레거시 버전

다음 레거시 버전은 권장되지 않지만 계속 지원됩니다.

레거시 **Multicloud Defense** 게이트웨이 버전

버전 **23.10**

버전 **23.10-03 2024**년 **1**월 **11**일

수정 사항

이 릴리스에는 다음과 같은 수정 사항이 포함되어 있습니다.

- 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.
- 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.
- 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.
- 게이트웨이 안정성을 개선합니다.

버전 23.10-02 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 23.10-01 2023년 11월 3일

개선 사항

이 업그레이드에는 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 이벤트로 이동합니다. 이렇게 하면 시나리오 발생 시 많은 시스템 로그 메시지가 삭제되며, 각 세션과 연결된 이벤트로 오류가 생성됩니다. 이 시나리오가 발생하면 세션이 거부되고 이벤트가 이유를 보고합니다. 거부는 트래픽 요약 로그에도 표시됩니다.
- 백엔드 TLS 세션을 협상할 때 서버 인증서를 검증하도록 정방향 프록시 정책을 개선합니다. 인증서 검증은 기본적으로 비활성화되어 있지만, 모든 TLS 세션의 암호 해독 프로파일과 도메인(또는 도메인 집합) 단위의 FQDN 일치 개체에서 구성할 수 있습니다.
- 텔레포트와 통합되어 역방향 SSH를 수용할 수 있어 특히 공용 IP 없이 게이트웨이가 오케스트레이션된 경우 게이트웨이 인스턴스 관리 인터페이스에 더욱 쉽게 SSH로 연결할 수 있습니다. SSH에 대한 요건은 드물며, 고급 문제 해결 목적으로만 필요합니다. 인바운드 통신은 기본적으로 클라우드 서비스 제공자 제한(보안 그룹, 네트워크 보안 그룹, 방화벽 규칙)을 사용하여 금지됩니다.

수정 사항

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

- 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.
- DNS 확인 간격을 설정해도 DNS 확인 빈도가 변경되지 않는 DNS 기반 FQDN 캐싱 문제를 수정합니다.
- 게이트웨이의 비정상을 유발할 수 있는 패킷 수집 관련 문제를 수정합니다.
- 게이트웨이의 특정 로그에 개인 키 정보가 포함될 수 있는 문제를 수정합니다.
- 다양한 게이트웨이 안정성 문제를 수정합니다.
- CPU 문제를 야기하여 트래픽 처리 문제를 일으킬 수 있는 게이트웨이 메모리 유출 문제를 수정합니다.
- URI 정보가 트래픽 요약 로그에 표시되지 않는 문제를 수정합니다.
- L7DOS 이벤트가 URI를 올바르게 표시하지 않는 문제를 수정합니다.

버전 23.06

버전 23.06-14 2023년 11월 12일

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 23.06-13 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 23.06-12 2023년 10월 6일

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 **23.06-11 2023**년 **9**월 **27**일

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 **23.06-10 2023**년 **9**월 **19**일

수정 사항

이 업그레이드에는 다음과 같은 수정 사항이 포함되어 있습니다.

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

버전 **23.06-09 2023**년 **9**월 **10**일

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 **23.06-08 2023**년 **9**월 **3**일

수정 사항

이 업그레이드에는 다음과 같은 수정 사항이 포함되어 있습니다.

- 고정 IP를 포함하는 DNS 기반 주소 개체가 제대로 일치되지 않는 문제를 수정합니다.

버전 **23.06-07 2023**년 **8**월 **29**일

수정 사항

이 업그레이드에는 다음과 같은 수정 사항이 포함되어 있습니다.

- 페이로드가 200KB보다 큰 HTTP POST를 전송할 때 트래픽이 삭제되는 정방향 프록시 문제를 수정합니다.

버전 23.06-06 2023년 8월 23일

수정 사항

이 업그레이드에는 다음과 같은 수정 사항이 포함되어 있습니다.

- SNI에 밑줄 표시가 있는 경우 프록시가 트래픽을 전달하지 않는 문제를 해결합니다. 이렇게 하면 프록시 구성에서 도메인 이름에 밑줄을 표시할 수 있습니다.
- 게이트웨이 안정성을 개선합니다.
- 프록시 시간 초과로 인해 408 상태 코드가 생성되는 HTTP 명령(예: GitHub 저장소 복제)과 관련된 추가적인 대용량 파일 전송 문제를 수정합니다.
- 트래픽이 올바른 정책과 일치하지만, 올바르지 않은 인증서가 발급되는 문제를 수정합니다.
- URL Filtering(URL 필터링) 범주 쿼리 시간 초과가 만료되어 트래픽이 거부되는 문제를 수정합니다.
- 프록시 연결 유출 문제를 수정합니다. 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.

버전 23.06-05 2023년 8월 4일

수정 사항

이 업그레이드에는 다음과 같은 수정 사항이 포함되어 있습니다.

- 밑줄 표시를 사용하는 HTTP 헤더가 프록시 규칙에서 전달되지 않는 문제를 수정합니다. 이렇게 하면 프록시 구성에서 헤더에 밑줄을 표시할 수 있습니다.
- 프록시 시간 초과로 인해 408 상태 코드가 생성되는 HTTP 명령(예: GitHub 저장소 복제)과 관련된 대용량 파일 전송 문제를 수정합니다.
- 처음에 정방향 프록시 규칙으로 처리된 후 일치 상태가 개선되어 전달 규칙으로 처리된 HTTP 트래픽이 거부되어야 하는데 허용되는 문제를 수정합니다.

