Multicloud Defense 컨트롤러 및 게이트웨이 릴리스

Multicloud Defense 컨트롤러 및 Multicloud Defense 게이트웨이 릴리스는 함께 패키지되지 않지만, 업데이트는 일반적으로 동일한 기간 내에 릴리스됩니다. 컨트롤러는 자동으로 업데이트되므로 URL 호스팅 컨트롤러 대시보드는 항상 최신 상태를 유지합니다. 게이트웨이는 환경 상태에 영향을 미칠 수 있는 보안 및 트래픽 검사 중단을 최소화하기 위해 사용자의 선호도에 따라 업데이트됩니다.

2025년 11월 18일 게이트웨이 24.06-18

이 릴리스에는 다음과 같은 수정 사항이 포함되어 있습니다.

- 규칙 설명 문자열이 메모리 할당 오버런을 유발하여 게이트웨이 인스턴스화 시 충돌하는 문제를 수정합니다. 이 문제는 설명 필드의 문자 수를 제한함으로써 해결됩니다.
- FQDN(완전한 도메인 이름) 일치 정책을 사용하는 HTTP 프록시 규칙에 의해 처리되는 암호화되지 않은 HTTP(Hypertext Transfer Protocol) 트래픽이 HTTP 502 오류 코드를 잘못 생성하여 연결을 종료하는 문제를 수정합니다.
- Azure에 GWLB 기반 아키텍처로 구축된 인그레스 게이트웨이에서 적용된 포워딩 정책이 SNI를 추출하지 못하는 문제를 수정합니다. 이 문제는 게이트웨이 인스턴스와 GWLB 간에 가상 확장형 근거리 통신망(VXLAN)을 사용하여 트래픽을 터널링하는 데서 비롯됩니다. 이 문제는 해결되었으며 SNI를 정상적으로 추출할 수 있습니다.
- 이그레스 게이트웨이 포워딩 정책에서 발생하는 문제를 수정합니다. 해당 문제로 인해 TCP 핸드셰이크 후 첫 번째 애플리케이션 패킷이 클라이언트가 아닌 서버에서 도착할 경우 데이터 경로에서 해당 패킷이 드롭되었습니다. 이번 수정으로 첫 번째 애플리케이션이 클라이언트 또는 서버 어느 쪽에서든 도착할 수 있도록 보장하며, 데이터 경로가 패킷을 올바르게 처리하고 전달하도록 합니다.
- 보안 파일 전송 프로토콜(SFTP) 트래픽에 적용되는 인그레스 게이트웨이 리버스 프록시 정책이 연결은 수립하지만 세션 관련 트래픽을 완전히 처리하지 못해 클라이언트 또는 서버가 시간 초과되는 문제를 수정합니다. 이번 수정으로 SFTP 트래픽이 완전히 처리되도록 보장합니다.
- Azure의 엣지 모드 게이트웨이 구축 시 VPN 연결 설정 실패를 유발할 수 있는 문제를 수정합니다. 이 문제는 보조 인터페이스 IP가 잘못 할당될 가능성이 있기 때문이며, 이 경우 필요한 서브넷과 다른 서브넷의 IP가 할당될 수 있습니다. 이번 수정으로 할당된 IP가 데이터 경로 서브넷에서 비롯되도록 보장하여 VPN이 설정되고 활성화되도록 합니다.
- 애플리케이션이 비표준 HTTP(S) 포트를 사용할 때 게이트웨이가 400 Bad Gateway 응답 코드로 응답하는 문제와 관련된 이그레스 포워드 프록시 정책 문제를 수정합니다. 이번 수정으로 정책 구성에 지정된 모든 포트에 대해 포워드 프록시가 정상적으로 작동하도록 보장합니다.
- 데이터 손실 방지(DLP) 엔진의 문제점을 수정하여, 게이트웨이가 인스턴스화 시 완전히 초기화되지 않을 수 있는 현상을 해결합니다.
- 전체 복호화를 수행하는 이그레스 게이트웨이 포워드 프록시 정책이 프런트엔드 연결에서 백엔드 연결로 URL을 전송할 때 URL 인코딩을 유지하지 못하는 문제를 수정합니다.
- 트래픽 요약 로그에서 애플리케이션 정보 -> 페이로드 앱 이름이 잘리는 문제를 수정합니다.

버전 25.12 Multicloud Defense 컨트롤러, 2025년 12월 10일

이 릴리스에는 다음과 같은 개선 사항이 포함되어 있습니다.

- **Red Hat Enterprise Linux 9(RHEL 9)** 마이그레이션 - Multicloud Defense가 이제 Red Hat Enterprise Linux 9(RHEL 9)에서 제공됩니다. 이는 AWS 및 Azure에서만 지원됩니다. 이 마이그레이션으로 일부 고객의 인프라 비용이 증가할 수 있지만 RHEL 9은 최신 취약성 패치를 사용하여 취약성에 대한 향상된 보안을 제공합니다.
- **Azure**용 **Firewall Threat Defense Virtual (FTDv)** 지원 - Multicloud Defense는 이제 Azure용 FTDv에 대해 Standard_D8s_v5 및 Standard_D16s_v5 인스턴스 유형을 지원합니다. 기존 인스턴스 유형은 더 이상 사용되지 않을 예정입니다. 새로운 인스턴스 유형이 더 나은 성능을 제공합니다.
- **Azure Dsv6** 지원 - Azure Dsv6 인스턴스에 대한 Microsoft Marketplace의 권한 관련 기술적 문제 수정. 이제 Multicloud Defense에서 Azure Dsv6가 지원됩니다. Azure 게이트웨이 인스턴스가 Red Hat Enterprise Linux 9(RHEL 9)을 사용함에 따라 성능이 향상되고 인프라 비용이 증가할 가능성이 있습니다.
- 사용자 지정 로드 밸런서 지원**(BYOLB)** - 사용자 구성 로드 밸런서 정책과 매니지드 로드 밸런서 정책 간의 충돌로 인해 사용자 정의 로드 밸런서 구성이 불가능했던 Azure의 제한 사항을 해결했습니다. 이제 로드 밸런서 규칙에 대해 플로팅 IP를 사용자 지정하고 활성화한 후, 해당 로드 밸런서를 Multicloud Defense 게이트웨이에 연결할 수 있습니다. 이는 25.08 게이트웨이 릴리스에서 지원됩니다.

2025년 10월 15일 게이트웨이 25.02-03

개선 사항

이 릴리스에는 다음과 같은 개선 사항이 포함되어 있습니다.

- 엣지 모드 게이트웨이 구축에 대한 VPN 지원을 추가합니다. 이를 위해 로컬 VPC/VNet의 보조 CIDR을 ASA(VPN) 라우팅 테이블에 오케스트레이션하여 VPN을 통해 대상 애플리케이션 또는 워크로드까지 적절한 라우팅이 이루어지도록 합니다. 이는 24.06-15 릴리스에서 제공된 기본 CIDR 조정 기능을 개선한 것입니다.
- 엣지 모드 게이트웨이 구축에 대한 VPN 지원을 추가합니다. 이를 위해 로컬 VPC/VNet CIDR을 ASA(VPN) 경로 테이블에 오케스트레이션하여 VPN을 통해 대상 애플리케이션 또는 워크로드까지 적절한 라우팅이 이루어지도록 합니다.
- AWS에서 게이트웨이의 기본 이미지로 RHEL 9를 사용할 수 있도록 상용 및 FedRAMP 환경 전반에 걸쳐 범용 지원을 추가합니다. 이는 기본 운영 체제가 상용 운영 체제임을 보장하며, 알려진 CVE를 해결하기 위해 잘 유지 관리되고 이용 가능한 취약점 패치를 제공합니다. 이 기본 운영 체제의 라이선스는 사용량 기반 요금제(PAYG)로, 구축 청구 계정에 청구됩니다. 이미지 사용으로 인해 CSP 내 인프라 비용이 증가할 것으로 예상됩니다. Azure 및 GCP의 경우 기본 운영 체제는 CentOS 9로 유지됩니다. OCI의 경우 기본 이미지는 AlmaLinux 9로 유지됩니다.

