Multicloud Defense 소개

Multicloud Defense 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 계정을 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

이 제품의 구성 요소에 대한 자세한 내용을 보려면 계속 읽으십시오.

멀티 클라우드 방어 구성 요소

멀티 클라우드 방어에서는 퍼블릭 클라우드 및 SDN(Software Defined Networking)에서 공통 원칙을 사용하며, 이는 컨트롤 플레인과 데이터 플레인을 분리하여 두 가지 솔루션 구성 요소인 멀티 클라우드 방어 컨트롤러 및 멀티 클라우드 방어 게이트웨이(으)로 변환합니다.

멀티 클라우드 방어 컨트롤러

멀티 클라우드 방어 컨트롤러은(는) 관리 및 컨트롤 플레인을 제공하는, 안정성과 확장성이 뛰어난 중앙 집중식 컨트롤러입니다. SaaS(Software-as-a-Service)로 실행되며 멀티 클라우드 방어에서 완전히 관리 및 유지 보수합니다. 고객은 멀티 클라우드 방어 컨트롤러을(를) 활용하기 위해 웹 포털에 액세스하거나 Terraform용 멀티 클라우드 방어 제공자를 사용하여 보안을 DevOps/DevSecOps 프로세스에 인스턴스화할 수 있습니다.

멀티 클라우드 방어 게이트웨이

멀티 클라우드 방어 게이트웨이은(는) 멀티 클라우드 방어 컨트롤러에 의해 고객 퍼블릭 클라우드 계정에 PaaS(patform-as-a-service)로 구축된 자동 확장 멀티 클라우드 방어 소프트웨어 집합입니다. 고급 인라인 보안 보호 기능을 제공하여 외부 공격을 차단하고 이그레스 데이터 유출을 방지하며 공격의 측면 이동을 방지합니다. 멀티 클라우드 방어 게이트웨이에는 TLS 암호 해독, 침입 탐지 및 방지(IDS/IPS), 웹 애플리케이션 방화벽(WAF), 안티바이러스 필터링, DLP(데이터 손실 방지) 및 FQDN/URL 필터링 기능이 포함됩니다.

멀티 클라우드 방어 **SaaS** 컨트롤러

멀티 클라우드 방어 SaaS 컨트롤러는 게이트웨이 스택을 관리합니다. 다양한 마이크로서비스가 장착된 컨트롤러에는 CSP LB 및 게이트웨이 인스턴스의 오케스트레이션을 지원하는 API 서버가 포함되어 있습니다. 이를 통해 로드 밸런서 자체에 의해 모니터링되는 로드 밸런서의 "대상 풀"에서 인스턴스 추가 및 제거로 동적 확장이 가능합니다.

구성

멀티 클라우드 방어 게이트웨이은(는) 약 3초마다 멀티 클라우드 방어 컨트롤러과(와) 지속적인 통신을 수행하여 상태 및 정책 업데이트를 전송합니다. 따라서 필요에 따라 사전 상태 보고, 게이트웨이 교체 및 확장성 조정을 활성화할 수 있습니다.

최적화된 게이트웨이 인스턴스

멀티 클라우드 방어 게이트웨이 인스턴스는 효율적인 트래픽 처리 및 고급 보안 시행을 위해 단일 패스 데이터 경로 파이프라인을 통합하여 고도로 최적화된 소프트웨어에서 작동합니다. 각 게이트웨이 인스턴스는 정책 시행을 담당하는 "worker" 프로세스, 트래픽 배포 및 세션 관리를 담당하는 "distributor" 프로세스, 컨트롤러와 통신하는 "agent" 프로세스의 3가지 핵심 프로세스로 구성됩니다. 게이트웨이 인스턴스를 "데이터 경로 재시작"을 위해 "서비스 중"으로 원활하게 전환할 수 있으므로 트래픽 흐름을 중단하지 않고 원활한 업데이트를 수행할 수 있습니다.

고급 보안 프로파일

멀티 클라우드 방어 게이트웨이은(는) 단일 패스 데이터 경로 파이프라인 내에서 세분화된 보안 프로파일을 구현하여 진화하는 트래픽 요구 사항을 충족합니다. 고객은 필요에 따라 고급 보안 프로파일을 유연하게 활성화 또는 비활성화할 수 있습니다. 파이프라인의 단일 패스 아키텍처는 서드파티 엔진으로 트래픽을 오프로드할 필요가 없습니다. 예를 들어, 전체 TLS 암호 해독이 파이프라인 내에서 선택적으로 트리거되므로 불필요한 데이터 전송 없이 효율적으로 처리할 수 있습니다.