버전 23.06-04 2023년 7월 27일

수정 사항

이 업그레이드에는 다음과 같은 수정 사항이 포함되어 있습니다.

- 안티멀웨어 엔진에서 처리한 특정 트래픽 유형으로 인해 CPU 과부하가 발생하여 트래픽 처리가 지연될 수 있는 문제를 수정합니다.

버전 **23.06-03 2023**년 **7**월 **21**일

수정 사항

이 업그레이드에는 다음과 같은 수정 사항이 포함되어 있습니다.

- 정책 규칙 집합에 IP/CIDR 포함 및 제외 혼합을 사용하는 주소 개체가 포함된 경우 새 게이트웨이 구축에서 가져오기 오류가 발생할 수 있는 문제를 수정합니다.

버전 **23.06-02 2023**년 **7**월 **19**일

수정 사항

이 업그레이드에는 다음과 같은 수정 사항이 포함되어 있습니다.

- CIDR 기반 주소 개체에 대한 업데이트가 데이터 경로 근무자에 제대로 적용되지 않아 잘못된 규칙 일치가 발생하는 문제를 수정합니다.
- DNS 캐시가 적절하게 설정되었지만, 데이터 경로 근무자에 올바르게 적용되지 않아 잘못된 규칙 일치가 발생하는 DNS 기반 FQDN 주소 개체 문제를 수정합니다.
- 동일한 L3/L4(IP/포트/프로토콜) 일치 기준에 대한 전달 규칙에 앞서 정방향 프록시 규칙이 선행되지만, L5(SNI) 일치가 뚜렷하면 적절한 규칙 일치가 발생하더라도 트래픽이 전달로 처리되는 데이터 경로 처리 동작을 수정합니다. 전달 및 정방향 프록시 규칙의 순서가 반대인 경우에도 유사한 동작이 발생합니다. 이 동작이 발생하는 이유는 L5(SNI) 일치를 수용하기 위해 SNI를 가져오려면 TLS hello 메시지를 수신할 수 있도록 TCP 핸드셰이크가 완전히 설정되어야 하기 때문입니다. TCP 핸드셰이크가 완료되면 첫 번째 규칙의 규칙 유형에 의해 트래픽이 이미 처리된 것입니다. 세션이 설정되면 트래픽 처리를 전달에서 정방향 프록시로, 또는 그 반대로 변경할 수 없습니다. 정책 규칙 집합에 이 충돌이 구성된 경우 데이터 경로가 충돌을 탐지하고 시스템 로그 메시지를 생성합니다. 충돌하는 규칙으로 트래픽을 성공적으로 처리할 수 없으므로 트래픽이 거부됩니다.
- 업스트림 프록시의 문제로 인해 데이터 경로가 저절로 복구될 수 있는 인그레스 게이트웨이 관련 안정성 문제를 수정합니다.
- 데이터 경로 재시작 시 CPU가 급증하여 불필요한 자동 확장이 발생할 수 있는 문제를 수정합니다.

버전 **23.06-01 2023**년 **7**월 **6**일

수정 사항

이 업그레이드에는 다음과 같은 수정 사항이 포함되어 있습니다.

- GCP 게이트웨이가 지원 관련 진단 번들을 생성할 수 없는 문제를 수정합니다.

- 프로파일 변경이 적용되지 않았는데 NTP 프로파일이 게이트웨이에 반복적으로 적용되는 문제를 수정합니다.
- 게이트웨이에 빈 주소 개체를 적용하면 트래픽 처리 문제가 발생하는 현상을 해결합니다.
- NTP 프로파일과 로그 전달 프로파일을 게이트웨이에 동시에 적용할 때 불필요한 데이터 경로 자가 복구가 발생하는 문제를 수정합니다. 이 문제는 프로파일이 오케스트레이션을 사용하여 적용되는 경우에만 표면화됩니다. 작업이 독립적이고, 모두 순차적으로 이루어지며, 매우 짧은 시간 내에 발생하기 때문입니다.
- 3개 이상의 레벨이 포함된 도메인으로 규칙이 구성된 경우 인그레스 게이트웨이가 잘못된 인증서를 발급할 수 있는 문제를 수정합니다.
- 주소 개체를 자주 변경하면 데이터 경로가 추가 변경 사항을 수락하지 않을 수 있는 문제를 수정합니다.
- FQDN 일치를 사용하는 규칙 집합으로 트래픽이 처리될 때 거부 시 재설정(TCP 재설정)이 실행되지 않는 문제를 수정합니다.
- 게이트웨이에서 처리하는 트래픽의 경우, L4_FW 이벤트가 일관되게 생성되지 않는 문제를 수정합니다.
- WAF 작업을 "Allow Log(로그 허용)"에서 "Rule Default(규칙 기본값)"로 변경할 때 데이터 경로가 여러 번 재시작될 수 있는 문제를 수정합니다.
- 청크화된 전송-인코딩을 사용한 HTTP 트래픽이 WAF에서 데이터 경로 자체 복구를 트리거하여 많은 메모리 소비를 유발할 수 있는 문제를 수정합니다. 트래픽을 중단시킬 수 있는 자동 데이터 경로 재시작으로 이어지는 느린 메모리 유출 문제를 수정합니다.
- 데이터 경로 자체 복구를 유발할 수 있는 메모리 문제를 수정합니다.

버전 23.04

버전 23.04-18 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.

버전 23.04-17 2023년 8월 23일

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.

버전 23.04-16 2023년 8월 22일

수정 사항

이 업그레이드에는 다음과 같은 개선 사항이 포함되어 있습니다.