수정

이 릴리스에는 다음과 같은 수정 사항이 포함되어 있습니다.

- Azure의 엣지 모드 게이트웨이 구축 시 VPN 연결 설정 실패를 유발할 수 있는 문제를 수정합니다. 이 문제는 보조 인터페이스 IP가 잘못 할당될 가능성이 있기 때문이며, 이 경우 필요한 서브

넷과 다른 서브넷의 IP가 할당될 수 있습니다. 이번 수정으로 할당된 IP가 데이터 경로 서브넷에서 비롯되도록 보장하여 VPN이 설정되고 활성화되도록 합니다.

- 애플리케이션이 비표준 HTTP(S) 포트를 사용할 때 게이트웨이가 400 Bad Gateway 응답 코드로 응답하는 문제와 관련된 이그레스 포워드 프록시 정책 문제를 수정합니다. 이번 수정으로 정책 구성에 지정된 모든 포트에 대해 포워드 프록시가 정상적으로 작동하도록 보장합니다.
- VPN 잠금 상태로 인한 경합 조건으로 인해 게이트웨이가 몇 분 동안 하트비트를 전송하지 못하는 문제를 수정합니다. 이러한 시나리오가 발생하면 컨트롤러는 게이트웨이를 HB_MISS로 표시하고 교체를 시작할 수 있습니다. 이번 수정으로 경합 상태가 발생하지 않도록 보장하며, 하트비트가 일관되게 전송되도록 합니다.
- AWS의 이그레스 게이트웨이를 통과하는 트래픽이 GENEVE 헤더에 표시되는 트래픽의 소스 VPC ID에 선행 '0' 문자가 포함되어 있어 거부될 수 있는 문제를 수정합니다. 게이트웨이가 선행 '0' 문자를 생략하여 알려진 VPC ID와 일치하지 않게 되었고, 이로 인해 트래픽이 잘못 차단되었습니다. 이번 수정으로 선행 '0' 문자가 포함된 VPC ID가 선행 문자를 유지하도록 하여 VPC ID를 적절히 일치시키고 트래픽을 올바르게 처리할 수 있도록 보장합니다.
- 포워딩 정책에 의해 처리되는 트래픽과 관련된 문제를 수정합니다. 클라이언트가 전송한 프래그먼트화된 TLS Hello 메시지가 프래그먼트 도착 순서가 뒤바뀐 경우 유효한 TLS Hello 메시지로 인식되지 않던 현상이 해결되었습니다. 이번 수정으로 순서에 관계없이 게이트웨이가 모든 프래그먼트를 올바르게 수신하고 처리하여 TLS Hello를 성공적으로 재조립하고 SNI를 추출할 수 있도록 보장합니다.
- URI 정보가 포함된 로그/이벤트에서 URL을 적절한 가독성을 위해 인코딩을 ASCII 문자열로 대체하지 않고 ASCII 인코딩 문자 그대로 표시하는 문제를 수정합니다. 이번 수정으로 문자가 ASCII 문자임을 보장합니다. 이 문제는 게이트웨이에 의한 트래픽 처리에 영향을 미치지 않습니다.
- 여러 포워드 프록시 규칙을 동시에 비활성화할 때 프록시 구성이 제대로 정리되지 않아 데이터 경로가 재시작 루프에 진입하는 문제를 수정합니다.
- 게이트웨이 정책 규칙 세트 내 서로 다른 규칙에 하나 이상의 악성 IP 프로파일이 할당된 경우 게이트웨이 초기화가 실패하는 문제를 수정합니다.
- 이그레스 게이트웨이 포워드 프록시 정책의 메모리 누수를 수정합니다. 이 누수로 인해 메모리 사용량이 80%를 초과할 경우 데이터 경로가 재시작될 수 있습니다.
- 이그레스 게이트웨이를 통해 트래픽을 처리할 때 가끔 발생하는 애플리케이션 소켓 시간 초과 문제를 수정합니다.
- HTTPS 포워드 프록시 트래픽 처리와 관련된 문제를 수정하여 연결 속도 저하가 발생할 수 있는 상황을 방지합니다.
- 트래픽 요약 로그에서 애플리케이션 정보 -> 페이로드 앱 이름이 잘리는 문제를 수정합니다.
- FQDN 일치를 사용하는 정책과 그렇지 않은 정책으로 처리되는 트래픽에 대해 SNI 이벤트의 `eventText` 필드가 다르게 사용되던 문제를 수정합니다. SNI가 존재하고 정책이 FQDN 일치를 사용하지 않을 경우, 해당 필드에는 도메인이 포함됩니다. 정책이 FQDN 일치를 사용할 경우, 해당 필드에는 해당 일치에 대한 추가 텍스트와 함께 도메인이 포함됩니다. 이번 수정으로 `eventText`

필드의 내용을 변경하지 않고, `fqdn`이라는 필드를 활용하여 도메인만 표시합니다. 이를 통해 도메인을 기준으로 트래픽을 검색하고 표시하는 것이 가능해집니다.

- 데이터 경로 자가 복구를 발생시키는 다양한 IP 테이블 안정성 문제를 수정합니다.
- 데이터 경로의 충돌 및 재시작을 유발할 수 있는 게이트웨이 데이터 경로의 안정성 문제를 수정합니다.
- 인그레스 게이트웨이의 CPU 사용률이 일시적으로 높아져 스케일 아웃이 발생한 후 스케일 인이 이어지는 문제를 수정합니다. 이 동작이 지속될 경우 영구적인 스케일 아웃 또는 스케일 인 동작이 발생할 수 있습니다.
- 포워딩 정책에 의해 처리되는 트래픽에 대해 TLS Hello에서 SNI(Service Name Indication)를 검색하는 게이트웨이 기능을 재구성합니다. 게이트웨이가 SNI를 검색할 수 없었던 원래 문제는 사후 양자 암호화를 수용하기 위한 TLS 라이브러리 변경으로 인해 발생했습니다. 이 변경으로 인해 TLS Hello는 1415바이트보다 커집니다. 이로 인해 정책에서 도메인과 일치하거나 필터링하는 데 사용하는 SNI를 검색할 수 없게 됩니다. 기존 수정 사항은 패킷 간 타이밍 차이로 인해 SNI 검색을 보장할 수 없었습니다. 이번 수정으로 게이트웨이가 TLS Hello 패킷을 처리하는 방식을 재구성하여 SNI를 성공적으로 검색할 수 있도록 보장합니다.

버전 25.09 Multicloud Defense 컨트롤러, 2025년 10월 7일

이 릴리스에는 다음과 같은 개선 사항이 포함되어 있습니다.

- 감사 및 시스템 로그 - 감사 로그 및 시스템 로그가 Multicloud Defense 애플리케이션의 새 페이지에 결합됩니다. **Investigate(**조사**)** > **System Status(**시스템 상태**)** > **Audit System Logs(**감사 및 시스템 로그**)**에서 이 통합된 페이지를 찾을 수 있습니다. 통합 페이지는 고급 검색 기능, 감사 및 시스템 로그의 명확한 식별, 이벤트와 로그의 더 간편한 상관관계, 이 모두를 한 곳에서 제공합니다.

