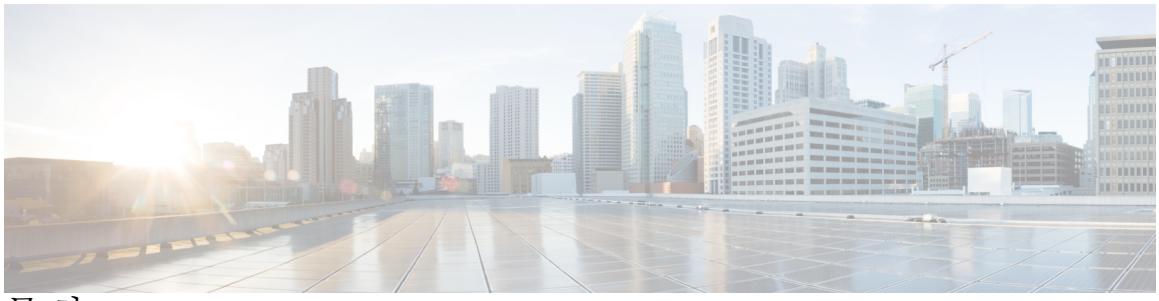
Cisco 멀티 클라우드 방어 사용 가이드

초판: 2023년 5월 19일

최종 변경: 2024년 6월 5일

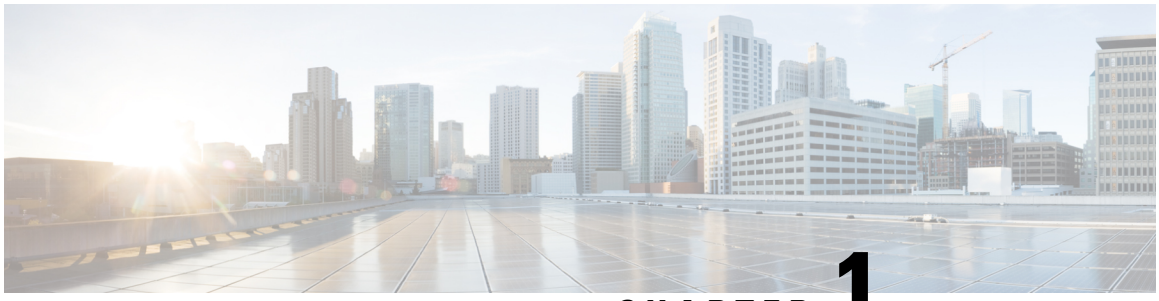
Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



목 차

부

멀티 클라우드 방어 사용 설명서



CHAPTER 1

멀티 클라우드 방어 소개

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

멀티 클라우드 방어 명명 규칙

멀티 클라우드 방어에서는 다양한 클라우드 서비스 제공자와 상호 작용하며, 플랫폼 전반에 걸쳐 범용 환경을 제공하기 위해 사용자가 게이트웨이 및 개체를 생성할 때 문자 수를 제한합니다. 멀티 클라우드 방어 외부에 있는 게이트웨이 및 개체는 이름 앞에 `ciscomcd`가 추가되며, 이는 원래 게이트웨이 또는 개체 이름이 너무 길면 문제가 발생할 수 있습니다.

멀티 클라우드 방어 내부 및 외부에서 게이트웨이나 개체의 이름을 지정할 때는 다음과 같은 문자 제한을 고려하십시오.

표 *1:* 명명 규칙에 대한 문자 제한

멀티 클라우드 방어 기능	최대 허용 문자 수
게이트웨이 인스턴스	55
개체 이름	63

참고 위의 값은 앞에 추가되는 멀티 클라우드 방어 태그가 없는 이름의 문자 제한을 나타냅니다. 게이트웨이나 개체의 이름을 지정할 때 태그를 포함할 수 없습니다.

지원 지역

멀티 클라우드 방어에서는 다음 지역을 지원합니다.

- 미국(US) - us-west-2
- 유럽(EU) - eu-central-1
- 도쿄(APJ) - ap-northeast-1
- 시드니(APJ) - ap-southeast-2
- 델리(APJ) - ap-south-1

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 멀티 클라우드 방어 릴리스 노트를 참조하십시오.

서드파티 제품 지원 및 버전 관리

멀티 클라우드 방어는 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 *2:* 인터넷 브라우저 지원

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)
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.

지원되는 디스크 크기

적절한 게이트웨이 버전에 대한 다음과 같은 디스크 크기 지원을 고려하십시오.

표 ***3:*** 게이트웨이 버전별 디스크 크기

게이트웨이 버전	지원되는 디스크 크기
23.12 이상	128GB
최대 23.10	256GB

멀티 클라우드 방어 **in Cisco Security Cloud** 제어

Security Cloud Control은 Cisco Security Cloud 전체에서 Cisco Secure 제품 인스턴스, 사용자 ID 및 사용자 액세스 관리의 중앙 집중식 관리를 제공하는 웹 애플리케이션입니다. Security Cloud Control 관리자는 새로운 Security Cloud 엔터프라이즈를 생성하고, 엔터프라이즈의 사용자를 관리하고, 도메인을 클레임하고, 조직의 SSO ID 제공자를 통합하는 등의 작업을 수행할 수 있습니다.

멀티 클라우드 방어에 등록하면 보안 클라우드 제어는 기본적으로 테넌시에 대한 어카운트를 생성하여 엔터프라이즈 전반에 걸쳐 더 효율적으로 관리합니다. Security Cloud 엔터프라이즈는 다음 경우를 지원합니다. 라이선스는 구매하고 이미 멀티 클라우드 방어 어카운트가 있는 경우와 라이선스를 구매했지만 현재 멀티 클라우드 방어 어카운트가 없는 경우입니다.

다음 여러 번의 릴리스에 걸쳐

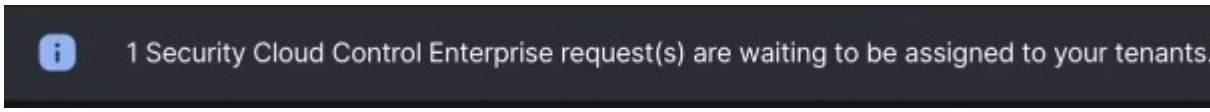
보안 클라우드 제어 대시보드에서 다음 단계를 완료해야 합니다. 다음 단계에 대한 자세한 내용은 Cisco Security Cloud 제어 사용자 설명서를 참조하십시오.

1. 구독 라이선스를 구매합니다. 구매한 후 회원님 또는 지정된 시스템 관리자가 구독 클레임 코드가 포함된 이메일을 받게 됩니다. 이 이메일을 잃어버리지 마십시오.
2. 구독을 클레임합니다. 위에서 언급한 이메일의 클레임 코드가 필요합니다. 자세한 내용은 "제품 및 구독 관리"를 참조하십시오.
3. 인스턴스를 활성화합니다. 이 "인스턴스"는 Cisco Defense Orchestrator 테넌트에 연결된 멀티 클라우드 방어 어카운트를 나타냅니다. 자세한 내용은 "제품 인스턴스 활성화"를 참조하십시오.

경고! 새 인스턴스 또는 기존 인스턴스를 활성화하라는 메시지가 표시됩니다. 엔터프라이즈에 아직 없는 멀티 클라우드 방어 어카운트에 라이선스를 적용하려면 새 인스턴스 활성화를 선택합니다. 기존 인스턴스에 라이선스 적용 옵션은 Security Cloud 엔터프라이즈에 이미 등록된 멀티 클라우드 방어 인스턴스에 라이선스를 적용합니다.

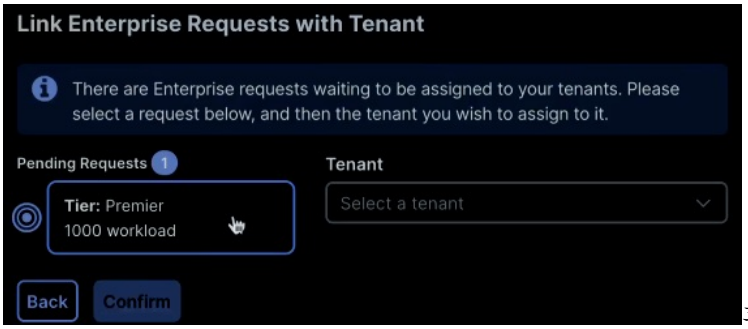
참고 Cisco Defense Orchestrator 테넌트와 아직 멀티 클라우드 방어 어카운트가 연결되어 있지 않은 경우, "멀티 클라우드 방어 라이선스와 연결할 기존 Cisco Defense Orchestrator 어카운트가 있습니까?"라는 메시지가 표시될 때 **No(**아니요**)**를 선택합니다. 이렇게 하면 Cisco Defense Orchestrator 테넌트에 대한 요청이 생성됩니다. 그런 다음 멀티 클라우드 방어를 요청하고 활성화할 수 있습니다. **No(**아니오**)**를 선택한 경우, 4단계를 무시합니다.

4. 활성화를 확인합니다. 이 단계는 Cisco Defense Orchestrator에서 이루어집니다. 활성화 버튼을 클릭하여 활성화를 확인해야 합니다. 이 버튼은 아래



에 설명된 것처럼 대시보드 창 위쪽에 새 배너로 표시됩니다.

참고 활성화를 확인하면 멀티 클라우드 방어 어카운트의 성능 계층을 선택해야 합니다. 제품에 대한 평가판 라이선스와 전체 라이선스 중 어떤 라이선스가 있는지에 따라 표시되는 옵션은 이 스크린샷



과 다를 수 있습니다.

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 어카운트에 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 게이트웨이는 약 3초마다 멀티 클라우드 방어 컨트롤러와 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.

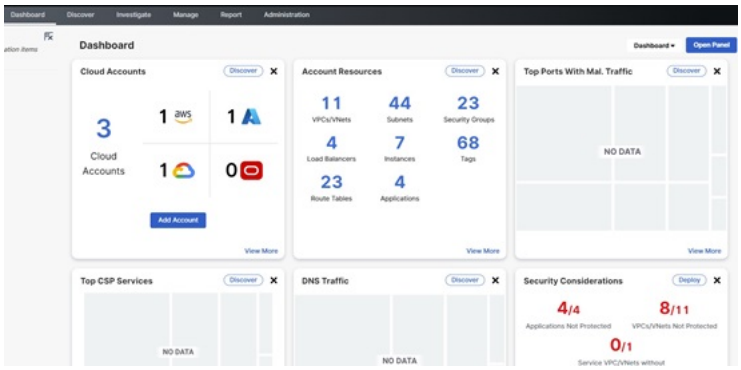
고급 보안 프로파일

멀티 클라우드 방어 게이트웨이는 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.

멀티 클라우드 방어 컨트롤러 대시보드

멀티 클라우드 방어 컨트롤러의 대시보드에는 어카운트, 어카운트 리소스 및 인기 정책 또는 프로파일의 현재 상태에 대한 빠른 스냅샷을 제공하는 다양한 위젯이 있습니다.



다음 위젯을 드래그/드롭하여 필요에 맞게 대시보드를 사용자 맞춤화 및 구성할 수 있습니다. 또한 위젯에서 "x"를 클릭하여 대시보드 보기에서 제거하거나, "View More(자세히 보기)"를 클릭하여 해당 위젯과 관련된 페이지로 바로 이동할 수 있습니다. 각 위젯의 상단에는 멀티 클라우드 방어 위젯이 제공하는 기능(검색, 탐지, 구축 또는 방어)이 표시되어 있습니다.

다음 위젯은 기본적으로 생성됩니다.

클라우드 어카운트

이는 멀티 클라우드 방어 컨트롤러에 연결한 클라우드 어카운트의 수와 클라우드 서비스 제공자의 수에 대한 개괄적인 보기입니다.

이 위젯에서 "Add Account(어카운트 추가)"를 쉽게 클릭하고 연결 마법사를 시작하여 새로운 클라우드 서비스 제공자의 온보딩을 지원할 수 있습니다.

어카운트 리소스

이는 연결된 모든 클라우드 어카운트에 할당된 리소스의 일반 목록입니다. 현재 사용되고 있는 다음 리소스의 수가 표시됩니다.

- VPC/VNets.
- 서브넷.
- 보안 그룹.
- 로드 밸런서.
- 인스턴스.
- 태그.
- 경로 테이블.
- 애플리케이션.

상위 **CSP** 서비스

클라우드 서비스 제공자 서비스의 이 하향식 표시는 이미 멀티 클라우드 방어 컨트롤러에 연결한 클라우드 서비스 제공자의 DNS 트래픽을 일반화합니다.

DNS 트래픽

이 DNS Traffic 위젯은 "Top CSP Services(상위 CSP 서비스)"와 유사하게 트래픽을 적극적으로 처리하고 있는 클라우드 서비스 제공자에 대한 현재 DNS 트래픽의 제한된 보기를 제공합니다. 더 많은 정보를 얻으려면 위젯을 전체 검색 범위로 확장하는 것이 좋습니다.

악성 트래픽의 **VPC/VNet**

이 위젯은 악성 트래픽이 발생한 최근 VPC 또는 VNet을 표시합니다. 이벤트 및 공격의 포괄적인 목록을 보려면 위젯을 확장하고 트래픽을 확인합니다..

악성 트래픽이 있는 상위 포트

이 소규모 스냅샷은 클라우드 어카운트 중에서 악성 트래픽에 대한 적중 수가 가장 많은 포트를 표시합니다.

보안 문제

Security 고려 사항 위젯은 멀티 클라우드 방어에 제공된 수단으로 보호되지 않는 애플리케이션, VPC 또는 VNet 및 연결된 게이트웨이를 요약하는 추천 위젯입니다.

시스템 로그

System Logs(시스템 로그) 창에서는 영향을 미치는 어카운트를 카탈로그화하는 로그, 연결된 게이트웨이, 이벤트 또는 공격의 심각도 등을 제공합니다. 이 위젯을 사용하거나 전체 System Log 페이지를 소중한 리소스로 활용할 것을 적극 권장합니다.

최상위 애플리케이션

이 창에는 사용되는 모든 클라우드 서비스 제공자 중에서 가장 많이 사용되는 애플리케이션이 표시됩니다.

위협

지난 7일간의 트래픽 및 수신 트래픽 중 위협으로 분류된 양을 나타내는 그래프를 확인합니다.

위협별 상위 국가

이 가로 막대 차트는 전체 기간 동안 가장 많은 이벤트를 생성한 상위 10개 국가의 스냅샷을 표시한 다음, 해당 볼륨을 해당 기간 동안 이벤트가 발생한 시간 단위로 세분화하여 표시합니다.

유출 시도

현재 멀티 클라우드 방어에 연결된 클라우드 서비스 제공자에서 발생한 이그레스 데이터 유출의 일반적인 표시를 확인합니다.

프로파일 정보

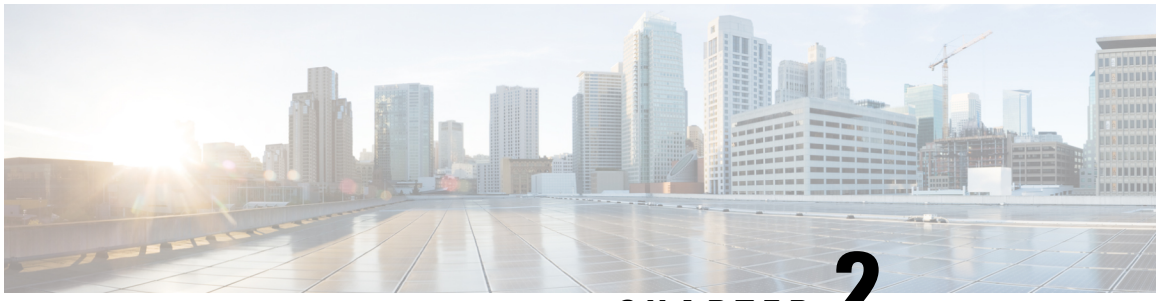
User Profile(사용자 프로파일) 페이지는 사용자 정보를 자세히 설명하는 페이지입니다. 멀티 클라우드 방어 대시보드의 오른쪽 상단에서 **Admin(**관리**)** 화살표를 눌러 이 페이지에 액세스합니다. 다음 정보를 보려면 사용자 이름을 클릭합니다.

- 이름.
- 멀티 클라우드 방어 어카운트와 연결된 이메일 주소.
- 현재 보유한 사용자 역할.
- 현재 로그인한 테넌트 이름.
- 모든 할당된 어카운트

이 페이지는 일반적인 지식을 파악하거나 Cisco 지원팀에 지원이 필요한 경우에 유용하게 활용할 수 있습니다.

II 부

멀티 클라우드 방어 마법사를 사용하여 설정



CHAPTER 2

멀티 클라우드 방어 마법사를 사용하여 설정

멀티 클라우드 방어 컨트롤러에서는 멀티 클라우드 방어를 구축 및 관리할 수 있는 SaaS 제공 중앙 집중식 컨트롤 플레인 및 해당 보안 정책을 제공합니다.

설정은 다음과 같은 일련의 간단한 단계를 통해 멀티 클라우드 방어 보안을 설정하는 프로세스를 사용자에게 안내합니다.

- 어카운트 연결- 이 프로세스에서는 클라우드 서비스 제공자 어카운트를 멀티 클라우드 방어에 온보딩하고 어카운트와 관련된 지역 및 추가 인벤토리 목록 및 자산을 검색합니다.
- 트래픽 가시성 활성화 - 쉬운 설정 방법을 사용하면 로그 수집을 활성화하여 트래픽 흐름을 파악합니다.
- 어카운트 보호 - 이 절차를 수행하면 보유한 클라우드 어카운트에 따라 VNET 또는 VPC를 쉽게 설정하고 멀티 클라우드 방어 게이트웨이로 환경을 보호할 수 있습니다.

- 클라우드 어카운트 연결, on page 13
- 트래픽 가시성 활성화, 20 페이지
- 어카운트 보안, 21 페이지

클라우드 어카운트 연결

첫 번째 단계는 하나 이상의 클라우드 어카운트를 온보딩하는 것입니다. 멀티 클라우드 방어 컨트롤러에서 인벤토리 목록을 검색하고 트래픽 및 로그를 활성화하고 보안 구축을 오케스트레이션하고 정책을 생성 및 관리하여 각 계정과 상호 작용할 수 있습니다.

다음 절차를 사용하여 클라우드 서비스 제공자 계정을 멀티 클라우드 방어 컨트롤러에 연결합니다.

AWS 어카운트 연결

다음 절차에 따라 멀티 클라우드 방어의 쉬운 설정 마법사를 통해 AWS 구독에 연결합니다.

시작하기 전에

- 활성 AWS(Amazon Web Services) 어카운트가 있어야 합니다.

- CDO 테넌트에 관리자 또는 슈퍼 관리자 사용자 역할이 있어야 합니다.
- CDO 테넌트에 대해 멀티 클라우드 방어를 활성화해야 합니다.

참고 멀티 클라우드 방어 컨트롤러 버전 23.10은 멀티 클라우드 방어 게이트웨이 버전 23.04 이상을 사용하는 경우 AWS EC2 인스턴스에서 기본적으로 IMDSv2를 사용합니다. IMDSv1과 IMDSv2의 차이점에 대한 자세한 내용은 AWS 설명서를 참조하십시오.

단계 **1** CDO 대시보드에서 왼쪽 탐색 창에 있는 멀티 클라우드 방어 탭을 클릭합니다.

단계 **2** 오른쪽 상단 창에 있는 멀티 클라우드 방어 컨트롤러을 클릭합니다.

단계 **3** 멀티 클라우드 방어 컨트롤러 대시보드에서 창 왼쪽에 있는 **Setup(**설정**)**을 클릭합니다.

단계 **4** **Connect Account(**어카운트 연결**)**를 선택합니다.

단계 **5** AWS 아이콘을 선택합니다.

단계 **6** 모달에 다음 정보를 입력합니다.

a) **Launch Stack(**스택 실행**)**을 클릭하여 CloudFormation 템플릿을 다운로드하고 구축합니다. 이렇게 하면 템플릿을 구축할 수 있는 다른 탭이 열립니다. AWS에 로그인해야 합니다.

b) CloudFormation 템플릿의 CloudFormation 스택 출력에서 컨트롤러 IAM 역할 ARN을 복사하여 붙여넣습니다.

c) 멀티 클라우드 방어 컨트롤러 쉬운 설정 모달에서 **AWS Account Number(AWS** 계정 번호**)**를 입력합니다. 이 번호는 CloudFormation 템플릿의 출력 값 **Current Account**에서 찾을 수 있습니다.

d) 멀티 클라우드 방어 컨트롤러에 계정에 할당될 **Account Name(**계정 이름**)**을 입력합니다.

e) (선택 사항) 계정 설명을 입력합니다.

f) 외부 **ID**를 입력합니다. IAM 역할의 신뢰 정책에 대한 임의의 문자열입니다. 이 값은 생성된 컨트롤러 IAM 역할에서 사용됩니다. 외부 ID를 편집하거나 다시 생성할 수 있습니다.

g) **Controller IAM Role(**컨트롤러 **IAM** 역할**)**을 입력합니다. 이 역할은 CFT(CloudFormation Template) 구축 중에 멀티 클라우드 방어 컨트롤러에 대해 생성되는 IAM 역할입니다. CFT 스택에서 출력 값 MCDControllerRoleArn을 찾습니다. 다음과 유사해야 합니다: `arn:aws:iam::<Acc Number>:role/ciscomcdcontrollerrole`.

h) **Inventory Monitor Role(**인벤토리 목록 모니터 역할**)**을 입력합니다. 이 역할은 CFT 구축 중에 멀티클라우드 방어 인벤토리 목록에 대해 생성된 IAM 역할입니다. CFT 스택에서 출력 값 MCDInventoryRoleArn을 찾습니다. 다음과 유사해야 합니다: `arn:aws:iam::<Acc Number>:role/ciscomcdinventoryrole`.

단계 **7** **Next(**다음**)**를 클릭합니다. 계정이 멀티 클라우드 방어 컨트롤러에 온보딩됩니다.

다음에 수행할 작업

계정을 연결하면 멀티 클라우드 방어 컨트롤러이(가) 클라우드 서비스 제공자 계정과 연결된 자산 및 인벤토리 목록을 검색하기 시작합니다. 이는 트래픽 검색과는 다릅니다. 멀티 클라우드 방어 컨트롤러은(는) 기본적으로 계정 자산 및 인벤토리 목록을 검색하므로 이 마법사의 다음 단계는 트래픽 가시성 활성화하는 것입니다.

Azure 어카운트 연결

다음 절차에 따라 멀티 클라우드 방어 컨트롤러의 쉬운 설정 마법사를 통해 Azure 구독에 연결합니다.

시작하기 전에

- 활성 Azure 구독이 있어야 합니다.
- CDO 테넌트에 관리자 또는 슈퍼 관리자 사용자 역할이 있어야 합니다.
- CDO 테넌트에 대해 멀티 클라우드 방어을(를) 활성화해야 합니다.

단계 **1** CDO 대시보드에서 왼쪽 탐색 창에 있는 멀티 클라우드 방어 탭을 클릭합니다.

단계 **2** 오른쪽 상단 창에 있는 멀티 클라우드 방어 컨트롤러을 클릭합니다.

단계 **3** 멀티 클라우드 방어 컨트롤러 대시보드에서 창 왼쪽에 있는 **Setup(**설정**)**을 클릭합니다.

단계 **4** **Connect Account(**어카운트 연결**)**를 선택합니다.

단계 **5** Azure 아이콘을 선택합니다.

단계 **6** 모달에 다음 정보를 입력합니다.

a) 링크를 클릭하여 Bash 모드에서 Azure Cloud Shell을 엽니다.
b) Azure 계정 모달에서 **Copy(**복사**)**를 클릭하여 온보딩 스크립트를 복사하고 1단계에서 연 Bash 쉘에서 실행합니다.
c) Azure 계정 모달에서 이 Azure 계정의 이름을 제공합니다. 이 이름은 Azure 구독 이름과 동일하게 지정할 수 있습니다. 이 이름은 멀티 클라우드 방어 컨트롤러 계정 페이지에만 표시됩니다.
d) (선택 사항) 구독에 대한 설명을 제공합니다.
e) 테넌트 ID라고도 하는 디렉터리 **ID**를 입력합니다.
f) 온보딩 중인 구독의 구독 **ID**를 입력합니다.
g) 온보딩 스크립트에서 생성한 애플리케이션 **ID**(클라이언트 ID라고도 함)를 입력합니다.
h) **Client Secret(**클라이언트 암호**)**(암호 ID라고도 함)을 입력합니다.

단계 **7** **Next(**다음**)**를 클릭합니다.

다음에 수행할 작업

계정을 연결하면 멀티 클라우드 방어 컨트롤러이(가) 클라우드 서비스 제공자 계정과 연결된 자산 및 인벤토리 목록을 검색하기 시작합니다. 이는 트래픽 검색과는 다릅니다. 멀티 클라우드 방어 컨트롤러은(는) 기본적으로 계정 자산 및 인벤토리 목록을 검색하므로 이 마법사의 다음 단계는 트래픽 가시성 활성화하는 것입니다.

Google Cloud 플랫폼 어카운트 연결

다음 절차에 따라 멀티 클라우드 방어 컨트롤러의 간편한 설정 마법사를 사용하여 GCP 프로젝트를 계정으로 온보딩합니다.

시작하기 전에

- 액티브 GCP(Google Cloud Platform) 프로젝트가 있어야 합니다.
- GCP 프로젝트 내에서 VPC, 서브넷, 서비스 어카운트를 생성하는 데 필요한 권한이 있어야 합니다. 자세한 내용은 GCP 문서를 참조하십시오.
- CDO 테넌트에 관리자 또는 슈퍼 관리자 사용자 역할이 있어야 합니다.
- CDO 테넌트에 대해 멀티 클라우드 방어을(를) 활성화해야 합니다.

단계 **1** CDO 대시보드에서 왼쪽 탐색 창에 있는 멀티 클라우드 방어 탭을 클릭합니다.

단계 **2** 오른쪽 상단 창에 있는 멀티 클라우드 방어 컨트롤러을 클릭합니다.

단계 **3** 멀티 클라우드 방어 컨트롤러 대시보드에서 창 왼쪽에 있는 **Setup(**설정**)**을 클릭합니다.

단계 **4** **Connect Account(**어카운트 연결**)**를 선택합니다.

단계 **5** GCP 아이콘을 선택합니다.

단계 **6** 모달에 다음 정보를 입력합니다.

a) **Cloud Platform Cloud Shell(**클라우드 플랫폼 클라우드 쉘**)**을 클릭하여 클라우드 쉘을 시작합니다.

b) 멀티 클라우드 방어 컨트롤러 쉬운 설정 모달에서 생성된 명령을 복사하여 클라우드 쉘에 붙여넣습니다. 명령을 실행하여 온보딩 프로세스를 시작합니다. 이 스크립트는 멀티 클라우드 방어 컨트롤러이(가) GCP 프로젝트와 직접 통신할 수 있도록 사용자 계정을 자동으로 생성합니다.

c) 멀티 클라우드 방어 컨트롤러 쉬운 설정 모달에서 계정의 이름을 입력합니다. GCP 프로젝트 이름과 동일하게 이름을 지정할 수 있습니다. 이 이름은 멀티 클라우드 방어 컨트롤러에서만 표시됩니다.

d) (선택 사항) **Description(**설명**)**을 입력합니다.

e) GCP 프로젝트의 프로젝트 **ID**를 입력합니다.

f) 멀티 클라우드 방어 컨트롤러에 대해 생성된 서비스 어카운트의 **Client Email(**클라이언트 이메일**)**을 입력합니다.

g) 서비스 어카운트의 개인 키를 입력합니다.

단계 **7** **Next(**다음**)**를 클릭합니다.

다음에 수행할 작업

계정을 연결하면 멀티 클라우드 방어 컨트롤러이(가) 클라우드 서비스 제공자 계정과 연결된 자산 및 인벤토리 목록을 검색하기 시작합니다. 이는 트래픽 검색과는 다릅니다. 멀티 클라우드 방어 컨트롤러은(는) 기본적으로 계정 자산 및 인벤토리 목록을 검색하므로 이 마법사의 다음 단계는 트래픽 가시성 활성화하는 것입니다.

OCI 연결

OCI(Oracle Cloud) 계정을 온보딩하기 전에 다음 사전 요건을 실행해야 합니다.

OCI에 로그인

1. OCI 테넌트에 로그인합니다.

그룹 생성

단계 **1** **Identity & Security(ID** 및 보안**)** > **Groups(**그룹**)**로 이동합니다.
단계 **2** **Create Group(**그룹 생성**)**을 클릭합니다.
단계 **3** 다음 항목을 지정합니다.

- **Name(**이름**):** 멀티 클라우드 방어-controller-group
- **Description(**설명**):** 멀티 클라우드 방어 그룹

단계 **4** **Create(**생성**)**를 클릭합니다.

정책 생성

멀티 클라우드 방어로 OCI 어카운트를 생성하는 경우 방화벽 정책을 생성하고 적용해야 합니다. 다음 절차와 권장 사항에 따라 정책을 생성합니다.

단계 **1** **Identity & Security(ID** 및 보안**)** > **Policies(**정책**)**로 이동합니다.
단계 **2** **Compartment(**컴파트먼트**)** *root(*루트*)*를 선택합니다.
단계 **3** **Create Policy(**정책 생성**)**를 클릭합니다.
단계 **4** 다음 항목을 지정합니다.

- **Name(**이름**):** 멀티 클라우드 방어-controller-policy.
- **Description(**설명**):** 멀티 클라우드 방어 정책.
- **Compartment(**컴파트먼트**):** ["root" 컴파트먼트여야 함].

단계 **5** **Policy Builder(**정책 빌더**)**에서 **Show manual Editor(**수동 편집기 표시**)**를 활성화합니다.
단계 **6** 다음 정책 수정 및 붙여넣기

```
Allow group <group_name> to inspect instance-images in compartment <compartment_name>
Allow group <group_name> to read app-catalog-listing in compartment <compartment_name>
Allow group <group_name> to use volume-family in compartment <compartment_name>
Allow group <group_name> to use virtual-network-family in compartment <compartment_name>
Allow group <group_name> to manage volume-attachments in compartment <compartment_name>
Allow group <group_name> to manage instances in compartment <compartment_name>
```

```
Allow group <group_name> to {INSTANCE_IMAGE_READ} in compartment <compartment_name>
Allow group <group_name> to manage load-balancers in compartment <compartment_name>
Allow group <group_name> to read marketplace-listings in tenancy
Allow group <group_name> to read marketplace-community-listings in tenancy
Allow group <group_name> to inspect compartments in tenancy
Allow group <group_name> to manage app-catalog-listing in compartment <compartment_name>
Allow group <group_name> to read virtual-network-family in tenancy
Allow group <group_name> to read instance-family in tenancy
Allow group <group_name> to read load-balancers in tenancy
```

- **group_name:** 멀티 클라우드 방어-controller-group.
- **compartment_name:**[멀티 클라우드 방어이(가) 구축될 컴파트먼트].

Note Cisco IOS 시스템을 교체할 때 **<compartment_name>**을 정책을 적용할 구역의 이름으로 바꿉니다. 구역이 하위 구역인 경우, 이름 형식은 **compliance:sub-compartment**(예: Prod:App1)입니다.

<compartment_name>이 루트 컴파트먼트(예: multicloud (root))로 지정된 경우 OCI는 정책을 수락하지 않고 오류: *Invalid parameter(*잘못된 매개변수*)*가 생성됩니다. 특정 컴파트먼트에 대해 정책을 정의해야 하며 해당 컴파트먼트는 루트 컴파트먼트일 수 없습니다.

단계 **7** **Create(**생성**)**를 클릭합니다.

사용자 생성

단계 **1** **Identity & Security(ID** 및 보안**)** > **Users(**사용자**)**로 이동합니다.
단계 **2** **Create User**(사용자 생성)를 클릭합니다.
단계 **3** 다음 항목을 지정합니다.

- **Name(**이름**):** 멀티 클라우드 방어*-controller-user*
- **Description(**설명**):** 멀티 클라우드 방어 *User(*사용자*)*

단계 **4** **Create(**생성**)**를 클릭합니다.

API 키 생성

단계 **1** 사용자에 대한 **User Details(**사용자 세부 정보**)** 보기에서 **API Keys(API** 키**)**를 선택합니다.
단계 **2** **Add API Key(API** 키 추가**)**를 클릭합니다.
단계 **3** **Download Private Key(**개인 키 다운로드**)**를 선택하고 나중에 사용할 수 있도록 개인 키를 보관합니다.
단계 **4** **Download Public Key(**공개 키 다운로드**)**를 선택하고 나중에 사용할 수 있도록 공개 키를 보관합니다.
단계 **5** **Add(**추가**)**를 클릭합니다.

약관 동의

다음 절차에 따라 OCI 어카운트의 이용 약관에 동의합니다.

단계 **1** **Compute**(계산) > **Instance**(인스턴스)를 선택합니다.
단계 **2** 원하는 **Compartment**(컴파트먼트)를 선택합니다.
단계 **3** **Create instance**(인스턴스 생성)를 클릭합니다.
단계 **4** **Image and shape**(이미지 및 모양)에서 **Change image**(이미지 변경)를 선택합니다.
단계 **5** **Image source**(이미지 소스)에서 **Community Images**(커뮤니티 이미지)를 선택합니다.
단계 **6** 멀티 클라우드 방어 검색을 수행합니다.
단계 **7** 멀티 클라우드 방어에 대한 확인란을 선택합니다.
단계 **8** *I have reviewed and accept the Publishers terms of use, Oracle Terms of Use, and the Oracle General Privacy Policy*(본인은 게시자 이용 약관, 오라클 이용 약관 및 오라클 일반 개인정보 취급방침을 검토하고 이에 동의합니다.)에 대한 상자를 선택합니다.
단계 **9** **Select Image**(이미지 선택)를 클릭합니다.
단계 **10** 종료합니다(이미지를 구축하지 않음).

멀티 클라우드 방어 게이트웨이을(를) 구축하려는 각 컴파트먼트에 대해 단계를 반복합니다.

Oracle 어카운트 연결

다음 절차에 따라 멀티 클라우드 방어 컨트롤러의 쉬운 설정 마법사를 통해 OCI 어카운트에 연결합니다.

시작하기 전에

- 기존 OCI(Oracle Cloud) 계정이 있어야 합니다.
- 온보딩 전에 OCI 계정에 대한 사전 요구 사항을 완료해야 합니다. 자세한 내용은 OCI 연결, 17 페이지를 참조하십시오.
- CDO 테넌트가 있어야 합니다.
- CDO 테넌트에 관리자 또는 슈퍼 관리자 사용자 역할이 있어야 합니다.
- CDO 테넌트에 대해 멀티 클라우드 방어을(를) 활성화해야 합니다.

단계 **1** CDO 대시보드에서 왼쪽 탐색 창에 있는 멀티 클라우드 방어 탭을 클릭합니다.
단계 **2** 오른쪽 상단 창에 있는 멀티 클라우드 방어 컨트롤러을 클릭합니다.
단계 **3** 멀티 클라우드 방어 컨트롤러 대시보드에서 창 왼쪽에 있는 **Setup**(설정)을 클릭합니다.
단계 **4** **Connect Account**(어카운트 연결)를 선택합니다.
단계 **5** OCI 아이콘을 선택합니다.

단계 **6** 모달에 다음 정보를 입력합니다.

a) **OCI Account Name(OCI** 계정 이름**)**을 입력합니다. 이 이름은 멀티 클라우드 방어 컨트롤러에서만 사용되며 식별 목적으로만 사용됩니다.
b) (선택 사항) 계정 설명을 입력합니다.
c) **Tenancy OCID(**테넌시 **OCID)**를 입력합니다. 이는 OCI 사용자로부터 가져온 테넌시 Oracle Cloud 식별자입니다.
d) OCI 사용자에게 할당된 개인 키를 입력합니다.

단계 **7** **Next(**다음**)**를 클릭합니다.

다음에 수행할 작업

계정을 연결하면 멀티 클라우드 방어 컨트롤러이(가) 클라우드 서비스 제공자 계정과 연결된 자산 및 인벤토리 목록을 검색하기 시작합니다. 이는 트래픽 검색과는 다릅니다. 멀티 클라우드 방어 컨트롤러은(는) 기본적으로 계정 자산 및 인벤토리 목록을 검색하므로 이 마법사의 다음 단계는 트래픽 가시성 활성화하는 것입니다.

트래픽 가시성 활성화

트래픽 가시성을 활성화하면 다음 로그를 수집하여 클라우드 어카운트 내의 트래픽 플로우를 확인할 수 있습니다.

- NSG 플로우 로그
- (**AWS**만 해당) VPC 플로우 로그
- DNS 로그
- Route53 쿼리 로깅

흐름 및 DNS 쿼리 로그는 멀티 클라우드 방어에서는 트래픽 흐름을 파악하고, 위협 인텔리전스 피드와 상호 연결하고, 멀티 클라우드 방어을(를) 사용하여 보호할 수 있는 기존 위협에 대한 통찰력을 제공하는 데 사용됩니다.

트래픽 가시성을 활성화하는 것은 클라우드 어카운트 유형마다 다른 프로세스이지만, 일반적으로 클라우드 어카운트의 지역, 모니터링할 VPC/VNet, 네트워크 보안 그룹 및 로그용 클라우드 스토리지 어카운트과 같은 어카운트 특성을 식별해야 합니다.

설정 마법사에서 트래픽 가시성을 활성화하려면 다음 절차를 사용합니다.

시작하기 전에

이미 하나 이상의 클라우드 서비스 제공자 계정을 멀티 클라우드 방어 컨트롤러에 연결해야 합니다.

단계 **1** 멀티 클라우드 방어 컨트롤러 포털의 왼쪽 내비게이션 바에서 **Setup(**설정**)**을 클릭합니다.

단계 **2** 설정 마법사에서 **Enable Traffic Visibility(**트래픽 가시성 활성화**)**를 클릭합니다.

단계 **3** **CSP Account(CSP** 계정**)** - 드롭다운 메뉴를 사용하여 멀티 클라우드 방어 컨트롤러이(가) 서비스 VPC/VNet을 구축할 클라우드 서비스 제공자 계정을 선택합니다.

단계 **4** **Region(**지역**)** - 드롭다운 메뉴를 사용하여 선택한 클라우드 서비스 제공자가 위치한 지역을 선택합니다.

단계 **5** 선택한 클라우드 서비스 제공자 유형에 적용 가능한 사용 가능한 VPC 테이블을 스크롤하여 적절한 VPC를 선택합니다. VPC가 즉시 표시되지 않는 경우 **Refresh(**새로 고침**)** 아이콘을 클릭하여 현재 목록을 새로 고칩니다.

단계 **6** (선택 사항) 드롭다운 메뉴를 사용하여 계정에서 DNS 쿼리 및 VPC 흐름 로그가 저장되는 S3 버킷을 선택합니다. 선택한 S3 버킷은 트래픽을 활성화할 때 프로세스의 일부로 멀티 클라우드 방어에 의해 생성됩니다.

단계 **7** **Next(**다음**)**를 클릭합니다.

다음에 수행할 작업

어카운트를 보호합니다.

어카운트 보안

중앙 집중식 또는 분산형 모델에 구축된 게이트웨이로 계정을 보호합니다.

중앙 집중식 모델에서는 멀티 클라우드 방어가 게이트웨이를 포함하기 위해 VPC 또는 VNet을 오케스트레이션하고 구축합니다. 즉, VPC 또는 VNet 및 필요한 모든 추가 구성 요소는 이 구문 내에서 게이트웨이의 구축과 함께 오케스트레이션됩니다.

분산형 모델에서 멀티 클라우드 방어는 네트워크에서 이미 사용 가능한 기존 인프라 내에서 게이트웨이를 빌드하고 구축합니다.

어카운트를 보호하려면 아래 절차 중 하나를 계속 진행합니다.

중앙 집중식 모델: **VPC** 또는 **VNet** 추가

다음 절차에 따라 게이트웨이를 수용하고 계정을 보호할 VPC 또는 VNet을 만들고 추가합니다.

시작하기 전에

이 마법사를 시작하기 전에 하나 이상의 클라우드 서비스 제공자가 멀티 클라우드 방어 컨트롤러에 연결되어 있어야 합니다. 일부 사업자의 경우, 이 절차는 필수 매개변수에 따라 변경됩니다.

단계 **1** 멀티 클라우드 방어 컨트롤러 포털의 왼쪽 내비게이션 바에서 **Setup(**설정**)**을 클릭합니다.

단계 **2** 설정 마법사에서 **Secure Account(**어카운트 보안**)**를 클릭합니다.

단계 **3** **Centralized(**중앙 집중식**)**를 선택하면 강조 표시됩니다.

단계 **4** **Next(**다음**)**를 클릭합니다.

단계 **5** 서비스 VPC/VNet 추가:

a) **Name(**이름**)** - 서비스 VPC/VNet의 이름을 입력합니다. 생성되면 이 이름이 **Manage(**관리**)** > **Gateways(**게이트웨이**)** > **Service VPC/VNETS(**서비스 **VPC/VNETS)** 페이지에 표시됩니다.

b) **CSP Account(CSP** 계정**)** - 드롭다운 메뉴를 사용하여 멀티 클라우드 방어 컨트롤러에 이미 연결된 클라우드 서비스 제공자 계정을 선택합니다. 서비스 VPC/VNet이 선택한 계정에 구축됩니다.
c) **Region(**지역**)** - 드롭다운 메뉴를 사용하여 선택한 클라우드 서비스 제공자가 있는 지역을 선택합니다.
d) **CIDR Block(CIDR** 차단**)** - 서비스 VPC/VNet이 연결되는 Transit Gateway의 고유한 값을 입력합니다.
e) **Availablity Zones(**가용성 영역**)** - 생성된 목록에서 가용성 영역을 하나 이상 선택합니다. 최상의 결과를 얻으려면 영역 2개를 선택하는 것이 좋습니다.
f) (Azure 계정만 해당) **Resource Group(**리소스 그룹**)** - 드롭다운 메뉴를 사용하여 게이트웨이를 연결할 리소스 그룹을 선택합니다. 현재 나열되지 않은 경우 이 화면에서 **Create Resource Group(**리소스 그룹 생성**)**을 수행할 수 있습니다.
g) (AWS 계정만 해당) **Transit Gateway(Transit Gateway)** - 드롭다운 메뉴를 사용하여 VPC에 연결할 사용 가능한 Transit Gateway를 선택합니다. 없는 경우 **create_new**를 클릭하여 이 창에서 Transit Gateway를 생성합니다.
h) (AWS 어카운트에만 해당) **Use NAT Gateway(NAT** 게이트웨이 사용**)** - 모든 이그레스 트래픽이 NAT 게이트웨이를 통과하도록 하려면 이 옵션을 선택합니다. 멀티 클라우드 방어에서는 선택된 각 가용성 영역에 대해 NAT 게이트웨이를 자동으로 생성합니다.

단계 **6** **Next(**다음**)**를 클릭합니다.

다음에 수행할 작업

게이트웨이를 추가합니다.

분산형 모델

분산형 게이트웨이 모델의 경우 사용 중인 클라우드 서비스 제공자에 따라 다음 절차를 사용합니다.

Azure 분산형 모델**:** 게이트웨이 생성

다음 절차를 사용하여 분산형 모델로 Azure 계정용 게이트웨이를 생성합니다.

단계 **1** 멀티 클라우드 방어 컨트롤러 포털의 왼쪽 내비게이션 바에서 **Setup(**설정**)**을 클릭합니다.
단계 **2** 설정 마법사에서 **Secure Account(**어카운트 보안**)**를 클릭합니다.
단계 **3** **Distributed(**분산됨**)**를 선택하면 강조 표시됩니다.
단계 **4** **Next(**다음**)**를 클릭합니다.
단계 **5** 다음 게이트웨이 정보를 입력합니다.
a) **Account(**계정**)** - 드롭다운 메뉴를 사용하여 게이트웨이를 구축할 Azure 계정을 선택합니다.
b) **Name(**이름**)** - 게이트웨이 이름을 입력합니다. 이 이름은 **Manage(**관리**)** > **Gateways(**게이트웨이**)** 페이지에 표시됩니다.
c) (선택 사항) **Description(**설명**)** - 다른 게이트웨이와 구별하는 게이트웨이의 설명을 입력합니다.
d) **Instance Type(**인스턴스 유형**)** - 드롭다운 메뉴를 사용하여 게이트웨이를 구축하는 인스턴스 유형을 선택합니다.
e) **Minimum Instances(**최소 인스턴스**)** - 가용성 영역당 자동 확장 그룹에 구축되는 최소 인스턴스 수를 선택합니다.

f) **Maximum Instance(**최대 인스턴스**)** - 가용성 영역당 자동 확장 그룹에 구축되는 최대 인스턴스 수를 선택합니다.

g) **HealthCheck Port(**상태 확인 포트**)** - 상태 확인 포트 번호를 입력합니다. 멀티 클라우드 방어 컨트롤러에서는 기본값으로 `65534`를 사용합니다.

h) **User Name(**사용자 이름**)** - 생성된 게이트웨이에 액세스하는 데 사용되는 사용자 이름을 입력합니다.

i) **Packet Capture Profile(**패킷 캡처 프로파일**)** - 드롭다운 메뉴를 사용하여 클라우드 스토리지 버킷에서 패킷이 저장되는 위치를 선택합니다. 옵션이 나열되지 않는 경우 **Create Packet Capture Profile(**패킷 캡처 프로파일 생성**)**을 클릭하여 이 창에서 하나를 생성합니다.

j) **Log Profile(**로그 프로파일**)** - 드롭다운 메뉴를 사용하여 어떤 클라우드 서비스 제공자에 로깅을 전달할지 선택합니다.

k) **Metrics Profile(**메트릭 프로파일**)** - 드롭다운 메뉴를 사용하여 메트릭을 전달할 엔터티를 선택합니다. 옵션이 나열되지 않는 경우 **Create Metrics Forward Profile(**메트릭 전달 프로파일 생성**)**을 클릭하여 이 창에서 생성합니다.

l) **NTP Profile(NTP** 프로파일**)** - 드롭다운 메뉴를 사용하여 게이트웨이와 연결된 NTP 프로파일을 선택합니다. 옵션이 나열되지 않으면 **Create(**생성**)**를 클릭하여 이 창에서 옵션을 생성합니다.

m) **Security(**보안**)** - 게이트웨이가 처리해야 하는 트래픽 플로우의 유형을 선택합니다. 인그레스 보안은 공용 인터넷에서 프라이빗 네트워크로 이동하는 트래픽을 대상으로 합니다. 이스트-웨스트 및 이그레스 보안은 프라이빗 네트워크에서 아웃바운드하는 트래픽과 데이터 센터 간에 이동하는 트래픽을 대상으로 합니다.

n) **Gateway Image(**게이트웨이 이미지**)** - 드롭다운 메뉴를 사용하여 게이트웨이에 구축할 게이트웨이 이미지를 선택합니다.

o) **Policy Ruleset(**정책 규칙 집합**)** - 드롭다운 메뉴를 사용하여 구축할 정책 규칙 집합을 선택하고 트래픽 처리를 시작합니다. 규칙 집합이 목록에 없으면 **Create new(**새로 만들기**)**를 클릭하여 이 창에서 정책 규칙 집합을 생성합니다.

p) **Region(**지역**)** - 드롭다운 메뉴를 사용하여 게이트웨이가 구축된 지역을 선택합니다.

q) **VPC/VNet ID** - 드롭다운 메뉴를 사용하여 게이트웨이가 구축된 VPC를 선택합니다.

r) **Key Selection(**키 선택**)** - SSH 공개 키 또는 SSH 키 쌍을 선택합니다. 게이트웨이에 적용할 값을 다음 텍스트 필드에 입력합니다.

s) **Resource Group(**리소스 그룹**)** - 드롭다운 메뉴를 사용하여 게이트웨이에 적용되는 기존 리소스 그룹을 선택합니다.

t) **User Assigned Identity ID(**사용자 할당 **ID)** - 유효한 값을 입력합니다.

u) **Mgmt. Security Group(**관리 보안 그룹**)** - 드롭다운 메뉴를 사용하여 게이트웨이 관리 인터페이스에 사용되는 보안 그룹을 선택합니다. 멀티 클라우드 방어에서 생성된 서비스 VPC를 선택할 경우 관리용으로 보안 그룹이 특별히 생성됩니다.

v) **Datapath Security Group(**데이터 경로 보안 그룹**)** - 드롭다운 메뉴를 사용하여 게이트웨이 데이터 경로 인터페이스에 사용되는 보안 그룹을 선택합니다. 멀티 클라우드 방어에서 생성한 서비스 VPC를 선택할 경우 해당 데이터 경로에 특별히 보안 그룹이 생성됩니다.

w) **Disk Encryption(**디스크 암호화**)** - Azure 관리 암호화 또는 고객 관리 암호화 키를 사용하여 디스크 암호화를 활성화합니다. 고객 관리 암호화 키를 선택하는 경우 성공적인 구축을 위해 IAM 정책을 생성하고 구축해야 합니다.

x) **Availability Zone(**가용성 영역**)** - 드롭다운 메뉴를 사용하여 가용성 영역을 선택합니다.

y) **Mgmt. Subnet(**관리 서브넷**)** - 드롭다운 메뉴를 사용하여 관리 인터페이스의 관리 서브넷을 선택합니다.

z) **Datapth Subnet(**데이터 경로 서브넷**)** - 드롭다운 메뉴를 사용하여 데이터 경로 인터페이스의 서브넷을 선택합니다.

인스턴스 유형을 더 추가하려면 "+" 아이콘을 클릭합니다. 이어서 "-" 아이콘을 사용하여 추가 인스턴스 유형을 제거할 수 있습니다.

단계 **6** **Next(**다음**)**를 클릭합니다.

단계 **7** 다음 고급 설정을 입력합니다.

a)

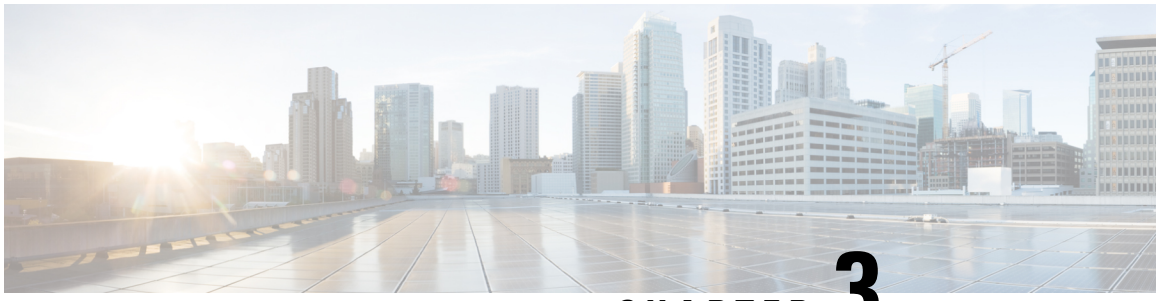
단계 **8** **Next(**다음**)**를 클릭합니다.

단계 **9** 검토

다음에 수행할 작업

III 부

어카운트 온보딩



CHAPTER 3

AWS

AWS 개요

멀티 클라우드 방어에서 AWS 계정을 멀티 클라우드 방어 컨트롤러에 연결할 때 사용하는 CloudFormation 템플릿을 만들었습니다.

멀티 클라우드 방어 컨트롤러과의 통합을 위한 클라우드 어카운트를 준비하려면 클라우드 어카운트에서 수행해야 하는 특정 단계가 있습니다. 다음은 AWS 클라우드 어카운트를 멀티 클라우드 방어 컨트롤러에 연결하기 전에 수행해야 하는 사전 요건 단계입니다. 이는 작업의 개요를 제공하기 위한 것이며 수동으로 수행할 수 없습니다. CloudFormation 섹션에 구축 세부 정보 및 매개변수 정보가 있습니다.

단계 개요

1. 멀티 클라우드 방어 컨트롤러에서 사용하는 교차 어카운트 IAM 역할을 생성하여 클라우드 어카운트를 관리합니다.
2. 계정에서 실행되는 멀티 클라우드 방어 게이트웨이 EC2 인스턴스에 할당될 IAM 역할을 생성합니다.
3. 관리 이벤트를 멀티 클라우드 방어 컨트롤러로 전송하는 CloudWatch 이벤트 규칙을 생성합니다.
4. 관리 이벤트 전송을 수행할 권한을 제공하는 위의 CloudWatch 이벤트 규칙에서 사용하는 IAM 역할을 생성합니다.
5. 필요에 따라 계정에 S3 버킷을 생성하여 CloudTrail 이벤트, Route53 DNS 쿼리 로그 및 VPC 플로우 로그를 저장할 수 있습니다.
6. 대상을 위에서 생성한 S3 버킷으로 하여 Route53 DNS 쿼리 로깅을 활성화하고 쿼리 로깅을 활성화해야 하는 VPC를 선택합니다.
7. CloudTrail을 활성화하여 모든 관리 이벤트를 위에서 생성한 S3 버킷에 로깅합니다.

8. 위에서 생성한 대상이 S3 버킷인 VPC 플로우 로그를 활성화합니다.

멀티 클라우드 방어 대시보드에서 멀티 클라우드 방어 컨트롤러에 **AWS** 계정을 연결합니다.

멀티 클라우드 방어이(가) AWS 계정을 멀티 클라우드 방어 컨트롤러에 쉽게 연결할 수 있는 CloudFormation 템플릿을 생성했습니다.

Before you begin

시작하기 전에 CDO 테넌트에 대해 멀티 클라우드 방어 컨트롤러를 요청해야 합니다.

Note 멀티 클라우드 방어 컨트롤러 버전 23.10은 멀티 클라우드 방어 게이트웨이 버전 23.04 이상을 사용하는 경우 AWS EC2 인스턴스에서 기본적으로 IMDSv2를 사용합니다. IMDSv1과 IMDSv2의 차이점에 대한 자세한 내용은 AWS 설명서를 참조하십시오.

단계 **1** CDO 메뉴 바에서 멀티 클라우드 방어을(를) 클릭합니다.

단계 **2** 멀티 클라우드 방어 컨트롤러 버튼을 클릭합니다.

단계 **3** Cloud Accounts(클라우드 어카운트) 창에서 **Add Account(**어카운트 추가**)**를 클릭합니다.

단계 **4** **General Information(**일반 정보**)** 페이지에 있는 **Account Type(**계정 유형**)** 목록 상자에서 AWS를 선택합니다.

단계 **5** **Launch Stack(**스택 실행**)**을 클릭하여 CloudFormation 템플릿을 다운로드하고 구축합니다. 이렇게 하면 템플릿을 구축할 수 있는 다른 탭이 열립니다. AWS에 로그인해야 합니다.

단계 **6** AWS CloudFormation이 맞춤형 이름으로 IAM 리소스를 생성할 수 있음을 확인합니다.

단계 **7** 다음 값을 입력합니다.

- **AWS Account Number(AWS** 계정 번호**)**: 보호하려는 계정의 AWS 계정 번호를 입력합니다. 이 번호는 CloudFormation 템플릿의 출력 값 CurrentAccount에서 찾을 수 있습니다.
- **Account Name(**계정 이름**)**: 온보딩된 계정에 지정할 이름을 입력합니다.
- **Description(**설명**):**(선택 사항) 계정 설명을 입력합니다.
- **External ID(**외부 **ID)**: IAM 역할의 신뢰 정책에 대한 임의 문자열입니다. 이 값은 생성된 컨트롤러 IAM 역할에서 사용됩니다. 외부 ID를 편집하거나 다시 생성할 수 있습니다.
- **Controller IAM Role(**컨트롤러 **IAM** 역할**)**: 이 역할은 CFT(CloudFormation Template) 구축 중에 멀티 클라우드 방어 컨트롤러에 대해 생성되는 IAM 역할입니다. CFT 스택에서 출력 값 MCDControllerRoleArn을 찾습니다. 다음과 유사해야 합니다: `arn:aws:iam::<Acc Number>:role/ciscomcdcontrollerrole`.
- **Inventory Monitor Role(**인벤토리 목록 모니터 역할**)**: 이 역할은 CFT 구축 중에 멀티클라우드 방어 인벤토리 목록에 대해 생성된 IAM 역할입니다. CFT 스택에서 출력 값 MCDInventoryRoleArn을 찾습니다. 다음과 유사해야 합니다: `arn:aws:iam::<Acc Number>:role/ciscomcdinventoryrole`.

단계 **8** **Save and Continue(**저장 후 계속 진행**)**를 클릭합니다.
새 AWS 클라우드 어카운트가 기록되었음을 확인할 수 있는 멀티 클라우드 방어 대시보드로 돌아갑니다.

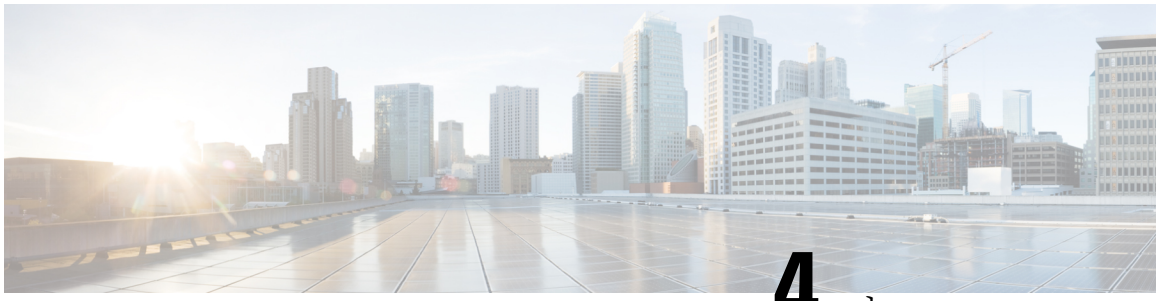
What to do next

트래픽 가시성을 활성화합니다.

CloudFormation 출력

Outputs(출력**)** 탭에서 다음 정보를 복사하고 텍스트 편집기에 붙여넣습니다.

- CurrentAccount(애플리케이션이 실행되고 멀티 클라우드 방어 게이트웨이이 구축될 AWS 계정 ID)
  - MCDControllerRoleArn
  - MCDGatewayRoleName
  - MCDInventoryRoleArn
  - MCDS3BucketArn
  - MCDBucketName



4 장

Azure

Azure 개요

Azure 환경을 준비하고 다음 단계에 따라 멀티 클라우드 방어 컨트롤러에 연결합니다.

- Azure 구독을 획득합니다. 구독이 Azure Active Directory에 연결되었는지 확인합니다.
- 멀티 클라우드 방어 대시보드에서 멀티 클라우드 방어 컨트롤러에 Azure 구독 연결, on page 31

자동화된 스크립트를 사용할 수 없는 경우 Azure 구독 수동 온보딩에서 수동으로 어카운트를 온보딩하는 대체 절차를 참조하십시오.

멀티 클라우드 방어 대시보드에서 멀티 클라우드 방어 컨트롤러에 Azure 구독 연결

이전 섹션에서 설명한 대로 Azure 계정 및 구독을 준비했으면 멀티 클라우드 방어 컨트롤러에 연결할 수 있습니다.

단계 **1** CDO 메뉴 바에서 멀티 클라우드 방어을(를) 클릭합니다.

단계 **2** 멀티 클라우드 방어 컨트롤러 버튼을 클릭합니다.

단계 **3** Cloud Accounts(클라우드 어카운트) 창에서 **Add Account(**어카운트 추가**)**를 클릭합니다.

단계 **4** General Information(일반 정보) 페이지에 있는 **Account Type(**계정 유형**)** 목록 상자에서 Azure를 선택합니다.

단계 **5** 1단계에서 링크를 클릭하여 Bash 모드에서 Azure Cloud Shell을 엽니다.

단계 **6** 2단계에서 **Copy(**복사**)** 버튼을 클릭합니다.

단계 **7** Bash 셸에서 온보딩 스크립트를 실행합니다.

Note

- 멀티 클라우드 방어에 이미 연결된 다른 Azure 구독이 있는 경우 동일한 기존 이름으로 IAM 역할을 생성하면 이 스크립트가 실패할 수 있습니다. IAM 역할은 둘 이상 있을 수 없습니다. 이 문제를 해결하려면 `-p` 접두사를 사용하여 Bash 스크립트를 실행합니다.
- 구독 전반에서 스포크 VNet 보호를 지원하려면 Active Directory 앱 등록을 사용하여 구독을 온보딩해야 합니다.

단계 **8** 이 Azure 계정의 이름을 제공합니다. 이 이름은 Azure 구독 이름과 동일하게 지정할 수 있습니다. 이 이름은 멀티 클라우드 방어 컨트롤러 계정 페이지에만 표시됩니다.

단계 **9** (선택 사항) 구독에 대한 설명을 제공합니다.

단계 **10** 테넌트 ID라고도 하는 디렉터리 **ID**를 입력합니다.

단계 **11** 온보딩 중인 구독의 구독 **ID**를 입력합니다.

단계 **12** 온보딩 스크립트에서 생성한 애플리케이션 **ID**(클라이언트 ID라고도 함)를 입력합니다.

단계 **13** **Client Secret(**클라이언트 암호**)**(암호 ID라고도 함)을 입력합니다.

단계 **14** **Save & Continue(**저장 후 계속**)**를 클릭합니다.

Azure 구독이 온보딩되고 새 디바이스가 추가된 것을 확인하기 위해 대시보드로 다시 연결되었습니다.

What to do next

- 사후 온보딩 절차, on page 32.
- 트래픽 가시성을 활성화합니다.

사후 온보딩 절차

서브넷

게이트웨이 구축을 구성할 때 멀티 클라우드 방어 컨트롤러에서 관리 및 데이터 경로서브넷 정보를 입력하라는 메시지가 표시됩니다.

관리 서브넷은 인터넷에 대한 기본 경로가 있는 라우트 테이블과 연결해야 하는 퍼블릭 서브넷입니다. 멀티 클라우드 방어 게이트웨이 인스턴스에 멀티 클라우드 방어 컨트롤러과(와)의 통신에 사용하는 이 서브넷에 연결된 인터페이스가 있습니다. 이 인터페이스는 멀티 클라우드 방어 컨트롤러 및 멀티 클라우드 방어 게이트웨이 인스턴스 간의 정책 푸시와 기타 관리, 텔레메트리 활동에 사용됩니다. 고객 애플리케이션 트래픽은 이 인터페이스 및 서브넷을 통과하지 않습니다. 아래의 보안 그룹 섹션에서 설명하는 관리 보안 그룹과 인터페이스가 연결됩니다.

데이터 경로 서브넷은 인터넷에 대한 기본 경로가 있는 라우트 테이블과 연결해야 하는 퍼블릭 서브넷입니다. 멀티 클라우드 방어 컨트롤러는 이 서브넷에 네트워크 로드 밸런서(NLB)를 생성합니다. 또한, 멀티 클라우드 방어 게이트웨이 인스턴스에 이 서브넷에 연결된 인터페이스가 있습니다. 고객 애플리케이션 트래픽은 이 인터페이스를 통해 흐릅니다. 이 인터페이스를 통해 인그레스하는 트래

픽에 보안 정책이 적용됩니다. 인터페이스는 보안 그룹 섹션에서 설명하는 데이터 경로 보안 그룹과 연결됩니다.

Azure VNet 설정

이 문서에서는 VNet에서 멀티 클라우드 방어 게이트웨이을(를) 생성할 수 있도록 VNet에서 생성해야 하는 요구 사항 및 리소스(서브넷, 보안 그룹)에 대해 설명합니다.

보안 그룹

관리 및 데이터 경로 보안 그룹은 위의 서브넷 섹션에서 설명한 대로 멀티 클라우드 방어 게이트웨이 인스턴스의 각 인터페이스와 연결됩니다.

관리 보안 그룹은 게이트웨이 인스턴스가 컨트롤러와 통신하도록 허용하는 아웃바운드 트래픽을 허용해야 합니다. 선택적으로, 인바운드 규칙의 경우 포트 22(SSH)를 활성화하여 게이트웨이 인스턴스에 대한 SSH 액세스를 허용합니다. 멀티 클라우드 방어 게이트웨이가 제대로 작동하기 위해 SSH가 반드시 필요한 것은 아닙니다.

데이터 경로 보안 그룹은 데이터 경로 인터페이스에 연결되며 인터넷에서 멀티 클라우드 방어 게이트웨이로의 트래픽을 허용합니다. 현재 멀티 클라우드 방어 컨트롤러는 보안 그룹을 관리하지 않습니다. 이 인터페이스의 트래픽 이그레스를 허용하는 아웃바운드 규칙이 있어야 합니다. 인바운드 포트는 멀티 클라우드 방어 컨트롤러 보안 정책에 구성되어 있고 멀티 클라우드 방어 게이트웨이에서 사용하는 각 포트에 대해 열려 있어야 합니다.

예를 들어 애플리케이션이 포트 3000에서 실행 중이고 포트 443의 멀티 클라우드 방어 게이트웨이에서 프록시되는 경우, 데이터 경로 보안 그룹에서 포트 443을 열어야 합니다. 또한 이 예시는 애플리케이션에 연결된 보안 그룹에서 포트 3000이 열려 있음을 의미합니다.

ARM 템플릿 실행

ARM 템플릿을 사용하여 이 페이지에 설명된 모든 리소스를 생성합니다.

이 템플릿은 새 VNet을 생성합니다. 기존 프로덕션 환경을 터치하지 않고 멀티 클라우드 방어을(를) 시작할 때 매우 유용합니다.

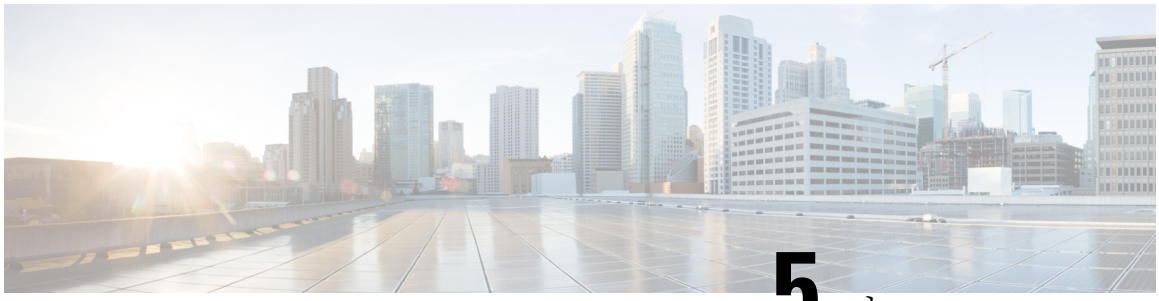
템플릿은 다음 리소스를 생성합니다.

- VNet.
- 관리 서브넷.
- 데이터 경로 서브넷.
- 아웃바운드 규칙이 있는 관리 보안 그룹.
- 포트 443에 대한 아웃바운드 규칙 및 인바운드 규칙이 있는 데이터 경로 보안 그룹.

필요에 따라 추가 서브넷을 생성하여 앱을 실행하고 앱별 보안 그룹을 생성할 수 있습니다.

ARM 템플릿을 실행하려면 다음 단계를 수행합니다.

단계 **1** Azure 어카운트에 로그인하여 맞춤형 템플릿을 구축합니다.
단계 **2** **Build your own template in the editor(**편집기에서 자체 템플릿 구축**)**를 클릭합니다.
단계 **3** ARM 템플릿의 내용을 복사하여 편집기에 붙여넣습니다.
단계 **4** **Save(**저장**)**를 클릭합니다.
단계 **5** *Subscription(*구독*), Resource group(*리소스 그룹*)* 및 *Region(*지역*)*을 선택합니다.
단계 **6** **Review+ Create(**검토+ 생성**)**를 클릭합니다.
단계 **7** 모든 리소스가 생성될 때까지 몇 분 정도 기다립니다.