- SNI에 밑줄 표시가 있는 경우 프록시가 트래픽을 전달하지 않는 문제를 해결합니다. 이렇게 하면 프록시 구성에서 도메인 이름에 밑줄을 표시할 수 있습니다.
- 프록시 시간 초과로 인해 408 상태 코드가 생성되는 HTTP 명령(예: GitHub 저장소 복제)과 관련된 추가적인 대용량 파일 전송 문제를 수정합니다.
- 트래픽이 올바른 정책과 일치하지만, 올바르지 않은 인증서가 발급되는 문제를 수정합니다.
- URL Filtering(URL 필터링) 범주 쿼리 시간 초과가 만료되어 트래픽이 거부되는 문제를 수정합니다.
- 프록시 연결 유출 문제를 수정합니다.
- 게이트웨이 안정성을 개선합니다.

버전 23.04-14 2023년 7월 27일

수정 사항

이 업그레이드에는 다음과 같은 수정 사항이 포함되어 있습니다.

- 안티멀웨어 엔진에서 처리한 특정 트래픽 유형으로 인해 CPU 과부하가 발생하여 트래픽 처리가 지연될 수 있는 문제를 수정합니다.

버전 23.04-13 2023년 7월 27일

수정 사항

이 업그레이드에는 다음과 같은 수정 사항이 포함되어 있습니다.

- 안티멀웨어 엔진에서 처리한 특정 트래픽 유형으로 인해 CPU 과부하가 발생하여 트래픽 처리가 지연될 수 있는 문제를 수정합니다.

버전 23.04-12 2023년 7월 19일

수정 사항

이 업그레이드에는 다음과 같은 수정 사항이 포함되어 있습니다.

- CIDR 기반 주소 개체에 대한 업데이트가 데이터 경로 근무자에 제대로 적용되지 않아 잘못된 규칙 일치가 발생하는 문제를 수정합니다.
- DNS 캐시가 적절하게 설정되었지만, 데이터 경로 근무자에 올바르게 적용되지 않아 잘못된 규칙 일치가 발생하는 DNS 기반 FQDN 주소 개체 문제를 수정합니다.
- 동일한 L3/L4(IP/포트/프로토콜) 일치 기준에 대한 전달 규칙에 앞서 정방향 프록시 규칙이 선행되지만, L5(SNI) 일치가 뚜렷하면 적절한 규칙 일치가 발생하더라도 트래픽이 전달로 처리되는 데이터 경로 처리 동작을 수정합니다. 전달 및 정방향 프록시 규칙의 순서가 반대인 경우에도 유사한 동작이 발생합니다. 이 동작이 발생하는 이유는 L5(SNI) 일치를 수용하기 위해 SNI를 가져오려면 TLS hello 메시지를 수신할 수 있도록 TCP 핸드셰이크가 완전히 설정되어야 하기 때문입니다. TCP 핸드셰이크가 완료되면 첫 번째 규칙의 규칙 유형에 의해 트래픽이 이미 처리된 것입니다. 세션이 설정되면 트래픽 처리를 전달에서 정방향 프록시로, 또는 그 반대로 변경할 수 없습니다. 정책 규칙 집합에 이 충돌이 구성된 경우 데이터 경로가 충돌을 탐지하고 시스템 로그 메시지를 생성합니다. 충돌하는 규칙으로 트래픽을 성공적으로 처리할 수 없으므로 트래픽이 거부됩니다.
- 업스트림 프록시의 문제로 인해 데이터 경로가 저절로 복구될 수 있는 인그레스 게이트웨이 관련 안정성 문제를 수정합니다.
- 데이터 경로 재시작 시 CPU가 급증하여 불필요한 자동 확장이 발생할 수 있는 문제를 수정합니다.

버전 23.04-11 2023년 7월 10일

수정 사항

이 업그레이드에는 다음과 같은 수정 사항이 포함되어 있습니다.

- 게이트웨이의 자가 복구를 유발할 수 있는 Snort 엔진의 안정성 문제를 수정합니다.
- 긴 헤더를 포함하는 인그레스 트래픽이 역방향 프록시에서 400 응답 코드를 생성하는 문제를 수정합니다.
- 규칙이 암호 해독 예외 설정을 포함하는 여러 행이 있는 FQDN 일치 프로파일을 사용할 때 트래픽을 전달 프록시 규칙에서 제대로 처리하지 않는 문제를 수정합니다.

버전 23.04-10: 2023년 6월 28일

수정 사항

이 업그레이드에는 다음과 같은 수정 사항이 포함되어 있습니다.

- DNS 기반 캐시 설정을 게이트웨이에 적용할 때 게이트웨이 인스턴스가 비정상 상태가 되는 문제를 수정합니다.

버전 23.04-09: 2023년 6월 25일

수정 사항

이 업그레이드에는 다음과 같은 수정 사항이 포함되어 있습니다.