2025년 10월 3일 게이트웨이 핫픽스 24.06-17-a1

이 릴리스에는 다음과 같은 수정 사항이 포함됩니다.

- Azure의 엣지 모드 게이트웨이 구축 시 VPN 연결 설정 실패를 유발할 수 있는 문제를 수정합니다. 이 문제는 보조 인터페이스 IP가 잘못 할당될 가능성이 있기 때문이며, 이 경우 필요한 서브넷과 다른 서브넷의 IP가 할당될 수 있습니다. 이번 수정으로 할당된 IP가 데이터 경로 서브넷에서 비롯되도록 보장하여 VPN이 설정되고 활성화되도록 합니다.

2025년 9월 24일 게이트웨이 24.06-17

개선 사항

이 릴리스에는 다음과 같은 개선 사항이 포함되어 있습니다.

- 엣지 모드 게이트웨이 구축에 대한 VPN 지원을 추가합니다. 이를 위해 로컬 VPC 또는 Net의 보조 CIDR을 ASA(VPN) 라우팅 테이블에 오케스트레이션하여 VPN을 통해 대상 애플리케이션 또는 워크로드까지 적절한 라우팅이 이루어지도록 합니다. 이는 24.06-15 릴리스에서 제공된 기본 CIDR 조정 기능을 개선한 것입니다.

수정

이 릴리스에는 다음과 같은 수정 사항이 포함되어 있습니다.

- VPN 잠금 상태로 인한 경합 조건으로 인해 게이트웨이가 몇 분 동안 하트비트를 전송하지 못하는 문제를 수정합니다. 이러한 시나리오가 발생하면 컨트롤러는 게이트웨이를 HB_MISS로 표시하고 교체를 시작할 수 있습니다. 이번 수정으로 경합 상태가 발생하지 않도록 보장하며, 하트비트가 일관되게 전송되도록 합니다.
- AWS의 이그레스 게이트웨이를 통과하는 트래픽이 GENEVE 헤더에 표시되는 트래픽의 소스 VPC ID에 선행 '0' 문자가 포함되어 있어 거부될 수 있는 문제를 수정합니다. 게이트웨이가 선행 '0' 문자를 생략하여 알려진 VPC ID와 일치하지 않게 되었고, 이로 인해 트래픽이 잘못 차단되었습니다. 이번 수정으로 선행 '0' 문자가 포함된 VPC ID가 선행 문자를 유지하도록 하여 VPC ID를 적절히 일치시키고 트래픽을 올바르게 처리할 수 있도록 보장합니다.
- 포워딩 정책에 의해 처리되는 트래픽과 관련된 문제를 수정합니다. 클라이언트가 전송한 프래그먼트화된 TLS Hello 메시지가 프래그먼트 도착 순서가 뒤바뀐 경우 유효한 TLS Hello 메시지로 인식되지 않던 현상이 해결되었습니다. 이번 수정으로 순서에 관계없이 게이트웨이가 모든 프래그먼트를 올바르게 수신하고 처리하여 TLS Hello를 성공적으로 재조립하고 SNI를 추출할 수 있도록 보장합니다.
- 이그레스 게이트웨이 포워드 프록시 정책의 메모리 누수를 수정합니다. 이 누수로 인해 메모리 사용량이 80%를 초과할 경우 데이터 경로가 재시작될 수 있습니다.
- 이그레스 게이트웨이를 통해 트래픽을 처리할 때 가끔 발생하는 애플리케이션 소켓 시간 초과 문제를 수정합니다.
- TLS Hello 메시지에 SNI(Service Name Indication)가 포함되지 않은 경우, 거부되어야 할 트래픽이 잘못 허용되는 문제를 해결합니다. SNI가 존재하지 않고 정책이 도메인을 기대하는 경우, 정책 규칙 일치가 발생하지 않아야 하며 트래픽은 기본 거부 정책에 의해 거부되어야 합니다. 이번 수정으로 트래픽이 제대로 차단되도록 보장합니다.
- 데이터 경로 자가 복구를 발생시키는 다양한 IP 테이블 안정성 문제를 수정합니다.
- 포워딩 정책에 의해 처리되는 트래픽에 대해 TLS Hello에서 SNI를 검색하는 게이트웨이 기능을 재구성합니다. 게이트웨이가 SNI를 검색할 수 없었던 원래 문제는 양자 암호화 이후를 수용하기 위한 TLS 라이브러리 변경으로 인해 발생했습니다. 이 변경으로 인해 TLS Hello는 1,415바이트보다 커집니다. 이로 인해 정책에서 도메인과 일치하거나 필터링하는 데 사용하는 SNI를 검색할 수 없게 됩니다. 기존 수정 사항은 패킷 간 타이밍 차이로 인해 SNI 검색을 보장할 수 없었습니다. 이번 수정으로 게이트웨이가 TLS Hello 패킷을 처리하는 방식을 재구성하여 SNI를 성공적으로 검색할 수 있도록 보장합니다.

2025년 8월 22일 게이트웨이 핫픽스 24.06-16-a1

핫픽스입니다. 이 핫픽스에는 다음과 같은 수정 사항이 포함되어 있습니다.

- 포워딩 정책에 의해 처리되는 트래픽과 관련된 문제를 수정합니다. 클라이언트가 전송한 프래그먼트화된 TLS Hello 메시지가 프래그먼트 도착 순서가 뒤바뀐 경우 유효한 TLS Hello 메시지로 인식되지 않던 현상이 해결되었습니다. 이번 수정으로 순서에 관계없이 게이트웨이가 모든 프래그먼트를 올바르게 수신하고 처리하여 TLS Hello를 성공적으로 재조립하고 SNI(Service Name Indication)를 추출할 수 있도록 보장합니다.
- 포워딩 정책에 의해 처리되는 트래픽에 대해 TLS Hello에서 SNI를 검색하는 게이트웨이 기능을 재구성합니다. 게이트웨이가 SNI를 검색할 수 없었던 원래 문제는 사후양자 암호화를 수용하기 위한 TLS 라이브러리 변경으로 인해 발생했습니다. 이 변경으로 인해 TLS Hello는 1415바이트보다 커집니다. 이로 인해 정책에서 도메인과 일치하거나 필터링하는 데 사용하는 SNI를 검색할 수 없게 됩니다. 기존 수정 사항은 패킷 간 타이밍 차이로 인해 SNI 검색을 보장할 수 없었습니다. 이번 수정으로 게이트웨이가 TLS Hello 패킷을 처리하는 방식을 재구성하여 SNI를 성공적으로 검색할 수 있도록 보장합니다.

2025년 8월 게이트웨이 버전 24.06-16 및 컨트롤러 버전 25.08

버전 **24.06-16 Multicloud Defense** 게이트웨이, **2025**년 **8**월 **22**일

이 릴리스에는 다음과 같은 수정 사항이 포함됩니다.

- FQDN 일치를 사용하는 정책과 사용하지 않는 정책으로 처리된 트래픽에서 SNI 이벤트의 `eventText` 필드가 다르게 사용되던 문제를 수정했습니다. SNI가 존재하고 정책이 FQDN 일치를 사용하지 않을 경우, 해당 필드에는 도메인이 포함됩니다. 정책이 FQDN 일치를 사용할 경우, 해당 필드에는 해당 일치에 대한 추가 텍스트와 함께 도메인이 포함됩니다. 이번 수정으로 `eventText` 필드의 내용을 변경하지 않고, `fqdn`이라는 필드를 활용하여 도메인만 표시합니다. 이를 통해 도메인을 기준으로 트래픽을 검색하고 표시하는 것이 가능해집니다.

