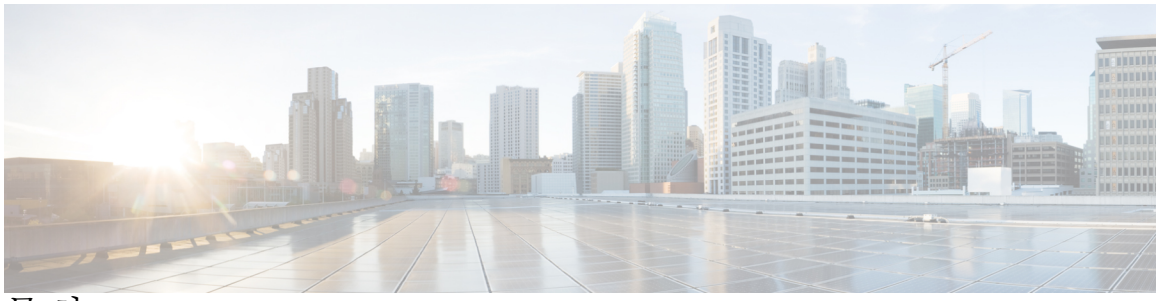
Cisco Multicloud Defense 릴리스 노트

초판: 2023년 8월 25일

최종 변경: 2024년 5월 29일

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

© 2023 Cisco Systems, Inc. 모든 권리 보유.



목 차

장 1 환영합니다. 1

멀티 클라우드 방어 소개 1

권장 버전 2

지원되는 버전 2

추가 리소스 및 지원 3

장 2 멀티 클라우드 방어 구성 요소 5

멀티 클라우드 방어 컨트롤러 5

멀티 클라우드 방어 게이트웨이 6

멀티 클라우드 Defense Terraform 제공자 6

장 3 개선 사항 및 수정 사항 7

멀티 클라우드 방어 컨트롤러 개선 사항 7

버전 24.02 2024년 2월 26일(권장) 7

버전 23.12 2023년 12월 14일 10

멀티 클라우드 방어 게이트웨이 개선 사항 13

버전 24.04 13

버전 24.04-01 2024년 5월 16일 13

버전 24.02 13

버전 24.02-02 2024년 4월 18일 13

버전 24.02-01 2024년 2월 28일 14

버전 23.10 16

버전 23.10-03 2024년 1월 11일 16

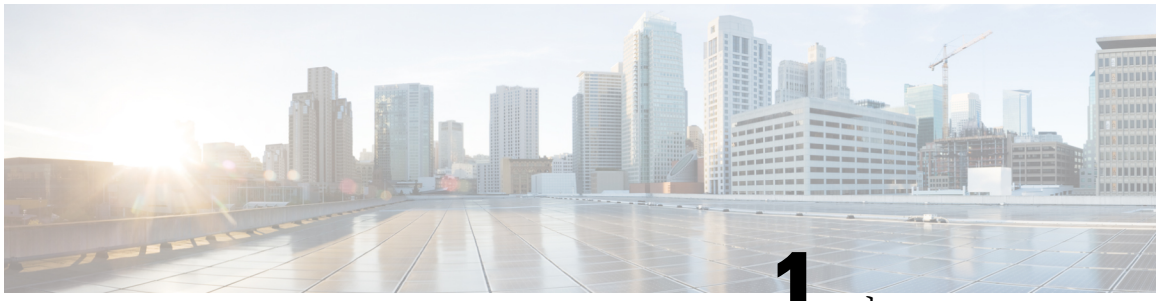
버전 23.10-02 2023년 11월 16일 16

버전 23.10-01 2023년 11월 3일 17
버전 23.08 18
버전 23.08-15-d1 2024년 5월 27일 18
버전 23.08-15-c1 2024년 5월 9일 18
버전 23.08-15-a2 2024년 5월 1일 18
버전 23.08-15-b1 2024년 4월 12일 19
버전 23.08-15-a1 2024년 4월 11일 19
버전 23.08-15: 2024년 3월 27일(권장) 19
버전 23.08-14-e1 2024년 3월 28일 20
버전 23.08-14-a2 2024년 3월 20일 20
버전 23.08-14-d1 2024년 3월 13일 21
버전 23.08-14-c1 2024년 2월 20일 21
버전 23.08-14-b1 2024년 2월 21일 21
버전 23.08-14-a1 2024년 2월 17일 22
버전 23.08-14 2024년 1월 25일 22
버전 23.08-12: 2024년 1월 18일 22
버전 23.08-11 2024년 1월 11일 22
버전 23.08-10 2023년 12월 18일 23
버전 23.08-09 2023년 11월 16일 23
버전 23.08-08 2023년 11월 8일 23
버전 23.08-07 2023년 10월 18일 24
버전 23.08-06 2023년 10월 7일 24
버전 23.08-05 2023년 10월 3일 24
버전 23.08-04 2023년 9월 19일 24
버전 23.08-03 2023년 9월 10일 24
버전 23.08-02 2023년 9월 3일 25
버전 23.08-01 2023년 8월 25일 25
레거시 게이트웨이 버전 26
버전 23.06 26
버전 23.04 30
버전 23.02 36

Terraform 제공자 개선 사항 40
버전 24.2.1 2024년 2월 31일(권장) 40
버전 23.10.1 2023년 11월 6일 41
버전 23.8.1 2023년 8월 22일 42
레거시 Terraform 버전 42
버전 23.7 42
버전 23.6 43
버전 23.5 43
버전 23.4 44

장 4 릴리스 및 서비스 정책 47
릴리스 버전 관리 및 일정 47
릴리스 수명 및 지원 48

51



1 장

환영합니다.

- 멀티 클라우드 방어 소개, on page 1
- 권장 버전, 2 페이지
- 지원되는 버전, on page 2
- 추가 리소스 및 지원, 3 페이지

멀티 클라우드 방어 소개

멀티 클라우드 방어(MCD)는 두 가지 주요 구성 요소인 멀티 클라우드 방어 컨트롤러 및 멀티 클라우드 방어 게이트웨이로 이루어진 포괄적인 보안 솔루션입니다. 이러한 구성 요소는 서로 함께 작동하여 안전한 멀티 클라우드 환경을 설정합니다.

멀티 클라우드 방어에서는 현재 AWS(Amazon Web Services), Azure, GCP(Google Cloud Platform) 및 Oracle OCI 클라우드 어카운트를 지원합니다. 이러한 플랫폼에 대한 지원 범위는 다양합니다.

기본적으로 멀티 클라우드 방어에서는 강력하고 효율적인 멀티 클라우드 보호 메커니즘을 위해 컨트롤러 오케스트레이션, 게이트웨이 통신 및 최적화된 데이터 경로 처리가 조화를 이루는 정교하고 간소화된 보안 프레임워크를 제공합니다.