- 일관된 게이트웨이 상태를 보장하기 위해 제공된 15일 주기의 게이트웨이 데이터 경로 자가 복구를 제거합니다. 이는 2년 전에 통합되어 파악하고 수정하기 어려운 문제를 해결하기 위해 통합되었습니다. 이 문제는 이후 해결되었지만 주기적인 자가 복구는 제거되지 않았습니다. 이는 더 이상 필요하지 않아 제거되었습니다.
- GCP 게이트웨이가 지원 관련 진단 번들을 생성할 수 없는 문제를 수정합니다.
- 프로파일 변경이 적용되지 않았는데 NTP 프로파일이 게이트웨이에 반복적으로 적용되는 문제를 수정합니다.
- FQDN 필터링 프로파일이 적용될 때 정책 규칙 집합이 지속적인 "Updating(업데이트)" 상태에 있을 수 있는 문제를 수정합니다.
- 게이트웨이에 빈 주소 개체를 적용하면 트래픽 처리 문제가 발생하는 현상을 해결합니다.
- NTP 프로파일과 로그 전달 프로파일을 게이트웨이에 동시에 적용할 때 불필요한 데이터 경로 자가 복구가 발생하는 문제를 수정합니다. 이 문제는 프로파일이 오케스트레이션을 사용하여 적용되는 경우에만 표면화됩니다. 작업이 독립적이고, 모두 순차적으로 이루어지며, 매우 짧은 시간 내에 발생하기 때문입니다.

버전 23.04-07 2023년 6월 14일

수정 사항

이 업그레이드에는 다음과 같은 수정 사항이 포함되어 있습니다.

- WAF 작업을 "Allow Log(로그 허용)"에서 "Rule Default(규칙 기본값)"로 변경할 때 데이터 경로가 여러 번 재시작될 수 있는 문제를 수정합니다.
- 사전 데이터 경로 자가 복구로 해결된 느린 세션 풀 유출과 관련하여 23.04-05에서 변경된 사항을 되돌리는 업데이트를 제공합니다. 이전 업데이트에서는 선점할 수 없는 데이터 경로 자가 복구를 유발할 수 있습니다. 이 릴리스는 초기 문제가 완전히 해결되는 동안 안정성을 보장합니다.

버전 23.04-06 2023년 6월 8일

수정 사항

이 업그레이드에는 다음과 같은 수정 사항이 포함되어 있습니다.

- 게이트웨이에서 처리하는 트래픽의 경우, L4_FW 이벤트가 일관되게 생성되지 않는 문제를 수정합니다.
- 청크 전송 인코딩이 포함된 HTTP 트래픽이 WAF에서 데이터 경로 자체 복구를 트리거하여 대규모 메모리 소비를 유발할 수 있는 문제를 수정합니다.

버전 **23.04-05 2023**년 **6**월 **1**일

수정 사항

이 업그레이드에는 다음과 같은 개선 사항이 포함되어 있습니다.

- 트래픽을 중단할 수 있는 자동 데이터 경로 재시작으로 이어지는 느린 메모리 누수를 수정합니다.
- 사전 데이터 경로 자가 복구로 이어질 수 있는 매우 느린 세션 풀 유출을 수정합니다.
- FQDN 일치를 사용하는 규칙 집합으로 트래픽이 처리될 때 거부 시 재설정(TCP 재설정)이 실행되지 않는 문제를 수정합니다.
- 3개 이상의 레벨이 포함된 도메인으로 규칙이 구성된 경우 인그레스 게이트웨이가 잘못된 인증서를 발급할 수 있는 문제를 수정합니다.
- 주소 개체를 자주 변경하면 데이터 경로가 추가 변경 사항을 수락하지 않을 수 있는 문제를 수정합니다.
- 데이터 경로 자가 복구를 발생시키는 다양한 게이트웨이 안정성 문제를 수정합니다.

버전 **23.04-04 2023**년 **5**월 **19**일

수정 사항

이 업그레이드에는 다음과 같은 수정 사항이 포함되어 있습니다.

- FQDN 일치를 사용하는 정책 규칙 집합 규칙에 대한 트래픽 처리 문제를 해결합니다. FQDN과 일치하는 TLS SNI를 포함하는 세션은 처음에는 거부되지만 후속 세션은 허용되지 않습니다.

버전 **23.04-03 2023**년 **5**월 **16**일

수정 사항

이 업그레이드에는 다음과 같은 수정 사항이 포함되어 있습니다.

- 게이트웨이 설정으로 활성화된 향상된 메모리 프로파일링 모드를 제공합니다. 고급 문제 해결에서 메모리 사용량을 파악하는 것이 유용합니다.

버전 23.04-02 2023년 5월 2일

수정 사항

이 업그레이드에는 다음과 같은 수정 사항이 포함되어 있습니다.

- OCI 게이트웨이 관리 인터페이스에 대한 SSH 세션을 설정하면 실패하고 유효하지 않은 사용자 어카운트로 인해 권한이 거부되는 문제를 수정합니다.
- 게이트웨이에 연결된 사용자 정의 NTP 프로파일을 게이트웨이에 적용할 경우 NTP 설정이 올바르게 구성되지 않는 문제를 수정합니다.

버전 23.04-01 2023년 4월 20일

개선 사항

이 업그레이드에는 다음과 같은 개선 사항이 포함되어 있습니다.

- 공유 암호 그룹이 없어 TLS 세션을 협상할 수 없는 경우 게이트웨이의 오류 메시지 보고 기능을 개선합니다. "TLS_ERROR" 유형의 보안 이벤트에 대한 오류 메시지를 보다 상세하게 설명하도록 개선하였습니다.
- Valtix 게이트웨이에서 사용되는 Centos 기본 이미지의 강화를 개선합니다. 이제 기본 이미지는 Centos9으로 이동되었으며 엄격한 규정 준수 요구 사항이 있는 환경을 수용하도록 강화되었습니다.
- 게이트웨이의 NTP 설정 구성을 지원합니다. 게이트웨이에 할당할 수 있는 NTP 프로파일을 사용하여 게이트웨이 NTP 설정을 구성할 수 있습니다.
- 인그레스 보호를 위한 Azure GLLB 기반 아키텍처를 지원합니다.

