10일

-

개선 사항

이 릴리스에는 다음과 같은 개선 사항이 포함되어 있습니다.

- 게이트웨이를 통과하는 GRE 터널 내부의 콘텐츠를 검사하는 기능을 지원합니다. 게이트웨이는 트래픽의 캡슐화를 해제하고, 캡슐화된 트래픽에 대한 검사를 수행하여 적절한 정책과 보호를 적용한 후, 해당 트래픽을 다시 GRE 터널로 캡슐화합니다.
- 게이트웨이 업그레이드 및 스케일 인 시나리오에서 활성 연결 재설정 기능을 지원합니다. 이러한 시나리오가 발생하고 게이트웨이가 클라이언트나 서버에 의해 닫히지 않은 장기 실행 연결을 처리 중인 경우, 게이트웨이는 오래된 인스턴스를 정리할 때 TCP RST를 전송하여 연결을 능동적으로 닫는 조치를 취합니다.
- Teleport(SSH 액세스)을 통해 게이트웨이 인스턴스에 로그인할 때 사용자 지정 배너를 지정할 수 있는 기능을 지원합니다. 이것은 FedRamp 환경에 구축된 게이트웨이에 대한 요구사항으로, SSH 접근 방식에 관계없이 고객이 정의한 배너가 표시되어야 합니다.

수정 사항

이 릴리스에는 다음과 같은 수정 사항이 포함되어 있습니다.

- 암호 해독 프로파일에서 "기본값" 이외의 인증서 유효성 검사 작업을 지정할 경우 게이트웨이가 비정상 상태가 되는 문제를 수정합니다.
- 사용자가 생성한 진단 번들에서 게이트웨이가 진단 번들을 생성하지 못하고 Multicloud Defense 컨트롤러로 전송하지 못하는 문제를 수정합니다.
- GeoIP 사용과 관련된 문제를 수정합니다. 공급자가 많은 국가들은 광고되는 접두사가 매우 많습니다. 해당 국가 코드가 GeoIP 주소 그룹에 사용될 경우, 해당 주소 그룹에는 다수의 CIDR 블록이 포함됩니다. 지리적 IP 주소 그룹은 64개의 CIDR로 제한되었으며, 이 한도를 초과할 경우 정책에 적용되는 CIDR 집합이 부분적으로만 적용됩니다. 이번 수정은 전체 CIDR 집합이 정책에 적용되도록 한도를 완화합니다. GeoIP로 인해 추가 메모리 요구 사항이 발생하므로 8코어 인스턴스 유형을 사용하는 것이 권장됩니다.
- Chrome 브라우저가 TLS 1.3을 사용하여 게이트웨이에 연결할 때 게이트웨이가 잘못된 인증서를 발급할 수 있는 문제를 수정합니다. 이는 2024년 4월에 사후양자 암호화로 전환하기 위해

Chrome에서 변경된 사항 때문에 발생합니다. 이 변경 사항을 적용하면 Client Hello가 1415바이트보다 커집니다. 이에 따라 프록시에서 발급할 인증서를 결정하는 데 사용되는 SNI(Server Name Indication)를 검색할 수 없게 됩니다. 이번 수정으로 프록시가 1415바이트보다 큰 Client Hello 크기를 지원할 수 있습니다.

- 게이트웨이가 **Investigate(**조사**)** > **Network Analytics(**네트워크 애널리틱스**)** > **Stats(**통계**)** 페이지에 표시할 올바른 통계를 생성하지 못하던 문제를 수정했습니다.
- 다양한 안정성 문제를 수정합니다.
- Blue/Green 정책 변경 관련 문제를 수정합니다. 정책 변경이 발생하고 새 데이터 경로가 활성화되면 게이트웨이는 기존 데이터 경로에서 현재 세션을 드레인하기 시작합니다. 데이터 경로에서 세션을 제대로 드레인할 수 없는 경우 데이터 경로를 비정상으로 처리하고 데이터 경로 재시작을 사용합니다. 이렇게 하면 기존 데이터 경로와 새 데이터 경로가 모두 종료되어 기존 세션과 새 세션의 중단이 발생할 수 있습니다. 이번 수정으로 세션 드레인이 올바르게 완료되고 데이터 경로가 비정상으로 표시되는 상황이 제거됩니다.
- VPN 터널 상태 전환 시 터널 설정 및 협상에 대한 문제 해결 및 디버깅 정보를 제공하는 시스템 로그 메시지가 생성되지 않던 문제를 수정합니다.
- 데이터 경로 자체 복구로 이어지는 인그레스 게이트웨이의 느린 메모리 누수를 수정합니다. 메모리 누수는 gzip 압축된 파일을 포함하는 트래픽과 관련이 있습니다.
- 연속된 POST 명령에 160k보다 큰 페이로드가 포함될 경우 인그레스 게이트웨이가 연결을 끊을 수 있는 문제를 수정합니다.

버전 **24.04**

버전 **24.04-01 2024**년 **5**월 **16**일

개선 사항

이 릴리스에는 다음과 같은 개선 사항이 포함되어 있습니다.

- AWS, Azure 및 GCP에서 실행되는 게이트웨이에 대한 사이트 간 VPN 지원을 추가합니다. 여기에는 IPSec 및 BGP 프로파일을 포함한 VPN 터널 구성이 포함되어 있습니다. VPN을 통과하는 트래픽을 처리하고 보호하기 위해 VPN은 게이트웨이에서 직접 종료됩니다. 이 기능에는 게이트웨이 버전 24.04 이상이 필요합니다.

수정 사항

이 릴리스에는 다음과 같은 수정 사항이 포함되어 있습니다.