이 설명서는 공용 클라우드 네트워킹 및 보안 개념에 대한 기본적인 이해를 갖추고 있으며, 다음과 같은 다양한 기능의 팀에 참여하는 실무자를 위해 마련되었습니다.

- 개발 운영(DevOps 및 DevSecOps)
- 보안 운영 센터(SOC)
- 보안 아키텍트 정보
- 보안 아키텍트 클라우드 아키텍트

추가 멀티 클라우드 방어 문서

멀티 클라우드 방어에 대한 추가 정보는 다음 문서에서 확인할 수 있습니다.

- 멀티 클라우드 방어 릴리스 정보

권장 버전

각 멀티 클라우드 방어 구성 요소에 대해 다음 릴리스를 사용할 것을 강력히 권장합니다.

멀티 클라우드 방어 컨트롤러

버전 24.02, 2024년 2월 26일

멀티 클라우드 방어 게이트웨이

버전 23.08-15, 2024년 3월 27일

멀티 클라우드 **Defense Terraform** 제공자

버전 24.2.1, 2024년 2월 31일

지원되는 버전

다음 버전은 현재 멀티 클라우드 방어 구성 요소에서 지원됩니다.

멀티 클라우드 방어 컨트롤러 버전

- 버전 24.02, 2024년 2월 26일
- 버전 23.12, 2023년 12월 14일

멀티 클라우드 방어 게이트웨이

- 버전 23.10-03, 2024년 1월 11일
- 버전 23.08-14, 2024년 1월 25일
- 버전 23.06-14, 2023년 11월 12일

멀티 클라우드 **Defense Terraform** 제공자

- 버전 23.10.1, 2023년 11월 6일
- 버전 23.8.1, 2023년 8월 22일
- 버전 23.7.2, 2023년 7월 27일
- 버전 23.6.1, 2023년 7월 17일

추가 리소스 및 지원

온라인 리소스

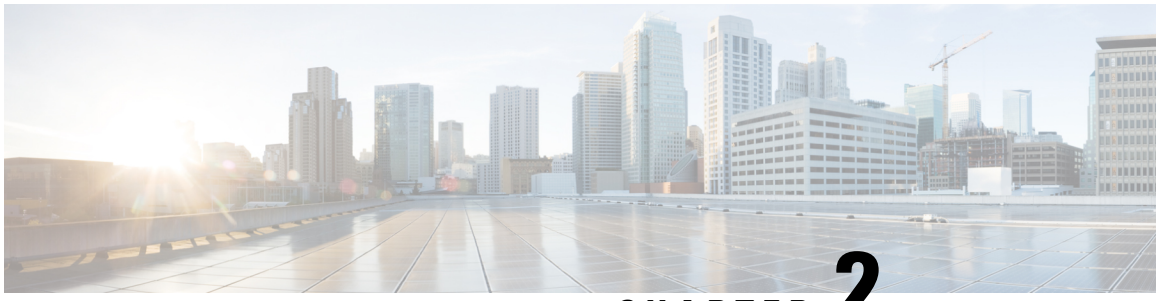
Cisco는 다음의 추가 문서를 제공합니다.

- Cisco Multicloud Defense 사용 설명서
- Cisco Multicloud Defense FAQ

Cisco에 문의

위에 나열된 온라인 리소스를 사용하여 문제를 해결할 수 없는 경우 Cisco TAC에 문의하십시오.

- Cisco TAC 이메일 문의: tac@cisco.com
- Cisco TAC(북미) 전화 문의: 1.408.526.7209 또는 1.800.553.2447
- Cisco TAC(전 세계) 전화 문의: Cisco 전 세계 지원 연락처



CHAPTER 2

멀티 클라우드 방어 구성 요소

다음 구성 요소가 멀티 클라우드 방어 경험을 구성합니다.

- 멀티 클라우드 방어 컨트롤러, on page 5
- 멀티 클라우드 방어 게이트웨이, on page 6
- 멀티 클라우드 Defense Terraform 제공자, on page 6

멀티 클라우드 방어 컨트롤러

멀티 클라우드 방어 컨트롤러는 CDO와 함께 제공되는 SaaS(Software as a Service) 구성 요소입니다. 멀티 클라우드 방어의 컨트롤 플레인으로 작동하며 관리자가 멀티 클라우드 방어의 모든 측면을 구축, 구성 및 관리할 수 있는 기능을 제공합니다. 또한 멀티 클라우드 방어 컨트롤러 또는 Terraform 제공자에서 수행되는 작업과 클라우드 서비스 제공자 내에서 해당 작업의 오케스트레이션 간의 변환 레이어이기도 합니다.

멀티 클라우드 방어 컨트롤러를 통해 제공되는 기능은 다음과 같습니다.

- 클라우드 서비스 제공자 계정 온보딩.
- 클라우드 서비스 제공자 자산 및 트래픽 가시성 검색.
- 서비스 VPC/VNet 생성 및 관리.
- 스포크 VPC/VNet 보호 관리.
- 게이트웨이 구축, 자동 확장 및 업데이트.
- 보안 정책 정의 및 구축.
- 타사 SIEM 및 알림 통합.
- 트래픽 및 보안 이벤트 조사와 분석.
- 검색 및 위협 인식 보고서 생성.

CDO 작업은 멀티 클라우드 방어 컨트롤러 업데이트를 담당합니다. 개선 사항 및 업데이트는 자주 제공되며, 계획된 릴리스 업데이트에 따라 정기적으로 제공되거나 중요 수정을 신속하게 해결하기 위해 핫픽스로 구축될 수 있습니다.

멀티 클라우드 방어 게이트웨이

멀티 클라우드 방어 게이트웨이는 클라우드 서비스 제공자 계정에 구축된 데이터플레인으로 작동하여 공용 클라우드 워크로드를 보호하는 PaaS(Platform as a service) 제공 구성 요소입니다. 멀티 클라우드 방어 게이트웨이는 전적으로 클라우드 서비스 제공자 계정 내에서 구축 및 운영됩니다. 모든 트래픽 처리 및 보안 보호는 클라우드 서비스 제공자 내부에서 이루어집니다.

멀티 클라우드 방어 게이트웨이가 제공하는 기능은 다음과 같습니다.