수정 사항

이 업그레이드에는 다음과 같은 수정 사항이 포함되어 있습니다.

- 트래픽에 SNI가 없을 때 트래픽이 잘못된 규칙에 의해 처리되는 FQDN 일치 개체 문제를 수정합니다.
- IDS/IPS 및 WAF 맞춤형 규칙을 지원하기 전에 생성된 DLP 및 IDS/IPS 프로파일이 프로파일을 수정 및 저장하지 않는 한 예상대로 작동하지 않을 수 있는 문제를 수정합니다.
- 게이트웨이가 클라이언트에 잘못된 인증서를 발급할 수 있는 대량의 버스트 TLS 트래픽과 관련된 인그레스 게이트웨이 문제를 수정합니다. 이 시나리오는 드물게 게이트웨이 릴리스 22.12-04 이하에서 발생할 수 있는 다운스트림 문제입니다. 이 수정은 다운스트림 문제에 도달하지 않도록 하여 다운스트림 문제를 해결하며, 문제가 발생하지 않도록 하기 위한 보호 장치입니다.
- 두 개 이상의 고유한 리스너 포트로 정책이 지정되고 각 리스너 포트가 동일한 SNI 및 백엔드 설정을 공유하도록 지정된 경우 동일한 인증서가 발급될 수 있는 문제를 수정합니다.

- 업데이트된 패키지를 로드하지 못한 후 데이터 경로 엔진이 시작되지 않는 문제를 수정합니다. 이 문제는 패키지 업데이트가 Linux 커널 자체가 아닌 Vertix에 의해 처리되는 새 CentOS 9 기본 이미지에서 해결되었습니다.
- FQDNFILTER 이벤트에서 반대 방향의 소스 및 대상 IP/Port 정보를 표시하는 문제를 수정합니다.
- 작업이 거부로 구성된 경우 이전 컨트롤러 버전을 사용하여 생성한 프로파일에서 URL을 올바르게 거부하지 않는 URL 필터 프로파일 관련 문제를 수정합니다.
- L7DOS 프로파일 설정 관련 트래픽 처리 문제를 수정합니다. 프로파일이 Request Rate(요청 속도) 또는 Burst Size(버스트 크기) 1로 설정된 경우 데이터 경로가 트래픽을 제대로 제한하지 않습니다.
- L7DOS 프로파일 설정 관련 트래픽 처리 문제를 수정합니다. Request Rate(요청 속도) 또는 Burst Size(버스트 크기) 값이 0인 프로파일을 설정하면 데이터 경로가 지정된 URL/URI와 관련된 모든 트래픽을 억제해야 합니다. L7DOS 프로파일을 사용하여 이 방법을 사용하여 URL/URI를 차단할 수 있지만, 권장 방법은 URL 필터 프로파일을 생성하고 이 프로파일을 URL 관련 트래픽을 처리하는 정책 규칙 집합 규칙에 적용하는 것입니다.
- 게이트웨이에서 CSP 스토리지 시스템(S3 버킷, GCP 로깅)으로 직접 전송되는 트래픽 요약 로그 및 이벤트의 문제를 해결하며, 여기서 필드 값에 대한 식별 이름이 정수로 표시됩니다. 이렇게 하려면 사용자가 문서화한 정수에서 식별 이름으로 변환해야 합니다. 이제 로그 및 이벤트에 정수 값이 아닌 식별 이름이 포함되어 있습니다.
- 다양한 트래픽 패턴과 관련된 이그레스 게이트웨이의 안정성 문제를 수정합니다.
- 중복 호스트 헤더가 백엔드 연결에 추가되는 Websockets 프록시 관련 문제를 수정합니다. 일반적으로 이는 RFC에서 다중(및 중복) 호스트 헤더가 허용된다고 지정하므로 문제가 되지 않습니다. 그러나 여러 호스트 헤더를 허용하지 않는 일부 애플리케이션 프레임워크도 있습니다. 애플리케이션 서버로서의 Ngnix는 이러한 시스템 중 하나입니다. Nginx는 여러 호스트 헤더가 포함된 HTTP 트래픽을 수신하면 세션을 거부하고 400 Bad Request(400 잘못된 요청)로 응답합니다.
- 취약성 스캐너에서 정보 알림이 수신될 수 있는 게이트웨이 관리 Centos Linux 컨테이너 관련 OS 취약성을 수정합니다.
- 드물게 데이터 경로 자가 복구를 유발할 수 있는 Azure 게이트웨이용 MLX4 DPDK 드라이버 문제를 수정합니다.
- CPU 기반 Auto-Scaling(자동 확장) 민감도를 줄이기 위해 Auto-Scaling CPU 임계값을 75%에서 95%로 변경합니다.

버전 **23.02**

버전 **23.02-10: 2023**년 **6**월 **28**일

수정 사항

이 업그레이드에는 다음과 같은 수정 사항이 포함되어 있습니다.

- DNS 기반 캐시 설정을 게이트웨이에 적용할 때 게이트웨이 인스턴스가 비정상 상태가 되는 문제를 수정합니다.

버전 23.02-09: 2023년 6월 25일

수정 사항

이 업그레이드에는 다음과 같은 수정 사항이 포함되어 있습니다.