5 장

GCP

GCP 개요

GCP 프로젝트 및 **GCP** 폴더

멀티 클라우드 방어 현재는 GCP 프로젝트 및 GCP 폴더를 모두 지원합니다. 단 이러한 구성 요소는 별도로 지원됩니다. 이러한 두 옵션에 대해 다음과 같은 제한 및 예외를 참고하십시오.

GCP 프로젝트에는 가상 머신, 스토리지 버킷, 데이터베이스 등과 같은 GCP 리소스가 포함되어야 합니다. 모든 Google Cloud 서비스를 생성, 활성화, 사용하는 데 사용할 수 있습니다.

- 프로젝트는 Terraform, 수동 온보딩, 스크립트 온보딩을 통해 온보딩할 수 있습니다.
- 프로젝트는 검색 및 조사 등 오케스트레이션이 필요한 환경에 적합합니다.
- 멀티 클라우드 방어 대시보드를 통해 각 프로젝트와 개별적으로 상호 작용할 수 있습니다.

버전 23.10부터는 GCP 폴더를 Terraform에 연결할 수 있습니다. GCP 폴더에는 프로젝트, 다른 폴더 또는 이 둘의 조합이 포함됩니다. 조직 리소스는 폴더를 사용하여 계층 구조의 조직 리소스 노드 아래에 프로젝트를 그룹화할 수 있습니다.

- `roles/compute.admin` 권한이 활성화되지 않은 폴더는 비어 있는 것으로 간주되어 사용되지 않습니다.
- 온보딩된 폴더와 연결된 프로젝트는 자산 및 트래픽 검색에만 사용됩니다.
- 온보딩된 폴더와 연결된 프로젝트에서는 오케스트레이션 서비스 VPC 또는 게이트웨이 생성을 수용하지 않습니다.
- GCP 콘솔에서 폴더에 만든 권한은 폴더 레벨에서 만들어야 합니다. 따라서 멀티 클라우드 방어 작업은 폴더 레벨에서도 이루어집니다.

GCP 폴더를 온보딩하려는 경우 Terraform 저장소를 참조하십시오.

절차 개요

다음은 GCP 프로젝트를 연결하는 방법에 대한 개요입니다. 셸 스크립트는 멀티 클라우드 방어에서 제공하며 마법사의 일부로 간편한 연결 프로세스를 지원합니다. 스크립트는 다음 단계를 자동화하므로 사용자가 수행할 필요가 없습니다.

1. 2개의 서비스 어카운트를 생성합니다.
2. 다음 API(Compute Engine, Secret Manager)를 활성화합니다.
3. 다음 2개의 VPC(management, datapath)를 생성합니다.
4. 데이터 경로 VPC에서 멀티 클라우드 방어 게이트웨이(앱 트래픽)에 대한 트래픽을 허용하는 방화벽 규칙을 생성합니다.
5. 관리 VPC에서 관리 트래픽이 멀티 클라우드 방어 게이트웨이에서 멀티 클라우드 방어 컨트롤러(으)로 이동할 수 있도록 방화벽 규칙을 생성합니다.

스크립트가 작동하지 않거나 설정을 수동으로 변경해야 하는 경우 GCP 클라우드 콘솔 웹 UI 또는 gcloud CLI를 사용하여 이러한 작업을 실행할 수 있습니다. GCP 프로젝트 수동 온보딩에서 프로젝트를 연결하는 다른 방법를 참조하십시오.

멀티 클라우드 방어 대시보드에서 멀티 클라우드 방어 컨트롤러에 **GCP** 프로젝트 연결

이전 섹션에서 설명한 대로 GCP 프로젝트를 준비했다면, 멀티 클라우드 방어 컨트롤러에 연결할 수 있습니다.

Before you begin

Google Cloud Platform(GCP) 프로젝트를 이미 생성했고 VPC, 서브넷, 서비스 어카운트를 생성할 수 있는 권한이 있어야 합니다.

단계 **1** CDO 메뉴 바에서 멀티 클라우드 방어을(를) 클릭합니다.
단계 **2** 멀티 클라우드 방어 컨트롤러 버튼을 클릭합니다.
단계 **3** **Cloud Accounts(**클라우드 어카운트**)** 창에서 **Add Account(**어카운트 추가**)**를 클릭합니다.
단계 **4** **General Information(**일반 정보**)** 페이지에 있는 Account Type(계정 유형) 목록 상자에서 **GCP**를 선택합니다.
단계 **5** 멀티 클라우드 방어 대시보드에 로그인합니다.
단계 **6** **Manage(**관리**)**, **Accounts(**계정**)**를 클릭합니다.
단계 **7** **Add Account(**어카운트 추가**)**를 클릭합니다.
단계 **8** 1단계에서 링크를 클릭하여 Google Cloud Platform Cloud Shell을 엽니다.
단계 **9** 2단계에서 **Copy(**복사**)** 버튼을 클릭합니다.
단계 **10** Google Cloud Platform Cloud Shell에서 bash 스크립트를 실행합니다.

단계 **11** 이 GCP 계정의 이름을 입력합니다. GCP 프로젝트 이름과 동일하게 이름을 지정할 수 있습니다. 이 이름은 멀티 클라우드 방어 컨트롤러에서만 표시됩니다.

단계 **12** (선택 사항) 설명을 입력합니다.

단계 **13** GCP 프로젝트의 프로젝트 **ID**를 입력합니다.

단계 **14** 멀티 클라우드 방어 컨트롤러에 대해 생성된 서비스 어카운트의 **Client Email(**클라이언트 이메일**)**을 입력합니다.

단계 **15** 서비스 어카운트의 개인 키를 입력합니다.

단계 **16** **Save & Continue(**저장 후 계속**)**를 클릭합니다.

What to do next

트래픽 가시성을 활성화합니다.

역할 생성자: 멀티 클라우드 방어

제공된 스크립트를 사용하여 클라우드 서비스 어카운트를 멀티 클라우드 방어 컨트롤러에 온보딩할 경우 서비스 간 통신이 보호되도록 클라우드 서비스 제공자의 매개변수 내에서 사용자 역할이 생성됩니다. 클라우드 서비스 제공자에 따라 서로 다른 역할 및 권한이 생성됩니다.

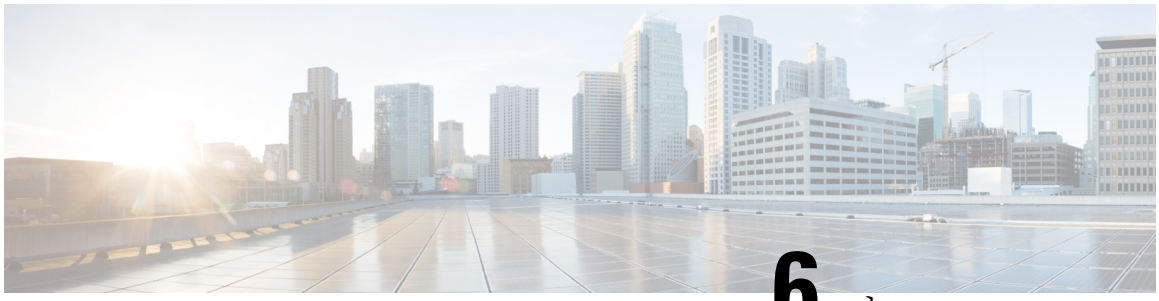
계정을 온보딩할 때 다음 역할이 생성됩니다.

GCP IAM 역할

이 문서에서는 이전 섹션에서 사용된 CloudFormation 템플릿으로 생성된 서비스 어카운트에 대해 자세히 설명합니다.

CloudFormation 템플릿은 다음 계정을 생성합니다.

- **ciscomcd-controller service account** - 이 어카운트는 멀티 클라우드 방어 컨트롤러가 GCP 프로젝트에 액세스하여 게이트웨이에 대한 리소스(멀티 클라우드 방어 게이트웨이), 로드 밸런서를 생성하고 VPC, 서브넷, 보안 그룹 태그 등에 대한 정보를 읽는 데 사용됩니다.
- **ciscomcd-firewall** 서비스 어카운트 - 이 어카운트는 멀티 클라우드 방어 게이트웨이(컴퓨팅 VM 인스턴스)에 할당됩니다. 계정은 Secret Manager(TLS 암호 해독용 개인 키) 및 스토리지에 대한 액세스를 제공합니다. 또한 여러 게이트웨이에는 (사용자가 구성한 경우) 멀티 클라우드 방어 게이트웨이에서 GCP 로그를 전송하려면 로그 작성자 권한이 필요합니다.



6 장

OCI

멀티 클라우드 방어 컨트롤러 개요에 **Oracle OCI** 테넌트 연결

OCI 테넌트를 멀티 클라우드 방어 컨트롤러에 온보딩하려면 OCI 테넌트를 올바르게 설정해야 합니다. 다음은 테넌트를 준비하는 데 필요한 일반적인 단계입니다.

OCI 테넌트를 설정하는 방법에 대한 자세한 내용은 OCI 문서를 참조하십시오. 테넌트가 완전히 설정되면 멀티 클라우드 방어 대시보드에서 Oracle OCI 테넌트를 멀티 클라우드 방어 컨트롤러에 연결합니다., on page 40를 수행할 수 있습니다.

Note 멀티 클라우드 방어은(는) OCI에 대한 인그레스 및 이그레스/이스트-웨스트 보호를 모두 지원합니다. 인벤토리 목록 및 트래픽 검색은 지원되지 않습니다.

OCI 테넌트를 온보딩하려면 미국 West(San Jose) 지역을 구독해야 합니다. 이 지역이 구독되지 않은 경우 OCI 테넌트가 온보딩할 때 오류가 발생합니다.

OCI에 멀티 클라우드 방어 게이트웨이를 구축하려면 각 OCI 구역에서 멀티 클라우드 방어 컴퓨팅 이미지에 대한 이용 약관에 동의해야 합니다. 그렇지 않으면 무단 오류와 함께 구축에 오류가 발생합니다.

단계 개요

OCI에서 테넌트 설정

1. 그룹을 생성합니다.
2. 정책을 생성합니다. 정책에는 루트 컴파트먼트가 선택되어 있어야 하며 다음 권한이 포함되어 있어야 합니다.

```
Allow group <group_name> to inspect instance-images in compartment <compartment_name>
Allow group <group_name> to read app-catalog-listing in compartment <compartment_name>
Allow group <group_name> to use volume-family in compartment <compartment_name>
Allow group <group_name> to use virtual-network-family in compartment <compartment_name>
Allow group <group_name> to manage volume-attachments in compartment <compartment_name>
Allow group <group_name> to manage instances in compartment <compartment_name>
Allow group <group_name> to {INSTANCE_IMAGE_READ} in compartment <compartment_name>
Allow group <group_name> to manage load-balancers in compartment <compartment_name>
Allow group <group_name> to read marketplace-listings in tenancy
Allow group <group_name> to read marketplace-community-listings in tenancy
Allow group <group_name> to inspect compartments in tenancy
Allow group <group_name> to manage app-catalog-listing in compartment <compartment_name>
Allow group <group_name> to read virtual-network-family in tenancy
Allow group <group_name> to read instance-family in tenancy
Allow group <group_name> to read load-balancers in tenancy
```

3. 사용자를 생성합니다.
4. 사용자를 그룹에 추가합니다.
5. 사용자에 대한 API 키를 생성합니다.
6. 사용자 및 테넌시 OCID를 기록합니다.
7. 사용 약관을 수락합니다.

다음 작업:

멀티 클라우드 방어 대시보드에서 Oracle OCI 테넌트를 멀티 클라우드 방어 컨트롤러에 연결합니다., on page 40을(를) 사용하여 OCI 테넌트를 온보딩합니다.

멀티 클라우드 방어 대시보드에서 **Oracle OCI** 테넌트를 멀티 클라우드 방어 컨트롤러에 연결합니다.

시작하기 전에

멀티 클라우드 방어 컨트롤러 개요에 Oracle OCI 테넌트 연결, 39 페이지의 요구 사항을 검토합니다.

단계 **1** CDO 대시보드의 CDO 메뉴 모음에서 멀티 클라우드 방어를 클릭합니다.

단계 **2** 멀티 클라우드 방어 컨트롤러 버튼을 클릭합니다.

단계 **3** Cloud Accounts(클라우드 어카운트) 창에서 **Add Account(**어카운트 추가**)**를 클릭합니다..

단계 **4** General Information(일반 정보) 페이지의 Account Type(계정 유형) 목록 상자에서 **OCI**를 선택합니다.

단계 **5** 다음 필드에 내용을 입력합니다.

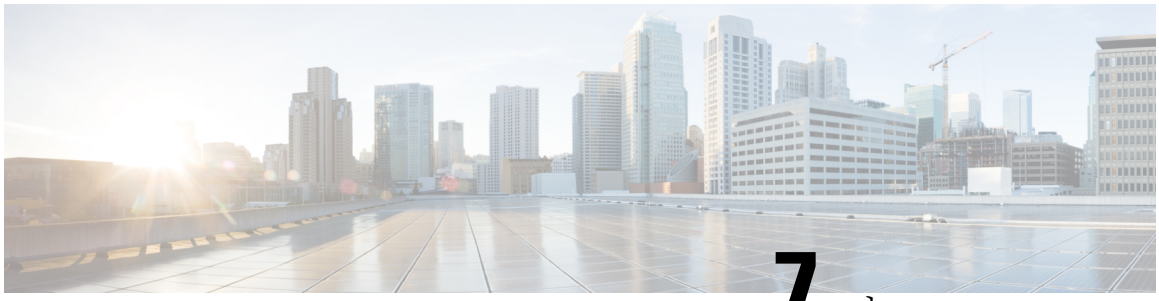
- **OCI Account Name(OCI** 계정 이름**)** - 멀티 클라우드 방어 컨트롤러 내에서 이 OCI 테넌트를 식별하는 데 사용됩니다.
- **Tenancy OCID(**테넌시 **OCID)** - OCI 사용자로부터 가져온 테넌시 Oracle Cloud 식별자입니다.

- **User OCID(**사용자 **OCID)** - OCI 사용자로부터 가져온 사용자 OCID입니다.
- **Private Key(**개인 키**)** - OCI 사용자에게 할당된 API 개인 키입니다.

다음에 수행할 작업

트래픽 가시성을 활성화합니다.

멀티 클라우드 방어 대시보드에서 **Oracle OCI** 테넌트를 멀티 클라우드 방어 컨트롤러에 연결합니다.



7 장

멀티 클라우드 방어에서 생성한 역할

역할 생성자: 멀티 클라우드 방어

제공된 스크립트를 사용하여 클라우드 서비스 어카운트를 멀티 클라우드 방어 컨트롤러에 온보딩할 경우 서비스 간 통신이 보호되도록 클라우드 서비스 제공자의 매개변수 내에서 사용자 역할이 생성됩니다. 클라우드 서비스 제공자에 따라 서로 다른 역할 및 권한이 생성됩니다.

계정을 온보딩할 때 다음 역할이 생성됩니다.

AWS IAM 역할

이 문서에서는 이전 섹션에서 사용된 CloudFormation 템플릿으로 생성된 IAM 역할에 대해 자세히 설명합니다.

CloudFormation 템플릿은 다음 3개의 IAM 역할과 1개의 CloudWatch 이벤트 규칙을 생성합니다.

- 멀티 클라우드 방어 **ControllerRole** - 멀티 클라우드 방어에서 AWS 클라우드 어카운트에 연결하는 데 사용합니다.
- 멀티 클라우드 방어 **FirewallRole** - 클라우드 어카운트에서 실행 중인 멀티 클라우드 방어 인스턴스에서 S3, SecretsManager, KMS에 액세스하는 데 사용됩니다.
- 멀티 클라우드 방어 **CloudWatchEventRole** - CloudWatch 이벤트 규칙에서 사용하여 인벤토리 변경 사항을 멀티 클라우드 방어(으)로 전송합니다.
- 멀티 클라우드 방어 **CloudWatchEventRule** - 인벤토리 변경 사항을 멀티 클라우드 방어(으)로 전송하기 위해 CloudWatch 이벤트에서 생성하는 규칙입니다. 규칙에서는 위에서 정의한 멀티 클라우드 방어 CloudWatchEventRole이 CloudWatch 이벤트를 전송할 수 있는 권한을 제공한다고 가정합니다.

MCDControllerRole

멀티 클라우드 방어이(가) 클라우드 어카운트에 액세스하여 EC2 인스턴스 생성, 로드 밸런서 생성, Route53 항목 변경 등의 필요한 작업을 수행할 수 있는 교차 어카운트 IAM 역할입니다. 서비스 보안 주체는 외부 ID가 적용된 멀티 클라우드 방어-controller-account입니다. 역할에 적용되는 IAM 정책은 다음과 같습니다(예: 이 예에서 사용된 컨트롤러 역할 이름은 멀티 클라우드 방어-***controller-role***).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "aacm:ListCertificates",
        "apigateway:Get",
        "ec2:*",
        "elasticloadbalancing:*",
        "events:DeleteRule",
        "events:ListTargetsByRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets",
        "globalaccelerator:*",
        "iam:ListPolicies",
        "iam:ListRoles",
        "iam:ListRoleTags",
        "logs:*",
        "route53resolver:*",
        "servicequotas:GetServiceQuota",
        "s3:ListAllMyBuckets",
        "s3:ListBucket"
        "wafv2:Get*"
        "wafv2:List*"
      ],
      "Effect": "Allow",
      "Resource": "*"
    },
    {
      "Action": [
        "iam:GetRole",
        "iam:ListRolePolicies",
        "iam:GetRolePolicy"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:iam::<ciscomcd-account>:role/ciscomcd-controller-role"
      ]
    },
    {
      "Effect": "Allow",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::<S3Bucket>/*"
    },
    {
      "Action": [
        "iam:GetRole",
        "iam:ListRolePolicies",
        "iam:GetRolePolicy",
        "iam:PassRole"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:iam::<customer- account>:role/ciscomcd_firewall_role"
    },
```

```
    {
      "Action": "iam:CreateServiceLinkedRole",
      "Effect": "Allow",
      "Resource": "arn:aws:iam::*:role/aws-service-role/*"
    }
  ]
}
```

서비스 보안 주체:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::<ciscomcd-account>:root"
        ]
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "sts:ExternalId": "ciscomcd-external-id"
        }
      }
    }
  ]
}
```

MCDGatewayRole

멀티 클라우드 방어 게이트웨이 (방화벽) EC2 인스턴스에 할당된 역할입니다. 역할은 게이트웨이 인스턴스에 애플리케이션의 개인 키가 저장되어 있는 secretsmanager에 액세스하는 기능, 키가 KMS에 저장된 경우 AWS KMS를 사용하여 키를 암호 해독하는 기능, 그리고 PCAP 같은 개체와 기술 지원 데이터를 S3 버킷에 저장하는 기능을 제공합니다. 이 역할의 서비스 보안 주체는 ec2.amazonaws.com입니다. 역할에 적용되는 IAM 정책은 다음과 같습니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:PutObject",
        "s3:ListBucket"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::*/*"
    },
    {
      "Action": [
        "kms:Decrypt"
      ],
      "Effect": "Allow",
      "Resource": "*"
    },
    {
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
```

```
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Tip CloudFormation 템플릿을 다운로드하고 편집하여 특정 키를 사용하도록 암호 해독을 제한하거나 PutObject를 정의된/특정 S3 버킷으로 제한하는 등 정책을 더 제한적으로 만들 수 있습니다.

MCDInventoryRole

이는 동적 인벤토리용으로 사용되며 컨트롤러의 AWS 계정으로 CloudTrail 이벤트를 전송할 수 있는 기능을 제공하는 역할입니다. 다음 작업을 수행합니다.

- 멀티 클라우드 방어 컨트롤러이(가) 있는 AWS 계정의 이벤트 버스에 이벤트를 배치합니다.
- 규칙과 일치하는 이벤트를 고객의 AWS 계정에서 직접 멀티 클라우드 방어 컨트롤러의 webhook 서버로 전송합니다.

이 역할의 서비스 보안 주체는 **events.amazonaws.com**입니다. 역할에 적용되는 정책은 다음과 같습니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": "events:PutEvents",
      "Effect": "Allow",
      "Resource": [
        "arn:aws:events:*:<ciscomcd-account>:event-bus/default"
      ]
    }
  ]
}
```

InventoryMonitorRule

멀티 클라우드 방어 컨트롤러가 실행되는 AWS 계정의 이벤트 버스에 복사할 EC2 및 API 게이트웨이에 대한 모든 CloudTrail 인벤토리 목록 변경 사항을 저장하기 위해 MCDInventoryRole에 추가되는 규칙입니다. 규칙은 고객의 AWS 계정에서 발생하는 특정 이벤트 패턴과 일치해야 합니다. 일치가 발생하면 규칙이 일치하는 이벤트를 컨트롤러의 webhook 서버(API 기반 대상)로 전송하도록 규정합니다. 이 규칙은 이전 섹션에서 생성된 멀티 클라우드 방어MCDInventoryRole을 사용하여 실행됩니다.

사용자 지정 이벤트 패턴:

```
{
  "detail-type": [
    "AWS API Call via CloudTrail",
    "EC2 Instance State-change Notification"
  ],
  "source": [
    "aws.ec2",
```

```
    "aws.elasticloadbalancing",
    "aws.apigateway"
  ]
}
```

대상:

```
Event Bus in another AWS Account (mcd-account) using the MCDInventoryRole
```

Azure IAM 역할

이 문서에서는 이전 섹션에서 사용된 CloudFormation 템플릿으로 생성된 IAM 역할에 대해 자세히 설명합니다.

CloudFormation 템플릿은 다음 역할을 생성합니다.

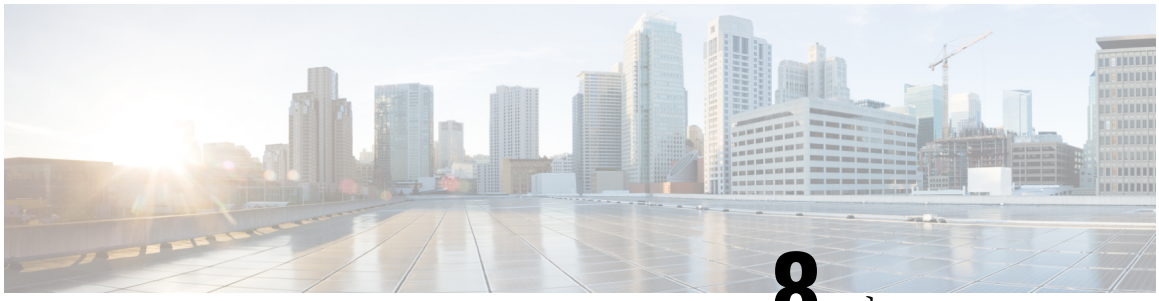
- **Custom Role(**사용자 지정 역할**)** - 사용자 지정 역할은 인벤토리 목록 정보를 읽고 리소스(예: VM, 로드 밸런서 등)를 생성할 수 있는 애플리케이션 권한을 제공합니다. 사용자 지정 역할은 여러 방법으로 생성할 수 있습니다.

GCP IAM 역할

이 문서에서는 이전 섹션에서 사용된 CloudFormation 템플릿으로 생성된 서비스 어카운트에 대해 자세히 설명합니다.

CloudFormation 템플릿은 다음 계정을 생성합니다.

- **ciscomcd-controller service account** - 이 어카운트는 멀티 클라우드 방어 컨트롤러가 GCP 프로젝트에 액세스하여 게이트웨이에 대한 리소스(멀티 클라우드 방어 게이트웨이), 로드 밸런서를 생성하고 VPC, 서브넷, 보안 그룹 태그 등에 대한 정보를 읽는 데 사용됩니다.
- **ciscomcd-firewall** 서비스 어카운트 - 이 어카운트는 멀티 클라우드 방어 게이트웨이(컴퓨팅 VM 인스턴스)에 할당됩니다. 계정은 Secret Manager(TLS 암호 해독용 개인 키) 및 스토리지에 대한 액세스를 제공합니다. 또한 여러 게이트웨이에는 (사용자가 구성한 경우) 멀티 클라우드 방어 게이트웨이에서 GCP 로그를 전송하려면 로그 작성자 권한이 필요합니다.



8 장

멀티 클라우드 방어에서 클라우드 서비스 제공자 제거

다음 절차에 따라 멀티 클라우드 방어 및 클라우드 서비스 제공자 간의 통신 및 권한을 종료할 수 있습니다. 이 작업에는 멀티 클라우드 방어 컨트롤러 내에서 생성된 게이트웨이 또는 Vnet은 물론 클라우드 서비스 제공자 내에 설정한 역할 또는 위험을 제거하는 작업이 포함됩니다. 모든 멀티 클라우드 방어 인스턴스를 정리하려면 모든 단계를 수행해야 합니다.

이러한 절차 중 일부는 멀티 클라우드 방어 컨트롤러에서 발생하지 않으며, 이러한 절차를 실행하기 위해 클라우드 서비스 제공자의 대시보드에 액세스해야 할 수 있습니다.

GCP 프로젝트 삭제 위치 멀티 클라우드 방어

멀티 클라우드 방어 컨트롤러에서 GCP 계정을 삭제하고 멀티 클라우드 방어의 모든 인스턴스를 GCP 프로젝트에서 제거하려면 다음 절차를 사용합니다. 계정에서 멀티 클라우드 방어을(를) 삭제하기 전에 멀티 클라우드 방어 컨트롤러에서 생성한 서브넷, VNet 또는 게이트웨이를 계정에서 삭제해야 합니다.

참고 이 절차를 수행하려면 멀티 클라우드 방어 UI 및 GCP 대시보드 모두에서 오케스트레이션 준비를 제거해야 합니다.

단계 **1** 멀티 클라우드 방어에서 현재 게이트웨이 또는 VNet을 삭제합니다.

a) 멀티 클라우드 방어 컨트롤러에서 **Manage(**관리**)** > **Gateways(**게이트웨이**)** > **Gateways(**게이트웨이**)**로 이동합니다.

b) 계정과 연결된 게이트웨이를 선택하여 확인란을 선택합니다.

c) **Actions(**작업**)** 드롭다운 메뉴를 확장하고 **Delete(**삭제**)**를 선택합니다.
d) 삭제를 확인합니다.
e) 멀티 클라우드 방어 컨트롤러에서 **Manage(**관리**)** > **Gateways(**게이트웨이**)** > **Service VPCs/VNets(**서비스 **VPCs/VNets)**로 이동합니다.
f) 계정과 연결된 VPC를 선택하여 확인란을 선택합니다.
g) **Actions(**작업**)** 드롭다운 메뉴를 확장하고 **Delete(**삭제**)**를 선택합니다.
h) 삭제를 확인합니다.

참고 VPC 및 게이트웨이를 삭제한 후에는 계열사 서브넷을 삭제할 필요가 없습니다.

단계 **2** 멀티 클라우드 방어 컨트롤러에서 GCP 프로젝트를 삭제합니다.
a) 멀티 클라우드 방어 컨트롤러에서 **Manage(**관리**)** > **Cloud Accounts(**클라우드 어카운트**)** > **Accounts(**어카운트**)**로 이동합니다.
b) Azure 계정을 선택하여 확인란을 선택합니다.
c) **Actions(**작업**)** 드롭다운 메뉴를 확장하고 **Delete(**삭제**)**를 선택합니다.
d) 삭제를 확인합니다.

단계 **3** GCP에서 멀티 클라우드 방어 컨트롤러 서비스 어카운트를 삭제합니다.
a) GCP 대시보드에 로그인합니다.
b) GCP 프로젝트에서 IAM을 엽니다.
c) 왼쪽 탐색창에서 **Service Accounts(**서비스 어카운트**)**를 클릭합니다.
d) 멀티 클라우드 방어과(와) 연결된 프로젝트를 선택합니다.
e) **View by Principals(**보안 주체별 보기**)** 탭에서 `ciscomcd-controller`를 검색합니다.
f) 행의 확인란이 선택된 다음 **Delete(**삭제**)**를 클릭합니다.

단계 **4** GCP에서 멀티 클라우드 방어 방화벽 서비스 어카운트를 삭제합니다.
a) GCP 대시보드에 로그인합니다.
b) GCP 프로젝트에서 IAM을 엽니다.
c) 왼쪽 탐색창에서 **Service Accounts(**서비스 어카운트**)**를 클릭합니다.
d) 멀티 클라우드 방어과(와) 연결된 프로젝트를 선택합니다.
e) **View by Principals(**보안 주체별 보기**)** 탭에서 `ciscomcd-gateway`를 검색합니다.
f) 행의 확인란이 선택된 다음 **Delete(**삭제**)**를 클릭합니다.

멀티 클라우드 방어에서 **AWS** 어카운트 삭제

다음 절차를 사용하여 멀티 클라우드 방어에서 AWS 어카운트를 완전히 제거합니다.

AWS 어카운트를 삭제한 후 클라우드 서비스 공급자가 사용자의 어카운트와 연결된 S3 버킷 내의 모든 개체를 정리하는 데 최대 24시간이 걸릴 수 있습니다.

단계 **1** CDO에 로그인하고 멀티 클라우드 방어 컨트롤러를 실행합니다.

단계 **2** 상단 메뉴 모음에서 **Manage(**관리**)** > **Gateways(**게이트웨이**)**를 클릭합니다.
단계 **3** 어카운트와 연결된 게이트웨이를 찾고 확인란을 선택한 다음 **Actions(**작업**)** 드롭다운 메뉴를 클릭합니다.
단계 **4** **Disable(**비활성화**)**을 선택합니다. 이 작업을 수행하면 어카운트와 연결된 모든 가상 머신이 자동으로 제거됩니다.
단계 **5** 게이트웨이의 확인란이 여전히 선택되어 있는지 확인하고 **Actions(**작업**)** 드롭다운 메뉴를 다시 클릭합니다.
단계 **6** **Delete(**삭제**)**를 선택합니다. 이 작업은 AWS 어카운트와 연결된 로드 밸런서를 제거합니다.
단계 **7** **Manage(**관리**)** > **Cloud Accounts(**클라우드 어카운트**)** > **Accounts(**어카운트**)**로 이동합니다.
단계 **8** 목록에서 AWS 어카운트를 찾아 선택하여 확인란을 선택합니다.
단계 **9** **Actions(**작업**)** 드롭다운 메뉴를 클릭하고 **Delete(**삭제**)**를 선택합니다.
단계 **10** 어카운트를 삭제할 것인지 확인합니다.

멀티 클라우드 방어에서 **Azure** 계정 삭제

다음 절차를 사용하여 멀티 클라우드 방어에서 Azure 계정의 모든 인스턴스를 제거합니다.

시작하기 전에

Azure 계정에서 멀티 클라우드 방어을(를) 삭제하기 전에 멀티 클라우드 방어 컨트롤러에서 생성한 서브넷 및 VNet을 삭제해야 합니다.

참고 이 절차를 수행하려면 멀티 클라우드 방어 UI 및 GCP 대시보드 모두에서 오케스트레이션 준비를 제거해야 합니다.

단계 **1** CDO에 로그인하고 멀티 클라우드 방어 컨트롤러을(를) 실행합니다.
단계 **2** 키 저장소에 대해 사용자 할당 관리 ID를 생성하지 않은 경우 4단계를 계속합니다. Azure 계정에 대한 키를 생성한 경우 다음을 수행합니다.
  a) **Manage(**관리**)** > **Security Policies(**보안 정책**)** > **Certificates(**인증서**)**로 이동합니다.
  b) 계정과 연결된 인증서를 선택한 다음 **Actions(**작업**)** 드롭다운 메뉴를 엽니다.
  c) **Delete(**삭제**)**를 선택하고 키 저장소에 대한 인증서 삭제를 확인합니다.
단계 **3** 멀티 클라우드 방어 컨트롤러에서 계정과 연결된 게이트웨이 또는 VNet을 삭제합니다.
  a) **Manage(**관리**)** > **Gateways(**게이트웨이**)** > **Gateways(**게이트웨이**)**로 이동하여 이전에 생성한 모든 게이트웨이를 삭제합니다.
  b) 계정과 연결된 게이트웨이를 선택하여 확인란을 선택합니다.
  c) **Actions(**작업**)** 드롭다운 메뉴를 확장하고 **Delete(**삭제**)**를 선택합니다.
  d) 삭제를 확인합니다.
  e) 멀티 클라우드 방어 컨트롤러에서 **Manage(**관리**)** > **Gateways(**게이트웨이**)** > **Service VPCs/VNets(**서비스 **VPC/VNet)**로 이동하여 이전에 만든 VNet을 삭제합니다.
  f) 계정과 연결된 VNet을 선택하면 확인란이 선택됩니다.

g) **Actions(**작업**)** 드롭다운 메뉴를 확장하고 **Delete(**삭제**)**를 선택합니다.
h) 삭제를 확인합니다.
i) 멀티 클라우드 방어 컨트롤러에서 **Manage(**관리**)** > **Cloud Accounts(**클라우드 어카운트**)** > **Accounts(**어카운트**)**로 이동합니다.
j) Azure 계정을 선택하여 확인란을 선택합니다.
k) **Actions(**작업**)** 드롭다운 메뉴를 확장하고 **Delete(**삭제**)**를 선택합니다.
l) 삭제를 확인합니다.

단계 **4** Azure에서 멀티 클라우드 방어 컨트롤러 역할을 삭제합니다.

a) Azure 포털에 로그인합니다.
b) **App Registrations(**앱 등록**)**로 이동합니다.
c) **Owned Appications(**소유 애플리케이션**)** 탭을 선택합니다.
d) **ciscomcd-controller-app** 애플리케이션을 선택합니다.
e) 선택이 끝나면 창 맨 위의 **Delete(**삭제**)**를 클릭합니다.
f) 삭제를 확인합니다.
g) **Subscription(**구독**)**으로 이동하거나 검색하고 **Access Control (IAM)(**액세스 제어**(IAM))**을 클릭합니다.
h) 창의 맨 위의 **Roles(**역할**)** 탭을 선택합니다.
i) **ciscomcd-controller-role-rw**를 검색하고 선택하면 확인란이 선택됩니다.
j) 창 맨 위의 **Remove(**제거**)**를 클릭합니다.

멀티 클라우드 방어에서 **OCI** 계정 삭제

다음 절차를 사용하여 멀티 클라우드 방어에서 OCI 클라우드 환경을 제거합니다.

단계 **1** OCI 콘솔에 로그인합니다.

단계 **2** API 키를 삭제합니다. 자세한 내용은 Oracle Cloud Infrastructure Documentation(오라클 클라우드 인프라 설명서)의 "**Deleting API Signing Keys from a Roaving Edge Infrastructure Device(Roaving Edge** 인프라 장치에서 **API** 서명 키 삭제**)**" 장을 참조하십시오.

단계 **3** 멀티 클라우드 방어 사용자를 삭제합니다. 자세한 내용은 Oracle Cloud Infrastructure Documentation의 "**Deleting a User(**사용자 삭제**)**" 장을 참조하십시오.

참고 즉, OCI 계정에서 사용자를 제거해도 사용자의 감사 데이터가 유효했을 때 삭제되지 않습니다.

단계 **4** 멀티 클라우드 방어 그룹을 삭제합니다. 자세한 내용은 Oracle Cloud Infastructure Documentation의 "**Deleting Groups(**그룹 삭제**)**" 장을 참조하십시오.

단계 **5** 모든 멀티 클라우드 방어 액세스 정책을 삭제합니다. 자세한 내용은 Oracle Cloud Infastructure Documentation의 "액세스 정책 삭제" 장을 참조하십시오.

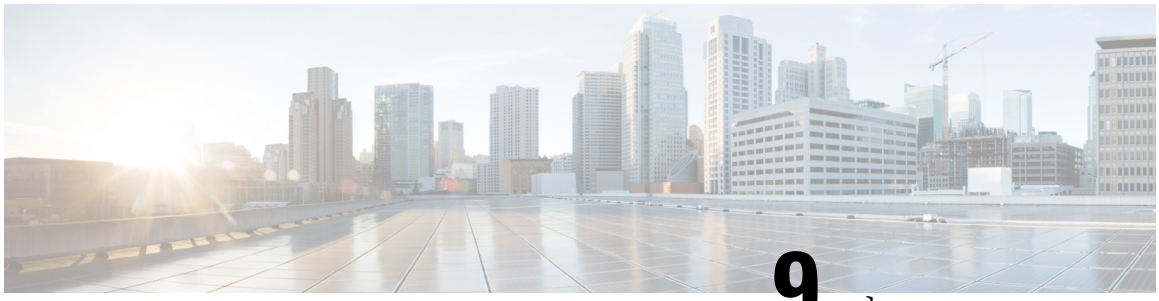
단계 **6** 멀티 클라우드 방어 컨트롤러에서 OCI 계정을 삭제합니다. .

a) 멀티 클라우드 방어 컨트롤러에서 **Manage(**관리**)** > **Cloud Accounts(**클라우드 어카운트**)** > **Accounts(**어카운트**)**로 이동합니다.

b) OCI 계정을 선택하여 확인란을 선택합니다.
c) **Actions(**작업**)** 드롭다운 메뉴를 확장하고 **Delete(**삭제**)**를 선택합니다.
d) 삭제를 확인합니다.

IV 부

검색



9 장

자산 및 인벤토리 목록 검색

검색은 멀티 클라우드 방어의 "검색, 구축 및 방어" 접근 방식에서 중요한 구성 요소입니다.

검색은 온보딩된 클라우드 어카운트에 구축된 현재 리소스에 대한 실시간 가시성을 제공합니다. 또한 VPC 플로우 로그 및 DNS 로그에 대한 인터페이스를 제공하여 클라우드 구축을 완벽하게 파악할 수 있습니다. IAM 역할(AWS 및 OCI), AD 앱 등록(Azure) 또는 서비스 어카운트(GCP)에 부여된 권한을 통해 멀티 클라우드 방어 컨트롤러는 클라우드 리소스를 주기적으로 크롤링하고 변경 사항을 계속 모니터링하여 "에버그린" 인벤토리 목록 모델을 유지합니다.

Discovery(검색**)** 탭을 사용하면 리소스의 속성과 이러한 리소스가 상호 연결된 방식을 확인할 수 있습니다. 멀티 클라우드 방어에서는 구성과 관련된 모든 리소스 보안 상태의 간결한 보기에 이 정보를 수집하고, 트래픽 흐름에 대한 컨텍스트도 파악합니다.

검색 요약

Discovery Summary(검색 요약) 페이지는 사용 가능한 트래픽 및 인벤토리를 요약하는 위젯 모음입니다. 페이지 맨 위의 필터 를 사용하여 위젯의 기록을 변경할 수 있습니다.

트래픽 요약 위젯

현재 멀티 클라우드 방어은 DNS 트래픽용 위젯과 VPC 및 VNet 플로우 로그용 위젯의 두 가지 위젯으로 트래픽의 압축된 블록을 표시합니다. 트래픽에 대한 이러한 창은 악성 트래픽과 DNS 또는 VPC/VNet 트래픽을 각각 구분합니다. 특정 시간 프레임으로 확대하려면 이러한 위젯의 내부를 클릭합니다.

이 요약 페이지에서 **Logs(**로그**)** 토글을 클릭하여 해당 위젯에 대한 로그를 활성화하거나 비활성화할 수 있습니다. 이러한 로그 유형과 컴파일되는 트래픽에 대한 자세한 내용은 트래픽 유형, 137 페이지를 참조하십시오.

검색 요약

검색 요약은 클라우드 서비스 제공자를 연결할 때 검색 프로세스의 일부로 멀티 클라우드 방어이 복구한 일련의 인벤토리 창입니다. 이러한 통계는 빠르게 미리 볼 수 있도록 여기에 요약되어 있습니다. 자세한 내용은 인벤토리, 58 페이지를 참조하십시오.

인벤토리

IAM 역할(AWS 및 OCI), AD 앱 등록(Azure) 또는 서비스 어카운트(GCP)에 부여된 권한을 통해 멀티 클라우드 방어는 클라우드 리소스의 "에버그린" 인벤토리 목록 모델을 지속적으로 유지하고 클라우드 서비스 공급자 어카운트, 구독 및 고급 네트워크 보안 적용과 관련된 프로젝트에 존재하는 실시간 검색을 유지합니다. 검색된 리소스는 관리자가 애플리케이션 노출의 위험을 완화하는 보안 규칙을 신속하게 구축할 수 있는 워크플로우에서 사용할 수 있습니다. 모든 활동은 멀티 클라우드 방어 컨트롤러을(를) 통해 즉시 보고됩니다.

인벤토리 목록이 활성화된 경우 멀티 클라우드 방어 컨트롤러에서 전체 인벤토리 목록 검색을 주기적으로 수행합니다. 기본값은 60분이지만 조정 가능합니다. 실시간 인벤토리 목록 검색은 CloudFormation 템플릿이 구축된 지역에서 활성화됩니다.

검색 프로세스 중 일부에서는 각 클라우드 서비스의 로그가 강조 표시됩니다. 서비스 제공자별로 다음과 같은 로그 유형을 확인할 수 있습니다.

- **AWS** - VPC 플로우 로그, Mount53 플로우 로그 및 DNS 로그.
- **Azure** - NSG 플로우 로그.
- **GCP** - VPC 플로우 로그.

멀티 클라우드 방어은(는) 모든 클라우드 서비스 제공자에게 동일한 레벨의 지원을 제공합니다.

애플리케이션

Application(애플리케이션)에 클라우드 어카운트에 대한 모든 로드 밸런서 및 API 게이트웨이가 표시됩니다. **Inventory(**인벤토리 목록**)**의 Applications(애플리케이션) 섹션에는 **Known Tags(**알려진 태그**)**, **Tags(**태그**)** 및 **Applications(**애플리케이션**)**이라는 3개의 필터 버튼이 있습니다. **Applications(**애플리케이션**)**에서 사용자는 특정 애플리케이션에 대한 보호를 생성하고 적용하는 워크플로우를 호출할 수 있습니다.

애플리케이션 태그

애플리케이션을 식별하는 데 사용되는 **Application Tags(**애플리케이션 태그**)** 목록을 만듭니다. 인벤토리 검색 중에 지정된 태그가 있는 모든 검색된 로드 밸런서가 애플리케이션으로 처리됩니다.

예를 들어 애플리케이션 역할을 하는 모든 로드 밸런서에 **Application Tags(**애플리케이션 태그**)**를 할당할 수 있습니다. 이 태그의 값은 검색된 인벤토리 목록에 애플리케이션 태그로 표시됩니다. 아래 표를 시각적 예로 참조하십시오.

로드 밸런서	태그	값
로드 밸런서 1	ApplicationName	Billing
로드 밸런서 2	ApplicationName	UserManagement

검색된 인벤토리 목록에는 검색된 애플리케이션 자산 내의 **Billing** 및 **UserManagement** 애플리케이션이 표시됩니다.

애플리케이션 태그 목록을 생성하려면 **Create(**생성**)**를 클릭합니다.

매개변수	설명
이름	사전 채워집니다.
설명	사용자 지정 설명입니다.
값	로드 밸런서에 할당하는 데 사용할 태그 값입니다.

애플리케이션 태그에 대한 자세한 내용은 애플리케이션 태그, on page 262를 참조하십시오.

Known Tags(알려진 태그**)**

Known Tags(알려진 태그**)**는 관리자가 알려진 태그로 식별한 클라우드 어카운트의 애플리케이션 로드 밸런서에서 식별한 애플리케이션을 보여줍니다. 이러한 알려진 태그가 **Settings(**설정**)** > **Management(**관리**)** > **Account(**계정**)** > **Application Tags(**애플리케이션 태그**)**에 나열되어 있습니다.

태그

Tags(태그)는 태그 키와 태그 값을 표시하는 필드와 함께 애플리케이션 로드 밸런서, 그리고 해당 애플리케이션이 멀티 클라우드 방어 게이트웨이로 보호되는지 여부를 통해 식별한 모든 애플리케이션을 표시합니다.

검색된 자산

클라우드 어카운트에 대한 지역의 인벤토리 목록 검색을 활성화하면 멀티 클라우드 방어 컨트롤러이(가) 클라우드 자산을 지속적으로 검색합니다. 검색된 자산을 보려면 **Discover(**검색**)** 또는 **Manage(**관리**)** > **Inventory(**인벤토리 목록**)**로 이동합니다. 기본 보기에는 모든 클라우드 어카운트에 대해 검색된 자산이 표시됩니다. 특정 클라우드 어카운트으로 필터링하려면 **Select Account(**어카운트 선택**)**를 사용하여 특정 클라우드 어카운트를 지정하고 검색된 자산을 확인합니다.

검색된 자산 범주 및 이러한 범주가 참조하는 항목은 다음과 같습니다.

- 보안 그룹 - AWS 보안 그룹(SG) 및 Azure NSG(네트워크 보안 그룹)
- 네트워크 ACL - AWS NACL(Network Access Control List).
- 서브넷.
- 경로 테이블.

- 네트워크 인터페이스.
- VPC/VNet - AWS VPC, Azure VNet 및 GCP VPC.
- 애플리케이션 - 애플리케이션은 AWS ALB(Application Load Balancer)에 의해 식별됩니다.
- 로드 밸런서.
- 인스턴스 - AWS 인스턴스, Azure 가상 머신 및 GCP 컴퓨팅 인스턴스.
- 태그 - AWS 태그, Azure 태그 및 GCP 레이블.
- 인증서 - AWS Certificates Manager(ACM) 인증서

자산 검색 및 인벤토리 목록 활성화

클라우드 어카운트에서 자산 검색을 활성화하려면:

단계 **1** **Manage(**관리**)** > **Accounts(**계정**)**로 이동합니다.

단계 **2** 클라우드 어카운트 옆의 확인란을 선택하고 **Manage Inventory(**인벤토리 관리**)**를 클릭합니다.

단계 **3** 멀티 클라우드 방어가 검색하려는 클라우드 자산이 있는 **Regions(**지역**)**을 선택합니다. 새로 고침 간격은 인벤토리 목록이 새로 고쳐지는 시간(분)입니다(권장 기본값은 60분). 또한 멀티 클라우드 방어는 일반 폴링 대신 클라우드 서비스 공급자의 API 및 이벤트를 사용하여 지속적 검색을 수행합니다. 여기에 지정된 새로 고침 시간 간격은 전체 재크롤링을 위한 것입니다. 이렇게 하면 실시간 검색 중에 누락된 이벤트에 대한 모든 자산이 조정됩니다.

새 행을 추가하고 원하는 영역을 선택하여 각 영역에 대해 다른 새로 고침 간격을 정의할 수 있습니다. 영역은 단일 새로 고침 간격에만 속할 수 있습니다.

단계 **4** **Finish(**마침**)**를 클릭하여 저장합니다.

Note 멀티 클라우드 방어 컨트롤러는 저장 후 즉시 새로 추가된 영역에 대한 자산 인벤토리 목록을 요청합니다.

What to do next

검색된 자산을 검토하려면 **Manage(**관리**)** > **Inventory(**인벤토리 목록**)**로 이동합니다.

보안 인사이트

인사이트는 AWS, Azure 및 GCP에서 검색되어 결과로 표시되는 자산에 대한 규칙 기반 평가입니다. 인사이트는 멀티 클라우드 방어 컨트롤러에서 수용하는 주기적인 실시간 인벤토리 목록 모니터링을 기반으로 작동하므로 멀티 클라우드 방어 게이트웨이을(를) 구축하지 않고도 사용할 수 있습니다.

단계 **1** 멀티 클라우드 방어 컨트롤러 인터페이스에서 **Add Account(**어카운트 추가**)**를 클릭합니다. 또는 멀티 클라우드 방어 마법사를 사용하여 설정 마법사를 사용하여 어카운트에 연결하는 것을 강력하게 권장합니다. 계정을 연결하는 단계를 진행합니다.

단계 **2** 계정이 연결되고 온보딩되면 자산 검색 및 인벤토리 목록 활성화합니다.

단계 **3** **Discover(**검색**)** > **Discovery Summary(**검색 요약**)**로 이동합니다. 이 페이지에는 검색된 모든 자산 및 인사이트 결과의 요약 보기가 표시됩니다.

보안 인사이트 유형

대시보드의 기능을 이해하려면 다음 보안 인사이트 유형을 자세히 읽어보십시오.

보안 그룹

고객은 종종 보안 그룹의 급증으로 어려움을 겪습니다. 보안 그룹은 위험을 초래할 수 있는 리소스 간에 공유되는 경우가 많습니다. 특정 리소스를 대상으로 하는 보안 그룹을 변경하면 더 큰 리소스 그룹에 영향을 줄 수 있습니다.

Security Groups(보안 그룹)은 모든 보안 그룹, 세부 정보 및 보안 그룹을 활용하는 리소스 집합의 목록을 제공합니다. **Is Inbound Public(**인바운드 공용 여부**)** 및 **Is Outbound Public(**아웃바운드 공용 여부**)** 필드는 0.0.0.0/0으로 설정된 보안 그룹을 나타냅니다.

검색 창에서 검색 기준을 기반으로 규칙을 생성하는 옵션을 사용하여 필드 및 해당 값을 기반으로 검색 기준을 정의합니다.

규칙

규칙은 구성된 인바운드 및 아웃바운드 규칙을 기반으로 보안 그룹을 보여줍니다.

포트

포트는 구성된 인바운드 및 아웃바운드 포트를 기반으로 보안 그룹을 볼 수 있습니다.

애플리케이션 보안 그룹

애플리케이션 보안 그룹 은 AWS 보안 그룹과 유사한 Azure 구조입니다. Azure 애플리케이션 보안 그룹에는 해당 시스템과 시스템의 인터페이스를 포함하는 보안 그룹의 멤버가 있습니다. 멤버십과 보안 컨트롤이 모두 있습니다. 따라서 멀티 클라우드 방어은 멤버십 구성을 사용하여 동적 정책을 구축합니다. Azure 환경 내에서 애플리케이션 보안 그룹을 생성하고 사용하면, 멀티 클라우드 방어이 변경 사항을 인식하고 정책을 조정하여 통합합니다.

Azure의 애플리케이션 보안 그룹 및 작동 방식에 대한 자세한 내용은 Microsoft Azure 설명서를 참조하십시오.

네트워크 **ACL**

네트워크 ACL(Access Control List)은 모든 네트워크 ACL의 목록과 세부 정보를 제공합니다. **Is Inbound Public(**인바운드 공용 여부**)** 및 **Is Outbound Public(**아웃바운드 공용 여부**)** 필드는 0.0.0.0/0으로 설정된 네트워크 ACL을 나타냅니다.

규칙

규칙은 구성된 인바운드 및 아웃바운드 규칙을 기반으로 네트워크 ACL을 보여줍니다.

서브넷

서브넷은 모든 서브넷 및 세부 정보의 목록을 제공합니다. **Is Public(**퍼블릭**)** 필드는 자동 할당 공용 IP의 활성화 여부에 따라 공개적으로 액세스 가능한 서브넷을 나타냅니다.

경로 테이블

경로 테이블은 모든 경로 테이블 및 세부 정보의 목록을 제공합니다. **Is Inbound Public(**인바운드 공용 여부**)** 및 **Is Outbound Public(**아웃바운드 공용 여부**)** 필드는 기본 액세스 인터넷을 제공하도록 구성된 경로 테이블을 나타냅니다.

네트워크 인터페이스

네트워크 인터페이스는 모든 네트워크 인터페이스 및 상세정보 목록을 제공합니다. **Is Inbound Public(**인바운드 퍼블릭**)** 및 **Is Outbound Public(**아웃바운드 퍼블릭**)** 필드는 개방형 보안 그룹(0.0.0.0/0)으로 구성된 네트워크 인터페이스 또는 인터넷에 대한 기본 액세스를 허용하는 경로 테이블을 나타냅니다.

VPC\VNets

VPC/VNet은 모든 VPC/VNet 및 해당 세부 정보의 목록을 제공합니다.

애플리케이션

Applications(애플리케이션)에서는 구축된 모든 애플리케이션 로드 밸런서 및 해당 세부 정보의 목록을 제공합니다. **Secured(**보안**)** 필드는 멀티 클라우드 방어 게이트웨이 및 보안 정책이 애플리케이션을 보호하기 위해 적용되는지 여부를 식별하며, 애플리케이션을 보호하는 워크플로우를 호출하는 기능을 제공합니다.

로드 밸런서

로드 밸런서는 모든 구축된 애플리케이션, 네트워크 및 게이트웨이 로드 밸런서 목록과 해당 세부 정보를 제공합니다. **Public** 필드에는 리소스가 인터넷 연결 로드 밸런서인지 여부가 표시됩니다. **CSP WAF Enabled(CSP WAF** 활성화**)**는 애플리케이션 로드 밸런서에 대해 CSP WAF가 활성화되었는지 여부를 표시합니다.

인스턴스

인스턴스는 리소스에 대해 할당 및 구성된 보안 그룹 및 인터페이스 수에 대한 요약 정보와 함께 모든 인스턴스의 목록을 제공합니다. **Is Inbound Public(**인바운드 퍼블릭**)** 및 **Is Outbound Public(**아웃바운드 퍼블릭**)** 필드는 개방형 보안 그룹(0.0.0.0/0)으로 구성된 네트워크 인터페이스가 있는 인스턴스 또는 인터넷에 대한 기본 액세스를 허용하는 경로 테이블을 나타냅니다.

태그

태그는 태그로 구성된 모든 VPC/VNet, 서브넷, 보안 그룹, 인스턴스 및 로드 밸런서의 목록을 제공합니다.

인증서

인증서는 AWS 인증서 관리자에서 사용 가능한 모든 인증서의 목록과 함께 발급자, 도메인 이름 및 만료일에 대한 요약 정보를 제공합니다.

토폴로지

이 탭에는 클라우드 어카운트에 있는 클라우드 자산의 지역별 개략적인 맵 보기가 표시됩니다. 화면 상단의 필터 막대를 사용하여 시각적 개체를 세부적으로 조정할 수 있습니다. 여기에서 데이터 drom을 가져올 클라우드 서비스 제공자 어카운트, 세계의 지역, 특정 VNet 또는 VPC, 인스턴스 및 기록의 기간을 결정할 수 있습니다.

세계 지도의 글로벌 보기를 사용하면 위에서 언급한 필터 표시줄로 지정한 특정 지역을 스크롤하여 자세히 살펴볼 수 있습니다. 맵의 바로 왼쪽에서 확인할 트래픽 및 인벤토리 유형을 표시할 수 있습니다. 표시할 내용에 대해 적절하게 확인란을 선택하고 선택 취소합니다.

통찰력

인사이트는 AWS, Azure 및 GCP에서 검색되어 결과로 표시되는 자산에 대한 규칙 기반 평가입니다.

규칙

규칙은 검색된 자산의 결과를 식별하기 위한 평가 집합입니다. 멀티 클라우드 방어에서는 기본 규칙 집합을 제공합니다. 인벤토리 목록 범주(예: 보안 그룹, 애플리케이션, 로드 밸런서, 태그 등)를 선택하고 검색 기준을 정의하고 **Add Rule(**규칙 추가**)**을 선택하고 추가 필수 정보를 지정하여 새 규칙을 생성할 수 있습니다. 새 규칙을 보려면 **Insights(**인사이트**)** > **Rules(**규칙**)** 로 이동합니다. 여기에서 기존 및 새로 검색된 자산을 대상으로 작업을 수행할 수 있습니다.

결과

결과는 정의된 규칙 집합과 일치하는 검색된 자산의 목록입니다.

규칙 및 결과

클라우드 리소스를 확인하고 가드 레일을 사용하도록 규칙을 구성할 수 있습니다.

규칙 및 결과

클라우드 리소스를 확인하고 가드 레일을 사용하도록 규칙을 구성할 수 있습니다.

사전 정의된 규칙

멀티 클라우드 방어 컨트롤러에는 몇 가지 사전 정의된 기본 규칙이 있습니다.

- 클라우드 서비스 제공자 WAF가 활성화되지 않은 애플리케이션 로드 밸런서.
- 인그레스가 열려 있는 인스턴스가 거의 없는 보안 그룹(5개 미만). 보안 그룹의 사용률이 낮으면 확인하기 어려운 격차가 발생하고 공격이 쉽게 발생할 수 있습니다.
- 네트워크 인터페이스가 두 개 이상인 인스턴스.
- 열린 아웃바운드(0.0.0.0/0) 액세스 권한이 있는 보안 그룹.
- 퍼블릭 서브넷 - **Auto-Assign Public IP(**자동 할당 공용 **IP)** 가 활성화된 모든 AWS 서브넷.
- 인터넷에 너무 많은 송신 포트(25개 이상)가 열려 있는 보안 그룹.
- 인터넷에 너무 많은 수신 포트(5개 이상)가 열려 있는 보안 포트.
- 공개 액세스가 활성화된 상태에서 65,535개의 포트가 열려 있는 보안 그룹.
- 30일 후에 만료되는 인증서 - AWS Certificate Manager에만 해당.

규칙과 일치하는 클라우드 리소스는 심각도와 일치하는 결과로 플래그가 지정됩니다.

맞춤형 규칙 생성에 대한 자세한 내용은 사전 정의된 규칙, on page 64를 참고하십시오.

맞춤형 규칙

사용자는 리소스에 대한 추가 규칙을 구성할 수 있습니다.

1. **Discovery(**검색**)** > **Inventory(**인벤토리 목록**)**으로 이동하고 리소스(예: 로드 밸런서)를 선택합니다.
2. 텍스트 영역에서 규칙 기준을 생성하고 **Add Rule(**규칙 추가**)**를 선택합니다.
3. 다음 항목의 콘텐츠와 규칙 기준을 충족하는 발견 항목 수를 입력합니다.
   - 이름
   - 설명
   - 심각도
   - 기본 작업
   - 유형
   - 계정

4. **Save(**저장**)**를 클릭합니다.

규칙의 기본 작업은 **info(**정보**)** 또는 알림**(alert)**일 수 있습니다. 규칙이 기본 작업으로 알림으로 구성된 경우, 규칙에 대한 새 결과가 발생하면 멀티 클라우드 방어 컨트롤러에서 알림 알림이 생성됩니다. 알림의 기본 작업을 원하는 경우 다음 구성이 필요합니다.

- 사용자가 ServiceNow, PagerDuty 또는 Webhook 알림을 원하는지 나타내도록 알림 프로파일을 구성합니다.
- 지정된 심각도 레벨을 사용하여 **Alert Rule of type Discovery(**검색 유형의 알림 규칙**)** 및 하위 유형 **Insights Rule(**인사이트 규칙**)**을 구성합니다.

결과

사전 정의된 규칙과 맞춤형 규칙을 기반으로 리소스에 대한 결과를 볼 수 있습니다. **Findings Summary(**결과 요약**)**는 대시보드에 위치하며 Inventory(인벤토리 목록) 탭의 Summary(요약) 보기에도 쉽게 액세스할 수 있습니다.

V 부

멀티 클라우드 방어 게이트웨이

10 장

멀티 클라우드 방어 게이트웨이 관리

개요

멀티 클라우드 방어 게이트웨이은(는) 멀티 클라우드 방어 게이트웨이 인스턴스의 클러스터가 있는 네트워크 로드 밸런서로 구성된 네트워크 기반 보안 플랫폼입니다. 이 클러스터는 트래픽 로드에 따라 확장 및 축소되는 자동 확장 및 자가 복구 클러스터입니다. 멀티 클라우드 방어 컨트롤러 및 게이트웨이 인스턴스는 상태 및 텔레메트리에 관한 일정하고 지속적인 정보를 교환합니다. 멀티 클라우드 방어 컨트롤러은(는) 게이트웨이 인스턴스에서 수신된 텔레메트리 데이터를 측정하여 확장/축소 결정을 내립니다. 고 가용성의 탄력적 아키텍처를 위해 여러 가용성 영역에서 게이트웨이를 실행하도록 구성할 수 있습니다. 이렇게 하면 클라우드 서비스 공급자의 단일 가용성 영역 장애가 발생해도 실행 중인 애플리케이션의 보안 상태가 손상되지 않습니다.

게이트웨이 및 해당 VPC 또는 VNet을 구성한 후에는 멀티 클라우드 방어 컨트롤러의 **Gateway Details(**게이트웨이 세부 정보**)** 페이지를 사용하여 해당 상태를 보고 관리할 수 있습니다.

멀티 클라우드 방어 게이트웨이는 두 가지 방법으로 구축할 수 있습니다. 허브 모드와 엣지 모드입니다.

게이트웨이 재시도

멀티 클라우드 방어 게이트웨이는 자가 복구 구성 요소 멀티 클라우드 방어입니다. 어느 시점에서든 게이트웨이 구축이 실패하거나 문제가 발생하면, 멀티 클라우드 방어는 자동으로 게이트웨이 재시도를 포함한 게이트웨이 재구축을 시도합니다. 이 작업은 컨트롤러에서 게이트웨이를 수동으로 비활성화하거나 삭제할 때까지 무제한으로 수행됩니다.

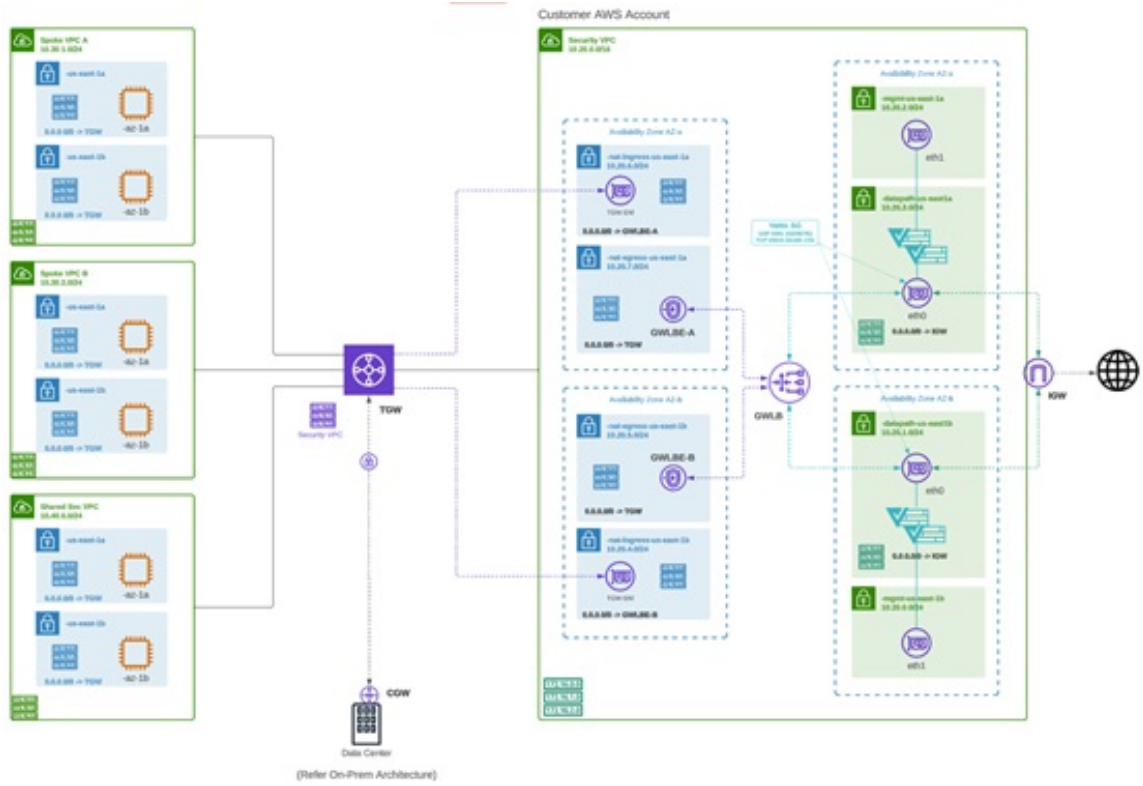
Terraform에서 두 가지 측면의 재시도 작업을 설정할 수 있습니다. 첫 번째, 게이트웨이 구축을 위해 멀티 클라우드 방어가 재시도하는 횟수를 구성할 수 있습니다. 최대 재구축 시도 횟수가 완료되면 멀티 클라우드 방어은 재시도를 중지합니다. 둘째, 재시도 사이의 시간을 구성할 수 있습니다. 예를 들어, 게이트웨이 재시도를 한 시간에 3회 구성할 수 있습니다. 즉, 1시간마다 멀티 클라우드 방어가 게이트웨이 구축을 3회 재시도한 다음 중지됩니다. 이 작업은 게이트웨이 문제가 해결되거나 컨트롤러에서 게이트웨이를 삭제하는 경우까지 반복됩니다.

지원되는 게이트웨이 활용 사례

이그레스

퍼블릭 클라우드 네트워크에서 나가는 트래픽을 보호하기 위해 이그레스/이스트-웨스트 게이트웨이 구축. 이그레스 게이트웨이는 투명 전달 프록시로 작동하여 전체 암호 해독을 수행하고 침입 방지, 악성코드 차단, 데이터 손실 방지, 전체 경로 URL 필터링과 같은 고급 보안 기능을 내장합니다. 선택적으로, 전달 모드에서 작동할 수도 있습니다. 이 모드에서는 트래픽을 프록시하거나 암호 해독하지 않지만 악의적인 IP 차단 및 FQDN 필터링과 같은 보안 기능이 계속 적용됩니다.

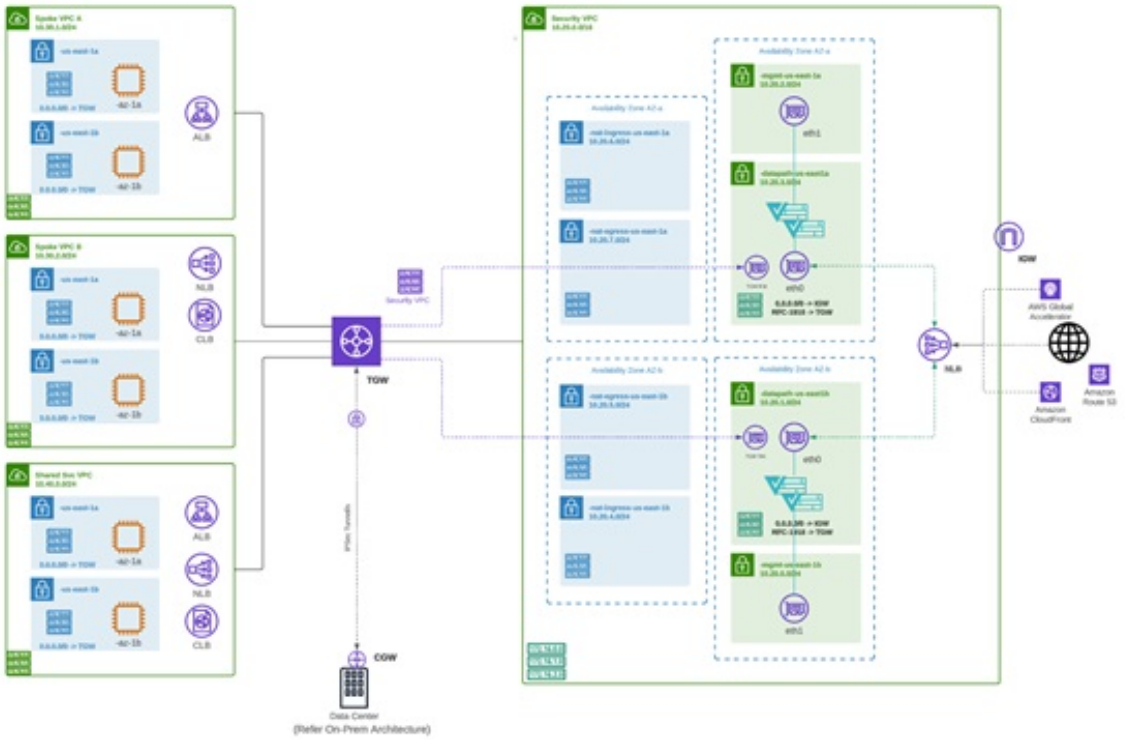
다음 다이어그램은 중앙 집중식 모드의 이그레스 게이트웨이가 있는 AWS 계정의 예입니다.



인그레스

인그레스 게이트웨이를 구축하면 공용으로 연결되는 애플리케이션이 보호됩니다. 인그레스 게이트웨이는 전체 암호 해독을 수행하고 침입 방지, 악성코드 차단, WAF(Web Application Firewall), 전체 경로 URL 필터링과 같은 고급 보안 기능을 적용하는 역방향 프록시 역할을 합니다.

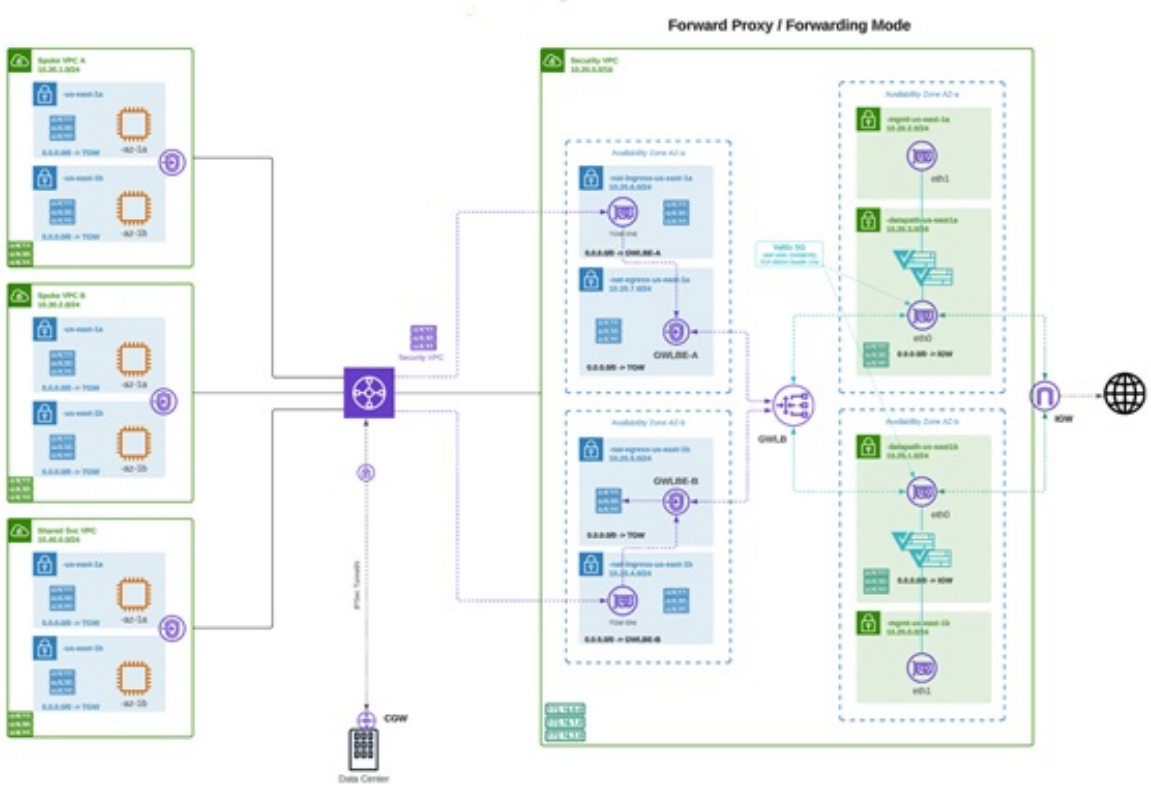
다음 다이어그램은 중앙 집중식 모드의 인그레스 게이트웨이가 있는 AWS 계정의 예입니다.



East-West

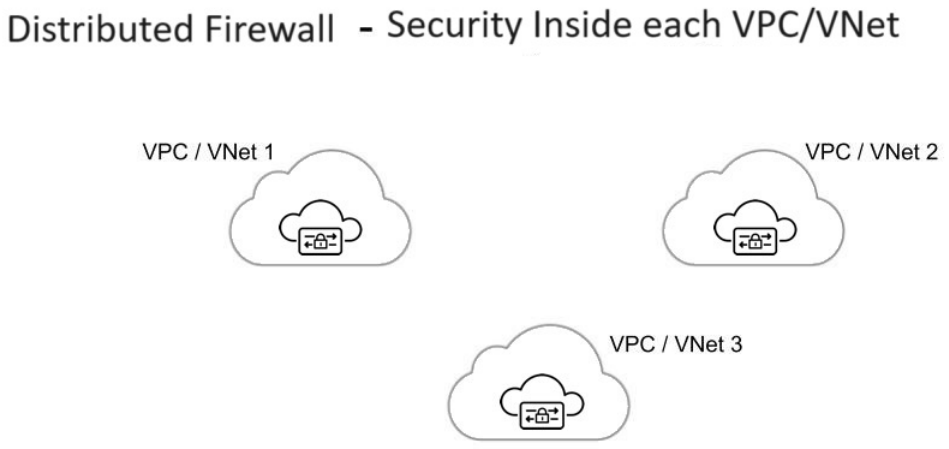
이그레스/이스트-웨스트 게이트웨이 구축은 퍼블릭 클라우드 환경 내에서 서브넷 또는 VPC/Vnet 간에 이스트-웨스트 L4 세분화를 구현합니다. 게이트웨이는 L4 방화벽 규칙을 통해 전달 모드로 작동하여 선택적 로깅이 활성화된 상태에서 설정된 매개변수를 기반으로 트래픽을 허용하거나 거부합니다.

다음 다이어그램은 중앙 집중식 모드의 이스트-웨스트 게이트웨이가 있는 AWS 계정의 예입니다.



분산화

여러 VPC/VNet에서 애플리케이션을 실행 중입니다. 각 VPC/VNet에 멀티 클라우드 방어 게이트웨이을(를) 구축합니다.



중앙 집중식/허브

여러 VPC/VNet에서 애플리케이션을 실행 중입니다. 중앙 집중식 보안 서비스 VPC/VNet을 통해 모든 애플리케이션을 보호하려고 합니다. 이 모델은 서비스 VPC에 멀티 클라우드 방어 게이트웨이를 구축합니다. 모든 애플리케이션 VPC(스포크 VPC)와 서비스 VPC를 Azure 및 GCP의 AWS Transit Gateway 또는 VNet/VPC 피어링에 연결합니다. 멀티 클라우드 방어는 AWS Transit Gateway, 서비스 VPC 및 스포크 VPC 첨부 파일을 오케스트레이션하는 옵션을 제공합니다. 이 솔루션은 여러 경로 테이블 및 Transit Gateway 첨부 파일의 복잡성을 제거하여 손쉽게 구축할 수 있는 권장 솔루션입니다.

Figure 1: AWS - AWS Transit Gateway 사용

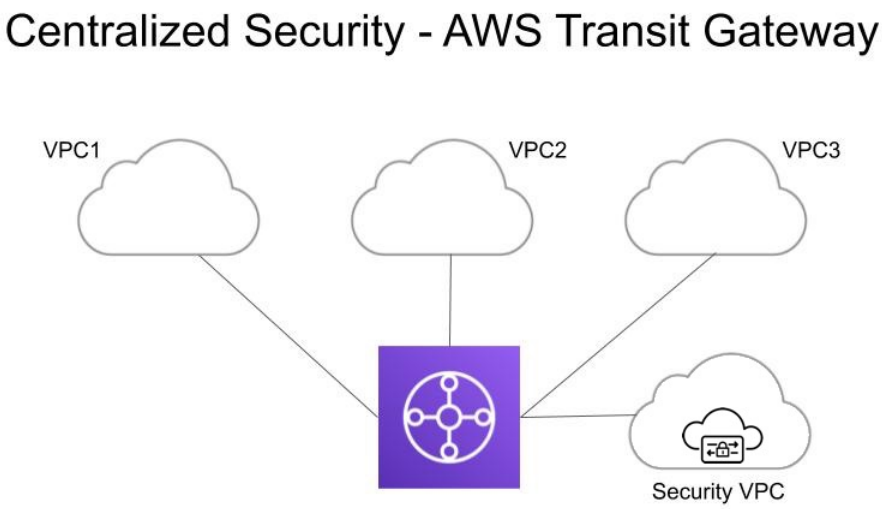


Figure 2: Azure - VNet 피어링

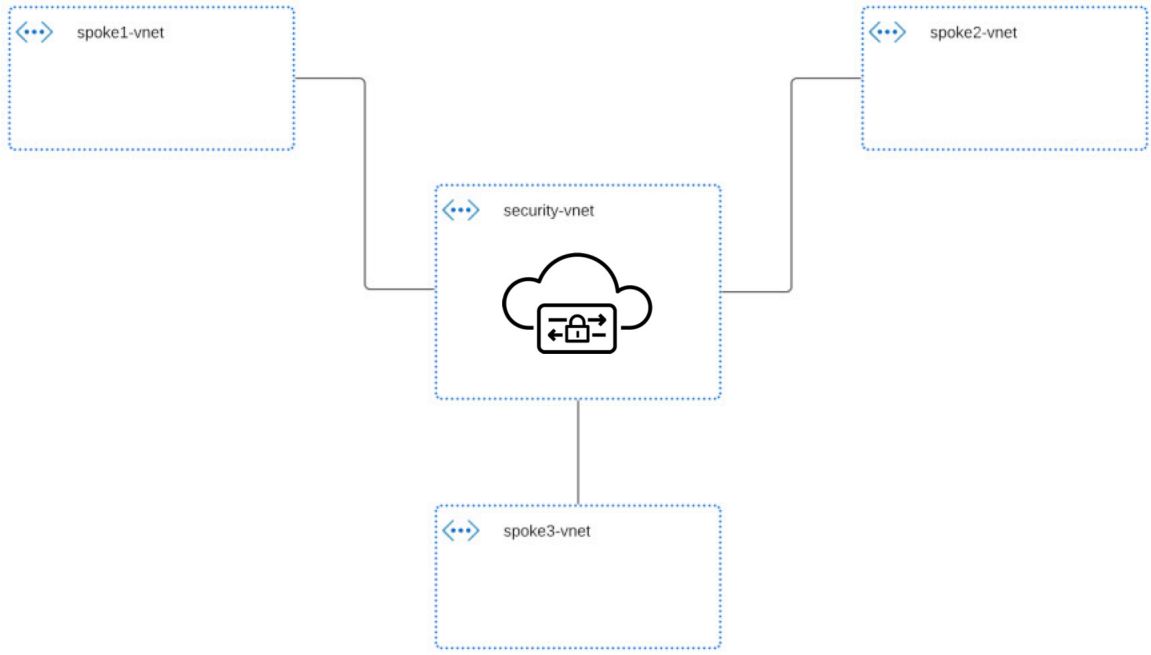
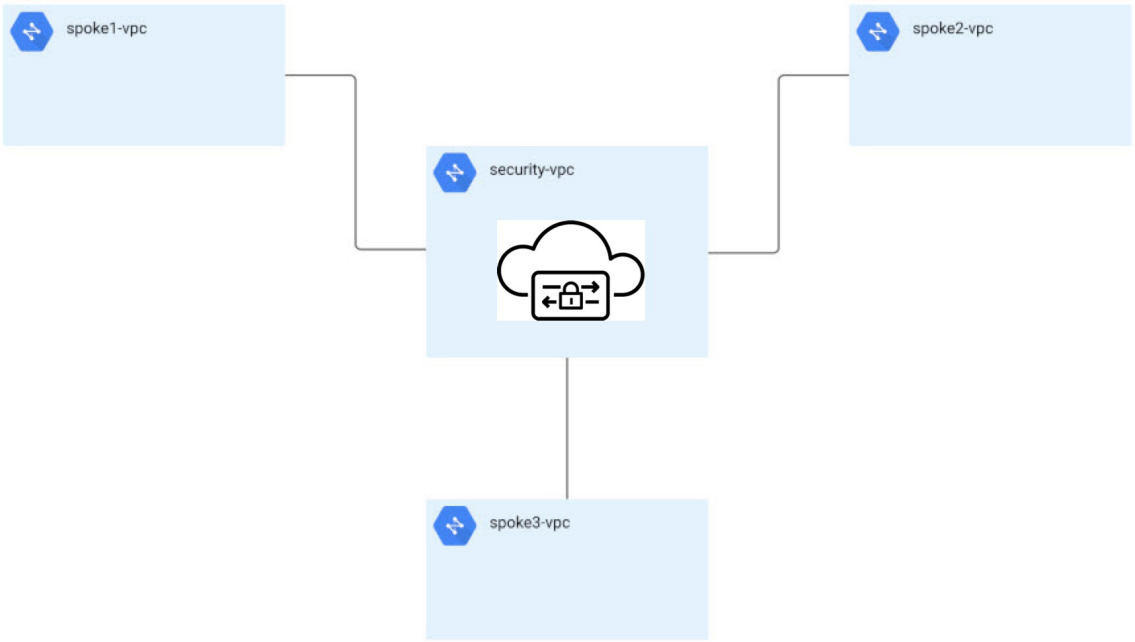


Figure 3: GCP - VPC 피어링



고급 활용 사례

일부 게이트웨이의 경우 추가 사전 요건 또는 사후 절차 단계가 있을 수 있습니다. 다음 환경을 고려하십시오.

AWS: 인그레스 게이트웨이에 대한 가속기

멀티 클라우드 방어는 멀티 클라우드 방어 게이트웨이 인스턴스 전체에서 트래픽을 로드 밸런싱하는 하나 이상의 AWS 글로벌 액셀러레이터 세트와 통합하여 인그레스 포인트로 사용할 수 있습니다. 이는 인그레스 게이트웨이가 구축될 때 멀티 클라우드 방어에서 생성 및 관리하는 AWS 네트워크 로드 밸런서와 유사하지만, 애플리케이션 및 워크로드를 보호하기 위해 인그레스 게이트웨이에 대체 인그레스 포인트를 제공합니다.

가속기를 사용하는 경우, 전역 가속기의 리스너 엔드포인트 그룹을 관리하여 엔드포인트 그룹에 활성 게이트웨이 인스턴스 집합이 있는지 확인합니다. 클라이언트 IP 주소는 멀티 클라우드 방어 인그레스 게이트웨이로 전역 가속기를 통과할 때 유지됩니다.

멀티 클라우드 방어를 전역 가속기와 통합하려면 사용자는 먼저 AWS 내에 전역 가속기를 생성하고, 원하는 리스너를 정의한 다음 빈 엔드포인트 그룹(또는 기존 멀티 클라우드 방어 인그레스 게이트웨이 인스턴스를 포함하는 엔드포인트 그룹)을 생성해야 합니다. AWS 리소스가 있으면 글로벌 가속기와 통합하도록 멀티 클라우드 방어 인그레스 게이트웨이를 구성할 수 있습니다.

게이트웨이 세부 정보

이미 설정된 게이트웨이에 대한 **Gateway Details(**게이트웨이 세부 정보**)** 페이지를 보는 방법은 **Manage(**관리**)** > **Gateways(**게이트웨이**)**에서 이미 설정한 게이트웨이를 사용할 수 있습니다. 이 페이지에서 모든 게이트웨이를 추가하고 관리할 수 있습니다. 게이트웨이를 관리하면 인스턴스를 편집, 업그레이드, 활성화, 비활성화, 내보내기 또는 삭제할 수 있습니다. 변경하기 전에 수정할 게이트웨이의 확인란을 클릭해야 합니다.

참고 이러한 작업을 수행하려면 관리자 또는 슈퍼 관리자여야 합니다.

다음 기준을 사용하여 게이트웨이 목록을 필터링하고 검색하려면 다음 항목 중 하나를 사용할 수 있습니다.

- **Name(**이름**)** - 게이트웨이의 이름입니다.
- **CSP Account(CSP** 계정**)** - 게이트웨이와 연결된 클라우드 서비스 제공자 계정입니다.
- **CSP Type(CSP** 유형**)** - 클라우드 서비스 제공자 계정의 유형입니다.
- **Region(**지역**)** - 검색 중인 게이트웨이와 연결된 클라우드 서비스 제공자의 지역입니다.
- **State(**상태**)** - 게이트웨이의 현재 상태입니다. 게이트웨이는 활성 또는 비활성, 또는 보류 중인 활성 또는 보류 중인 비활성 상태일 수 있습니다.
- **Instance Type(**인스턴스 유형**)** - 각 클라우드 서비스 제공자는 여러 인스턴스 유형을 지원합니다.
- **Mode(**모드**)** - 허브 또는 엣지 모드에서 멀티 클라우드 방어 게이트웨이 인스턴스를 구축할 수 있습니다.

Switch to Advanced Search(고급 검색으로 전환**)**를 클릭하여 검색을 직접 구성합니다. 필요한 경우 검색 창의 드롭다운 옵션을 사용하여 자동 생성된 검색 기준을 활용합니다. 를 반복해야 하는 검색의 경우 나중에 사용할 수 있도록 검색을 복사하거나 저장할 수 있습니다.

멀티 클라우드 방어 게이트웨이 및 **VPC/VNet** 구성

시작하기 전에

지원되는 클라우드 서비스 제공자는 고유한 용어 및 게이트웨이 환경을 사용하는 별도의 엔터티입니다. 멀티 클라우드 방어 컨트롤러에서 사용 가능한 모든 옵션이 클라우드 서비스 제공자와 호환되는 것은 아닙니다. 예를 들어 AWS는 자체 Transit 게이트웨이를 사용하며 사용자는 VPC를 추가할 수 있으며 Azure에서는 로드 밸런서를 사용하여 웹 트래픽 및 애플리케이션을 관리하며 사용자는 여기에 VNet을 추가할 수 있습니다. 계속 진행할 때 이 점에 유의하십시오.

참고 AWS 환경의 경우 중앙 집중식 모드에서 스포크 VPC를 보호할 때 멀티 클라우드 방어은 VPC를 서비스 VPC와 연결된 Transit Gateway에 연결합니다. 기본적으로 멀티 클라우드 방어은(는) Transit Gateway 연결에 대해 각 가용성 영역에서 서브넷을 무작위로 선택합니다. VPC를 추가할 때 이 옵션을 변경할 수도 있고, 게이트웨이에 이미 할당된 VPC를 수정할 수도 있습니다.

멀티 클라우드 방어 게이트웨이를 통해 Transit Gateway를 오케스트레이션하거나 기존 Transit Gateway를 연결할 수도 있습니다.

제한 사항

멀티 클라우드 방어 게이트웨이를 생성할 때 다음 제한 사항에 유의합니다.

- IPSec 프로파일이 포함된 사이트 간 VPN 터널을 사용하는 멀티 클라우드 방어 게이트웨이을 구축하는 경우, VPN 연결의 양쪽에 NAT(Network Address Translation) 게이트웨이 없이 서비스 VPC 또는 서비스 VNet을 사용하여 게이트웨이를 구축해야 합니다.
- IPSec 프로파일을 포함하는 게이트웨이에 대해서는 Autoscaling이 지원되지 않습니다.
- 게이트웨이 내의 정책 규칙은 전달 전용이어야 합니다.
- AWS 또는 Azure 어카운트에 대한 멀티 클라우드 방어 게이트웨이에 IPSec 프로파일을 포함하려면 코어 8 로 게이트웨이 인스턴스를 설정 해야 합니다. 멀티 클라우드 방어 게이트웨이는 현재 코어 2 또는 코어 4 옵션이 있는 게이트웨이를 지원하지 않습니다.

멀티 클라우드 방어에서 생성한 리소스

다음 리소스는 게이트웨이, VPC 또는 VNet을 생성할 때 멀티 클라우드 방어에 의해 생성됩니다. 이러한 프로세스의 일부로 생성되며 사용자의 추가 작업이 필요하지 않습니다. 각 클라우드 서비스 제공자 요구 사항에 따라 다른 리소스가 생성됩니다.

GCP 리소스

멀티 클라우드 방어은(는) 2개의 서비스 VPC와 4개의 방화벽을 생성합니다. 정확한 리소스 할당은 다음을 참조하십시오.

Service VPC(서비스 **VPC)**

- 관리
- 데이터 경로

방화벽 규칙

- 관리(인그레스)
- 관리(이그레스)
- 데이터 경로(이그레스)
- 데이터 경로(이그레스)

참고 서비스 VPC CIDR은 스포크 VPC와 중복될 수 없습니다.

AWS 리소스

멀티 클라우드 방어은(는) 지원되는 활용 사례(인그레스, 이그레스/이스트-웨스트)를 처리하기 위해 3개의 서비스 VPC를 생성합니다. 각 VPC는 다음과 같이 생성되고 연계됩니다.

- 각 가용성 영역에 4개의 서브넷.
- 각 서브넷에 경로 테이블 1개.
- 보안 그룹 2개: 관리 및 데이터 경로.
- Transit 게이트웨이 1개.

참고 이 Transit 게이트웨이는 서비스 VPC 생성 중에 생성되어 게이트웨이에 연결됩니다. 이 게이트웨이는 다른 서비스 VPC와 함께 재사용할 수 있습니다.

- Transit 게이트웨이 경로 테이블.

참고 경로 테이블은 생성 프로세스의 일부로 서비스 VPC에 연결됩니다.

참고 AWS 게이트웨이 로드 밸런서(GWLB)는 GWLB의 초기 구축 후 가용성 영역 추가/제거를 지원하지 않습니다. 가용성 영역을 변경해야 하는 경우 서비스 VPC를 다시 구축해야 합니다. 자세한 내용은 AWS 설명서를 참조하십시오.

Azure 리소스

멀티 클라우드 방어에서 다음 리소스로 하나의 서비스 VNet을 생성했습니다.

- VNet 1개.
- 네트워크 보안 그룹 2개.

서비스 VNet CIDR 값은 스포크 VNet과 겹치지 않아야 합니다.

서비스 **VPC** 또는 **VNet** 생성

다음 절차에 따라 생성하려는 게이트웨이에 따라 서비스 VPC 또는 서비스 VNet을 생성합니다. 클라우드 서비스 제공자에게 있는 옵션을 확인하십시오.

단계 **1** 멀티 클라우드 방어 컨트롤러에서 **Manage(**관리**)** > **Service VPCs/VNets(**서비스 **VPC/VNets)**로 이동합니다.

단계 **2** **Create Service VPC/VNet(**서비스 **VPC/VNet** 생성**)**을 클릭합니다.

단계 **3** 입력 매개변수 값:

- **Name(**이름**)** -서비스 VPC/VNet에 이름을 할당합니다.
- **CSP Account(CSP** 계정**)** - 서비스 VPC/VNet을 생성할 CSP 계정을 선택합니다.
- **Region(**지역**)** - 이 서비스 VPC 를 구축할 지역을 선택합니다.
- (Azure 전용) **CIDR Block(CIDR** 블록**)** - 서비스 VNet의 CIDR 블록입니다. 스포크(애플리케이션) VNet과 겹치지 않아야 합니다.
- (AWS/GCP 전용) **Datapath CIDR Block(**데이터 경로 **CIDR** 블록**)** - 멀티 클라우드 방어 게이트웨이 데이터 경로 서비스 VPC에 대한 CIDR 블록입니다. 이 CIDR 블록은 스포크(애플리케이션) VPC의 주소 범위와 중복되지 않아야 합니다.
- (AWS/GCP 전용) **Management CIDR Block(**관리 **CIDR** 블록**)** - 멀티 클라우드 방어 게이트웨이 관리 서비스 VPC에 대한 CIDR 블록입니다. 이 CIDR 블록은 스포크(애플리케이션) VPC의 주소 범위와 중복되지 않아야 합니다.
- **Availability Zones(**가용성 영역**)** - VPC를 생성하는 경우에는 하나 의 가용성 영역만 구성해야 합니다. VNet의 경우 멀티 클라우드 방어에서는 복원력을 위해 최소 두 개의 가용성 영역을 선택하는 것이 좋습니다.
- (Azure 전용) **Resource Group(**리소스 그룹**)** - 서비스 VNet을 구축할 리소스 그룹입니다.
- (AWS 전용)**Transit Gateway** - Transit Gateway는 중앙 허브를 통해 가상 프라이빗 클라우드와 온프레미스 네트워크를 연결합니다. 드롭다운 메뉴를 사용하여 이 VPC에 대한 기존 게이트웨이를 선택합니다. 선택할 기존 게

이트웨이가 없는 경우 **Create_new(**새로 생성**)**를 선택합니다. 이 옵션을 사용하면 멀티 클라우드 방어가 VPC 생성 프로세스의 일부로 하나를 생성할 수 있습니다.

- (AWS 전용) **Transit Gateway Name(Transit Gateway** 이름**)** - 새 트랜짓 게이트웨이를 생성하도록 선택한 경우 이 필드에 게이트웨이의 이름을 입력합니다.
- (AWS에만 해당) **Auto accept shared attachments(**공유 첨부 파일 자동 수락**)** - 새 트랜짓 게이트웨이를 생성하지 않고 다중 어카운트 허브 게이트웨이 구축에 이 VPC를 사용하려는 경우, 이 옵션을 선택합니다.
- **Use NAT Gateway(NAT** 게이트웨이 사용**)** - 모든 이그레스 트래픽이 NAT 게이트웨이를 통과하도록 하려면 이 옵션을 활성화합니다.

  주의 이 서비스 VPC를 구축하여 AWS에서 멀티 클라우드 방어 VPN 게이트웨이를 구축하려는 경우 이 NAT 게이트웨이 옵션을 활성화하지 마십시오.

다음에 수행할 작업

멀티 클라우드 방어 게이트웨이 추가.

멀티 클라우드 방어 게이트웨이 추가

다음 절차에 따라 클라우드 서비스 제공자용 멀티 클라우드 방어 게이트웨이을 추가합니다.

단계 **1** **Manage(**관리**)** > **Gateways(**게이트웨이**)**로 이동합니다.

단계 **2** **Add Gateway(**게이트웨이 추가**)**를 클릭합니다.

단계 **3** 게이트웨이를 추가할 클라우드 서비스 제공자를 선택합니다.

단계 **4** **Next(**다음**)**를 클릭합니다.

단계 **5** 다음 정보를 입력합니다.

- **Instance Type(**인스턴스 유형**)** - 클라우드 서비스 제공자의 유형을 선택합니다. 사용 중인 클라우드 서비스 제공자에 따라 인스턴스의 여러 변형이 있을 수 있습니다.
- **Gateway Tpe(**게이트웨이 유형**)** - Ingress(인그레스) 또는 Egress(이그레스)를 선택합니다.

  참고 이스트-웨스트 네트워크 플로우가 있는 경우 **Egress(**이그레스**)**를 선택합니다.

- **Minimum Instances(**최소 인스턴스**)** - 구축하려는 최소 인스턴스 수를 선택합니다.
- **Maximum Instances(**최대 인스턴스**)** - 구축하려는 최대 인스턴스 수를 선택합니다. 이는 각 가용성 영역에서 자동 확장에 사용되는 최대 수입니다.
- **HealthCheck Port(HealthCheck** 포트**)** - 기본값은 65534입니다. 멀티 클라우드 방어 로드 밸런서에서 인스턴스의 상태를 확인하는 데 사용하는 포트 번호입니다. 인스턴스에 할당된 데이터 경로 보안 그룹은 이 포트에서 트래픽을 허용해야 합니다.

- (선택 사항) **Packet Capture Profile(**패킷 캡처 프로파일**)** - 위협 및 플로우 PCAP에 대한 패킷 캡처 프로파일입니다.
- (선택 사항) **Diagnostics Profile(**진단 프로파일**)** - 기술 지원 정보를 저장하는 데 사용되는 진단 프로파일입니다.
- (선택 사항) **Log Profile(**로그 프로파일**)** - 이벤트/로그를 SIEM으로 전달하는 데 사용되는 로그 전달 프로파일입니다.
- (선택 사항) **NTP Profile(NTP** 프로파일**)** - 시간 동기화를 위한 NTP(Network Time Protocol).
- (선택 사항) **BGP profile(BGP** 프로파일**)** - VPN 연결을 지원하는 데 사용되는 BGP(Border Gateway Protocol). 멀티 클라우드 방어 게이트웨이를 사용하여 사이트 간 VPN 터널을 생성하려면 이 프로파일을 포함해야 합니다.

단계 **6** **Next(**다음**)**를 클릭합니다.

단계 **7** 다음 매개변수를 제공합니다.

- **Security** (보안) - Egress(이그레스) 또는 Ingress(인그레스)를 선택합니다.

  참고 이스트-웨스트 네트워크 플로우가 있는 경우 **Egress(**이그레스**)**를 선택합니다.

- **Gateway Image(**게이트웨이 이미지**)** - 구축할 이미지.
- **Policy Ruleset(**정책 규칙 집합**)** - 이 게이트웨이와 연결할 정책 규칙 집합을 선택합니다.
- **Region(**지역**)** - 이 게이트웨이를 구축할 지역을 선택합니다.
- **Resource Groups(**리소스 그룹**)** - 게이트웨이를 연결할 리소스 그룹을 선택합니다.
- **SSHPublic Key(SSH** 공용 키**)** - SSH 공개 키를 붙여넣습니다. 이 공개 키는 컨트롤러에서 디버그 및 모니터링을 위해 구축된 게이트웨이 인스턴스의 CLI에 액세스하는 데 사용됩니다.
- **VNet ID** - 게이트웨이와 연결할 VNet을 선택합니다.
- **User Assigned Identity ID(**사용자 할당 **ID)** - 이 게이트웨이와 연결할 클라우드 서비스 제공자 ID를 입력합니다.
- **Mgmt. Security Group(**관리 보안 그룹**)** - 관리 인터페이스와 연결할 보안 그룹을 선택합니다.
- **Datapath Security Group(**데이터 경로 보안 그룹**)** - 데이터 경로 인터페이스와 연결할 보안 그룹을 선택합니다.
- **Disk Encryption(**디스크 암호화**)** - 드롭다운 메뉴에서 적절한 옵션을 선택합니다. 고객 관리 암호화 키의 경우, 사용자는 암호화 키의 리소스 ID를 입력해야 합니다.

단계 **8** **Availability Zone(**가용성 영역**)**, **Mgmt Subnet(**관리 서브넷**)** 및 **Datapath Subnet(**데이터 경로 서브넷**)**을 선택합니다. 사용 가능한 서브넷은 위에서 선택한 VPC 또는 VNet을 기반으로 합니다. 고가용성을 위해 게이트웨이 인스턴스를 여러 가용성 영역에 구축할 수 있습니다. 더하기 버튼을 클릭하여 새 가용성 영역을 추가하고 선택한 영역에 대한 매개변수를 선택합니다.

참고 일부 클라우드 서비스 제공자 지역은 다중 가용성 영역을 지원하지 않습니다. 이러한 지역에서는 게이트웨이 인스턴스가 단일 영역에만 구축됩니다.

단계 **9** (Azure 전용, 선택 사항) 애플리케이션과 동일한 VNet에서 멀티 클라우드 방어 게이트웨이을(를) 사용하여 분산형 모델을 구축하는 경우 다음을 완료해야 합니다.

- Azure 포털에서 경로 테이블을 추가하고 모든 서브넷에 경로 테이블을 연결합니다.
- **next-hop**을 게이트웨이 네트워크 로드 밸런서의 IP 주소로 사용하는 0.0.0.0/0에 대한 기본 경로를 추가합니다.

단계 **10** 고급 설정을 보려면 **Next(**다음**)**를 클릭합니다.

단계 **11** 기본적으로 멀티 클라우드 방어 게이트웨이는 사용 가능한 라우터의 공용 IP 사용을 활성화합니다. 이 기능을 활성화하지 않으려면 **Disable Public IP(**공용 **IP** 비활성화**)** 확인란을 선택합니다.

단계 **12** **Save(**저장**)**를 클릭합니다. 멀티 클라우드 방어는 게이트웨이를 구축합니다.

다음에 수행할 작업

스포크 VPC/VNet을 보호하기 전에 게이트웨이에 하나 이상의 규칙 집합을 연결해야 합니다. 자세한 내용은 규칙 집합 및 규칙 집합 그룹, 96 페이지를 참조하십시오.

서비스 메뉴의 보안 스포크 **VPC/VNet**

다음 절차를 사용하여 서비스 메뉴에서 스포크 VPC 또는 스포크 VNet을 게이트웨이에 추가합니다.

시작하기 전에

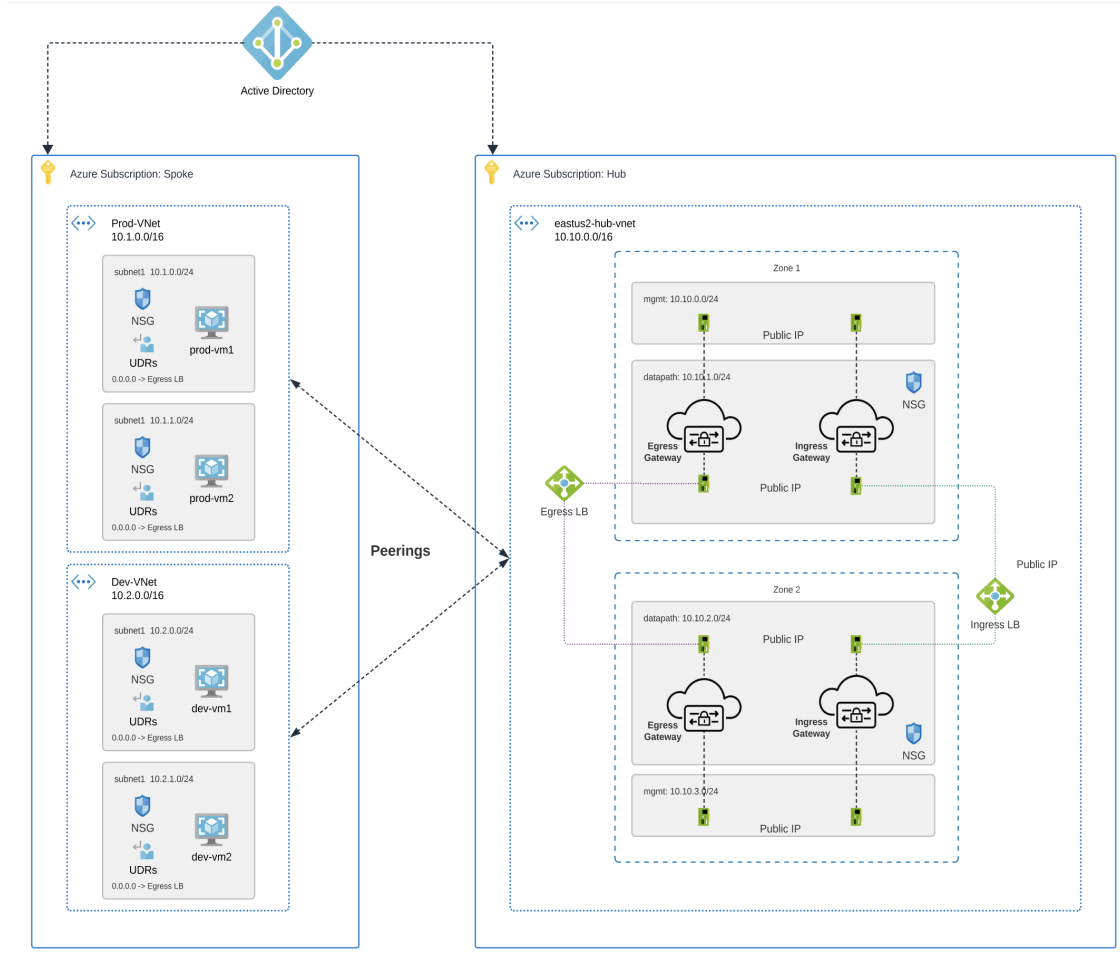
스포크 VPC 또는 VNet을 생성하고 할당하기 전에 다음 작업을 수행해야 합니다.

- AWS 및 GCP 계정에서는 게이트웨이를 추가하기 전에 원격 계정을 보호해야 합니다.
- Azure 환경에서는 스포크 VPC/VNet을 보호하기 전에 경로 테이블을 연결해야 합니다. 자세한 내용은 Azure 사용자 가이드의 "경로 테이블을 서브넷에 연결" 장을 참조하십시오.

중앙 집중식 모델에서 VPC로 AWS 스포크를 보호하는 경우, 멀티 클라우드 방어은(는) 서비스 VPC에 연결된 Transit 게이트웨이에 VPC를 연결합니다. VPC를 Transit 게이트웨이에 연결할 때 사용자는 ENI를 배치할 각 가용성 영역의 서브넷을 선택할 수 있습니다. 기본적으로 멀티 클라우드 방어은(는) Transit Gateway 연결에 대해 각 가용성 영역에서 서브넷을 무작위로 선택합니다.

VNet 페어링은 동일한 CSP 유형 내의 계정 간에 지원됩니다. 계정 내에서 그리고 계정 간에 스포크 VPC/VNet을 추가할 수 있습니다. Azure의 구독 간 스포크 VPC 피어링의 경우 동일한 앱 등록을 사용하여 CSP 계정을 온보딩해야 하며 구독은 동일한 Active Directory 내에 있어야 합니다.

그림 ***4: Azure*** 결합 허브 **-** 다중 구독



단계 **1** 멀티 클라우드 방어 컨트롤러 대시보드에서 **Manage(**관리**)** > **Service VPCs/VNets(**서비스 **VPC/VNets)**로 이동합니다.

단계 **2** Service VPC(서비스 VPC) 또는 Service VNet(서비스 VNet)을 선택하고 **Actions(**작업**)** > **Manage Spoke VPC/VNet(**스포크 **VPC/VNet** 관리**)**으로 이동합니다.

단계 **3** 모든 스포크 VPC 또는 VNet을 추가하여 스포크 테이블을 보호합니다.

Spoke VNets for Current Account(현재 계정에 대한 스포크 **VNets)**에서 스포크 VPC 또는 VNets을 선택할 수 있습니다. 다른 계정의 스포크 VPC 또는 VNets를 추가하려면 **Spoke VNet for Other Accounts(**다른 계정에 대한 스포크 **VNet)**를 선택합니다.

단계 **4** Route Tables(경로 테이블) 열에서 **View/Edit(**보기/편집**)** 링크를 클릭합니다.

단계 **5** 검사를 위해 멀티 클라우드 방어 게이트웨이을(를) 가리키도록 기본 경로를 업데이트하려면 **Send Traffic via** 멀티 클라우드 방어 **Gateway(**멀티 클라우드 게이트웨이를 통해 트래픽 전송**)** 확인란을 선택합니다.

단계 **6** **Update routes(**경로 업데이트**)**를 클릭합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

게이트웨이 관리

관리자 > 게이트웨이에서 멀티 클라우드 방어 게이트웨이 및 통계를 봅니다. 이 페이지에서 게이트웨이를 검색 및 필터링하고, 각 게이트웨이와 관련된 클라우드 서비스 제공자, 현재 인스턴스 수 및 유형 등을 볼 수 있습니다.

특정 게이트웨이 환경에서 지원되는 활용 사례에 대한 자세한 내용은 지원되는 게이트웨이 활용 사례, 70 페이지를 참조하십시오.

멀티 클라우드 방어 게이트웨이 편집

활성화 또는 비활성화 여부에 상관없이 모든 상태의 게이트웨이를 편집할 수 있습니다. 다음 절차에 따라 기존 멀티 클라우드 방어 게이트웨이을 편집합니다.

단계 **1** **Manage(**관리**)** > **Gateways(**게이트웨이**)**로 이동합니다.

단계 **2** 테이블에서 편집할 멀티 클라우드 방어 게이트웨이를 선택하여 강조 표시합니다.

단계 **3** **Actions(**작업**)** 드롭다운 메뉴를 확장하고 **Edit(**편집**)**를 선택합니다.

단계 **4** 필요에 따라 게이트웨이 구성을 수정합니다.

단계 **5** **Save(**저장**)**를 클릭하여 변경 사항을 확인합니다. 또는 변경을 취소하려면 **Cancel(**취소**)**을 클릭합니다.

멀티 클라우드 방어 게이트웨이 업그레이드

멀티 클라우드 방어 게이트웨이는 자동 확장 자동 복구 PaaS(Platform-as-a-Service)로 작동하고 인라인 네트워크 기반 보안 시행 노드로 작동합니다. 기존 방화벽과 달리 멀티 클라우드 방어에서는 고객이 가상 방화벽을 구성하거나 고가용성 설정을 구성하거나 소프트웨어 설치를 관리할 필요가 없습니다.

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 업그레이드를 수행할 수 있습니다.

새 인스턴스가 새 이미지와 함께 회전합니다. 인스턴스는 완전히 가동되면 로드 밸런서(게이트웨이 인스턴스로의 플로우의 레이어 4 스프레이어)의 대상 풀에 배치됩니다. 기존 인스턴스는 이를 통과하는 기존 플로우에 대해 플로우 배수 모드 또는 플로우 시간 초과 모드가 됩니다. 새 플로우는 새 인스턴스에 적용됩니다. 시간 초과(Azure) 또는 플로우가 드레인(AWS)되면 컨트롤러에서 기존 인스턴스를 가져옵니다.

다음 절차를 사용하여 수행할 수 있습니다.

단계 **1** **Manage(**관리**)** > **Gateways(**게이트웨이**)**로 이동합니다.

단계 **2** 업그레이드할 게이트웨이의 확인란을 선택합니다. 현재 하나의 항목만 선택할 수 있습니다.

단계 **3** **Actions(**작업**)** > **Upgrade(**업그레이드**)**를 선택합니다.

단계 **4** **Gateway Image(**게이트웨이 이미지**)** 목록에서 원하는 이미지를 선택합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

단계 **6** 업그레이드에 필요한 클라우드 서비스 제공자 리소스 할당을 확인합니다.

단계 **7** 리소스 할당이 충분하면 **Yes(**예**)**를 클릭합니다. 리소스 할당이 충분하지 않은 경우 **No(**아니요**)**를 클릭하고 클라우드 서비스 제공자의 리소스 할당을 늘린 다음 돌아가서 업그레이드를 계속합니다.

Note 게이트웨이의 인스턴스 정보에서 업그레이드 진행 상황 및 새 게이트웨이 인스턴스를 볼 수 있습니다. 게이트웨이를 선택하고 Details(세부 사항) 창에서 **Instances(**인스턴스**)**를 확인합니다.

멀티 클라우드 방어 게이트웨이 중단

현재 게이트웨이 업데이트가 진행 중인 멀티 클라우드 방어 게이트웨이만 중단할 수 있습니다.

기존 멀티 클라우드 방어 게이트웨이를 중단하려면 다음 절차를 사용합니다.

단계 **1** **Manage(**관리**)** > **Gateways(**게이트웨이**)**로 이동합니다.

단계 **2** 테이블에서 중단하려는 멀티 클라우드 방어 게이트웨이를 선택하여 강조 표시합니다.

단계 **3** **Actions(**작업**)** 드롭다운 메뉴를 확장하고 **Abort(**중단**)**를 선택합니다.

단계 **4** 게이트웨이 중단을 확인하고 **Yes**(예)를 클릭합니다. 작업을 취소하려면 **No(**아니요**)**를 클릭합니다.

멀티 클라우드 방어 게이트웨이을 활성화

비활성화된 게이트웨이만 활성화할 수 있습니다. 다음 절차에 따라 활성화합니다.

단계 **1** **Manage(**관리**)** > **Gateways(**게이트웨이**)**로 이동합니다.

단계 **2** 표에서 활성화하려는 멀티 클라우드 방어 게이트웨이를 선택하여 강조 표시합니다.

단계 **3** **Actions(**작업**)** 드롭다운 메뉴를 확장하고 **Enable(**활성화**)**을 선택합니다.

단계 **4** 멀티 클라우드 방어은 게이트웨이 구성을 검증합니다. 검증에 성공하면 검토를 위해 업그레이드에 대한 현재 및 필수 리소스의 표가 생성됩니다. 게이트웨이 리소스 할당을 승인하는 경우 **Yes(**예**)**를 클릭하여 작업을 확인합니다.

다음에 수행할 작업

멀티 클라우드 방어 게이트웨이이 성공적으로 활성화될 때까지 몇 분 정도 기다립니다.

멀티 클라우드 방어 게이트웨이를 비활성화하고 연결된 사이트 간 VPN 터널을 삭제한 경우, 새 사이트 간 VPN 터널 연결을 생성해야 하거나 이전 VPN 터널 연결을 다시 생성한 다음 게이트웨이에 추가해야 합니다. 게이트웨이가 비활성화되면 멀티 클라우드 방어은 VPN 터널과 연결된 공용 IP 주소를 무시합니다. 게이트웨이 인스턴스에 대해 새 IP를 설정하려면 새 터널 연결을 생성해야 합니다.

멀티 클라우드 방어 게이트웨이 비활성화

멀티 클라우드 방어 게이트웨이가 현재 활성화되어 있는 경우에만 비활성화할 수 있습니다. 이미 비활성화된 게이트웨이는 비활성화할 수 없습니다.

다음 절차에 따라 멀티 클라우드 방어 게이트웨이를 비활성화합니다.

단계 **1** **Manage(**관리**)** > **Gateways(**게이트웨이**)**로 이동합니다.

단계 **2** 표에서 중단하려는 멀티 클라우드 방어 게이트웨이를 선택하여 강조 표시합니다.

단계 **3** **Actions(**작업**)** 드롭다운 메뉴를 확장하고 **Disable(**비활성화**)**를 선택합니다.

단계 **4** 게이트웨이를 비활성화할 것인지 확인하고 **Yes**(예)를 클릭합니다. 이 작업을 취소하려면 **No(**아니요**)**를 클릭합니다.

다음에 수행할 작업

게이트웨이가 성공적으로 비활성화될 때까지 몇 분 정도 기다립니다.

게이트웨이를 완전히 비활성화하려면 게이트웨이와 연계된 모든 사이트 간 VPN 터널을 삭제해야 합니다.

멀티 클라우드 방어 게이트웨이 내보내기

다음 절차에 따라 멀티 클라우드 방어 게이트웨이의 구성을 내보냅니다.

단계 **1** **Manage(**관리**)** > **Gateways(**게이트웨이**)**로 이동합니다.

단계 **2** 표에서 내보내려는 멀티 클라우드 방어 게이트웨이을 선택하여 강조 표시합니다.

단계 **3** **Actions(**작업**)** 드롭다운 메뉴를 확장하고 **Export(**내보내기**)**를 선택합니다.

단계 **4** 멀티 클라우드 방어이 내보내기 마법사를 생성합니다.

단계 **5** **Download(**다운로드**)**를 클릭하여 terraform을 로컬로 다운로드하거나 아래로 스크롤하여 **Copy Code(**코드 복사**)**를 클릭하여 JSON 리소스를 복사합니다.

단계 **6** Terraform 스크립트에 수동으로 붙여넣습니다.

단계 **7** terraform 프롬프트에서 창 하단에 있는 명령을 실행합니다. `terraform import "ciscomcd_gateway"."object-name" <object name>`.

단계 **8** Terraform 프롬프트의 프롬프트에 따라 작업을 완료합니다. 멀티 클라우드 방어에서 내보내기 창을닫습니다**.** 대시보드에 더 이상 단계가 없습니다.

멀티 클라우드 방어 게이트웨이 삭제

다음 절차에 따라 멀티 클라우드 방어 게이트웨이을 삭제합니다. 이 작업은 게이트웨이 비활성화와 다릅니다.

단계 **1** **Manage(**관리**)** > **Gateways(**게이트웨이**)**로 이동합니다.

단계 **2** 표에서 중단하려는 멀티 클라우드 방어 게이트웨이를 선택하여 강조 표시합니다.

단계 **3** **Actions(**작업**)** 드롭다운 메뉴를 확장하고 **Delete(**삭제**)**를 선택합니다.

단계 **4** 작업을 확인하고 **Yes(**예**)**를 클릭합니다. 삭제 작업을 취소하려면 **Cancel(**취소**)**을 클릭합니다.

다음에 수행할 작업

이 게이트웨이와 연결된 사이트 간 VPN 터널 연결은 게이트웨이 표에서 성공적으로 삭제된 후에 삭제하는 것이 좋습니다.

11 장

사이트 간 VPN 터널 연결

사이트 간 VPN 터널은 다양한 위치에 있는 네트워크를 연결합니다. 서로 다른 두 멀티 클라우드 방어 게이트웨이사이에 또는 멀티 클라우드 방어 게이트웨이와 모든 관련 표준을 준수하는 클라우드 서비스 제공자 간에 사이트 간 IPsec 연결을 생성할 수 있습니다. VPN 연결이 설정되면 로컬 게이트웨이의 뒤에 있는 호스트는 보안 VPN 터널을 통해 원격 게이트의 뒤에 있는 호스트와 연결할 수 있습니다.

일반적으로 동적 피어는 연결을 시작하는 피어여야 합니다. 다른 피어는 동적 피어의 IP 주소를 알지 못하기 때문입니다. 원격 피어가 연결을 설정하려고 시도하면 다른 피어가 사전 공유 키, IKE 설정 및 IPsec 구성을 사용하여 연결을 검증합니다.

원격 피어에서 연결을 시작한 후에만 VPN 연결이 설정되므로 VPN 터널에서 트래픽을 허용하는 액세스 제어 규칙과 일치하는 모든 아웃바운드 트래픽은 연결이 설정될 때까지 중단됩니다. 이를 통해 데이터가 적절한 암호화 및 VPN 보호 없이 네트워크를 벗어나지 않게 합니다.

현재 멀티 클라우드 방어는 다음 플랫폼 또는 제품과의 사이트 간 VPN 터널 연결을 지원합니다.

- AWS
- Azure
- GCP

사이트 간 VPN 터널에 대한 사전 요건 및 제한 사항

멀티 클라우드 방어 게이트웨이 사전 요건 및 제한 사항

연결의 대상에 관계없이 VPN 터널을 생성하기 전에 다음 사전 요건을 완료해야 합니다.

- 멀티 클라우드 방어 게이트웨이 버전 24.04 또는 버전 24.04-01을 실행 중 이어야 합니다. 여기에는 Terraform 버전이 포함됩니다.
- 게이트웨이에서 **VPN** 이 활성화되어 있어야 합니다.
- 하나 이상의 클라우드 서비스 제공자 또는 서드파티 디바이스가 이미 멀티 클라우드 방어에 연결되었습니다.
- VPN 터널 연결을 허용하고 생성하도록 클라우드 서비스 제공자 또는 서드파티 디바이스를 구성해야 합니다. 자세한 내용은 서비스 또는 플랫폼 설명서를 참조하십시오.
- 하나 이상의 IPSec 프로파일이 있어야 합니다. 이 프로파일은 VPN 터널 연결에 연결해야 합니다.
- VPC 및 VNET은 양쪽에 N Address Translation 게이트웨이 없이 구축해야 합니다.
- (선택 사항) 하나 이상의 BGP 프로파일을 생성하는 것이 좋습니다. 이 프로파일은 VPN 터널 연결과 연결된 게이트웨이 인스턴스에 연결되어야 합니다.

VPN 터널 연결을 생성할 때는 다음 제한 사항에 유의합니다.

- 선택한 멀티 클라우드 방어 게이트웨이는 이그레스/이스트-웨스트 게이트웨이 여야 합니다.
- AWS 및 Azure 게이트웨이는 **8** 코어 인스턴스 유형이어야 합니다. 현재 2코어 및 4코어는 지원되지 않습니다.
- 사이트 간 VPN 연결은 최대 10개의 VPN 피어만 지원합니다.
- AWS 또는 Azure 환경용 VPC 및 VNET은 단일 가용성 영역을 사용하여 생성해야 합니다. 다중 가용성 영역은 현재 지원되지 않습니다.
- 사이트 간 VPN 터널은 현재 정방향 프록시 방화벽 규칙을 지원하지 않습니다.
- 대역폭은 800Mbps 이상이어야 합니다.

참고 게이트웨이를 활성화하거나 비활성화하는 경우에는 게이트웨이와 연결된 사이트 대 사이트 연결을 삭제하고 VPN 연결을 다시 생성해야 합니다.

게이트웨이 내에서 **VPN** 활성화

멀티 클라우드 방어 컨트롤러 대시보드에서 게이트웨이용 VPN을 활성화 하려면 다음 절차를 따릅니다.

시작하기 전에

멀티 클라우드 방어을(를) 사용하여 두 디바이스 간 VPN 연결을 설정하려면 먼저 게이트웨이가 IPSec 프로파일과 BGP 프로파일을 모두 활용할 수 있도록 활성화해야 합니다. IPSec 프로파일은 필수이며 BGP 프로파일은 선택 사항입니다.

참고 BGP 프로파일을 사용하는 경우 BGP 프로파일은 원격 피어와 함께 IPSEC 터널을 통해 실행됩니다.

단계 **1** **Manage(**관리**)** > **Gateways(**게이트웨이**)**로 이동합니다.

단계 **2** **Add Gateway(**게이트웨이 추가**)**를 클릭하여 새 게이트웨이를 생성하거나 기존 게이트웨이를 선택하고 Actions(작업) 드롭다운 메뉴에서 **Edit(**편집**)**를 선택합니다.

단계 **3** 게이트웨이를 생성하거나 편집할 때 창의 하단으로 스크롤한 다음, 프롬프트가 표시되면 드롭다운 메뉴에서 **BGP profile(BGP** 프로파일**)**을 선택합니다.

단계 **4** **Advanced Settings(**고급 설정**)**에서 **VPN Connection(VPN** 연결**)** 옵션을 찾습니다. VPN 터널 연결을 옵트인하려면 **Enable VPN(VPN** 활성화**)** 옵션을 선택합니다.

단계 **5** **BGP Profile(BGP** 프로파일**)** 드롭다운 메뉴를 확장하고 이미 생성된 프로파일을 선택합니다.

다음에 수행할 작업

사이트 간 터널 연결 생성.

사이트 간 터널 연결 생성

이 절차를 수행하면 게이트웨이와 Azure, AWS 및 GCP 클라우드 서비스 제공자 간에 사이트 간 VPN 터널 연결을 생성할 수 있습니다.

참고 가상 인터페이스 **IP** 주소를 입력할 때는 Threat Defense 예약 범위 169.254.1.x/24를 제외하고 169.254.xx/16 범위의 IP를 사용하는 것이 좋습니다.

넷 마스크의 경우 /30을 사용하는 것이 좋습니다. 이를 통해 가상 터널 인터페이스 연결의 엔드포인트에 대해 2개의 IP 주소만 사용할 수 있습니다. 예: 169.254.100.1/30

다음 절차에 따라 멀티 클라우드 방어 컨트롤러를 사용하여 사이트 간 VPN 터널을 생성합니다.

단계 **1** **Manage(**관리**)** > **Networking(**네트워킹**)** > **Site-2-Site Connections(**사이트간 연결**)**로 이동합니다.

단계 **2** **Create VPN Connection(VPN** 연결 생성**)**을 클릭합니다.

단계 **3** 연결의 이름을 입력합니다.

단계 **4** **Device 1(**디바이스 **1)** 드롭다운 메뉴를 확장하여 멀티 클라우드 방어 게이트웨이를 선택하거나 원격 엔드포인트의 공용 IP 주소를 수동으로 입력합니다.

단계 **5** **Device 1 Virtual Interface IP(**디바이스 **1** 가상 인터페이스**)** 주소를 입력합니다. 이 필드를 최적화하는 방법에 대한 지침은 이 절차의 시작 부분에 있는 참고 사항를 참조하십시오.

단계 **6** **Device 2(**디바이스 **2)** 드롭다운 메뉴를 확장하여 멀티 클라우드 방어 게이트웨이를 선택하거나 원격 엔드포인트의 공용 IP 주소를 수동으로 입력합니다. 디바이스 1과 디바이스 2에 동일한 디바이스 또는 게이트웨이를 사용하지 마십시오.

단계 **7** **Device 2 Virtual Interface IP(**디바이스 **2** 가상 인터페이스**)** 주소를 입력합니다. 이 필드를 최적화하는 방법에 대한 지침은 이 절차의 시작 부분에 있는 참고 사항를 참조하십시오.

단계 **8** 터널의 **Authentication Value(**인증 값**)**를 입력합니다. 현재 PreShared Key(사전 공유 키)가 기본 인증 방법입니다.

단계 **9** **IPSec Profile(IPSec** 프로파일**)** 드롭다운 메뉴를 확장하여 이미 생성된 프로파일을 선택합니다.

단계 **10** (선택 사항) **BGP Profile(BGP** 프로파일**)** 드롭다운 메뉴를 확장해 이미 생성된 프로파일을 선택합니다. 이 옵션을 활성화하면 IPsec 프로파일이 계속 사용되는 기본 프로파일로 유지되며 BGP 프로파일은 원격 피어를 사용하여 IPSEC 터널을 통해 실행됩니다.

단계 **11** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

연결 상태를 보고 연결 양쪽의 수신 및 발신 바이트 통계를 검토합니다.

사이트 간 **VPN** 터널 편집

다음 절차에 따라 멀티 클라우드 방어 컨트롤러 대시보드를 사용하여 기존 사이트 간 VPN 연결을 편집합니다.

단계 **1** **Manage(**관리**)** > **Networking(**네트워킹**)** > **Site-2-Site Connections(**사이트간 연결**)**로 이동합니다.

단계 **2** VPN 연결을 선택하여 강조 표시합니다.

단계 **3** **Actions(**작업**)** 드롭다운 메뉴에서 **Edit(**편집**)**을 선택합니다.

단계 **4** 복제된 다음 정보를 수정합니다.

- Name(이름)입니다.
- 디바이스 1.
- 디바이스 1 가상 인터페이스 IP.
- 디바이스 2.
- 디바이스 1 가상 인터페이스 IP.
- 인증 값.
- IPSec 프로파일 선택.

단계 **5** **Save(**저장**)**를 클릭합니다. 언제든지 취소할 수 있습니다.

사이트 간 **VPN** 터널 연결 복제

다음 절차에 따라 멀티 클라우드 방어 컨트롤러 대시보드에서 VPN 터널 연결을 복제합니다.

단계 **1** **Manage(**관리**)** > **Networking(**네트워킹**)** > **Site-2-Site Connections(**사이트간 연결**)**로 이동합니다.
단계 **2** VPN 연결을 선택하여 강조 표시합니다.
단계 **3** **Actions(**작업**)** 드롭다운 메뉴에서 **Clone(**복제**)**을 선택합니다.
단계 **4** 연결의 이름을 입력합니다. 복제 중인 연결과 달라야 합니다.
단계 **5** 복제된 다음 정보를 수정합니다.

- 디바이스 1.
- 디바이스 1 가상 인터페이스 IP.
- 디바이스 2.
- 디바이스 1 가상 인터페이스 IP.
- IPSec 프로파일 선택.

단계 **6** 인증 유형이 복제되었지만 해당 키 값은 복제되지 않습니다. 터널의 **Authentication Value(**인증 값**)**를 입력합니다.
단계 **7** **Save(**저장**)**를 클릭합니다.

VPN 터널 연결 삭제

다음 절차에 따라 멀티 클라우드 방어 컨트롤러 대시보드에서 VPN 터널 연결을 삭제합니다.

단계 **1** **Manage(**관리**)** > **Networking(**네트워킹**)** > **Site-2-Site Connections(**사이트간 연결**)**로 이동합니다.
단계 **2** VPN 연결을 선택하여 강조 표시합니다.
단계 **3** **Actions(**작업**)** 드롭다운 메뉴에서 **Delete(**복제**)**를 선택합니다.
단계 **4** 삭제 작업을 확인하고 **Delete(**삭제**)**를 클릭합니다.

다음에 수행할 작업

방금 삭제한 VPN 터널에 대해 생성한 모든 BGP 프로파일을 삭제하는 것이 좋습니다.

VI 부

보안 정책

고급 정책 설정

일부 정책은 추가 특징을 지원합니다.

인그레스 정책의 **XFF** 헤더

인그레스 정책은 HTTP 패킷의 XFF(X-Forwarded-For) 헤더를 지원합니다. XFF는 프록시 서버를 통해 웹 서버에 연결하는 클라이언트의 원래 IP 주소를 식별하기 위한 표준 헤더입니다.

12 장

규칙 및 규칙 집합

규칙

일반적으로 규칙은 도메인 내에서 지정된 유형 및 상태의 개체에 액세스할 수 있는 사용자, 그룹, 역할 또는 조직의 권한을 지정합니다. 멀티 클라우드 방어은(는) 다양한 클라우드 서비스 제공자를 지원하며 이러한 각 환경에는 규칙에 대한 고유한 요구 사항 또는 방법이 있습니다. 클라우드 어카운트에서 생성된 규칙은 멀티 클라우드 방어 컨트롤러에서 생성된 규칙과 다르게 처리될 수 있습니다. 일부 규칙은 기본적으로 게이트웨이 및 인스턴스에 적용되므로 최적의 성능 및 커버리지를 위해 규칙과 정책을 계속 추가하고 수정하면 환경이 기본 보호 레벨을 갖게 됩니다.

규칙 유형은 제공하려는 게이트웨이 환경의 유형을 고려할 때 중요합니다. 모든 규칙 또는 규칙 유형이 모든 게이트웨이 환경과 완전히 호환되는 것은 아닙니다. 멀티 클라우드 방어 컨트롤러에서 지원되는 게이트웨이 유형은 인그레스, 이그레스, 이스트-웨스트입니다.

규칙 및 규칙 집합에 대한 정보 또는 정책 및 그룹에 대한 규칙과 규칙 집합을 생성 또는 수정하는 방법은 이 장의 나머지 부분을 참조하십시오.

정책 관리

정책은 멀티 클라우드 방어 대시보드에서 생성되거나 멀티 클라우드 방어 Terraform 제공자를 사용하는 오케스트레이션을 통해 생성됩니다. 정책은 멀티 클라우드 방어 컨트롤러 데이터베이스의 일부로 저장 및 유지됩니다. 게이트웨이는 주기적 하트비트를 통해 정책 또는 정책 변경 사항을 검색합니다. 여기서 게이트웨이는 컨트롤러 상태 및 텔레메트리 정보를 제공하는 동시에 적용해야 하는 정책 변경이 있는지 요청합니다. 게이트웨이-컨트롤러 통신은 상호 TLS 세션을 통해 완전히 암호화되고 설정됩니다. 하트비트는 5초마다 전송되어 게이트웨이의 정책이 사용자가 생성하거나 수정한 정책과 동기화되도록 합니다.

정책 규칙 집합 게이트웨이 및 관리

정책 규칙 관리

게이트웨이에 할당된 정책 규칙 집합은 다른 정책 규칙 집합으로 동적으로 변경할 수 있습니다. 다른 정책 규칙 집합을 활성 게이트웨이로 교체해야 하는 경우, 이 작업은 영향을 미치지 않는 방식으로 시작될 수 있습니다. 새 정책 규칙 집합의 할당은 게이트웨이 업데이트/업그레이드 프로세스와 유사하게 작동합니다. 새 게이트웨이 인스턴스는 새 정책 규칙 집합으로 인스턴스화됩니다. 새 트래픽 세션이 활성 상태이고 정상 상태이면 새 게이트웨이 인스턴스에 리디렉션됩니다. 이전 트래픽 세션은 이전 게이트웨이 인스턴스에서 플러시됩니다. 이전 게이트웨이 인스턴스는 삭제됩니다. 작업은 몇 분 내에 완료됩니다. 이 변경은 게이트웨이 구성 설정의 일부로 시작됩니다. **Manage(**관리**)** > **Gateways(**게이트웨이**)** > **Gateways(**게이트웨이**)**로 이동합니다. 멀티 클라우드 방어 포털 또는 멀티 클라우드 방어 Terraform 제공자를 사용하여 변경을 시작할 수 있습니다.

정책 규칙 집합 게이트웨이 상태

정책 규칙과 정책 규칙이 연결된 게이트웨이 간 연결 상태는 다음 두 가지 옵션 중 하나일 수 있습니다.

- **Updated(**업데이트됨**)** - 정책이 게이트웨이에서 활성 상태이며 컨트롤러와 동기화되었습니다.
- **Updating(**업데이트 중**)** - 게이트웨이가 정책 변경을 처리 중입니다. 정책 변경 사항은 게이트웨이에 알려지지만 아직 활성화되지 않았습니다. 게이트웨이는 현재 정책을 사용하여 여전히 트래픽을 처리합니다.

규칙 집합 및 규칙 집합 그룹

규칙 집합

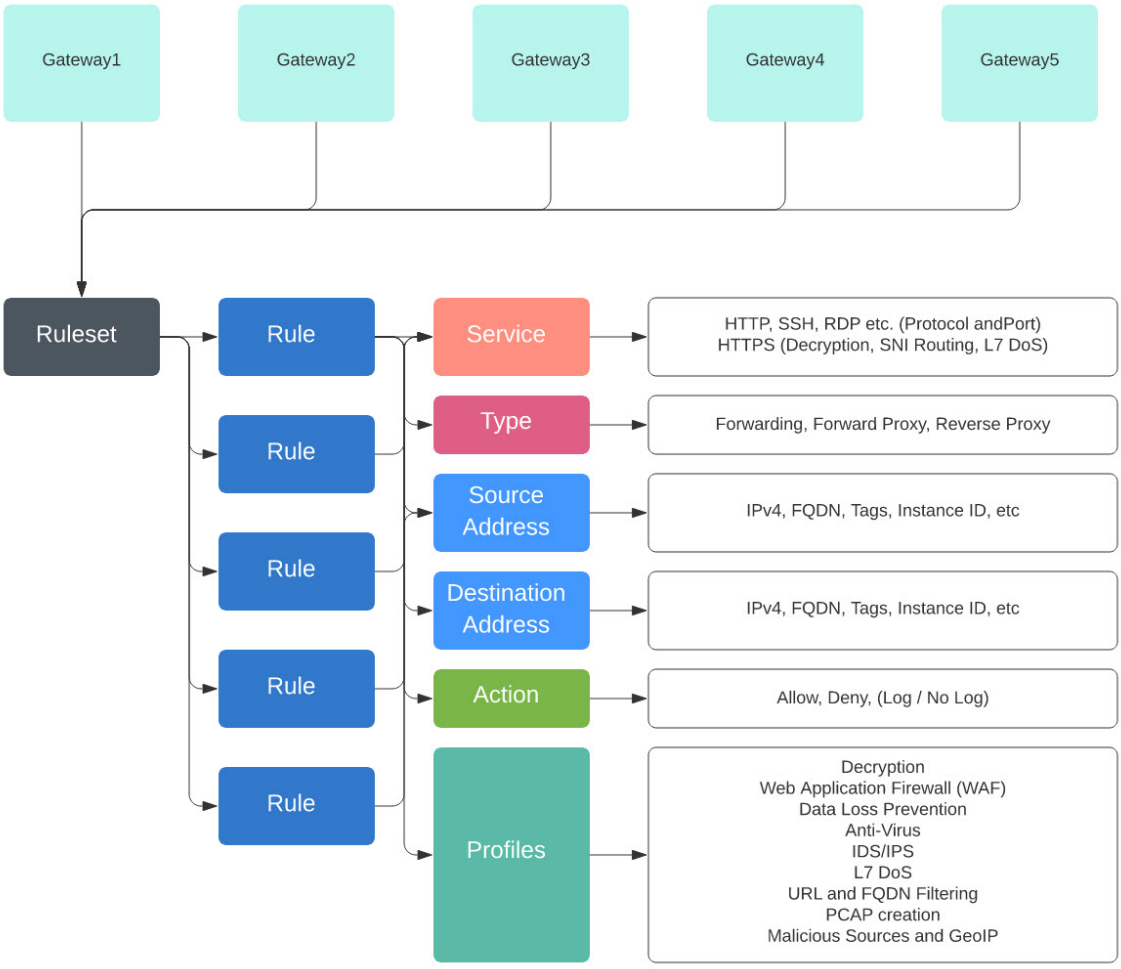
규칙 집합은 애플리케이션 및 워크로드 보호를 수용하기 위해 하나 이상의 게이트웨이 집합에 적용되는 세분화 및 고급 보안 정책을 정의하는 규칙 집합으로 구성됩니다. 규칙은 트래픽이 일치하는 규칙에 의해 처리되는 우선순위 목록으로 구성되고, 허용하거나 거부하기 위해 일반적인 작업이 수행되며, 고급 보안을 통해 추가 검사가 수용됩니다.

규칙 집합은 하나 이상의 멀티 클라우드 방어 게이트웨이와 연결되어야 합니다. 다음과 같은 제한 사항이 규칙 집합에 적용됩니다.

- 규칙 집합은 클라우드 환경에 구애 받지 않고 여러 클라우드에서 하나 이상의 게이트웨이 작업에 적용할 수 있습니다.
- 규칙 집합 그룹을 사용하여 둘 이상의 규칙 집합을 적용할 수 있지만 게이트웨이는 단일 규칙 집합에만 연결할 수 있습니다.
- 규칙 집합 내의 규칙은 검색된 클라우드 자산 정보를 사용하여 변경 사항에 대해 실시간으로 적용되는 정책인 동적 정책을 형성할 수 있습니다.

- 규칙 집합은 클라우드 환경을 통과하는 게이트웨이에 적용되지만, 특정 클라우드 어카운트 및/또는 클라우드 영역에만 적용되는 규칙을 포함할 수 있습니다. 예를 들면 다음과 같습니다.
  - 두 클라우드의 두 게이트웨이에 적용되는 규칙 집합 내의 규칙에 사용되는 동적 태그 기반 주소 개체는 한 클라우드의 게이트웨이와 연결된 IP 주소 집합으로 확인하면서 다른 클라우드의 게이트웨이와 연결된 다른 IP 주소 집합으로 확인할 수 있습니다.

- 규칙 집합은 **Manage(**관리**)** > **Security Policies(**보안 정책**)** > **Rule Sets(**규칙 집합**)** 페이지에서 또는 게이트웨이 생성 워크플로우 내에서 생성할 수 있습니다. 다음 다이어그램은 여러 게이트웨이에 적용된 단일 규칙 집합을 보여줍니다.



지원되는 또 다른 활용 사례는 여러 게이트웨이와 연결된 여러 규칙 집합입니다.

정책 규칙 집합 그룹

정책 규칙 집합 그룹은 독립형 규칙 집합의 모음입니다. 사용자는 여러 독립형 규칙 집합을 하나의 정책 규칙 집합 그룹으로 결합하고 그룹을 하나 이상의 멀티 클라우드 방어 게이트웨이에 연결할 수

있습니다. 정책 규칙 집합 그룹을 사용하면 조직에서 정책을 체계에 따라 분리하고 하나의 전반적인 정책에 결합할 수 있습니다.

Note

- 정책 규칙 집합 그룹은 규칙 집합 멤버로만 구성될 수 있습니다.
- 정책 규칙 집합 그룹과 연관된 모든 규칙 집합에 충돌하는 규칙이 없는지 확인합니다.
- 정책 규칙 집합 그룹에는 최대 100개의 규칙 집합 멤버를 포함할 수 있습니다.

정책 규칙 집합 생성

정책 규칙 집합을 생성하려면 다음을 수행합니다.

단계 **1** **Manage(**관리**)** > **Security Policies(**보안 정책**)** > **Rule Sets(**규칙 집합**)**로 이동합니다.
단계 **2** **Create(**생성**)**를 클릭합니다.
단계 **3** 정책 규칙 집합의 이름과 설명을 추가합니다.
단계 **4** **Save(**저장**)**를 클릭합니다.

What to do next

정책 규칙 집합이 생성되면 규칙 집합에 규칙 집합에서 정방향 프록시 규칙 추가 또는 편집합니다.

규칙 집합에서 규칙 생성

-

규칙 집합에서 전달 규칙 추가 또는 편집

다음 절차를 사용하여 기존 규칙을 정책 규칙 집합에 추가하거나 정책 규칙 집합에 이미 포함된 규칙을 편집합니다.

시작하기 전에

멀티 클라우드 방어 게이트웨이 내에서 새 규칙을 생성할 수 있습니다. 규칙 집합에 규칙을 추가하거나 편집하기 전에 다음 제한 사항에 유의하십시오.

- 단일 정책 규칙 집합에는 최대 2,047개의 규칙을 사용할 수 있습니다.
- 정책 규칙 집합 그룹에는 최대 2,047개의 규칙 집합을 포함할 수 있습니다.

단계 **1** **Manage(**관리**)** > **Security Policies(**보안 정책**)** > **Rule Sets(**규칙 집합**)**로 이동합니다.

단계 **2** 정책 규칙 집합을 보려면 정책 규칙 집합 이름을 클릭합니다.

단계 **3** **Add Rule(**규칙 추가**)**를 클릭하여 새 규칙을 생성하거나 기존 규칙을 추가합니다. 프롬프트가 생성됩니다.

단계 **4** 다음 속성을 입력합니다.

- **Name(**이름**)** -규칙을 참조하는 데 사용되는 친숙하고 고유한 이름입니다.
- (선택 사항) **Description(**설명**)** - 규칙에 대한 간단한 설명입니다.
- **Type(**유형**)** - **Forwarding(**정방향**)**을 선택합니다.

단계 **5** 다음 개체 정보를 입력합니다.

- **Service(**서비스**)** - 규칙을 적용할 프로토콜 및 포트를 결정하는 데 사용되는 서비스 개체입니다.
- **Source(**소스**)** - 규칙을 적용할 리소스를 결정하는 데 사용되는 주소 개체입니다.
- **Destination(**대상**)** - 규칙을 적용할 대상 리소스를 결정하는 데 사용되는 주소 개체입니다. **ReverseProxy** 규칙 유형의 경우 대상은 항상 멀티 클라우드 방어 게이트웨이입니다. **ForwardProxy** 규칙 유형의 경우 대상은 항상 any(모두)입니다.
- **FQDN** - 드롭다운 메뉴를 사용하여 SNI 일치에 사용되는 FQDN 집합을 선택합니다. **Forwarding(**전달**)** 규칙 유형에만 적용됩니다.

단계 **6** 다음 세부사항을 입력합니다.

- **Action(**작업**)** - 작업은 트래픽을 허용할지 아니면 거부할지, 그리고 트래픽을 Events(이벤트)에 기록할지 여부를 정의합니다. 트래픽은 Action(작업)이 **Log(**로그**)** 또는 **No Log(**로그 없음**)**로 설정되어 있는지 여부에 상관없이 항상 Traffic Summary(트래픽 요약)에 로깅됩니다. 규칙에서 허용하는 트래픽의 경우 고급 보안 프로파일이 평가됩니다. 각 고급 보안 프로파일에는 이 작업을 사용하거나 재정의하는 자체 작업이 있습니다.
- **Reset On Deny(**거부 시 재설정**)** - 활성화된 경우 멀티 클라우드 방어 게이트웨이에서는 이 정책과 일치하는 세션에 대해 TCP 재설정 패킷을 전송하지만 게이트웨이에 의해 삭제됩니다. **Forwarding(**전달**)** 규칙 유형에만 적용됩니다.

단계 **7** 다음 프로파일 정보를 입력합니다.

- (선택 사항) **Network Intrusion(**네트워크 침입**)** - 고급 보안에 사용할 IPS(Network Intrusion) 프로파일입니다.
- (선택 사항) **Anti-malware(**악성코드 차단**)** - 고급 보안에 사용할 악성코드 차단 프로파일입니다. 악성코드 차단 프로파일을 아직 생성하지 않은 경우 **+ Create an Anti Malware(+** 악성코드 차단 생성**)**를 클릭합니다.
- (선택 사항) **Data Loss Prevention(**데이터 손실 방지**)** - 고급 보안에 사용할 DLP(데이터 손실 방지) 프로파일입니다. **ForwardProxy** 규칙 유형에만 적용됩니다.
- (선택 사항) **FQDN Filtering(FQDN** 필터링**)** - 고급 보안에 사용할 FQDN(FQDN Filtering)(FQDN) 프로파일입니다.
- (선택 사항) **Malicious IPs(**악의적인 **IP)** - 고급 보안에 사용할 MIP(Malicious IP) 프로파일입니다.
- (선택 사항) **PCAP** - 활성화하려면 이 확인란을 선택합니다. 규칙에 대해 패킷 캡처를 활성화할지 아니면 비활성화할지 여부입니다. 트래픽이 PCAP가 활성화된 규칙과 일치할 때마다 세션 트래픽의 패킷 캡처가 발생하고

PCAP는 PCAP 프로파일에 의해 지정된 위치에 저장됩니다. PCAP 프로파일은 멀티 클라우드 방어 게이트웨이에 구성됩니다.

단계 **8** 규칙에 대한 구성을 지정한 후 **Save(**저장**)**를 클릭합니다.

단계 **9** 규칙을 계속 추가합니다. 원하는 규칙을 모두 추가했으면 **Save Changes(**변경 사항 저장**)**를 클릭합니다. 규칙 집합에 대한 모든 변경 사항의 전후 보기가 표시됩니다. 변경 사항에 만족하면 **Save(**저장**)**를 클릭합니다. 추가로 변경해야 하는 경우에는 **Cancel(**취소**)**을 클릭하여 규칙 집합 편집으로 돌아갑니다.

규칙 집합에서 정방향 프록시 규칙 추가 또는 편집

다음 절차를 사용하여 기존 규칙을 정책 규칙 집합에 추가하거나 정책 규칙 집합에 이미 포함된 규칙을 편집합니다.

시작하기 전에

멀티 클라우드 방어 게이트웨이 내에서 새 규칙을 생성할 수 있습니다. 규칙 집합에 규칙을 추가하거나 편집하기 전에 다음 제한 사항에 유의하십시오.

- 단일 정책 규칙 집합에는 최대 2,047개의 규칙을 사용할 수 있습니다.
- 정책 규칙 집합 그룹에는 최대 2,047개의 규칙 집합을 포함할 수 있습니다.

단계 **1** **Manage(**관리**)** > **Security Policies(**보안 정책**)** > **Rule Sets(**규칙 집합**)**로 이동합니다.

단계 **2** 정책 규칙 집합을 보려면 정책 규칙 집합 이름을 클릭합니다.

단계 **3** **Add Rule(**규칙 추가**)**를 클릭하여 새 규칙을 생성하거나 기존 규칙을 추가합니다. 프롬프트가 생성됩니다.

단계 **4** 다음 속성을 입력합니다.

- **Name(**이름**)** -규칙을 참조하는 데 사용되는 친숙하고 고유한 이름입니다.
- (선택 사항) **Description(**설명**)** - 규칙에 대한 간단한 설명입니다.
- **Type(**유형**)** - **ReverseProxy**를 선택합니다.

단계 **5** 다음 개체 정보를 입력합니다.

- **Service(**서비스**)** - 규칙을 적용할 프로토콜 및 포트를 결정하는 데 사용되는 서비스 개체입니다.
- **Source(**소스**)** - 규칙을 적용할 리소스를 결정하는 데 사용되는 주소 개체입니다.
- **Destination(**대상**)** - 규칙을 적용할 대상 리소스를 결정하는 데 사용되는 주소 개체입니다. **ReverseProxy** 규칙 유형의 경우 대상은 항상 멀티 클라우드 방어 게이트웨이입니다.
- **Target(**대상**)** - 멀티 클라우드 방어 게이트웨이에서 게이트웨이-서버 연결을 설정할 대상을 지정하는 데 사용되는 주소 개체입니다.

단계 **6** 기본 규칙 **Action(**작업**)**을 선택합니다. 트래픽을 허용할지 아니면 거부할지, 그리고 트래픽을 Events(이벤트)에 기록할지 여부를 정의합니다. 트래픽은 Action(작업)이 **Log(**로그**)** 또는 **No Log(**로그 없음**)**로 설정되어 있는지 여부에

상관없이 항상 Traffic Summary(트래픽 요약)에 로깅됩니다. 규칙에서 허용하는 트래픽의 경우 고급 보안 프로파일이 평가됩니다. 각 고급 보안 프로파일에는 이 작업을 사용하거나 재정의하는 자체 작업이 있습니다.

단계 **7** 다음 프로파일 정보를 입력합니다.

- (선택 사항) **Network Intrusion(**네트워크 침입**)** - 고급 보안에 사용할 IPS(Network Intrusion) 프로파일입니다.
- (선택 사항) **Anti-malware(**악성코드 차단**)** - 고급 보안에 사용할 악성코드 차단 프로파일입니다. 악성코드 차단 프로파일을 아직 생성하지 않은 경우 **+ Create an Anti Malware(+** 악성코드 차단 생성**)**를 클릭합니다.
- (선택 사항) **Web Protection(**웹 보호**)** - 고급 보안에 사용할 WAF(Web Protection) 프로파일입니다. 이는 **ReverseProxy** 규칙 유형에만 적용됩니다.
- (선택 사항) **URL Filtering(URL** 필터링**)** - 고급 보안에 사용할 URL(URL 필터링) 프로파일입니다. 이는 **ForwardProxy** 및 **ReverseProxy** 규칙 유형에만 적용됩니다.
- (선택 사항) **Malicious IPs(**악의적인 **IP)** - 고급 보안에 사용할 MIP(Malicious IP) 프로파일입니다.
- (선택 사항) **PCAP** - 활성화하려면 이 확인란을 선택합니다. 규칙에 대해 패킷 캡처를 활성화할지 아니면 비활성화할지 여부입니다. 트래픽이 PCAP가 활성화된 규칙과 일치할 때마다 세션 트래픽의 패킷 캡처가 발생하고 PCAP는 PCAP 프로파일에 의해 지정된 위치에 저장됩니다. PCAP 프로파일은 멀티 클라우드 방어 게이트웨이에 구성됩니다.

단계 **8** 규칙에 대한 구성을 지정한 후 **Save(**저장**)**를 클릭합니다.

단계 **9** 규칙을 계속 추가합니다. 원하는 규칙을 모두 추가했으면 **Save Changes(**변경 사항 저장**)**를 클릭합니다. 규칙 집합에 대한 모든 변경 사항의 전후 보기가 표시됩니다. 변경 사항에 만족하면 **Save(**저장**)**를 클릭합니다. 추가로 변경해야 하는 경우에는 **Cancel(**취소**)**을 클릭하여 규칙 집합 편집으로 돌아갑니다.

규칙 집합에서 정방향 프록시 규칙 추가 또는 편집

다음 절차를 사용하여 기존 규칙을 정책 규칙 집합에 추가하거나 정책 규칙 집합에 이미 포함된 규칙을 편집합니다.

Before you begin

멀티 클라우드 방어 게이트웨이 내에서 새 규칙을 생성할 수 있습니다. 규칙 집합에 규칙을 추가하거나 편집하기 전에 다음 제한 사항에 유의하십시오.

- 단일 정책 규칙 집합에는 최대 2,047개의 규칙을 사용할 수 있습니다.
- 정책 규칙 집합 그룹에는 최대 2,047개의 규칙 집합을 포함할 수 있습니다.

단계 **1** **Manage(**관리**)** > **Security Policies(**보안 정책**)** > **Rule Sets(**규칙 집합**)**로 이동합니다.

단계 **2** 정책 규칙 집합을 보려면 정책 규칙 집합 이름을 클릭합니다.

단계 **3** **Add Rule(**규칙 추가**)**를 클릭하여 새 규칙을 생성하거나 기존 규칙을 추가합니다. 프롬프트가 생성됩니다.

단계 **4** 다음 속성을 입력합니다.

- **Name(**이름**)** -규칙을 참조하는 데 사용되는 친숙하고 고유한 이름입니다.

- (선택 사항) **Description(**설명**)** - 규칙에 대한 간단한 설명입니다.
- **Type(**유형**)** - **ForwardProxy**를 선택합니다.

단계 **5** 다음 개체 정보를 입력합니다.

- **Service(**서비스**)** - 규칙을 적용할 프로토콜 및 포트를 결정하는 데 사용되는 서비스 개체입니다.
- **Source(**소스**)** - 규칙을 적용할 리소스를 결정하는 데 사용되는 주소 개체입니다.
- **Destination(**대상**)** - 규칙을 적용할 대상 리소스를 결정하는 데 사용되는 주소 개체입니다. **ForwardProxy** 규칙 유형의 경우 대상은 항상 any(모두)입니다.
- **FQDN** - 드롭다운 메뉴를 사용하여 SNI 일치에 사용되는 FQDN 집합을 선택합니다. **Forwarding(**전달**)** 규칙 유형에만 적용됩니다.

단계 **6** 기본 규칙 **Action(**작업**)**을 입력합니다. 트래픽을 허용할지 아니면 거부할지, 그리고 트래픽을 Events(이벤트)에 기록할지 여부를 정의합니다. 트래픽은 Action(작업)이 **Log(**로그**)** 또는 **No Log(**로그 없음**)**로 설정되어 있는지 여부에 상관없이 항상 Traffic Summary(트래픽 요약)에 로깅됩니다. 규칙에서 허용하는 트래픽의 경우 고급 보안 프로파일이 평가됩니다. 각 고급 보안 프로파일에는 이 작업을 사용하거나 재정의하는 자체 작업이 있습니다.

단계 **7** 다음 프로파일 정보를 입력합니다.

- (선택 사항) **Network Intrusion(**네트워크 침입**)** - 고급 보안에 사용할 IPS(Network Intrusion) 프로파일입니다.
- (선택 사항) **Anti-malware(**악성코드 차단**)** - 고급 보안에 사용할 악성코드 차단 프로파일입니다. 악성코드 차단 프로파일을 아직 생성하지 않은 경우 **+ Create an Anti Malware(+** 악성코드 차단 생성**)**를 클릭합니다.
- (선택 사항) **Data Loss Prevention(**데이터 손실 방지**)** - 고급 보안에 사용할 DLP(데이터 손실 방지) 프로파일입니다. **ForwardProxy** 규칙 유형에만 적용됩니다.
- (선택 사항) **URL Filtering(URL** 필터링**)** - 고급 보안에 사용할 URL(URL 필터링) 프로파일입니다. 이는 **ForwardProxy** 및 **ReverseProxy** 규칙 유형에만 적용됩니다.
- (선택 사항) **FQDN Filtering(FQDN** 필터링**)** - 고급 보안에 사용할 FQDN(FQDN Filtering)(FQDN) 프로파일입니다.
- (선택 사항) **Malicious IPs(**악의적인 **IP)** - 고급 보안에 사용할 MIP(Malicious IP) 프로파일입니다.
- (선택 사항) **PCAP** - 활성화하려면 이 확인란을 선택합니다. 규칙에 대해 패킷 캡처를 활성화할지 아니면 비활성화할지 여부입니다. 트래픽이 PCAP가 활성화된 규칙과 일치할 때마다 세션 트래픽의 패킷 캡처가 발생하고 PCAP는 PCAP 프로파일에 의해 지정된 위치에 저장됩니다. PCAP 프로파일은 멀티 클라우드 방어 게이트웨이에 구성됩니다.

단계 **8** 규칙에 대한 구성을 지정한 후 **Save(**저장**)**를 클릭합니다.

단계 **9** 규칙을 계속 추가합니다. 원하는 규칙을 모두 추가했으면 **Save Changes(**변경 사항 저장**)**를 클릭합니다. 규칙 집합에 대한 모든 변경 사항의 전후 보기가 표시됩니다. 변경 사항에 만족하면 **Save(**저장**)**를 클릭합니다. 추가로 변경해야 하는 경우에는 **Cancel(**취소**)**을 클릭하여 규칙 집합 편집으로 돌아갑니다.

규칙 집합의 규칙 비활성화, 편집, 복제 또는 삭제

다음 절차를 사용하여 규칙 집합에 대해 구성된 기존 규칙을 편집하거나 복제합니다. 현재 정책 또는 규칙 집합에 대해 활성화할 필요가 없는 경우에는 규칙을 비활성화할 수도 있습니다. 지금 또는 향후 구축에 필요하지 않은 경우 규칙을 삭제할 수 있습니다.

한 번에 하나의 규칙만 편집하거나 복제할 수 있다는 점에 유의하십시오. 여러 규칙을 동시에 삭제하거나 비활성화할 수 있습니다.

단계 **1** **Manage(**관리**)** > **Security Policies(**보안 정책**)** > **Rule Sets(**규칙 집합**)**로 이동합니다.

단계 **2** 비활성화, 편집, 복제 또는 삭제할 규칙이 포함된 규칙 집합을 찾은 다음 규칙 집합 이름을 클릭합니다.

단계 **3** 독립형 규칙의 확인란을 선택합니다.

단계 **4** **Actions(**작업**)** 버튼을 확장합니다.

단계 **5** 실행 가능한 항목을 선택합니다.

- **Disable(**비활성화**)** - 이 옵션은 규칙 집합의 규칙을 유지하지만 트래픽에 영향을 미치지 않는 규칙 및 구성된 규칙 작업을 비활성화합니다.
- **Edit(**편집**)** - 이 옵션은 Properties(속성) 창을 실행하며 규칙의 구성을 편집할 수 있습니다. **Save(**저장**)**를 클릭하여 변경 사항을 저장합니다.
- **Clone(**복제**)** - 이 옵션은 규칙의 복제본을 생성하며, 복제된 규칙의 이름을 지정하거나 규칙의 구성을 추가로 변경할 수 있는 Properties(속성) 창을 엽니다. **Save(**저장**)**를 클릭하여 구성을 확인합니다. 복제된 규칙을 저장하면 현재 보고 있는 규칙 집합에 자동으로 추가됩니다.
- **Delete(**삭제**)** - 이 옵션은 규칙 집합에서 규칙을 영구적으로 제거합니다. 그 결과 게이트웨이에서도 규칙이 제거되었습니다.

단계 **6** **Save Changes(**변경사항 저장**)**를 클릭하여 규칙에 대해 수행한 변경사항을 확인하고 규칙 집합을 간접적으로 수행합니다. 변경 사항을 저장하지 않으려면 **Cancel(**취소**)**을 클릭합니다. 게이트웨이에 대한 변경 사항의 손실이 정상적인지 확인합니다.

정책 규칙 집합 그룹 생성

정책 규칙 집합 그룹을 생성하려면 다음을 수행합니다.

단계 **1** **Manage(**관리**)** > **Security Policies(**보안 정책**)** > **Rules(**규칙**)**로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** 정책 규칙 집합의 이름과 설명을 추가합니다.

단계 **4** **Type(**유형**)**을 Group(그룹)으로 선택합니다.

단계 **5** 드롭다운 메뉴를 확장하여 **Rule Set List(**규칙 집합 목록**)** 섹션에서 규칙 집합을 추가합니다. 규칙 집합을 더 추가하려면 **Add Rule Sets(**규칙 집합 추가**)**를 클릭하여 다른 행을 추가합니다.

13 장

주소 개체

주소 개체

주소 개체는 정의된 방법에 따라 보안 정책 규칙 집합 규칙의 소스 또는 대상 또는 역방향 프록시 서비스 개체의 대상 백엔드 주소로 사용할 하나 이상의 IP, CIDR 또는 FQDN 집합을 나타냅니다. 주소 개체는 기존 구조를 사용하여 정적으로 구성하거나 클라우드 구조를 사용하여 동적으로 구성할 수 있습니다.

주소 개체는 보안 정책 규칙 또는 규칙 집합 내의 **Source(**소스**)**, **Destination(**대상**)** 또는 **Reverse Proxy Target(**역방향 프록시 대상**)** 필드에 있는 하나 이상의 IP, CIDR 또는 FQDN 집합을 나타냅니다. 이는 역방향 프록시 서비스 개체 내에서 대상 백엔드 주소로 정의될 수도 있습니다. 이 섹션에서는 소스 및 대상 개체에 중점을 둡니다.

버전 24.04 이상부터 이제 특정 IP 주소 또는 IP 주소 범위를 제외하도록 주소 개체를 구성할 수 있습니다.

Src/Dest

이러한 개체는 IP 주소 또는 CIDR에 명시적으로 매핑되는 일치 기준을 정의하는 데 사용됩니다. 개체는 정책 규칙 내에서 참조되며 정책 규칙이 처리될 때 게이트웨이 인스턴스로 들어가는 트래픽에 대해 평가됩니다.

소스 및 대상 주소 개체는 게이트웨이 인스턴스로 들어오는 애플리케이션 트래픽을 매칭하기 위해 IP 주소와 CIDR이 명시적으로 필요한 경우에 유용합니다. 이러한 개체는 정책 규칙 정의의 소스 및 대상 필드 내에서 참조됩니다. 이 각각의 필드를 채우는 데 사용되는 주소 개체 유형은 트래픽 흐름, 애플리케이션 유형, 활용 사례에 따라 달라집니다.

소스 및 대상 주소 개체

소스 또는 대상 주소 개체는 보안 정책 규칙 집합 내부의 규칙에 대한 소스 또는 대상을 지정합니다. 규칙에서 소스 또는 대상 IP 주소를 기준으로 트래픽을 매칭하는 데 사용됩니다. 다양한 유형의 주소 개체는 다음과 같이 정의됩니다.

IP/CIDR/FQDN(고정**)** 주소 개체

IP/CIDR/FQDN 주소 개체는 IP 주소, CIDR 블록 또는 FQDN의 집합으로 구성됩니다. 다음은 IP/CIDR 주소 개체의 예입니다.

- DNS 서버의 대상 IP.
- SMTP 릴레이 서버의 대상 IP.
- NTP 서버의 대상 IP.
- 애플리케이션 워크로드의 소스 IP 또는 서브넷.

FQDN 주소 개체는 DNS 확인을 기반으로 IP를 허용 또는 차단하기 위한 명시적 FQDN 집합을 정의합니다. FQDN이 FQDN 주소 개체 내에서 정의된 다음 정책 규칙 내에서 참조되는 경우 게이트웨이 인스턴스는 DNS 확인을 수행하여 수신 트래픽과 일치하는 해당 IP 주소를 검색합니다. 기본적으로 캐싱은 활성화되어 있지 않습니다. 이 경우 DNS 확인은 60초마다 이루어지며 게이트웨이 인스턴스는 60초 동안 검색된 확인을 사용합니다. FQDN 주소 개체 내에 지정된 FQDN이 대규모 IP 주소 집합(예: 각각 400개 초과)으로 확인되는 경우 캐싱을 활성화할 수 있습니다. 이 경우 캐시 크기 및 캐시 TTL과 함께 DNS 확인 간격을 지정할 수 있습니다.

FQDN 주소 개체는 UDP 기반(예: NTP)이거나 요청 패킷에 호스트 정보가 없는 TCP 트래픽(예: SMTP)인 애플리케이션 트래픽에서 일치시킬 때 유용합니다. 두 경우 모두 내부 워크로드가 연결해야 하는 모든 적절한 NTP 서버 또는 SMTP 서버에 대한 IP 주소 목록을 수동으로 정의하는 대신 이러한 종류의 애플리케이션 트래픽에서 일치시킬 FQDN 주소 개체를 사용하는 것이 좋습니다.

동적 클라우드 구문

클라우드-네이티브 주소 개체는 주기적인 인벤토리 목록 수집(API 기반) 또는 실시간 이벤트 추적(GCP Pub/Sub 통합)을 통해 멀티 클라우드 방어 컨트롤러에서 검색한 동적 클라우드 리소스입니다. 이러한 리소스는 VPC/VNET, 인스턴스 ID, 보안 그룹, 서브넷 ID와 같은 개별 리소스 또는 사용자 정의 태그를 통해 참조되는 리소스 집합일 수 있습니다. 멀티 클라우드 방어 컨트롤러는 실시간 이벤트 추적과 대상 API 호출을 결합하여 클라우드 리소스와 연결된 IP 주소를 동적으로 채웁니다. 따라서 클라우드 네이티브 리소스에 대한 모든 후속 변경 사항은 이 리소스를 참조하는 주소 개체 내부에 자동으로 반영됩니다.

Note 클라우드 네이티브 구조를 사용하여 소스 또는 대상 주소 개체를 정의하면 단일 및 멀티 클라우드 환경 모두에서 동적 클라우드 정책을 생성할 수 있습니다. 클라우드 환경 내에서 클라우드 리소스가 추가, 삭제 또는 변경되면 주소 개체가 동적으로 업데이트되어 이러한 변경 사항을 반영하므로 환경의 모든 애플리케이션 및 기능에서 보안 태세가 자동으로 업데이트됩니다.

VNet 및 **VPC** 환경의 사용자 정의 태그

태그는 일련의 태그로 정의된 클라우드 리소스의 IP 주소 또는 CIDR을 주소 개체에 매핑합니다. GCP에서 레이블은 다양한 환경(예: 개발, 스테이징, 프로덕션 등) 전용 리소스를 분류하는 데 자주 사용되는 키-값 쌍입니다. 소스 또는 대상 주소 개체 내에서 사용자 정의 태그를 사용하여 인스턴스, VPC/VNET, 서브넷, 보안 그룹 등의 리소스를 참조할 수 있습니다. 대개 조직에서는 태그를 사용하여 인스턴스를 분류합니다.

태그 기반 정책 규칙은 동적 클라우드 정책의 매우 강력한 구성 요소입니다. 특정 태그가 있는 인스턴스 그룹에 대해 세분화된 정책 규칙을 정의할 수 있습니다. 이러한 정책 규칙이 있으면 새 인스턴스가 적절한 태그를 사용하여 구축될 때마다, 새 인스턴스가 속한 인스턴스 범주에 대해 정의된 원하는 보안 정책을 자동으로 상속합니다. 이는 멀티 클라우드 방어 컨트롤러이(가) 새 인스턴스가 구축된 것을 검색할 뿐만 아니라 해당 인스턴스에 할당된 태그도 검색하기 때문입니다. 그런 다음 이 인스턴스 기반 태그를 참조하는 소스 또는 대상 주소 개체를 새 인스턴스의 IP 주소와 함께 동적으로 업데이트합니다. 잘못된 태그를 사용하여 인스턴스가 구축되었거나 태그가 없는 경우 적절한 정책 규칙이 일치하지 않으므로 다른 리소스와 통신할 수 없습니다.

VNet 및 VPC에서 태그는 VPC와 연결된 CIDR을 주소 개체 CIDR에 매핑합니다. VPC 또는 VNET 내에 구축된 인스턴스와 일치하는 규칙을 생성하는 상황에 맞는 방법을 제공합니다. 특정 VPC 또는 VNET과 연결된 CIDR을 수동으로 파악하는 대신 검색된 VPC 또는 VNET의 이름을 사용하여 일치 기준을 정의할 수 있습니다. VPC 또는 VNET에 대한 변경 사항은 개입 없이 정책 규칙에서 동적으로 업데이트됩니다. VPC 또는 VNET이 제거되고 새 VPC/VNET이 생성되는 경우, CIDR을 재사용하더라도 규칙이 더 이상 적용되지 않습니다.

인스턴스 **ID**

인스턴스 ID는 인스턴스와 연결된 IP 주소를 주소 개체 내의 IP 주소 목록에 매핑합니다. 이를 통해 인스턴스의 구성 방식을 수동으로 파악하지 않고도 특정 인스턴스에 대한 정책 규칙을 상황에 따라 생성할 수 있습니다. 정책 규칙은 인스턴스 변경 사항 또는 제거 사항을 반영합니다. 인스턴스를 삭제하고 동일한 구성의 새 인스턴스로 교체하더라도, 정책 규칙은 다른 인스턴스에 적용할 수 없습니다.

보안 그룹

보안 그룹은 보안 그룹과 연결된 네트워크 인터페이스의 IP 주소를 주소 개체 내의 IP 주소 목록에 매핑합니다. 모든 인터페이스 관련 변경 사항(예: 보안 그룹에 추가 또는 제거된 필드)은 주소 개체 내의 IP 주소 목록에 동적으로 반영됩니다. 이를 통해 조직은 기존 보안 그룹을 게이트웨이 데이터 경로 파이프라인의 고급 보안 기능에 조정할 수 있습니다.

서브넷 **ID**

서브넷 ID는 서브넷과 연결된 CIDR을 주소 개체 CIDR에 매핑합니다. 이를 통해 서브넷의 구성 방식을 수동으로 파악하지 않고도 특정 서브넷 ID와 연결된 모든 리소스에 대한 정책 규칙을 상황에 따라 생성할 수 있습니다. VPC 또는 VNET은 일반적으로 여러 서브넷으로 구분되며 이러한 서브넷 내에 구축된 리소스는 다양한 용도로 사용될 수 있습니다. 예를 들어, 서브넷의 인스턴스에 특정 고급 보안 프로파일 집합이 필요하거나 트래픽 흐름 요구 사항이 다를 수 있습니다. 각 서브넷에 대해 서로 다른 보안 규칙을 생성하는 프로세스를 간소화하기 위해 멀티 클라우드 방어을(를) 사용하면 서브넷의 이름을 일치 기준으로 사용하여 정책 규칙을 정의할 수 있습니다. 따라서 각 서브넷은 고유한 보

안 프로파일을 가진 고유한 정책 규칙을 가질 수 있습니다. 서브넷 및 서브넷 내에 구축된 인스턴스에 대한 변경 사항은 정책 규칙에 동적으로 반영됩니다.

지역 IP

지역 IP 주소 개체는 지역 IP 국가 이름 집합으로 구성됩니다. 이러한 개체는 지리적 위치(국가)를 기준으로 IP 주소에서 들어오거나 IP 주소로 나가는 트래픽을 허용하거나 차단하는 데 사용됩니다. 멀티 클라우드 방어은(는) 업데이트된 GeoIP 목록을 유지하기 위해 MaxMind GeoIP2 데이터베이스와 통합됩니다.

국가 이름과 코드의 전체 목록 또는 IP 주소에서 GeoIP 국가 코드에 이르는 IP 주소를 검토하려면 GeoName 웹사이트로 이동하십시오.

그룹

그룹 주소 개체는 소스 또는 대상 주소 개체의 집합으로 구성됩니다. 그룹은 개별 주소 개체를 정의한 다음 함께 그룹화하여 유연성을 제공하며, 그룹의 멤버에 따라 트래픽을 일치시키는 데 필요한 규칙 수를 간소화합니다. 그룹은 멤버가 고정, 동적 또는 이 둘의 조합인지 여부에 상관없이 그룹 멤버로부터 IP, CIDR 또는 FQDN 집합을 상속합니다.

소스 또는 대상 주소 개체 매개변수

유형	모드: 동적 또는 정적	매개변수	필수 또는 선택	참고
IP/CIDR/FQDN	고정	값	필수	주소 개체당 총 FQDN의 수는 200으로 제한되며, 각 FQDN은 최대 400개의 IP로 확인할 수 있습니다. 멀티 클라우드 방어 게이트웨이에서는 DNS 레코드 TTL에 관계없이 60초마다 DNS 확인을 수행합니다.
VPC/VNet ID	동적	CSP 계정	필수	
		지역	필수	
		리소스 그룹	선택 사항	Azure 전용
		VPC/VNet ID	필수	

유형	모드: 동적 또는 정적	매개변수	필수 또는 선택	참고
보안 그룹	동적	CSP 계정	필수	
		지역	필수	
		VPC/VNet ID	필수	
		리소스 그룹	선택 사항	Azure 전용
		보안 그룹 ID	필수	
애플리케이션 보안 그룹	동적	CSP 계정	필수	Azure 전용
		지역	필수	
		리소스 그룹	필수	
		애플리케이션 보안 그룹	필수	
인스턴스 ID	동적	CSP 계정	필수	
		지역	필수	
		VPC/VNet ID	필수	
		리소스 그룹	선택 사항	선택 사항
		인스턴스 ID	필수	
서브넷 ID	동적	CSP 계정	필수	
		지역	필수	
		VPC/VNet ID	필수	
		리소스 그룹	선택 사항	Azure 전용
		서브넷 ID	필수	

유형	모드: 동적 또는 정적	매개변수	필수 또는 선택	참고
사용자 정의 태그	동적	CSP 계정	선택 사항	
		지역	선택 사항	
		VPC/VNet ID	선택 사항	
		리소스 그룹	선택 사항	Azure 전용
		리소스/태그/값	필수	리소스 및 태그 키-값 쌍의 목록입니다. 리소스는 인스턴스, VPC/VNet, 서브넷, 로드 밸런서, 보안 그룹, 보안 그룹(Azure)일 수 있습니다.
지역 IP		값	필수	
그룹		주소	필수	

역방향 프록시 대상 주소 개체

역방향 프록시 대상 주소 개체는 역방향 프록시 서비스 개체에 백엔드 대상 주소로 지정됩니다. 서비스 개체에서 애플리케이션에 백엔드 연결을 설정하는 데 사용됩니다. 애플리케이션은 IP 또는 FQDN 형식의 하나 이상의 애플리케이션 로드 밸런서 또는 인스턴스 주소일 수 있습니다. 다양한 유형의 역방향 프록시 대상 주소 개체는 다음과 같이 정의됩니다.

정적 **IP/FQDN** 주소 개체

IP/FQDN 주소 개체는 IP 주소 또는 FQDN의 집합으로 구성됩니다. 둘 이상의 IP 또는 FQDN이 구성된 경우 게이트웨이는 백엔드 연결을 설정할 때 구성된 필드 중 우선순위 없이 주소를 처리합니다. FQDN이 구성되면 게이트웨이에서는 DNS를 통해 FQDN을 확인하여 백엔드 연결을 설정할 때 사용할 IP 주소를 결정합니다.

동적 애플리케이션 주소 개체

애플리케이션 주소 개체는 애플리케이션 태그에 의해 결정되는 개별 애플리케이션 로드 밸런서 클라우드 리소스로 구성됩니다. 구성은 멀티 클라우드 방어 실시간 인벤토리 목록 검색을 사용하여 클라우드 어카운트에서 가져온 클라우드 리소스로 표시되는 IP 또는 FQDN을 동적으로 채웁니다. 클라우드 리소스에 대한 모든 변경 사항은 주소 개체에 자동으로 반영됩니다. 구성으로 인해 IP 또는 FQDN이 두 개 이상 생성되면 게이트웨이는 백엔드 연결을 설정할 때 설정된 필드 중 우선 순위가 없는 필드를 처리합니다. 구성 결과가 FQDN인 경우 게이트웨이는 DNS를 통해 FQDN을 확인하여 백엔드 연결을 설정할 때 사용할 IP 주소를 결정합니다.

역방향 프록시 대상 주소 개체 매개변수

유형	모드: 동적 또는 정적	매개변수	필수 또는 선택	참고
IP/FQDN	고정	값	필수	
애플리케이션	동적	CSP 계정	필수	
		지역	필수	
		VPC/VNet ID	필수	
		리소스 그룹	선택 사항	Azure 전용
		태그/값	필수	단일 태그 키-값 쌍

시스템 개체

멀티 클라우드 방어은(는) 정책 생성을 간소화하기 위해 사전 정의된 주소 개체 목록을 제공합니다. 모든 시스템 개체는 편집하거나 삭제할 수 없습니다. 사용자는 수정이 필요한 경우 시스템 개체를 복제하도록 선택할 수 있습니다.

이름	설명
Any(모든)	전체 IPv4 주소 공간을 나타냅니다.
any-private-rfc-1918	RFC-1918에 정의된 모든 IPv4 전용 주소를 나타냅니다.
인터넷	전체 IPv4 공용 주소 공간에서 프라이빗 IPv4 주소(RFC1918)를 뺀 것을 나타냅니다.

소스/대상 주소 개체 생성

이 개체에 대한 정보는 소스 또는 대상 주소 개체 매개변수, on page 108를 참조하십시오. 다음 절차에 따라 멀티 클라우드 방어에 src/dst 주소 개체를 생성합니다.

단계 **1** **Manage(**관리**)** > **Security Policies(**보안 정책**)** > **Addresses(**주소**)**로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** **Src/Dest(Src/**대상**)**를 선택합니다.

단계 **4** 주소 개체를 식별하기 위한 고유한 이름을 입력합니다.

단계 **5** (선택 사항) 개체의 설명을 입력합니다. 이 명령은 개체를 다른 개체와 구분하는 데 도움이 되는 컨텍스트를 제공할 수 있습니다.

단계 **6** **Object Type(**개체 유형**)**을 선택합니다. 개체 유형 및 개체 유형에 대한 자세한 내용은 주소 개체, on page 105를 참조하십시오. 다음 유형 중 하나를 선택합니다.

- IP/CIDR/FQDN
- VPC/VNet ID
- 보안 그룹
- 애플리케이션 ID(Azure만 해당)
- 인스턴스 ID
- 서브넷 ID
- 사용자 정의 태그
- 지역 IP
- 서비스 엔드포인트(클라우드 서비스 IP)
- 그룹

Note **Group(**그룹**)**을 선택하는 경우, 포함하거나 제외할 특정 IP 주소 또는 IP 주소의 범위를 포함할 수 있습니다.

단계 **7** 6단계에서 선택한 유형에 따라 다음 매개 변수를 입력합니다.

- **Value(**값**)** - 유효한 IP, CIDR 또는 FQDN IP 주소를 입력합니다.
- **CSP Account(CSP** 계정**)** - 드롭다운 메뉴를 사용하여 컨트롤러에 이미 연결된 클라우드 서비스 제공자 계정을 선택합니다.
- **Region(**지역**)** - 클라우드 서비스 제공자가 위치한 지역을 선택합니다.
- **VPC** - 드롭다운 메뉴를 사용하여 VPC 또는 VNet을 선택합니다. 선택하는 클라우드 서비스 제공자 계정에 따라 사용 가능한 옵션이 달라질 수 있습니다.
- **Subnet(**서브넷**)** - 드롭다운 메뉴를 사용하여 VPC 또는 VNet에 적용할 서브넷을 선택합니다.
- (Azure 전용) **Resource Group(**리소스 그룹**)** - 드롭다운 메뉴를 사용하여 선택 항목과 호환되는 리소스 그룹을 선택합니다.
  - **Resource Level(**리소스 레벨**)** - 드롭다운 메뉴를 사용하여 값을 선택합니다.
  - **Resource Tag(**리소스 태그**)** - 드롭다운 메뉴를 사용하여 키워드를 리소스 태그로 선택합니다.
  - **Value(**값**)** - 리소스 그룹에 대한 유효한 값을 입력합니다. 이는 IP/CIDR/FQDN 개체에 필요한 값 항목과는 다릅니다.
- **Geo IP(**지역 **IP)** - 드롭다운 메뉴를 사용하여 선택한 지리위치와 연결된 특정 IP를 선택합니다.
- **X-Forwarded-For Match Enabled(X-Forwarded-For** 일치 활성화**)** - 게이트웨이를 XFF HTTP 헤더 필드와 일치시킬 수 있게 하려면 이 확인란을 선택합니다.

- **Address(**주소**)** - 기존 개체를 선택합니다. 이 선택은 인증할 주소 그룹을 결정합니다.
- **Include Addresses(**주소 포함**)** - 이 옵션은 6단계에서 유형으로 "그룹"을 선택한 경우에만 적용 가능합니다. 포함할 특정 IP 주소 또는 IP 주소 범위를 입력합니다. `any`를 사용하여 모든 유효한 주소를 포함할 수도 있습니다.
- **Exclude Addresses(**주소 제외**)** - 이 옵션은 6단계에서 유형으로 "Group(그룹)"을 선택하는 경우에만 적용 가능합니다. 포함할 특정 IP 주소 또는 IP 주소 범위를 입력합니다. `any`를 사용하여 모든 유효한 주소를 포함할 수도 있습니다. 주소 제외에 대해 멀티 클라우드 방어 컨트롤러로부터의 검증이 없다는 점에 유의하십시오.

단계 **8** (선택 사항) **Matching Expression(**일치 식**)**을 포함합니다. 이는 개체가 실행하기 위해 일치해야 하는 조건 집합을 나타냅니다.

단계 **9** 완료되면 **Save(**저장**)**를 클릭하십시오.

역방향 프록시 대상 주소 개체 생성

이 개체에 대한 정보는 역방향 프록시 대상 주소 개체 매개변수, 111 페이지를 참조하십시오. 다음 절차에 따라 멀티 클라우드 방어에 역방향 프록시 대상 주소 개체를 생성합니다.

단계 **1** **Manage(**관리**)** > **Security Policies(**보안 정책**)** > **Addresses(**주소**)**로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** **Reverse Proxy Target(**역방향 프록시 대상**)**을 선택합니다.

단계 **4** 주소 개체를 식별하기 위한 고유한 이름을 입력합니다.

단계 **5** (선택 사항) 개체의 설명을 입력합니다. 이 명령은 개체를 다른 개체와 구분하는 데 도움이 되는 컨텍스트를 제공할 수 있습니다.

단계 **6** **Object Type(**개체 유형**)**을 선택합니다. 개체 유형 및 개체 유형에 대한 자세한 내용은 주소 개체, 105 페이지를 참조하십시오. 다음 유형 중 하나를 선택합니다.

- IP/CIDR/FQDN
- 애플리케이션

단계 **7** 6단계에서 선택한 유형에 따라 다음 매개 변수를 입력합니다.

- **Value(**값**)** - 유효한 IP, CIDR 또는 FQDN IP 주소를 입력합니다.
- **CSP Account(CSP** 계정**)** - 드롭다운 메뉴를 사용하여 컨트롤러에 이미 연결된 클라우드 서비스 제공자 계정을 선택합니다.
- **Region(**지역**)** - 클라우드 서비스 제공자가 위치한 지역을 선택합니다.
- **VPC** - 드롭다운 메뉴를 사용하여 VPC 또는 VNet을 선택합니다. 선택하는 클라우드 서비스 제공자 계정에 따라 사용 가능한 옵션이 달라질 수 있습니다.
- **Subnet(**서브넷**)** - 드롭다운 메뉴를 사용하여 VPC 또는 VNet에 적용할 서브넷을 선택합니다.

- (Azure 전용) **Resource Group(**리소스 그룹**)** - 드롭다운 메뉴를 사용하여 선택 항목과 호환되는 리소스 그룹을 선택합니다.

단계 **8** 드롭다운 메뉴를 사용하여 이 개체에 대한 기존 **Applications Tag(**애플리케이션 태그**)** 와 해당 **Value(**값**)**를 모두 선택합니다.

단계 **9** 완료되면 **Save(**저장**)**를 클릭하십시오.

주소 개체 편집

수정할 수 없는 매개변수를 수정할 경우 주소 개체를 주소 개체 복제한 다음 매개변수를 원하는 대로 변경해야 합니다.

주소 개체를 편집하려면 다음 단계를 수행합니다. 모든 매개변수를 편집할 수 있는 것은 아닙니다.

단계 **1** **Manage(**관리**)** > **Security Policies(**보안 정책**)** > **Addresses(**주소**)**로 이동합니다.

단계 **2** 편집할 주소 개체 옆의 확인란을 선택합니다.

단계 **3** **Edit(**편집**)**를 클릭합니다.

단계 **4** 필요에 따라 매개변수를 수정합니다.

단계 **5** 완료되면 **Save(**저장**)**를 클릭하십시오.

주소 개체 복제

원본 대신 복제본을 사용하려는 경우 원본의 모든 연결을 복제본과 교체해야 합니다. 연결은 하나 이상의 보안 정책 규칙 집합 규칙 또는 역방향 프록시 서비스 개체의 집합에 포함됩니다. 세부사항 보기를 확인하여 연결을 확인할 수 있습니다.

기존 주소 개체를 복제하려면 다음 단계를 수행합니다.

단계 **1** **Manage(**관리**)** > **Security Policies(**보안 정책**)** > **Addresses(**주소**)**로 이동합니다.

단계 **2** 복제할 주소 개체 옆의 확인란을 선택합니다.

단계 **3** **Clone(**복제**)**를 클릭합니다.

단계 **4** 매개변수를 지정하고 원하는 대로 수정합니다.

단계 **5** 완료되면 **Save(**저장**)**를 클릭하십시오.

주소 개체 삭제

주소 개체가 정책 규칙 집합 규칙 또는 역방향 프록시 서비스 개체에서 활발하게 사용되는 경우, 주소 개체가 하나 더 연결되게 되며 주소 개체를 삭제할 수 없습니다. 주소 개체를 삭제하려면 먼저 모든 연결을 제거해야 합니다. 그러면 주소 개체를 삭제할 수 있습니다. 세부사항 보기를 확인하여 연결을 확인할 수 있습니다.

단계 **1** **Manage(**관리**)** > **Security Policies(**보안 정책**)** > **Addresses(**주소**)**로 이동합니다.

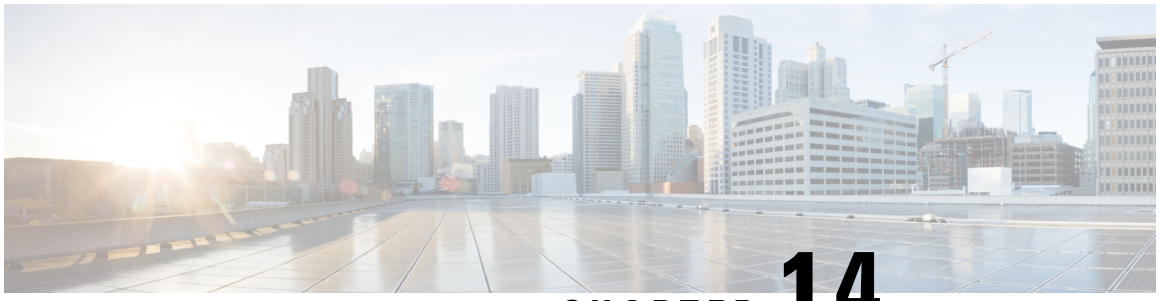
단계 **2** 삭제할 주소 개체 옆의 확인란을 선택합니다.

단계 **3** **Delete(**삭제**)**를 클릭합니다.

단계 **4** **Save(**저장**)**를 클릭하여 삭제를 확인합니다.

세부사항 보기

Manage(관리**)** > **Security Policies(**보안 정책**)** > **Addresses(**주소**)** 페이지에서 개체의 **Name(**이름**)**을 클릭하여 주소 개체 **Details(**세부 정보**)**를 볼 수 있습니다. **Details(**세부 정보**)**에는 해당 유형 및 구성에 따라 채워진 IP, CDIR 및 FQDN이 표시됩니다. 또한 정책 규칙 집합 및 모든 개체 서비스와의 연결도 표시됩니다.



CHAPTER 14

FQDN 개체

FQDN 일치 개체

FQDN(Fully Qualified Domain Name) 일치 개체는 TLS 암호화 트래픽과 관련된 SNI(Server Name Indication)를 평가합니다. 규칙 일치에 대한 평가의 결과를 사용합니다. 트래픽이 규칙과 연결된 모든 일치 개체(주소, FQDN, 서비스)와 일치하는 경우 규칙은 트래픽 처리에 사용됩니다. FQDN을 평가하려면 트래픽이 TLS로 암호화되어야 하며 TLS hello 헤더에 SNI를 포함해야 합니다. FQDN에서는 전달 또는 전달 프록시 규칙에 의해 처리된 트래픽을 평가할 수 있습니다. 프로파일의 FQDN 집합은 전체 도메인을 나타내는 문자열 또는 PCRE(Perl Compatible Regular Expression)로 표시되는 문자열로 지정됩니다.

Note FQDN 일치 개체는 FQDN(user-specified row)을 포함하는 테이블로 구성됩니다.

행에는 수행할 로그 관련 작업이 포함되지 않습니다. 이는 FQDN 일치 개체가 첫 번째 레벨 일치 기준이기 때문입니다. 허용하려는 FDQN의 명확한 목록이 있는 경우 FQDN 일치 개체를 사용할 수 있습니다. 규칙 일치 후 기준에 따라 허용하려는 범주가 있는 경우 FQDN 필터링을 사용합니다. 자세한 내용은 FQDN(Fully Qualified Domain Name) 필터 프로파일, on page 159를 참고하십시오.

각 FQDN 일치 개체의 제한은 다음과 같습니다.

- 사용자 지정 최대 행: 254(독립형 또는 독립형 그룹)
- 행당 최대 FQDN 수: 60
- 최대 FQDN 문자 길이: 255

다단계 도메인(예: `www.example.com`)을 지정할 때 . 문자를 이스케이프해야 합니다(예: `www\.example\.com`). 그렇지 않으면 단일 문자에 대한 와일드카드로 처리합니다.

독립형 및 그룹

FQDN 일치 개체는 독립형 또는 그룹 유형으로 지정할 수 있습니다.

FQDN 일치 독립형 개체에는 FQDN이 포함되어 있습니다. 개체가 하나 이상의 정책 규칙 집합 규칙 집합에 직접 적용되거나 FQDN 일치 그룹 개체와 연결됩니다.

FQDN 일치 그룹 개체에는 여러 용도로 정의하고 그룹 개체로 함께 결합할 수 있는 독립형 FQDN 개체의 순서가 지정된 목록이 포함되어 있습니다. 그룹 개체는 하나 이상의 정책 규칙 집합 규칙에 직접 적용할 수 있습니다. 각 팀은 특정 독립형 프로파일을 생성하고 관리할 수 있습니다. 이러한 독립형 프로파일은 그룹 프로파일로 결합하여 활용 사례에 따라 계층 구조 또는 다양한 조합을 생성할 수 있습니다. 모든 항목에 적용되는 전역 FQDN 목록, 서로 다른 CSP에 적용되는 CSP 관련 목록, 그리고 애플리케이션에 적용되는 애플리케이션 관련 목록 등의 조합을 예로 들 수 있습니다.

독립형 **FQDN** 일치 개체 생성

단계 **1** **Manage(**관리**)** > **Security Policies(**보안 정책**)** > **FQDNs**로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** 프로파일 이름 및 설명을 제공합니다

단계 **4** Type(유형)을 Standalone(독립형)으로 지정합니다.

단계 **5** **Add(**추가**)**를 클릭하여 새 행을 생성합니다.

단계 **6** 개별 FQDN 지정합니다(예: www.twitter.com,.*.google.com).

a) 각 FQDN은 PCRE(Perl Compatible Regular Expression)로 지정됩니다.

b) . 문자를 이스케이프하지 않으면 단일 문자 와일드카드로 처리됩니다.

단계 **7** (선택 사항) 암호 해독이 바람직하지 않거나 가능한 FQDN에 대해 Decryption Exception(암호 해독 예외)을 지정합니다. 암호 해독 예외를 고려해야 하는 가능한 이유는 다음과 같습니다.

단계 **8** 암호화된 트래픽(금융 서비스, 방위, 의료 등)의 검사에 대한 거부 요청

단계 **9** 암호 해독이 불가능한 SSO 인증 트래픽

단계 **10** 프록시 설정할 수 없는 NTLM 트래픽

단계 **11** 완료되면 **Save(**저장**)**를 클릭합니다.

그룹 **FQDN** 일치 개체 생성

단계 **1** **Manage(**관리**)** > **Security Policies(**보안 정책**)** > **FQDNs**로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** 프로파일 이름 및 설명을 제공합니다

단계 **4** Type(유형)을 Group(그룹)으로 지정합니다.

단계 **5** 초기 독립형 프로파일을 선택합니다(하나 이상의 독립형 프로파일이 필요함).

단계 **6** 추가 독립형 프로파일을 지정합니다.
단계 **7** **Add FQDN Profile(FQDN** 프로파일 추가**)**을 클릭하여 새 행을 생성합니다.
단계 **8** 독립형 프로파일을 선택합니다.
단계 **9** 완료되면 **Save(**저장**)**를 클릭합니다.

개체 연결

정책 규칙을 생성/편집하려면 규칙를 확인합니다.

15 장

서비스 개체

역방향 프록시 서비스 개체(인그레스)

인그레스 서비스 개체는 인그레스/역방향 프록시 규칙에서 사용됩니다. 개체는 멀티 클라우드 방어 게이트웨이가 수신하고 대상/백엔드 주소에 전달하는 트래픽을 수신하는 리스너 포트를 정의합니다. TLS 인증서가 구성된 암호 해독 프로파일로 리스너 포트를 구성할 수 있습니다. 트래픽이 리스너 포트에 도달하면 멀티 클라우드 방어 게이트웨이은(는) 설정된 TLS 인증서를 반환합니다. 다음과 같은 구성 가능한 옵션을 고려하십시오.

- 이 포트에서 SNI를 설정할 수 있습니다. 이렇게 하면 단일 리스너 포트(예: 443)를 SNI를 기반으로 여러 백엔드 대상에 프록시할 수 있습니다.
- 서비스에 L7 DoS(L7 Denial of Service)를 구성하여 URI 및/또는 HTTP 메서드에 대한 속도 제한을 설정할 수 있습니다.
- 대상은 트래픽을 전달할 포트 및 백엔드 주소 개체를 정의합니다. 프록시 설정된 트래픽은 HTTP, HTTPS, TCP 또는 TLS로 전달할 수 있습니다.

역방향 프록시 서비스 개체를 생성하고 추가하려면 다음 절차를 따르십시오.

단계 **1** **Manage(**관리**)** > **Security Policies(**보안 정책**)** > **Services(**서비스**)**로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** **Reverse Proxy(**역방향 프록시**)**를 클릭합니다.

단계 **4** **Name(**이름**)**과 **Description(**설명**)**을 제공합니다.

단계 **5** 아래에 정의된 대로 프록시 매개변수를 구성합니다.

옵션	설명
암호 해독 프로파일	프록시 서비스에 사용할 서버 인증서도 포함하는 암호 해독 프로파일을 할당합니다.
대상 포트	대상 포트를 할당합니다. 대부분의 웹 기반 서비스의 경우 대상 포트는 443입니다. 이 포트는 수신 트래픽을 수신하는 포트 멀티 클라우드 방어 게이트웨이입니다.
프로토콜	TCP가 기본값입니다.
SNI	SNI 목록을 입력합니다.
L7 DoS	이 프록시 서비스에 할당할 레이어 7 DoS 프로파일을 입력합니다.
대상 백엔드 포트	대상/백엔드 애플리케이션 포트 번호를 입력합니다.
프로토콜	백엔드 프로토콜을 선택합니다.
주소	백엔드 IP 주소를 선택합니다. 대부분의 경우 IP 주소는 내부 로드 밸런서의 프런트엔드 IP가 됩니다.

Note 여러 포트에서 프록시 서비스를 실행해야 하는 경우 항목을 더 추가할 수 있습니다. 그러나 모든 포트는 동일한 인증서를 제공하며 동일한 백엔드 대상 주소 개체에 프록시됩니다.

전달 프록시 서비스 개체(이그레스/이스트-웨스트)

전달 프록시 서비스는 특히 HTTP 기반 트래픽에 사용됩니다. 개체는 멀티 클라우드 방어 게이트웨이이(가) 수신 트래픽을 수신하고 TLS SNI 확장 헤더 또는 HTTP 호스트 헤더에서 사용 가능한 주소/호스트에 전달하는 리스너 포트를 정의합니다.

Note 이그레스/이스트웨스트 트래픽에 이를 사용하는 것이 좋습니다.

다음 절차를 사용하여 정방향 프록시 서비스를 생성하고 추가합니다.

단계 **1** **Manage(**관리**)** > **Security Policies(**보안 정책**)** > **Services(**서비스**)**로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** **Forward Proxy(**전달 프록시**)**를 클릭합니다.

단계 **4** 이름과 설명을 제공합니다.

단계 **5** 경우에 따라 일치시킬 애플리케이션 ID를 선택합니다.

단계 **6** 아래에 정의된 대로 프록시 매개변수를 구성합니다.

옵션	설명
암호 해독 프로파일	인증서도 포함하는 암호 해독 프로파일을 할당합니다. 멀티 클라우드 방어은(는) 이 프로파일에서 제공하는 인증서로 서명하여 외부 인증서를 가장합니다. 루트 인증서는 모든 클라이언트 애플리케이션 인스턴스에 설치된 것으로 가정됩니다.
대상 포트	대상 포트를 할당합니다. 대부분의 웹 기반 서비스의 경우 대상 포트는 443입니다.
프로토콜	HTTP 또는 HTTPS.

Note
- 멀티 클라우드 방어은(는) **Dst Port(**대상 포트**)** 에서 수신 대기하고 HTTP 호스트 헤더 또는 TLS SNI 헤더 패킷을 기다립니다. 멀티 클라우드 방어이(가) 패킷을 수신한 후 프로토콜을 사용하여 호스트에 연결합니다. 프로토콜이 HTTPS인 경우, 외부 호스트에서 수신된 인증서 데이터는 암호 해독 프로파일의 인증서에 의해 서명되고 클라이언트로 전송됩니다. 인증서 오류를 방지하려면 클라이언트 앱 인스턴스에 루트 인증서를 설치해야 합니다.
- 지정된 대상 포트의 경우 모든 서비스 개체의 정책 규칙 집합에는 암호 해독 프로파일(루트 CA 인증서) 연결이 하나만 있을 수 있습니다.
- 정방향 프록시 세션 중에 멀티 클라우드 방어 게이트웨이에서는 DNS 요청 시간 초과 30초 및 캐시 만료 시간 초과 TTL 초로 대상에 대한 DNS 조회를 수행합니다.

서비스 개체 전달(이그레스/이스트-웨스트)

전달 서비스 개체는 전달 규칙에서 사용됩니다. 이 유형의 규칙/서비스와 일치하는 트래픽은 프록시 설정되지 않고 있는 그대로 전달됩니다. 이는 암호화된 트래픽에 대한 심층 패킷 검사와 애플리케이션 ID가 없음을 의미합니다.

Note East-West 트래픽에 이 옵션을 사용하는 것이 좋습니다.

전달 서비스 개체를 생성하고 추가하려면 다음 절차를 따르십시오.

단계 **1** **Manage(**관리**)** > **Security Policies(**보안 정책**)** > **Services(**서비스**)**로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** **Forwarding(**전달**)**을 클릭합니다.

단계 **4** 이름과 설명을 제공합니다.

단계 **5** 멀티 클라우드 방어은(는) 서비스 레벨별 소스 NAT를 지원합니다. 소스 IP 보존이 필요한 트래픽(예: 이스트-웨스트 트래픽)의 경우 SNAT를 비활성화합니다.

이그레스 트래픽의 경우 SNAT는 항상 활성화되어야 합니다.

단계 **6** 아래에 정의된 대로 포트 매개변수를 구성합니다.

옵션	설명
대상 포트	대상 포트 또는 대상 포트 범위를 `start-end`로 할당합니다.
프로토콜	TCP, UDP, ICMP

Note 전달 정책에서 심층 패킷 검사 작업은 암호화되지 않은 트래픽 에서만 발생합니다.

16 장

인증서 및 키

인증서 및 키

TLS 인증서 및 키는 프록시 시나리오에서 멀티 클라우드 방어 게이트웨이에 의해 사용됩니다. 인그레스(역방향 프록시) 사용자는 멀티 클라우드 방어 게이트웨이을(를) 통해 애플리케이션에 액세스하며 서비스에 대해 구성된 인증서를 제공합니다. 이그레스(정방향 프록시)의 경우 외부 호스트의 인증서가 가장되고 정의된 인증서로 서명됩니다.

인증서 본문을 멀티 클라우드 방어 컨트롤러(으)로 가져옵니다. 개인 키는 다음과 같은 방식으로 제공할 수 있습니다.

- 개인 키 콘텐츠를 가져옵니다.
- AWS Secrets Manager에 저장하고 암호 이름을 제공합니다.
- AWS KMS에 저장하고 암호 텍스트 콘텐츠를 제공합니다.
- GCP Secrets Manager에 저장하고 암호 이름을 제공합니다.
- Azure 키 저장소 및 암호에 저장하고 키 저장소 및 암호 이름을 입력합니다.

테스트 목적으로 멀티 클라우드 방어 컨트롤러에서 자체 서명 인증서를 생성할 수도 있습니다. 이는 로컬 파일 시스템에서 개인 키 콘텐츠를 가져오는 것과 유사합니다.

Note 생성된 인증서는 편집할 수 없습니다. 기존 인증서를 교체해야 하는 경우, 새 인증서를 생성하고 새 인증서를 참조하도록 암호 해독 프로파일을 편집한 다음 기존 인증서를 삭제해야 합니다.

인증서 및 개인 키를 가져올 때 멀티 클라우드 방어 컨트롤러/UI는 불일치가 있는 경우 이를 탐지할 수 있습니다. 그러나 클라우드 서비스 제공자 내에 개인 키가 저장되어 있는 다른 가져오기 방법을 사용하는 경우, 멀티 클라우드 방어 컨트롤러/UI는 불일치가 있는 경우 이를 탐지할 수 없습니다. 이는 클라우드 서비스 제공자 내에서 개인 키를 비공개로 유지하기 위한 설계입니다. 멀티 클라우드 방어 게이트웨이에서 개인 키가 필요할 때 개인 키에 액세스하여 사용되며, 불일치가 발생하면 오류가 생성됩니다.

인증서 가져오기

단계 **1** **Mange(**관리**)** > **Security Policies(**보안 정책**)** > **Certificates(**인증서**)**로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** **Method(**방법**)**에 대한 프롬프트가 나타나면 **Import your Certificate and Private Key(**인증서 및 개인 키 가져오기**)**를 선택합니다.

단계 **4** **Certificate Body(**인증서 본문**)**에 인증서 파일의 내용을 복사합니다. 여기에는 인증서 및 체인이 포함될 수 있습니다.

단계 **5** **Certificate Private Key(**인증서 개인 키**)**에 있는 개인 키의 내용을 복사합니다.

단계 **6** (선택 사항) 인증서와 체인이 다른 파일에 있는 경우 체인을 **Certificate Chain(**인증서 체인**)**으로 가져옵니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

AWS - KMS

단계 **1** **Mange(**관리**)** > **Security Policies(**보안 정책**)** > **Certificates(**인증서**)**로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** Method(방법)에서 *Import AWS - KMS(AWS* 가져오기 *- KMS)*를 선택합니다.

단계 **4** 클라우드 어카운트 및 지역을 선택합니다.

단계 **5** *Certificate Body(*인증서 본문*)*에 인증서 파일의 내용을 복사합니다. 여기에는 인증서 및 체인이 포함될 수 있습니다.

단계 **6** AWK KMS 암호화 암호 텍스트를 *Private Key Cipher Text(*프라이빗 키 암호 텍스트*)*에 복사합니다. .

단계 **7** **Save(**저장**)**를 클릭합니다.

AWS - Secrets Manager

단계 **1** **Mange(**관리**)** > **Security Policies(**보안 정책**)** > **Certificates(**인증서**)**로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** Method(방법)에서 *Import AWS - Secret(AWS* 가져오기 - 암호*)*을 선택합니다.

단계 **4** 클라우드 어카운트 및 지역을 선택합니다.

단계 **5** *Certificate Body(*인증서 본문*)*에 인증서 파일의 내용을 복사합니다. 여기에는 인증서 및 체인이 포함될 수 있습니다.

단계 **6** 개인 키가 저장된 Secret Name(비밀 이름)을 제공합니다. 개인 키 콘텐츠는 AWS Secrets Manager에서 *Other type of Secrets(*기타 유형의 비밀*)* > *Plain Text(*일반 텍스트*)*로 저장해야 합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

Azure 키 저장소

단계 **1** **Mange(**관리**)** > **Security Policies(**보안 정책**)** > **Certificates(**인증서**)**로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** Method(방법)에서 *Import Azure - Key Vault Secret(Azure* 가져오기 -키 저장소 암호)을 선택합니다.

단계 **4** 클라우드 어카운트 및 지역을 선택합니다.

단계 **5** *Certificate Body(*인증서 본문*)*에 인증서 파일의 내용을 복사합니다. 여기에는 인증서 및 체인이 포함될 수 있습니다.

단계 **6** Key Vault Name(키 저장소 이름) 및 개인 키가 저장된 암호 이름을 제공합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

GCP - Secret Manager

단계 **1** **Mange(**관리**)** > **Security Policies(**보안 정책**)** > **Certificates(**인증서**)**로 이동합니다.

단계 **2** **Create(**생성**)** 클릭

단계 **3** Method(방법)에서 *Import GCP - Secret(*가져오기 *GCP* - 암호*)*을 선택합니다.

단계 **4** 클라우드 어카운트를 선택합니다.

단계 **5** 암호 이름(전체 경로) 및 암호 버전을 제공합니다.

단계 **6** *Certificate Body(*인증서 본문*)*에 인증서 파일의 내용을 복사합니다. 여기에는 인증서 및 체인이 포함될 수 있습니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

서버 인증서 검증

게이트웨이가 정방향 프록시로 작동할 경우에는 서버 인증서 검증이 트래픽 처리에 자동으로 포함됩니다. 트래픽을 처리하기 위해 지정된 서버 인증서 검증 작업이 필요하지는 않지만, 일반적인 보안을 향상시킬 수 있습니다. 기본적으로 서버 인증서 검증이 활성화되어 있지 않으며 유효하지 않은 서버 인증서가 있을 수 있는 서버로 이동하는 트래픽은 통과합니다. 서버 인증서 검증 작업을 활성화하여 허용해서는 안 되는 트래픽 또는 서버 인증서 검증 상태와 상관없이 신뢰해야 하는 특정 트래픽에 대한 규칙의 우선 순위를 지정합니다.

참고 이 검증 프로세스는 정방향 프록시 환경 및 암호 해독이 활성화된 경우에만 적용됩니다.

일반 규칙 작업의 TLS 암호 해독 프로파일에서 서버 인증서 검증 작업을 활성화하는 것이 좋습니다. TLS 암호 해독 선택을 재정의해야 하는 경우 FQDN 서비스 개체를 수정하여 검증 작업을 활성화할 수 있습니다. 두 가지 방법으로 서버 인증서 검증을 포함하고 활성화할 수 있습니다.

- TLS 암호 해독 프로파일의 서버 인증서 검증
- FQDN 서비스 개체의 서버 인증서 검증

TLS 암호 해독 프로파일의 서버 인증서 검증

TLS 암호 해독 프로파일 내에서 서버 인증서 검증을 위한 작업을 선택하는 경우, 이 암호 해독 프로파일을 사용하는 모든 규칙 집합에서 이 작업이 사용됩니다. 기본적으로 검증 작업은 서버 인증서의 유효 여부에 관계없이 모든 트래픽을 허용하도록 구성되며 멀티 클라우드 방어은(는) HTTP 로그 내에 알림을 생성하지 않습니다.

참고 **Log(로그)**에 대한 검증 확인을 활성화한 경우 **Investigate(조사)** > **Flow Analytics(플로우 분석)** > **HTTPS Logs(HTTPS** 로그**)**에서 로그를 찾습니다.

다음 절차를 사용하여 TLS 암호 해독 프로파일에서 서버 인증서 검증을 활성화합니다.

단계 **1** 멀티 클라우드 방어 컨트롤러에서 **Manage(관리)** > **Profiles(프로파일)** > **Decryption(암호 해독)**으로 이동합니다.

단계 **2** 서버 인증서 검증을 추가할 TLS 암호 해독 프로파일을 선택합니다. 프로파일이 준비되지 않았다면 여기에서 생성하십시오. 자세한 내용은 암호 해독 프로파일, 145 페이지를 참조하십시오.

단계 **3** 암호 해독 프로파일을 편집합니다.

단계 **4** **Profile Properties(프로파일 속성)** 섹션에서 **Invalid Server Certificate Action(유효하지 않은 서버 인증서 작업)** 드롭다운 목록을 확장합니다.

단계 **5** 다음 옵션 중 하나를 선택합니다.

- **Deny Log(**거부 로그**)** - 이 옵션은 검증된 서버 인증서를 제공하지 않는 연결을 자동으로 삭제하고 인시던트를 로깅합니다.
- **Deny No Log(**거부 로그 없음**)**- 이 옵션은 검증된 서버 인증서를 제공하지 않으며 인시던트를 로깅하지 않는 연결을 자동으로 삭제합니다.
- **Allow Log(**허용 로그**)** - 이 옵션은 검증된 서버 인증서를 제공하지 않는 연결의 통과를 허용하고 인시던트를 로깅합니다.
- **Allow No Log(**허용 로그 없음**)**- 이 옵션은 검증된 서버 인증서를 제공하지 않는 연결이 통과하도록 허용하며, 인시던트를 로깅하지 않습니다. 이것이 기본 작업 선택 사항입니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

TLS 암호 해독 프로파일이 전달 프록시 서비스 개체와 올바르게 연결되어 있는지 확인하십시오. 자세한 내용은 전달 프록시 서비스 개체(이그레스/이스트-웨스트), 122 페이지를 참조하십시오.

TLS 암호 해독 프로파일이 서비스 개체에 포함되면 정책 내의 규칙 순서가 원하는 트래픽 처리 방법을 지원하는 순서로 지정되었는지 확인합니다.

FQDN 서비스 개체의 서버 인증서 검증

FQDN 서비스 개체 내 잘못된 서버 인증서 검증은 선택 사항입니다. 지정된 경우 TLS 암호 해독 프로파일에 지정된 동작을 재정의합니다. 여기서 선택 항목을 지정하지 않으면 추가 작업이 없거나 재정의 작업이 수행되지 않습니다. FQDN 서비스 개체 내에서 유효하지 않은 서버 인증서 검증을 사용하여 특정 서버로 향하는 트래픽을 차단하거나 허용할 수 있습니다. 다른 방법으로는 TLS 암호 해독 프로파일에 의해 차단되거나 허용될 수 있습니다.

로그 검증 확인을 활성화하면 이러한 로그는 **Investigate(**검사**)** > **Flow Analytics(**플로우 분석**)** > **HTTPS Logs(HTTPS** 로그**)**에 위치합니다.

FQDN 서비스 개체에 서버 인증서 검증 작업을 포함하려면 다음 절차를 사용합니다.

단계 **1** 멀티 클라우드 방어 컨트롤러에서 **Manage(**관리**)** > **Security Profile(**보안 프로파일**)** > **FQDNs**로 이동합니다.

단계 **2** 수정할 FQDN 서비스 개체를 선택합니다.

단계 **3** 선택한 FQDN 서비스 개체를 편집합니다.

단계 **4** 규칙 집합에 포함된 FQDN 서비스 개체의 목록에서 **Invalid Server Certificate Action(**유효하지 않은 서버 인증서 작업**)** 드롭다운 메뉴를 확장하고 다음 옵션 중 하나를 선택합니다.

- **Deny Log(**거부 로그**)** - 검증된 서버 인증서를 제공하지 않는 연결을 자동으로 삭제하고 인시던트를 로깅합니다.
- **Deny No Log(**거부 로그 없음**)** - 검증된 서버 인증서를 제공하지 않으며 인시던트를 로깅하지 않는 연결을 자동으로 삭제합니다.

- **Allow Log(**허용 로그**) -** 검증된 서버 인증서를 제공하지 않는 연결의 통과를 허용하고 인시던트를 로깅합니다.
- **Allow No Log(**허용 로그 없음**) -** 서버 인증서를 제공하지 않는 연결이 통과하도록 허용하며, 인시던트를 로깅하지 않습니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

FQDN 서비스 개체가 규칙 또는 규칙 집합과 올바르게 연결되어 있는지 확인하십시오. 자세한 내용은 규칙 집합 및 규칙 집합 그룹, 96 페이지를 참조하십시오.

FQDN 서비스 개체가 정책에 설정된 규칙 또는 규칙과 성공적으로 연결되면 정책의 규칙 순서가 원하는 트래픽 처리 방법을 지원하는 순서로 지정되어 있는지 확인합니다.

17 장

인증서 및 키 기술 노트

자체 서명된 루트 CA 생성

자체 서명된 루트 CA(인증 기관)를 생성합니다.