- 게이트웨이가 주소 개체를 63자 이하로 제한하는지 확인합니다.
- 정책 변경 사항을 적용하는 데 시간이 너무 오래 걸리기 때문에 데이터 경로가 재시작될 수 있는 문제를 수정합니다.

- 두 개의 데이터 경로가 동시에 실행되는 파란색/녹색 정책 업데이트 도중 CPU 사용량이 증가하는 문제를 수정합니다. 각 데이터 경로는 실행 중인 유일한 데이터 경로라고 가정하는 방식으로 CPU를 사용합니다. 새 정책을 수용하기 위해 두 번째 데이터 경로가 인스턴스화되면 CPU가 제대로 공유되지 않으며 CPU 메트릭이 제대로 기록되지 않습니다.
- 사전 데이터 경로 자가 복구로 이어질 수 있는 메모리 누수 관련 문제를 수정합니다.
- 게이트웨이 정책 업데이트 상태가 업데이트에서 중단될 수 있는 문제를 수정합니다.
- 게이트웨이의 안정성을 개선하는 다양한 문제를 수정합니다.

버전 **24.02**

버전 **24.02-02 2024**년 **4**월 **18**일

수정 사항

이 릴리스에는 다음과 같은 수정 사항이 포함됩니다.

- 새 게이트웨이 인스턴스가 활성화되지 못하도록 하는 게이트웨이 초기화 중 메모리 버퍼 액세스 관련 문제를 수정합니다.

버전 **24.02-01 2024**년 **2**월 **28**일

개선 사항

이 릴리스에는 다음과 같은 개선 사항이 포함되어 있습니다.

- [프라이빗 미리보기] 사이트 간 VPN에 대한 지원을 추가합니다. 여기에는 IPSec 및 BGP를 포함한 VPN 터널 구성이 포함되어 있습니다. VPN을 통과하는 트래픽을 처리하고 보호하기 위해 VPN은 Multicloud Defense 게이트웨이에서 직접 종료됩니다. 이 개선 사항은 Multicloud Defense 게이트웨이 버전 24.02 이상이 필요합니다.
- 개인 키가 클라우드 서비스 제공자에 저장되고 Multicloud Defense 게이트웨이로 검색되는 인증서 개체에 대한 변경 사항을 동적으로 추적할 수 있도록 지원을 추가합니다. 클라우드 서비스 제공자 리소스가 변경될 때 Multicloud Defense 컨트롤러는 게이트웨이에 클라우드 서비스 제공자 리소스의 개인 키를 다시 읽고 액세스 가능한지, 업데이트된 콘텐츠가 사용되는지 확인하도록 지시합니다. 인증서 액세스에 문제가 발생하면 시스템 로그 메시지가 생성됩니다.
- SSH를 통해 로그인하는 경우 관리 Linux 셸에 메시지를 추가합니다. 메시지는 디바이스가 Cisco 매니지드 디바이스(예: Multicloud Defense 컨트롤러에 의해 관리되는 디바이스)임을 강조합니다.
- 로그 전달 그룹에서 둘 이상의 시스템 로그 서버 구성에 대한 지원을 추가합니다.

수정 사항

이 릴리스에는 다음과 같은 수정 사항이 포함되어 있습니다.

- libwebp 버전 1.2.0-3.el9와 관련된 CVE-2023-4863 취약점을 수정합니다.
- 데이터 경로 무중단 재시작을 유발하는 정책 변경이 높은 레이턴시를 야기하고 약하거나 보통의 로드에서 로드 밸런서 상태 확인을 비롯한 트래픽 처리에 영향을 미칠 수 있는 문제를 수정합니다.
- 여전히 4코어 인스턴스 유형에 영향을 주던 버전 23.08-12에서 해결된 문제를 수정합니다. 이 문제는 디버그 I/O 활동으로 인해 발생하는 높은 CPU 사용률을 해결합니다. 이전 수정은 이제 모든 클라우드 서비스 제공자의 모든 인스턴스 유형을 해결합니다.
- I/O 관련 디버그 활동으로 인해 발생했던 높은 CPU 사용률과 관련된 문제를 수정합니다.
- 간헐적 로드 밸런서 상태 확인 실패 관련 문제를 수정합니다. 이번 수정으로 로드 밸런서가 인스턴스를 비정상으로 잘못 표시하지 않도록 상태 체크의 우선순위를 지정하여 게이트웨이를 개선합니다.
- 자가 복구 사전 데이터 경로 재시작을 트리거하여 자동으로 수정되는 이그레스 게이트웨이 메모리 유출을 수정합니다.
- 생성된 게이트웨이 진단 번들이 Multicloud Defense 컨트롤러로 전송하도록 허용된 것보다 커서 게이트웨이 로그를 분석할 수 없는 문제를 수정합니다. 이 수정은 생성된 진단 번들이 Multicloud Defense 컨트롤러에 성공적으로 전송되도록 제한을 해결합니다.
- 정방향 프록시 규칙으로 처리된 각 세션에 대해 둘 이상의 SNI 이벤트가 기록되는 문제를 수정합니다.
- Multicloud Defense 게이트웨이 안정성 개선.
- DNS 기반 FQDN 캐싱과 관련된 경쟁 조건으로 인해 TCP 및 TLS 이후에 트래픽이 처리를 중지하는 트래픽 처리 문제를 수정합니다.
- 활성 또는 비활성 규칙에 DNS 기반 FQDN 캐싱이 구성된 경우 Multicloud Defense 게이트웨이가 IP 캐시를 성공적으로 구축하지 못할 수 있는 문제를 해결합니다. 캐시가 제대로 구축되지 않으면 정책이 트래픽을 매칭하지 못할 수 있습니다. 이번 수정을 통해 정책이 일치하고 트래픽을 올바르게 처리할 수 있도록 IP 캐시가 올바르게 구축됩니다.
- SYN을 수신한 후 SYN ACK를 대기하는 시간 초과를 변경합니다. 원래 시간 초과는 120초입니다. SYN ACK가 반환되지 않는 특정 시나리오(예: 포트 스캐닝)에서 긴 시간 초과는 원하는 세션 끌어오기의 항목을 사용합니다. 많은 세션이 SYN ACK로 응답하지 않는 시나리오의 경우 세션 풀이 소진될 수 있습니다. 이를 SYN 플러드라고 합니다. 시간 초과를 줄이면 유효한 세션 처리에 사용할 세션 풀을 확보하기 위해 세션이 더 빨리 릴리스됩니다. 시간 초과는 30초로 감소했으며 Multicloud Defense 게이트웨이 설정을 통해 구성할 수 있습니다.
- DNS 캐싱을 활성화하면 정책 변경과 DNS 확인 간격 간에 경합 조건이 발생하여 도메인의 캐시가 0(캐시 없음) 값으로 재설정될 수 있는 DNS 기반 FQDN 주소 개체 리소스와 관련된 문제를 수정합니다. 이러한 상황이 발생하면 도메인 확인이 캐시되지 않으며 TTL이 만료되면 기존 캐시 값이 플러시됩니다. 최종 결과는 Multicloud Defense 게이트웨이가 해당 도메인의 트래픽과 일치하지 않게 됩니다. 이번 수정으로 캐시가 예상대로 작동하도록 경쟁 조건을 해결합니다.