- 일관된 게이트웨이 상태를 보장하기 위해 제공된 15일 주기의 게이트웨이 데이터 경로 자가 복구를 제거합니다. 이는 2년 전에 통합되어 파악하고 수정하기 어려운 문제를 해결하기 위해 통합되었습니다. 이 문제는 이후 해결되었지만 주기적인 자가 복구는 제거되지 않았습니다. 이는 더 이상 필요하지 않아 제거되었습니다.
- GCP 게이트웨이가 지원 관련 진단 번들을 생성할 수 없는 문제를 수정합니다.
- 프로파일 변경이 적용되지 않았는데 NTP 프로파일이 게이트웨이에 반복적으로 적용되는 문제를 수정합니다.
- FQDN 필터링 프로파일이 적용될 때 정책 규칙 집합이 지속적인 "Updating(업데이트)" 상태에 있을 수 있는 문제를 수정합니다.
- 게이트웨이에 빈 주소 개체를 적용하면 트래픽 처리 문제가 발생하는 현상을 해결합니다.
- NTP 프로파일과 로그 전달 프로파일을 게이트웨이에 동시에 적용할 때 불필요한 데이터 경로 자가 복구가 발생하는 문제를 수정합니다. 이 문제는 프로파일이 오케스트레이션을 사용하여 적용되는 경우에만 표면화됩니다. 작업이 독립적이고, 모두 순차적으로 이루어지며, 매우 짧은 시간 내에 발생하기 때문입니다.

버전 23.02-08 2023년 6월 15일

수정 사항

이 업그레이드에는 다음과 같은 수정 사항이 포함되어 있습니다.

- WAF 작업을 "Allow Log(로그 허용)"에서 "Rule Default(규칙 기본값)"로 변경할 때 데이터 경로가 여러 번 재시작될 수 있는 문제를 수정합니다.
- 사전 데이터 경로 자가 복구로 해결된 느린 세션 풀 유출과 관련하여 23.04-05에서 변경된 사항을 되돌리는 업데이트를 제공합니다. 이전 업데이트에서는 선점할 수 없는 데이터 경로 자가 복구를 유발할 수 있습니다. 이 릴리스는 초기 문제가 완전히 해결되는 동안 안정성을 보장합니다.

버전 23.02-07 2023년 6월 8일

수정 사항

이 업그레이드에는 다음과 같은 수정 사항이 포함되어 있습니다.

- 게이트웨이에서 처리하는 트래픽의 경우, L4_FW 이벤트가 일관되게 생성되지 않는 문제를 수정합니다.
- 청크 전송 인코딩이 포함된 HTTP 트래픽이 WAF에서 데이터 경로 자체 복구를 트리거하여 대규모 메모리 소비를 유발할 수 있는 문제를 수정합니다.

버전 **23.02-06 2023**년 **6**월 **2**일

수정 사항

이 업그레이드에는 다음과 같은 수정 사항이 포함되어 있습니다.

- 트래픽을 중단할 수 있는 자동 데이터 경로 재시작으로 이어지는 느린 메모리 누수를 수정합니다.
- 사전 데이터 경로 자가 복구로 이어질 수 있는 매우 느린 세션 풀 유출을 수정합니다.
- FQDN 일치를 사용하는 규칙 집합으로 트래픽이 처리될 때 거부 시 재설정(TCP 재설정)이 실행되지 않는 문제를 수정합니다.
- 3개 이상의 레벨이 포함된 도메인으로 규칙이 구성된 경우 인그레스 게이트웨이가 잘못된 인증서를 발급할 수 있는 문제를 수정합니다.
- 주소 개체를 자주 변경하면 데이터 경로가 추가 변경 사항을 수락하지 않을 수 있는 문제를 수정합니다.
- 데이터 경로 자가 복구를 발생시키는 다양한 게이트웨이 안정성 문제를 수정합니다.

버전 **23.02-05 2023**년 **5**월 **22**일

개선 사항

이 업그레이드에는 다음과 같은 개선 사항이 포함되어 있습니다.

- 게이트웨이 설정으로 활성화된 향상된 메모리 프로파일링 모드를 제공합니다. 고급 문제 해결에서 메모리 사용량을 파악하는 것이 유용합니다.

수정 사항

이 업그레이드에는 다음과 같은 수정 사항이 포함되어 있습니다.

- FQDN 일치를 사용하는 정책 규칙 집합 규칙에 대한 트래픽 처리 문제를 해결합니다. FQDN과 일치하는 TLS SNI를 포함하는 세션은 처음에는 거부되지만 후속 세션은 허용되지 않습니다.

버전 **23.02-04 2023**년 **4**월 **14**일

수정 사항

이 업그레이드에는 다음과 같은 수정 사항이 포함되어 있습니다.

- 중복 호스트 헤더가 백엔드 연결에 추가되는 Websockets 프록시 관련 문제를 수정합니다. 일반적으로 이는 RFC에서 다중(및 중복) 호스트 헤더가 허용된다고 지정하므로 문제가 되지 않습니다. 그러나 여러 호스트 헤더를 허용하지 않는 일부 애플리케이션 프레임워크도 있습니다. 애플리케이션 서버로서의 Ngnix는 이러한 시스템 중 하나입니다. Nginx는 여러 호스트 헤더가 포함된 HTTP 트래픽을 수신하면 세션을 거부하고 400 Bad Request(400 잘못된 요청)로 응답합니다.
- TLS 재협상 구성을 구성 가능한 설정으로 이동했습니다. 재협상을 사용하는 이전 클라이언트와의 잠재적인 문제로 인해, 재협상을 기본 상태인 활성화로 변경했습니다.
- CPU 기반 Auto-Scaling(자동 확장) 민감도를 줄이기 위해 Auto-Scaling CPU 임계값을 75%에서 95%로 변경합니다.