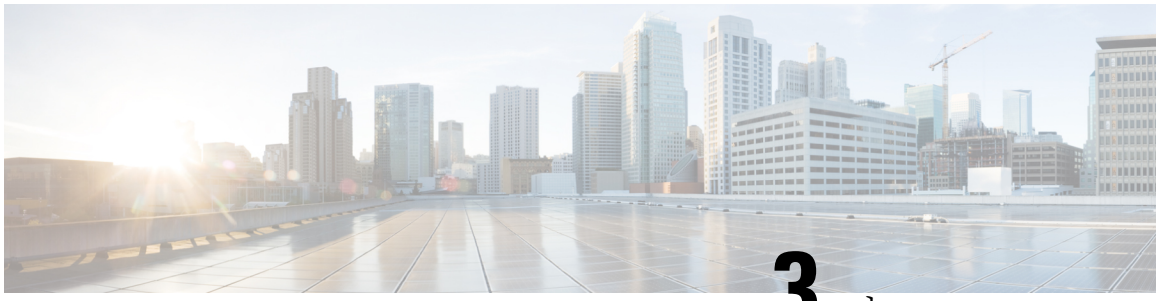
- 워크로드를 보호하는 클라우드 네이티브 아키텍처.
- 인그레스, 이그레스 및 이스트-웨스트 활용 사례.
- 전달 및 프록시 기반 처리.
- 트래픽 페이로드 검사를 위한 전체 암호 해독.
- WAF(Web Application Firewall), IDS/IPS, DLP 및 L7 DOS의 고급 보안 기능.
- L4, URL/URI, 악성 및 지리적 IP를 통한 필터링.
- 멀티 클라우드 방어 컨트롤러 및 Terraform 제공자를 통한 오케스트레이션.
- 멀티 클라우드, 다중 지역 및 다중 가용성 영역 구축.
- 워크로드 수요에 기반한 동적 자동 확장.
- 클라우드 구조를 사용하는 동적 멀티 클라우드 보안 정책.

고객은 중단 없이 몇 분 안에 끝나는 간단한 업그레이드 절차를 통해 멀티 클라우드 방어 게이트웨이를 업데이트해야 합니다. 게이트웨이 개선 사항 및 업데이트는 자주 제공됩니다.

멀티 클라우드 **Defense Terraform** 제공자

멀티 클라우드 방어 terraform 제공자는 CICD(지속적인 통합, 지속적인 구축) 파이프라인을 통해 전체 멀티 클라우드 방어 구축을 구축, 구성 및 관리하는 데 사용되는 멀티 클라우드 서비스 제공자 IaC(infrastructure-as-code) 오케스트레이션 언어입니다. 독점적으로 또는 멀티 클라우드 방어 컨트롤러와 함께 사용할 수 있으며 컨트롤러로 수행할 수 있는 대부분의 작업을 수용합니다.

고객은 원하는 Terraform 릴리스를 참조하여 멀티 클라우드 방어 terraform 제공자를 업데이트하고 참조된 버전을 로드하는 `Terraform update` 명령을 실행해야 합니다.



3 장

개선 사항 및 수정 사항

다음 항목에는 각 릴리스 시점의 모든 구성 요소에서 발생한 모든 기능, 개선 사항 및 버그 수정 사항이 포함되어 있습니다.

- 멀티 클라우드 방어 컨트롤러 개선 사항, 7 페이지
- 멀티 클라우드 방어 게이트웨이 개선 사항, 13 페이지
- Terraform 제공자 개선 사항, 40 페이지

멀티 클라우드 방어 컨트롤러 개선 사항

버전 **24.02 2024**년 **2**월 **26**일(권장)

기능

이 릴리스에는 다음과 같은 기능이 포함되어 있습니다.

하이브리드 클라우드

- (프라이빗 미리 보기) 사이트 간 VPN(멀티 클라우드 방어 게이트웨이 버전 24.02 이상 필요)

오케스트레이션

- 구독 간 스포크 VNet 보호(Azure).
- 스포크 VPC/VNet 보호를 위한 경로 테이블 생성.
- LB 상태 확인 보안 그룹 오케스트레이션.

게이트웨이

- 모든 게이트웨이 인스턴스 유형의 디스크 크기 감소.
- 게이트웨이 SSH 액세스 활성화/비활성화.
- 세부 정보 페이지에서 게이트웨이를 업그레이드.
- 게이트웨이 업그레이드 취소.

- 인스턴스 레벨 작업(보호 종료, 인스턴스 교체, 데이터 경로 재시작).

통합

- 클라우드 서비스 제공자 인증서에 대한 변경 사항을 동적 추적.
- Azure Active Directory를 사용한 사용자 관리.

기타

- 성능 향상.
- 작업 개선.
- 버그 수정 및 안정성 개선.

개선 사항

이 릴리스에는 다음과 같은 개선 사항이 포함되어 있습니다.

- (프라이빗 미리 보기) 사이트 간 VPN에 대한 지원을 추가했습니다. 여기에는 IPSec 및 BGP를 포함한 VPN 터널 구성이 포함되어 있습니다. VPN을 통과하는 트래픽을 처리하고 보호하기 위해 VPN은 게이트웨이에서 직접 종료됩니다. 이 개선 사항은 멀티 클라우드 방어 게이트웨이 버전 24.02 이상이 필요합니다.
- 스포크 VNet/VPC에서 시작되거나 반환되는 트래픽이 멀티 클라우드 방어 게이트웨이가 포함된 서비스 VPC/VNet으로 라우팅되도록 스포크 VPC 및 VNet에서 라우트 테이블 오케스트레이션에 대한 지원을 추가합니다. 이러한 개선 사항에는 경로 테이블 및 경로 항목을 생성하고 경로 테이블을 서브넷과 연결하기 위한 워크플로우가 포함되어 있습니다.
- 스포크 VNet 피어링을 오케스트레이션하여 스포크 VNet에서 멀티 클라우드 방어가 포함된 서비스 VNet으로 트래픽을 라우팅함으로써 교차 구독 스포크 VNet 보호에 대한 지원을 추가합니다. 이렇게 하면 Azure의 오케스트레이션이 AWS 및 GCP의 유사한 오케스트레이션과 패리티가 됩니다.
- 클라우드 서비스 제공자 로드 밸런서(Azure, GCP, OCI) 또는 상태 확인 서비스(GCP)의 상태 확인과 관련된 보안 그룹, 네트워크 보안 그룹 및 방화벽 규칙 CIDR의 오케스트레이션에 대한 지원을 추가합니다.
- 텔레포트를 사용하는 역방향 SSH를 수용하기 위해 **Gateway Details(**게이트웨이 세부 정보**)** 페이지에서 SSH 활성화 및 비활성화에 대한 지원을 추가합니다. Teleport 통합을 지원하는 멀티 클라우드 방어 게이트웨이 버전 23.10 이상이 필요합니다.
- **Gateway Details(**게이트웨이 세부 정보**)** 페이지에서 멀티 클라우드 방어 게이트웨이 업그레이드에 대한 지원을 추가합니다.
- 멀티 클라우드 방어 게이트웨이 업그레이드를 취소(중단)하는 기능을 추가합니다.
- 게이트웨이 인스턴스 레벨 작업(보호 종료, 인스턴스 교체, 데이터 경로 재시작)을 추가합니다.
- 모든 클라우드 서비스 제공자에서 모든 인스턴스에 대한 디스크 크기를 256GB에서 128GB로 줄입니다.