- 시스템 로그 서버로 전송된 DPI(IDS/IPS) 보안 이벤트에 **Action(**작업**)** 필드가 없는 문제를 수정합니다. **Action(**작업**)** 필드가 있지만 값이 UI에 있는 작업 값 또는 다른 SIEM으로 전송된 이벤트 정보와 일치하지 않습니다. 수정은 **Action(**작업**)** 필드 값이 `ALLOW` 또는 `DENY`임을 보장하기 위해 모든 보안 이벤트에서 이 문제를 범용적으로 수정합니다.
- 규칙 집합 버전이 변경되지 않는 경우 보안 프로파일 자동 업데이트를 수동으로 변경하면 불필요한 데이터 경로가 다시 시작되는 문제를 수정합니다. 이 문제를 해결하면 데이터 경로를 다시 시작할 필요 없이 변경 사항이 적용됩니다.
- Multicloud Defense 게이트웨이 안정성 개선.
- Multicloud Defense 게이트웨이 성능 개선.
- TLS hello 메시지의 SNI 필드에서 가져온 도메인이 FQDN 필드가 아닌 이벤트의 텍스트 필드에 채워지는 SNI 보안 이벤트 문제를 수정합니다. FQDN 필드를 채우기 위한 변경 사항은 FQDN 필드를 사용하여 도메인별로 보고 필터링할 때 로그 및 이벤트 전체에서 일관성을 제공합니다.
- 세션 풀 유출을 유발할 수 있는 데이터 경로 프로세스 관련 문제를 수정합니다. 이러한 상황이 발생하면 유출이 운영에 영향을 미치기 전에 데이터 경로가 세션 풀 사용 및 자가 복구를 평가합니다. 이번 수정으로 유출을 수정하여 데이터 경로가 자가 복구해야 하는 상황을 방지합니다.
- 게이트웨이 프로파일 정보를 검색하기 위해 Multicloud Defense 컨트롤러에 대한 API 호출을 최적화하여 Multicloud Defense 게이트웨이의 성능을 개선합니다.
- 정책 규칙 집합 작업을 `No Log(로그 없음)` 값으로 설정해도 로그 메시지가 생성되는 문제를 수정합니다.

버전 **23.08**

버전 **23.08-17-b1 2024**년 **9**월 **27**일

핫픽스입니다.

수정 사항

이 핫픽스에는 다음과 같은 수정 사항이 포함되어 있습니다.

- 게이트웨이가 TLS Client Hello 메시지로부터 SNI(Service Name Indication)를 검색하지 못해, TCP RST를 사용하여 연결을 종료하는 문제를 수정합니다. 이는 2024년 4월에 사후양자 암호화로 전환하기 위해 Chrome에서 변경된 사항 때문에 발생합니다. 이 변경 사항을 적용하면 Client Hello가 1415바이트보다 커집니다. 이에 따라 프록시에서 발급할 인증서를 결정하는 데 사용되는 SNI(Server Name Indication)를 검색할 수 없게 됩니다. 이번 수정으로 프록시가 1415바이트보다 큰 Client Hello 크기를 지원할 수 있습니다.

버전 23.08-17-a1 2024년 9월 4일

핫픽스입니다.

해결

이 핫픽스에는 다음과 같은 수정 사항이 포함되어 있습니다.

- DNS 기반 FQDN 캐시를 사용하는 정책 규칙이 손상되어 Multicloud Defense 게이트웨이가 트래픽을 제대로 처리하지 않을 수 있는 문제를 수정합니다.

버전 23.08-17 2024년 9월 4일

수정 사항

이 릴리스에는 다음과 같은 수정 사항이 포함되어 있습니다.