```
openssl genrsa -out myca.key 2048
# password protect key: openssl genrsa -out myca.key -des3 2048
openssl req -x509 -new -key myca.key -sha384 -days 1825 -out myca.crt \
  -subj "/C=US/ST=CA/L=Santa
Clara/O=MyOrg/OU=SecurityOU/CN=rootca.myorg.com/emailAddress=rootca@myorg.com"
```

이 루트 CA는 사용자(클라이언트) 머신에 신뢰할 수 있는 루트 CA로 설치해야 합니다.

Note **MacOS**를 사용하여 셀프 서명한 인증서를 생성하면 정방향 및 역방향 프록시 시나리오에 사용할 수 있는 적절한 인증서가 생성되지 않습니다. 인증서에서는 *Is CA* 옵션이 *True*로 설정되어 있어야 하며, MacOS를 사용하여 생성된 인증서는 그렇지 않습니다. 셀프 서명 인증서는 멀티 클라우드 방어 UI(Certificates(인증서)(Certificates(인증서)(Certificates)) - Create(생성(Create)) - Generate(생성) 내에서 또는 **Linux**를 사용하여 생성하는 것이 좋습니다.

자체 서명 루트 CA에서 서명한 인증서 생성

위의 루트 인증 기관(CA)에서 서명한 인증서를 생성합니다. 이 인증서는 애플리케이션에서 사용할 수 있습니다.