- 개인 키가 클라우드 서비스 제공자에 저장되고 멀티 클라우드 방어 게이트웨이로 검색되는 인증서 개체에 대한 변경 사항을 동적으로 추적할 수 있도록 지원을 추가합니다. 클라우드 서비스 제공자 리소스가 변경되면 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.
- 게이트웨이 구축을 위해 영역을 선택할 경우, 모든 지역의 지역 식별 이름이 실제 영역 이름(소문자 이름)과 함께 표시되어야 합니다. 이러한 기능 향상을 통해 모든 영역이 식별 및 실제 영역 이름으로 모두 표시됩니다.
- 인증을 위해 Azure Active Directory와 통합하도록 멀티 클라우드 방어 컨트롤러 구성에 대한 지원을 추가합니다.
- 다양한 리소스 보기 페이지의 성능을 개선하여 API 호출 수를 줄이고 전반적인 로드 시간을 단축합니다.
- 성능을 개선하기 위해 **Traffic Summary(**트래픽 요약**)** 페이지에 대한 페이지 지원을 추가합니다.
- 성능 개선을 위해 **Stats(**통계**)** 페이지에 대한 페이지 매김 지원을 추가합니다.

수정

이 릴리스에는 다음과 같은 수정 사항이 포함되어 있습니다.

- 해당 지역에 게이트웨이 구축이 포함되어 있지 않으면 인벤토리 및 검색 보기에 자산 정보가 표시되지 않는 문제를 수정합니다.
- 인그레스 정책 규칙 집합이 비어 있는 경우 인그레스 게이트웨이 Azure가 구축되지 않는 문제를 수정합니다.
- 그룹 로그 전달 프로파일에서 로그 전달 프로파일이 사용되는 경우, S3 버킷으로의 로그 전달이 작동하지 않는 문제를 수정합니다.
- UI에서 게이트웨이를 삭제해도 백엔드의 게이트웨이가 완전히 삭제되지 않는 문제를 해결하고 동일한 이름의 대체 게이트웨이를 구축할 수 있습니다.
- Azure에 구축된 게이트웨이에 대해 공용 IP 주소 할당을 비활성화하면 블루/녹색 게이트웨이 교체가 수행되지만, 공용 IP는 계속 할당되는 문제를 수정합니다.
- FQDN 필터 프로파일의 첫 번째 범주와 FQDN 행을 삭제할 수 없는 문제를 수정합니다.
- 게이트웨이 필터의 게이트웨이 이름이 알파벳순으로 정렬되는 문제를 수정합니다.
- 계정 및 게이트웨이 리소스에 대한 Terraform으로 내보내기 관련, 내보낸 결과 Terraform이 비어 있었던 문제를 수정합니다.
- 게이트웨이 정책 상태가 **Updated(**업데이트됨**)**으로 표시되더라도 정책 규칙 집합 상태가 **Updating(**업데이트 중**)**으로표시되는 문제를 수정합니다.
- 인스턴스가 정상이었더라도 상태 확인 장애로 인해 확장에 실패하는 문제를 수정합니다.

- 상태 확인 비정상 시간 기간을 120초로 변경합니다. 새 게이트웨이가 구축되면 로드 밸런서 상태 확인 또는 상태 확인 서비스가 오케스트레이션되어 2분(120초) 동안 인스턴스 상태를 평가합니다. 이전 오케스트레이션은 20초 동안 평가되었습니다.
- 시간대 선택 기본적으로 **UTC**가 아닌 **Local**로 설정되는 문제를 수정합니다.
- **Stats(**통계**)** 페이지에서 CPU 메트릭이 항상 표시되어야 하는 것보다 10배 적게 표시되는 문제를 수정합니다.
- 스포크 VPC가 삭제되지 않는 GCP에서 스포크 VPC 피어링을 삭제할 때 발생하는 문제를 수정합니다. 이 문제는 셀프 링크 대신 VPC ID가 사용될 때만 발생합니다.
- 리소스 전체의 **Last Modified(**마지막 수정**)** 정보 표시 관련 문제를 수정합니다.
- 링크가 연결된 리소스로 리디렉션되지 않는 여러 UI 관련 리소스 링크를 수정합니다.
- 고급 검색과 관련된 다양한 UI 관련 문제를 수정합니다.
- 적절한 동작을 보장하기 위해 다양한 UI 워크플로우를 수정합니다.

버전 **23.12 2023**년 **12**월 **14**일

기능

이 릴리스에는 다음과 같은 기능이 포함되어 있습니다.

오케스트레이션

- GCP에서 게이트웨이 생성을 위해 사용자가 제공한 NLB IP.
- 데이터 경로 방화벽 규칙의 GCP 상태 확인 CIDR.

정책

- ICMP 정책을 여러 클라우드 서비스 제공자의 게이트웨이에 적용.

통합

- 로그 전달 그룹의 여러 시스템 로그 서버.

사용 편의성

- 필터링 및 고급 검색을 위한 추가 필드.
- 정책 규칙 집합의 SNAT 구성 표시.

기타

- 성능 향상.
- 작업 개선.
- 버그 수정 및 안정성 개선.

개선 사항

이 릴리스에는 다음과 같은 개선 사항이 포함되어 있습니다.

- 처음에는 사용할 수 없었던 필드를 고급 검색에 추가합니다.
- 사용자가 제공한 IP 리소스를 로드 밸런서 프런트엔드 IP로 사용할 수 있도록 GCP에서 게이트웨이 생성을 개선합니다. Terraform을 사용하는 경우에만 제공할 수 있습니다.
- 정책 규칙 집합 보기에 서비스 개체 SNAT 설정 표시를 추가합니다.
- 클라우드 서비스 제공자가 해당 클라우드 서비스 제공자에 구축된 게이트웨이에 ICMP 정책을 적용하기 위해 ICMP를 지원해야 한다는 엄격한 요건을 완화합니다. 이제 클라우드 서비스 제공자가 ICMP를 지원하는지 여부에 상관없이 ICMP 정책을 포함하는 정책 규칙 집합을 모든 클라우드 서비스 제공자에 있는 모든 게이트웨이에 적용할 수 있습니다.
- 로그 전달 그룹에서 둘 이상의 시스템 로그 서버 구성에 대한 지원을 추가합니다.
- 데이터 경로 방화벽 규칙을 오케스트레이션할 때 GCP 상태 확인 CIDR을 추가합니다.

수정

이 릴리스에는 다음과 같은 수정 사항이 포함되어 있습니다.