버전 **25.08 Multicloud Defense** 컨트롤러, **2025**년 **9**월 **4**일

이 릴리스에는 다음과 같은 개선 사항이 포함되어 있습니다.

- **Azure Cloud** 서비스 - Multicloud Defense에서 Microsoft Azure에 맞게 Azure Cloud 서비스를 재구성하여 일관되고 균일한 사용자 경험을 보장합니다. 이제 Azure에서 사용하는 것과 동일한 명명법을 사용하면서 Multicloud Defense에서 지역을 구성할 수 있습니다.
- **Red Hat Enterprise Linux 9(RHEL 9)** 마이그레이션 - Multicloud Defense가 이제 Red Hat Enterprise Linux 9(RHEL 9)에서 제공됩니다. 이 마이그레이션으로 일부 고객의 인프라 비용이 증가할 수 있지만 RHEL 9은 취약성에 대한 향상된 보안을 제공합니다.

- **AWS(Amazon Web Services) S3**로 시스템 로그 전달 – 이제 시스템 로그 전달의 대상 으로 AWS S3를 선택할 수 있으며, 선택한 SIEM(Security 정보 및 이벤트 관리) 툴로 이러한 로그를 전달할 수 있습니다.
- **Azure Dsv6** 지원 - Multicloud Defense는 Azure Dsv6의 최신 인스턴스 유형을 지원하여 더 나은 성능을 제공합니다.
- **Talos** 악성 **IP** 통합 - Multicloud Defense에서 이제 Cisco Talos 에 의해 악의적인 IP 소스가 구동되어 보안 보호를 제공합니다.

버전 25.07 Multicloud Defense 컨트롤러, 2025년 7월 31일

이 릴리스에는 다음과 같은 개선 사항이 포함되어 있습니다.

- **VNet(Virtual Network)** 플로우 로그 지원 - Multicloud Defense는 Microsoft Azure에서 더 이상 사용되지 않을 때까지 NSG 플로우 로그를 지원합니다. VNet(Virtual Network) 플로우 로그 지원 - Multicloud Defense는 Microsoft Azure에서 더 이상 사용되지 않을 때까지 NSG 플로우 로그를 지원합니다. Multicloud Defense는 NSG 플로우 로그가 더 이상 지원되지 않을 때까지 계속 지원하지만, 사용자는 새로운 NSG 플로우 로그를 생성할 수 없습니다. 사용자는 대신 VNet 플로우 로그를 생성할 수 있습니다.
- 버그 수정 및 개선 사항

2025년 7월 17일 게이트웨이 핫픽스 24.06-15-a1

핫픽스입니다. 이 핫픽스에는 다음과 같은 수정 사항이 포함되어 있습니다.

- 포워딩 정책에 의해 처리되는 트래픽에 대해 TLS Hello에서 SNI(Service Name Indication)를 검색하는 게이트웨이 기능을 재구성합니다. 게이트웨이가 SNI를 검색할 수 없었던 원래 문제는 사후 양자 암호화를 수용하기 위한 TLS 라이브러리 변경으로 인해 발생했습니다. 이 변경으로 인해 Client Hello가 1415바이트보다 커집니다. 이로 인해 정책에서 도메인과 일치하거나 필터링하는 데 사용하는 SNI를 검색할 수 없게 됩니다. 기존 수정 사항은 패킷 간 타이밍 차이로 인해 SNI 검색을 보장할 수 없었습니다. 이번 수정으로 SNI를 성공적으로 검색할 수 있도록 게이트웨이가 TLS Hello 패킷을 처리하는 방법을 재작업합니다.

2025년 6월 게이트웨이 버전 24.06-15 및 컨트롤러 버전 25.06

버전 **24.06-15 Multicloud Defense** 게이트웨이, **2025**년 **7**월 **17**일

개선 사항

이 릴리스에는 다음과 같은 개선 사항이 포함되어 있습니다.

- 엣지 모드 게이트웨이 구축에 대한 VPN 지원을 추가합니다. 이를 위해 로컬 VPC/VNet CIDR을 ASA(VPN) 경로 테이블에 오케스트레이션하여 VPN을 통해 대상 애플리케이션 또는 워크로드까지 적절한 라우팅이 이루어지도록 합니다.
- AWS에서 게이트웨이의 기본 이미지로 RHEL 9를 사용할 수 있도록 상용 및 FedRAMP 환경 전반에 걸쳐 범용 지원을 추가합니다. 이는 기본 운영 체제가 상용 운영 체제임을 보장하며, 알려진 CVE를 해결하기 위해 잘 유지 관리되고 이용 가능한 취약점 패치를 제공합니다. 이 기본 운영 체제의 라이선스는 사용량 기반 요금제(PAYG)로, 구축 청구 계정에 청구됩니다. 이미지 사용으로 인해 CSP 내 인프라 비용이 증가할 것으로 예상됩니다. Azure 및 GCP의 경우 기본 운영 체제는 CentOS 9로 유지됩니다. OCI의 경우 기본 이미지는 AlmaLinux 9로 유지됩니다.

수정

이 릴리스에는 다음과 같은 수정 사항이 포함되어 있습니다.

- 여러 포워드 프록시 규칙을 동시에 비활성화할 때 프록시 구성이 제대로 정리되지 않아 데이터 경로가 재시작 루프에 진입하는 문제를 수정합니다.
- 이그레스 게이트웨이의 CPU 문제를 수정하여 CPU 사용률이 100%에 달해 트래픽 처리 문제가 발생하는 현상을 해결합니다. 이는 수백 또는 수천 개의 정책 규칙이 존재하는 환경에서 데이터 경로 초기화가 높은 CPU 사용률을 유발하고 트래픽과 무관하게 해당 상태를 유지하는 현상으로 관찰될 수 있습니다.
- m7i.xlarge 인스턴스 유형을 사용하여 구축된 게이트웨이가 시간이 지남에 따라 예상보다 높은 CPU 사용률을 유발할 수 있는 문제를 수정합니다.
- HTTPS 포워드 프록시 트래픽 처리와 관련된 문제를 수정하여 연결 속도 저하가 발생할 수 있는 상황을 방지합니다.
- 네트워크 침입 방지(IDS/IPS)가 활성화된 포워딩 정책으로 처리되는 트래픽 관련 문제를 수정합니다. 클라이언트가 TCP RST를 사용하여 연결을 종료할 경우, 게이트웨이가 해당 RST를 전달하지 않을 가능성이 있습니다. 이러한 동작은 애플리케이션 속도 저하 및 시간 초과로 이어질 수 있습니다. 이번 수정으로 RST 패킷이 게이트웨이를 통해 목적지까지 올바르게 전달되도록 보장합니다.
- 인그레스 게이트웨이의 CPU 사용률이 일시적으로 높아져 스케일 아웃이 발생한 후 스케일 인이 이어지는 문제를 수정합니다. 이 동작이 지속될 경우 영구적인 스케일 아웃 또는 스케일 인 동작이 발생할 수 있습니다.
- 소스 IP/CIDR 화이트리스트를 사용하는 인그레스 정책이 화이트리스트에 포함되지 않은 IP의 트래픽을 허용하는 문제를 수정합니다.

버전 25.06 Multicloud Defense 컨트롤러, 2025년 7월 2일

이 릴리스에는 다음과 같은 기능이 포함되어 있습니다.