```
openssl genrsa -out app1.key 2048
# password protect key: openssl genrsa -out -des3 app1.key 2048
```

```
openssl req -new -key app1.key -out app1.csr \
  -subj "/C=US/ST=CA/L=Santa
Clara/O=MyOrg/OU=AppOU/CN=app1.myorg.com/emailAddress=app1@myorg.com"
openssl x509 -req -in app1.csr -CA myca.crt -CAkey myca.key -out app1.crt -sha384\
  -days 365 -CAcreateserial -extensions SAN \
  -extfile <(printf "
[SAN]\nbasicConstraints=CA:false\nsubjectAltName=DNS:app1.myorg.com,DNS:app1-
1.myorg.com,IP:192.168.10.21,IP:192.168.10.22")
```

루트 CA에 의해 서명된 중간 CA 생성

루트 CA(인증 기관)를 사용하여 앱 인증서에 서명하지 않으려면 루트 CA가 서명한 중간 CA를 생성한 다음 중간 CA를 사용하여 앱 인증서에 서명합니다. 앱 인증서에 중간 인증서를 추가합니다. 이 시점에서 앱 인증서에 체인으로 연결된 2개의 인증서가 있습니다.

```
openssl genrsa -out interca.key 2048
# password protect key: openssl genrsa -out -des3 interca.key 2048
openssl req -new -key interca.key -out interca.csr \
  -subj "/C=US/ST=CA/L=Santa
Clara/O=MyOrg/OU=InterSecurityOU/CN=interca1.myorg.com/emailAddress=interca1@myorg.com"
openssl x509 -req -in interca.csr -CA myca.crt -CAkey myca.key -out interca.crt - sha384 \
  -days 365 -CAcreateserial -extensions SAN \
  -extfile <(printf "[SAN]\nbasicConstraints=CA:true")
```

중간 CA를 사용하여 서명된 앱 인증서

```
openssl genrsa -out app1.key 2048
# password protect key: openssl genrsa -out -des3 app1.key 2048
openssl req -new -key app1.key -out app1.csr \
  -subj "/C=US/ST=CA/L=Santa
Clara/O=MyOrg/OU=AppOU/CN=app1.myorg.com/emailAddress=app1@myorg.com"
openssl x509 -req -in app1.csr -CA interca.crt -CAkey interca.key -out app1.crt - sha384 \
  -days 365 -CAcreateserial -extensions SAN \
  -extfile <(printf "
[SAN]\nbasicConstraints=CA:false\nsubjectAltName=DNS:app1.myorg.com,DNS:app1-
1.myorg.com,IP:192.168.10.21,IP:192.168.10.22")
```

파일에 app1.crt 및 interca.crt를 추가하여 결합된 인증서를 만들고 애플리케이션에서 결합된 인증서를 사용합니다. 루트 CA는 클라이언트 머신에 신뢰할 수 있는 루트 CA로 설치해야 합니다.

호스트에서 루트 CA를 신뢰할 수 있는 CA로 설치

OS	명령
Ubuntu	인증서 파일을 `/usr/local/share/ca-certificates`로 복사하고 `sudo update-ca- certificates` 명령을 실행합니다.
CentOS	인증서 파일을 `/etc/pki/ca-trust/source/anchors`로 복사하고 `sudo update-ca- trust extract` 명령을 실행합니다.

OS	명령
Windows	파일을 더블 클릭하고 신뢰할 수 있는 루트에 인증서를 추가하거나 `certutil -addstore "Root" <crt-file>` 명령을 실행합니다.

VII 부

트래픽 검색 및 가시성

18 장

트래픽 유형

활성화된 경우, 트래픽이 규칙에 도달할 때마다 트래픽 로그가 생성됩니다. 이러한 로그 상호 작용은 소스 및 대상 IP 주소, 포트 번호 및 사용된 프로토콜을 포함하여 수신 및 발신 트래픽에 대한 정보를 기록합니다. 로그는 활동을 모니터링하거나, 잠재적인 보안 침해를 조사하거나, 방화벽의 상태를 계속 감시하는 네트워크 감사에 매우 유용합니다. 트래픽 가시성은 언제든지 활성화할 수 있지만 클라우드 서비스 제공자 계정을 온보딩하고 게이트웨이 정책을 할당한 직후에는 트래픽을 활성화하는 것이 좋습니다.

트래픽 가시성을 활성화하는 것은 클라우드 어카운트 유형마다 다른 프로세스이지만, 일반적으로 클라우드 어카운트의 지역, 모니터링할 VPC/VNet, 네트워크 보안 그룹 및 로그용 클라우드 스토리지 어카운트과 같은 어카운트 특성을 식별해야 합니다.

쉬운 설정 마법사를 사용하여 계정을 온보딩하지 않은 경우 또는 트래픽 가시성 활성화에서 트래픽 가시성을 활성화하지 않은 경우에는 다음 로그를 활성화하는 것이 좋습니다.

- NSG 플로우 로그
- VPC 플로우 로그
- DNS 로그
- Route53 쿼리 로깅

- DNS 로그 활성화, 137 페이지
- VPC 플로우 로그 활성화, 139 페이지

DNS 로그 활성화

AWS: DNS 로그 활성화

이전 섹션의 CloudFormation 템플릿에서 스택을 생성하는 동안 S3 버킷이 생성된 경우, route53 쿼리 로그의 대상 역할을 하는 템플릿에 의해 S3 버킷이 생성됩니다. DNS 쿼리 로그에 대해 모니터링되는 VPC는 수동으로 추가해야 합니다.

단계 **1** AWS 콘솔에서 Route53Query Logging(Route53Query 로깅)을 클릭합니다.

단계 **2** 템플릿으로 생성된 쿼리 로거를 선택합니다. 템플릿에 제공된 접두사 이름을 가진 로거를 찾습니다.

단계 **3** 선택 및 트래픽 인사이트를 가져올 모든 VPC를 선택하고 **Add(**추가**)**를 클릭합니다.

1. "쿼리를 로깅하는 VPC" 섹션에서 **Log querys for VPCs(VPC**에 대한 쿼리 로깅**)** 또는 **Add VPC(VPC** 추가**)**를 클릭합니다.
2. 모든 VPC를 선택하고 **Choose(**선택**)**를 클릭합니다.

GCP: DNS 로그 활성화

GCP DNS 쿼리 로그를 활성화하려면 아래 단계를 수행합니다.

단계 **1** GCP 콘솔에서 VPC 네트워크로 이동합니다.

단계 **2** Google Cloud 쉘을 열고 다음 명령을 실행합니다.

```
gcloud dns policies create POLICY_NAME --networks=NETWORK --enable-logging
```

단계 **3** **Cloud Storage(**클라우드 스토리지**)** 섹션으로 이동하여 스토리지 버킷을 생성합니다. 스토리지 버킷을 생성할 때 모든 항목을 기본값으로 둘 수 있습니다.

Note *DNS* 및 *VPC* 로그 모두 동일한 클라우드 스토리지 버킷을 공유할 수 있습니다.

단계 **4** **Logs Route(**로그 경로**)** 섹션으로 이동합니다.

단계 **5** **Create Sink(**싱크 생성**)**를 클릭합니다.

단계 **6** 싱크 이름을 제공합니다.

단계 **7** 싱크 서비스에 대해 "클라우드 스토리지 버킷"을 선택합니다.

단계 **8** 위에서 생성한 클라우드 스토리지 버킷을 선택합니다.

단계 **9** "Choose logs to include in sink(싱크에 포함할 로그 선택)" 섹션에서 `resource.type="dns_query"` 문자열을 입력합니다.

아래 단계는 GCP에 대한 VPC 플로우 로그의 단계와 동일합니다. 클라우드 스토리지 버킷을 공유하는 경우 아래 단계를 한 번만 수행하면 됩니다.

단계 **10** **Create Sink(**싱크 생성**)**를 클릭합니다.

단계 **11** **IAM** > **Roles(**역할**)**로 이동합니다.

단계 **12** **storage.buckets.list** 권한이 있는 사용자 지정 역할을 생성합니다.

단계 **13** 다음 권한으로 다른 사용자 지정 역할을 생성합니다.

storage.buckets.get storage.objects.get storage.objects.list.

단계 **14** 두 맞춤형 역할을 모두 멀티 클라우드 방어 컨트롤러에 대해 생성된 서비스 어카운트에 추가합니다. 두 번째 사용자 지정 역할을 추가할 때 다음 조건을 입력합니다.

```
(resource.type == "storage.googleapis.com/Bucket" || resource.type ==
 "storage.googleapis.com/Object") &&
resource.name.startsWith('projects/_/buckets/<cloud storage name>')
```

단계 **15** **Pub/Subs**로 이동합니다.

단계 **16** **Create Topic(**주제 생성**)**을 클릭합니다.

단계 **17** 주제 이름을 제공하고 **create(**생성**)**를 클릭합니다.

단계 **18** **Subscriptions(**구독**)**를 클릭합니다. 방금 생성한 주제에 대해 생성된 구독이 있음을 확인할 수 있습니다.

단계 **19** 구독을 편집합니다.

단계 **20** 전달 유형을 **Push(**푸시**)**로 변경합니다.

단계 **21** **Push(**푸시**)**를 선택하면 엔드포인트 URL을 입력합니다.

`https://prod1-webhook.vtxsecurityservices.com:8093/webhook/<tenant name> /gcp/cloudstorage.sys`. 테넌트 이름은 멀티 클라우드 방어에 의해 할당됩니다. 테넌트 이름을 보려면 멀티 클라우드 방어 컨트롤러(으)로 이동하고 사용자 이름을 클릭합니다.

단계 **22** **Update(**업데이트**)**를 클릭합니다.

단계 **23** Google Cloud 쉘을 열고 클라우드 스토리지 알림을 생성하고 `gsutil notification create -t <TOPIC_NAME\> -f json gs://<BUCKET_NAME>` 명령을 실행합니다.

Azure: DNS 로그

Azure는 현재 DNS 로그 쿼리를 표시하지 않습니다. 멀티 클라우드 방어 컨트롤러은(는) 이 클라우드 서비스 제공자의 로그를 활성화할 수 없습니다.

VPC 플로우 로그 활성화

AWS: VPC 플로우 로그 활성화

이전 섹션의 CloudFormation 템플릿에서 스택을 생성하는 동안 S3 버킷이 생성된 경우, VPC 플로우 로그의 대상 역할을 하는 템플릿에 의해 S3 버킷이 생성됩니다. 각 VPC에 대해 플로우 로그를 활성화해야 합니다.

AWS VPC 흐름 로그를 활성화하려면 아래 단계를 수행합니다.

단계 **1** AWS 콘솔에서 VPC 섹션으로 이동합니다.

단계 **2** VPC를 선택하고 해당 VPC에 대한 **Flow Logs(**플로우 로그**)** 탭을 선택합니다.

단계 **3** 필터로 **All(**모두**)**을 선택합니다.

단계 **4** 대상으로 **Send to an Amazon S3 bucket(Amazon S3** 버킷으로 보내기**)**를 선택합니다.

단계 **5** CloudFormation 템플릿 스택의 tutput에서 복사한 S3 버킷 ARN을 제공합니다.

단계 **6** 로그 기록 형식으로 **Custom Format(**사용자 지정 형식**)**을 선택합니다.

단계 **7** 로그 형식 드롭다운에서 모든 필드를 선택합니다.

단계 **8** **Create Flow Log(**플로우 로그 생성**)**를 클릭합니다.

GCP: VPC 플로우 로그 활성화

GCP VPC 흐름 로그를 활성화하려면 아래 단계를 수행합니다.

단계 **1** GCP 콘솔에서**VPC network(VPC** 네트워크**)**로 이동합니다.

단계 **2** VPC 흐름 로그를 활성화하려면 **subnet(**서브넷**)**을 선택합니다.

단계 **3** 플로우 로그가 **On(**켜짐**)**으로 설정되어 있는지 확인합니다. 꺼져 있는 경우 **Edit(**편집**)** 옵션을 클릭하고 플로우 로그를 켭니다.

단계 **4** 플로우 로그를 활성화할 모든 서브넷에서 플로우 로그를 켭니다.

단계 **5** **Cloud Storage(**클라우드 스토리지**)** 섹션으로 이동하여 스토리지 버킷을 생성합니다. 스토리지 버킷을 생성할 때 모든 항목을 기본값으로 둘 수 있습니다.

Note DNS 및 VPC 로그 모두 동일한 클라우드 스토리지 버킷을 공유할 수 있습니다.

단계 **6** **Logs Route(**로그 경로**)** 섹션으로 이동합니다.

단계 **7** **Create Sink(**싱크 생성**)**를 클릭합니다.

단계 **8** 싱크의 이름을 입력합니다.

단계 **9** 싱크 서비스용 **Cloud Storage bucket(**클라우드 스토리지 버킷**)**을 선택합니다.

단계 **10** 위에서 생성한 클라우드 스토리지 버킷을 선택합니다.

단계 **11** **Choose logs to include inink(**싱크에 포함할 로그 선택**)** 섹션에 `logName:(projects/<project-id>/logs/compute.googleapis.com%2Fvpc_flows)` 문자열을 입력합니다.

클라우드 스토리지 버킷을 공유하는 경우 이 절차의 남은 단계를 한 번만 수행하면 됩니다.

단계 **12** **Create Sink(**싱크 생성**)**를 클릭합니다.

단계 **13** **IAM** > **Roles(**역할**)**로 이동합니다.

단계 **14** `storage.buckets.list` 권한이 있는 사용자 지정 역할을 하나 생성합니다.

단계 **15** 다음 권한이 있는 맞춤형 역할을 하나 생성합니다. `storage.buckets.get storage.objects.get storage.objects.list`.

단계 **16** 두 맞춤형 역할을 모두 멀티 클라우드 방어 컨트롤러에 대해 생성된 서비스 어카운트에 추가합니다. 두 번째 사용자 지정 역할을 추가할 경우 다음 조건을 입력합니다.

```
(resource.type == "storage.googleapis.com/Bucket" || resource.type ==
"storage.googleapis.com/Object") && resource.name.startsWith('projects/_/buckets/<cloud
storage name>')
```

단계 **17** **Pub/Subs**로 이동합니다.

단계 **18** **Create Topic(**주제 생성**)**을 클릭합니다.

단계 **19** 주제 이름을 제공하고 **Create(**생성**)**를 클릭합니다.

단계 **20** **Subscriptions(**구독**)**를 클릭합니다. 18단계에서 생성한 주제에 대한 구독이 생성됩니다.

단계 **21** 구독을 편집합니다.

단계 **22** **Delivery(**전달**)** 유형을 **Push(**푸시**)**로 변경합니다.

단계 **23** 이 URL을 엔드포인트 URL로 입력합니다. `https://prod1-webhook.vtxsecurityservices.com:8093/webhook/<tenant name> /gcp/cloudstorage.sys`.

멀티 클라우드 방어은(는) 테넌트 이름을 자동으로 할당합니다. 테넌트 이름을 보려면 멀티 클라우드 방어 컨트롤러(으)로 이동하고 사용자 이름을 클릭합니다.

단계 **24** **Update(**업데이트**)**를 클릭합니다.

단계 **25** Google Cloud 쉘을 열고 `gsutil notification create -t <TOPIC_NAME> -f json gs://<BUCKET_NAME>` 명령을 실행합니다.

Azure: NSG 플로우 로그 활성화

Azure VPC 흐름 로그를 활성화하려면 아래 단계를 수행합니다.

단계 **1** Azure 포털에서 **Resource Groups(**리소스 그룹**)** 섹션으로 이동합니다.

단계 **2** **Create(**생성**)** 버튼을 클릭합니다.

단계 **3** 구독을 선택하고 이 새 리소스 그룹의 이름을 제공합니다.

단계 **4** **Region(**지역**)**을 선택합니다. (예: (US) 미국동부).

단계 **5** **Review + create(**검토 + 생성**)** 버튼을 클릭합니다.

단계 **6** 스토리지 계정 섹션으로 이동하여 **Create(**생성**)** 버튼을 클릭합니다.

단계 **7** 방금 생성한 **Subscription(**구독**)** 및 **Resource(**리소스**)** 그룹을 선택합니다.

단계 **8** 리소스 그룹으로 동일한 **region(**지역**)**을 선택합니다.

단계 **9** 스토리지 계정의 이름을 제공합니다.

이중화는 LRS(Local-redundancy storage)를 사용할 수 없습니다.

단계 **10** **Review + create(**검토 + 생성**)** 버튼을 클릭합니다. NSG 플로우 로그가 저장되는 스토리지 계정이 생성됩니다.

단계 **11** **Subscription(**구독**)** 섹션으로 이동하여 최근에 생성된 구독을 찾습니다.

단계 **12** **Resource Providers(**리소스 제공자**)**로 이동합니다.

단계 **13** `microsoft.insights` 및 `Microsoft.EventGrid` 제공자가 등록되었는지 확인합니다. 등록되지 않은 경우 **Register(**등록**)** 버튼을 클릭합니다.

단계 **14** **Network Watcher(**네트워크 감시자**)** 섹션으로 이동합니다.

단계 **15** **Add(**추가**)**를 클릭하고 NSG 플로우 로그를 활성화할 지역을 추가합니다.

단계 **16** **Network Watcher(**네트워크 감시자**)** > **NSG flow logs(NSG** 플로우 로그**)**로 이동합니다.

단계 **17** NSG 플로우 로그를 활성화할 NSG에 대한 플로우 로그를 생성합니다. 위에서 생성한 스토리지 계정을 제공합니다. **Retention days(**보존 일수**)**를 30으로 설정합니다.

단계 **18** 생성된 스토리지 계정으로 이동하여 **Events(**이벤트**)**를 클릭합니다.

단계 **19** **Event Subscription(**이벤트 구독**)**을 클릭합니다.

단계 **20** 이 이벤트 구독의 이름을 제공합니다.

단계 **21** 위에서 생성한 리소스 그룹을 선택합니다.

단계 **22** 시스템 항목 이름을 제공합니다.

단계 **23** **Filter to Event Types(**이벤트 유형 필터링**)**의 경우 기본값은 **Blob Created(**블롭 생성됨**)** 및 **Blob Deleted(**블롭 삭제됨**)**입니다.

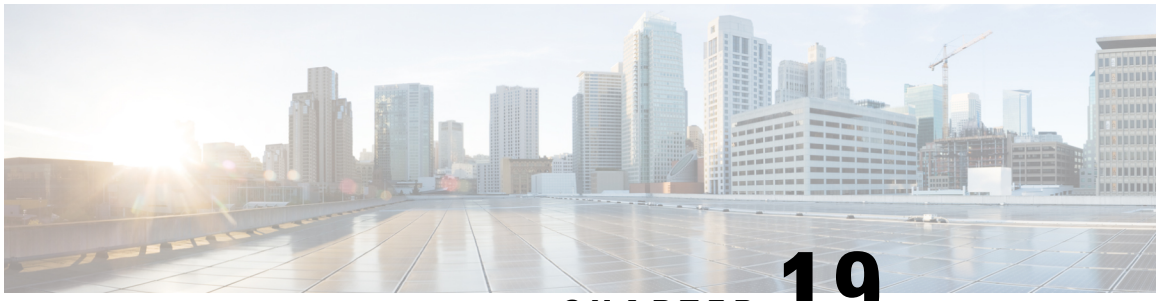
단계 **24** **Endpoint Type(**엔드포인트 유형**)**에 대해 **Webhook**를 선택합니다.

단계 **25** **Select endpoint(**엔드포인트 선택**)** 링크를 클릭합니다.

구독자 엔드포인트는 `https://prod1-webhook.vtxsecurityservices.com:8093/webhook/<tenant_name>/azure` 입니다. 테넌트 이름은 멀티 클라우드 방어에 의해 할당됩니다. 멀티 클라우드 방어 컨트롤러에서 사용자 이름을 클릭하여 테넌트 이름을 찾을 수 있습니다.

VIII 부

보안 프로파일



CHAPTER 19

보안 프로파일

암호 해독 프로파일

암호 해독 프로파일은 역방향 프록시 또는 정방향 프록시 시나리오에서 멀티 클라우드 방어 게이트웨이에 의해 사용됩니다. 연결이 프록시되면 프런트엔드 세션은 게이트웨이에서 종료되고, 서버에 새 백엔드 세션이 설정됩니다. 이러한 종료의 목적은 트래픽을 암호 해독하고 검사하여 악의적인 활동으로부터 보호하기 위한 것입니다. 암호화된 트래픽을 해독하려면 Decryption Profile(암호 해독 프로파일)이 필요합니다.

암호 해독 프로파일 생성

다음 절차에 따라 암호 해독 프로파일을 생성합니다.

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)** > **Decryption(**암호 해독**)**으로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 3 **Profile Name(**프로파일 이름**)** 및 **Description(**설명**)**을 지정합니다.

단계 4 **Certificate Method(**인증서 방법**)**으로 **Select Existing(**기존 선택**)**을 선택합니다.

단계 5 **Certificate(**인증서**)**로 원하는 인증서를 선택합니다.

단계 6 **Min TLS Version(**최소 **TLS** 버전**)**에서 암호 해독 프로파일이 허용하는 가장 낮은 TLS 버전을 선택합니다. 기본값은 TLS 1.0입니다.

단계 7 기본값 이외의(비 PFS) 암호 그룹을 사용하는 경우 Diffie-Hellman 또는 PKCS (RSA) 메뉴에서 원하는 암호 그룹 집합을 선택합니다.

단계 8 **Save(**저장**)**를 클릭합니다.

What to do next

- 프로파일 세부 정보 보기, on page 173
- 프로파일에 게이트웨이 연결 추가, on page 174

암호 해독 프로파일의 **TLS** 버전

멀티 클라우드 방어 게이트웨이은(는) 모든 TLS 버전(TLS 1.3, TLS 1.2, TLS 1.1, TLS 1.0)을 지원합니다. 사용자는 사용할 최소 TLS 버전을 지정할 수 있으며, 멀티 클라우드 방어 게이트웨이은(는) 지정된 최소 TLS 버전 이상인 TLS 버전을 협상합니다. 멀티 클라우드 방어 게이트웨이은(는) TLS 협상 중에 항상 가능한 가장 높은 TLS 버전을 사용합니다. 멀티 클라우드 방어 게이트웨이이(가) 지정된 최소 TLS 버전을 충족하는 버전을 협상할 수 없는 경우 멀티 클라우드 방어 게이트웨이에서는 세션을 삭제하고 `TLS_ERROR` 이벤트를 로깅합니다.

Note 게이트웨이에는 단일 최소 TLS 버전만 적용할 수 있습니다. 정책 규칙 집합 또는 정책 규칙 집합 그룹 내에서 사용되는 모든 서비스 개체에서 참조하는 모든 암호 해독 프로파일에 일관된 최소 TLS 버전을 사용해야 합니다. 다른 최소 TLS 버전이 지정된 경우, 적용할 최소 TLS 버전을 미리 결정할 수 없습니다.

암호 그룹

멀티 클라우드 방어 게이트웨이는 사용자가 선택 가능한 기본 암호 그룹 집합을 지원합니다. 기본 집합은 항상 선택되는 PFS 암호 그룹입니다. 사용자 선택 가능한 집합은 Diffie-Hellman 및 PKCS(RSA) 암호 그룹(사용자가 선택할 수 있음)입니다. 결합된 암호 그룹 집합(기본 및 사용자 선택)은 게이트웨이에서 안전한 프런트 엔드 암호화 세션을 설정하는 데 사용됩니다. 클라이언트는 선호하는 암호 그룹의 순서가 지정된 목록을 전송합니다. 게이트웨이는 클라이언트가 제출한 순서가 지정된 집합과 게이트웨이에서 사용 가능한 집합에서 선택한 암호 그룹으로 응답합니다. 클라이언트가 서버가 순서를 정의하도록 허용하는 경우, 게이트웨이에서 사용 가능한 순서가 지정된 집합과 클라이언트가 제출한 집합에서 암호 그룹을 선택합니다.

다음은 게이트웨이에서 지원하고 암호 해독 프로파일에서 사용 가능한 암호 그룹의 순서가 지정된 목록입니다.

카테고리	암호 그룹	키 교환	암호화	해시	기본
PFS	ECDHE-RSA-AES256-GCM-SHA384	ECDHE-RSA	AES256-GCM	SHA384	☐
PFS	ECDHE-RSA-AES256-CBC-SHA384	ECDHE-RSA	AES256-CBC	SHA384	☐
Diffie-Hellman	DH-RSA-AES256-GCM-SHA384	DH-RSA	AES256-GCM	SHA384	
PFS	DHE-RSA-AES256-GCM-SHA384	DHE-RSA	AES256-GCM	SHA384	☐
PFS	DHE-RSA-AES256-CBC-SHA256	DHE-RSA	AES256-CBC	SHA384	☐
PFS	DHE-RSA-AES256-CBC-SHA	DHE-RSA	AES256-CBC	SHA	☐
Diffie-Hellman	DH-RSA-AES256-SHA256	DH-RSA	AES256-CBC	SHA256	
Diffie-Hellman	DH-RSA-AES256-SHA	DH-RSA	AES256-CBC	SHA160	
PKCS(RSA)	AES256-GCM-SHA384	PKCS-RSA	AES256-GCM	SHA384	
PKCS(RSA)	AES256-SHA256	PKCS-RSA	AES256-CBC	SHA256	
PKCS(RSA)	AES256-SHA	PKCS-RSA	AES256-CBC	SHA160	
PFS	ECDHE-RSA-AES128-GCM-SHA256	ECDHE-RSA	AES128-GCM	SHA256	☐
PFS	ECDHE-RSA-AES128-CBC-SHA256	ECDHE-RSA	AES128-CBC	SHA256	☐
Diffie-Hellman	DH-RSA-AES128-GCM-SHA256	DH-RSA	AES128-GCM	SHA256	
PFS	DHE-RSA-AES128-GCM-SHA256	DHE-RSA	AES128-GCM	SHA256	☐
PFS	DHE-RSA-AES128-CBC-SHA256	DHE-RSA	AES128-CBC	SHA256	☐
Diffie-Hellman	DH-RSA-AES128-SHA256	DH-RSA	AES128-CBC	SHA256	
Diffie-Hellman	DH-RSA-AES128-SHA	DH-RSA	AES128-CBC	SHA160	
PKCS(RSA)	AES128-GCM-SHA256	PKCS-RSA	AES128-GCM	SHA256	
PKCS(RSA)	AES128-SHA256	PKCS-RSA	AES128-CBC	SHA256	
PKCS(RSA)	AES128-SHA	PKCS-RSA	AES128-CBC	SHA160	
PFS	ECDHE-RSA-DES-CBC3-SHA	ECDHE-RSA	DES-CBC3	SHA	☐
PFS	ECDHE-RSA-RC4-SHA	ECDHE-RSA	RC4	SHA	☐
PKCS(RSA)	RC4-SHA	PKCS-RSA	RC4	SHA160	
PKCS(RSA)	RC4-MD5	PKCS-RSA	RC4	SHA160	

네트워크 침입**(IDS/IPS)** 프로파일

네트워크 침입 프로파일은 트래픽이 악의적이지 않은지 확인하는 트랜잭션을 평가하는 데 사용할 수 있는 침입 탐지 및 보호(IDS/IPS) 규칙의 모음입니다.

멀티 클라우드 방어에서는 다음 IDS/IPS 규칙 집합을 지원합니다.

Table 4: 멀티 클라우드 방어에서는 다음 ***IDS/IPS*** 규칙 집합을 지원합니다.

규칙 집합	설명
Talos 규칙	Rules규칙은 애플리케이션 및 프레임워크에 고급 수준의 보호를 제공하는 실제 조사, 침입 테스트 및 연구를 통해 수집된 인텔리전스를 기반으로 하는 Cisco의 고급 규칙 집합입니다.
맞춤형 규칙	맞춤형 규칙은 맞춤형 애플리케이션에 특수 수준의 보호를 제공하며 고객이 작성한 특정 규칙 집합입니다.

IDS/IPS 프로파일 생성

다음 절차에 따라 IPS/IDS 프로파일을 생성하고 규칙 집합에 추가합니다.

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)** > **IPS/IDS**로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** **General Settings(**일반 설정**)** 탭을 클릭합니다.

단계 **4** 고유 **Profile Name(**프로파일 이름**)**을 입력합니다.

단계 **5** (선택 사항) **Description(**설명**)**을 입력합니다. 이렇게 하면 유사한 이름의 프로파일을 구분하는 데 도움이 될 수 있습니다.

단계 **6** IDS/IPS 프로파일이 악성 활동을 탐지하는 경우 위협 PCAP 옵션 파일을 토글합니다. 이 옵션을 켜는 경우 게이트웨이에 PCAP 프로파일이 연결되어 있어야 합니다.

단계 **7** 일반 설정의 **Rule Set(**규칙 집합**)** 섹션에서 규칙 라이브러리(Talos, 맞춤형)의 규칙 세트가 IDS/IPS 프로파일에 하나 이상 지정되어 있어야 합니다. Talos 규칙 및 맞춤형 규칙 집합을 사용하는 경우, 둘 중 하나 이상을 활성화해야 합니다. 전체 IDS/IPS 프로파일을 비활성화하려는 경우 정책 규칙 집합에서 IDS/IPS 프로파일을 제거하면 IDS/IPS 프로파일이 평가되지 않습니다. 드롭다운 메뉴를 사용하여 이 프로파일 내의 모든 규칙에 적용되는 다음 설정 중 하나를 선택합니다.

- **Disabled(**비활성화됨**)** - Talos 규칙 사용을 비활성화할지 여부를 지정합니다.
- **Manual(**수동**)** - Talos 규칙 버전을 지정합니다.
- **Automatic(**자동**)** - 게시 날짜로부터 최신 Talos Rules 버전으로의 자동 업데이트를 연기할 기간(일)을 지정합니다.

다른 드롭다운 메뉴를 사용하여 이 프로파일의 규칙을 업데이트할 시기를 선택합니다. Talos가 업데이트를 전송한 직후 또는 업데이트 며칠 후에 규칙 집합을 업데이트하도록 선택할 수 있습니다.

단계 **8** **Talos Rules: Policy(Talos** 규칙**:** 정책**)**를 클릭하고 표에서 기본으로 사용할 정책 프로파일을 선택합니다. 프로파일은 하나만 선택할 수 있습니다.

창 보기가 최대화되지 않은 경우, 창의 오른쪽으로 스크롤하여 선택한 프로파일에 대해 작업을 할당합니다.

- **Rule Default(**규칙 기본값**)** - 트리거된 각 규칙에 지정된 작업에 따라 요청을 허용하거나 거부하고 이벤트를 로깅합니다.
- **Allow Log(**허용 로그**)** - 요청을 허용하고 이벤트를 로깅합니다.
- **Allow No Log(**허용 로그 없음**)** - 요청을 허용하고 이벤트를 로깅하지 않습니다.
- **Deny Log(**거부 로그**)** - 요청을 거부하고 이벤트를 로깅합니다.
- **Deny No Log(**거부 로그 없음**)** - 요청을 거부하고 이벤트를 로깅하지 않습니다.

단계 **9** **Talos Rules: Category(Talos** 규칙**:** 범주**)** 탭을 클릭하고 표에서 프로파일에 있는 범주를 하나 이상 선택합니다.

단계 **10** **Talos rules: Class(Talos** 규칙**:** 클래스**)** 탭을 클릭하고 표에서 프로파일에 대한 클래스를 하나 이상 선택합니다.

단계 **11** 화면 상단에서 **Advanced Settings(**고급 설정**)** 탭을 클릭합니다.

단계 **12** **Rule Supression(**규칙 억제**)**에서 **Add(**추가**)**를 클릭하고 IP 주소의 유효한 **Source IP/CIDR List(**소스 **IP/CIDR** 목록**)** 및 해당 **Rule ID List(**규칙 **ID** 목록**)**를 입력합니다. 일련의 목록을 제거하려면 행 오른쪽의 빼기 아이콘을 클릭합니다.

단계 **13** **Event Filtering: Profile Event Filtering(**이벤트 필터링**:** 프로파일 이벤트 필터링**)**에서 다음 정보를 입력합니다.

- **Type(**유형**)** - 속도 또는 샘플을 선택할 수 있습니다. 생성된 이벤트는시간 평가 간격(초) 동안 지정된 트리거 **Number of Events(**이벤트 수**)**에 따라 속도 또는 샘플 제한이 적용됩니다.
- **Number of Events(**이벤트 수**)** - 허용되는 이벤트 수의 값을 수동으로 입력합니다.
- (속도 유형에서 사용 가능) **Time (Seconds)(**시간**(**초**))** - 숫자 값을 초 단위로 입력합니다.

단계 **14** **Event Filtering: Rule Event Filtering(**이벤트 필터링**:** 규칙 이벤트 필터링**)**에서 **Add(**추가**)**를 클릭합니다. 다음 정보를 입력합니다.

- **Rule ID List(**규칙 **ID** 목록**)** - 쉼표로 구분된 규칙 ID 목록을 지정합니다.
- **Number of Events(**이벤트 수**)** - 허용되는 이벤트 수의 값을 수동으로 입력합니다.
- (속도 유형에서 사용 가능) **Time (Sec)(**시간**(**초**))** - 숫자 값을 초 단위로 입력합니다.
- **Type(**유형**)** - 속도 또는 샘플을 선택합니다. 생성된 이벤트는 시간 평가 간격(초) 동안 지정된 트리거 이벤트 수에 따라 속도 또는 샘플 제한이 적용됩니다.

단계 **15** 고급 설정의 **Rule Setting List** (규칙 설정 목록) 섹션에서 **Add** (추가)를 클릭하고 다음을 입력합니다.

- **Source IP/CIDR List(**소스 **IP/CIDR** 목록**)** - 쉼표로 구분된 IP 또는 CIDR 목록을 제공합니다.

- **Rule ID List(**규칙 **ID** 목록**)** - 쉼표로 구분된 규칙 ID 목록을 제공합니다. 많은 수의 규칙에는 규칙 ID만 필요합니다. 수가 적은 규칙의 경우, 규칙 ID에 GID 및 ID를 GID:ID로 지정해야 합니다. 예를 들면 119:3와 같습니다.
- **Action(**작업**)** - 소스 IP/CIDR 목록 또는 규칙 ID 목록이 트리거되는 경우의 작업을 선택합니다. 규칙이 억제되면 어떤 작업도 수행되지 않으며 로그가 전송 또는 캡처되지 않습니다.
  - **Allow Log(**허용 로그**)** - 요청을 허용하고 이벤트를 로깅합니다.
  - **Allow No Log(**허용 로그 없음**)** - 요청을 허용하고 이벤트를 로깅하지 않습니다.
  - **Deny Log(**거부 로그**)** - 요청을 거부하고 이벤트를 로깅합니다.
  - **Deny No Log(**거부 로그 없음**)** - 요청을 거부하고 이벤트를 로깅하지 않습니다.

What to do next

- 프로파일 세부 정보 보기, on page 173
- 프로파일에 게이트웨이 연결 추가, on page 174

데이터 손실 방지(DLP) 프로파일

DLP(Data Loss Prevention) 프로파일은 멀티 클라우드 방어 솔루션이 정방향 프록시(이그레스) 모드로 구축될 때 데이터에서 유출 패턴을 찾는 것을 탐지하고 조치를 취하는 정책 규칙을 지정할 수 있는 기능을 멀티 클라우드 방어 고객에게 제공합니다.

멀티 클라우드 방어은(는) 고객이 이를 통해 맞춤형 PCRE 기반 정규식 패턴 외에도 사회 보장 번호(SSN), AWS 비밀번호, 신용카드 번호와 같은 사전 패키징된 일반적인 데이터 패턴을 지정할 수 있도록 합니다. 따라서 쉽게 PCI, PII 및 PHI 데이터에 대한 보호를 시행하여 규정 준수 요건을 충족할 수 있습니다. 이 기능은 별도의 DLP 서비스가 필요하지 않은 기존 멀티 클라우드 방어 기능 집합과 통합됩니다.

데이터 손실 방지 프로파일 생성

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)** > **Network Threats(**네트워크 위협**)**로 이동합니다.
단계 **2** **Create Intrusion Profile(**침입 프로파일 생성**)**을 클릭합니다.
단계 **3** **Data Loss Prevention(**데이터 손실 방지**)**을 선택합니다.
단계 **4** 프로파일의 고유한 이름을 제공하고 설명을 입력합니다.
단계 **5** 테이블에 **DLP** 필터 목록을 입력합니다.
단계 **6** 필요에 따라 행을 더 삽입하려면 **Add(**추가**)**를 클릭합니다.
단계 **7** 필터에 대한 설명을 제공합니다.

단계 **8** 드롭다운 목록에서 사전 정의된 정적 패턴(예: CVE 번호)을 선택하거나 사용자 정의 정규식을 제공합니다.

단계 **9** 카운트를 입력하여 트래픽에서 패턴이 표시되어야 하는 횟수를 정의합니다.

단계 **10** 패턴이 개수와 일치하는 경우 수행할 작업을 선택합니다.

참고 패턴이 더 제한적이므로 AWS 액세스 키 및 AWS 암호 키에 대해 사전 정의된 패턴이 DLP 검사에서 일치하지 않는 경우가 있습니다. DLP 프로파일에서 다음과 같은 완화된 사용자 지정 패턴을 사용하여 AWS 액세스 키와 AWS 암호 키를 탐지합니다. 이렇게 하면 오탐 로그 이벤트가 생성될 수 있습니다.