- GeoIP 사용과 관련된 문제를 수정합니다. 공급자가 많은 국가들은 광고되는 접두사가 매우 많습니다. 해당 국가 코드가 GeoIP 주소 그룹에 사용될 경우, 해당 주소 그룹에는 다수의 CIDR 블록이 포함됩니다. 지리적 IP 주소 그룹은 64개의 CIDR로 제한되었으며, 이 한도를 초과할 경우 정책에 적용되는 CIDR 집합이 부분적으로만 적용됩니다. 이번 수정은 전체 CIDR 집합이 정책에 적용되도록 한도를 완화합니다. GeoIP로 인해 추가 메모리 요구 사항이 발생하므로 8코어 인스턴스 유형을 사용하는 것이 권장됩니다.
- TCP 설정 시간 초과 값을 240초보다 큰 값으로 변경했음에도 불구하고, 이그레스 게이트웨이가 240초에 TCP 연결을 무음으로 종료하는 문제를 수정합니다.
- URL 필터링 프로파일을 사용하여 트래픽을 필터링할 때 ggress 게이트웨이의 데이터 경로가 자체 복구될 수 있는 문제를 수정합니다.

버전 23.08-16-a1 2024년 8월 6일

핫픽스입니다.

수정 사항

이 핫픽스에는 다음과 같은 수정 사항이 포함되어 있습니다.

- DNS 기반 FQDN 캐시를 사용하는 정책 규칙이 손상되어 게이트웨이가 트래픽을 제대로 처리하지 않을 수 있는 문제를 수정합니다.

버전 23.08-16 2024년 6월 25일

수정 사항

이 릴리스에는 다음과 같은 수정 사항이 포함되어 있습니다.

- Chrome 브라우저가 TLS 1.3을 사용하여 게이트웨이에 연결할 때 Multicloud Defense 게이트웨이가 잘못된 인증서를 발급할 수 있는 문제를 수정합니다. 이는 2024년 4월에 사후양자 암호화로 전환하기 위해 Chrome에서 변경된 사항 때문에 발생합니다. 이 변경 사항을 적용하면 Client Hello가 1415바이트보다 커집니다. 이에 따라 프록시에서 발급할 인증서를 결정하는 데 사용되는 SNI(Server Name Indication)를 검색할 수 없게 됩니다. 이번 수정으로 프록시가 1415바이트보다 큰 Client Hello 크기를 지원할 수 있습니다.
- 세션을 닫기 위해 데이터 경로에서 TCP RST를 전송하면 데이터 경로가 자동으로 복구될 수 있는 문제를 수정합니다.
- Multicloud Defense 게이트웨이가 트래픽을 처리하는 기능에 영향을 줄 수 있는 수신 버퍼 소진 관련 문제를 수정합니다. 게이트웨이가 연결 재설정(TCP RST)을 수용하려면 마지막으로 수신한 패킷의 정보를 유지(수신 버퍼)해야 합니다. 활성 세션 볼륨이 높으면 수신 버퍼가 소진되어 Multicloud Defense 게이트웨이가 새 패킷을 수신하지 않을 위험이 있습니다. 이 시나리오는 의도적 또는 의도적이지 않은 SYN 플러드와 관련하여 연결이 절반만 열린 경우 더욱 일반적으로 발생할 수 있습니다. 이번 수정으로 각 활성 세션의 마지막 패킷에서 필요한 정보를 추출하고 게이트웨이 활성 세션 제한을 수용하기에 충분히 큰 버퍼에 이 정보를 저장하므로 버퍼가 소진될 가능성이 없습니다.
- Blue/Green 정책 변경 관련 문제를 수정합니다. 정책 변경이 발생하고 새 데이터 경로가 활성화되면 Multicloud Defense 게이트웨이는 기존 데이터 경로에서 현재 세션을 드레인하기 시작합니다. 데이터 경로에서 세션을 제대로 드레인할 수 없는 경우 데이터 경로를 비정상으로 처리하고 데이터 경로 재시작을 사용합니다. 이렇게 하면 기존 데이터 경로와 새 데이터 경로가 모두 종료되어 기존 세션과 새 세션의 중단이 발생할 수 있습니다. 이번 수정으로 세션 드레인이 올바르게 완료되고 데이터 경로가 비정상으로 표시되는 상황이 제거됩니다.
- OCI에서 Multicloud Defense 게이트웨이에 대한 로그 회전 문제 해결 이번 수정으로 불필요한 디스크 공간을 사용하지 않도록 로그가 올바르게 교체됩니다.
- TCP RST가 잘못된 시퀀스 번호로 전송되며 연결을 적극적으로 재설정하지 않는 활성 연결 재설정 관련 문제를 수정합니다.
- 데이터 경로 자체 복구로 이어지는 인그레스 게이트웨이의 느린 메모리 누수를 수정합니다. 메모리 누수는 gzip 압축된 파일을 포함하는 트래픽과 관련이 있습니다.

버전 23.08-15-a3 2024년 6월 22일

핫픽스입니다.

수정 사항

이 핫픽스에는 다음과 같은 수정 사항이 포함되어 있습니다.

- GeoIP 사용과 관련된 문제를 수정합니다. 공급자가 많은 국가들은 광고되는 접두사가 매우 많습니다. 해당 국가 코드가 GeoIP 주소 그룹에 사용될 경우, 해당 주소 그룹에는 다수의 CIDR 블록이 포함됩니다. 지리적 IP 주소 그룹은 64개의 CIDR로 제한되었으며, 이 한도를 초과할 경우 정책에 적용되는 CIDR 집합이 부분적으로만 적용됩니다. 이번 수정은 전체 CIDR 집합이 정책에

적용되도록 한도를 완화합니다. GeoIP로 인해 추가 메모리 요구 사항이 발생하므로 8코어 인스턴스 유형을 사용하는 것이 권장됩니다.

버전 23.08-14-c3 2024년 6월 8일

핫픽스입니다.

수정 사항

이 핫픽스에는 다음과 같은 수정 사항이 포함되어 있습니다.