- **Azure** 가상 **WAN** 경로 오케스트레이션 - Multicloud Defense는 Azure 내 지사, 원격 사용자 및 온프레미스 네트워크 간 원활한 가상 네트워크 연결을 오케스트레이션하여 Azure Virtual WAN(VWAN)과의 통합을 제공합니다. Multicloud Defense는 서비스 가상 네트워크(VNet)와 가

상 허브(vHub) 간 가상 네트워크 연결 및 경로 전파를 조정하여 온프레미스 트래픽을 클라우드로 연결하는 데 도움을 줍니다.

- 버그 수정 및 개선 사항

2025년 7월 3일 게이트웨이 핫픽스 24.06-14-b1

핫픽스입니다. 이 핫픽스에는 다음과 같은 수정 사항이 포함되어 있습니다.

- 이그레스 게이트웨이의 CPU 문제를 수정하여 CPU 사용률이 100%에 달해 트래픽 처리 문제가 발생하는 현상을 해결합니다. 이는 수백 또는 수천 개의 정책 규칙이 존재하는 환경에서 데이터 경로 초기화가 높은 CPU 사용률을 유발하고 트래픽과 무관하게 해당 상태를 유지하는 현상으로 관찰될 수 있습니다.

2025년 7월 3일 게이트웨이 25.02-02

개선 사항

이 릴리스에는 다음과 같은 개선 사항이 포함되어 있습니다.

- AWS에서 게이트웨이를 구축할 때 M7i(2코어, 4코어, 8코어) 인스턴스 유형에 대한 지원을 추가합니다. 이 개선 사항은 최신 M-클래스 제품군이 필요한 최근 도입된 지역에 게이트웨이 구축를 지원합니다.
- 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.

- 이그레스 게이트웨이의 CPU 문제를 수정하여 CPU 사용률이 100%에 달해 트래픽 처리 문제가 발생하는 현상을 해결합니다. 이는 수백 또는 수천 개의 정책 규칙이 존재하는 환경에서 데이터 경로 초기화가 높은 CPU 사용률을 유발하고 트래픽과 무관하게 해당 상태를 유지하는 현상으로 관찰될 수 있습니다.
- m7i.xlarge 인스턴스 유형을 사용하여 구축된 게이트웨이가 시간이 지남에 따라 예상보다 높은 CPU 사용률을 유발할 수 있는 문제를 수정합니다.
- 이그레스 게이트웨이 FQDN(도메인) 일치 정책에서 TLS Hello 메시지에 SNI가 존재하지 않을 경우 거부되어야 할 트래픽이 잘못 허용되는 문제를 해결합니다. SNI가 존재하지 않고 정책이 도메인을 기대하는 경우, 정책 규칙 일치가 발생하지 않아야 하며 트래픽은 기본 거부 정책에 의해 거부되어야 합니다. 이번 수정으로 트래픽이 제대로 차단되도록 보장합니다.

- 네트워크 침입 방지(IDS/IPS)가 활성화된 포워딩 정책으로 처리되는 트래픽 관련 문제를 수정합니다. 클라이언트가 TCP RST를 사용하여 연결을 종료할 경우, 게이트웨이가 해당 RST를 전달하지 않을 가능성이 있습니다. 이러한 동작은 애플리케이션 속도 저하 및 시간 초과로 이어질 수 있습니다. 이번 수정으로 RST 패킷이 게이트웨이를 통해 목적지까지 올바르게 전달되도록 보장합니다.
- 데이터 경로의 충돌 및 재시작을 유발할 수 있는 게이트웨이 데이터 경로의 안정성 문제를 수정합니다.
- 정책 변경 시 장시간 실행되는 플로우에 대한 능동 종료가 제대로 적용되지 않아, 연결이 수동적으로 닫히는 문제를 수정합니다. 번 수정으로 장기 실행 세션이 TCP 재설정을 통해 능동적으로 종료됩니다.
- 높은 CPU를 유발하여 세션 처리 기능에 영향을 미칠 수 있는 안티멀웨어 탐지 관련 문제를 수정합니다. 이 문제는 포워딩 정책에 의해 처리되는 트래픽에 대해 보호 기능이 활성화된 경우에 발생할 수 있습니다. 이번 수정으로 안티멀웨어 엔진이 트래픽을 보다 효율적으로 처리하여 성능에 영향을 주지 않으면서도 멀웨어를 정확히 탐지할 수 있도록 보장합니다.
- 정책 규칙 집합 전달 규칙을 비활성화하거나 활성화할 때 파란색/녹색 데이터 경로가 교체되는 문제를 수정합니다. 이 시나리오에서는 데이터 경로 교체가 필요하지 않으며 정책 변경 사항이 기존 세션에 영향을 주지 않고 빠르게 적용되어야 합니다. 수정을 통해 파란색/녹색 데이터 경로를 교체하지 않고도 이러한 유형의 정책 변경을 수용할 수 있습니다.
- 인증서 개체에 대한 업데이트가 게이트웨이에 적용되지 않는 문제를 수정합니다. 게이트웨이는 게이트웨이 인스턴스가 교체되거나 데이터 경로가 재시작될 때까지 기존 인증서를 계속 사용합니다. 이번 수정으로 업데이트된 인증서가 게이트웨이 정책에 적용되고 트래픽 처리에 사용되도록 보장합니다.
- 파란색/녹색 데이터 경로 교체를 트리거하는 정책 변경으로 인해 트래픽 처리가 예상보다 길어져 데이터 경로가 세션을 처리할 수 없게 되는 문제를 수정합니다. 이 시나리오는 정책 변경 중에 게이트웨이 및/또는 진단 번들에서 캐싱이 활성화된 DNS 기반 FQDN 주소 개체를 사용하는 경우가 발생할 수 있습니다. 각각은 이러한 요청을 처리하기 위해 데이터 경로가 세션 처리와 병행하여 서비스를 제공해야 하므로, 후자의 지연을 초래합니다. 이번 수정으로 세션 처리에 최우선 순위를 부여하여 중단이 발생하지 않도록 보장합니다.
- 디스크 공간 부족으로 인해 정책이 완료되지 않아 게이트웨이 정책 변경이 업데이트 중 상태에서 중단될 수 있는 문제를 수정합니다. 이 시나리오는 게이트웨이 인스턴스가 활성 상태인 매우 긴 시간 동안에만 발생합니다. 이번 수정으로 장기 실행 게이트웨이 인스턴스가 정책 변경 사항을 성공적으로 처리할 수 있도록 디스크 공간 문제의 근본 원인을 해결합니다.
- CPU 및 메모리 소비를 정상 수준보다 높게 유발하는 방치된 연결과 관련된 문제를 수정합니다. 방치된 연결은 클라이언트와 서버가 연결을 닫거나 재설정하지 않고 사라지기 때문에 열려 있는 연결입니다. 이전에는 게이트웨이가 이러한 연결을 최대 12분 동안 유지하여 연결 풀 용량을 소모했고, 그 결과 CPU 및 메모리 사용량이 증가하여 추가 용량 요구를 충족하기 위한 불필요한 스케일 아웃이 이루어졌습니다. 이번 수정에서는 방치된 연결의 유지 시간을 줄일 수 있도록 조정 가능한(튜너블) 설정을 도입합니다. 이러한 시나리오가 발생하면 시스코 지원팀에 문의하여 시나리오를 평가하고 방치된 연결이 게이트웨이 용량에 미치는 영향을 줄이도록 설정을 조정하십시오.