- Splunk 엔드포인트에 연결할 수 있는데 Splunk에 대한 로그 전달 프로파일이 연결할 수 없음으로 표시되는 문제를 수정합니다.
- AWS 서비스 VPC를 역 오케스트레이션하면 VPC 자체를 포함하여 모든 VPC 리소스가 완전히 정리되지 않는 문제를 해결합니다.
- 사용자가 역방향 프록시 서비스 개체를 생성하거나 수정할 때 모든 주소 개체가 표시되는 문제를 해결합니다. 이제 역방향 프록시 서비스 개체만 표시됩니다.
- GCP 공유 VPC 시나리오로 게이트웨이를 오케스트레이션할 때 컨트롤러가 잘못된 프로젝트 ID를 사용하는 문제를 수정합니다.
- 그룹 주소 개체를 생성하거나 수정할 때 주소 개체 목록이 드롭다운에 표시되지 않는 문제를 수정합니다.
- 게이트웨이 워크플로우에서 클라우드 서비스 제공자 계정에 대한 자동 완성 검색을 수정합니다.
- 성능을 개선하고 작업을 신속하게 수행하기 위해 정책 규칙 집합 내에 규칙을 추가할 때의 문제를 수정합니다.
- CDO 페이지를 통해 AWS 계정을 추가할 때 시간 초과가 발생할 수 있는 문제를 수정합니다.
- FQDN 일치 및 FQDN 필터링 개체의 개수 문제를 수정합니다. 이러한 개수는 각 보기에 있는 두 가지 유형의 개체를 모두 나타내는 것입니다.
- 다양한 고급 검색 및 필터 문제를 수정합니다.
- Azure에 가용 용량이 없을 때 Azure에 게이트웨이를 구축하면 구축에 실패하고 생성된 리소스가 정리되지 않는 문제를 수정합니다. Azure에 용량이 없으면 가상 머신 및 관련 리소스의 생성을 억제하지 않습니다. VM을 생성하지만 오류 메시지와 함께 실패 상태의 VM을 표시합니다. 이

시나리오는 해당 문제가 인식될 수 있도록 구체적인 방법으로 처리해야 하며, 리소스를 정리하기 위한 적절한 조치를 취하며, 시스템 로그 메시지를 통해 사용자에게 클라우드 서비스 제공자의 문제를 알릴 수 있어야 합니다.

- Azure에서 게이트웨이를 구축할 때 클라우드 서비스 제공자 리소스 및 용량 정보가 표시되지 않는 문제를 수정합니다.
- 정책 규칙 집합의 규칙 목록 표시 성능을 개선합니다.
- GCP 기반 계정을 삭제하면 재고 목록 검색과 관련된 모든 재고 목록 개체가 삭제되지 않는 문제를 수정합니다.
- 사용자가 첫 번째 행을 제거하지 못하도록 하는 게이트웨이 인스턴스 영역별 행 문제를 해결합니다. 이는 게이트웨이가 사용자 관리 VPC 또는 VNet에 구축되는 시나리오에만 적용됩니다.
- GCP에 게이트웨이를 구축하면 오케스트레이션된 서비스 VPC로의 이그레스 경로를 오케스트레이션하지 않는 문제를 수정합니다.
- 스포크 VPC 보호 오케스트레이션이 실패할 수 있는 문제를 수정합니다.
- 역방향 프록시 서비스 개체를 편집할 때 SNI 및 L7 DOS 프로파일이 표시되지 않는 문제를 해결합니다.
- 공용 IP 할당 설정을 위한 UI 변경 작업이 불필요한 파란색/녹색 게이트웨이 교체를 트리거할 수 있는 문제를 수정합니다.
- 게이트웨이를 여러 GCP 지역으로 오케스트레이션할 때 게이트웨이가 활성화되지 않는 경합 상태가 발생할 수 있는 문제를 수정합니다.
- 내부 오류로 인해 새 게이트웨이 구축이 즉시 비활성화되는 문제를 수정합니다.
- Terraform에서 생성한 전달 또는 전달 프록시 정책 규칙 집합이 UI에 역방향 프록시 규칙으로 표시되는 문제를 수정합니다.
- 정책 규칙 집합을 편집할 때 규칙의 순서를 변경할 수 없는 문제를 수정합니다.
- 20개가 넘는 행을 포함하는 서비스 개체가 수락되어 게이트웨이에 푸시되어 게이트웨이 충돌이 발생하는 문제를 수정합니다. 서비스 개체는 이제 20개 행으로 제한됩니다. 이 제한 검증은 컨트롤러와 게이트웨이에서 모두 수행합니다.
- Gateway Details(게이트웨이 세부 정보) 페이지에서 수정한 날짜 및 데이터 생성 시간이 표시되는 문제를 수정합니다.
- 여러 페이지에 걸쳐 있는 개체 및 프로파일을 포함하는 보기의 올바른 정렬 문제를 수정합니다.
- 다양한 개체 생성 페이지의 성능을 개선합니다.
- UI 전반의 수정 및 개선 사항을 통해 사용자 환경을 개선합니다.
- 사용자가 지정한 로컬 또는 UTC 시간 설정이 모든 보기에서 적용되고 포털 호출 전체에서 유지되도록 합니다. 포털 호출에 대한 지속성은 이 설정을 브라우저 캐시에 저장함으로써 달성됩니다.
- 맞춤형 관리 암호화 키 게이트웨이 설정에 대한 툴팁 정보가 누락된 UI 문제를 수정합니다.

- 클라우드 서비스 제공자 오류로 인해 게이트웨이를 활성화하지 못한 경우 컨트롤러에서 시스템 로그 메시지를 생성합니다.

멀티 클라우드 방어 게이트웨이 개선 사항

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

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 멀티 클라우드 방어 게이트웨이에서 직접 종료됩니다. 이 개선 사항은 멀티 클라우드 방어 게이트웨이 버전 24.02 이상이 필요합니다.
- 개인 키가 클라우드 서비스 제공자에 저장되고 멀티 클라우드 방어 게이트웨이로 검색되는 인증서 개체에 대한 변경 사항을 동적으로 추적할 수 있도록 지원을 추가합니다. 클라우드 서비스 제공자 리소스가 변경될 때 멀티 클라우드 방어 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: 멀티 클라우드 방어 컨트롤러에 의해 관리되는 디바이스)임을 강조합니다.
- 로그 전달 그룹에서 둘 이상의 시스템 로그 서버 구성에 대한 지원을 추가합니다.