버전 **23.02-03 2023**년 **3**월 **7**일

수정 사항

이 업그레이드에는 다음과 같은 수정 사항이 포함되어 있습니다.

- IDS/IPS 및 WAF 맞춤형 규칙을 지원하기 전에 생성된 DLP 및 IDS/IPS 프로파일이 프로파일을 수정 및 저장하지 않는 한 예상대로 작동하지 않을 수 있는 문제를 수정합니다.

버전 **23.02-02 2023**년 **2**월 **20**일

수정 사항

이 업그레이드에는 다음과 같은 수정 사항이 포함되어 있습니다.

- 게이트웨이가 클라이언트에 잘못된 인증서를 발급할 수 있는 대량의 버스트 TLS 트래픽과 관련된 인그레스 게이트웨이 문제를 수정합니다. 이 시나리오는 드물게 게이트웨이 릴리스 23.02-01에서 발생할 수 있는 다운스트림 문제입니다. 이 수정은 다운스트림 문제에 도달하지 않도록 하여 다운스트림 문제를 해결하며, 문제가 발생하지 않도록 하기 위한 보호 장치입니다.
- CVE-2009-3555와 관련된 취약성을 해결하기 위해 TLS 재협상을 비활성화했습니다.
- FQDN 필터링 이벤트에 역방향 소스/대상 IP/포트 정보가 표시되는 문제를 수정합니다.

버전 **23.02-01 2023**년 **2**월 **15**일

개선 사항

이 업그레이드에는 다음과 같은 개선 사항이 포함되어 있습니다.

- IP 주소 캐싱을 수용하도록 DNS 기반 FQDN 주소 개체를 개선합니다. 이 개선 사항에서는 DNS 확인 빈도(업데이트 간격), IP 주소 TTL(항목 TTL) 및 IP 주소 캐시 크기(캐시)와 관련된 구성 가능한 게이트웨이 설정 집합을 제공합니다. 이러한 설정은 Terraform만을 사용하여 적용할 수 있습니다. 적용되지 않는 경우 기본값은 DNS 확인 빈도가 60(초), IP 주소 TTL(캐싱 없음)의 경우 0(초), IP 주소 캐시 크기(캐싱 없음)의 경우 0(주소 수)입니다.

- FQDN 일치 프로파일이라는 FQDN 프로파일의 새로운 변형을 도입하도록 이그레스/이스트-웨스트 정책 규칙 집합 규칙 일치 기준을 개선합니다. FQDN 프로파일 변형은 정책이 SNI에서 매칭될 수 있도록 TLS 암호화 트래픽에 적용할 수 있는 PCRE 정의 FQDN 집합입니다. 이를 통해 FQDN을 기반으로 세분화된 제어가 필요한 정책에 대한 유연성을 강화하여 세분화 정책을 개선할 수 있습니다.

수정 사항

이 업그레이드에는 다음과 같은 수정 사항이 포함되어 있습니다.

- 연결이 null이면 데이터 경로 자체 복구가 발생할 수 있는 세션 업스트림 연결과 관련된 인그레스 게이트웨이 문제를 수정합니다.
- 청크 인코딩이 활성화된 상태에서 대형 POST 명령과 관련된 WAF의 안정성 문제를 수정합니다.
- 프론트엔드(클라이언트에서 게이트웨이로)가 활성화되고 백엔드(게이트웨이에서 서버)에서 KA가 비활성화된 HTTP Keepalives와 관련된 인그레스 게이트웨이 세션 풀 소진 문제를 수정합니다.
- 서비스가 존재하지 않아 정책이 빈 IP/CIDR을 포함하는 GCP 서비스를 활용하는 동적 정책과 관련된 문제를 수정합니다. 설정이 유효하므로 게이트웨이가 정책에 빈 IP/CIDR이 포함될 수 있는 경우를 처리해야 합니다.
- 데이터 경로 자가 복구를 유발할 수 있는 규칙 일치 관련 문제를 수정합니다.
- Azure가 요청된 것과 다른 인터페이스 유형을 할당하는 경우 게이트웨이 프로비저닝과 관련된 시스템 로그 메시지로 표시되는 Azure 생성 메시지를 제거하고, 잠재적인 성능 저하를 암시하는 경고 메시지를 게시합니다. 메시지는 `TYPE_AZURE_DEGRADED_PERFORMANCE`로 표시됩니다. 할당된 인터페이스 유형과 관련된 성능 영향은 없습니다.
- 모든 활용 사례의 게이트웨이 안정성을 개선하여 잠재적인 세션 풀 소진을 제거합니다.

레거시 **Multicloud Defense Terraform** 제공자 버전

버전 **23.7**

버전 **23.7.2 2023**년 **7**월 **27**일

수정 사항

이 버전에는 다음과 같은 수정 사항이 포함되어 있습니다.

- 정책 인수 없이 `mode=MATCH`인수를 사용하는 FQDN 프로파일(`valtix_fqdn_profile`) 리소스의 경우 일치하는 트래픽이 거부되는 문제를 수정합니다. 정책 인수는 지정할 필요가 없으며 Terraform Provider 설명서에 인수로 나열되어 있지 않습니다.

버전 23.7.1 2023년 7월 24일

수정 사항

이 릴리스에는 다음과 같은 수정 사항이 포함되어 있습니다.