- Chrome 브라우저가 TLS 1.3을 사용하여 게이트웨이에 연결할 때 게이트웨이가 잘못된 인증서를 발급할 수 있는 문제를 수정합니다. 이는 2024년 4월에 사후양자 암호화로 전환하기 위해 Chrome에서 변경된 사항 때문에 발생합니다. 이 변경 사항을 적용하면 Client Hello가 1415바이트보다 커집니다. 이에 따라 프록시에서 발급할 인증서를 결정하는 데 사용되는 SNI(Server Name Indication)를 검색할 수 없게 됩니다. 이번 수정으로 프록시가 1415바이트보다 큰 Client Hello 크기를 지원할 수 있습니다.
- 데이터 경로 자체 복구로 이어지는 인그레스 게이트웨이의 느린 메모리 누수를 수정합니다. 메모리 누수는 gzip 압축된 파일을 포함하는 트래픽과 관련이 있습니다.

버전 23.08-15-c1 2024년 5월 9일

핫픽스입니다.

수정 사항

이 핫픽스에는 다음과 같은 수정 사항이 포함되어 있습니다.

- 게이트웨이가 트래픽을 처리하는 기능에 영향을 줄 수 있는 수신 버퍼 소진 관련 문제를 수정합니다. 게이트웨이가 연결 재설정(TCP RST)을 수용하려면 마지막으로 수신한 패킷의 정보를 유지(수신 버퍼)해야 합니다. 활성 세션 볼륨이 높으면 수신 버퍼가 소진되어 게이트웨이가 새 패킷을 수신하지 않을 위험이 있습니다. 이 시나리오는 의도적 또는 의도적이지 않은 SYN 플러드와 관련하여 연결이 절반만 열린 경우 더욱 일반적으로 발생할 수 있습니다. 이번 수정으로 각 활성 세션의 마지막 패킷에서 필요한 정보를 추출하고 게이트웨이 활성 세션 제한을 수용하기에 충분히 큰 버퍼에 이 정보를 저장하므로 버퍼가 소진될 가능성이 없습니다.

버전 23.08-15-a2 2024년 5월 1일

핫픽스입니다.

수정 사항

이 핫픽스에는 다음과 같은 수정 사항이 포함되어 있습니다.

- 세션을 닫기 위해 데이터 경로에서 TCP RST를 전송하면 데이터 경로가 자동으로 복구될 수 있는 문제를 수정합니다.

버전 23.08-15-b1 2024년 4월 12일

핫픽스입니다.

수정 사항

이 핫픽스에는 다음과 같은 수정 사항이 포함되어 있습니다.

- OCI에서 게이트웨이에 대한 로그 회전 문제 해결 이번 수정으로 불필요한 디스크 공간을 사용하지 않도록 로그가 올바르게 교체됩니다.

버전 23.08-15-a1 2024년 4월 11일

핫픽스입니다.

수정 사항

이 핫픽스에는 다음과 같은 수정 사항이 포함되어 있습니다.

- Blue/Green 정책 변경 관련 문제를 수정합니다. 정책 변경이 발생하고 새 데이터 경로가 활성화되면 게이트웨이는 기존 데이터 경로에서 현재 세션을 드레인하기 시작합니다. 데이터 경로에서 세션을 제대로 드레인할 수 없는 경우 데이터 경로를 비정상으로 처리하고 데이터 경로 재시작을 사용합니다. 이렇게 하면 기존 데이터 경로와 새 데이터 경로가 모두 종료되어 기존 세션과 새 세션의 중단이 발생할 수 있습니다. 이번 수정으로 세션 드레인이 올바르게 완료되고 데이터 경로가 비정상으로 표시되는 상황이 제거됩니다.

버전 23.08-15 2024년 3월 27일

수정 사항

이 릴리스에는 다음과 같은 수정 사항이 포함되어 있습니다.

- 인그레스 게이트웨이를 통과하는 HTTP 트래픽이 매칭된 정책 규칙 세트와 연결된 역방향 프록시 대상에 지정된 적절한 도메인을 사용하지 않는 문제를 수정합니다.
- 인그레스 게이트웨이를 통과하는 HTTP 트래픽이 적절한 정책 규칙 집합과 일치하지 않는 문제를 수정합니다.
- 전달 및 데이터 경로 프로토콜 스택이 TCP FIN 및 RST 타이밍을 처리하는 방법과 관련된 문제를 수정합니다. 서버의 FIN과 클라이언트의 RST는 프로토콜 스택이 이미 FIN을 확인한 후 RST 수락 및 전달을 억제하는 순서로 발생할 수 있습니다. 이 변경 사항은 RST에 대한 프로토콜 스택의 수락을 완화하여 RST가 서버에 전달되고 프로토콜 스택에 의해 삭제되지 않을 수 있도록 합

니다. 프로토콜 스택이 서버에서 이미 FIN을 수신했기 때문에 예상되는 시퀀스 번호의 불일치로 인해 RST 삭제가 발생합니다.