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.

서드파티 제품 지원 및 버전 관리

멀티 클라우드 방어은(는) 추가 제품 및 기능을 사용합니다. 최적의 작업을 위해 나열된 적절한 버전을 사용하는 것이 좋습니다.

인터넷 브라우저

멀티 클라우드 방어 구성 요소에 대해 다음과 같은 인터넷 브라우저를 지원 및 권장합니다.

표 *1:*

브라우저	지원
Chrome	예. 이 브라우저를 사용하는 것이 좋습니다.
Firefox	예.
Edge	예.
Safari	예.
Internet Explorer	예.

AWS용 인스턴스 메타데이터 서비스

IMDS(Instance Metadata Service)는 Amazon EC2 인스턴스에서 인스턴스 메타데이터에 액세스하는 데 사용됩니다. 멀티 클라우드 방어 컨트롤러 버전 23.10은 해당 멀티 클라우드 방어 게이트웨이버전에 따라 IMDSv2를 필수 또는 옵션으로 설정합니다.

Amazon EC2 인스턴스의 최적의 보안을 위해 **Required(**필수**)** 모드에서는 IMDSv2를 특별히 지원하는 멀티 클라우드 방어 게이트웨이 버전으로 업그레이드하는 것이 좋습니다.

참고 멀티 클라우드 방어 컨트롤러 버전 23.10은 EC2 인스턴스의 경우 23.04 이후 멀티 클라우드 방어 게이트웨이 버전을 기본 IMDSv2로 설정합니다.

아래 표를 사용하여 환경의 EC2 인스턴스 내부에 설정할 IMDS 버전을 확인하십시오.

멀티 클라우드 방어 게이트웨이 버전	필수 **IMDS** 버전
23.08	IMDSv2(필수)
23.06	IMDSv2(필수)

멀티 클라우드 방어 게이트웨이 버전	필수 **IMDS** 버전
23.04	IMDSv2(필수)
23.02	IMDSv1 IMDSv2(옵션)
22.12	IMDSv1 IMDSv2(옵션)

IMDS 버전 및 선택한 버전으로 마이그레이션하는 방법에 대한 자세한 내용은 AWS 설명서를 참조하십시오.

멀티 클라우드 방어 구성 요소의 권장 버전

개선 사항, 새로운 기능, 버그 수정을 위해 최신 업그레이드 및 업데이트를 통해 구성 요소를 최신 상태로 유지하는 것이 좋습니다. 사용 가능한 업데이트 및 업그레이드, 각 패키지의 솔루션에 대한 자세한 내용은 Cisco Multicloud Defense 릴리스 노트를 참조하십시오.

지원되는 디스크 크기

적절한 게이트웨이 버전에 대한 다음과 같은 디스크 크기 지원을 고려하십시오.

표 *2:* 게이트웨이 버전별 디스크 크기

게이트웨이 버전	지원되는 디스크 크기
최대 23.10	256GB

서비스 공지 사항

다음 공지 사항은 멀티 클라우드 방어 제품 및 구성 요소 전체에 적용됩니다. 이러한 문제에 대한 질문이나 문제가 있는 경우 지원 팀에 문의하여 자세한 내용을 확인하십시오.

IP 기반 지역 차단

멀티 클라우드 방어 게이트웨이버전 23.10부터 Cisco의 내보내기 및 계약 컴플라이언스는 멀티 클라우드 방어 플랫폼 및 구성 요소를 사용하는 고객에게 적용됩니다. 다음 동작은 IP 기반 지역 차단에서 구현됩니다.

- 지역 차단이 있는 제재 지역에서 제공되는 것으로 식별된 IP 주소에서 시작하는 쿼리에 대한 DNS 서비스에는 보안 또는 콘텐츠 필터링 정책이 적용되지 않습니다. 보고도 비활성화됩니다. DNS 쿼리는 여전히 유효한 응답을 수신하며 나머지 지역의 트래픽과 동일한 서비스 수준으로 처리됩니다.

- 로밍 클라이언트 동기화 및 내부 도메인 목록은 계속해서 대시보드와 동기화되어야 하며 정상적인 동작(내부 도메인을 내부 DNS 서버로 전송)을 제공해야 합니다. 이 내용은 나중에 변경될 수 있습니다.
- IP 기반 지역 차단이 국가에 완전히 구현되면 Umbrella 대시보드와 API 액세스도 차단됩니다.