- VPN을 지원하지 않는 게이트웨이 버전에서 VPN을 지원하는 버전으로 업그레이드하는 경우, VPN 라우트 테이블에 라우트 접두사를 추가하는 과정과 관련된 불안정성으로 인해 새 버전의 게이트웨이 인스턴스가 활성화되지 않을 수 있는 문제를 수정합니다.
- no SNAT 포워딩 정책에서 TLS Client Hello 메시지로부터 SNI(Service Name Indication)를 검색하지 못해, 게이트웨이가 TCP RST를 사용하여 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.
- WAF 보호가 활성화된 정책에서 WAF 규칙 집합 업데이트 중에 트래픽이 중단될 수 있는 인그레스 게이트웨이 문제를 수정합니다. 현상은 WAF 프로파일 이름이 특정한 방식으로 지정된 경우에만 발생합니다. 이번 수정으로 사용자가 지정하고 컨트롤러/UI에서 허용한 이름을 게이트웨이에서 올바르게 수락하여 규칙 집합 업데이트 중에 중단이 발생하지 않도록 하여 문제를 해결합니다.
- 정책의 작업이 거부로 설정된 트래픽 처리 시 CPU 사용률이 예상보다 높아지는 문제를 수정합니다.
- SMB 트래픽 처리 시 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.
- 소스 IP/CIDR 화이트리스트를 사용하는 인그레스 정책이 화이트리스트에 포함되지 않은 IP의 트래픽을 허용하는 문제를 수정합니다.
- 다중 부분 데이터에서 데이터 손실 방지(DLP) 탐지 관련 문제를 수정합니다. 탐지 대상 문자열이 파일 시작 부분 또는 끝 부분에 있을 경우 탐지에 성공합니다. 다른 위치에 있으면 탐지에 실패합니다. 파일 크기도 적절한 탐지에 영향을 줄 수 있습니다. 이번 수정으로 문자열이 멀티파트 데이터 내에서 위치에 관계없이 반드시 탐지되도록 보장합니다.
- 이그레스 게이트웨이에서 처리된 트래픽에 대해 DLP 보호 기능이 악성 활동을 감지하여 해당 트래픽을 악성으로 표시했지만, 해당 세션의 이벤트 보기에서 DLP 이벤트가 누락되는 문제를 수정합니다. 이 수정으로 DLP 이벤트가 세션 이벤트에 표시됩니다.
- 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.
- UDP 프래그먼트화가 포함된 UDP 세션에서 프래그먼트가 수신되지 않을 경우 해당 세션이 종료 및 정리되지 않는 문제를 수정합니다.
- 트래픽 요약 로그에서 프래그먼트화가 발생한 세션에 대해 올바른 UDP 프래그먼트 수를 표시하지 않는 문제를 수정합니다.

- 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 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, 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. 향후 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.

- 새로 인스턴스화된 게이트웨이 인스턴스가 활성 상태가 될 때 Azure 인그레스 게이트웨이가 충돌할 수 있는 문제를 수정합니다.

- 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.

- 소스 IP/CIDR 화이트리스트를 사용하는 인그레스 정책이 화이트리스트에 포함되지 않은 IP의 트래픽을 허용하는 문제를 수정합니다.

2025년 2월 28일 게이트웨이 25.02-01

개선 사항

이 릴리스에는 다음과 같은 개선 사항이 포함되어 있습니다.

- UDP 프래그먼트화에 대한 지원을 추가합니다. 이 기능 향상을 위해서는 게이트웨이 설정이 활성화되어야 하며, 이는 Terraform 게이트웨이 리소스에서 지정할 수 있습니다.
- 세션 상태 요약 정보를 개선합니다. 개선 사항: 게이트웨이 및 프록시 시간 초과로 인해 종료된 세션 표시 - 어떠한 사유(시간 초과, 데이터 경로 재시작)로든 게이트웨이에 의해 종료된 모든 연결 재설정 - 게이트웨이에 의해 종료된 세션에 대해 클라이언트와 서버 양측에 연결 재설정 전송 - 장시간 실행 세션에 대해 주기적으로 생성되는 세션 요약 로그
- FedRamp에 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.
- 트래픽 요약 로그에 세션 지속 시간 기록 기능을 추가합니다. 기간은 TCP SYN 또는 첫 번째 UDP 패킷 전송 시점부터 세션이 종료되거나 중단될 때까지입니다.
- 네트워크 침입 탐지(IDS/IPS) 엔진을 강화하여 HTTP 0.9, 디플레이트 압축, gzip 압축, 이중 압축(디플레이트 + gzip), 청크 전송 및 HTTP/1.1 100 OK 응답 코드를 포함한 HTTP 회피 기법을 탐지하고 차단합니다.
- 정책 규칙 집합 규칙의 로그 미기록 동작을 준수하기 위해 게이트웨이 활성화 로그 전달 프로파일에 구성된 모든 대상에 로그를 전송하지 않도록 개선 사항을 제공합니다.
- FedRAMP 환경에 구축하기 위해 필요한 STIG 및 CIS 레벨 2 요구사항을 수용하기 위한 게이트웨이 강화 기능의 지속적인 개선.
- FedRAMP 요구 사항을 수용하기 위해 기본 이미지를 CentOS에서 RHEL9로 변경. 이 변경 사항은 향후 릴리스에서 FedRAMP 인증이 적용되지 않은 게이트웨이 기본 이미지에 통합될 예정입니다.
- 장시간 실행 세션에 대해 주기적으로 트래픽 요약 로그를 기록하는 기능을 지원합니다. 역사적으로, 트래픽 요약 로그는 세션이 종료될 때만 기록되었습니다. 짧은 기간의 세션에는 효과적이지만, 장시간 실행되는 세션에는 적합하지 않습니다. 이 개선 사항은 동일한 세션 ID 및 튜플 정보를 유지하되 업데이트된 통계(바이트/패킷)를 포함하여 5분마다 트래픽 요약 로그를 생성합니다. 세션이 종료될 때 최종 로그도 생성됩니다.
- 드레인 타임아웃을 구성하기 위한 게이트웨이 설정을 제공합니다. 기본 설정값은 2분입니다. 이 게이트웨이 설정을 적용할 때 사용자는 드레인 타이머를 구성할 수 있습니다. 기본값 변경이 필요한 경우 시스코 지원팀에 문의하십시오.

수정 사항

이 릴리스에는 다음과 같은 수정 사항이 포함되어 있습니다.

- 사후양자 암호화가 활성화된 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.

- 브라우저 기반 클라이언트에서 사후양자 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.

- 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 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, 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. 향후 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.

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

- GCP의 게이트웨이가 헬스 체크 서비스 실패로 인해 정상 상태와 비정상 상태 사이를 오가며 인스턴스 교체가 발생할 수 있는 문제를 수정합니다.

- 게이트웨이 교체, 정책 변경 또는 시간 초과 시 일부 장기간 활성 상태인 연결이 제대로 재설정되지 않는(TCP RST) 문제를 수정합니다.

- 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 발견되었습니

다. 이번 업데이트로 문제가 해결되어 새로운 탈로스 규칙 세트를 성공적으로 적용할 수 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.
- 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.
- 트래픽을 적절한 정책 규칙과 일치시키려고 할 때 이그레스 게이트웨이 포워드 프록시 정책이 중단될 수 있는 문제를 수정합니다.
- 백엔드 연결이 응답하지 않아 트래픽 처리에 지연이 발생하는 프록시 시나리오에서 게이트웨이가 불필요하게 CPU를 소모하는 문제를 수정합니다.
- 인그레스 게이트웨이 역방향 프록시 정책에서 멀웨어가 탐지될 때 발생하던 게이트웨이 충돌을 수정합니다.
- Kyber 암호화 모음을 포함하는 TLS 세션으로 인해 CPU 사용량이 증가하여 트래픽 처리가 불가능해지는 문제를 수정합니다.
- 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.
- SNAT 포워딩 정책에서 TLS Client Hello 메시지로부터 SNI(Service Name Indication)를 검색하지 못해, 게이트웨이가 TCP RST를 사용하여 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 SNAT 포워딩 정책이 1415바이트를 초과하는 Client Hello 크기도 지원할 수 있습니다.
- 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.
- 알려진 악성 코드가 탐지 및 차단되지 않던 안티멀웨어 엔진의 문제를 수정합니다. 이번 수정에 안티멀웨어 엔진 업데이트가 포함됩니다.