- 정책 변경 사항을 적용하는 데 시간이 너무 오래 걸리기 때문에 데이터 경로가 재시작될 수 있는 문제를 수정합니다.
- 두 개의 데이터 경로가 동시에 실행되는 파란색/녹색 정책 업데이트 도중 CPU 사용량이 증가하는 문제를 수정합니다. 각 데이터 경로는 실행 중인 유일한 데이터 경로라고 가정하는 방식으로 CPU를 사용합니다. 새 정책을 수용하기 위해 두 번째 데이터 경로가 인스턴스화되면 CPU가 제대로 공유되지 않으며 CPU 메트릭이 제대로 기록되지 않습니다.
- 사전 데이터 경로 자가 복구로 이어질 수 있는 메모리 누수 관련 문제를 수정합니다.
- libwebp 버전 1.2.0-3.el9와 관련된 CVE-2023-4863 취약점을 수정합니다.
- 백엔드 서버에 대한 쓰기 작업이 EAGAIN을 반환한 후 손실된 쓰기 이벤트 관련 문제를 수정합니다. 이 손실 이벤트로 인해 게이트웨이는 요청 본문을 백엔드 서버에 전송했다고 생각하고 도착하지 않을 응답을 기다리고 있습니다. 이는 게이트웨이 속도 및 백엔드 서버 속도와 관련된 타이밍 문제입니다.
- OCI에 구축된 게이트웨이에 대한 진단 번들 생성 문제를 수정합니다.
- TCP RST가 잘못된 시퀀스 번호로 전송되며 연결을 적극적으로 재설정하지 않는 활성 연결 재설정 관련 문제를 수정합니다.
- 정책 변경 중에 기존 정책을 실행 중인 데이터 경로를 통과하는 트래픽이 불필요하게 지연되는 트래픽 처리 문제를 수정합니다.
- WAF 구성 요소가 클라이언트 요청 본문을 사용하는 대량 요청 본문 트래픽 관련 문제를 수정합니다. 이로 인해 클라이언트가 게이트웨이로부터 응답을 기대하는 동안 게이트웨이가 계속 요청 본문을 기대하게 되어 클라이언트 타임아웃이 발생합니다.

버전 23.08-14-e1 2024년 3월 28일

핫픽스입니다.

수정 사항

이 핫픽스에는 다음과 같은 수정 사항이 포함되어 있습니다.

- DNS 기반 FQDN 캐시를 사용하는 정책 규칙이 손상되어 게이트웨이가 트래픽을 제대로 처리하지 않을 수 있는 문제를 수정합니다.
- libwebp 버전 1.2.0-3.el9와 관련된 CVE-2023-4863 취약점을 수정합니다.

버전 23.08-14-a2 2024년 3월 20일

핫픽스입니다.

수정 사항

이 핫픽스에는 다음과 같은 수정 사항이 포함되어 있습니다.

- 전달 및 데이터 경로 프로토콜 스택이 TCP FIN 및 RST 타이밍을 처리하는 방법과 관련된 문제를 수정합니다. 서버의 FIN과 클라이언트의 RST는 프로토콜 스택이 이미 FIN을 확인한 후 RST 수락 및 전달을 억제하는 순서로 발생할 수 있습니다. 이 변경 사항은 RST에 대한 프로토콜 스택의 수락을 완화하여 RST가 서버에 전달되고 프로토콜 스택에 의해 삭제되지 않을 수 있도록 합니다. 프로토콜 스택이 서버에서 이미 FIN을 수신했기 때문에 예상되는 시퀀스 번호의 불일치로 인해 RST 삭제가 발생합니다.
- 두 개의 데이터 경로가 동시에 실행되는 파란색/녹색 정책 업데이트 도중 CPU 사용량이 증가하는 문제를 수정합니다. 각 데이터 경로는 실행 중인 유일한 데이터 경로라고 가정하는 방식으로 CPU를 사용합니다. 새 정책을 수용하기 위해 두 번째 데이터 경로가 인스턴스화되면 CPU가 제대로 공유되지 않으며 CPU 메트릭이 제대로 기록되지 않습니다.

버전 23.08-14-d1 2024년 3월 13일

핫픽스입니다.

수정 사항

이 핫픽스에는 다음과 같은 수정 사항이 포함되어 있습니다.

- 인그레스 게이트웨이를 통과하는 HTTP 트래픽이 매칭된 정책 규칙 세트와 연결된 역방향 프록시 대상에 지정된 적절한 도메인을 사용하지 않는 문제를 수정합니다.
- 인그레스 게이트웨이를 통과하는 HTTP 트래픽이 적절한 정책 규칙 집합과 일치하지 않는 문제를 수정합니다.

버전 23.08-14-c1 2024년 2월 20일

핫픽스입니다.

수정 사항

이 핫픽스에는 다음과 같은 수정 사항이 포함되어 있습니다.

- libwebp 버전 1.2.0-3.el9와 관련된 CVE-2023-4863 취약점을 수정합니다.

버전 23.08-14-b1 2024년 2월 21일

핫픽스입니다.

수정 사항

이 핫픽스에는 다음과 같은 수정 사항이 포함되어 있습니다.

- 백엔드 서버에 대한 쓰기 작업이 EAGAIN을 반환한 후 손실된 쓰기 이벤트 관련 문제를 수정합니다. 이 손실 이벤트는 Multicloud Defense 게이트웨이이 백엔드 서버에 요청 본문을 보냈고 도착하지 않을 응답을 기다리고 있다고 생각하게 만듭니다. 이는 게이트웨이 속도 및 백엔드 서버 속도와 관련된 타이밍 문제입니다.
- OCI에 구축된 게이트웨이에 대한 진단 번들 생성 문제를 수정합니다.
- WAF 구성 요소가 클라이언트 요청 본문을 사용하는 대량 요청 본문 트래픽 관련 문제를 수정합니다. 이로 인해 클라이언트가 Multicloud Defense 게이트웨이로부터 응답을 기대하는 동안 Multicloud Defense 게이트웨이이 계속 요청 본문을 기대하게 되어 클라이언트 타임아웃이 발생합니다.

버전 23.08-14-a1 2024년 2월 17일

핫픽스입니다.

수정 사항

이 핫픽스에는 다음과 같은 수정 사항이 포함되어 있습니다.