- Azure VNet에 대한 동적 VPC 주소 개체(`valix_address_object`) 리소스를 생성할 때 "'지역' 매개변수가 지원되지 않습니다." 오류가 발생하는 문제를 수정합니다.
- `mode=MATCH`인수가 잘못된 FQDN 프로파일(`valtix_fqdn_profile`) 리소스에 'policy' 인수를 요구하는 문제를 수정합니다.

버전 23.6

버전 23.6.1, 2023년 7월 17일

개선 사항

이 릴리스에는 다음과 같은 개선 사항이 포함되어 있습니다.

- 알림 프로파일(`valtix_alert_profile`) 리소스를 개선하여 Webex Teams에 알림(시스템 로그, 감사 로그) 전송을 지원했습니다.
- 동적 사용자 정의 태그 주소 개체(`valtix_address_object`) 리소스의 범위로 서브넷 리소스를 포함하도록 지원을 추가합니다.

수정 사항

이 릴리스에는 다음과 같은 수정 사항이 포함됩니다.

- Azure VNet에 대한 동적 VPC 주소 개체(`valix_address_object`) 리소스를 생성할 때 "'지역' 매개변수가 지원되지 않습니다." 오류가 발생하는 문제를 수정합니다.
- Azure에서 게이트웨이(`valtix_gateway`) 리소스를 구축할 때 중남부/미국 지역에 구축하려고 하면 오류가 발생하는 문제를 수정합니다.

버전 23.5

버전 23.5.1 2023년 6월 12일

개선 사항

이 릴리스에는 다음과 같은 개선 사항이 포함되어 있습니다.

- Valtix Terraform Provider를 미러링하는 Multicloud Defense Terraform 제공자을 게시했습니다. 새로운 Provider는 `ciscomcd` 이며 가까운 시일 내에 공개될 예정입니다. 제공자는 동시에 업데이트

되며 별도로 공지되지 않는 한 서로의 미러링을 나타냅니다. 가까운 시일 내에 Valtix 제공자는 더 이상 사용되지 않으며 시스코 제공자로 완전히 대체됩니다.

수정 사항

이 릴리스에는 다음과 같은 수정 사항이 포함되어 있습니다.

- 게이트웨이(`valtix_gateway`) 리소스를 Azure 영역 1 중남부/미국 지역으로 구축하여 오류가 발생하는 문제를 수정합니다.
- Azure 게이트웨이 로드 밸런서 기반 아키텍처에서 인그레스 게이트웨이를 구축할 때 Azure 게이트웨이 로드 밸런서 프런트 엔드 리소스 ID를 출력하도록 게이트웨이(`valtix_gateway`) 리소스의 특성을 개선합니다. 출력은 게이트웨이 엔드포인트(`gateway_gwlb_endpoints`) 속성의 일부로 지정됩니다.
- 정책 규칙 집합(`valtix_policy_rule_set`) 그룹 리소스가 적절한 구성원 리소스 인수를 참조하도록 수정합니다.

버전 23.4

버전 23.4.3 2023년 5월 23일

수정 사항

이 릴리스에는 다음과 같은 수정 사항이 포함됩니다.

- Azure 게이트웨이 로드 밸런서 기반 아키텍처에서 인그레스 게이트웨이를 구축할 때 Azure 게이트웨이 로드 밸런서 프런트 엔드 리소스 ID를 출력하도록 게이트웨이(`valtix_gateway`) 리소스의 특성을 개선합니다. 출력은 게이트웨이 엔드포인트(gateway_gwlb_endpoints) 속성의 일부로 지정됩니다.

버전 23.4.2 2023년 5월 11일

수정 사항

이 섹션에는 다음과 같은 수정 사항이 포함되어 있습니다.

- NTP 프로파일(`valtix_ntp_profile`) 데이터 소스 관련 리소스에 액세스하려고 하면 유효하지 않은 데이터 소스 오류가 발생하는 문제를 수정합니다.
- NTP 프로파일(`valtix_ntp_profile`) 리소스 및 데이터 소스 정보를 포함하도록 Terraform 문서를 업데이트합니다.

버전 23.4.1 2023년 4월 20일

개선 사항

이 릴리스에는 다음과 같은 개선 사항이 포함되어 있습니다.

- 더 이상 사용되지 않는 `child_rule_set_ids`인수를 대체하는 `group_member_ids` 인수를 포함하도록 정책 규칙 집합(`valtix_policy_rule_set`) 리소스를 변경합니다.

수정 사항

이 릴리스에는 다음과 같은 수정 사항이 포함되어 있습니다.

- 게이트웨이 리소스(`valtix_gateway`)와 관련된 Terraform **Import(**가져오기**)**작업 관련 문제를 수정합니다.
- Azure 게이트웨이에 대한 SSH 키 쌍(`ssh_key_pair`)을 지정할 때 인수가 지원되지 않는다는 오류가 발생하는 게이트웨이 리소스(')의 문제를 수정합니다.
- WAF 규칙 ID 949110 및 959100의 억제와 관련된 문제를 수정합니다. 이러한 규칙 ID는 정보 제공용이며, WAF 이상 점수(각각 요청 및 응답)가 초과되었음을 알리는 보안 이벤트를 정의하며 WAF 프로파일 리소스(`valtix_profile_application_threat`) 설정을 기준으로 수행된 작업이 있습니다. 이러한 규칙 ID를 억제하면 Events(이벤트) 정보가 생성되지 않습니다. 이 수정은 이러한 규칙 ID를 억제하여 정보 제공 이벤트가 항상 생성되는 기능을 금지합니다.
- 정책 규칙 리소스(`valtix_policy_rules`)와 관련된 Terraform 가져오기 작업의 문제를 수정합니다.