```
AWS 액세스 키: (?<![A-Z0-9])[A-Z0-9]{20}(?![A-Z0-9])
```

```
AWS 암호 키: (?<![AZa-z0-9/+=])[A-Za-z0-9/+=]{40}(?![A-Za-z0-9/+=])
```

다음에 수행할 작업

- 프로파일 세부 정보 보기, 173 페이지
- 프로파일에 게이트웨이 연결 추가, 174 페이지

Anti-Malware Profile

안티 멀웨어 프로파일은 Talos ClamAV 바이러스 탐지 엔진을 사용하여 안티 멀웨어 보호를 활성화합니다. ClamAV®는 트로이 목마, 바이러스, 악성코드 및 기타 악성 위협을 탐지하기 위한 안티바이러스 엔진입니다.

다음 단계에서는 안티 멀웨어 프로파일을 생성하고 정책 규칙에 연결하는 방법을 설명합니다.

안티맬웨어 프로파일 생성

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)** > **Network Threats(**네트워크 위협**)**로 이동합니다.

단계 **2** **Anti-malware(**악성코드 차단**)**를 선택합니다.

단계 **3** 고유한 이름을 입력하고 설명을 입력합니다.

단계 **4** Talos 규칙 집합에 대해 다음 모드 중 하나를 선택합니다.

- **Manual Mode(**수동 모드**)** - 드롭다운에서 Talos Ruleset Version(Talos 규칙 집합 버전)을 선택합니다. 선택한 규칙 집합 버전은 이 프로파일을 사용하는 모든 게이트웨이의 멀티 클라우드 방어 데이터 경로 엔진에 의해 사용되며 최신 규칙 집합 버전으로 자동 업데이트되지 않습니다.
- Automatic(자동) 모드 - 멀티 클라우드 방어에서 규칙 집합 버전을 게시한 후 구축을 며칠 단위로 지연할지 선택합니다. 멀티 클라우드 방어에서는 새 규칙 집합을 매일 게시하며 이 프로파일을 사용하는 게이트웨이는 **N** 일 이상의 최신 규칙 집합 버전으로 자동 업데이트됩니다. 여기서 **N**은 드롭다운에서 선택한 "delay by days(지연 일수)" 인수입니다. 예를 들어 2024년 1월 10일의 구축을 5일 연기하도록 선택하는 경우 멀티 클라우드 방어 컨트롤러은(는) 1월 5일 또는 그 이전에 게시된 규칙 집합 버전을 선택합니다. 해당 규칙 집합 버전을 사용한 내부 테스트가 어떤 이유로 실패할 경우 멀티 클라우드 방어이(가) 게시되지 않을 수도 있습니다.

단계 **5** 바이러스 서명과 일치하는 항목이 발견된 경우 수행할 작업을 선택합니다.

다음에 수행할 작업

- 프로파일 세부 정보 보기, 173 페이지
- 프로파일에 게이트웨이 연결 추가, 174 페이지

웹 애플리케이션 방화벽(WAF) 프로파일

웹 보호 프로파일은 트래픽이 악의적이지 않은지 확인하기 위해 웹 기반 트랜잭션을 평가하는 데 사용할 수 있는 WAF(Web Application Firewall) 규칙 모음입니다.

멀티 클라우드 방어에서는 다음 WAF 규칙 집합을 지원합니다.

Table 5: 멀티 클라우드 방어에서는 다음 ***WAF*** 규칙 집합을 지원합니다.

규칙 집합	설명
핵심 규칙	핵심 규칙은 모든 웹 애플리케이션에 기본 보호 레벨을 제공하는 ModSecurity CRS(핵심 규칙 집합)의 표준 규칙 집합입니다.
TrustWave 규칙	TrustWave 규칙은 특정 웹 애플리케이션 및 프레임워크에 고급 수준의 보호를 제공하는 실제 조사, 침입 테스트 및 연구를 통해 수집된 인텔리전스를 기반으로 하는 ModSecurity의 고급 규칙 집합입니다.
맞춤형 규칙	맞춤형 규칙은 맞춤형 웹 애플리케이션에 특수 수준의 보호를 제공하며 고객이 작성한 특정 규칙 집합입니다.

WAF 프로파일 생성

다음 절차에 따라 WAF 프로파일을 생성합니다.

Note 핵심 규칙 집합이 지정된 경우, 핵심 규칙을 비활성화할 수 없습니다. 핵심 규칙을 비활성화하려면 WAF 프로파일에서 모든 핵심 규칙 집합을 제거하여 평가되지 않도록 합니다.

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)** > **WAF**로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** 다음 일반 설정을 지정합니다.

a) 고유 **Profile Name(**프로파일 이름**)**을 입력합니다.
b) (선택 사항) **Description(**설명**)**을 입력합니다. 이렇게 하면 유사한 이름의 프로파일을 구분하는 데 도움이 될 수 있습니다.
c) 다음 작업을 지정합니다.
    - **Rule Default(**규칙 기본값**)** - 트리거된 각 규칙에 지정된 작업에 따라 요청을 허용하거나 거부하고 이벤트를 로깅합니다.
    - **Allow Log(**허용 로그**)** - 요청을 허용하고 이벤트를 로깅합니다.
    - **Deny Log(**거부 로그**)** - 요청을 거부하고 이벤트를 로깅합니다.
d) WAF 프로파일이 악의적인 활동을 탐지하는 경우, 위협 HAR 파일을 생성할지 여부를 지정합니다. 이 기능을 사용하려면 게이트웨이에 Pcap 프로파일이 첨부되어 있어야 합니다.
e) WAF 프로파일이 악의적인 활동을 탐지하는 경우 HTTP 요청 HAR 파일을 생성할지 여부를 지정합니다.
f) **RULE SETS(**규칙 설정**)** 섹션의 왼쪽에 있는 세로 탭에서 **Core Rules(**핵심 규칙**)**을 클릭합니다. 규칙 라이브러리(Core, TrustWave, Custom)에서 하나 이상의 규칙 집합을 지정해야 합니다.
    - 다음 항목을 지정합니다.
        - **Manual(**수동**)** - 사용할 핵심 규칙 버전을 지정합니다.
        - **Automatic(**자동**)** - 게시 날짜로부터 최신 핵심 규칙 버전으로의 자동 업데이트를 지연하는 기간(일)을 지정합니다.
    - 프로파일에 추가할 규칙을 확인하고 **Add to Profile(**프로파일에 추가**)**을 클릭합니다. 선택 사항이 오른쪽 테이블에 표시됩니다.
g) 왼쪽에 있는 세로 방향 탭에서 **TrustWave Rules(TrustWave** 규칙**)**를 클릭합니다.
    - 다음 항목을 지정합니다.
        - **Disabled(**비활성화됨**)** - Trustwave 규칙 사용을 비활성화할지 여부를 지정합니다.
        - **Manual(**수동**)** - 사용할 TrustWave 규칙 버전을 지정합니다.
        - **Automatic(**자동**)** - 게시 날짜로부터 최신 TrustWave Rules 버전으로의 자동 업데이트를 연기할 기간(일)을 지정합니다.
    - 프로파일에 추가할 규칙을 확인하고 **Add to Profile(**프로파일에 추가**)**을 클릭합니다. 선택 사항이 오른쪽에 있는 **Profile Selections(**프로파일 선택**)** 표에 표시됩니다.
h) 왼쪽에 있는 세로 방향 탭에서 **Custom Rules(**맞춤형 규칙**)**를 클릭합니다.
    - 다음 옵션 중 하나를 지정합니다.
        - **Disabled(**비활성화됨**)** - 맞춤형 규칙 사용을 비활성화할지 여부를 지정합니다.
        - **Manual(**수동**)** - 사용할 맞춤형 규칙 버전을 지정합니다.
        - **Automatic(**자동**)** - 게시 날짜로부터 최신 맞춤형 규칙 버전으로의 자동 업데이트를 지연하는 기간(일)을 지정합니다.

- 프로파일에 추가할 규칙을 확인하고 **Add to Profile(**프로파일에 추가**)**을 클릭합니다. 선택 사항이 오른쪽에 있는 **Profile Selections(**프로파일 선택**)** 표에 표시됩니다.

단계 **4** 창 상단으로 스크롤하고 **Advanced Settings(**고급 설정**)** 탭을 클릭합니다.

a) "Rule Suppression(규칙 억제)"에서 **Add(**추가**)**를 클릭하여 규칙에 대한 행을 하나 이상 추가합니다. 특정 IP 또는 CIDR 목록에 대한 규칙을 억제할 수 있습니다.

- **Source IP/CIDR List(**소스 **IP/CIDR** 목록**)**에서 쉼표로 구분된 IP 또는 CIDR 목록을 제공합니다.
- **Rule ID List(**규칙 **ID** 목록**)**에 쉼표로 구분된 규칙 ID 목록을 제공합니다.

b) "Event Filtering(이벤트 필터링)"에서 다음 정보를 제공합니다.

- **Type(**유형**) - Rate(**속도**)** 또는 **Sample(**샘플**)**
- 이벤트 수
- 시간**(**초**)**

c) "Rule Event Filtering(규칙 이벤트 필터링)"에서 **Add(**추가**)**를 클릭하여 규칙에 대한 행을 하나 이상 추가합니다. 생성하는 모든 행에 대해 유효한 **Rule ID List(**규칙 **ID** 목록**)**, **Number of Events(**이벤트 수**)**, **Time (Sec)(**시간**(**초**))** 을 입력하고 유형 또는 샘플 중 하나를 **Type(**유형**)**으로 선택합니다.

d) "Core Rule Set(핵심 규칙 집합)"에서 **Request Anomaly(**요청 이상 징후**)** 및 **Response Anomaly(**응답 이상 징후**)** 모두에 대한 값을 선택합니다. "Request Anomaly(요청 이상 징후)"에 대해 3보다 작은 값을 사용하면 방대한 양의 알림이 생성됩니다.

e) **Paranoia Level(**편집증 수준**)**을 선택합니다. 옵션 범위는 1~4입니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

What to do next

- 프로파일 세부 정보 보기, on page 173
- 프로파일에 게이트웨이 연결 추가, on page 174

이벤트 필터링

WAF 프로파일이 트리거될 때 생성되는 보안 이벤트 수를 줄이기 위해, **Advanced Settings(**고급 설정**)**에서 이벤트 속도를 제한하거나 샘플링하도록 이벤트 필터링을 구성할 수 있습니다. 설정은 탐지 또는 보호 동작을 변경하지 않습니다.

Type(유형)을 **Rate(**속도**)**로 지정하면 생성되는 이벤트는 *Time(*시간*)* 평가 간격(초) 동안 트리거된 지정된 *Number of Events(*이벤트 수*)*에 따라 속도가 제한됩니다. 예를 들어 *Number of Events(*이벤트 수*)*가 50으로 지정되고 *Time(*시간*)*이 5초로 지정된 경우 초당 10개 이벤트만 생성됩니다.

Type(유형)을 **Sample(**샘플**)**로 지정하면 생성된 Events(이벤트)는 지정된 *Number of Events(*이벤트 수*)*를 기준으로 샘플링됩니다. 예를 들어 *Number of Events(*이벤트 수*)*가 10으로 지정된 경우, 트리거된 10개 이벤트마다 1개의 이벤트만 생성됩니다.

프로파일 이벤트 필터링

프로파일 이벤트 필터링은 WAF 프로파일에 설정된 모든 규칙에 적용됩니다.

- Type(유형)을 **Rate(**속도**)** 또는 **Sample(**샘플**)**로 지정합니다.
  - **Rate(**속도**)** - *Number of Events(*이벤트 수*)* 및 *Time(*시간*)* 평가 간격(초)을 지정합니다.
  - **Sample(**샘플**)** - *Number of Events(*이벤트 수*)*를 지정합니다.

규칙 이벤트 필터링

WAF 프로파일이 트리거될 때 생성되는 보안 이벤트 수를 줄이기 위해 이벤트 속도를 제한하거나 샘플링하도록 이벤트 필터링을 구성할 수 있습니다. 설정은 탐지 또는 보호 동작을 변경하지 않습니다.

규칙 이벤트 필터링은 WAF 프로파일에 구성된 특정 규칙에 적용됩니다.

단계 **1** Rule Event Filtering(규칙 이벤트 필터링) 아래에서 **Add(**추가**)**를 클릭합니다.

단계 **2** **Rule ID List(**규칙 **ID** 목록**)**에서 쉼표로 구분된 **Rule ID(**규칙 **ID)** 목록을 지정합니다.

단계 **3** Type(유형)을 **Rate(**속도**)** 또는 **Sample(**샘플**)**로 지정합니다.

- **Rate(**속도**)** - **Number of Events(**이벤트 수**)** 및 **Time(**시간**)** 평가 간격(초)을 지정합니다.
- **Sample(**샘플**)** - **Number of Events(**이벤트 수**)**를 지정합니다.

다음에 수행할 작업

규칙 집합에서 정방향 프록시 규칙 추가 또는 편집

L7 DoS 프로파일 생성

멀티 클라우드 방어 게이트웨이는 백엔드 웹 서버에 대한 클라이언트 요청을 지속적으로 모니터링하여 애플리케이션 계층 공격을 모니터링, 탐지 및 치료할 수 있는 기능을 제공합니다. 레이어 7 DoS 공격은 웹 서버 리소스를 고갈시키기 위한 것으로, 많은 HTTP 요청을 전송하여 서비스 가용성에 영향을 미칩니다. 이 기능은 웹 기반 애플리케이션의 가용성을 유지하기 위해 게이트웨이가 백엔드 웹 서비스에 대한 인바운드 연결을 프록시하도록 활성화된 경우 활성화됩니다. 이 기능을 활성화하면 프론트엔드 로드 밸런서가 지원하지 않거나 애플리케이션 DoS 공격을 탐지하고 교정하도록 최적화되지 않은 경우에도 게이트웨이가 추가적인 보안을 제공할 수 있습니다.

이 기능은 API 서비스를 호스팅하는 백엔드 웹 서버에 대한 DoS 보호를 제공하는 데에도 사용할 수 있습니다.

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)**로 이동합니다.

단계 **2** **Layer 7 DOS**를 선택합니다.

단계 **3** 고유한 프로파일 이름을 제공합니다.

단계 **4** (선택 사항) **Description(**설명**)**을 입력합니다. 이렇게 하면 유사한 이름을 가질 수 있는 다른 프로파일을 구분하는 데 도움이 될 수 있습니다.

단계 **5** 요청 속도 제한을 추가합니다.

리소스에 대한 과도한 요청은 다음 매개변수를 기반으로 제한합니다. 이 매개변수의 값은 레이어 7 DoS 옵션으로 보호하려는 웹 서비스의 트래픽 패턴 측정 및 이해를 기반으로 해야 합니다.

Table 6: 매개변수

매개변수	설명
URI	리소스에 대한 요청을 제한하는 경로를 나타내는 데 사용되는 상대적 URI입니다. 예를 들어 https://www.example.com/login.html에서 서비스 리소스를 모니터링하고 보호하려는 경우 **Request Rate Limits(**요청 속도 제한**)** 테이블에 URI 매개변수로 /login.html을 입력합니다.
HTTP 메서드	리소스 URI당 HTTP 메서드를 지정하여 클라이언트 요청에서 속도가 제한되는 HTTP 메서드와 속도가 제한되지 않는 HTTP 메서드를 제어할 수 있습니다. 테이블의 각 행에 대해 드롭다운에서 여러 메서드를 선택할 수 있습니다. 빈 HTTP 메서드 목록은 메서드가 무시되고 속도가 리소스에 대한 모든 호출에 적용됨을 의미합니다. **Note** 속도는 각 리소스별로 적용됩니다. 따라서 여러 메서드가 해당 행의 요청 속도에 지정된 속도 제한을 공유합니다. 예를 들어 속도가 매초 3개 요청이고 GET, POST 및 PUT이 HTTP 메서드에 지정되어 있으며 동일한 시간(초)에 단일 클라이언트 IP에서 해당 URI에 2개의 GET과 1개의 POST가 발생하는 경우, 같은 초에 PUT은 허용되지 않습니다.
요청 속도	1초당 요청 수 단일 클라이언트가 규칙의 URI 부분에 언급된 URI 리소스에 요청을 전송할 수 있는 속도를 결정합니다.
Burst Size(버스트 크기)	클라이언트가 규칙의 URI 부분에 언급된 URI 리소스에 전송할 수 있는 최대 동시 요청 수를 지정합니다. 이 임계값을 초과하며 동시에 프록시에 도착하는 요청은 백엔드 서버로 전송되지 않습니다.

단계 **6** 완료되면 **Save(**저장**)**를 클릭합니다. 규칙은 위에서 아래로 확인되고 첫 번째 일치에 적용되므로 URI를 기준으로 하면 규칙의 순서가 중요합니다. 목록의 상위에 추가된 URI가 그 아래에 있는 규칙의 리소스를 포함하는 리소스 경로를 포함하는 경우, 일치하는 첫 번째 규칙이 적용됩니다.

What to do next

- 프로파일 세부 정보 보기, on page 173
- 서비스 개체에 L7 DoS 프로파일을 추가합니다. 그런 다음 프로파일에 게이트웨이 연결 추가, on page 174. 규칙 집합을 업데이트하는 경우, 변경 사항이 즉시 구축되지 않을 수 있습니다.

URL(Uniform Resource Locator) 필터 프로파일

URL 필터링 프로파일은 HTTP 요청의 URL을 평가하고 트래픽을 허용 또는 거부하는 작업을 적용합니다. URL을 평가하려면 정방향 프록시 규칙으로 트래픽을 처리해야 합니다. 프로파일의 URL 집합은 전체 경로를 나타내는 문자열 또는 PCRE(Perl Compatible Regular Expression)를 나타내는 문자열로 지정할 수 있습니다. 도메인 필터링만 필요한 경우 FQDN 필터링 프로파일을 사용하는 것이 가장 좋습니다. FQDN 필터링 프로파일은 URL 필터링과 함께 사용할 수도 있습니다. 여기서 도메인은 FQDN 필터링 프로파일을 사용하여 평가되고 URL은 URL 필터링 프로파일을 사용하여 평가됩니다.

URL 필터링 프로파일은 사전 정의된 범주 집합을 사용할 수 있습니다. 범주에 대한 자세한 내용은 FQDN / URL 필터링 범주, on page 177의 내용을 참조하십시오.

Note URL 필터링은 2개의 기본 행(**Uncategorized(**미분류**)** 및 **ANY(**모두**)**와 함께 사용자가 지정한 행(URL 및 Categories(범주))을 포함하는 테이블로 구성됩니다. 원하는 경우 각 행 내에서 범주와 URL을 결합할 수 있습니다.

각 URL 필터링 프로파일의 제한은 다음과 같습니다.

- 사용자 지정 최대 행: 254(독립형 또는 독립형 그룹)
- 행당 최대 범주 및 URL: 60
- 최대 URL 문자 길이: 2048

다단계 도메인(예: 'www.example.com')을 지정할 때 '.' 문자를 이스케이프해야 합니다(예: 'www\.example\.com'). 그렇지 않으면 단일 문자에 대한 와일드카드로 처리됩니다.

미분류

- **Uncategorized(**미분류**)**로 표시되는 URL 필터링 프로파일의 마지막에서 두 번째 행.
- 사용자가 지정한 URL과 일치하지 않거나 범주가 없는 URL에 대해 수행할 정책 작업을 지정합니다.
- 그룹 프로파일에서 독립형 프로파일이 사용되고 그룹 프로파일이 정책 규칙 집합 규칙에 적용된 경우 **Uncategorized(**미분류**)** 행은 그룹 프로파일에서 가져옵니다. 독립형 프로파일의 **Uncategorized(**미분류**)** 행은 독립형 프로파일이 정책 규칙 집합 규칙에 직접 적용된 경우에만 적용 가능합니다.

기본값**(ANY)**

- **ANY(**모든**)**로 표시되는 URL 필터링 프로파일의 마지막 행.
- 사용자가 지정한 URL 또는 범주와 일치하지 않거나 미분류가 아닌 URL에 대해 수행할 정책 작업을 지정합니다.

- 그룹 프로파일에서 독립형 프로파일이 사용되고 그룹 프로파일이 정책 규칙 집합 규칙에 적용된 경우 **ANY(**모든**)** 행은 그룹 프로파일에서 가져옵니다. 독립형 프로파일의 **ANY(**모든**)** 행은 독립형 프로파일이 정책 규칙 집합에 직접 적용된 경우에만 적용 가능합니다.

URL 필터링 프로파일 생성

다음 절차를 사용하여 독립형 URL 필터링 프로파일을 생성합니다.

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)** > **URL Filtering(URL** 필터링**)**으로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** 고유한 이름을 제공합니다.

단계 **4** (선택 사항) **Description(**설명**)**을 입력합니다. 이렇게 하면 유사한 이름의 다른 프로파일을 구분하는 데 도움이 될 수 있습니다.

단계 **5** **Add(**추가**)**를 클릭하여 새 행을 생성합니다.

단계 **6** 개별 URL을 지정합니다(예: https://www.google.com).

- 각 URL은 PCRE(Perl Compatible Regular Expression)로 지정됩니다.
- 각 URL은 전체 경로로 지정해야 합니다.
- 소수점 "." 문자를 이스케이프하지 않으면 단일 문자 와일드카드로 처리됩니다.

단계 **7** **Category(**범주**)**를 지정합니다(예: 게임, 스포츠, 소셜 네트워킹).

단계 **8** 정책이 적용되는 HTTP 메서드를 지정합니다.

단계 **9** 메서드의 하위 집합으로 다음 중 하나를 선택합니다.

- Delete
- Get
- Head
- Options
- Patch
- Post
- Put

단계 **10** 모든 메서드에 대해 **All(**모두**)**을 지정합니다.

단계 **11** 사용자 지정 URL/Categories(URL/범주), Uncategorized(미분류) 및 ANY(모든) 행에 대한 Policy(정책) 작업을 지정합니다.

- **Allow Log(**허용 로그**)** - 요청을 허용하고 이벤트를 로깅합니다.
- **Allow No Log(**허용 로그 없음**)** - 요청을 허용하고 이벤트를 로깅하지 않습니다.

- **Deny Log(**거부 로그**)** - 요청을 거부하고 이벤트를 로깅합니다.
- **Deny No Log(**거부 로그 없음**)** - 요청을 거부하고 이벤트를 로깅하지 않습니다.

단계 **12** 반환 상태 코드를 지정합니다.

단계 **13** **100** 이상 **600** 미만의 정수 값을 지정합니다. 값은 요청을 수행하는 클라이언트에 반환될 HTTP 상태를 나타냅니다. 일반적인 반환 코드는 **503**입니다.

단계 **14** **Save(**저장**)**를 클릭합니다.

What to do next

- 프로파일 세부 정보 보기, on page 173
- 프로파일에 게이트웨이 연결 추가, on page 174

FQDN(Fully Qualified Domain Name) 필터 프로파일

FQDN(Fully Qualified Domain Name) 필터 프로파일은 트래픽과 연결된 FQDN을 평가하고 트래픽을 허용 또는 거부하는 작업을 적용합니다. FQDN을 평가하려면 트래픽이 TLS로 암호화되어 있어야 하며 TLS hello 헤더의 SNI 필드에 FQDN이 포함되어 있어야 합니다. FQDN에서는 전달 또는 전달 프록시 규칙에 의해 처리된 트래픽을 평가할 수 있습니다. 프로파일의 FQDN 집합은 전체 도메인을 나타내는 문자열 또는 PCRE(Perl Compatible Regular Expression)로 표시되는 문자열로 지정할 수 있습니다. 도메인 허용 목록만 필요한 경우에는 FQDN 필터링 프로파일을 사용하는 것이 가장 좋습니다. FQDN 필터링 프로파일을 URL 필터링 프로파일과 함께 사용할 수도 있습니다. 여기서 도메인은 FQDN 필터링 프로파일 사용하여 평가되고 URL은 URL 필터링 프로파일을 사용하여 평가됩니다.

FQDN 필터링을 사용하여 규칙 일치 후 기준에 따라 허용하거나 거부할 범주를 필터링합니다. 세분화된 수준에서 필터를 설정할 수 있습니다. FQDN 필터 행에는 거부 또는 허용과 같은 로그 관련 작업이 포함되어 있습니다.

FQDN 필터링 프로파일은 사전 정의된 범주 집합을 사용할 수도 있습니다. 범주에 대한 자세한 내용을 FQDN / URL 필터링 범주, on page 177를 참조하십시오.

Note FQDN 필터링 프로파일은 사용자가 지정한 행(FQDN 및 Categories(범주))을 포함하는 테이블 형식으로 구성되며, 두 개의 기본 행(Uncategorized(미분류) 및 ANY(모든))이 있습니다. 필요한 경우 각 행 내에서 범주 및 FQDN을 결합할 수 있습니다.

각 FQDN 필터 프로파일의 제한은 다음과 같습니다.

- 사용자 지정 최대 행: 254(독립형 또는 독립형 그룹)
- 행당 최대 범주 및 FQDN: 60
- 최대 FQDN 문자 길이: 255

다단계 도메인(예: 'www.example.com')을 지정할 때 `.' 문자를 이스케이프해야 합니다(예: `www.example\.com'). 그렇지 않으면 단일 문자에 대한 와일드카드로 처리됩니다.

독립형 및 그룹

FQDN 필터 프로파일은 독립형 또는 그룹으로 지정할 수 있습니다.

독립형 FQDN 필터 프로파일에는 FQDN 및 범주가 포함됩니다. 프로파일은 하나 이상의 정책 규칙 집합에 직접 적용되거나 FQDN 그룹 프로파일과 연결됩니다.

FQDN 필터 그룹 프로파일에는 다양한 용도로 정의하고 그룹 프로파일로 함께 결합할 수 있는 독립형 프로파일의 순서가 지정된 목록이 포함되어 있습니다. 그룹 프로파일을 하나 이상의 정책 규칙 집합에 직접 적용할 수 있습니다. 각 팀은 특정 독립형 프로파일을 생성하고 관리할 수 있습니다. 이러한 독립형 프로파일은 그룹 프로파일로 결합하여 활용 사례에 따라 계층 구조 또는 다양한 조합을 생성할 수 있습니다. 모든 항목에 적용되는 전역 FQDN 목록, 서로 다른 CSP에 적용되는 CSP 관련 목록, 그리고 애플리케이션에 적용되는 애플리케이션 관련 목록 등의 조합을 예로 들 수 있습니다.

미분류

- **Uncategorized(**미분류**)**로 표시되는 FQDN 필터 프로파일의 두 번째에서 마지막 행.
- 사용자가 지정한 FQDN과 일치하지 않거나 범주가 없는 FQDN에 대해 수행할 정책 작업을 지정합니다.
- 그룹 프로파일에서 독립형 프로파일이 사용되고 그룹 프로파일이 정책 규칙 집합 규칙에 적용된 경우 **Uncategorized(**미분류**)** 행은 그룹 프로파일에서 가져옵니다. 독립형 프로파일의 **Uncategorized(**미분류**)** 행은 독립형 프로파일이 정책 규칙 집합 규칙에 직접 적용된 경우에만 적용 가능합니다.

기본값**(ANY)**

- **ANY(**모든**)**로 표시되는 FQDN 필터 프로파일의 마지막 행.
- 사용자가 지정한 FQDN 또는 범주와 일치하지 않거나 미분류가 아닌 FQDN에 대해 수행할 정책 작업을 지정합니다.

- 그룹 프로파일에서 독립형 프로파일이 사용되고 그룹 프로파일이 정책 규칙 집합 규칙에 적용된 경우 **ANY(**모든**)** 행은 그룹 프로파일에서 가져옵니다. 독립형 프로파일의 **ANY(**모든**)** 행은 독립형 프로파일이 정책 규칙 집합에 직접 적용된 경우에만 적용 가능합니다.

독립형 FQDN 필터 프로파일 생성

다음 절차에 따라 독립형 FQDN 필터 프로파일을 생성합니다.

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)** > **FQDN Filtering(FQDN** 필터링**)**로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** 고유한 이름을 제공합니다.

단계 **4** (선택 사항) **Description(**설명**)**을 입력합니다. 이렇게 하면 유사한 이름의 프로파일을 구분하는 데 도움이 될 수 있습니다.

단계 **5** Type(유형)을 **Standalone(**독립형**)**으로 지정합니다.

단계 **6** **Add(**추가**)**를 클릭하여 새 행을 생성합니다.

단계 **7** 개별 FQDN 지정합니다(예: google.com).

a) 각 FQDN은 PCRE(Perl Compatible Regular Expression)로 지정됩니다.

b) "**.**" 문자를 이스케이프하지 않으면 단일 문자 와일드카드로 처리됩니다.

단계 **8** **Category(**범주**)**를 지정합니다(예: 게임, 스포츠, 소셜 네트워킹).

단계 **9** 사용자 지정 FQDN/Categories(FQDN/범주), Uncategorized(미분류) 및 ANY(모든) 행에 대한 정책 작업을 지정합니다.

- **Allow Log(**허용 로그**)** - 요청을 허용하고 이벤트를 로깅합니다.
- **Allow No Log(**허용 로그 없음**)** - 요청을 허용하고 이벤트를 로깅하지 않습니다.
- **Deny Log(**거부 로그**)** - 요청을 거부하고 이벤트를 로깅합니다.
- **Deny No Log(**거부 로그 없음**)** - 요청을 거부하고 이벤트를 로깅하지 않습니다.

단계 **10** (선택 사항) 암호 해독이 바람직하지 않거나 가능한 FQDN에 대해 **Decryption Exception(**암호 해독 예외**)**을 지정합니다. 암호 해독 예외를 고려해야 하는 가능한 이유는 다음과 같습니다.

- 암호화된 트래픽(예: 금융 서비스, 방위, 의료 등)의 검사에 대한 거부 요청
- 암호 해독이 불가능한 SSO 인증 트래픽
- 프록시 설정할 수 없는 NTLM 트래픽

단계 **11** 완료되면 **Save(**저장**)**를 클릭합니다.

What to do next

- 프로파일 세부 정보 보기, on page 173

- 프로파일에 게이트웨이 연결 추가, on page 174

그룹 FQDN 필터 프로파일 생성

다음 절차를 사용하여 두 개 이상의 독립형 프로파일이 있는 그룹 FQDN 필터 프로파일을 생성합니다.

단계 1 **Manage(**관리**)** > **Profiles(**프로파일**)** > **FQDN Filtering(FQDN** 필터링**)**로 이동합니다.

단계 2 **Create(**생성**)**를 클릭합니다.

단계 3 고유한 이름을 제공합니다.

단계 4 (선택 사항) **Description(**설명**)**을 입력합니다. 이렇게 하면 유사한 이름을 가질 수 있는 프로파일을 구분하는 데 도움이 될 수 있습니다.

단계 5 Type(유형)을 **Group(**그룹**)**으로 지정합니다.

단계 6 초기 독립형 프로파일을 선택합니다(하나 이상의 독립형 프로파일이 필요함).

단계 7 **Add FQDN Profile(FQDN** 프로파일 추가**)**을 클릭하여 추가 프로파일에 대해 새 행을 생성합니다.

단계 8 독립형 프로파일을 선택합니다.

단계 9 Uncategorized(미분류) FQDN에 대한 Policy(정책) 작업을 지정합니다.

단계 10 **ANY(**모두**)** FQDN에 대한 Policy(정책) 작업을 지정합니다(기본값).

단계 11 선택 사항: 암호 해독이 필요하지 않거나 가능한 경우 Uncategorized(미분류) 또는 ANY(모두)로 암호 해독 예외를 지정합니다. 암호 해독 예외를 고려해야 하는 가능한 이유는 다음과 같습니다.

- 암호화된 트래픽(금융 서비스, 방위, 의료 등)의 검사에 대한 거부 요청
- 암호 해독이 불가능한 SSO 인증 트래픽
- 프록시 설정할 수 없는 NTLM 트래픽

단계 12 **Save(**저장**)**를 클릭합니다.

What to do next

- 프로파일 세부 정보 보기, on page 173
- 프로파일에 게이트웨이 연결 추가, on page 174

악의적인 IP 프로파일

추가 보안 보호 기능을 활성화하여 알려진 악성 IP와의 통신을 차단할 수 있습니다. 이러한 악성 IP는 TrustWave에서 정의하며 보안 프로파일 규칙 집합으로 멀티 클라우드 방어에 통합됩니다. 규칙 집합은 TrustWave에서 업데이트를 제공하므로 자주 업데이트됩니다. 업데이트는 자동 업데이트 구성 또

는 수동 업데이트 구성을 사용하여 정책 규칙 집합에 동적으로 또는 수동으로 적용할 수 있습니다. 자세한 내용은 악의적인 IP 프로파일 생성, on page 163를 참고하십시오.

Note TrustWave는 학습된 다양한 동작을 기반으로 악성 IP를 식별합니다.

- 웹 허니팟에서 악의적인 공격자 식별
- 봇넷 C&C 호스트
- TOR 출구 노드
- 기타 학습된 행동

악의적인 IP 프로파일 생성

다음 절차에 따라 악의적인 IP 프로파일을 생성합니다.

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)** > **Malicious IP(**악성 **IP)**로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** 고유한 프로파일 이름을 제공합니다.

단계 **4** (선택 사항) **Description(**설명**)**을 입력합니다. 이렇게 하면 유사한 이름의 다른 프로파일을 구분하는 데 도움이 될 수 있습니다.

단계 **5** **IP Reputation(IP** 평판**)**을 활성화하려면 확인란을 선택합니다.

단계 **6** **TrustWave Ruleset Version(TrustWave** 규칙 집합 버전**)** 드롭다운 메뉴의 두 가지 옵션 중 하나를 선택합니다.

- **Manual(**수동**)** - 선택한 규칙 집합 버전은 이 프로파일을 사용하는 모든 게이트웨이의 멀티 클라우드 방어 데이터 경로 엔진에 사용됩니다. 프로파일은 최신 규칙 집합 버전으로 자동 업데이트되지 않습니다.
- **Automatic(**자동**)** - 멀티 클라우드 방어에서 규칙 집합 버전을 게시한 후 업데이트를 지연할 일수를 선택합니다. 새 규칙 집합은 멀티 클라우드 방어에 의해 자주 게시됩니다. 이 프로파일을 사용하는 게이트웨이는 **N**일 이상의 최신 규칙 집합 버전으로 자동 업데이트됩니다. 여기서 **N**은 드롭다운에서 선택한 "delay by days(지연 일수)" 인수입니다. 예를 들어 2021년 1월 10일의 구축을 5일 연기하도록 선택하는 경우 멀티 클라우드 방어 컨트롤러는 1월 5일 또는 그 이전에 게시된 규칙 집합 버전을 선택합니다. 해당 규칙 집합 버전을 사용한 내부 테스트가 어떤 이유로 실패할 경우 멀티 클라우드 방어이(가) 게시되지 않을 수도 있습니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

What to do next

- 프로파일 세부 정보 보기, on page 173
- 프로파일에 게이트웨이 연결 추가, on page 174

IP 평판

IP Reputation(IP 평판) 확인란은 프로파일을 활성화 또는 비활성화하는 수단으로 사용됩니다. 프로파일을 선택하고 프로파일이 정책 규칙 집합에 첨부되면, 악성 IP 보호가 시행됩니다. 선택하지 않고 프로파일이 정책 규칙 집합에 첨부되면, 악성 IP 보호가 시행되지 않습니다. 항상 IP 평판 확인란을 선택하는 것이 좋습니다. 악성 IP 프로파일을 비활성화하려면 확인란의 선택을 취소하는 대신 정책 규칙 집합에서 해당 연결을 제거합니다.

패킷 캡처 프로파일

패킷 캡처 프로파일은 멀티 클라우드 방어 게이트웨이에 구성되고 연결됩니다. 그리고 정책 규칙, 네트워크 위협 프로파일, 웹 보호 프로파일에서 활성화됩니다. 패킷 캡처는 트래픽 흐름(PCAP 파일)과 애플리케이션 및 네트워크 위협(HAR 파일)을 캡처할 수 있습니다.

패킷 캡처 형식

다음 형식 규칙을 고려하십시오.

Policy Rule Capture - <bucketname>/<cspaccountname>/<gatewayname>/flow-packet-captures/<year>/<month>/<day>/<instanceid>_<timestamp>_<policyname>.pcap.gz

IPS Threat Capture - <bucketname>/<cspaccountname>/<gatewayname>/network-threats-captures/<year>/<month>/<day>/<instanceid>_<timestamp>_<sessionid>.pcap.gz

WAF Threat Capture - <bucketname>/<cspaccountname>/<gatewayname>/web-protection-captures/<year>/<month>/<day>/<instanceid>_<timestamp>_<sessionid>.har.gz

API Logging - <bucketname>/<cspaccountname>/<gatewayname>/api-logging-captures/<year>/<month>/<day>/<instanceid>_<timestamp>_<sessionid>.har.gz

패킷 캡처 프로파일 생성

다음 절차에 따라 팩 캡처 프로파일을 생성합니다.

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)** > **Packet Capture(**패킷 캡처**)**로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** 고유한 이름을 지정합니다.

단계 **4** (선택 사항) **Description(**설명**)**을 입력합니다. 이렇게 하면 유사한 이름의 다른 프로파일을 구분하는 데 도움이 될 수 있습니다.

단계 **5** **CSP** 계정을 지정합니다.

단계 **6** 클라우드 서비스 제공자의 유형에 따라 스토리지 버킷의 매개변수를 결정할 수 있습니다. 클라우드 서비스 제공자별 다음 요구 사항에 유의하십시오.

- **AWS** - S3 버킷.
- **Azure** - 스토리지 계정 이름, 블로그 컨테이너 및 스토리지 액세스 키.
- **GCP** - 스토리지 버킷.

단계 **7** **Save(**저장**)**를 클릭합니다.

What to do next

- 프로파일 세부 정보 보기, on page 173
- 프로파일에 게이트웨이 연결 추가, on page 174

로그 전달 프로파일

로그 전달 프로파일을 사용하면 게이트웨이, VPC 및 VNet 로그 모음을 서드파티에 전송할 수 있습니다. 멀티 클라우드 방어과 선택한 서드파티 간의 통신에는 전달해야 하는 로그 유형 및 로그가 전송될 대상 서버 프로파일이 포함됩니다. 단일 프로파일을 사용하거나 여러 엔드포인트에 로그를 동시에 전송하는 프로파일 그룹을 사용할 수도 있습니다.

이 프로파일은 메트릭을 포함하지 않습니다. 로그 메트릭 전달에 대한 자세한 내용은 게이트웨이 메트릭 전달 프로파일, 166 페이지를 참조하십시오.

독립형 로그 전달 프로파일 생성

다음 절차에 따라 독립형 로그 전달 프로파일을 생성합니다.

단계 **1** **Manager(**관리자**)** > **Profiles(**프로파일**)** > **Log Forwarding(**로그 전달**)**으로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** 고유 **Profile Name(**프로파일 이름**)**을 입력합니다.

단계 **4** (선택 사항) **Description(**설명**)**을 입력합니다. 이렇게 하면 유사한 이름의 다른 프로파일과 구분할 수 있습니다.

단계 **5** **Type(**유형**)** 드롭다운 메뉴를 확장하고 **Standalone(**독립형**)**을 선택합니다.

단계 **6** **Destination(**대상**)** 드롭다운 메뉴를 확장하고 로그를 전송할 서드파티 애플리케이션을 선택합니다.

단계 **7** 6단계에서 선택한 대상 유형에 따라 로그가 전달되는 최종 엔드포인트를 보호하라는 메시지가 표시되면 적절한 정보를 입력합니다. 대상 유형에 따라 모든 옵션을 사용할 수 있는 것은 아닙니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 프로파일 세부 정보 보기, 173 페이지
- 프로파일에 게이트웨이 연결 추가, 174 페이지

로그 전달 그룹 생성

다음 절차에 따라 그룹화된 메트릭 전달 프로파일을 생성합니다.

시작하기 전에

- 이 프로파일을 생성하기 전에 메트릭을 전달할 서드파티 애플리케이션이 하나 이상 있어야 합니다.
- 둘 이상의 독립형 메트릭 전달 프로파일이 이미 생성되어 있어야 합니다. 자세한 내용은 독립형 로그 전달 프로파일 생성, 165 페이지를 참조하십시오.

단계 **1** **Manager(**관리자**)** > **Profiles(**프로파일**)** > **Log Forwarding(**로그 전달**)**으로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** 고유 **Profile Name(**프로파일 이름**)**을 입력합니다.

단계 **4** (선택 사항) **Description(**설명**)**을 입력합니다. 이렇게 하면 유사한 이름의 다른 프로파일과 구분할 수 있습니다.

단계 **5** **Type(**유형**)** 드롭다운 메뉴를 확장하고 **Group(**그룹**)**을 선택합니다.

단계 **6** **Group Details(**그룹 세부 정보**)**에서 프로파일에 추가해야 하는 모든 새 행에 대해 **Add(**추가**)**를 클릭합니다.

단계 **7** 각 행에 대한 드롭다운 메뉴를 확장하여 그룹에 추가할 프로파일을 선택합니다. 저장하기 전에 언제든지 프로파일을 제거하려면, 해당 프로파일의 확인란을 선택하고 **Remove(**제거**)**를 선택합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 프로파일 세부 정보 보기, 173 페이지
- 프로파일에 게이트웨이 연결 추가, 174 페이지

게이트웨이 메트릭 전달 프로파일

이 프로파일은 데이터 모니터링 및 분석을 위해 멀티 클라우드 방어 게이트웨이에 의해 생성된 게이트웨이 메트릭을 전달하는 데 사용됩니다. 메트릭은 게이트웨이에 의해 생성되지만 메트릭을 서드파티 분석 애플리케이션에 전달하는 멀티 클라우드 방어 컨트롤러입니다. 이 전달 프로파일을 사용하면 멀티 클라우드 방어에 로그인하지 않고도 게이트웨이 메트릭을 모니터링, 분석 및 구성할 수 있습니다. 이 정보를 사용하여 게이트웨이 환경의 성능 및 동작을 측정합니다. 또한 환경 문제 해결을 위해 이 정보를 활용합니다.

참고 멀티 클라우드 방어 컨트롤러 버전 23.09부터는 DataDog만 서드파티 분석 애플리케이션으로 지원됩니다.

DataDog와 같이 사용 가능한 대부분의 분석 애플리케이션의 경우, 반드시 권한이 부여된 사용자여야 툴의 API 및 렌더링된 데이터에 액세스할 수 있습니다.

독립형 메트릭 전달 프로파일 생성

다음 절차에 따라 독립형 프로파일을 생성하고 서드파티에서 처리할 메트릭을 전달합니다.

시작하기 전에

이 프로파일을 생성하기 전에 메트릭을 전달할 서드파티 애플리케이션이 하나 이상 있어야 합니다.

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)** > **Metrics Forwarding(**메트릭 전달**)**로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** 고유한 프로파일 이름을 입력합니다.

단계 **4** (선택 사항) **Description(**설명**)**을 입력합니다. 이렇게 하면 유사한 이름의 다른 프로파일과 구분할 수 있습니다.

단계 **5** **Type(**유형**)** 드롭다운 메뉴를 확장하고 **Standalone(**독립형**)**을 선택합니다.

단계 **6** **Destination(**대상**)** 드롭다운 메뉴를 확장하고 메트릭을 처리하고 분석할 서드파티 애플리케이션을 선택합니다.

단계 **7** 메트릭의 엔드포인트 위치로 사용할 **Endpoint(**엔드포인트**)**를 입력합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

분석 애플리케이션으로 DataDog를 선택하는 경우, 엔드포인트는 기본적으로 HTTP Webhook로 채워집니다. 이 항목이 기본값인 경우 프로파일을 저장하기 전에 수정할 수 있습니다.

다음에 수행할 작업

- 프로파일 세부 정보 보기, 173 페이지
- 프로파일에 게이트웨이 연결 추가, 174 페이지

그룹 메트릭 전달 프로파일 생성

이 프로세스에서는 프로파일을 생성한 다음 특정 게이트웨이에 할당합니다. 그룹 프로파일은 최대 5개의 독립형 메트릭 전달 프로파일을 결합한 다음 단일 게이트웨이에 할당할 수 있습니다. 다음 절차를 사용하여 그룹화된 메트릭 전달 프로파일을 생성합니다.

시작하기 전에

- 이 프로파일을 생성하기 전에 메트릭을 전달할 서드파티 애플리케이션이 하나 이상 있어야 합니다.
- 둘 이상의 독립형 메트릭 전달 프로파일이 이미 생성되어 있어야 합니다. 자세한 내용은 독립형 메트릭 전달 프로파일 생성, 167 페이지를 참조하십시오.

단계 **1** 멀티 클라우드 방어 컨트롤러 인터페이스에서 **Manager(**관리자**)** > **Profiles(**프로파일 **)** > **Metrics Forwarding(**메트릭 전달**)**으로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** 고유 **Profile Name(**프로파일 이름**)**을 입력합니다.

단계 **4** (선택 사항) **Description(**설명**)**을 입력합니다. 이렇게 하면 유사한 이름의 프로파일을 구분하는 데 도움이 될 수 있습니다.

단계 **5** **Type(**유형**)** 드롭다운 메뉴를 확장하고 **Group(**그룹**)**을 선택합니다.

단계 **6** **Group Details(**그룹 세부 정보**)**에서 프로파일에 추가해야 하는 모든 새 행에 대해 **Add(**추가**)**를 클릭합니다.

단계 **7** 각 행에 대한 드롭다운 메뉴를 확장하여 그룹에 추가할 프로파일을 선택합니다. 저장하기 전에 언제든지 프로파일을 제거하려면, 해당 프로파일의 확인란을 선택하고 **Remove(**제거**)**를 선택합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 프로파일 세부 정보 보기, 173 페이지
- 프로파일에 게이트웨이 연결 추가, 174 페이지

NTP

멀티 클라우드 방어 게이트웨이은(는) NTP를 사용하여 동기화된 시간을 보장합니다. NTP는 관리 인터페이스를 통해 작동하며 관리 목적으로 사용되는 Linux 쉘의 일부로 설정됩니다. NTP 기본 구성은 다음과 같이 각 CSP마다 약간 다릅니다.

- **AWS:** `2.centos.pool.ntp.org`, `169.254.169.123`
- **Azure:** `0.centos.pool.ntp.org`, `1.centos.pool.ntp.org`, `2.centos.pool.ntp.org`, `3.centos.pool.ntp.org`
- **GCP:** `metadata.google.internal`
- **OCI:** `0.centos.pool.ntp.org`, `1.centos.pool.ntp.org`, `2.centos.pool.ntp.org`, `3.centos.pool.ntp.org`, `169.254.169.254`

기본 설정을 재정의하기 위해 NTP 프로파일을 생성하여 각 게이트웨이에 적용할 수 있습니다. NTP 프로파일이 게이트웨이에 적용되면 새 설정이 사용됩니다. 이 작업은 즉시 적용됩니다.

프로파일 생성

다음 절차에 따라 NTP 프로파일을 생성합니다.

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)** > **NTP**로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** 고유한 이름을 지정합니다.

단계 **4** (선택 사항) **Description(**설명**)**을 입력합니다. 이렇게 하면 유사한 이름의 다른 프로파일을 구분하는 데 도움이 될 수 있습니다.

단계 **5** NTP 서버 목록을 지정합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

What to do next

- 프로파일 세부 정보 보기, on page 173
- 프로파일에 게이트웨이 연결 추가, on page 174

BGP 프로파일

BGP(Border Gateway Protocol)는 IETF(Internet Engineering Task Force) 표준이며 모든 라우팅 프로토콜 중에서 가장 확장성이 뛰어납니다. BGP는 글로벌 인터넷 및 통신 사업자 프라이빗 네트워크의 라우팅 프로토콜입니다. BGP를 사용하면 VPN 게이트웨이와 BGP 인접한 라우터가 커넥터의 양쪽에 있는 게이트웨이에 관련 게이트웨이 또는 라우터의 가용성을 알리는 경로를 교환할 수 있습니다.

BGP 프로파일 생성

다음 절차에 따라 멀티 클라우드 방어 컨트롤러 대시보드에서 BGP 프로파일을 생성합니다.

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)** > **BGP**로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** 고유 **Profile Name(**프로파일 이름**)**을 입력합니다.

단계 **4** (선택 사항) **Description(**설명**)**을 입력합니다. 이렇게 하면 유사한 이름의 다른 프로파일과 구분할 수 있습니다.

단계 **5** **LocalAS** 값을 입력합니다. 이 값은 BGP4 디바이스가 상주하는 로컬 자율 시스템(AS)을 나타냅니다.

단계 **6** **Add Neighbor(**네이버 추가**)**를 클릭하여 프로파일에 하나 이상의 피어를 추가합니다.

단계 **7** **Neighbor(**인접한 라우터**)**에 다음 정보를 추가합니다.

a) **IP Address(IP** 주소**)** - IP 주소 및 BGP 피어 그룹의 단일 주소 또는 범위를 입력합니다. 여러 주소를 추가하는 경우에는 공백으로 각 주소를 구분합니다.

b) **Autonomous System(**자동 시스템**)** - 인접한 라우터가 상주하는 위치에 대한 **LocalAS**를 입력합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

BGP 프로파일을 멀티 클라우드 방어 게이트웨이에 추가합니다. 새 게이트웨이를 생성 하거나 새 프로파일을 포함하도록 기존 게이트웨이를 편집할 수 있습니다.

IPSec 프로파일

가상 터널 인터페이스에 IPSec(Internet Protocol Security) 프로파일을 사용하면 원격 액세스를 위한 보호를 제공해야 하는 경우 구성 프로세스를 간소화할 수 있습니다. IPSec 프로파일에는 두 사이트 간 VPN 피어 간의 안전한 논리적 통신 경로를 보장하는 데 필요한 필수 보안 프로토콜 및 알고리즘이 포함되어 있습니다. VPN은 네트워크-네트워크, 호스트-네트워크, 호스트-호스트 통신에 IPsec 터널에 의존하므로 터널을 생성할 때 필수 구성 요소입니다.

IPsec 프로파일을 사용하면 추가 보안 및 암호화 보호를 위해 IKE 및 IPSEC 매개 변수를 한 곳에서 구성할 수 있습니다.

IPSec 프로파일 생성

다음 절차에 따라 멀티 클라우드 방어 컨트롤러 대시보드에서 IPSec 프로파일을 생성합니다.

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)** > **IPSec**으로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** 고유 **Profile Name(**프로파일 이름**)**을 입력합니다.

단계 **4** (선택 사항) **Description(**설명**)**을 입력합니다. 이렇게 하면 유사한 이름의 다른 프로파일과 구분할 수 있습니다.

단계 **5** 프롬프트가 표시되면 적절한 IKE 정보를 입력합니다.

a) **DH Group(DH** 그룹**)** - DH(Diffie-Hellman) 그룹은 키 교환 프로세스에 사용되는 키의 강도를 결정합니다. 드롭다운 메뉴를 확장하여 프로파일에 적절한 그룹을 선택합니다.

b) **Authentication(**인증**)** - 이 터널에 대해 원하는 인증 유형을 선택하려면 드롭다운 메뉴를 확장합니다.

c) **Encryption(**암호화**)** - 가로채기된 스택에는 암호화 및 암호 해독이 필요합니다. 드롭다운 메뉴를 확장하여 암호화 방법을 선택합니다.

d) **Hash(**해시**)** - SHA1은 160비트 다이제스트를 생성하는 단방향 해싱 알고리즘입니다. 드롭다운 메뉴를 사용하여 적절한 옵션을 선택합니다.

e) **Key Lifetime(**키 수명**)** - 키가 지속되는 시간 값을 초 단위로 입력합니다. 사용 가능한 값은 60초 ~ 86400초입니다.

f) **IKE Version(IKE** 버전**)** - IKE(Internet Key Exchange)는 IP 패킷의 강력한 인증 및 암호화를 제공하는 IPSec 프로토콜 제품군의 보안 연결을 설정하는 데 사용되는 프로토콜입니다. 드롭다운 메뉴를 사용하여 IKE 버전 1 또는 버전 2를 선택합니다. 버전 간에는 상당한 차이점이 있으므로 환경에 가장 적합한 버전을 선택해야 합니다.

단계 **6** 프롬프트가 표시되면 적절한 IPsec 정보를 입력합니다.

a) **Authentication(**인증**)** - 드롭다운 메뉴를 확장하여 인증 방법으로 None(없음), SHA256, SHA 또는 Null을 선택합니다.

b) **Encryption(**암호화**)** - 드롭다운을 확장하고 키 유형(AES GCM 256, AES GCM 192 또는 AES GCM)을 선택합니다. 이렇게 하면 연결된 디바이스 간 고유 키 교환이 생성되므로 각 디바이스에서 다른 디바이스의 메시지를 암호 해독할 수 있습니다.
c) **Mode(**모드**)** - 드롭다운 메뉴를 확장하여 IPSec 정책 인증 프로토콜을 선택합니다. 둘 이상 선택할 수 있습니다.

다음에 수행할 작업

사이트 간 VPN 터널에 IPSec 프로파일을 연결합니다. 사이트 간 터널 연결 생성, 89 페이지를 수행하거나 새 IPSec 프로파일을 포함하도록 사이트 간 VPN 터널 편집할 수 있습니다.

20 장

프로파일 조치

프로파일 세부 정보 보기

다음 절차를 사용하여 패킷 캡처 프로파일의 세부 정보를 확인합니다.

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)**로 이동하고 적절한 프로파일 **Type(**유형**)**을 선택합니다.
단계 **2** 세부 정보를 보려는 프로파일을 선택합니다.
단계 **3** 프로파일 세부 정보를 봅니다.

독립형 메트릭 전달 프로파일 편집

이미 생성된 독립형 프로파일을 편집하려면 다음 절차를 사용합니다.

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)**로 이동하고 적절한 프로파일 **Type(**유형**)**을 선택합니다.
단계 **2** 편집할 프로파일 옆의 상자를 선택합니다.
단계 **3** **Edit(**편집**)**를 클릭합니다.
단계 **4** 필요에 따라 매개변수를 수정합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

그룹 프로파일 편집

이미 생성된 그룹화된 프로파일 집합을 편집하려면 다음 절차를 사용합니다.

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)**로 이동하고 적절한 프로파일 **Type(**유형**)**을 선택합니다.
단계 **2** 편집할 프로파일 옆의 상자를 선택합니다.
단계 **3** **Edit(**편집**)**를 클릭합니다.
단계 **4** 그룹 프로파일을 수정, 추가 또는 제거합니다.
단계 **5** **Save(**저장**)**를 클릭합니다.

프로파일에 게이트웨이 연결 추가

다음 절차를 사용하여 원하는 패킷 캡처 프로파일에 게이트웨이 연결을 추가합니다.

단계 **1** **Manage(**관리**)** > **Gateways(**게이트웨이**)** > **Gateways(**게이트웨이**)**로 이동합니다.
단계 **2** 프로파일을 연결할 게이트웨이 옆의 확인란을 선택합니다.
단계 **3** **Edit(**편집**)**를 클릭합니다.
단계 **4** 프로파일의 드롭다운 메뉴를 확장하고 메뉴에서 원하는 **Profile(**프로파일**)**을 선택합니다.
단계 **5** **Save(**저장**)**를 클릭합니다.

게이트웨이 연결 제거

다음 절차를 사용하여 패킷 캡처 프로파일과 연결된 기존 게이트웨이를 제거합니다. 이 프로세스는 프로파일에서 게이트웨이 연결만 제거합니다. 멀티 클라우드 방어에서 게이트웨이나 프로파일은 삭제되지 않습니다.

단계 **1** **Manage(**관리**)** > **Gateways(**게이트웨이**)** > **Gateways(**게이트웨이**)**로 이동합니다.
단계 **2** 패킷 캡처 프로파일에서 연결을 해제하려는 게이트웨이 옆의 확인란을 선택합니다.
단계 **3** **Edit(**편집**)**를 클릭합니다.
단계 **4** 페이지 하단으로 스크롤한 다음 해당 프로파일 드롭다운 메뉴에서 '**X**'를 클릭하여 연결을 제거합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

프로파일 삭제

다음 절차를 사용하여 패킷 캡처 프로파일을 삭제합니다. 이 프로세스에는 기존의 모든 게이트웨이 연결을 제거하고 프로파일을 삭제하는 작업이 포함됩니다.

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)**로 이동하고 적절한 프로파일 **Type(**유형**)**을 선택합니다.

단계 **2** 프로파일 세부 정보를 보고 연결된 게이트웨이를 검사합니다.

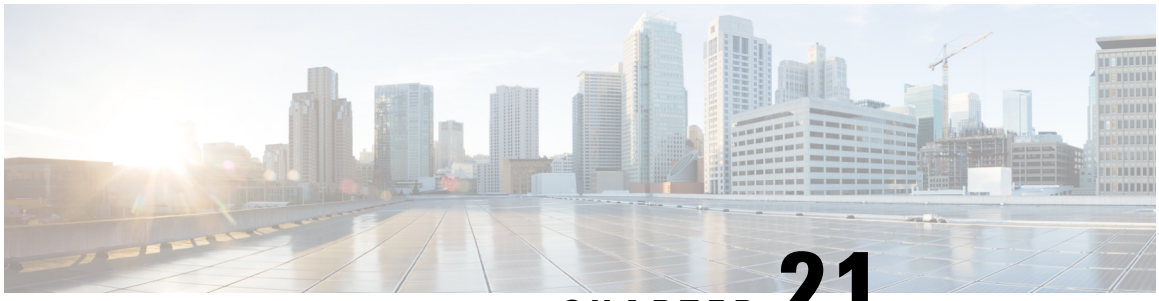
단계 **3** 모든 게이트웨이 연결을 제거합니다. 자세한 내용은 게이트웨이 연결 제거를 참조하십시오.

단계 **4** **Manage(**관리**)** > **Profiles(**프로파일**)**로 이동하여 1단계에서 선택한 것과 동일한 프로파일 유형을 선택합니다.

단계 **5** 삭제할 프로파일 옆의 상자를 선택합니다.

단계 **6** **Delete(**삭제**)**를 클릭합니다.

단계 **7** **Yes(**예**)** 또는 **No(**아니요**)**를 클릭하여 삭제 작업을 확인하거나 취소합니다.



CHAPTER 21

FQDN 및 URL 필터링 범주

FQDN / URL 필터링 범주

멀티 클라우드 방어은(는) WebRootTM BrightCloud(www.brightcloud.com)의 위협 인텔리전스를 사용하여 위험 점수에 따라 웹 사이트를 분류합니다. 여기에는 FQDN(Fully Qualified Domain Name)(도메인 이름이라고도 함) 및 URL이 포함됩니다. 퍼블릭 클라우드 환경의 트래픽이 다음 사이트로 아웃바운드 연결(이그레스)할 때 84개 범주에 대한 사이트를 제공합니다.

- FQDN(도메인) - 10억 개 이상 분류된 FQDN(도메인)
- URL - 450억 개 이상의 분류된 URL

트래픽 인식 및 처리의 효율성을 개선하기 위해 게이트웨이는 상위 100만 개 FQDN/URL 및 해당 범주의 캐시를 사전 로드합니다. 게이트웨이는 또한 상위 100만 개에 포함되지 않는 10k FQDN/URL 및 해당 범주의 런타임 캐시를 활용합니다. 트래픽에 캐시된 FQDN/URL이 포함되어 있으면 범주가 즉시 알려집니다. FQDN/URL을 캐시에 없는 경우 게이트웨이는 컨트롤러에 쿼리하여 BrightCloud를 통해 범주를 확인합니다. 이 작업은 200ms 이내에 완료될 것으로 예상됩니다. 예상 시간 내에 완료되면 학습한 범주에 따라 트래픽이 처리되고, 프로파일은 범주에 대해 정의된 정책에 따라 트래픽에서 작동합니다. 작업이 예상 시간 내에 완료되지 않으면 트래픽은 미분류로 처리되며, 프로파일은 미분류에 대해 정의된 정책에 따라 트래픽에서 작동합니다. 해결 방법이 반환되면 학습된 범주는 후속 해결을 위해 캐시에 추가됩니다. 해결 방법이 예상 시간 내에 발생하고 트래픽이 이미 처리된 경우에도 마찬가지입니다. 런타임 캐시가 소진되면 게이트웨이는 가장 최근에 액세스한 FQDN/URL 및 해당 범주에 사용할 수 있는 공간을 보장하기 위해 가장 오래된 FQDN/URL 및 해당 범주를 10개 항목씩 배치로 비웁니다.

Note 범주를 사용한 FQDN 필터링은 다음에 대해 발생합니다.

1. TLS Client Hello의 SNI
2. FQDN 조회를 위한 DNS 쿼리
3. HTTP 호스트 이름 헤더(일반 텍스트 HTTP 트래픽용)

악성 범주

멀티 클라우드 방어는 다음과 같은 범주를 특히 악성으로 간주합니다.

Table 7: 악성 범주 멀티 클라우드 방어는 다음 범주를 특히 악성으로 간주합니다.

범주 이름	범주 설명
악성코드 사이트	사이트는 실행 파일, 드라이브 바이 감염 사이트, 악성 스크립트, 바이러스, 트로이 목마 및 코드를 비롯한 악성 콘텐츠를 호스팅합니다.
피싱 및 기타 사기	일반적으로 사용자의 개인 정보를 수집하기 위해 평판이 좋은 사이트를 사칭하는 피싱, 파밍 및 기타 사이트입니다. 이러한 사이트는 일반적으로 수명이 매우 짧기 때문에 가동 시간 측면에서 오래 가지 않습니다.
프록시 회피 및 익명 서비스	프록시 서버 및 기타 방법을 사용하여 URL 필터링 또는 모니터링을 우회하는 모든 방식으로 URL에 액세스할 수 있습니다. 필터링을 우회하는 웹 기반 번역 사이트
키로거 및 모니터링	사용자의 키 입력을 추적하거나 웹서적을 모니터링하는 소프트웨어 에이전트입니다. 사용자 이름 및 비밀번호와 같은 민감한 데이터를 수집하는 데 자주 사용됩니다.
스팸 URL	원치 않는 이메일(스팸) 메시지를 배포하는 것으로 알려진 사이트입니다.
스파이웨어와 애드웨어	최종 사용자나 조직에 알려지지 않은 또는 최종 사용자나 조직의 명시적인 동의 없는 정보 수집이나 추적을 제공하거나 조장하는 스파이웨어 또는 애드웨어 사이트는 또한 사용자의 컴퓨터에 설치될 수 있는 원치 않는 광고 팝업 및 프로그램에 대한 광고를 진행합니다.

범주 이름	범주 설명
봇넷	이러한 URL은 봇 네트워크의 일부로 확인되는 URL 이며(주로 IP 주소) 네트워크 공격이 시작되는 지점 입니다. 공격에는 스팸 메시지, DOS, SQL 주입, 프록시 재킹 및 기타 요청하지 않은 접촉이 포함될 수 있습니다.

멀티 클라우드 방어에서는 **Discover(**검색**)** > **Traffic(**트래픽**)** > **DNS** 및 **Investigate(**조사**)** > **Flow Analytics(**플로우 분석**)** > **Traffic Summary(**트래픽 요약**)**를 통해 트래픽을 볼 때 트래픽 분석을 제공합니다. 여기서 사전 정의된 *Malicious Categories(*악성 범주*)* 필터를 선택하여 이러한 악성 범주 FQDN 및 URL과 통신하는 인스턴스 및 VPC를 표시할 수 있습니다.

전체 범주 목록은 아래에 나와 있습니다.

전체 범주 목록

범주 이름	범주 이름	범주 이름	범주 이름
낙태	게임	자동차	성교육
마약 남용	정부 기관	음악	셰어웨어 및 프리웨어
성인 및 음란물	혐오물	뉴스 및 미디어	쇼핑
주류 및 담배	해킹	노출	소셜 네트워킹
경매	증오 및 인종 차별	온라인 연하장	사회
봇넷	건강 및 약품	공개 HTTP 프록시	스팸 URL
비즈니스 및 경제	가정 및 원예	파킹된 도메인	스포츠
부정행위	사냥 및 낚시	유료 웹서핑	스파이웨어와 애드웨어
컴퓨터 및 인터넷 정보	불법	P2P(peer-to-peer)	스트리밍 미디어
컴퓨터 및 인터넷 보안	이미지 및 비디오 검색	개인 사이트 및 블로그	수영복 및 속옷
확인된 스팸 소스	개별 주식 자문 및 툴	개인 저장소	교육 및 툴
콘텐츠 전달 네트워크	인터넷 통신	철학 및 정치적 지지	변환
신앙 숭배 및 주술	인터넷 포털	피싱 및 기타 사기	여행
데이트	채용 정보 검색	프라이빗 IP 주소	미분류
데드 사이트	키로거 및 모니터링	프록시 회피 및 익명 서비스	확인되지 않은 스팸 소스
동적으로 생성된 콘텐츠	아동	의심스러운 항목	폭력
교육 기관	법무	부동산	무기

범주 이름	범주 이름	범주 이름	범주 이름
엔터테인먼트 및 예술	로컬 정보	레크리에이션 및 취미	웹 알림
패션 및 뷰티	악성코드 사이트	참조 및 연구	웹 호스팅
금융 서비스	대마초	종교	웹 기반 이메일
도박	군 검색 엔진	서비스	

필터링 프로파일을 정책 규칙 집합 규칙과 연결

- FQDN 필터링 프로파일을 생성/편집하려면 FQDN(Fully Qualified Domain Name) 필터 프로파일을 참조하십시오.
- URL 필터링 프로파일을 생성/편집하려면 URL(Uniform Resource Locator) 필터 프로파일을 참조하십시오.

BrightCloud URL/IP 조회 툴

BrightCloud는 특정 FQDN/URL이 웹 평판과 함께 어떤 범주로 분류되는지 파악하는 데 사용할 수 있는 온라인 URL/IP 조회 툴(https://www.brightcloud.com/tools/url-ip-lookup.php)을 제공합니다.

IX 부

조사 및 분석

조사 요약 페이지

멀티 클라우드 방어 컨트롤러의 Investigate(조사) 탭은 정책 효과 및 위협을 진단하는 데 도움이 될 수 있는 트래픽, 이벤트 및 로그 모음을 제공합니다.

플로우 분석

Flow Analytics(플로우 분석**)**는 멀티 클라우드 방어 게이트웨이에서 확인, 처리, 보호되는 트래픽에 대한 전반적인 가시성을 제공합니다. 트래픽은 트래픽 요약 로그와 보안 이벤트라는 두 가지 주요 범주로 구성됩니다. 트래픽 요약 로그는 게이트웨이에서 처리 중인 각 트래픽 세션과 관련된 정보를 제공합니다. 보안 이벤트는 게이트웨이 데이터 경로가 각 트래픽 세션을 보호하는 방법과 관련된 정보를 제공합니다.

네트워크 분석

Network Stats(네트워크 통계**)**는 게이트웨이의 성능에 대한 정보를 제공합니다. 생성된 그래프는 용량 임계값에 대응하기 위해 게이트웨이 및 연결된 게이트웨이 및 인스턴스가 자동으로 어떻게 확장

되는지 표시할 수 있습니다. 이는 게이트웨이 동작, 추세 또는 급증, 게이트웨이 관리 문제 해결에 유용한 도구가 될 수 있습니다.

시스템 상태

System Logs(시스템 로그**)**는 멀티 클라우드 방어 컨트롤러에 로그인한 사용자(시간 및 시간 범위 기준), 수행한 작업 등을 자세히 설명합니다.

22 장

플로우 분석

플로우 분석 - 트래픽 요약

이 보기에서는 정방향 또는 역방향 게이트웨이 프록시에서 멀티 클라우드 방어에 의해 기록된 이벤트에 대한 자세한 가시성, 필터링 및 분석을 제공합니다. 트래픽 요약 이벤트는 세 가지(3) 이벤트 유형, 즉 `Firewall Events(방화벽 이벤트)`, `Network Events(네트워크 이벤트)` 및 `Web Attacks(웹 공격)` 중 하나와 관련이 있을 수 있습니다.

트래픽 요약

Session Summary(세션 요약)에서 사용 가능한 테이블 및 필드는 다음과 같습니다.

이벤트 세부사항	설명
날짜 및 시간	ISO 8601 형식: YYYY-MM-DD T HH:MM:SS:S 예: `2020-11-22T10:58:46.820`
CSP 계정	멀티 클라우드 방어 CSP 계정
게이트웨이	멀티 클라우드 방어 게이트웨이
지역	멀티 클라우드 방어 게이트웨이의 지역
레벨	INFO
세션 ID	..

클라이언트 측 연결	설명
소스 IP	소스 IP 주소
소스 포트	소스 포트
대상 IP	대상 IP 주소
대상 포트	대상 포트
프로토콜	UDP, TCP

클라이언트 측 통계	클라이언트와 멀티 클라우드 방어 게이트웨이 간 트래픽
수신된 바이트	클라이언트에서 수신한 바이트 수
전송된 바이트	클라이언트로 전송된 바이트 수
수신된 패킷	클라이언트에서 수신한 패킷 수
전송된 패킷	클라이언트로 전송된 패킷 수

정책 일치 정보	설명
대상 주소 그룹	일치하는 정책 규칙에 구성된 대상 주소 그룹
소스 주소 그룹	일치하는 정책 규칙에 구성된 소스 주소 그룹
SNI 요청	요청의 서버 이름 표시
서비스 유형	Service Type(서비스 유형). 예: `PROXY`
소스 국가	클라이언트 측에서 요청이 시작된 국가
대상 국가	서버 측에서 요청이 대상으로 지정된 국가. 예: 미국.

서버 측 연결	설명
소스 IP	소스 IP 주소
소스 포트	소스 포트
대상 IP	대상 IP 주소
대상 포트	대상 포트
프로토콜	UDP, TCP

서버 측 통계	멀티 클라우드 방어 게이트웨이와 서버 간의 트래픽
수신된 바이트	서버에서 수신한 바이트 수
전송된 바이트	서버로 전송된 바이트 수
수신된 패킷	서버에서 수신한 패킷 수
전송된 패킷	서버로 전송된 패킷 수

애플리케이션 정보	설명
클라이언트 앱 이름	세션의 클라이언트 측과 연결된 애플리케이션 이름입니다. 예: `고급 패키징 툴`
페이로드 앱 이름	웹서버 호스트와 연결된 HTTP 애플리케이션 이름입니다. 예: `Facebook`
서비스 앱 이름	세션의 서버 측과 연결된 애플리케이션 이름입니다. 예: `HTTP`

작업	설명
조치	ALLOW, DENY.

클라우드 서비스	설명
클라우드 서비스	요청과 함께 액세스한 대상 클라우드 서비스의 이름입니다. 예: `AMAZON, EC2.`

소스 인스턴스 정보	설명
인스턴스 ID	클라이언트 인스턴스 ID
인스턴스 이름	클라이언트 인스턴스 이름(태그를 볼 수 있는 기능 제공)
VPC ID	클라이언트 VPC ID

HTTP 요청	설명
호스트	URL의 호스트 부분
방법	GET, PUT, POST, HEAD, DELETE, PATCH, OPTIONS
URI	URI 식별자 RFC 3986

규칙	설명
ID	멀티 클라우드 방어 규칙의 ID 번호/설명입니다. 예: `59 (egress-prod-apt-80).`

FQDN	설명
FQDN	전체(Fully Qualified) 도메인 이름
범주 이름	FQDN의 범주 분류. 예: 소셜 미디어
평판	FQDN의 평판 점수

Flow Analytics - All Events(플로우 분석 - 모든 이벤트)

Flow Analytics - All Events(플로우 분석 - 모든 이벤트**)**는 전체 멀티 클라우드 방어 솔루션에서 네트워크 및 보안 이벤트에 대한 전반적인 가시성을 제공합니다.

All Events(모든 이벤트)에서 사용 가능한 테이블과 필드는 다음과 같습니다.

이벤트 세부사항	설명
날짜 및 시간	ISO 8601 형식: YYYY-MM-DD T HH:MM:SS.S 예: `2020-11-22T10:58:46.820.`
유형	APPID, AV, DLP, DPI, FLOW_LOG, FQDNFILTER, L4_FW, L7DOS, MALICIOUS_SRC, SNI, TLS_ERROR, TLS_LOG, URLFILTER입니다.
CSP 계정	멀티 클라우드 방어 CSP 계정.
게이트웨이	멀티 클라우드 방어 게이트웨이.
지역	멀티 클라우드 방어 게이트웨이의 지역입니다.
레벨	DEBUG, INFO, NOTICE, WARNING, ERROR, CRITICAL, ALERT, EMERGENCY.
세션 ID	..

서비스	설명
소스 IP	소스 IP 주소.
소스 포트	소스 포트.
대상 IP	대상 IP 주소.
대상 포트	대상 포트.

서비스	설명
프로토콜	UDP, TCP.

애플리케이션 정보	설명
클라이언트 앱 이름	세션의 클라이언트 측과 연결된 애플리케이션 이름입니다. 예: 고급 패키징 툴.
페이로드 앱 이름	웹서버 호스트와 연결된 HTTP 애플리케이션 이름입니다. 예: Facebook.
서비스 앱 이름	세션의 서버 측과 연결된 애플리케이션 이름입니다. 예: HTTP.

작업	설명
조치	ALLOW, DENY.
주/도	ESTABLISHED, CLOSE, CLOSED, CLOSE_WAIT, TIME_WAIT, FIN_WAIT, LAST_ACK.

HTTP 요청	설명
호스트	URL의 호스트 부분.
방법	GET, PUT, POST, HEAD, DELETE, PATCH, OPTIONS.
URI	URI 식별자 RFC 3986.

규칙	설명
ID	멀티 클라우드 방어 규칙의 ID 번호/설명입니다. 예: 59 (egress-prod-apt-80).

FQDN	설명
FQDN	전체(Fully Qualified) 도메인 이름.
범주 이름	FQDN의 범주 분류. 예: 소셜 미디어.
평판	FQDN의 평판 점수입니다.

이벤트 로그

이벤트 로그는 멀티 클라우드 방어 게이트웨이을 통과하는 모든 트래픽의 세부 사항을 포함합니다.

검사 후 멀티 클라우드 방어은 패킷의 내용과 정책에 정의된 내용을 기반으로 세션 및 이벤트를 생성합니다. 이벤트의 분석, 관련 세부사항 및 수행되는 작업은 모두 **Investigate(**조사**)** > **Flow Analytics(**플로우 분석**)** > **All Events(**모든 이벤트**)**에서 로그 형식으로 모두 캡처됩니다. 시스템은 이러한 로그를 30일 동안 보존합니다.

로그가 캡처하는 이벤트 유형:

표 *8:* 이벤트 유형 및 설명

이벤트 유형	이벤트 이름	설명
FQDN 필터	FQDN(Fully Qualified Domain Name) 필터링	FQDN, 소스, 대상 IP 등의 세부 정보를 사용하여 관련 로그가 생성됩니다. FQDN 필터링 이벤트는 정책에 FQDN 필터링 프로파일이 있는 경우에만 생성됩니다.
SNI	SNI(Server Name Indication)	SNI를 사용하면 HTTPS를 통해 여러 호스트 이름을 제공할 수 있습니다. 이는 멀티 클라우드 방어이 TLS 핸드셰이크에서 SNI를 관찰할 때 생성됩니다.
APPID	앱 ID(APPID)	APPID는 네트워크 트래픽을 분석하여 L7 애플리케이션을 결정합니다. APPID 로그는 이벤트가 데이터베이스의 알려진 애플리케이션과 일치할 경우 생성됩니다.
L4_FW	L4 방화벽	이벤트가 규칙 집합의 정책과 일치하면 L4 방화벽 이벤트가 생성됩니다.
URL 필터	URL 필터링	URL 필터링은 URL을 기준으로 네트워크 트래픽을 필터링하는 데 사용됩니다. 이 이벤트 로그는 URL 필터링 프로파일과 일치할 때 생성됩니다.
IPS	IPS(침입 방지 시스템)	네트워크 트래픽이 IPS 규칙 집합과 일치하는 경우 IPS 이벤트가 생성됩니다.
DLP	DLP(Data Loss Protection)	네트워크 트래픽이 구성된 DLP 프로파일과 일치하는 경우 DLP 이벤트가 생성됩니다. 로그에는 엔드포인트, 도메인, 사용자 이름, 규칙, 소스, 대상, 수행한 작업 등의 전송 세부정보와 함께 이러한 인시던트가 기록됩니다.
WAF	웹 애플리케이션 방화벽	네트워크 트래픽이 구성된 WAF 프로파일과 일치하는 경우 WAF 이벤트가 생성됩니다.

이벤트 유형	이벤트 이름	설명
L7_DOS	레이어 7 DoS(Denial of Service)	네트워크 트래픽이 구성된 L7 DoS 프로파일과 일치하면 레이어 7 DoS 이벤트가 생성됩니다. 이러한 로그에는 이벤트 세부사항, 공격 시간, 요청, 완화 등이 포함됩니다.
AV	안티바이러스(AV)	AV 이벤트는 이벤트가 네트워크 트래픽의 AV 규칙 집합과 일치하는 경우 생성됩니다.
DPI	DPI(Deep Packet Inspection)	네트워크 트래픽이 고급 보안이 구성된 규칙과 일치할 경우 DPI 이벤트가 생성됩니다.
MALICIOUS_SRC	악성 소스	악성 소스는 네트워크 트래픽이 악성 IP와 일치할 때 생성됩니다.
TLS_ERROR	TLS 오류	TLS 핸드셰이크 중에 오류가 발생하는 경우 TLS 오류가 생성됩니다.
TLS_LOG	TLS 로그	TLS 로그는 네트워크 트래픽이 TLS를 사용할 때 생성됩니다. 암호 그룹 및 TLS 버전과 같은 TLS 핸드셰이크 정보를 캡처합니다.

Flow Analytics - Firewall Events(플로우 분석 - 방화벽 이벤트)

이 보기에서는 멀티 클라우드 방어 방화벽 구성에서 기록되고 방화벽 이벤트범주에 요약된 이벤트에 대한 자세한 가시성, 필터링 및 분석을 제공합니다.

Firewall Events(방화벽 이벤트)에서 사용 가능한 테이블과 필드는 다음과 같습니다.

이벤트 세부사항	설명
날짜 및 시간	ISO 8601 형식: YYYY-MM-DD T HH:MM:SS:S 예: `2020-11-22T10:58:46.820`
유형	APPID, L4_FW, MALICIOUS_SRC, SNI
CSP 계정	멀티 클라우드 방어 CSP 계정
게이트웨이	멀티 클라우드 방어 게이트웨이
지역	멀티 클라우드 방어 게이트웨이의 지역
레벨	DEBUG, INFO, NOTICE, WARNING, ERROR, CRITICAL, ALERT, EMERGENCY

이벤트 세부사항	설명
세션 ID	..

서비스	설명
소스 IP	소스 IP 주소
소스 포트	소스 포트
대상 IP	대상 IP 주소
대상 포트	대상 포트
프로토콜	UDP, TCP

애플리케이션 정보	설명
클라이언트 앱 이름	세션의 클라이언트 측과 연결된 애플리케이션 이름입니다. 예: 고급 패키징 툴
페이로드 앱 이름	웹서버 호스트와 연결된 HTTP 애플리케이션 이름입니다. 예: Facebook
서비스 앱 이름	세션의 서버 측과 연결된 애플리케이션 이름입니다. 예: HTTP

작업	설명
조치	ALLOW, DENY.
주/도	ESTABLISHED, CLOSE, CLOSED, CLOSE_WAIT, TIME_WAIT, FIN_WAIT, LAST_ACK

HTTP 요청	설명
호스트	URL의 호스트 부분
방법	GET, PUT, POST, HEAD, DELETE, PATCH, OPTIONS
URI	URI 식별자 RFC 3986

규칙	설명
ID	멀티 클라우드 방어 규칙의 ID 번호/설명입니다. 예: 59(egress-prod-apt-80)

FQDN	설명
FQDN	전체(Fully Qualified) 도메인 이름
범주 이름	FQDN의 범주 분류. 예: 소셜 미디어
평판	FQDN의 평판 점수

플로우 분석 - 네트워크 위협

이 보기는 멀티 클라우드 방어 위협 분석 엔진에 의해 기록되고 네트워크 위협에 요약된 위협에 대한 자세한 가시성, 필터링 및 분석을 제공합니다.

네트워크 위협

Network Threats(네트워크 위협)에서 사용 가능한 테이블과 필드는 다음과 같습니다.

이벤트 세부사항	설명
날짜 및 시간	ISO 8601 형식: YYYY-MM-DD T HH:MM:SS:S 예: `2020-11-22T10:58:46.820`
유형	AV, DLP, DPI
CSP 계정	멀티 클라우드 방어 CSP 계정
게이트웨이	멀티 클라우드 방어 게이트웨이
지역	멀티 클라우드 방어 게이트웨이의 지역
레벨	DEBUG, INFO, NOTICE, WARNING, ERROR, CRITICAL, ALERT, EMERGENCY
세션 ID	..

서비스	설명
소스 IP	소스 IP 주소
소스 포트	소스 포트
대상 IP	대상 IP 주소
대상 포트	대상 포트
프로토콜	UDP, TCP

애플리케이션 정보	설명
클라이언트 앱 이름	세션의 클라이언트 측과 연결된 애플리케이션 이름입니다. 예: 고급 패키징 툴
페이로드 앱 이름	웹서버 호스트와 연결된 HTTP 애플리케이션 이름입니다. 예: Facebook
서비스 앱 이름	세션의 서버 측과 연결된 애플리케이션 이름(예: HTTP)

작업	설명
조치	ALLOW, DENY.
주/도	ESTABLISHED, CLOSE, CLOSED, CLOSE_WAIT, TIME_WAIT, FIN_WAIT, LAST_ACK

HTTP 요청	설명
호스트	URL의 호스트 부분
방법	GET, PUT, POST, HEAD, DELETE, PATCH, OPTIONS
URI	URI 식별자 RFC 3986

FQDN	설명
FQDN	전체(Fully Qualified) 도메인 이름
범주 이름	FQDN의 범주 분류. 예: 소셜 미디어
평판	FQDN의 평판 점수

규칙	설명
ID	멀티 클라우드 방어 규칙의 ID 번호/설명입니다. 예: 59(egress-prod-apt-80)

플로우 분석 - 웹 공격

이 보기는 멀티 클라우드 방어 웹 보호 엔진에 의해 기록된 위협에 대한 자세한 가시성, 필터링 및 분석을 제공합니다. 웹 공격 이벤트 유형에는 WAF 및 L7DOS가 포함됩니다.

웹 공격

Web Attacks(웹 공격)에서 사용 가능한 테이블과 필드는 다음과 같습니다.

이벤트 세부사항	설명
날짜 및 시간	ISO 8601 형식: YYYY-MM-DD T HH:MM:SS:S 예: `2020-11-22T10:58:46.820`
유형	L7DOS, WAF
CSP 계정	멀티 클라우드 방어 CSP 계정
게이트웨이	멀티 클라우드 방어 게이트웨이
지역	멀티 클라우드 방어 게이트웨이의 지역
레벨	DEBUG, INFO, NOTICE, WARNING, ERROR, CRITICAL, ALERT, EMERGENCY
세션 ID	..

서비스	설명
소스 IP	소스 IP 주소
소스 포트	소스 포트
대상 IP	대상 IP 주소
대상 포트	대상 포트
프로토콜	UDP, TCP

애플리케이션 정보	설명
클라이언트 앱 이름	세션의 클라이언트 측과 연결된 애플리케이션 이름입니다. 예: `고급 패키징 툴`
페이로드 앱 이름	웹서버 호스트와 연결된 HTTP 애플리케이션 이름입니다. 예: `Facebook`
서비스 앱 이름	세션의 서버 측과 연결된 애플리케이션 이름(예: `HTTP`)

작업	설명
조치	ALLOW, DENY.
주/도	ESTABLISHED, CLOSE, CLOSED, CLOSE_WAIT, TIME_WAIT, FIN_WAIT, LAST_ACK

HTTP 요청	설명
호스트	URL의 호스트 부분

HTTP 요청	설명
방법	GET, PUT, POST, HEAD, DELETE, PATCH, OPTIONS
URI	URI 식별자 RFC 3986

FQDN	설명
FQDN	전체(Fully Qualified) 도메인 이름
범주 이름	FQDN의 범주 분류. 예: 소셜 미디어
평판	FQDN의 평판 점수

규칙	설명
ID	멀티 클라우드 방어 규칙의 ID 번호/설명입니다. 예: 59(egress-prod-apt-80)

플로우 분석 - URL 필터링

이 보기에서는 멀티 클라우드 방어 URL 필터링 구성에서 기록된 이벤트에 대한 자세한 가시성, 필터링 및 분석을 제공합니다. URL 필터링 이벤트는 세 가지 이벤트 유형, 즉 `Firewall Events(방화벽 이벤트)`, `Network Events(네트워크 이벤트)` 및 `Web Attacks(웹 공격)` 중 하나와 관련이 있을 수 있습니다.

URL 필터링

URL 필터링에서 사용할 수 있는 테이블과 필드는 다음과 같습니다.

이벤트 세부사항	설명
날짜 및 시간	ISO 8601 형식: YYYY-MM-DD T HH:MM:SS:S 예: `2020-11-22T10:58:46.820`
유형	URLFILTER
CSP 계정	멀티 클라우드 방어 CSP 계정
게이트웨이	멀티 클라우드 방어 게이트웨이
지역	멀티 클라우드 방어 게이트웨이의 지역
레벨	DEBUG, INFO, NOTICE, WARNING, ERROR, CRITICAL, ALERT, EMERGENCY
세션 ID	..

서비스	설명
소스 IP	소스 IP 주소
소스 포트	소스 포트
대상 IP	대상 IP 주소
대상 포트	대상 포트
프로토콜	UDP, TCP

애플리케이션 정보	설명
클라이언트 앱 이름	세션의 클라이언트 측과 연결된 애플리케이션 이름입니다. 예: `고급 패키징 툴`.
페이로드 앱 이름	웹서버 호스트와 연결된 HTTP 애플리케이션 이름입니다. 예: `Facebook`
서비스 앱 이름	세션의 서버 측과 연결된 애플리케이션 이름(예: `HTTP`)

작업	설명
조치	ALLOW, DENY.
주/도	ESTABLISHED, CLOSE, CLOSED, CLOSE_WAIT, TIME_WAIT, FIN_WAIT, LAST_ACK

HTTP 요청	설명
호스트	URL의 호스트 부분
방법	GET, PUT, POST, HEAD, DELETE, PATCH, OPTIONS
URI	URI 식별자 RFC 3986

규칙	설명
ID	멀티 클라우드 방어 규칙의 ID 번호/설명입니다. 예: 59(egress-prod-apt-80)

FQDN	설명
FQDN	전체(Fully Qualified) 도메인 이름
범주 이름	FQDN의 범주 분류. 예: `소셜 미디어`
평판	FQDN의 평판 점수

플로우 분석 - FQDN 필터링

이 보기에서는 FQDN 필터링 구성에서 기록된 이벤트에 대한 자세한 가시성, 필터링 및 분석 옵션을 제공합니다. FQDN 필터링 이벤트는 세 가지 이벤트 유형, 즉 `Firewall Events(방화벽 이벤트)`, `Network Events(네트워크 이벤트)` 및 `Web Attacks(웹 공격)` 중 하나와 관련이 있을 수 있습니다.

FQDN 필터링

FQDN 필터링에서 사용할 수 있는 테이블과 필드는 다음과 같습니다.

이벤트 세부사항	설명
날짜 및 시간	ISO 8601 형식: YYYY-MM-DD T HH:MM:SS:S 예: `2020-11-22T10:58:46.820`.
유형	FQDNFILTER.
CSP 계정	멀티 클라우드 방어 CSP 계정.
게이트웨이	멀티 클라우드 방어 게이트웨이.
지역	멀티 클라우드 방어 게이트웨이의 지역입니다.
레벨	DEBUG, INFO, NOTICE, WARNING, ERROR, CRITICAL, ALERT, EMERGENCY.
세션 ID	..

서비스	설명
소스 IP	소스 IP 주소.
소스 포트	소스 포트.
대상 IP	대상 IP 주소.
대상 포트	대상 포트.
프로토콜	UDP, TCP.

작업	설명
조치	ALLOW, DENY.
주/도	ESTABLISHED, CLOSE, CLOSED, CLOSE_WAIT, TIME_WAIT, FIN_WAIT, LAST_ACK.

HTTP 요청	설명
호스트	URL의 호스트 부분.
방법	GET, PUT, POST, HEAD, DELETE, PATCH, OPTIONS.
URI	URI 식별자 RFC 3986.

FQDN	설명
FQDN	전체(Fully Qualified) 도메인 이름.
범주 이름	FQDN의 범주 분류. 예: 소셜 미디어.
평판	FQDN의 평판 점수입니다.

규칙	설명
ID	멀티 클라우드 방어 규칙의 ID 번호/설명입니다. 예: 59(egress-prod-apt-80).

플로우 분석 - **HTTPS** 로그

이 보기에서는 HTTPS 로그에서 기록된 이벤트에 대한 자세한 가시성, 필터링 및 분석 옵션을 제공합니다. HTTPS 로그는 세 가지 이벤트 유형, 즉 `Firewall Events(방화벽 이벤트)`, `Network Events(네트워크 이벤트)` 및 `Web Attacks(웹 공격)` 중 하나와 관련이 있을 수 있습니다.

HTTPS 로그

HTTPS Logs(HTTPS 로그)에서 사용 가능한 테이블과 필드는 다음과 같습니다.

이벤트 세부사항	설명
날짜 및 시간	ISO 8601 형식: YYYY-MM-DD T HH:MM:SS:S 예: `2020-11-22T10:58:46.820`
유형	TLS_ERROR, TLS_LOG.
CSP 계정	멀티 클라우드 방어 CSP 계정.
게이트웨이	멀티 클라우드 방어 게이트웨이.
지역	멀티 클라우드 방어 게이트웨이의 지역입니다.
레벨	DEBUG, INFO, NOTICE, WARNING, ERROR, CRITICAL, ALERT, EMERGENCY.
세션 ID	..

서비스	설명
소스 IP	소스 IP 주소.
소스 포트	소스 포트.
대상 IP	대상 IP 주소.
대상 포트	대상 포트.
프로토콜	UDP, TCP.

애플리케이션 정보	설명
클라이언트 앱 이름	세션의 클라이언트 측과 연결된 애플리케이션 이름입니다. 예: 고급 패키징 툴.
페이로드 앱 이름	웹서버 호스트와 연결된 HTTP 애플리케이션 이름입니다. 예: Facebook.
서비스 앱 이름	세션의 서버 측과 연결된 애플리케이션 이름(예: HTTP) .

작업	설명
조치	ALLOW, DENY.
주/도	ESTABLISHED, CLOSE, CLOSED, CLOSE_WAIT, TIME_WAIT, FIN_WAIT, LAST_ACK.

HTTP 요청	설명
호스트	URL의 호스트 부분.
방법	GET, PUT, POST, HEAD, DELETE, PATCH, OPTIONS.
URI	URI 식별자 RFC 3986.

FQDN	설명
FQDN	전체(Fully Qualified) 도메인 이름.
범주 이름	FQDN의 범주 분류. 예: 소셜 미디어.
평판	FQDN의 평판 점수입니다.

23 장

네트워크 분석

Stats

이 보기에서는 선택한 멀티 클라우드 방어 게이트웨이의 대역폭 및 연결에 대한 즉각적 및 선택한 기간의 가시성을 자세히 확인할 수 있습니다.

단계 **1** **Investigate(**조사**)** > **Network Analytics(**네트워크 분석**)** > **Stats(**통계**)**로 이동합니다.

단계 **2** 처음에 `All CSP Accounts(모든 CSP 계정)` 및 `All Gateways(모든 게이트웨이)`에 대한 통계가 표시되며 기간은 `Last 1 hour(지난 1시간)`입니다.

단계 **3** X축과 Y축은 기간 선택/대역폭을 기준으로 자동 크기 조정되고, 보는 동안 자동 업데이트됩니다. 통계는 이 페이지를 보는 동안 5초마다 새로 고침됩니다.

단계 **4** 필터 표시줄의 드롭다운 옵션을 사용하여 표시를 세부적으로 변경하고 특정 **Account(**계정**)**, **CSP Type(CSP** 유형**)** 또는 **Instance Type(**인스턴스 유형**)**의 통계를 볼 수 있습니다.

Instance Type(인스턴스 유형**)**을 선택하면 두 개의 추가 통계, 즉 CPU 사용량과 메모리 사용량이 표시됩니다.

단계 **5** 아래와 같이 풀다운에서 **Timeframe(**기간**)**을 선택합니다. 옵션은 다음과 같습니다. `Last 15 mins(지난 15분)` `Last 1 hour(지난 1시간)` `Last 1 day(지난 1일)` `Last 7 Days(지난 7일)` `Last 30 days(지난 30일)`.

총 대역폭

총 네트워크 대역폭은 지정된 시간 동안 네트워크 연결을 통해 데이터를 전송하는 유선 또는 무선 링크의 최대 용량을 나타내는 측정 단위입니다. 이 값은 총 속도(선택한 게이트웨이의 인바운드 및 아웃바운드 대역폭 추가), 인바운드 대역폭(게이트웨이를 인그레스하는 대역폭) 및 아웃바운드 대역폭(게이트웨이를 이그레스하는 대역폭)의 컴파일입니다.

CPU 사용

참고 이 통계는 페이지 상단에 있는 필터 표시줄에서 선택 사항으로 인스턴스 유형을 포함하는 경우에만 사용할 수 있습니다.

이 보기는 정상 메모리 사용보다 높을 수 있는 게이트웨이 인스턴스에 대한 정보를 제공합니다. 이 정보를 사용하여 CPU 용량에 따라 게이트웨이 활동의 성능을 모니터링하고 최적화할 수 있습니다. 또한 이러한 통계를 사용하여 트래픽의 추세 및 동작에 대해 CPU가 나타내는 노력을 평가할 수도 있습니다.

메모리 사용

참고 이 통계는 페이지 상단에 있는 필터 표시줄에서 선택 사항으로 인스턴스 유형을 포함하는 경우에만 사용할 수 있습니다.

이 보기는 정상 메모리 사용보다 높을 수 있는 게이트웨이 인스턴스에 대한 정보를 제공합니다. 이 정보를 사용하여 메모리 사용량 용량에 따라 게이트웨이 활동의 성능을 모니터링하고 최적화할 수 있습니다.

연결 속도

연결 속도는 총 시도된 통화 중 성공적으로 연결된 통화의 백분율을 나타냅니다. 특히 연결(총 활성 연결 수) 및 초당 연결(게이트웨이에 대한 인바운드 및 아웃바운드 연결의 대역폭)과 동일합니다.

HTTP 요청 속도

HTTP 요청 속도는 일반적으로 상위 수준 시스템별 메트릭으로 측정된 시스템에 대한 수요가 얼마나 되는지 측정합니다. 웹 서비스의 경우 측정은 일반적으로 초당 HTTP 요청 수입니다.

24 장

시스템 상태

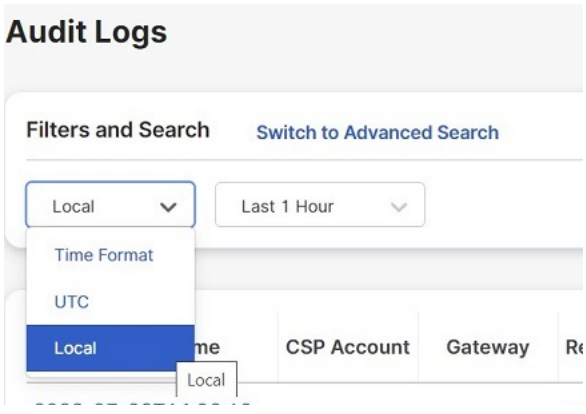
감사 로그

감사 로그에는 사용자가 수행한 작업의 세부사항이 포함됩니다. 여기에는 로그인/로그아웃 활동, 프로파일, 규칙, 게이트웨이의 생성, 삭제, 업데이트, 활성화, 비활성화 등이 포함되며 이에 국한되지 않으며, 멀티 클라우드 방어 솔루션의 구성 및 운영과 관련된 모든 사용자 활동을 포함합니다.

시간 형식

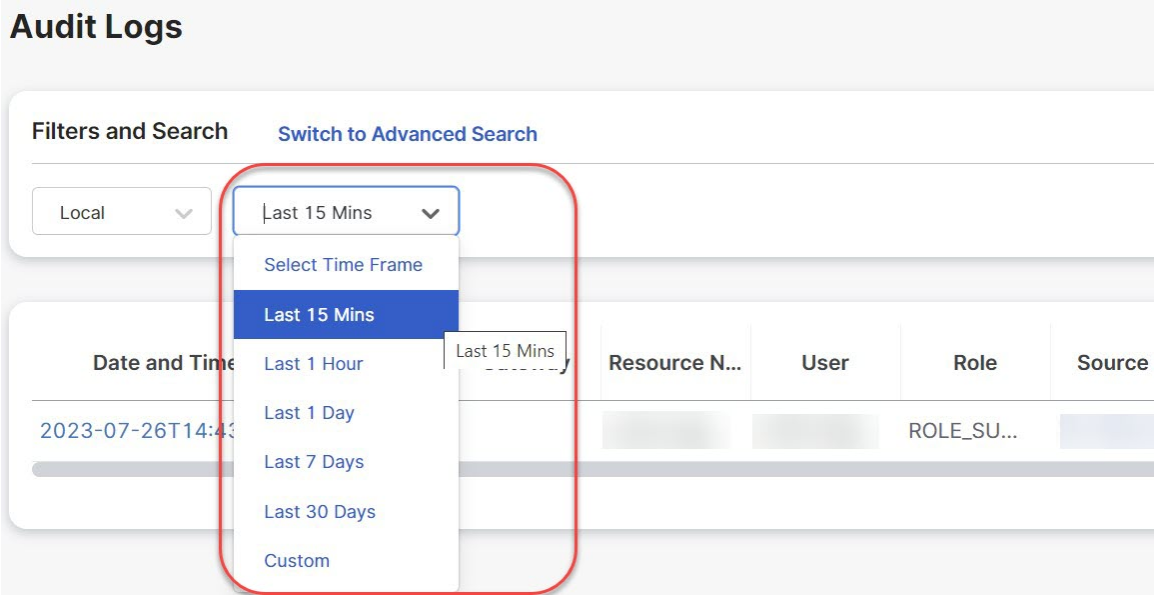
로그는 UTC(Coordinated Universal Time) 또는 현지 시간 형식으로 표시할 수 있습니다. Local(지역)은 구성된 사용자의 표준 시간대를 의미합니다(예: 미국/태평양). 로그의 날짜 및 시간은 ISO 8601 형식으로 표시됩니다(전체 날짜와 시간, 분, 초 및 소수점 이하 초 - YYYY-MM-DD T HH:MM:SS:S). 예: `2020-11-22T10:58:46.820`

다른 시간 형식을 선택하거나 다른 시간 형식 간에 전환하려면 다음과 같이 라디오 버튼을 클릭합니다.



타임프레임

로그는 15분~30일 사이의 증분 옵션 또는 사용자 지정 기간으로 표시할 수 있습니다. 기간을 선택하거나 기간을 전환하려면 드롭다운 메뉴를 클릭하고 다음과 같이 기간을 선택합니다.



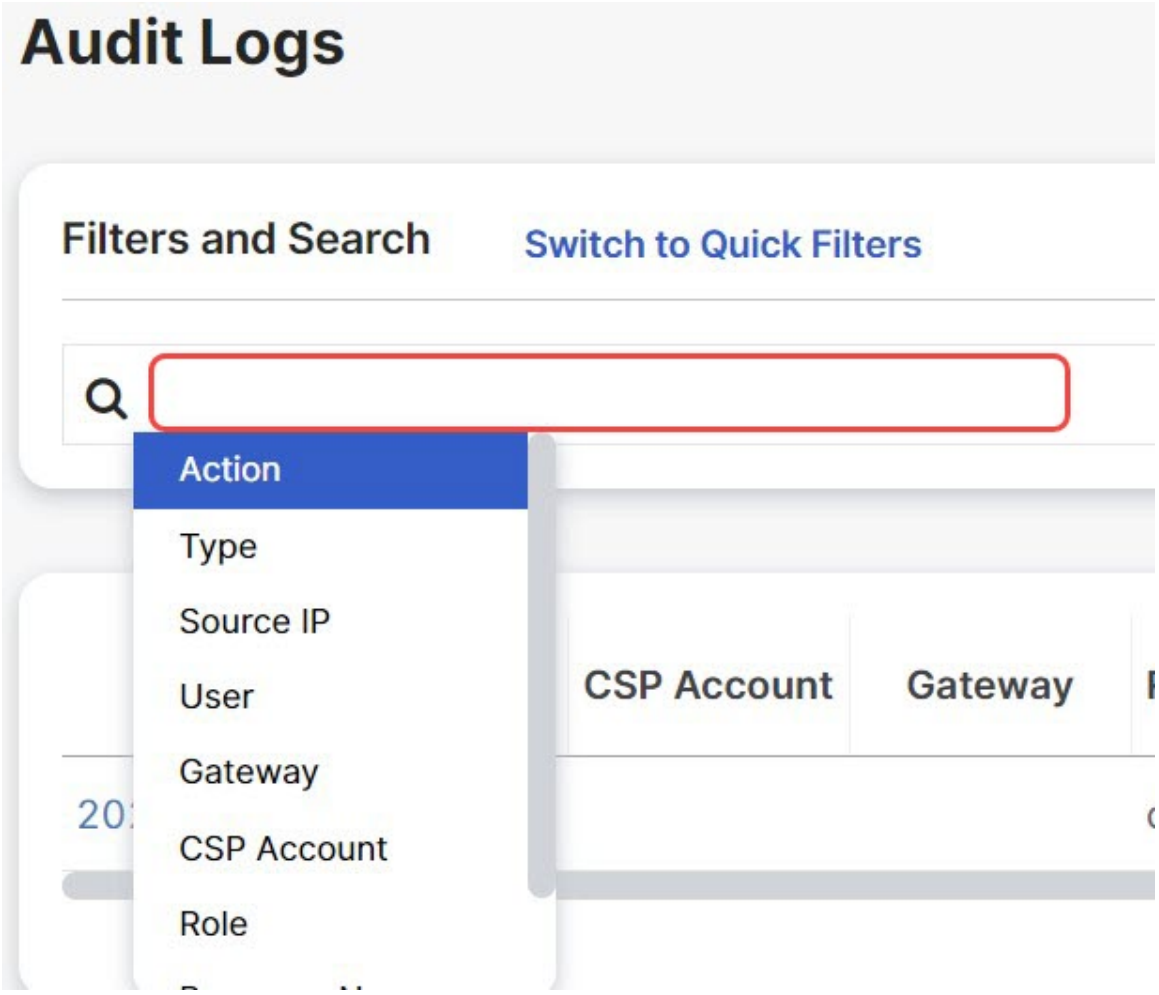
맞춤형 기간의 경우 달력 개체를 클릭하여 **Custom(맞춤형)**, **Start(시작)** 및 **End(종료)** 날짜 또는 시간을 선택하고 저장합니다.

검색 필터

로그는 검색 기능 및 감사 로그 필드를 사용하여 필터링할 수 있습니다. 감사 로그 필드는 `Action(작업)` `Type(유형)` `Source IP(소스 IP)` `User(사용자)` `Gateway(게이트웨이)` `CSP Account(CSP 계정)` `Role(역할)` 입니다.

하나 또는 여러 개의 필드에서 감사 로그를 필터링하려면 다음을 수행합니다.

단계 **1** 풀다운 메뉴에 액세스하려면 Search(검색) 필드에서 왼쪽 마우스를 클릭합니다.



단계 **2** 필드를 선택합니다.

단계 **3** 원하는 검색 문자열을 입력합니다.

단계 **4** 필요에 따라 검색 기준에 필드를 추가합니다.

예: Filter for Actions = **"DELETE"**이고 **"steve"**를 포함하는 문자열과 사용자가 수행한 경우 필터 기준과 결과에 표시됩니다.

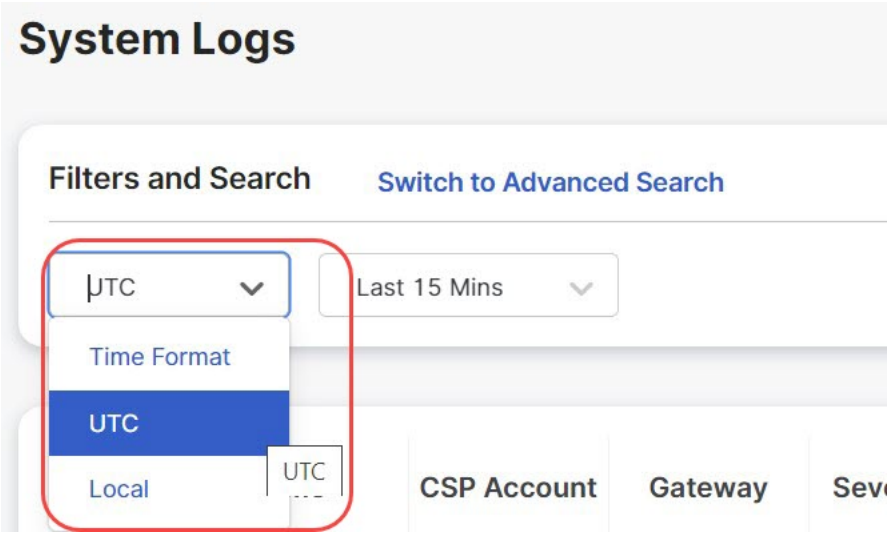
시스템 로그

시스템 로그에는 멀티 클라우드 방어 솔루션이 수행하는 작업의 세부 정보가 포함됩니다. 여기에는 시스템 메시지, 게이트웨이 이벤트, 인스턴스 생성 또는 삭제, 멀티 클라우드 방어 솔루션의 기타 구성 및 운영 수정 등이 포함됩니다. 시스템은 이 로그를 1년 동안 저장합니다.

시간 형식

로그는 UTC(Coordinated Universal Time) 또는 로컬 형식으로 표시합니다. 로컬은 구성된 사용자의 시간대를 의미합니다. 예: 미국/태평양. 로그의 날짜 및 시간은 ISO 8601 형식으로 표시합니다(전체 날짜와 시간, 분, 초 및 소수점 이하 초 - YYYY-MM-DD T HH:MM:SS:S). 예: `2020-11-22T10:58:46.820`

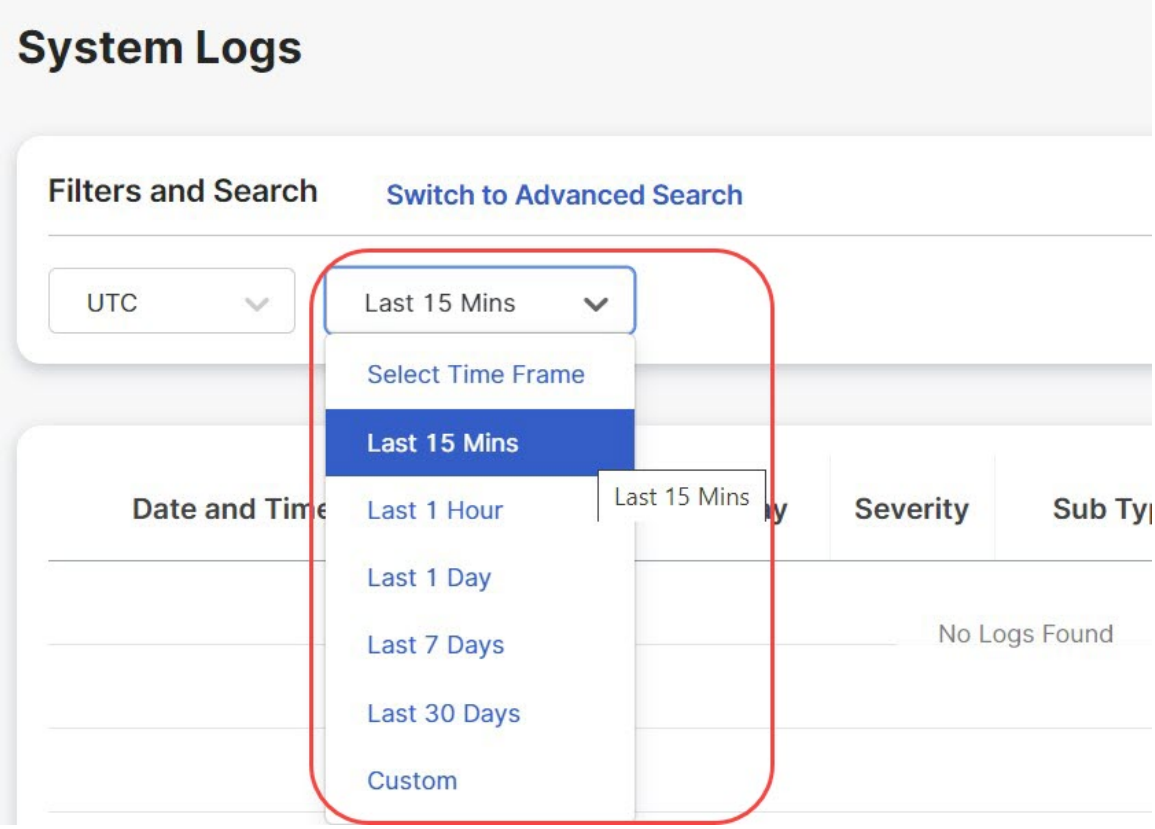
다른 시간 형식을 선택하거나 다른 시간 형식 간에 전환하려면 다음과 같이 라디오 버튼을 클릭합니다.



타임프레임

로그는 15분~30일 사이의 증분 옵션 또는 맞춤형 기간으로 표시합니다.

기간을 선택하거나 기간을 전환하려면 드롭다운을 클릭하고 다음과 같이 기간을 선택합니다.



맞춤형 기간의 경우 달력 개체를 클릭하여 **Custom(맞춤형)**, **Start(시작)** 및 **End(종료)** 날짜 또는 시간을 선택하고 저장합니다.

심각도 레벨

시스템 로그의 심각도 레벨은 다음과 같습니다.

- `Info(정보)` - 로그인, 로그아웃, 비밀번호 변경, 구성 변경 등과 같은 정보를 제공하는 세부 정보입니다. 여기에는 다른 심각도 레벨의 자격이 없는 이벤트가 포함됩니다.
- `Warning(경고)` - 비밀번호 업데이트 등의 가능한 시스템 작업 또는 변경 사항에 대해 알려주는 알림입니다.
- `Medium(중간)` - 패키지 업그레이드 등 심각도가 중간인 문제입니다.
- `High(높음)` - 외부 디바이스와의 네트워크 연결 끊김 등의 심각한 문제입니다.
- `Critical(중대)` - 하드웨어 오류 등과 같이 본질적으로 중요한 주요 문제입니다.

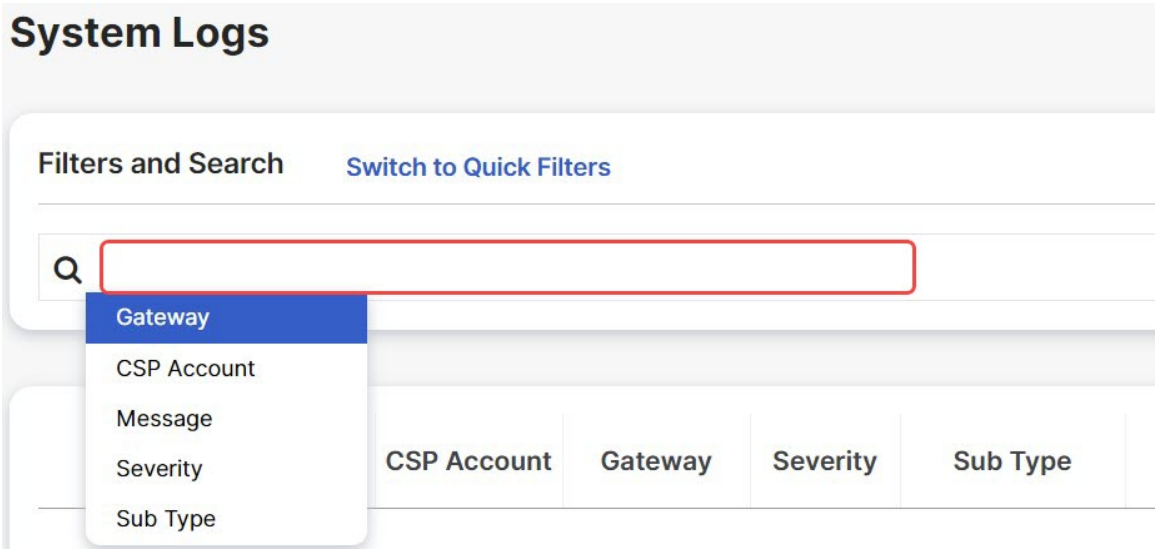
검색 필터

로그는 Search(검색) 기능 및 System log(시스템 로그) 필드를 사용하여 필터링할 수 있습니다.

시스템 로그 필드는 `Gateway(게이트웨이)` `CSP Account(CSP 계정)` `Message(메시지)`입니다.

하나 또는 여러 개의 필드에서 시스템 로그를 필터링하려면 다음을 수행합니다.

단계 **1** 풀다운 메뉴에 액세스하려면 Search(검색) 필드에서 왼쪽 마우스를 클릭합니다.



단계 **2** 필드(예: `Gateway(게이트웨이)`)를 선택합니다.

단계 **3** 원하는 검색 문자열을 입력합니다(예: `ingress`).

단계 **4** 필요에 따라 검색 기준에 필드를 추가합니다.

예: Filter for Gateway = **"ingress"** 및 **"created"**를 포함하는 메시지가 필터 기준 및 결과에 표시됩니다.

X 부

위협 조사

25 장

위협 조사

위협 연구는 위협 및 악성 활동을 탐지하기 위해 검사 엔진에 적용되는 규칙 집합에서 생성됩니다. 이 페이지에서 이러한 규칙을 볼 수 있습니다. 하루에 한 번 멀티 클라우드 방어는 네트워크 침입에 대해 새롭거나 수정된 규칙을 검색하고, 내부 라이브러리에 규칙 및 알려진 악성 소스를 포함하거나 제거합니다. 이 작업은 자동화되어 있습니다. 이 기능에는 새 IP 주소 목록을 소스로 다운로드 및 검증하여 이를 새 규칙 집합에서 구현하는 작업이 포함됩니다. 그런 다음 이러한 규칙 집합이 구축됩니다.

규칙은 정책, 클래스, 애플리케이션, 규칙 집합 라이브러리 날짜 및 기타 매개변수 등 다양한 방식으로 구성됩니다. 트립된 규칙(예: 위협 또는 악성 활동 감지)에 대해 자세히 알고 싶은 경우 **Threat Research(**위협 조사**)** 페이지에서 규칙에 대한 자세한 내용을 확인하십시오. 각 페이지의 다음 부분을 사용할 수 있습니다.

검색 창

창 상단의 검색 창을 사용하면 위협 조사에서 각 페이지에서 알려진 IP 주소, 동작, 규칙 이름, 게이트웨이 이름, 공격 유형 또는 프로파일 이름과 같은 특정 식별 요소를 검색할 수 있습니다. 스크롤하여 특정 필드 값을 찾는 경우 **Add to Search(**검색에 추가**)**를 사용하여 더 쉽게 검색할 수 있습니다.

검색은 각 페이지로 분리되어 있으며, 서로 다른 유형의 위협 조사를 교차 검색할 수 없습니다. 자세한 내용은 아래 참조하십시오.

세부사항 보기

위협 조사 중인 각 측면은 단일 인시던트 또는 공격의 세부 정보 보기 기능을 제공합니다. 이러한 세부 사항에서 제공되는 값은 위협 조사 유형에 따라 다르지만 정책, 보안 프로파일, 규칙 또는 규칙 집합을 세부적으로 조정하려는 경우 유용할 수 있습니다.

검색에 추가

여기에서 사용 가능한 모든 조사 유형의 경우, 행 내의 값 하나를 클릭하면 **Add to Search(**검색에 추가) 옵션을 자동으로 포함할 수 있습니다. 이렇게 하면 선택한 값이 창 상단의 검색창에 자동으로 적용되고 검색창의 콘텐츠에 맞게 보기 창이 필터링됩니다. 이 작업은 여러 번 수행할 수 있으며 선택한 값이 복잡한 검색 요청과 결합합니다.

- 네트워크 침입, 210 페이지
- 웹 보호, 210 페이지

• 악성 소스, 211 페이지

네트워크 침입

네트워크 침입은 네트워크에서의 무단 활동을 의미합니다. 이 표에는 IDS/IPS 엔진에 기본 제공되는 규칙 또는 이러한 규칙의 계열사 정보는 포함되지 않습니다. 이러한 규칙은 탐지 전용으로 지정됩니다. IDS/IPS 규칙의 나머지 부분은 다양한 침입 또는 공격 레벨에 따라 보호하고 작업을 수행하도록 설정됩니다.

Network Intrusion(네트워크 침입) 페이지에 다음 정보가 표시됩니다.

- **Gateway Names(**게이트웨이 이름**)** - 악성 소스를 처리한 영향을 받은 게이트웨이의 이름.
- **Profile Names(**프로파일 이름**)**- 악의적인 소스에 의해 트리거된 보안 프로파일의 이름.
- **IPS** 정책 - 이벤트 또는 공격에 의해 트리거된 멀티 클라우드 방어 내의 정책.
- **IPS** 클래스 - 공격 신호의 데이터베이스에 의해 결정된 공격 유형을 비교.
- **IPS** 범주 - 이벤트 또는 공격에 의해 트리거된 IPS 서명 범주.
- 규칙 **ID** - 멀티 클라우드 방어 내에 내부적으로 문서화된 이벤트 또는 공격에 의해 트리거된 규칙 ID.
- 영향을 받은 서비스 - 이벤트 또는 공격의 영향을 받는 웹 서비스의 유형.
- 영향 - 이벤트 또는 공격에 의한 영향의 심각도 수준(알려졌거나 가정).
- 메시지 - 공격으로 식별된 이벤트의 내용.
- 규칙 콘텐츠 - 이벤트 또는 공격에 의해 트리거된 규칙의 콘텐츠.
- **CVSS** 점수 - CVSS(Common Vulnerability Scoring System)는 정보 보안 취약점의 심각도에 숫자 점수를 할당하는 체계. CVSS 점수의 범위는 0~10이며, 10이 가장 심각합니다.
- **CVE** - CVE(Common Vulnerabilities and Exposures)는 취약점을 분류하는 용어집. 공격 또는 이벤트의 유형과 관련된 CVE가 있으면 내부 라이브러리가 자동으로 여기에서 값을 생성합니다.
- 참조 - 공개적으로 사용할 수 있는 경우 이 링크는 CVE의 원래 공지 사항 및 분류로 이동합니다.

웹 보호

WAF(Web Application Firewall) 연구는 "Web Protection(웹 보호)"으로 표시됩니다. 이를 통해 웹 위협으로부터 디바이스를 보호하고 원치 않는 콘텐츠를 규제할 수 있습니다. Web Protection(웹 보호) 페이지에 다음 정보가 표시됩니다.

- **Gateway Names(**게이트웨이 이름**)** - 악성 소스를 처리한 영향을 받은 게이트웨이의 이름.
- **Profile Names(**프로파일 이름**)**- 악의적인 소스에 의해 트리거된 보안 프로파일의 이름.
- **CRS Category(CRS** 범주**)** - 일반 공격 탐지 규칙 집합당 식별된 CRS(Core Rule Set) 범주.

- **Inspection Type(**검사 유형**)** - 공격 또는 이벤트를 캡슐화한 트래픽에서 수행한 검사 멀티 클라우드 방어.
- **Attack Type(**공격 유형**)** - 네트워크를 통해 이루어지는 무단 공격의 유형입니다.
- **Platform(**플랫폼**)** - 공격 또는 이벤트에서 식별된 플랫폼 유형.
- **Lanuage(**언어**)** - 이벤트에서 탐지된 명시된 웹 개발 언어.

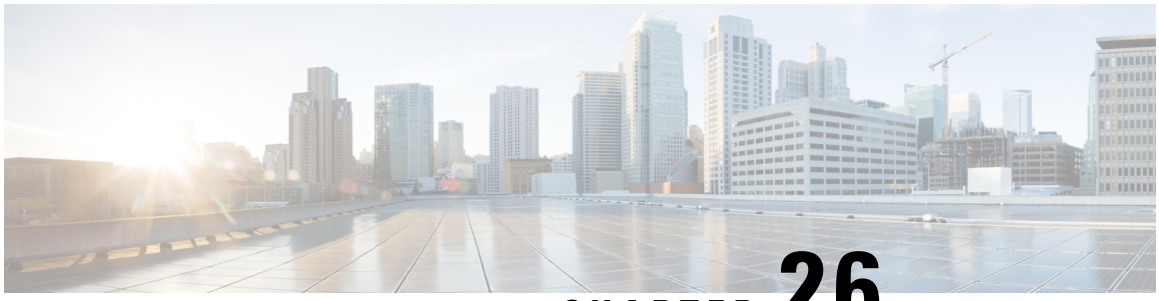
악성 소스

악성 소스는 네트워크에 피해를 주는 모든 유형의 코드 또는 패킷입니다. Malicious Sources(악성 소스) 페이지에는 다음 정보가 표시됩니다.

- **Gateway Names(**게이트웨이 이름**)** - 악성 소스를 처리한 영향을 받은 게이트웨이의 이름.
- **Profile Names(**프로파일 이름**)** - 악의적인 소스에 의해 트리거된 보안 프로파일의 이름.
- **Malicious Sources Action(**악성 소스 작업**)** - 악성 소스가 식별되었을 때 수행된 작업.
- **Impact(**영향**)** - 라이브러리 내에서 순위가 매겨진 방식에 따라 결정된 악성 자료의 영향.
- **Malicious Source IP(**악성 소스 **IP)** - 악성 소스가 시작된 IP 주소.

XI 부

클라우드 가시성 보고서



CHAPTER 26

클라우드 가시성 보고서

보고서는 네트워크 및 전반적인 상태에 대한 통찰력과 그에 따른 의사 결정에 활용할 수 있는 귀중한 통계 정보를 제공합니다. 멀티 클라우드 방어에서는 다음 유형의 보고서를 생성할 수 있습니다.

Discovery

DNS 쿼리 및 VPC 플로우 로그에서 대역 외 트래픽 정보를 가져오고 데이터를 위협 인텔리전스 및 클라우드 인벤토리 정보와 상호 연결하여 검색 보고서 생성가 생성됩니다. 이러한 로그는 클라우드 서비스 제공업체의 VPC가 S3 버킷으로 로그를 전송하도록 구성한 경우에만 사용할 수 있습니다. 이러한 로그는 멀티 클라우드 방어 컨트롤러로 직접 전송됩니다.

보고서에는 다음이 포함됩니다.

- 검색 상위 수준 보고 - 네트워크 및 클라우드 자산 분석으로, 볼륨 및 고유한 필드 값 카운트로 표시합니다. 네트워크 행동을 수량화하여 클라우드 환경에서 진행 중인 상황에 대한 인사이트를 도출할 수 있습니다.
- 네트워크 트래픽 - 바이트 - 이 그래프는 트래픽 방향별 바이트의 볼륨을 표시합니다. 바이트 볼륨이 이동하는 위치(인그레스, 이그레스 또는 이스트-웨스트)를 볼 수 있습니다.
- 네트워크 트래픽 - 패킷 - 이 그래프는 트래픽 방향별 패킷 볼륨을 표시합니다. 패킷 볼륨이 이동하는 위치(인그레스, 이그레스 또는 이스트-웨스트)를 볼 수 있습니다.
- 네트워크 트래픽 - 이벤트 - 이 그래프는 트래픽 방향별 이벤트 볼륨을 표시합니다. 이벤트 볼륨이 전송되는 위치(인그레스, 이그레스 또는 이스트-웨스트)를 확인할 수 있습니다.
- 인그레스 어카운트 요약 - 이 요약에는 인그레스 네트워크 트래픽이 있는 클라우드 자산의 고유한 수가 CSP별로 표시됩니다. CSP 환경으로 통신하는 자산의 흐름을 검토할 수 있습니다.
- 이그레스 어카운트 요약 - 이 요약은 이그레스 네트워크 트래픽이 있는 클라우드 자산의 고유한 수를 CSP(Cloud Service Provider, 클라우드 서비스 제공자)별로 표시합니다. CSP 환경에서 통신하는 자산의 흐름을 검토할 수 있습니다.
- 국가별 인그레스 네트워크 이벤트 - 이 지리 히트맵은 국가별 인그레스 트래픽의 양을 보여줍니다. 클라우드 환경과 통신하는 국가를 볼 수 있습니다.
- 국가별 이그레스 네트워크 이벤트 - 이 지리 히트맵은 국가별 이그레스 트래픽의 양을 보여줍니다. 클라우드 환경과 통신하는 국가를 볼 수 있습니다.

- 상위 **10**개 소스 국가 - 이 그래프는 기타 네트워크 분석과 함께 이벤트 규모 기준 상위 10개 소스 국가를 표시합니다. 클라우드 환경과 가장 많이 통신하는 소스 국가를 요약한 것입니다.
- 상위 **10**개 대상 국가 - 이 그래프는 기타 네트워크 분석과 함께 이벤트 양 기준 상위 10개 대상 국가를 표시합니다. 클라우드 환경과 통신하는 주요 대상 국가에 대한 요약입니다.
- 상위 **10**개 인그레스 소스 **IP** 주소 - 이 그래프는 기타 네트워크 분석과 함께 볼륨 기준 상위 10개 소스 IP 주소를 표시합니다. 가장 많은 인바운드 이벤트를 생성하는 엔터티를 볼 수 있습니다.
- 상위 **10**개 이그레스 대상 **IP** 주소 - 이 그래프는 기타 네트워크 분석과 함께 볼륨별 상위 10개 대상 IP 주소를 표시합니다. 클라우드 환경이 주로 통신하는 엔터티를 볼 수 있습니다.
- 볼륨별 상위 **10**개 **FQDN** 범주 이름 - 이 그래프는 FQDN에 대한 범주 이름을 볼륨별로 표시합니다. 클라우드 환경에서 요청하는 FQDN을 기준으로 상위 범주 유형을 볼 수 있습니다.
- 볼륨별 상위 **10**개 **FQDN** - 이 그래프는 볼륨별 상위 10개 FQDN을 표시합니다. 클라우드 환경에서 요청한 상위 FQDN을 볼 수 있습니다.
- 볼륨별 상위 **10**개의 악성 **FQDN** - 이 그래프는 볼륨별 상위 10개의 악성 FQDN을 표시합니다. 악의적인 또는 의심스러운 범주 이름이 발견되면 해당 범주 이름의 상위 FQDN이 여기에 표시됩니다.
- **MITRE ATT&CK**에 매핑된 **FQDN** 범주 이름 - MITRE ATT+CK에 매핑된 상위 10개의 악성 범주 이름을 표시합니다. 이 보기에서는 엔터프라이즈 MITRE ATT+CK 프레임워크를 사용하여 FQDN 범주 이름이 공격 체인과 어떤 관련이 있는지에 대한 추가 상황을 제공합니다.

위협 지표 스냅샷

위협 및 클라우드 분석 보고서 생성 보고서는 게이트웨이 인스턴스에 대한 데이터를 편집한 것입니다. 이 보고서를 이용하여 트래픽 패턴, 임계값 충족 시기와 방법, 공격 추세 및 특정 인스턴스를 검토하여 게이트웨이의 위협 상황을 파악할 수 있습니다. 보고서에는 다음 사항이 포함되어 있습니다.

- **IDS/IPS** 탐지 - 이 데이터는 선택한 시간 범위 동안 탐지된 공격의 수, 공격 유형, 탐지된 공격 시간, 그리고 상위 10개의 IDS/IPS 서명을 보여줍니다.
- **WAF** 탐지 - 이 데이터는 WAF 규칙에 의해 탐지된 공격의 수, 탐지된 공격 시간, 선택한 시간 범위 동안의 상위 10개 WAF 서명입니다.
- 볼륨별 위협 재배치 - 이 단계 구분도는 WAF 및 IDS/IPS 이벤트 모두에 대한 공격의 볼륨을 볼륨 기준으로 국가별로 표시합니다.
- 볼륨 및 시간별 상위 **10**개 공격 국가 - 이 가로 막대 차트는 전체 기간 동안 가장 많은 이벤트를 생성한 상위 10개 국가의 볼륨을 표시한 다음, 해당 볼륨을 해당 기간 동안 이벤트가 발생한 시간 단위로 세분화하여 표시합니다.
- 정책 및 방지 - 이 데이터 차트는 게이트웨이가 구축된 CSP 환경에서 게이트웨이 보안 유형이 수행하는 작업을 보여줍니다. 여기에는 작업 유형, 작업에서 생성되는 이벤트 수, 게이트웨이 보안 유형 등이 포함됩니다.

멀티 클라우드 방어 게이트웨이에서 데이터를 수집하고 폴링하려면 정책에서 웹 애플리케이션 방화벽(WAF), 침입 탐지 및 방지(IDS/IPS) 규칙이 활성화되어 있어야 합니다.

추가 정보:

- 검색 보고서 생성, on page 217
- 위협 및 클라우드 분석 보고서 생성, 217 페이지

검색 보고서 생성

멀티 클라우드 방어 컨트롤러에서 처리하기 전에 S3 버킷으로 전송된 DNS 쿼리 및 VPC 플로우 로그를 가져와서 검색 보고서를 생성합니다.

단계 **1** 멀티 클라우드 방어 컨트롤러 페이지에서 **Report(**보고서**)**로 이동합니다.

단계 **2** **Discovery(**검색**)**를 선택합니다.

단계 **3** Threat & Cloud Analytics Report(위협 및 클라우드 분석 보고서)에서 가져오는 데이터의 드롭다운 목록에서 일별, 주별, 월별, 분기별 또는 연간 **Frequency(**빈도**)**를 선택합니다.

- **Daily(**매일**)** - 오전 12시부터 24시간 동안. 이는 UTC 시간입니다.
- **Weekly(**매주**)** - 월요일부터 일요일까지
- **Monthly(**매월**)** - 일반적으로 월의 시작부터 말일까지
- **Quarterly(**분기별**)** - 분기의 시작부터 끝까지. 일반적으로 분기는 1월 1일~3월 31일, 4월 1일~6월 30일, 7월 1일~9월 30일 및 10월 1일~12월 31일로 정의됩니다.
- **Yearly(**매년**)** - 선택한 연도의 1월 1일부터 12월 31일까지.

단계 **4** 날짜를 선택합니다. **Calendar(**달력**)** 드롭다운을 사용하여 데이터를 수집할 시간 범위 또는 특정 날짜를 선택합니다. 회색으로 표시된 날짜는 컴파일할 데이터가 없는 것입니다. 보고서를 생성하는 데 사용할 수 있는 데이터가 없는 경우 정책에 WAF 및 IDS/IP 규칙이 포함되어 있는지 확인합니다.

단계 **5** **Generate Report(**보고서 생성**)**를 클릭합니다. 검색 보고서가 새 탭에서 생성됩니다.

단계 **6** 보고서를 로컬로 저장하려면 **Print Report(**보고서 인쇄**)**를 클릭합니다. 로컬 서버의 위치로 이동하여 보고서를 저장합니다.

위협 및 클라우드 분석 보고서 생성

위협 및 클라우드 분석 보고서는 멀티 클라우드 방어 게이트웨이에서 수집하고 검사한 트래픽을 사용하여 생성되는 위협 지표 스냅샷입니다. 이 기능은 멀티 클라우드 방어이(가) 현재 데이터 경로에 있는 것처럼 더욱 포괄적인 보고서를 제공하며 검색 보고서를 보완합니다.

마감일, 월말, 분기 말 또는 연말까지는 이벤트의 질적 요약을 수행할 수 없으므로 당일의 보고서는 생성할 수 없습니다.

참고 멀티 클라우드 방어 게이트웨이에서 데이터를 수집하고 폴링하려면 정책에서 WAF(Web Application Firewall), 침입 탐지 및 보호(IDS/IPS) 규칙을 활성화해야 합니다. 자세한 내용은 각각 다음 링크를 참조하십시오.

- 웹 애플리케이션 방화벽(WAF) 프로파일
- 네트워크 침입(IDS/IPS) 프로파일, 148 페이지

위협 지표 스냅샷을 포함하여 위협 및 클라우드 분석을 생성하려면 다음 절차를 사용하십시오.

단계 **1** 멀티 클라우드 방어 컨트롤러 페이지에서 **Report(**보고서**)**로 이동합니다.

단계 **2** **Threat Indicators Snapshot(**위협 지표 스냅샷**)**을 선택합니다.

단계 **3** Threat & Cloud Analytics Report(위협 및 클라우드 분석 보고서)에서 가져오는 데이터의 드롭다운 목록에서 일별, 주별, 월별, 분기별 또는 연간 **Frequency(**빈도**)**를 선택합니다.

- **Daily(**매일**)** - 오전 12시부터 24시간 동안. 이는 UTC 시간입니다.
- **Weekly(**매주**)** - 월요일부터 일요일까지
- **Monthly(**매월**)** - 일반적으로 월의 시작부터 말일까지
- **Quarterly(**분기별**)** - 분기의 시작부터 끝까지. 일반적으로 분기는 1월 1일~3월 31일, 4월 1일~6월 30일, 7월 1일~9월 30일 및 10월 1일~12월 31일로 정의됩니다.
- **Yearly(**매년**)** - 선택한 연도의 1월 1일부터 12월 31일까지.

단계 **4** 날짜를 선택합니다. **Calendar(**달력**)** 드롭다운을 사용하여 데이터를 수집할 시간 범위 또는 특정 날짜를 선택합니다. 회색으로 표시된 날짜는 컴파일할 데이터가 없는 것입니다. 보고서를 생성하는 데 사용할 수 있는 데이터가 없는 경우 정책에 WAF 및 IDS/IP 규칙이 포함되어 있는지 확인합니다.

단계 **5** **Generate Report(**보고서 생성**)**를 클릭합니다.

단계 **6** 보고서가 생성됩니다. 보고서를 로컬로 저장하려면 **Print Report(**보고서 인쇄**)**를 클릭합니다. 로컬 서버의 위치로 이동하여 보고서를 저장합니다.

XII 부

알림, 로그 전달 및 보고서

27 장

알림 개요

알림 서비스 개요

멀티 클라우드 방어는 널리 구축된 알림 서비스와 통합하기 위해 Microsoft Sentinel, PagerDuty, ServiceNow 및 Slack과 통합하여 중요한 시스템 레벨 알림을 전달합니다. 이렇게 하면 클라우드 운영 팀은 멀티 클라우드 방어 클라우드 컨트롤러가 탐지한 사용자 정의 시스템 이벤트 및 심각도 수준에 대해 알림을 받고 이에 대응할 수 있습니다. 이는 지정된 통합에 대해 알림 규칙과 함께 알림 서비스 프로파일을 사용하여 멀티 클라우드 방어 컨트롤러 내에서 수행됩니다.

지원되는 알림 서비스와의 통합을 구성하려면 **Administration(**관리**)** > **Alert Profiles(**알림 프로파일**)** > **Services(**서비스**)**로 이동합니다.

이러한 서비스와 통합하려면 API URL, API 키 또는 둘 모두가 필요합니다. 일반적으로 API 키 및 URL은 조직의 이러한 서비스 관리자가 생성해야 합니다.

Note ServiceNow 통합의 경우에는 ServiceNow가 멀티 클라우드 방어 컨트롤러에서 알림을 수신하고 표시할 수 있도록 Webhook을 구성해야 합니다.

28 장

알림 대상/SIEM

Datadog

설정이 완료되면 정의된 알림 서비스 프로파일 및 알림 규칙을 사용하여 멀티 클라우드 방어 알림이 DataDog로 전송됩니다.

알림 프로파일 서비스 생성

Before you begin

DataDog에 알림을 전송하려면 다음 정보가 필요합니다.

- DataDog 계정
- API 키

Tip

- Datadog 계정에 등록하려면 Datadog 계정(https://www.datadoghq.com/)을 참조하십시오.
- Datadog API 키를 생성하려면 Datadog API 키(https://app.datadoghq.com/account/login?next=%2Faccount%2Fsettings#api)를 참조하십시오.

단계 **1** **Administration**(관리) > **Alert Profiles**(알림 프로파일) > **Services**(서비스)로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.
단계 **3** **Name(**이름**)** - 알림 통합의 고유한 이름을 입력합니다. 예: `멀티 클라우드 방어-Datadog-profile`.
단계 **4** **Description(**설명**)**(선택 사항) - 알림 통합에 대한 설명을 입력합니다.
단계 **5** **Type(**유형**)** - 풀다운을 사용하여 **Datadog**를 선택합니다.
단계 **6** **API Key(API** 키**)** - 통신 인증에 사용되는 DataDog API 키를 지정합니다.
단계 **7** **Save(**저장**)**를 클릭합니다.

What to do next

이 새 프로파일로 알림 규칙을 생성합니다.

알림 규칙 생성

Before you begin

DataDog에 알림을 전송하려면 다음 정보가 필요합니다.

- DataDog 계정
- API 키

Tip

- Datadog 계정에 등록하려면 Datadog 계정(https://www.datadoghq.com/)을 참조하십시오.
- Datadog API 키를 생성하려면 Datadog API 키(https://app.datadoghq.com/account/login?next=%2Faccount%2Fsettings#api)를 참조하십시오.

단계 **1** **Settings(**설정**)** > **Alert Profiles(**알림 프로파일**)** > **Alert Rules(**알림 규칙**)**으로 이동합니다.
단계 **2** **Create(**생성**)**를 클릭합니다.
단계 **3** **Profile Name(**프로파일 이름**)** - 통합의 고유한 이름을 입력합니다. 예: `멀티 클라우드 방어-DataDog-alert-rule`.
단계 **4** **Description(**설명**)**(선택 사항) - 알림 규칙에 대한 설명을 입력합니다.
단계 **5** **Alert Profile(**알림 프로파일**)** - 풀다운을 사용하여 PagerDuty 알림 프로파일을 선택합니다. 예를 들어 `멀티 클라우드 방어-DataDog-profile`에서 생성된 프로파일을 선택합니다.
단계 **6** **Type(**유형**)** - 풀다운을 사용하여 **System Logs(**시스템 로그**)** 또는 **Discovery(**검색**)**를 선택합니다.
단계 **7** **Sub Type(**하위 유형**)** - **System Logs(**시스템 로그**)**의 경우 하위 유형 풀다운 옵션은 **Gateway(**게이트웨이**)** 또는 **Account(**계정**)** 중 하나입니다. **Discovery(**검색**)**의 경우 하위 유형 풀다운 옵션은 **Insights Rule(**인사이트 규칙**)**입니다.
단계 **8** **Severity(**심각도**)** - 선택한 유형 **System Logs(**시스템 로그**)**에 대해 풀다운을 사용하여 `Info Warning Medium High(정보 경고 중간 높음)` 또는 `Critical(위험)` 옵션에서 심각도 레벨을 선택합니다. 유형 **Discovery(**검색**)**의 경우, `Info Medium Critical(정보 중간 위험)` 옵션에서 Severity(심각도) 레벨을 선택합니다.

단계 **9** **Enabled(**활성화됨**)** - 확인란을 사용하여 이 알림 프로파일을 활성화합니다.

단계 **10** **Save(**저장**)**를 클릭합니다.

Microsoft Sentinel

구성한 멀티 클라우드 방어 알림은 정의된 알림 서비스 프로파일 및 알림 규칙을 사용하여 Microsoft Sentinel로 전송됩니다.

알림 프로파일 서비스 생성

Before you begin

Microsoft Sentinel에 알림을 전송하려면 다음 정보가 필요합니다.

- Azure 로그 분석 작업 영역을 생성합니다.
- Azure 로그 테이블을 정의합니다.

단계 **1** **Administration(**관리**)** > **Alert Profiles(**알림 프로파일**)** > **Services(**서비스**)**로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** **Name(**이름**)** - 알림 통합의 고유한 이름을 입력합니다. 예: `mcd-mssentinel-profile`.

단계 **4** **Description(**설명**)**(선택 사항) - 알림 통합에 대한 설명을 입력합니다.

단계 **5** **Type(**유형**)** - 풀다운을 사용하여 **Microsoft Sentinel**을 선택합니다.

단계 **6** **API Key(API** 키**)** - Azure 로그 분석 작업 공간에 대해 Azure에서 생성된 공유 키를 지정합니다.

단계 **7** **Azure Log Table Name(Azure** 로그 테이블 이름**)** - Azure 로그 분석 작업 공간을 생성할 때 정의된 Azure 로그의 이름을 지정합니다.

단계 **8** **Azure Log Analytics Workspace ID(Azure** 로그 분석 작업 공간 **ID)** - Azure 로그 분석 작업 공간의 ID를 지정합니다.

단계 **9** **Save(**저장**)**를 클릭합니다.

What to do next

이 새 프로파일로 알림 규칙을 생성합니다.

알림 규칙 생성

Before you begin

Microsoft Sentinel에 알림을 전송하려면 다음 정보가 필요합니다.

- Azure 로그 분석 작업 영역을 생성합니다.

• Azure 로그 테이블을 정의합니다.

단계 1 **Administration(**관리**)** > **Alert Profiles(**알림 프로파일**)** > **Alert(**알림**)**로 이동합니다.

단계 2 **Create(**생성**)**를 클릭합니다.

단계 3 **Profile Name(**프로파일 이름**)** - 통합의 고유한 이름을 입력합니다. 예: `mcd-mssentinel-alert-rule`.

단계 4 **Description(**설명**)**(선택 사항) - 알림 규칙에 대한 설명을 입력합니다.

단계 5 **Alert Profile(**프로파일 알림**)** - 풀다운을 사용하여 이전에 생성한 적절한 프로파일을 선택합니다. 예를 들어 위에서 생성한 프로파일을 선택합니다`mcd-mssentinel-profile`.

단계 6 **Type(**유형**)** - 풀다운을 사용하여 **System Logs(**시스템 로그**)** 또는 **Discovery(**검색**)**를 선택합니다.

단계 7 **Sub Type(**하위 유형**)** - **System Logs(**시스템 로그**)**의 경우 하위 유형 풀다운 옵션은 **Gateway(**게이트웨이**)** 또는 **Account(**계정**)** 중 하나입니다. **Discovery(**검색**)**의 경우 하위 유형 풀다운 옵션은 **Insights Rule(**인사이트 규칙**)**입니다.

단계 8 **Severity(**심각도**)** - 선택한 유형 **System Logs(**시스템 로그**)**에 대해 풀다운을 사용하여 `Info Warning Medium High(정보 경고 중간 높음)` 또는 `Critical(위험)` 옵션에서 심각도 레벨을 선택합니다. 유형 **Discovery(**검색**)**의 경우, `Info Medium Critical(정보 중간 위험)` 옵션에서 Severity(심각도) 레벨을 선택합니다.

단계 9 **Enabled(**활성화됨**)** - 확인란을 사용하여 이 알림 프로파일을 활성화합니다.

단계 10 **Save(**저장**)**를 클릭합니다.

PagerDuty

구성이 완료되면 멀티 클라우드 방어 알림이 정의된 알림 서비스 프로파일 및 알림 규칙을 사용하여 PagerDuty API 게이트웨이로 전송됩니다.

알림 프로파일 서비스 생성

Before you begin

이 가이드의 단계를 완료하려면 다음이 필요합니다.

• API 키가 구성된 PagerDuty 계정.

Tip

• PagerDuty 계정에 등록합니다(https://www.servicenow.com/my-account/sign-up.html 참조).

• API 키(https://developer.pagerduty.com/api-reference)를 설정합니다.

단계 1 **Administration(**관리**)** > **Alert Profiles(**알림 프로파일**)** > **Services(**서비스**)**로 이동합니다.

단계 2 **Create(**생성**)**를 클릭합니다.

단계 **3** **Name(**이름**)** - 알림 통합의 고유한 이름을 입력합니다. 예: `mcd-pagerduty-profile`.
단계 **4** **Description(**설명**)**(선택 사항) - 알림 통합에 대한 설명을 입력합니다.
단계 **5** **Type(**유형**)** - 풀다운을 사용하여 **PagerDuty**를 선택합니다.
단계 **6** **API Key(API** 키**)** - 위에서 생성한 PagerDuty API 키 또는 원하는 다른 PagerDuty API 키를 복사합니다.
단계 **7** **Save(**저장**)**를 클릭합니다.

What to do next

이 새 프로파일로 알림 규칙을 생성합니다.

알림 규칙 생성

Before you begin

이 가이드의 단계를 완료하려면 다음이 필요합니다.

API 키가 구성된 PagerDuty 계정.

Tip

- PagerDuty 계정에 등록합니다(https://www.servicenow.com/my-account/sign-up.html 참조).
- API 키(https://developer.pagerduty.com/api-reference)를 설정합니다.

단계 **1** **Administration(**관리**)** > **Alert Profiles(**알림 프로파일**)** > **Services(**서비스**)**로 이동합니다.
단계 **2** **Create(**생성**)**를 클릭합니다.
단계 **3** **Profile Name(**프로파일 이름**)** - 통합의 고유한 이름을 입력합니다. 예: `mcd-pagerduty-alert-rule`.
단계 **4** **Description(**설명**)**(선택 사항) - 알림 규칙에 대한 설명을 입력합니다.
단계 **5** **Alert Profile(**알림 프로파일**)** - 풀다운을 사용하여 PagerDuty 알림 프로파일을 선택합니다. 예를 들어 위에서 생성한 프로파일을 선택합니다`mcd-pagerduty-profile`.
단계 **6** **Type(**유형**)** - 풀다운을 사용하여 **System Logs(**시스템 로그**)** 또는 **Discovery(**검색**)**를 선택합니다.
단계 **7** **Sub Type(**하위 유형**)** - **System Logs(**시스템 로그**)**의 경우 하위 유형 풀다운 옵션은 **Gateway(**게이트웨이**)** 또는 **Account(**계정**)** 중 하나입니다. **Discovery(**검색**)**의 경우 하위 유형 풀다운 옵션은 **Insights Rule(**인사이트 규칙**)**입니다.
단계 **8** **Severity(**심각도**)** - 선택한 유형 **System Logs(**시스템 로그**)**에 대해 풀다운을 사용하여 `Info Warning Medium High or Critical(정보 경고 중간 높음 또는 위험)` 옵션에서 심각도 레벨을 선택합니다. 유형 **Discovery(**검색**)**의 경우, `Info Medium Critical(정보 중간 위험)` 옵션에서 Severity(심각도) 레벨을 선택합니다.
단계 **9** **Enabled(**활성화됨**)** - 확인란을 사용하여 이 알림 프로파일을 활성화합니다.
단계 **10** **Save(**저장**)**를 클릭합니다.

ServiceNow

구성한 멀티 클라우드 방어 알림은 정의된 알림 서비스 프로파일 및 알림 규칙을 사용하여 ServiceNow API 게이트웨이로 전송됩니다.

알림 프로파일 서비스 생성

Before you begin

이 가이드의 단계를 완료하려면 다음이 필요합니다.

- 수신 Webhook URL이 있는 ServiceNow 계정.
- API 키가 구성되었습니다.

Tip

- ServiceNow 계정(https://www.servicenow.com/my-account/sign-up.html)에 등록
- Webhook 및 API 키(https://docs.servicenow.com/search?q=setup%20webhook) 설정

단계 **1** **Administration(**관리**)** > **Alert Profiles(**알림 프로파일**)** > **Services(**서비스**)**로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** **Name(**이름**)** - 알림 통합의 고유한 이름을 입력합니다. 예: `mcd-servicenow-profile`.

단계 **4** **Description(**설명**)**(선택 사항) - 알림 통합에 대한 설명을 입력합니다.

단계 **5** **Type(**유형**)** - 풀다운을 사용하여 **ServiceNow**를 선택합니다.

단계 **6** **API Key(API** 키**)** - 위에서 생성한 ServiceNow API 키 또는 다른 ServiceNow API 키를 지정합니다.

단계 **7** **API URL** - 위에서 생성한 ServiceNow Webhook URL 또는 원하는 경우 다른 ServiceNow Webhook URL을 지정합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

What to do next

이 새 프로파일로 알림 규칙을 생성합니다.

알림 규칙 생성

Before you begin

이 가이드의 단계를 완료하려면 다음이 필요합니다.

- 수신 Webhook URL이 있는 ServiceNow 계정.

- 구성된 API 키.

Tip

- ServiceNow 계정(https://www.servicenow.com/my-account/sign-up.html)에 등록
- Webhook 및 API 키(https://docs.servicenow.com/search?q=setup%20webhook) 설정

단계 **1** **Administration(**관리**)** > **Alert Profiles(**알림 프로파일**)** > **Services(**서비스**)**로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** **Profile Name(**프로파일 이름**)** - 통합의 고유한 이름을 입력합니다. 예: `mcd-servicenow-alert-rule`.

단계 **4** **Description(**설명**)**(선택 사항) - 알림 규칙에 대한 설명을 입력합니다.

단계 **5** **Alert Profile(**알림 프로파일**)** - 풀다운을 사용하여 ServiceNow 알림 프로파일을 선택합니다. 예를 들어 위에서 생성한 프로파일을 선택합니다`mcd-servicenow-profile`.

단계 **6** **Type(**유형**)** - 풀다운을 사용하여 **System Logs(**시스템 로그**)** 또는 **Discovery(**검색**)**를 선택합니다.

단계 **7** **Sub Type(**하위 유형**)**을 선택합니다.

- **System Logs(**시스템 로그**)** 유형의 경우 옵션은 **Gateway(**게이트웨이**)** 또는 **Account(**계정**)** 중 하나입니다.
- **Discovery(**검색**)** 유형의 경우 유일한 옵션은 **Insights Rule(**인사이트 규칙**)**입니다.

단계 **8** **Severity(**심각도**)**를 선택합니다.

- 선택한 유형 **System Logs(**시스템 로그**)**에 대해 풀다운을 사용하여 **Info Warning Medium High or Critical(**정보 경고 중간 높음 또는 위험**)** 옵션에서 심각도 레벨을 선택합니다.
- 유형 **Discovery(**검색**)**의 경우 **Info Medium Critical(**정보 미디어 중요**)**을 선택합니다.

단계 **9** **Enabled(**활성화됨**)** - 확인란을 사용하여 이 알림 프로파일을 활성화합니다.

단계 **10** **Save(**저장**)**를 클릭합니다.

Slack

구성되면 정의된 알림 서비스 프로파일 및 규칙을 사용하여 멀티 클라우드 방어 알림이 Slack 수신 Webhook URL로 전송됩니다.

알림 프로파일 서비스 생성

Before you begin

이 가이드의 단계를 완료하려면 다음이 필요합니다.

- 수신 Webhook URL이 구성된 Slack 계정.

Tip

1. Slack 계정(https://slack.com/get-started#/create)을 생성합니다.
2. 수신 Webhook(https://slack.com/help/articles/115005265063-Incoming-webhooks-for-Slack#set-up-incoming-webhooks)을 생성합니다.

단계 **1** **Administration(**관리**)** > **Alert Profiles(**알림 프로파일**)** > **Services(**서비스**)**로 이동합니다.
단계 **2** **Create(**생성**)**를 클릭합니다.
단계 **3** **Name(**이름**)** - 알림 통합의 고유한 이름을 입력합니다. 예: `mcd-slack-profile`.
단계 **4** **Description(**설명**)**(선택 사항) - 알림 통합에 대한 설명을 입력합니다.
단계 **5** **Type(**유형**)** - 풀다운을 사용하여 **Slack**을 선택합니다.
단계 **6** **API URL** - 위에서 생성한 Slack Webhook URL 또는 원하는 경우 다른 Slack Webhook URL을 지정합니다.

What to do next

이 새 프로파일로 알림 규칙을 생성합니다.

알림 규칙 생성

Before you begin

이 가이드의 단계를 완료하려면 다음이 필요합니다.

수신 Webhook URL이 구성된 Slack 계정.

Tip

1. Slack 계정(https://slack.com/get-started#/create)을 생성합니다.
2. 수신 Webhook(https://slack.com/help/articles/115005265063-Incoming-webhooks-for-Slack#set-up-incoming-webhooks)을 생성합니다.

단계 **1** **Administration(**관리**)** > **Alert Profiles(**알림 프로파일**)** > **Services(**서비스**)**로 이동합니다.
단계 **2** **Create(**생성**)**를 클릭합니다.
단계 **3** **Profile Name(**프로파일 이름**)** - 통합의 고유한 이름을 입력합니다. 예: `mcd-slack-alert-rule`.
단계 **4** **Description(**설명**)**(선택 사항) - 알림 규칙에 대한 설명을 입력합니다.
단계 **5** **Alert Profile(**알림 프로파일**)** - 풀다운을 사용하여 Slack 알림 프로파일을 선택합니다. 예를 들어 위에서 생성한 프로파일을 선택합니다`mcd-slack-profile`.

단계 **6** **Type(**유형**)** - 풀다운을 사용하여 **System Logs(**시스템 로그**)** 또는 **Discovery(**검색**)**를 선택합니다.

단계 **7** **Sub Type(**하위 유형**)** - **System Logs(**시스템 로그**)**의 경우 하위 유형 풀다운 옵션은 **Gateway(**게이트웨이**)** 또는 **Account(**계정**)** 중 하나입니다. **Discovery(**검색**)**의 경우 하위 유형 풀다운 옵션은 **Insights Rule(**인사이트 규칙**)**입니다.

단계 **8** **Severity(**심각도**)** - 선택한 유형 **System Logs(**시스템 로그**)**에 대해 풀다운을 사용하여 `Info Warning Medium High or Critical(정보 경고 중간 높음 또는 위험)` 옵션에서 심각도 레벨을 선택합니다. 유형 **Discovery(**검색**)**의 경우, `Info Medium Critical(정보 중간 위험)` 옵션에서 Severity(심각도) 레벨을 선택합니다.

단계 **9** **Enabled(**활성화됨**)** - 확인란을 사용하여 이 알림 프로파일을 활성화합니다.

단계 **10** **Save(**저장**)**를 클릭합니다.

Webex

구성이 완료되면 멀티 클라우드 방어 알림이 정의된 알림 서비스 프로파일 및 알림 규칙을 사용하여 Webex API 게이트웨이로 전송됩니다.

알림 프로파일 서비스 생성

다음 절차에 따라 Webex 서비스용 알림 프로파일을 생성합니다.

시작하기 전에

이 가이드의 단계를 완료하려면 다음이 필요합니다.

- 수신 Webhook URL이 있는 Webex 계정.
- API 키가 구성되었습니다.

참고

1. Webex 계정을 생성하거나 액세스합니다.
2. Webex 수신 Webhook을 생성합니다.
3. 수신 Webhook 권한을 수락합니다.
4. 이름을 제공하고 Webex Space를 선택합니다.
5. 알림 서비스 프로파일의 설정에 사용할 Webex Webhook URL을 복사합니다.

단계 **1** **Administration(**관리**)** > **Alert Profiles(**알림 프로파일**)** > **Services(**서비스**)**로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** **Name(**이름**)** - 알림 통합의 고유한 이름을 입력합니다.

단계 **4** (선택 사항) **Description(**설명**)** - 알림 통합에 대한 설명을 입력합니다.

단계 **5** **Type(**유형**)** - 풀다운을 사용하여 **Webex**를 선택합니다.

단계 **6** **API URL** - 사전 요구 사항의 일부로 생성된 Webex Webhook URL 또는 원하는 경우 다른 Webhook URL을 지정합니다.

다음에 수행할 작업

이 새 프로파일로 알림 규칙을 생성합니다.

알림 규칙 생성

단계 **1** **Administration(**관리**)** > **Alert Profiles(**알림 프로파일**)** > **Services(**서비스**)**로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** **Profile Name(**프로파일 이름**)** - 통합의 고유한 이름을 입력합니다. `mcd-servicenow-alert-rule`을(를) 예로 들 수 있습니다.

단계 **4** (선택 사항) **Description(**설명**)** - 알림 규칙에 대한 설명을 입력합니다.

단계 **5** **Alert Profile(**알림 프로파일**)** - 풀다운을 사용하여 **Webex** 알림 프로파일을 선택합니다. 예를 들어 위의 mcd-servicenow-profile에서 생성한 프로파일을 선택합니다.

단계 **6** **Type(**유형**)** - 풀다운을 사용하여 **System Logs(**시스템 로그**)** 또는 **Discovery(**검색**)**를 선택합니다.

단계 **7** **Sub Type(**하위 유형**)**을 선택합니다.

- System Logs(시스템 로그) 유형의 경우 옵션은 **Gateway(**게이트웨이**)** 또는 **Account(**계정**)** 중 하나입니다.
- Discovery(검색) 유형의 경우 유일한 옵션은 **Insights Rule(**인사이트 규칙**)**입니다.

단계 **8** **Severity(**심각도**)**를 선택합니다.

- 선택한 유형 System Logs(시스템 로그)에 대해 풀다운을 사용하여 **Info Warning Medium High(**정보 경고 중간 높음**)** 또는 **Critical(**위험**)**을 선택합니다.
- 유형 Discovery(검색)의 경우 **Info Medium Critical(**정보 미디어 중요**)**을 선택합니다.

단계 **9** **Enabled(**활성화됨**)** - 확인란을 사용하여 이 알림 프로파일을 활성화합니다.

단계 **10** **Save(**저장**)**를 클릭합니다.

Splunk

구성이 완료되면 멀티 클라우드 방어 알림이 정의된 알림 서비스 프로파일 및 알림 규칙을 사용하여 API 게이트웨이로 전송됩니다.

Splunk 프로파일 서비스 생성

다음 절차에 따라 Splunk 서비스용 알림 프로파일을 생성합니다.

시작하기 전에

다음 항목이 구성되어 있고 준비되어 있어야 합니다.

- 멀티 클라우드 방어 에서 API 키를 생성하고 키와 암호를 모두 저장합니다. 자세한 내용은 멀티 클라우드 방어에서 API 키 생성, 261 페이지를 참조하십시오.
- Splunk Web에서 HEC(HTTP Event Collector, HTTP 이벤트 컬렉터)를 설정합니다. 자세한 내용 은 Splunk Cloud에서 HTTP 이벤트 컬렉터 설정 를 참조하십시오.
- Splunk HEC에는 다음 항목이 설정되어 있어야 합니다.
  - HEC는 활성화되어야 합니다.
  - 사용 가능한 활성 HEC 토큰이 하나 이상 있어야 합니다.
  - HEC를 인증하려면 액티브 토큰을 사용해야 합니다.
  - HEC로 이동하는 데이터의 형식을 지정해야 합니다. HTTP 이벤트 컬렉터의 이벤트 형식 지정을 참조하십시오.

단계 **1** **Administration(**관리**)** > **Alert Profiles(**알림 프로파일**)** > **Services(**서비스**)**로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** **Name(**이름**)** - 알림 통합의 고유한 이름을 입력합니다.

단계 **4** **Description(**설명**)**(선택 사항) - 알림 통합에 대한 설명을 입력합니다.

단계 **5** **Type(**유형**)** - 풀다운을 사용하여 **Splunk**를 선택합니다.

단계 **6** **API Key(API** 키**)** - 위에서 생성한 Splunk API 키 또는 원하는 다른 PagerDuty API 키를 복사합니다.

단계 **7** 서버에 도메인과 일치하는 SAN 필드가 있는 인증서가 없는 경우 **Skip Certificate(**인증서 확인 건너뛰기**)** 상자를 선택합니다. 서버에 SAN 필드가 도메인과 일치하는 인증서가 있는 경우 선택하지 않은 상태로 둡니다.

단계 **8** **Index(**색인**)(**기본값 - 메인**)** 은 처리된 모든 데이터가 저장되는 Splunk의 기본 인덱스입니다. 이는 Splunk HEC를 구성할 때 제공됩니다.

단계 **9** Splunk HTTP 이벤트 컬렉터에 대한 **API URL** 을 입력합니다. 이 URL을 사용하는 것이 좋습니다.