수정

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. 이 수정 사항은 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 멀티 클라우드 방어 컨트롤러로 전송하도록 허용된 것보다 커서 게이트웨이 로그를 분석할 수 없는 문제를 수정합니다. 이 수정은 생성된 진단 번들이 멀티 클라우드 방어 컨트롤러에 성공적으로 전송되도록 제한을 해결합니다.
- 정방향 프록시 규칙으로 처리된 각 세션에 대해 둘 이상의 SNI 이벤트가 기록되는 문제를 수정합니다.
- 멀티 클라우드 방어 게이트웨이 안정성을 개선합니다.
- 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 멀티 클라우드 방어 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 멀티 클라우드 방어 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 멀티 클라우드 방어 게이트웨이가 해당 도메인의 트래픽과 일치하지 않게 됩니다. 이 수정 사항은 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.
- 멀티 클라우드 방어 게이트웨이 안정성 개선.
- 멀티 클라우드 방어 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. 이 수정은 유출을 수정하여 데이터 경로가 자가 복구해야 하는 상황을 방지합니다.

- 게이트웨이 프로파일 정보를 검색하기 위해 멀티 클라우드 방어 컨트롤러에 대한 API 호출을 최적화하여 멀티 클라우드 방어 게이트웨이의 성능을 개선합니다.
- 정책 규칙 집합 작업을 `No Log(로그 없음)` 값으로 설정해도 로그 메시지가 생성되는 문제를 수정합니다.

버전 23.10

버전 23.10-03 2024년 1월 11일

수정

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. 이 수정 사항은 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 23.08

버전 23.08-15-d1 2024년 5월 27일

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 1514바이트보다 커집니다. 이에 따라 프록시에서 발급할 인증서를 결정하는 데 사용되는 SNI(Server Name Indication, 서버 이름 표시)를 검색할 수 없게 됩니다. 이 수정 사항을 통해 프록시가 1514바이트보다 큰 Client Hello 크기를 지원할 수 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. 이 수정 사항은 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 이 문제를 해결하면 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. 이 문제를 해결하면 세션 드레인이 올바르게 완료되고 데이터 경로가 비정상으로 표시되는 상황이 제거됩니다.

버전 23.08-15: 2024년 3월 27일(권장)

수정

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 합니다. 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 멀티 클라우드 방어 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 멀티 클라우드 방어 게이트웨이로부터 응답을 기대하는 동안 멀티 클라우드 방어 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

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. 이 수정 사항은 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

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. 이 수정 사항은 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

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

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

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

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

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 확장이 발생할 수 있는 문제를 수정합니다.
- 프록시 연결 유출 문제를 수정합니다.
- 멀티 클라우드 방어 게이트웨이 안정성을 개선합니다.

레거시 게이트웨이 버전

다음 레거시 버전은 권장되지 않지만 계속 지원됩니다.

버전 **23.06**

버전 **23.06-14 2023**년 **11**월 **12**일

수정

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. 이 수정 사항은 캐시가 예상대로 작동하도록 경쟁 조건을 해결합니다.

버전 **23.06-13 2023**년 **10**월 **18**일

수정

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 2023**년 **10**월 **6**일

수정

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

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

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

이 업그레이드에는 다음과 같은 수정 사항이 포함되어 있습니다.

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

버전 23.06-07 2023년 8월 29일

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 2023**년 **7**월 **27**일

수정

이 업그레이드에는 다음과 같은 수정 사항이 포함되어 있습니다.

- 안티맬웨어 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

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 2023년 7월 6일

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 자동 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 2023**년 **8**월 **23**일

수정

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 2023**년 **8**월 **22**일

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 2023**년 **7**월 **27**일

수정

이 업그레이드에는 다음과 같은 수정 사항이 포함되어 있습니다.

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

버전 **23.04-13 2023**년 **7**월 **27**일

수정

이 업그레이드에는 다음과 같은 수정 사항이 포함되어 있습니다.

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

버전 **23.04-12 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 **23.04-11 2023**년 **7**월 **10**일

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: 2023**년 **6**월 **28**일

수정

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: 2023**년 **6**월 **25**일

수정 사항

이 업그레이드에는 다음과 같은 수정 사항이 포함되어 있습니다.

- 일관된 게이트웨이 상태를 보장하기 위해 제공된 15일 주기의 게이트웨이 데이터 경로 자동 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 자동 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 2023**년 **6**월 **14**일

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 자동 복구로 해결된 느린 세션 풀 유출과 관련하여 23.04-05에서 변경된 사항을 되돌리는 업데이트를 제공합니다. 이전 업데이트에서는 선점할 수 없는 데이터 경로 자동 복구를 유발할 수 있습니다. 이 릴리스는 초기 문제가 완전히 해결되는 동안 안정성을 보장합니다.

버전 **23.04-06 2023**년 **6**월 **8**일

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 2023년 6월 1일

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 자동 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 자동 복구를 발생시키는 다양한 게이트웨이 안정성 문제를 수정합니다.

버전 23.04-04 2023년 5월 19일

수정

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 2023년 5월 16일

수정

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 2023**년 **4**월 **20**일

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 자체 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

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 자동 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 자동 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 자동 복구로 해결된 느린 세션 풀 유출과 관련하여 23.04-05에서 변경된 사항을 되돌리는 업데이트를 제공합니다. 이전 업데이트에서는 선점할 수 없는 데이터 경로 자동 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 자동 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 자동 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

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

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 자체 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.

Terraform 제공자 개선 사항

버전 24.2.1 2024년 2월 31일(권장)

개선 사항

이 릴리스에는 다음과 같은 개선 사항이 포함되어 있습니다.

- Windows, Linux 및 MacOS에 대한 arm64 지원을 추가합니다.
- 사용자가 제공한 IP 리소스를 로드 밸런서 프런트엔드 IP로 사용할 수 있도록 GCP에서 멀티 클라우드 방어 게이트웨이 `ciscomcd_gateway` 리소스 생성을 개선합니다.
- Azure `ciscomcd_spoke_vpc`에서 교차 구독 스포크 VNet 피어링 오케스트레이션에 대한 지원을 추가합니다. 이렇게 하면 클라우드 서비스 제공자 간에 기능이 동일해집니다.
- OCI에서 오케스트레이션을 위해 `ciscomcd_account` 및 멀티 클라우드 방어 게이트웨이 구축 `ciscomcd_gateway` 리소스를 온보딩하는 어카운트에 대한 지원을 추가합니다.

수정

이 릴리스에는 다음과 같은 수정 사항이 포함되어 있습니다.

- FQDN 필터링 ciscomcd_profile_fqdn 리소스를 생성하려고 하면 "unknown action Inherit from decryption profile for profile type FQDN_FILTER(프로파일 유형 FQDN_FILTER에 대한 암호 해독 프로파일로부터 상속된 알 수 없는 동작)"오류 메시지가 표시되는 문제를 수정합니다.
- 암호 해독 프로파일 ciscomcd_profile_decryption 리소스의 변경 사항이 메시지: "변경 사항이 없습니다. 인프라가 구성과 일치합니다."를 생성하는 변경 사항을 인식하지 못하는 문제를 수정합니다.
- 스포크 VPC 피어링이 삭제되지 않는 GCP에서 스포크 VPC ciscomcd_spoke_vpc 피어링 삭제 시 발생하는 문제를 수정합니다. 이 문제는 셀프 링크 대신 VPC ID가 사용될 때만 발생합니다.