- TCP RST가 잘못된 시퀀스 번호로 전송되며 연결을 적극적으로 재설정하지 않는 활성 연결 재설정 관련 문제를 수정합니다.
- 정책 변경 중에 기존 정책을 실행 중인 데이터 경로를 통과하는 트래픽이 불필요하게 지연되는 트래픽 처리 문제를 수정합니다.

버전 23.08-14 2024년 1월 25일

수정 사항

이 릴리스에는 다음과 같은 수정 사항이 포함되어 있습니다.

- 여전히 4코어 인스턴스 유형에 영향을 주던 23.08-12에서 해결된 문제를 수정합니다. 이 문제는 디버그 I/O 활동으로 인해 발생하는 높은 CPU 사용률을 해결합니다. 이전 수정은 이제 모든 클라우드 서비스 제공자의 모든 인스턴스 유형을 해결합니다.
- 데이터 경로 무중단 재시작을 유발하는 정책 변경이 높은 레이턴시를 야기하고 약하거나 보통의 로드에서 로드 밸런서 상태 확인을 비롯한 트래픽 처리에 영향을 미칠 수 있는 문제를 수정합니다.

버전 23.08-12: 2024년 1월 18일

수정 사항

이 릴리스에는 다음과 같은 수정 사항이 포함되어 있습니다.

- I/O 관련 디버그 활동으로 인해 발생했던 높은 CPU 사용률과 관련된 문제를 수정합니다.

- 간헐적 로드 밸런서 상태 확인 실패 관련 문제를 수정합니다. 이번 수정으로 로드 밸런서가 인스턴스를 비정상으로 잘못 표시하지 않도록 상태 체크의 우선순위를 지정하여 게이트웨이를 개선합니다.
- 게이트웨이 프로파일 정보를 검색하기 위해 컨트롤러에 대한 API 호출을 최적화하여 게이트웨이의 성능을 개선합니다.

버전 23.08-11 2024년 1월 11일

개선 사항

이 릴리스에는 다음과 같은 개선 사항이 포함되어 있습니다.

- 정책 유형(전달 및 정방향 프록시)이 불일치하는 두 가지 규칙에 의해 처리된 각 세션에 대해 생성된 정책 유형 불일치 메시지를 각 세션 관련 보안 이벤트 로그로 이동합니다. 이렇게 하면 세션별 로그를 제거하지 않고 많은 양의 세션별 시스템 로그 메시지가 제거됩니다. 이 시나리오가 발생하면 세션이 거부되고 세션 관련 이벤트가 이유를 보고합니다. 거부는 트래픽 요약 로그에도 표시됩니다.

버전 23.08-10 2023년 12월 18일

수정 사항

이 릴리스에는 다음과 같은 수정 사항이 포함되어 있습니다.

- SYN을 수신한 후 SYN ACK를 대기하는 시간 초과를 변경합니다. 원래 시간 초과는 120초입니다. SYN ACK가 반환되지 않는 특정 시나리오(예: 포트 스캐닝)에서 긴 시간 초과는 원하는 세션 끌어오기의 항목을 사용합니다. 많은 세션이 SYN ACK로 응답하지 않는 시나리오의 경우 세션 풀이 소진될 수 있습니다. 이를 SYN 플러드라고 합니다. 시간 초과를 줄이면 유효한 세션 처리에 사용할 세션 풀을 확보하기 위해 세션이 더 빨리 릴리스됩니다. 시간 초과는 30초로 감소했으며 게이트웨이 설정을 통해 구성할 수 있습니다.
- 활성 또는 비활성 규칙에 DNS 기반 FQDN 캐싱이 구성된 경우 게이트웨이가 IP 캐시를 성공적으로 구축하지 못할 수 있는 문제를 해결합니다. 캐시가 제대로 구축되지 않으면 정책이 트래픽을 매칭하지 못할 수 있습니다. 이번 수정을 통해 정책이 일치하고 트래픽을 올바르게 처리할 수 있도록 IP 캐시가 올바르게 구축됩니다.
- 생성된 게이트웨이 진단 번들이 컨트롤러로 전송하도록 허용된 것보다 커서 게이트웨이 로그를 분석할 수 없는 문제를 수정합니다. 이 수정은 생성된 진단 번들이 컨트롤러에 성공적으로 전송되도록 제한을 해결합니다.
- 게이트웨이 안정성을 개선합니다.

버전 23.08-09 2023년 11월 16일

수정 사항

이 업그레이드에는 다음과 같은 수정 사항이 포함되어 있습니다.

- DNS 캐싱을 활성화하면 정책 변경과 DNS 확인 간격 간에 경합 조건이 발생하여 도메인의 캐시가 0(캐시 없음) 값으로 재설정될 수 있는 DNS 기반 FQDN 주소 개체 리소스와 관련된 문제를 수정합니다. 이러한 상황이 발생하면 도메인 확인이 캐시되지 않으며 TTL이 만료되면 기존 캐시 값이 플러시됩니다. 최종 결과는 게이트웨이가 해당 도메인의 트래픽과 일치하지 않게 됩니다. 이번 수정으로 캐시가 예상대로 작동하도록 경쟁 조건을 해결합니다.

버전 23.08-08 2023년 11월 8일

수정 사항

이 업그레이드에는 다음과 같은 수정 사항이 포함되어 있습니다.

- 모든 활용 사례에 대해 게이트웨이 안정성을 개선합니다.

버전 23.08-07 2023년 10월 18일

수정 사항

이 업그레이드에는 다음과 같은 수정 사항이 포함되어 있습니다.

- GCP 로깅으로의 로그 전달이 JSON으로 인코딩된 문자열이 아닌 JSON 구조로 로그를 보내도록 문제를 수정합니다.