```
https://<host>:<port>/services/collector .
```

단계 **10** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

이 새 프로파일로 알림 규칙을 생성합니다.

Splunk 규칙 생성

다음 절차에 따라 splunk 알림 서비스가 포함된 규칙을 생성합니다.

단계 **1** **Administration(**관리**)** > **Alert Profiles(**알림 프로파일**)** > **Alert(**알림**)**로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** **Profile Name(**프로파일 이름**)** - 통합의 고유한 이름을 입력합니다. 예: `mcd-mssentinel-alert-rule`.

단계 **4** **Description(**설명**)**(선택 사항) - 알림 규칙에 대한 설명을 입력합니다.

단계 **5** **Alert Profile(**프로파일 알림**)** - 풀다운을 사용하여 이전에 생성한 적절한 프로파일을 선택합니다. 예를 들어 위의 `mcd-splunk-rule`에서 생성한 프로파일을 선택합니다.

단계 **6** **Type(**유형**)** - 풀다운을 사용하여 **System Logs(**시스템 로그**)** 또는 **Discovery(**검색**)**를 선택합니다.

단계 **7** **Sub Type(**하위 유형**)** - **System Logs(**시스템 로그**)**의 경우 하위 유형 풀다운 옵션은 **Gateway(**게이트웨이**)** 또는 **Account(**계정**)** 중 하나입니다. **Discovery(**검색**)**의 경우 하위 유형 풀다운 옵션은 **Insights Rule(**인사이트 규칙**)**입니다.

단계 **8** **Severity(**심각도**)** - 선택한 유형 **System Logs(**시스템 로그**)**에 대해 풀다운을 사용하여 `Info Warning Medium High(정보 경고 중간 높음)` 또는 `Critical(위험)` 옵션에서 심각도 레벨을 선택합니다. 유형 **Discovery(**검색**)**의 경우, `Info Medium Critical(정보 중간 위험)` 옵션에서 Severity(심각도) 레벨을 선택합니다.

단계 **9** **Enabled(**활성화됨**)** - 확인란을 사용하여 이 알림 프로파일을 활성화합니다.

단계 **10** **Save(**저장**)**를 클릭합니다.

29 장

로그 전달 개요

보안 이벤트 및 트래픽 로그

SIEM(Security Information Event Management) 시스템은 보안 정보 및 보안 이벤트 정보를 단일 관리 플랫폼으로 결합하는 것을 전문으로 하는 솔루션입니다. 보안 및 이벤트 정보는 이 정보를 SIEM에 전달하도록 구성된 서드파티 보안 솔루션에서 가져옵니다.

멀티 클라우드 방어에서는 UI 내에서 직접 보안 이벤트 정보 보기를 지원합니다. 이러한 이벤트는 **Investigate(**조사**)** > **Flow Analytics(**플로우 분석**)** 섹션에서 사용할 수 있습니다. 이벤트는 다음과 같이 분류되고 볼 수 있습니다.

카테고리	유형	설명
플로우 로그	FLOW_LOG	트래픽 흐름의 여러 단계와 관련된 정보

카테고리	유형	설명
방화벽 이벤트	APPID	애플리케이션 ID를 기준으로 일치하는 트래픽(OpenAppID)
	GEOIP	Geo IP에서 제공되거나 Geo IP로 전송되는 트래픽(MaxMind)
	L4_FW	레이어 4 정보(소스/대상 IP/포트 및 프로토콜)를 기반으로 일치하는 트래픽
	MALICIOUS_IP	악의적인 IP에서 발생하거나 악성 IP로 향하는 트래픽 (TrustWave)
	SNI	SNI 정보를 기준으로 일치하는 트래픽
네트워크 위협	AV	바이러스가 탐지된 트래픽 (ClamAV)
	DPI	IDS/IPS 위협이 탐지된 트래픽 (TALOS)
	DLP	민감한 데이터가 유출되는 트래픽
웹 보호	WAF	웹 애플리케이션 위협이 탐지된 트래픽(ModSecurity)
	L7DOS	Layer7 DOS 공격에 기여하는 트래픽
URL 필터링	URLFILTER	URL 범주 또는 URL과 일치하는 트래픽(BrightCloud)
FQDN 필터링	FQDNFILTER.	FQDN 범주 또는 FQDN과 일치하는 트래픽(BrightCloud)
HTTPS 로그	HTTP_REQUEST	웹 기반 트래픽 관련 정보(HTTP)
	TLS_ERROR	TLS 오류 관련 정보
	TLS_LOG	TLS 동작 관련 정보
트래픽 요약 로그	SESSION_SUMMARY	처리된 각 트래픽 세션에 대한 요약 정보

Note 2.10 이상 게이트웨이 릴리스에서 플로우 로그가 더 이상 사용되지 않습니다. 각 플로우 로그에 포함된 정보는 **Traffic Summary(**트래픽 요약**)** > **Logs(**로그**)**에서 제공되는 세션 정보의 일부로 제공됩니다.

로그 전달 프로파일을 사용하여 각 이벤트 범주를 SIEM으로 전송할 수 있습니다. 현재 멀티 클라우드 방어에서 지원되는 SIEM은 다음과 같습니다.

- AWS S3 버킷
- Datadog
- GCP 로깅
- Microsoft Sentinel
- Splunk
- Sumo Logic
- Syslogs

로그 전달 프로파일은 아래에 설명된 단계를 사용하여 작동할 수 있습니다.

독립형 이벤트 또는 트래픽 로그 프로파일 생성

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)** > **Log Forwarding(**로그 전달**)**으로 이동합니다.
단계 **2** **Create(**생성**)**를 클릭합니다.
단계 **3** 프로파일 이름 및 설명을 지정합니다.
단계 **4** *Type(*유형*)*을 Standalone(독립형)으로 지정합니다.
단계 **5** 적절한 매개변수를 입력합니다(SIEM 관련 문서 참조).
단계 **6** **Save(**저장**)**를 클릭합니다.
단계 **7** 원하는 게이트웨이 연결을 추가합니다(게이트웨이에 이벤트, 트래픽 로그 전달 프로파일 또는 메트릭 전달 프로파일 추가 참조).

독립형 이벤트 또는 트래픽 로그 프로파일 편집

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)** > **Log Forwarding(**로그 전달**)**으로 이동합니다.
단계 **2** 편집할 프로파일 옆의 상자를 선택합니다.
단계 **3** **Edit(**편집**)**를 클릭합니다.
단계 **4** 원하는 대로 매개변수를 수정합니다(SIEM 관련 문서 참조).
단계 **5** **Save(**저장**)**를 클릭합니다.

그룹 이벤트 또는 트래픽 로그 프로파일 생성

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)** > **Log Forwarding(**로그 전달**)**으로 이동합니다.
단계 **2** **Create(**생성**)**를 클릭합니다.
단계 **3** 프로파일 이름 및 설명을 지정합니다.
단계 **4** *Type(*유형*)*을 Group(그룹)으로 지정합니다.
단계 **5** 그룹화하려는 독립형 프로파일의 수를 수용하기 위해 행을 필요한 만큼 추가합니다.
단계 **6** **Save(**저장**)**를 클릭합니다.
단계 **7** 원하는 게이트웨이 연결을 추가합니다(게이트웨이에 이벤트, 트래픽 로그 전달 프로파일 또는 메트릭 전달 프로파일 추가 참조).

그룹 이벤트 또는 트래픽 로그 프로파일 편집

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)** > **Log Forwarding(**로그 전달**)**으로 이동합니다.
단계 **2** 편집할 프로파일 옆의 상자를 선택합니다.
단계 **3** **Edit(**편집**)**를 클릭합니다.
단계 **4** 독립형 프로파일을 수정, 추가 또는 제거합니다.
단계 **5** **Save(**저장**)**를 클릭합니다.

이벤트 또는 트래픽 로그 전달 프로파일 보기

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)** > **Log Forwarding(**로그 전달**)**으로 이동합니다.
단계 **2** 세부 정보를 보려는 프로파일 링크를 선택합니다.
단계 **3** 세부 정보를 봅니다.

이벤트 또는 트래픽 로그 프로파일 삭제

대시보드에서 프로파일을 삭제하려면 다음 절차를 따르십시오.

Before you begin

대시보드에서 프로파일을 삭제하기 전에 이벤트 또는 프로파일과 게이트웨이 간의 연결을 반드시 제거해야 합니다. 자세한 내용은 게이트웨이에서 이벤트, 트래픽 로그 전달 프로파일 또는 메트릭 전달 프로파일 제거를 참조하십시오.

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)** > **Log Forwarding(**로그 전달**)**으로 이동합니다.
단계 **2** 삭제할 프로파일 옆의 상자를 선택합니다.
단계 **3** **Delete(**삭제**)**를 클릭합니다.
단계 **4** **Yes(**예**)** 또는 **No(**아니요**)**를 클릭하여 삭제 작업을 확인합니다.

검색 로그

검색 로그는 SIEM(Security Information Event Management) 시스템으로 전달되어 단일 관리 플랫폼으로 집계될 수 있습니다.

멀티 클라우드 방어에서는 UI 내에서 직접 보안 이벤트 정보 보기를 지원합니다. 이러한 이벤트는 **Investigate(**조사**)** > **Traffic(**트래픽**)** 섹션에서 사용할 수 있습니다. 이벤트는 다음과 같이 분류되고 볼 수 있습니다.

카테고리	유형	설명
DNS 로그	DNS_LOG	클라우드 제공자로부터 수집된 DNS 로그 정보와 위협 인텔리전스의 상관 관계
VPC 로그	VPC_LOG	클라우드 제공자로부터 수집된 VPC/VNet 플로우 로그 정보와 위협 인텔리전스의 상관 관계

로그 전달 프로파일을 사용하고 온보딩된 클라우드 어카운트에 프로파일을 연결하여 각 범주를 SIEM으로 전송할 수 있습니다. 현재 멀티 클라우드 방어에서 지원하는 로그 전달 대상은 다음과 같습니다.

- AWS S3 버킷
- Datadog
- GCP 로깅
- Microsoft Sentinel
- Splunk
- Sumo Logic
- Syslogs

검색 로그를 전달하려면 아래 단계를 사용합니다.

독립형 검색 로그 프로파일 생성

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)** > **Log Forwarding(**로그 전달**)**으로 이동합니다.
단계 **2** **Create(**생성**)**를 클릭합니다.
단계 **3** 프로파일 이름 및 설명을 지정합니다.
단계 **4** *Type(*유형*)*을 Standalone(독립형)으로 지정합니다.
단계 **5** 적절한 매개변수를 입력합니다(SIEM 관련 문서 참조).
단계 **6** **Save(**저장**)**를 클릭합니다.
단계 **7** 로그 프로파일을 원하는 클라우드 어카운트에 연결합니다(클라우드 어카운트로 검색 로그 프로파일 추가 참조).

독립형 검색 로그 프로파일 편집

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)** > **Log Forwarding(**로그 전달**)**으로 이동합니다.
단계 **2** 편집할 프로파일 옆의 상자를 선택합니다.
단계 **3** **Edit(**편집**)**를 클릭합니다.
단계 **4** 원하는 대로 매개변수를 수정합니다(SIEM 관련 문서 참조).
단계 **5** **Save(**저장**)**를 클릭합니다.

그룹 검색 로그 프로파일 생성

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)** > **Log Forwarding(**로그 전달**)**으로 이동합니다.
단계 **2** **Create(**생성**)**를 클릭합니다.
단계 **3** 프로파일 이름 및 설명을 지정합니다.
단계 **4** *Type(*유형*)*을 Group(그룹)으로 지정합니다.
단계 **5** 독립형 프로파일을 연결할 행을 추가합니다.
단계 **6** **Save(**저장**)**를 클릭합니다.
단계 **7** 원하는 게이트웨이 연결을 추가합니다(게이트웨이에 이벤트, 트래픽 로그 전달 프로파일 또는 메트릭 전달 프로파일 추가 참조).

그룹 검색 로그 프로파일 편집

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)** > **Log Forwarding(**로그 전달**)**으로 이동합니다.
단계 **2** 편집할 프로파일 옆의 상자를 선택합니다.
단계 **3** **Edit(**편집**)**를 클릭합니다.
단계 **4** 독립형 프로파일을 수정, 추가 또는 제거합니다.
단계 **5** **Save(**저장**)**를 클릭합니다.

검색 로그 프로파일 세부 정보 보기

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)** > **Log Forwarding(**로그 전달**)**으로 이동합니다.
단계 **2** 세부 정보를 보려는 프로파일 링크를 선택합니다.
단계 **3** 세부 정보를 봅니다.

클라우드 어카운트로 검색 로그 프로파일 추가

단계 **1** **Manage(**관리**)** > **Cloud Accounts(**클라우드 어카운트**)** > **Accounts(**어카운트**)**로 이동합니다.
단계 **2** 프로파일을 연결할 클라우드 어카운트 옆의 확인란을 선택합니다.
단계 **3** **Actions(**작업**)** > **Update Log Profile(**로그 프로파일 업데이트**)**를 클릭합니다.
단계 **4** 클라우드 로그 전달 프로파일에 대한 **Log Profile(**로그 프로파일**)** 개체를 선택합니다.
단계 **5** **Save & Continue(**저장 후 계속**)**를 클릭합니다.

클라우드 어카운트에서 검색 로그 프로파일 제거

단계 **1** **Manage(**관리**)** > **Cloud Accounts(**클라우드 계정**)** > **Accounts(**계정**)**로 이동합니다.
단계 **2** 프로파일을 연결할 클라우드 어카운트 옆의 확인란을 선택합니다.
단계 **3** **Actions(**작업**)** > **Update Log Profile(**로그 프로파일 업데이트**)**를 클릭합니다.
단계 **4** *Cloud Logs Forwarding Profile(*클라우드 로그 전달 프로파일*)* 매개변수의 경우 *Profile(*프로파일*)* 옆에 있는 'X'를 클릭하여 제거합니다.
단계 **5** **Save & Continue(**저장 후 계속**)**를 클릭합니다.

검색 로그 프로파일 삭제

대시보드에서 프로파일을 삭제하려면 다음 절차를 따르십시오.

Before you begin

대시보드에서 프로파일을 삭제하기 전에 프로파일과 게이트웨이 간의 연결을 반드시 제거해야 합니다. 자세한 내용은 클라우드 어카운트에서 검색 로그 프로파일 제거를 참조하십시오.

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)** > **Log Forwarding(**로그 전달**)**으로 이동합니다.

단계 **2** 삭제할 프로파일 옆의 상자를 선택합니다.

단계 **3** **Delete(**삭제**)**를 클릭합니다.

단계 **4** **Yes(**예**)** 또는 **No(**아니요**)**를 클릭하여 삭제 작업을 확인합니다.

게이트웨이 메트릭 전달 프로파일

이 프로파일은 데이터 모니터링 및 분석을 위해 멀티 클라우드 방어 게이트웨이에 의해 생성된 게이트웨이 메트릭을 전달하는 데 사용됩니다. 메트릭은 게이트웨이에 의해 생성되지만 메트릭을 서드파티 분석 애플리케이션에 전달하는 멀티 클라우드 방어 컨트롤러입니다. 이 전달 프로파일을 사용하면 멀티 클라우드 방어에 로그인하지 않고도 게이트웨이 메트릭을 모니터링, 분석 및 구성할 수 있습니다. 이 정보를 사용하여 게이트웨이 환경의 성능 및 동작을 측정합니다. 또한 환경 문제 해결을 위해 이 정보를 활용합니다.

참고 멀티 클라우드 방어 컨트롤러 버전 23.09부터는 DataDog만 서드파티 분석 애플리케이션으로 지원됩니다.

DataDog와 같이 사용 가능한 대부분의 분석 애플리케이션의 경우, 반드시 권한이 부여된 사용자여야 툴의 API 및 렌더링된 데이터에 액세스할 수 있습니다.

독립형 메트릭 전달 프로파일 생성

다음 절차에 따라 독립형 프로파일을 생성하고 서드파티에서 처리할 메트릭을 전달합니다.

시작하기 전에

이 프로파일을 생성하기 전에 메트릭을 전달할 서드파티 애플리케이션이 하나 이상 있어야 합니다.

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)** > **Metrics Forwarding(**메트릭 전달**)**로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** 고유한 프로파일 이름을 입력합니다.

단계 **4** (선택 사항) **Description(**설명**)**을 입력합니다. 이렇게 하면 유사한 이름의 다른 프로파일과 구분할 수 있습니다.

단계 **5** **Type(**유형**)** 드롭다운 메뉴를 확장하고 **Standalone(**독립형**)**을 선택합니다.

단계 **6** **Destination(**대상**)** 드롭다운 메뉴를 확장하고 메트릭을 처리하고 분석할 서드파티 애플리케이션을 선택합니다.

단계 **7** 메트릭의 엔드포인트 위치로 사용할 **Endpoint(**엔드포인트**)**를 입력합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

분석 애플리케이션으로 DataDog를 선택하는 경우, 엔드포인트는 기본적으로 HTTP Webhook로 채워집니다. 이 항목이 기본값인 경우 프로파일을 저장하기 전에 수정할 수 있습니다.

다음에 수행할 작업

- 프로파일 세부 정보 보기, 173 페이지
- 프로파일에 게이트웨이 연결 추가, 174 페이지

독립형 메트릭 전달 프로파일 편집

이미 생성된 독립형 프로파일을 편집하려면 다음 절차를 사용합니다.

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)**로 이동하고 적절한 프로파일 **Type(**유형**)**을 선택합니다.

단계 **2** 편집할 프로파일 옆의 상자를 선택합니다.

단계 **3** **Edit(**편집**)**를 클릭합니다.

단계 **4** 필요에 따라 매개변수를 수정합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

그룹 메트릭 전달 프로파일 생성

이 프로세스에서는 프로파일을 생성한 다음 특정 게이트웨이에 할당합니다. 그룹 프로파일은 최대 5개의 독립형 메트릭 전달 프로파일을 결합한 다음 단일 게이트웨이에 할당할 수 있습니다. 다음 절차를 사용하여 그룹화된 메트릭 전달 프로파일을 생성합니다.

시작하기 전에

- 이 프로파일을 생성하기 전에 메트릭을 전달할 서드파티 애플리케이션이 하나 이상 있어야 합니다.
- 둘 이상의 독립형 메트릭 전달 프로파일이 이미 생성되어 있어야 합니다. 자세한 내용은 독립형 메트릭 전달 프로파일 생성, 167 페이지를 참조하십시오.

단계 **1** 멀티 클라우드 방어 컨트롤러 인터페이스에서 **Manager(**관리자**)** > **Profiles(**프로파일 **)** > **Metrics Forwarding(**메트릭 전달**)**으로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** 고유 **Profile Name(**프로파일 이름**)**을 입력합니다.

단계 **4** (선택 사항) **Description(**설명**)**을 입력합니다. 이렇게 하면 유사한 이름의 프로파일을 구분하는 데 도움이 될 수 있습니다.

단계 **5** **Type(**유형**)** 드롭다운 메뉴를 확장하고 **Group(**그룹**)**을 선택합니다.

단계 **6** **Group Details(**그룹 세부 정보**)**에서 프로파일에 추가해야 하는 모든 새 행에 대해 **Add(**추가**)**를 클릭합니다.

단계 **7** 각 행에 대한 드롭다운 메뉴를 확장하여 그룹에 추가할 프로파일을 선택합니다. 저장하기 전에 언제든지 프로파일을 제거하려면, 해당 프로파일의 확인란을 선택하고 **Remove(**제거**)**를 선택합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 프로파일 세부 정보 보기, 173 페이지
- 프로파일에 게이트웨이 연결 추가, 174 페이지

그룹 프로파일 편집

이미 생성된 그룹화된 프로파일 집합을 편집하려면 다음 절차를 사용합니다.

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)**로 이동하고 적절한 프로파일 **Type(**유형**)**을 선택합니다.

단계 **2** 편집할 프로파일 옆의 상자를 선택합니다.

단계 **3** **Edit(**편집**)**를 클릭합니다.

단계 **4** 그룹 프로파일을 수정, 추가 또는 제거합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

프로파일 삭제

대시보드에서 프로파일을 삭제하려면 다음 절차를 따르십시오.

시작하기 전에

대시보드에서 프로파일을 삭제하기 전에 프로파일과 게이트웨이 간의 연결을 반드시 제거해야 합니다. 자세한 내용은 게이트웨이에서 이벤트, 트래픽 로그 전달 프로파일 또는 메트릭 전달 프로파일 제거를 참조하십시오.

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)**로 이동하고 적절한 프로파일 **Type(**유형**)**을 선택합니다.
단계 **2** 삭제할 프로파일 옆의 상자를 선택합니다.
단계 **3** **Delete(**삭제**)**를 클릭합니다.
단계 **4** **Yes(**예**)** 또는 **No(**아니요**)**를 클릭하여 삭제 작업을 확인하거나 취소합니다.

게이트웨이에 이벤트, 트래픽 로그 전달 프로파일 또는 메트릭 전달 프로파일 추가

단계 **1** **Manage(**관리**)** > **Gateways(**게이트웨이**)**로 이동합니다.
단계 **2** 프로파일을 연결할 게이트웨이 옆의 확인란을 선택합니다.
단계 **3** **Edit(**편집**)**를 클릭합니다.
단계 **4** *Log Profile(*로그 프로파일*)* 매개변수에 대해서는 메뉴에서 원하는 프로파일을 선택합니다.
단계 **5** **Save(**저장**)**를 클릭합니다.

게이트웨이에서 이벤트, 트래픽 로그 전달 프로파일 또는 메트릭 전달 프로파일 제거

단계 **1** **Manage(**관리**)** > **Gateways(**게이트웨이**)**로 이동합니다.
단계 **2** 프로파일의 연결을 해제할 게이트웨이 옆의 확인란을 선택합니다.
단계 **3** **Edit(**편집**)**를 클릭합니다.
단계 **4** *Log Profile(*로그 프로파일*)* 매개변수의 경우 *Profile(*프로파일*)* 옆에 있는 'X'를 클릭하여 제거합니다.
단계 **5** **Save(**저장**)**를 클릭합니다.

Note 또한 로그 전달 프로파일을 게이트웨이 생성 시 게이트웨이와 연결할 수 있습니다. *Log Profile(*로그 프로파일*)* 매개변수는 게이트웨이 생성 프로세스 중에 사용할 수 있으며, 이 프로세스에서는 메뉴에서 원하는 프로파일을 선택할 수 있습니다.

30 장

로그 전달 대상/SIEM

AWS S3 버킷

멀티 클라우드 방어에서는 처리, 저장, 액세스 및 상관관계를 위해 보안 이벤트 및 트래픽 로그를 AWS S3 버킷으로 전송하여 보안 이벤트 및 트래픽 로그 정보를 전송할 수 있습니다. 전송되는 정보는 속성-값 쌍을 액세스하고 처리할 수 있는 준정형 JSON 형식으로 전송됩니다.

요구 사항

AWS S3 버킷에 이벤트/로그를 전달하려면 다음이 필요합니다.

1. 새 AWS 버킷을 만들거나 기존 AWS S3 버킷을 사용합니다.
2. 다음 정책을 AWS S3 버킷에 적용하여 멀티 클라우드 방어 컨트롤러이(가) 버킷에 대한 액세스 및 쓰기를 허용합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "<controller-role-arn>"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::<s3bucketname>/*",
        "arn:aws:s3:::<s3bucketname>"
      ]
    }
```

```
    ]
}
```