버전 23.10.1 2023년 11월 6일

개선 사항

이 릴리스에는 다음과 같은 개선 사항이 포함되어 있습니다.

- 폴더 계층 구조에 포함된 모든 프로젝트의 자산 및 트래픽 검색을 수용하기 위해 클라우드 서비스 공급자 계정 ciscomcd_cloud_account 리소스에서 GCP 폴더 계층 구조를 온보딩하는 데 대한 지원을 추가합니다. GCP 폴더를 온보딩하면 자산 및 트래픽 검색이 허용되지만, 전체 오케스트레이션은 허용되지 않습니다. 검색은 GCP 프로젝트 내에서 수행된 변경 사항에 맞춰 실시간으로 조정되는 동적 정책을 만드는 데 유용하고 필요합니다. 프로젝트 내에서 오케스트레이션하려면 오케스트레이션이 필요한 각 프로젝트를 개별적으로 온보딩해야 합니다.
- 서드파티 SIEM으로 멀티 클라우드 방어 게이트웨이 메트릭을 전송하도록 지원을 추가합니다. 게이트웨이 메트릭을 SIEM으로 전송하기 위하여 구성하고 멀티 클라우드 방어 게이트웨이 ciscomcd_gateway 리소스에 할당할 수 있는 새로운 메트릭 전송 프로파일 ciscomcd_profile_metrics_forwarding 리소스를 도입합니다. 첫 번째 구현은 Datadog를 SIEM으로 지원합니다. 다른 SIEM에 대한 지원은 향후 릴리스에서 제공될 예정입니다.
- 멀티 클라우드 방어 게이트웨이 ciscomcd_gateway 리소스 aws_gateway_lb 인수 기본값을 false에서 true로 변경합니다. AWS 이그레스 게이트웨이를 구축할 때 지원되는 트랜짓 아키텍처는 AWS TWLB(게이트웨이 로드 밸런서) 아키텍처입니다. 이 인수는 선택 사항이며 지정하지 않은 경우 적절한 값으로 기본 설정되어야 합니다.
- Splunk로의 감사 및 시스템 로그 전송에 대한 지원을 추가합니다. 이렇게 하면 Splunk가 유형 인수의 새 값으로 추가되어 알림 프로파일 ciscomcd_alert_profile 리소스가 업데이트됩니다.
- Microsoft Teams로의 감사 및 시스템 로그 전송에 대한 지원을 추가합니다. 이렇게 하면 Microsoft Teams를 유형 인수에 대한 새 값으로 추가하여 알림 프로파일 ciscomcd_alert_profile 리소스가 업데이트됩니다.
- 백엔드 TLS 세션을 협상할 때 서버 인증서를 검증하도록 정방향 프록시 정책을 개선합니다. 인증서 검증은 기본적으로 비활성화되어 있지만 모든 TLS 세션의 암호 해독 프로파일 ciscomcd_profile_decryption 리소스 및 도메인(또는 도메인 집합) 단위로 FQDN 일치 개체 ciscomcd_profile_fqdn 리소스에서 구성할 수 있습니다.
- Service VPC(VNet) ciscomcd_service_vpc의 일부로 Azure RG(Resource Group) 생성에 대한 지원을 추가합니다. 멀티 클라우드 방어 컨트롤러이 오케스트레이션한 모든 리소스가 지정된(또는 새로 생성된) RG 내에서 연결되려면 RG가 필요합니다.

수정 사항

이 릴리스에는 다음과 같은 수정 사항이 포함됩니다.

- `Transport_mode` 인수에 할당된 보안 프록시(TLS, HTTPS, WEBSOCKETS) 값을 사용할 때 암호 해독 프로파일 `ciscomcd_profile_decryption`이 tls_profile 인수에 할당되도록 정방향 또는 역방향 프록시 서비스 개체 `ciscomcd_service_object` 리소스를 구성할 때 검증이 수행되지 않는 문제를 해결합니다. 보안 프록시가 구성된 경우에는 암호 해독 프로파일이 할당되어 있어야 합니다. 그렇지 않으면 프록시는 보안 프록시로 작동하지 않으며 TLS 암호화 트래픽이 거부됩니다.

버전 23.8.1 2023년 8월 22일

개선 사항

이 릴리스에는 다음과 같은 개선 사항이 포함되어 있습니다.

- L4(TCP) 및 L5(TLS) 프록시를 수용하도록 정방향 프록시 서비스 개체 `ciscomcd_service_object` 리소스를 개선합니다. TCP 또는 TLS를 `transport_mode` 인수에 대한 유효한 값으로 지정하여 이를 수행할 수 있습니다.
- assign_public_ip 설정이 변경될 때 파란색/녹색 게이트웨이 교체를 수행하도록 멀티 클라우드 방어 게이트웨이 `ciscomcd_gateway` 리소스를 개선합니다.

수정

이 릴리스에는 다음과 같은 수정 사항이 포함되어 있습니다.

- 정책 인수 없이 `mode=MATCH` 인수가 있는 FQDN 프로파일 `ciscomcd_fqdn_profile` 리소스를 사용하면 일치하는 트래픽이 거부되는 문제를 수정합니다. 정책 인수는 지정할 필요가 없으며 Terraform Provider 설명서에 인수로 나열되어 있지 않습니다.
- 정책 규칙 `ciscomcd_policy_rule_set` 리소스를 업데이트하는 데 시간이 오래 걸리고 RPC 오류가 생성될 수 있는 문제를 수정합니다.

레거시 Terraform 버전

다음 레거시 버전은 권장되지 않지만 계속 지원됩니다.

버전 23.7

버전 23.7.2 2023년 7월 27일

수정 사항

이 버전에는 다음과 같은 수정 사항이 포함되어 있습니다.

- 정책 인수 없이 mode=MATCH인수를 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 2023**년 **7**월 **24**일

수정

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=MATCH인수가 잘못된 FQDN 프로파일(valtix_fqdn_profile) 리소스에 'policy' 인수를 요구하는 문제를 수정합니다.

버전 **23.6**

버전 **23.6.1, 2023**년 **7**월 **17**일

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 포함되어 있습니다.

- 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 2023**년 **6**월 **12**일

개선 사항

이 릴리스에는 다음과 같은 개선 사항이 포함되어 있습니다.

- Valtix Terraform Provider를 미러링하는 멀티 클라우드 Defense Terraform 제공자을 게시했습니다. 새로운 Provider는 `ciscomcd` 이며 가까운 시일 내에 공개될 예정입니다. 제공자는 동시에 업데이트되며 별도로 공지되지 않는 한 서로의 미러링을 나타냅니다. 가까운 시일 내에 Valtix 제공자는 더 이상 사용되지 않으며 시스코 제공자로 완전히 대체됩니다.