버전 23.08-06 2023년 10월 7일

수정 사항

이 업데이트에는 다음과 같은 수정 사항이 포함되어 있습니다.

- 트래픽 처리 문제를 일으킬 수 있는 암호 해독 예외에 FQDN 일치 개체를 사용하는 정방향 프록시 규칙과 관련된 문제를 수정합니다.

버전 23.08-05 2023년 10월 3일

수정 사항

이 업데이트에는 다음과 같은 수정 사항이 포함되어 있습니다.

- 인증서 검증 지연으로 인해 FQDN 일치 프로파일로 구성된 정방향 프록시 규칙에 의해 트래픽이 잘못 거부되는 문제를 수정합니다. FQDN 필터링 프로파일이 적용되지 않더라도 거부는 FQDNFILTER 보안 이벤트로 간주됩니다.

버전 23.08-04 2023년 9월 19일

수정 사항

이 업그레이드에는 다음과 같은 수정 사항이 포함되어 있습니다.

- FQDN 일치 개체를 사용하는 규칙이 미분류 도메인에 대한 트래픽을 잘못 처리하는 문제를 수정합니다.

버전 23.08-03 2023년 9월 10일

수정 사항

이 업그레이드에는 다음과 같은 수정 사항이 포함되어 있습니다.

- IP 수가 많고 해당 IP를 많이 변경하면 데이터 경로에서 변경 사항이 수락되지 않아 일치 문제가 발생함으로써 트래픽이 부정확하게 처리될 수 있는 동적 주소 개체 관련 문제를 수정합니다.
- DP가 유출을 탐지하고 데이터 경로를 재시작하게 할 수 있는 UDP 트래픽과 관련된 느린 세션 풀 유출 문제를 수정합니다.

버전 23.08-02 2023년 9월 3일

수정 사항

이 업그레이드에는 다음과 같은 수정 사항이 포함되어 있습니다.

- 페이로드가 200KB보다 큰 HTTP POST를 전송할 때 트래픽이 삭제되는 역방향 프록시 문제를 수정합니다.
- 고정 IP를 포함하는 DNS 기반 주소 개체가 제대로 일치되지 않는 문제를 수정합니다.
- TCP 전달 프록시의 SNI 또는 호스트 헤더에 대한 종속성을 제거합니다.

버전 23.08-01 2023년 8월 25일

개선 사항

이 업그레이드에는 다음과 같은 개선 사항이 포함되어 있습니다.

- 게이트웨이 연결 및 프록시 타이머가 초과될 경우 세션 요약 이벤트를 생성하도록 데이터 경로를 개선합니다. 이 개선 사항은 타이머 설정으로 인해 게이트웨이에서 세션을 닫을 때 문제 해결에 도움이 됩니다.
- L4(TCP) 및 L5(TLS) 프록시를 수용하도록 정방향 프록시 서비스 개체를 개선합니다. TCP 또는 TLS를 `transport_mode` 인수에 대한 유효한 값으로 지정하여 이를 수행할 수 있습니다.
- 세션 성능을 추적하기 위해 게이트웨이 데이터 경로를 개선합니다.
- 데이터 경로를 재시작하는 동안 연결을 능동적으로 닫을 수 있도록 TCP 재설정을 생성하기 위해 게이트웨이 데이터 경로 프로세스를 개선합니다.

수정 사항

이 업그레이드에는 다음과 같은 수정 사항이 포함되어 있습니다.

- HTTP 개체 이름에서 [및]의 URL 인코딩 문자가 게이트웨이에서는 디코딩되지만, 서버로 요청을 전송하기 전에 다시 인코딩되지 않는 문제를 수정합니다. 이로 인해 서버가 개체를 올바르게 찾을 수 없고 400 응답 코드를 반환합니다. 이 수정 사항을 통해 요청을 서버로 전송하기 전에 문자가 올바르게 다시 인코딩됩니다.
- SNI에 밑줄 표시가 있는 경우 프록시가 트래픽을 전달하지 않는 문제를 해결합니다. 이렇게 하면 프록시 구성에서 도메인 이름에 밑줄을 표시할 수 있습니다.
- 트래픽이 올바른 정책과 일치하지만, 올바르지 않은 인증서가 발급되는 문제를 수정합니다.
- 트래픽이 올바른 정책과 일치하지만, 올바르지 않은 인증서가 발급되는 문제를 수정합니다.
- 프록시 시간 초과로 인해 408 상태 코드가 생성되는 HTTP 명령(예: GitHub 저장소 복제)과 관련된 대용량 파일 전송 문제를 수정합니다.
- URL Filtering(URL 필터링) 범주 쿼리 시간 초과가 만료되어 트래픽이 거부되는 문제를 수정합니다.
- 업스트림 프록시의 문제로 인해 데이터 경로가 저절로 복구될 수 있는 인그레스 게이트웨이 관련 안정성 문제를 수정합니다.
- 특정 유형의 트래픽을 처리할 때 게이트웨이에서 추가 레이턴시가 발생할 수 있는 문제를 수정합니다.
- 메모리 프로파일링을 활성화할 때 트리거되는 불필요한 데이터 경로 재시작 문제를 수정합니다.
- 정책 변경으로 인해 트리거되는 데이터 경로 재시작으로 인해 게이트웨이가 간헐적으로 502를 생성할 수 있는 문제를 수정합니다.
- CPU 기반 자동 확장으로 인해 불필요한 스케일 아웃이 발생할 수 있는 문제를 수정합니다.
- 프록시 연결 유출 문제를 수정합니다.
- Multicloud Defense 게이트웨이 안정성 개선.