- 멀웨어 서명을 제대로 감지하지 못하는 문제가 간헐적으로 발생할 수 있는 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.
- 기본 구성과 다르게 설정된 해독 프로파일이 게이트웨이에 제대로 적용되지 않아 클라이언트와 게이트웨이 간 암호 모음 불일치로 TLS 협상 실패가 발생하는 문제를 수정합니다.
- UDP 세션이 정상적으로 제대로 집계되지 않아 관련된 활성 연결 및 연결율 통계가 잘못 기록되던 문제를 수정합니다.
- 빈 FQDN/URL 필터링 프로파일이 정책 규칙 집합 규칙에 할당된 경우 게이트웨이가 자가 복구되던 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.
- 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 64,000개의 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.
- 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.
- 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, 다른 모든 도메인은 거부됩니다.
- 거부 시 재설정이 활성화된 상태에서 FQDN 일치 프로파일을 사용하는 거부 동작을 가진 전달 정책으로 처리된 트래픽에 대해 TCP 재설정이 전송되지 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 20,000k 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.
- 다양한 CVE를 해결하도록 게이트웨이 라이브러리 업데이트.
- 인증서가 Key Vault, Secrets Manager 및 KMS와 같은 CSP 서비스에서 개인 키에 액세스하도록 구성된 경우 인증서의 개인 키 업데이트와 관련된 다양한 문제를 수정합니다. 이번 수정으로 CSP 서비스 내 리소스에 대한 모든 업데이트가 게이트웨이에 의해 감지되도록 하여, 게이트웨이가 업데이트를 검색하고 트래픽 처리 중에 이를 반영할 수 있도록 보장합니다.
- 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.
- 웹 보호(WAF) 또는 네트워크 침입(IDS/IPS) 프로파일의 PCAP을 변경할 때 불필요하게 블루/그린 데이터 경로 교체가 트리거되는 문제를 수정합니다.
- 네트워크 침입(IDS/IPS) 프로파일에서 PCAP을 활성화하거나 비활성화할 때 불필요하게 블루/그린 데이터 경로 재시작이 트리거되던 문제를 수정합니다.
- 포워딩 서비스 개체에서 SNAT를 활성화하거나 비활성화할 때 불필요하게 블루/그린 데이터 경로 재시작이 트리거되던 문제를 수정합니다.
- 고급 보안 프로파일(WAF, IDS/IPS, 안티멀웨어 등)의 이름을 변경할 때 불필요하게 블루/그린 데이터 경로 교체가 트리거되던 문제를 수정합니다.

2025년 6월 5일 게이트웨이 핫픽스 24.06-14-a1

핫픽스입니다. 이 핫픽스에는 다음과 같은 수정 사항이 포함되어 있습니다.

- **no SNAT** 포워딩 정책에서 TLS Client Hello 메시지로부터 SNI(Service Name Indication)를 검색하지 못해, 게이트웨이가 TCP RST를 사용하여 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 no SNAT 포워딩 정책에서 1415바이트를 초과하는 Client Hello 크기도 지원할 수 있습니다.
- **SNAT** 포워딩 정책에서 TLS Client Hello 메시지로부터 SNI(Service Name Indication)를 검색하지 못해, 게이트웨이가 TCP RST를 사용하여 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 SNAT 포워딩 정책이 1415바이트를 초과하는 Client Hello 크기도 지원할 수 있습니다.

- 사후양자 암호화가 활성화된 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.

2025년 5월 게이트웨이 버전 24.06-14 및 컨트롤러 버전 25.05

버전 **24.06-14 Multicloud Defense** 게이트웨이**, 2025**년 **6**월 **5**일

이 릴리스에는 다음과 같은 수정 사항이 포함되어 있습니다.

- 정책 변경 시 장시간 실행되는 플로우에 대한 능동 종료가 제대로 적용되지 않아, 연결이 수동적으로 닫히는 문제를 수정합니다. 번 수정으로 장기 실행 세션이 TCP 재설정을 통해 능동적으로 종료됩니다.
- 데이터 경로의 충돌 및 재시작을 유발할 수 있는 게이트웨이 데이터 경로의 안정성 문제를 수정합니다.
- 정책 규칙 집합 전달 규칙을 비활성화하거나 활성화할 때 파란색/녹색 데이터 경로가 교체되는 문제를 수정합니다. 이 시나리오에서는 데이터 경로 교체가 필요하지 않으며 정책 변경 사항이 기존 세션에 영향을 주지 않고 빠르게 적용되어야 합니다. 수정을 통해 파란색/녹색 데이터 경로를 교체하지 않고도 이러한 유형의 정책 변경을 수용할 수 있습니다.
- 파란색/녹색 데이터 경로 교체를 트리거하는 정책 변경으로 인해 트래픽 처리가 예상보다 길어져 데이터 경로가 세션을 처리할 수 없게 되는 문제를 수정합니다. 이 시나리오는 정책 변경 중에 게이트웨이 및/또는 진단 번들에서 캐싱이 활성화된 DNS 기반 FQDN 주소 개체를 사용하는 경우가 발생할 수 있습니다. 각각은 이러한 요청을 처리하기 위해 데이터 경로가 세션 처리와 병행하여 서비스를 제공해야 하므로, 후자의 지연을 초래합니다. 이번 수정으로 세션 처리에 최우선 순위를 부여하여 중단이 발생하지 않도록 보장합니다.

버전 **25.05 Multicloud Defense** 컨트롤러**, 2025**년 **6**월 **5**일

이 릴리스에는 다음과 같은 개선 사항이 포함되어 있습니다.

- **Secure Firewall Threat Defense Virtual** 디바이스 오케스트레이션 - 이제 Multicloud Defense 방어를 사용하여 Secure Firewall Threat Defense Virtual 디바이스를 오케스트레이션, 구축 및 등록할 수 있습니다. 이렇게 하면 동일한 위치에서 정책을 관리하는 동시에 방화벽을 온프레미스 및 클라우드 환경에 사용하는 것과 동일하게 유지하는 데 도움이 됩니다. Multicloud Defense는 구축을 관리하며 클라우드에서 쉽게 구축할 수 있도록 지원합니다.
- **Cloud Explorer**는 모든 리소스와 그 관계를 시각화할 수 있는 단일 통합 보기를 제공합니다. Cloud Explorer를 사용하면 강력한 보안 태세를 쉽게 구축할 수 있습니다. 끌어다 놓기(drag and drop)와 간단한 클릭을 통해 연결을 형성하고 보호 조치를 통해 자산을 보호할 수 있습니다.
- 버그 수정 및 개선 사항

2025년 5월 23일 게이트웨이 핫픽스 24.06-13-a1

핫픽스입니다. 이 핫픽스에는 다음과 같은 수정 사항이 포함되어 있습니다.

- **no SNAT** 포워딩 정책에서 TLS Client Hello 메시지로부터 SNI(Service Name Indication)를 검색하지 못해, 게이트웨이가 TCP RST를 사용하여 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 no SNAT 포워딩 정책에서 1415바이트를 초과하는 Client Hello 크기도 지원할 수 있습니다.
- **SNAT** 포워딩 정책에서 TLS Client Hello 메시지로부터 SNI(Service Name Indication)를 검색하지 못해, 게이트웨이가 TCP RST를 사용하여 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 SNAT 포워딩 정책이 1415바이트를 초과하는 Client Hello 크기도 지원할 수 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.