수정

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

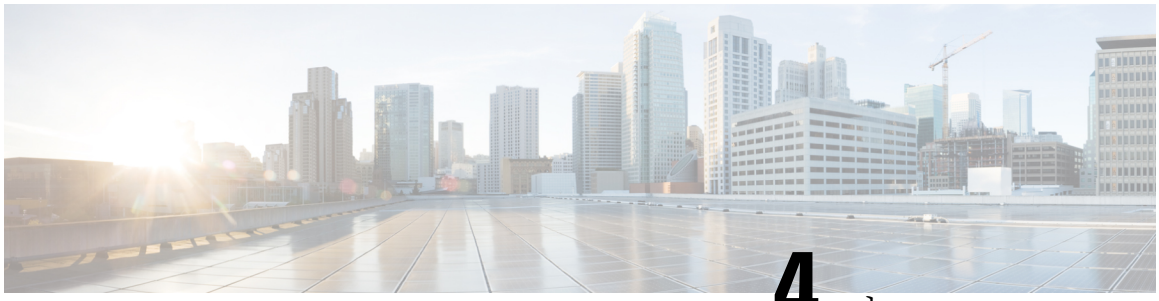
이 릴리스에는 다음과 같은 개선 사항이 포함되어 있습니다.

- 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

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.



4 장

릴리스 및 서비스 정책

- 릴리스 버전 관리 및 일정, on page 47
- 릴리스 수명 및 지원, on page 48

릴리스 버전 관리 및 일정

릴리스 버전 관리

멀티 클라우드 방어 릴리스 버전 관리는 X.Y-Z 또는 X.Y.Z로 정의됩니다. 여기서 X는 주요 릴리스(역년으로 표시), Y는 부 릴리스(역월로 표시), Z는 유지 보수 릴리스(1의 값으로 시작하는 정수로 표시)입니다.

주요 릴리스

주요 버전은 멀티 클라우드 방어의 릴리스이며 주요 개선 사항, 안정성 개선 및 버그 수정이 포함될 예정입니다.

부 릴리스

부 버전은 멀티 클라우드 방어의 릴리스이며 부 개선 사항, 안정성 개선 및 버그 수정이 포함된 릴리스입니다.

유지 보수 릴리스

유지 보수 버전은 멀티 클라우드 방어의 빈번한 업데이트 릴리스이며 안정성 개선과 버그 수정을 포함합니다. 드문 경우이지만 개선 사항도 선보입니다.

핫픽스 릴리스

핫픽스 릴리스는 소수의 구축(일반적으로 단일 구축)에 영향을 미치는 운영 문제를 해결하는 버그 수정이 포함된 우선순위 릴리스입니다.

핫픽스는 해당 주, 부 및 유지 보수 릴리스의 개선 사항입니다. 각 핫픽스 릴리스에는 문자로 표시된 핫픽스 릴리스 전체의 누적 개선 사항이 포함되어 있지 않습니다(예: 핫픽스 B에는 핫픽스 A의 개선

사항이 포함되어 있지 않음). 그러나 숫자로 표시되는 핫픽스 릴리스 문자 내의 각 핫픽스 릴리스에는 누적 개선 사항이 포함되어 있습니다(예: 핫픽스 A2는 핫픽스 A1의 개선 사항을 포함합니다).

각 핫픽스 릴리스의 릴리스 노트에는 주, 부 및 유지 보수 릴리스 개선 사항 이외의 구체적인 개선 사항에 대한 정보가 포함됩니다.

핫픽스 릴리스 개선 사항은 최종적으로 유지 보수 릴리스로 롤링됩니다. 핫픽스 릴리스로의 업그레이드는 Cisco 지원의 지침에 따라서만 이루어져야 합니다.

릴리스 일정

멀티 클라우드 방어에서는 최선을 다해 3개월마다 주요 또는 부 릴리스를 배포할 계획입니다. 유지 보수 릴리스는 지원 종료 및 단종 정책에 따라 각 주요 또는 부 릴리스에 대해 주기적으로 제공됩니다.

릴리스 수명 및 지원

릴리스 날짜부터 지원 종료 및 단종까지 릴리스의 수명을 알리고 시행하기 위한 정의 및 프로세스입니다.

단종/지원 정책

릴리스 날짜부터 지원 종료 및 단종까지 릴리스의 수명을 알리고 시행하기 위한 정의 및 프로세스입니다.

EoS(지원 종료**)**

모든 유지 보수 릴리스를 포함하여 주요 또는 부 릴리스의 문제 해결이나 수정이 더 이상 지원되지 않는 마지막 날입니다. 새로운 유지 보수 릴리스가 배포되지 않습니다. 멀티 클라우드 방어에서는 권장 주요 또는 부 릴리스 및 유지 보수 릴리스로의 업그레이드를 지원하고, 문제가 여전히 존재하는지 확인하고, 수정 또는 해결 방법을 제공하기 위해 노력합니다.

주요 또는 부 릴리스는 릴리스 날짜로부터 6개월 후에 지원 종료로 표시됩니다.

발표

- 1개월 전
- 1주일 전
- 당일

EoL(단종**)**

관련 유지 보수 릴리스를 포함하여 주요 또는 부 릴리스를 더 이상 설치할 수 없는 마지막 날입니다. 멀티 클라우드 방어에서는 권장 주요 또는 부 릴리스 및 유지 보수 릴리스로의 업그레이드를 지원하고, 문제가 여전히 존재하는지 확인하고, 수정 또는 해결 방법을 제공하기 위해 노력합니다.

주요 또는 부 릴리스(및 모든 유지 보수 릴리스)는 주요 또는 부 릴리스가 지원 종료로 표시된 지 2개월 후에 단종으로 표시됩니다.

발표

- 1개월 전
- 1주일 전
- 당일

가속화 **EoS/EoL**

멀티 클라우드 방어는 주요 또는 부 릴리스(및 모든 관련 유지 보수 릴리스)의 단종 및/또는 지원 종료를 가속화할 권한을 보유합니다. 멀티 클라우드 방어에서는 고객에게 알림을 제공하고 권장 릴리스로 업그레이드하도록 지원합니다.

발표

- 사례별 정의

Cisco 및 Cisco 로고는 미국과 기타 국가에서 Cisco 및 계열사의 상표 또는 등록 상표입니다. Cisco 상표 목록을 보려면 다음 URL로 이동하십시오. https://www.cisco.com/c/en/us/about/legal/trademarks.html. 언급된 타사 상표는 해당 소유권자의 재산입니다. 파트너라는 용어의 사용이 Cisco와 다른 업체 사이의 제휴 관계를 의미하는 것은 아닙니다. (1721R)

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.