2025년 5월 23일 게이트웨이 24.06-13

이 릴리스에는 다음과 같은 수정 사항이 포함되어 있습니다.

- 디스크 공간 부족으로 인해 정책이 완료되지 않아 게이트웨이 정책 변경이 업데이트 중 상태에서 중단될 수 있는 문제를 수정합니다. 이 시나리오는 게이트웨이 인스턴스가 활성 상태인 매우 긴 시간 동안에만 발생합니다. 이번 수정으로 장기 실행 게이트웨이 인스턴스가 정책 변경 사항을 성공적으로 처리할 수 있도록 디스크 공간 문제의 근본 원인을 해결합니다.
- WAF 보호가 활성화된 정책에서 WAF 규칙 집합 업데이트 중에 트래픽이 중단될 수 있는 인그레스 게이트웨이 문제를 수정합니다. 현상은 WAF 프로파일 이름이 특정한 방식으로 지정된 경우에만 발생합니다. 이번 수정으로 사용자가 지정하고 컨트롤러/UI에서 허용한 이름을 게이트웨이에서 올바르게 수락하여 규칙 집합 업데이트 중에 중단이 발생하지 않도록 하여 문제를 해결합니다.
- 이그레스 게이트웨이에서 처리된 트래픽에 대해 DLP 보호 기능이 악성 활동을 감지하여 해당 트래픽을 악성으로 표시했지만, 해당 세션의 이벤트 보기에서 DLP 이벤트가 누락되는 문제를 수정합니다. 이 수정으로 DLP 이벤트가 세션 이벤트에 표시됩니다.

2025년 5월 9일 게이트웨이 핫픽스 24.06-12-a1

핫픽스입니다. 이 핫픽스에는 다음과 같은 수정 사항이 포함되어 있습니다.

- **no SNAT** 포워딩 정책에서 TLS Client Hello 메시지로부터 SNI(Service Name Indication)를 검색하지 못해, 게이트웨이가 TCP RST를 사용하여 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 no SNAT 포워딩 정책에서 1415바이트를 초과하는 Client Hello 크기도 지원할 수 있습니다.
- **SNAT** 포워딩 정책에서 TLS Client Hello 메시지로부터 SNI(Service Name Indication)를 검색하지 못해, 게이트웨이가 TCP RST를 사용하여 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 SNAT 포워딩 정책이 1415바이트를 초과하는 Client Hello 크기도 지원할 수 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.

2025년 5월 9일 게이트웨이 24.06-12

이 릴리스에는 다음과 같은 수정 사항이 포함되어 있습니다.

- CPU 및 메모리 소비를 정상 수준보다 높게 유발하는 방치된 연결과 관련된 문제를 수정합니다. 방치된 연결은 클라이언트와 서버가 연결을 닫거나 재설정하지 않고 사라지기 때문에 열려 있는 연결입니다. 이전에는 게이트웨이가 이러한 연결을 최대 12분 동안 유지하여 연결 풀 용량을 소모했고, 그 결과 CPU 및 메모리 사용량이 증가하여 추가 용량 요구를 충족하기 위한 불필요한 스케일 아웃이 이루어졌습니다. 이번 수정에서는 방치된 연결의 유지 시간을 줄일 수 있도록 조정 가능한(튜너블) 설정을 도입합니다. 이러한 시나리오가 발생하면 시스코 지원팀에 문의하여 시나리오를 평가하고 방치된 연결이 게이트웨이 용량에 미치는 영향을 줄이도록 설정을 조정하십시오.
- VPN을 지원하지 않는 게이트웨이 버전에서 VPN을 지원하는 버전으로 업그레이드하는 경우, VPN 라우트 테이블에 라우트 접두사를 추가하는 과정과 관련된 불안정성으로 인해 새 버전의 게이트웨이 인스턴스가 활성화되지 않을 수 있는 문제를 수정합니다.

2025년 5월 7일 게이트웨이 핫픽스 24.06-11-a1

핫픽스입니다. 이 핫픽스에는 다음과 같은 수정 사항이 포함되어 있습니다.

- **no SNAT** 포워딩 정책에서 TLS Client Hello 메시지로부터 SNI(Service Name Indication)를 검색하지 못해, 게이트웨이가 TCP RST를 사용하여 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 no SNAT 포워딩 정책에서 1415바이트를 초과하는 Client Hello 크기도 지원할 수 있습니다.
- **SNAT** 포워딩 정책에서 TLS Client Hello 메시지로부터 SNI(Service Name Indication)를 검색하지 못해, 게이트웨이가 TCP RST를 사용하여 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 SNAT 포워딩 정책이 1415바이트를 초과하는 Client Hello 크기도 지원할 수 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.

2025년 4월 게이트웨이 버전 24.06-11 및 컨트롤러 버전 25.04

버전 **24.06-11 Multicloud Defense** 게이트웨이, **2025**년 **5**월 **7**일

이 릴리스에는 다음과 같은 수정 사항이 포함되어 있습니다.

- **no SNAT** 포워딩 정책에서 TLS Client Hello 메시지로부터 SNI(Service Name Indication)를 검색하지 못해, 게이트웨이가 TCP RST를 사용하여 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 no SNAT 포워딩 정책에서 1415바이트를 초과하는 Client Hello 크기도 지원할 수 있습니다.
- **SNAT** 포워딩 정책에서 TLS Client Hello 메시지로부터 SNI(Service Name Indication)를 검색하지 못해, 게이트웨이가 TCP RST를 사용하여 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 SNAT 포워딩 정책이 1415바이트를 초과하는 Client Hello 크기도 지원할 수 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.

버전 **25.04 Multicloud Defense** 컨트롤러, **2025**년 **4**월 **30**일

이 릴리스에는 다음과 같은 개선 사항이 포함되어 있습니다.

- **M7i** 지원 - Multicloud Defense는 AWS 계정의 M7i 인스턴스 유형에 대한 지원을 제공합니다.
- 메트릭 전달 로그에서 이제 **AmazonS3** 및 **Splunk** 지원 - 이제 Multicloud Defense 컨트롤러에서 S3/Splunk에 대한 메트릭 전달 로그를 설정할 수 있습니다. S3/Splunk는 클라우드 개체 저장 서비스인 Amazon S3와 데이터 분석 플랫폼인 Splunk 간의 통합을 의미합니다.
- **Security Cloud Control** 지원 - Security Cloud Control에 대한 지속적인 통합 지원에는 일반 대시보드 및 호환성 업데이트가 포함됩니다.
- 개선된 보고서 요약 - "검색" 및 "위협 지표 스냅샷" 보고서에는 이제 클라우드 네트워크 환경에서 발생하는 상황을 요약해 보여주는 AI 생성 요약이 포함됩니다. 검색 보고서는 검색이 활성화된 경우에만 생성됩니다. 마찬가지로, 위협 지표 스냅샷 보고서는 게이트웨이가 활성 상태로 구축된 경우에만 적용됩니다.
- 전달 대상 검증을 위한 새로운 "테스트" 버튼 - 이제 로그 전달 프로파일의 대상 위치를 구성 완료 전에 검증할 수 있습니다. 표시되는 텍스트 필드에 테스트 메시지를 입력하고 **Validate(**확인**)** 를 클릭하여 메시지를 전송하면 됩니다. 메시지가 성공적으로 전송되었음을 확인한 후 로그 전달 프로파일을 완료할 수 있습니다.