프로파일 매개변수

매개변수	정확도	기본값	설명
프로파일 이름	필수		프로파일을 참조하는 데 사용할 고유한 이름입니다.
설명	선택 사항		프로파일에 대한 설명입니다.
대상	필수	AWS S3	AWS S3 버킷
CSP 계정	필수		AWS S3 버킷이 있는 CSP 계정입니다.
S3 버킷	필수		이벤트/로그가 전달할 AWS S3 버킷 이름입니다.

Datadog

DataDog는 많은 기업에서 사용하는 매우 일반적이고 강력한 SIEM입니다. 멀티 클라우드 방어은(는) DataDog로의 로그 전달을 지원하여 처리, 저장, 액세스 및 상관 관계를 위해 보안 이벤트 및 트래픽 로그 정보를 전송합니다. 전송되는 정보는 속성-값 쌍을 액세스하고 처리할 수 있는 준정형 JSON 형식으로 전송됩니다.

요구 사항

DataDog에 로그를 전달하려면 다음 정보가 필요합니다.

- DataDog 계정
- 엔드포인트 URL
- API 키

Tip

- Datadog 계정에 등록하려면 **Datadog** 계정(https://www.datadoghq.com/)을 참조하십시오.
- Datadog API 키를 생성하려면 **Datadog API** 키(https://app.datadoghq.com/account/login?next=%2Faccount%2Fsettings#api)를 참조하십시오.

프로파일 매개변수

매개변수	정확도	기본값	설명
프로파일 이름	필수		프로파일을 참조하는 데 사용할 고유한 이름입니다.
설명	선택 사항		프로파일에 대한 설명입니다.
대상	필수	Datadog	프로파일에 사용되는 SIEM입니다.
인증서 확인 건너뛰기	선택 사항	선택 취소됨	인증서의 신뢰성 확인을 건너뛸지 여부입니다.
API 키	필수		통신 인증을 위한 DataDog API 키입니다.
엔드포인트	필수	https://http-intake.logs.datadoghq.com/	전달된 이벤트/로그를 수신하는 데 사용되는 URL 엔드포인트

GCP 로깅

GCP Stack드라이버 로깅은 애플리케이션 및 서비스에서 로그 수집 및 저장을 위해 GCP(Google Cloud Provider)가 제공하는 서비스입니다. 멀티 클라우드 방어은(는) GCP Stack드라이버 로깅으로의 로그 전달을 지원하여 처리, 저장, 액세스 및 상관관계를 위해 보안 이벤트 및 트래픽 로그 정보를 전송합니다. 전송되는 정보는 속성-값 쌍을 액세스하고 처리할 수 있는 준정형 JSON 형식으로 전송됩니다.

요구 사항

게이트웨이에서 GCP StackDriver 로그에 이벤트를 기록하려면 GCP 멀티 클라우드 방어-*firewall* 서비스 어카운트에 로그 작성자 역할이 할당되어야 합니다.

프로파일 매개변수

매개변수	정확도	기본값	설명
프로파일 이름	필수		프로파일을 참조하는 데 사용할 고유한 이름입니다.
설명	선택 사항		프로파일에 대한 설명입니다.

매개변수	정확도	기본값	설명
대상	필수	GCP 로깅(게이트웨이에서)	프로파일에 사용되는 SIEM입니다.
로그 이름	필수	ciscomcd -gateway-logs	이벤트를 저장하는 데 사용되는 Stackdriver 로그의 이름입니다.

필드 정수 대 문자열 매핑

이벤트가 컨트롤러에서 전달되면 컨트롤러는 이벤트 필드 값을 식별 이름에 매핑합니다. 이벤트가 게이트웨이에서 직접 전달될 경우(예: GCP 로깅) 컨트롤러는 관련되지 않으며, 따라서 이벤트 필드 값은 식별 이름에 매핑되지 않습니다. 이러한 필드를 해석하려면 사용자는 식별 이름 매핑에 대한 필드 값을 수행해야 합니다.

식별 매핑에 대한 필드, 하위 필드 및 해당 값은 아래에 나와 있습니다.

필드	정수	문자열
action	0	DUMMY_ACTION
	1	ALLOW
	2	DENY
	3	DROP
	4	REDIRECT
	5	PROXY
	6	LOG
	7	OTHER
	8	DELAY
	9	DETECT_SIG

필드	정수	문자열
gatewaySecurityType	1	INGRESS_FIREWALL
	2	EAST_WEST_AND_EGRESS_FIREWALL

필드	정수	문자열
level	1	DEBUG
	2	INFO
	3	NOTICE
	4	WARNING
	5	ERROR
	6	CRITICAL
	7	ALERT
	8	EMERGENCY

필드	정수	문자열
policyMatchInfo.serviceType	0	UNKNOWN
	1	PROXY
	2	FORWARDING
	3	REVERSE_PROXY
	4	FORWARD_PROXY

필드	정수	문자열
protocol **sessionSummaryInfo.egressConnection.protocol** **sessionSummaryInfo.ingressConnect.protocol**	0	DUMMY
	1	ICMP
	6	TCP
	17	UDP
	252	HTTP

필드	정수	문자열
rule.type	0	DUMMY_RULE_TYPE
	1	THIRD_PARTY
	2	USER_DEFINED

필드	정수	문자열
statusText **ingressConnectionStates.state**	0	CLOSED
	1	SYN_SENT
	2	SYN_RECV
	3	ESTABLISHED
	4	FIN_WAIT
	5	CLOSE_WAIT
	6	LAST_ACK
	7	TIME_WAIT
	8	CLOSE

필드	정수	문자열
type	1	WAF
	2	DPI
	3	HTTP_REQUEST
	4	L4_FW
	5	FLOW_LOG
	6	MALICIOUS_IP
	7	TLS_ERROR
	8	TLS_LOG
	9	L7DOS
	10	SNI
	11	APPID
	12	URLFILTER
	13	SESSION_SUMMARY
	14	DLP
	15	FQDNFILTER.
	16	AV

Microsoft Sentinel

Microsoft Sentinel은 많은 기업에서 사용하는 강력한 SIEM입니다. 멀티 클라우드 방어은(는) Microsoft Sentinel로의 로그 전달을 지원하여 처리, 저장, 액세스 및 상관 관계를 위해 보안 이벤트 및 트래픽 로그 정보를 전송합니다. 전송되는 정보는 속성-값 쌍을 액세스하고 처리할 수 있는 준정형 JSON 형식으로 전송됩니다.

요구 사항

Microsoft Sentinel에 로그를 전달하려면 다음 정보가 필요합니다.

- Azure 로그 분석 작업 영역을 생성합니다.
- Azure 로그 테이블을 정의합니다.

프로파일 매개변수

매개변수	정확도	기본값	설명
프로파일 이름	필수		프로파일을 참조하는 데 사용할 고유한 이름입니다.
설명	선택 사항		프로파일에 대한 설명입니다.
대상	필수	Microsoft Sentinel	프로파일에 사용되는 SIEM입니다.
Azure 로그 분석 작업 영역 ID	필수		Azure 로그 분석 작업 영역의 ID입니다.
공유 키	필수		통신 인증에 사용되는 공유 키입니다.
Azure 로그 테이블 이름	필수		로그/이벤트가 저장될 Azure 로그 테이블의 이름입니다.

Splunk

Splunk는 많은 기업에서 사용하는 매우 일반적이고 강력한 SIEM입니다. 멀티 클라우드 방어은(는) Splunk로의 로그 전달을 지원하여 처리, 저장, 액세스 및 상관 관계를 위해 보안 이벤트 및 트래픽 로그 정보를 전송합니다. 전송되는 정보는 속성-값 쌍을 액세스하고 처리할 수 있는 준정형 JSON 형식으로 전송됩니다.

요구 사항

Splunk에 로그를 전달하려면 다음 정보가 필요합니다.

- Splunk 계정
- Splunk 컬렉터 URL
- 이벤트 컬렉터 키
- 색인 이름

Tip Splunk 이벤트 컬렉터에 대한 자세한 내용은 **Splunk HTTP** 이벤트 컬렉터(https://docs.splunk.com/Documentation/Splunk/8.1.0/Data/UsetheHTTPEventCollector)를 참조하십시오.

프로파일 매개변수

매개변수	정확도	기본값	설명
프로파일 이름	필수		프로파일을 참조하는 데 사용할 고유한 이름입니다.
설명	선택 사항		프로파일에 대한 설명입니다.
대상	필수	Datadog	프로파일에 사용되는 SIEM입니다.
인증서 확인 건너뛰기	선택 사항	선택 취소됨	인증서의 신뢰성 확인을 건너뛸지 여부입니다.
엔드포인트	필수		HTTP 이벤트 컬렉터에 액세스하는 데 사용되는 URL입니다.
토큰	필수		멀티 클라우드 방어에 Splunk와 통신에 허용하는 Splunk 토큰입니다.
색인	필수	기본	이벤트를 저장하는 데 사용되는 Splunk 인덱스의 이름입니다.

Sumo Logic

Sumo Logic은 많은 기업에서 사용하는 매우 일반적이고 강력한 SIEM입니다. 멀티 클라우드 방어은(는) Sumo Logic으로의 로그 전달을 지원하여 처리, 저장, 액세스 및 상관 관계를 위해 보안 이벤트 및 트래픽 로그 정보를 전송합니다. 전송되는 정보는 속성-값 쌍을 액세스하고 처리할 수 있는 준정형 JSON 형식으로 전송됩니다.

요구 사항

Sumo Logic에 로그를 전달하려면 다음 정보가 필요합니다.

- Sumo Logic 계정
- Sumo Logic 컬렉터 엔드포인트

Tip Sumo Logic 컬렉터 설정 방법에 대한 자세한 내용은 **Sumo Logic** 설정 가이드(https://help.sumologic.com/docs/send-data/setup-wizard/)를 참조하십시오.

프로파일 매개변수

매개변수	정확도	기본값	설명
프로파일 이름	필수		프로파일을 참조하는 데 사용할 고유한 이름
설명	선택 사항		프로파일에 대한 설명
대상	필수	Sumo Logic	프로파일에 사용되는 SIEM
엔드포인트	필수		전달된 이벤트/로그를 수신하는 데 사용되는 URL 엔드포인트

Syslogs

시스템 로그 서버는 표준 형식의 시스템 로그 메시지를 수락하는 공통 로그 컬렉터입니다. 각 시스템 로그 메시지에는 시설, 심각도, 메시지에 대한 필드가 포함되어 있습니다. 대부분의 SIEM은 다른 메시지 형식을 지원하지만 거의 모든 SIEM은 시스템 로그 형식의 메시지를 수락할 수 있습니다. 멀티 클라우드 방어에서는 보안 이벤트 및 트래픽 로그를 시스템 로그 서버로 전송하도록 지원합니다. 전달할 수 있는 이벤트 및 로그의 목록은 다음과 같습니다.

- 플로우 로그(트래픽 요약)

- 방화벽 이벤트(AppID, L4FW, GeoIP, MaliciousIP, SNI)
- HTTPS 로그(HTTP, TLS)
- 네트워크 위협(AV, DLP, IDS/IPS)
- 웹 보호(WAF, L7 DoS)

Note 플로우 로그는 게이트웨이 버전 2.10 이상 릴리스에서 더 이상 사용되지 않습니다. 각 플로우 로그에 포함된 정보는 **Traffic Summary(**트래픽 요약**)** > **Logs(**로그**)**에서 제공되는 세션 정보의 일부로 제공됩니다.

이벤트는 로그 전달 프로파일을 사용하여 시스템 로그 서버로 전달할 수 있습니다. 생성된 프로파일을 새 게이트웨이 또는 기존 게이트웨이와 연결해야 이벤트가 시스템 로그 서버로 전송됩니다. 로그 전달 프로파일의 게이트웨이 연결을 생성, 수정 또는 변경하려면 보안 이벤트 및 트래픽 로그를 참조하십시오.

프로파일 매개변수

매개변수	정확도	기본값	설명
프로파일 이름	필수		프로파일을 참조하는 데 사용할 고유한 이름입니다.
설명	선택 사항		프로파일에 대한 설명입니다.
SIEM 벤더	필수	시스템 로그	프로파일에 사용되는 SIEM입니다.
서버 IP	필수		시스템 로그 서버의 IP 주소입니다.
프로토콜	필수	UDP	메시지를 전송할 때 사용할 프로토콜(TCP/UDP)입니다.
포트	필수		메시지를 전송할 때 사용할 포트입니다.
형식	필수	IETF	메시지의 형식입니다(IETF만 지원됨).
플로우 로그	필수	아니요	플로우 로그를 보낼지 여부(예/아니요)입니다.

매개변수	정확도	기본값	설명
방화벽 이벤트	필수	아니요	방화벽 이벤트를 전송할지 여부(예/아니요)입니다.
HTTPS 로그	필수	아니요	HTTPS 로그를 전송할지 여부(예/아니요)입니다.
네트워크 위협	필수	긴급	가장 낮은 심각도 수준으로 네트워크 위협을 전송할 수 있습니다.
웹 공격	필수	긴급	웹 공격을 전송할 가장 낮은 심각도 레벨입니다.

Note 다음의 심각도 레벨(가장 높은 것부터 가장 낮은 것)을 사용할 수 있습니다.

- 긴급
- 알림
- 심각
- 오류
- 경고
- 알림
- 정보
- 디버그

지정한 심각도 레벨 이상을 포함하는 범주에 대한 모든 이벤트는 시스템 로그 서버로 전송됩니다.

XIII 부

관리

31 장

관리

Administration(관리) 페이지에서 어카운트의 상태 및 어카운트와 관련된 클라우드 서비스 제공자의 전체 상태를 확인할 수 있습니다.

관리

Administration(관리) 페이지에서 어카운트의 상태 및 어카운트와 관련된 클라우드 서비스 제공자의 전체 상태를 확인할 수 있습니다.

API 키

이 페이지를 보려면 **Administration(관리)** > **Management(관리)** > **API Keys(API 키)**로 이동합니다.

검색

검색 막대를 사용하여 키워드가 포함된 API 키 목록을 찾거나 필터링합니다. 검색을 정규화하려면 3개 이상의 문자를 사용해야 합니다.

API 키 테이블 및 작업

이 표에는 클라우드 서비스 제공자에 대해 멀티 클라우드 방어 구성 요소가 생성하는 모든 API 키가 나와 있습니다. 역할, 키 ID, 키가 멀티 클라우드 방어에 추가된 날짜 및 키가 만료된 날짜를 확인합니다.

여기에서 API 키를 생성하거나 삭제할 수 있습니다. 이러한 키는 멀티 클라우드 방어에 의해 생성되며 클라우드 서비스 제공자가 통신을 유지하기 위해 생성할 수 있는 키와 관련이 없습니다. 자세한 내용을 보려면 계속 읽으십시오.

멀티 클라우드 방어에서 API 키 생성

다음 절차에 따라 API 키를 생성합니다.

단계 **1** **Administration(**관리**)** > **Management(**관리**)** > **API Keys(API** 키**)**로 이동합니다.

단계 **2** **Create API Key(API** 키 생성**)**를 클릭합니다.

단계 **3** 고유한 **Name(**이름**)**을 입력합니다.

단계 **4** 멀티 클라우드 방어에서 자동으로 생성하는 이메일 주소 를 확인합니다. 이 옵션은 변경할 수 없습니다.

단계 **5** 드롭다운 메뉴를 사용하여 다음 주요 역할 중 하나를 선택합니다.

- **admin_read_only -** 이 역할은 상호 작용을 제한하므로 어떤 것도 수정하거나 조치를 취할 수 없으며 사용 가능한 데이터를 "보기"만 할 수 있습니다.
- **admin_read_rw -** 사용 가능한 데이터를 읽고 수정할 수 있는 역할을 제공합니다.

단계 **6** **API Key Lifetime (days)(API** 키 수명**(**일**))**에 적절한 값을 입력합니다. 기본값은 365일입니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

멀티 클라우드 방어에서 **API** 키 삭제

다음 절차에 따라 API 키를 삭제합니다.

단계 **1** **Administration(**관리**)** > **Management(**관리**)** > **API Keys(API** 키**)**로 이동합니다.

단계 **2** 테이블에서 API Key(API 키)를 선택하고 강조 표시되도록 확인란을 선택합니다.

단계 **3** **Delete(**삭제**)**를 클릭합니다.

단계 **4** 키 삭제를 확인하고 **Yes(**예**)**를 클릭합니다. 키는 멀티 클라우드 방어에서 즉시 제거됩니다.

계정 레벨 설정

이 페이지에는 애플리케이션 태그 및 맞춤형 태그를 포함하여 멀티 클라우드 방어에 사용되는 태그 중 일부가 표시됩니다. 자세한 내용을 보려면 계속 읽으십시오.

애플리케이션 태그

애플리케이션 태그는 문자의 문자열이며 프로세스 또는 스레드의 자동 분류를 위한 분류 기준 중 하나로 사용됩니다. 태깅을 사용하면 고유한 요구 사항을 기반으로 앱을 그룹화하여 앱을 검색하고 취약점을 찾을 수 있습니다. 모든 클라우드 서비스 제공자가 애플리케이션 태그 사용을 지원하는 것은 아닙니다.

참고 애플리케이션 태그는 한 번에 하나만 생성할 수 있습니다. 새 태그를 생성해야 하는 경우 기존 태그를 삭제한 다음 새 애플리케이션 태그를 생성해야 합니다**.**

애플리케이션 태그 생성

다음 절차에 따라 애플리케이션 태그를 생성합니다. 이러한 태그는 내부 전용이며 클라우드 서비스 제공자의 인터페이스에서 인식되거나 사용되지 않을 수 있습니다.

단계 **1** **Administration(**관리**)** > **Management(**관리**)** > **Account(**어카운트**)**로 이동합니다.

단계 **2** **Application Tag(**애플리케이션 태그**)** 표에서 **Create(**생성**)**를 클릭합니다.

단계 **3** 애플리케이션 태그의 유형은 기본적으로 `APPLICATION_TAG_KEYS` 입니다.

단계 **4** 태그에 대한 간략한 **Description(**설명**)**을 입력합니다. 이렇게 하면 유사한 이름이나 개념을 가질 수 있는 다른 태그를 식별하거나 구분하는 데 도움이 됩니다.

단계 **5** 하나 이상의 **Value(**값**)**를 입력합니다. 둘 이상의 값을 생성하려면 각 값 후에 `Enter(엔터)`를 입력합니다. 이 값은 대소문자를 구분합니다.

단계 **6** **Save(**저장**)**를 클릭합니다. 태그가 생성되어 표에서 사용할 수 있습니다.

애플리케이션 태그 편집

다음 절차에 따라 멀티 클라우드 방어에서 생성된 기존 애플리케이션 태그를 편집합니다. 이 절차를 클라우드 서비스 제공자의 인터페이스에서 생성된 태그를 수정하는 데 사용할 수 없습니다.

단계 **1** **Administration(**관리**)** > **Management(**관리**)** > **Account(**어카운트**)**로 이동합니다.

단계 **2** **Application Tag (**애플리케이션 태그**)** 표에서 편집할 애플리케이션 태그를 찾고 왼쪽에 있는 상자를 선택하여 강조 표시합니다.

단계 **3** **Edit(**편집**)**를 클릭합니다.

단계 **4** 다음 매개변수를 수정합니다.

- **Description(**설명**) -** 설명을 수정하거나 삭제할 수 있습니다.
- **Tag Values(**태그 값**) -** 여기에서 태그를 추가하거나 제거할 수 있습니다.

단계 **5** **Save(**저장**)**를 클릭합니다. 또는 변경 사항을 저장하지 않고 언제든지 취소할 수 있습니다.

애플리케이션 태그 삭제

다음 절차에 따라 기존 애플리케이션 태그를 삭제합니다.

단계 **1** **Administration(**관리**)** > **Management(**관리**)** > **Account(**어카운트**)**로 이동합니다.

단계 **2** **Application Tag(**애플리케이션 태그**)** 표에서 편집할 애플리케이션 태그를 찾고 왼쪽에 있는 상자를 선택하여 강조 표시합니다.

단계 **3** **Delete(**삭제**)**를 클릭합니다.

단계 **4** 애플리케이션 태그를 삭제할 것인지 확인하고 **Yes(**예**)**를 클릭합니다.

맞춤형 태그

맞춤형 태그는 항목에 대한 세부 정보를 제공하는 간단한 데이터이며 동일한 태그가 있는 관련 항목을 쉽게 찾을 수 있습니다. 태그를 사용하여 개체, 정책, 규칙 등을 쉽게 식별하거나 구분할 수 있습니다.

맞춤형 태그 생성

다음 절차에 따라 멀티 클라우드 방어에서 맞춤형 태그를 생성합니다. 이러한 태그는 내부 전용이며 클라우드 서비스 제공자의 인터페이스에서 인식되거나 사용되지 않을 수 있습니다.

단계 **1** **Administration(**관리**)** > **Management(**관리**)** > **Account(**어카운트**)**로 이동합니다.

단계 **2** **Custom Tag(**맞춤형 태그**)** 표에서 **Create(**생성**)**를 클릭합니다.

단계 **3** 태그의 **Value(**값**)**를 입력합니다. 이렇게 하면 유사한 이름이나 개념을 가질 수 있는 다른 태그를 식별하거나 구분하는 데 도움이 됩니다.

단계 **4** 하나 이상의 **Value(**값**)**를 입력합니다.

단계 **5** **Save(**저장**)**를 클릭합니다. 태그가 생성되어 표에서 사용할 수 있습니다.

맞춤형 태그 편집

다음 절차에 따라 기존 맞춤형 태그를 수정합니다.

단계 **1** **Administration(**관리**)** > **Management(**관리**)** > **Account(**어카운트**)**로 이동합니다.

단계 **2** **Custom Tag(**맞춤형 태그**)** 표에서 편집할 애플리케이션 태그를 찾고 왼쪽에 있는 상자를 선택하여 강조 표시합니다.

단계 **3** **Edit(**편집**)**를 클릭합니다.

단계 **4** 다음 매개변수를 수정합니다.

- 키.
- 값을 복원했습니다.

단계 **5** **Save(**저장**)**를 클릭합니다. 또는 변경 사항을 저장하지 않고 언제든지 취소할 수 있습니다.

맞춤형 태그 삭제

다음 절차에 따라 기존 맞춤형 태그를 삭제합니다.

단계 **1** **Administration(**관리**)** > **Management(**관리**)** > **Account(**어카운트**)**로 이동합니다.

단계 **2** **Custom Tag(**맞춤형 태그**)** 표에서 편집할 애플리케이션 태그를 찾고 왼쪽에 있는 상자를 선택하여 강조 표시합니다.

단계 **3** **Delete(**삭제**)**를 클릭합니다.

단계 **4** 애플리케이션 태그를 삭제할 것인지 확인하고 **Yes(**예**)**를 클릭합니다.

시스템

System(시스템**)** 페이지는 최소 1년치 업데이트를 카탈로그로 만드는 기록 문서입니다. 이러한 세부 정보를 통해 일반 정보를 파악하고, 올바른 릴리스 노트 버전을 찾고, Cisco 지원에 문의하여 제품 도움을 받을 수 있습니다. 다음 정보 모음이 여기에 표시됩니다.

구성 요소

이 섹션에는 멀티 클라우드 방어 컨트롤러 및 사용자 인터페이스의 현재 버전이 모두 표시됩니다. 이 페이지에서는 업데이트 또는 이전 버전으로 롤백할 수 없습니다.

게이트웨이 이미지

Gateway Images(게이트웨이 이미지) 표는 멀티 클라우드 방어 게이트웨이이 업그레이드된 시간, 게이트웨이의 버전, 유지 기간, 게이트웨이가 설정된 표준 시간대를 나타냅니다.

Talos/네트워크 침입

이 표에는 Cisco의 Talos 인텔리전스 그룹의 모든 업데이트가 표시됩니다. 이러한 업데이트는 일반 제품 소프트웨어 릴리스와 별도로 시스코 제품에 푸시됩니다.

웹 보호

이 테이블에는 최신 웹 애플리케이션 취약점 및 위협에 대한 모든 WF(Web Application Firewall) 코어 및 트러스트웨이브 규칙 업데이트가 표시됩니다.

미터링

Metering(미터링**)** 페이지에는 멀티 클라우드 방어의 전체 사용량과 클라우드 서비스 제공자를 위해 생성된 게이트웨이 인스턴스에 대한 사용량 그래프가 표시됩니다.

필터

페이지 상단에 있는 필터를 사용하여 페이지에 표시되는 데이터를 결정합니다. 월과 연도를 선택하여 이 보기를 변경할 수 있습니다. 이러한 필터 설정을 사용하여 사용 보고서를 생성할 수 있습니다.

사용 보고서 생성

이 페이지에서 두 가지 옵션 중 하나에 대한 사용량 보고서를 생성할 수 있습니다. **Administration(**관리**)** > **Management(**관리**)** > **Metering(**미터링**)**으로 이동하고 페이지의 **Filter(**필터**)**에서 **Download(**다

운로드**)** 드롭다운 옵션을 확장하여 사용량 또는 인스턴스를 선택합니다. 파일은 .csv 파일로 로컬에 다운로드됩니다. 필터링 옵션을 사용하여 보고서를 생성해야 하는 기간을 결정합니다.

사용 기록**(UR)**

Usage Records(사용 기록**)** 표에는 테넌트와 연결된 어카운트 수, 어카운트가 상호 작용한 시간, 필터 섹션에서 선택한 월의 요일에 대한 정보가 나와 있습니다. 사용량/월 비율에서 가장 활발했던 요일을 확인할 수 있습니다.

인스턴스 기록

Instance Records(인스턴스 기록**)** 표에는 다음 인스턴스 통계가 표시됩니다.

- 어카운트 이름
- 클라우드 서비스 제공자별 어카운트 유형.
- 인스턴스 ID.
- 인스턴스 유형.
- 가용성 영역.
- 게이트웨이.
- Started(시작됨) - 게이트웨이 인스턴스가 생성된 시간입니다.
- Ended(종료됨) - 게이트웨이 인스턴스가 만료되거나 종료된 시간입니다.

알림 프로파일

Administration(관리**)** > **Alert Profiles(**알림 프로파일**)**로 이동하여 다음 관리 보기에 액세스합니다.

Services(서비스**)**와 **Alerts(**알림**)** 페이지 모두 멀티 클라우드 방어의 알림에 중점을 둡니다. **Alerts(**알림**)** 페이지는 알림이 전송된 위치에 중점을 두며 **Alerts(**알림**)** 페이지는 구성된 엔드포인트로 어떤 알림이 전송될 지에 대해 자세히 설명합니다. 이상적인 구성을 위해 두 페이지의 항목을 설정하는 데 시간을 투자하여 대시보드 내에서 알림 기회를 성공적으로 그리고 전체적으로 최적화합니다.

서비스

이 페이지를 보려면 **Administration(**관리**)** > **Management(**관리**)** > **Service(**서비스**)**로 이동합니다.

서비스에서는 알림을 전송할 대상에 중점을 둡니다. 이 페이지에서 옵션을 성공적으로 구성하려면 서드파티 애플리케이션의 기준을 제공해야 합니다.

검색

검색 막대를 사용하여 키워드가 포함된 서비스 목록을 찾거나 필터링합니다. 검색을 정규화하려면 3개 이상의 문자를 사용해야 합니다.

서비스 표 및 작업

이 표에는 클라우드 서비스 제공업체를 위해 멀티 클라우드 방어 구성 요소가 만든 모든 서비스가 나열되어 있습니다. 서비스 이름, 유형, 서비스가 업데이트된 날짜를 봅니다.

여기에서 서비스를 생성하거나 삭제할 수 있습니다. 이러한 서비스는 멀티 클라우드 방어에 의해 생성되며 클라우드 서비스 제공자가 제공하는 서비스와 관련이 없습니다.

서비스 생성

다음 절차에 따라 서비스를 생성합니다.

시작하기 전에

서드파티 메시징 애플리케이션에서 서비스 알림 또는 통합을 활성화 하거나 허용해야 합니다.

단계 **1** **Administration(**관리**)** > **Management(**관리**)** > **Services(**서비스**)**로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** 고유한 **Name(**이름**)**을 입력합니다.

단계 **4** (선택 사항) **Description(**설명**)**을 입력합니다. 이렇게 하면 유사한 이름을 가질 수 있는 다른 서비스를 구분하는 데 도움이 될 수 있습니다.

단계 **5** 드롭다운 메뉴를 사용하여 서비스 **Type(**유형**)**을 선택합니다.

- Pager Duty.
- ServiceNow.
- Slack.
- Datadog.
- Microsoft Sentinel.
- Microsoft Teams.
- Webex
- Splunk

단계 **6** 서비스 유형에 따라 프롬프트가 표시되면 다음 항목을 입력합니다.

- API 키.
- API URL.
- Azure 로그 테이블 이름.
- Azure 로그 분석 작업 영역 ID
- (Splunk의 선택 사항) 인덱스.

단계 **7** **Save(**저장**)**를 클릭합니다.

서비스 편집

다음 절차에 따라 기존 서비스를 편집합니다.

단계 **1** **Administration(**관리**)** > **Management(**관리**)** > **Services(**서비스**)**로 이동합니다.
단계 **2** 표에서 서비스를 찾아 선택하여 강조 표시합니다.
단계 **3** Actions(작업) 드롭다운 메뉴를 확장하고 **Edit(**편집**)**를 선택합니다.
단계 **4** 서비스의 다음과 같은 부분을 수정합니다.

- Name(이름).
- Description(설명)
- Type(유형).
- 유형별 구성 기준.

단계 **5** **Save(**저장**)**를 클릭하여 변경 사항을 확인합니다. 언제든지 **Cancel(**취소**)**을 클릭하여 창을 닫고 변경을 취소합니다.

다음에 수행할 작업

변경 사항을 확인하려면 페이지 **Refresh(**새로 고침**)**을 수행해야 할 수 있습니다.

서비스 복제

다음 절차에 따라 기존 서비스를 복제합니다.

단계 **1** **Administration(**관리**)** > **Management(**관리**)** > **Services(**서비스**)**로 이동합니다.
단계 **2** 표에서 서비스를 찾아 선택하여 강조 표시합니다.
단계 **3** Actions(작업) 드롭다운 메뉴를 확장하고 **Clone(**복제**)**을 선택합니다.
단계 **4** 서비스의 복제본이 생성됩니다. 기본적으로는 서비스 **Type(**유형**)** 및 서비스별 설정 기준만 유지됩니다.
단계 **5** 고유한 이름을 입력합니다.
단계 **6** (선택 사항) 설명을 입력합니다.
단계 **7** **Save(**저장**)**를 클릭하여 변경 사항을 확인합니다. 언제든지 **Cancel(**취소**)**을 클릭하여 창을 닫고 변경을 취소합니다.

다음에 수행할 작업

표에 대한 변경 사항 또는 추가된 내용을 보려면 페이지를 **Refresh(**새로 고침**)** 해야 할 수 있습니다.

서비스 내보내기

다음 절차에 따라 기존 서비스를 내보냅니다.

단계 **1** **Administration(**관리**)** > **Management(**관리**)** > **Services(**서비스**)**로 이동합니다.

단계 **2** 표에서 서비스를 찾아 선택하여 강조 표시합니다.

단계 **3** Actions(작업) 드롭다운 메뉴를 확장하고 **Export(**내보내기**)**를 선택합니다.

단계 **4** 멀티 클라우드 방어이 내보내기 마법사를 생성합니다.

단계 **5** **Download(**다운로드**)**를 클릭하여 terrform을 로컬로 다운로드하거나 **Copy Code(**코드 복사**)**를 클릭하여 JSON 리소스를 복사하여 terroform 스크립트에 수동으로 붙여 넣습니다.

단계 **6** terrform 프롬프트에서 창 하단에 있는 명령을 실행합니다. `terraform import "ciscomcd_alert_profile". "servicename" <number in table>`

단계 **7** terraform 내의 지시에 따라 작업을 완료합니다. 대시보드에 더 이상 단계가 없습니다.

서비스 삭제

다음 절차에 따라 기존 서비스를 삭제합니다.

단계 **1** **Administration(**관리**)** > **Management(**관리**)** > **Services(**서비스**)**로 이동합니다.

단계 **2** 표에서 서비스를 찾아 선택하여 강조 표시합니다.

단계 **3** Actions(작업) 드롭다운 메뉴를 확장하고 **Delete(**삭제**)**를 선택합니다.

단계 **4** 서비스 삭제를 확인하고 **Yes(**예**)**를 클릭합니다.

단계 **5** 서비스가 멀티 클라우드 방어에서 제거됩니다.

알림

Alerts(알림) 페이지에서는 서드파티 엔드포인트에 어떤 알림이 전송되는지에 중점을 둡니다. 알림 기회를 활용하려면 알림과 서비스를 모두 구성하는 것이 좋습니다.

알림 생성

다음 절차에 따라 알림을 생성합니다.

단계 **1** **Administration(**관리**)** > **Management(**관리**)** > **Services(**서비스**)**로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** 고유한 **Name(**이름**)**을 입력합니다.

단계 **4** (선택 사항) **Description(**설명**)**을 입력합니다. 이렇게 하면 유사한 이름을 가질 수 있는 다른 서비스를 구분하는 데 도움이 될 수 있습니다.

단계 **5** **Alert Profile(**알림 프로파일**)**을 선택합니다. 현재 `Pagerduty` 만 사용할 수 있습니다.

단계 **6** 드롭다운 메뉴를 사용하여 **Type(**유형**)** 알림을 선택합니다.

- 시스템 로그.
- 감사 로그.
- 발견.

단계 **7** (선택 사항) 드롭다운 메뉴를 사용하여 **Sub Type(**하위 유형**)**을 선택합니다. 6단계에서 선택한 Type(유형)에 따라 이러한 옵션이 변경되거나 사용되지 않을 수 있습니다.

- 게이트웨이.
- 어카운트.
- 컨트롤러.
- 인사이트 규칙.

단계 **8** 드롭다운 메뉴를 사용하여 **Severity(**심각도**)** 레벨을 선택합니다.

- Info.
- Warning(경고)
- Medium(중간).
- High(높음).
- Critical(중대).

단계 **9** 기본적으로 **Enabled(**활성화됨**)** 확인란이 선택되어 있습니다. 이 옵션은 알림 프로파일이 활성 상태이며 사용 가능한지를 지정합니다. 비활성화된 경우 멀티 클라우드 방어는 알림을 생성할 때 이를 포함하지 않습니다.

다음에 수행할 작업

서비스하여 이러한 알림을 전송할 대상을 지정합니다.

알림 편집

다음 절차에 따라 기존 알림을 내보냅니다.

단계 **1** **Administration(**관리**)** > **Management(**관리**)** > **Alert(**알림**)**로 이동합니다.

단계 **2** 표에서 알림을 찾아 선택하여 강조 표시합니다.

단계 **3** Actions(작업) 드롭다운 메뉴를 확장하고 **Edit(**편집**)**를 선택합니다.

단계 **4** 알림 프로파일의 필드 및 선택 항목을 수정합니다. 선택 사항에 따라 사용 가능한 필드 중 일부가 변경될 수 있습니다.

단계 **5** **Save(**저장**)**를 클릭하여 변경 사항을 확인합니다. 언제든지 **Cancel(**취소**)**을 클릭하여 변경을 취소하고 편집 창을 닫습니다.

알림 복제

다음 절차에 따라 기존 알림을 복제합니다.

단계 **1** **Administration(**관리**)** > **Management(**관리**)** > **Alert(**알림**)**로 이동합니다.

단계 **2** 표에서 알림을 찾아 선택하여 강조 표시합니다.

단계 **3** Actions(작업) 드롭다운 메뉴를 확장하고 **Edit(**편집**)**를 선택합니다.

단계 **4** 알림의 복제본이 생성됩니다. 기본적으로는 **Alert Profile(**알림 프로파일**)** 및 **Type(**유형**)**만 유지됩니다.

단계 **5** 알림의 나머지 필드 및 선택 항목을 수정합니다. 선택 사항에 따라 사용 가능한 필드 중 일부가 변경될 수 있습니다.

단계 **6** **Save(**저장**)**를 클릭하여 변경 사항을 확인합니다. 언제든지 **Cancel(**취소**)**을 클릭하여 변경을 취소하고 편집 창을 닫습니다.

알림 내보내기

다음 절차에 따라 기존 알림을 내보냅니다.

단계 **1** **Administration(**관리**)** > **Management(**관리**)** > **Alert(**알림**)**로 이동합니다.

단계 **2** 표에서 알림을 찾아 선택하여 강조 표시합니다.

단계 **3** Actions(작업) 드롭다운 메뉴를 확장하고 **Export(**내보내기**)**를 선택합니다.

단계 **4** 멀티 클라우드 방어이 내보내기 마법사를 생성합니다.

단계 **5** **Download(**다운로드**)**를 클릭하여 terrform을 로컬로 다운로드하거나 **Copy Code(**코드 복사**)**를 클릭하여 JSON 리소스를 복사합니다.

단계 **6** Terraform 스크립트에 수동으로 붙여넣습니다.

단계 **7** terraform 프롬프트에서 창 하단에 제공된 명령을 실행합니다. `terraform import "ciscomcd_alert_rule"."alertname" <number in table>`

단계 **8** Terraform 프롬프트의 프롬프트에 따라 작업을 완료합니다. 멀티 클라우드 방어에서 내보내기 창을 닫습니다**.** 대시보드에 더 이상 단계가 없습니다.

알림 삭제

다음 절차에 따라 기존 알림을 삭제합니다.

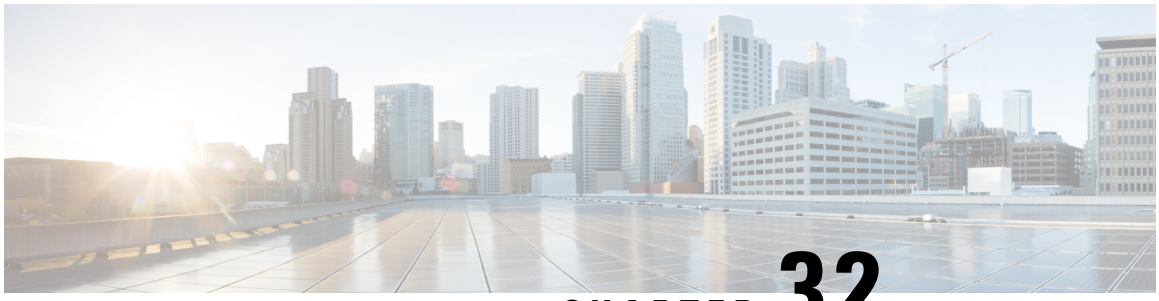
단계 **1** **Administration(**관리**)** > **Management(**관리**)** > **Alert(**알림**)**로 이동합니다.

단계 **2** 표에서 알림을 찾아 선택하여 강조 표시합니다.

단계 **3** Actions(작업) 드롭다운 메뉴를 확장하고 **Delete(**삭제**)**를 선택합니다.
단계 **4** 서비스 삭제를 확인하고 **Yes(**예**)**를 클릭합니다.
단계 **5** 멀티 클라우드 방어에서 알림이 제거됩니다.

XIV 부

멀티 클라우드 어카운트 관리



CHAPTER 32

멀티 클라우드 방어계정 관리

계정(멀티 클라우드 방어 테넌트)

계정 정보는 관리자가 다음 기능을 생성하고 편집하는 데 사용됩니다.

Administration(관리**)** > **Management(**관리**)** > **Account(**어카운트**)**로 이동합니다.

CDO의 사용자 역할

Cisco Defense Orchestrator(CDO)에는 읽기 전용, 편집 전용, 구축 전용, 관리자, 슈퍼 관리자 등 다양한 사용자 역할이 있습니다. 사용자 역할은 각 테넌트의 각 사용자에 대해 구성됩니다. CDO 사용자가 둘 이상의 테넌트에 액세스할 수 있는 경우, 사용자 ID는 동일하지만 테넌트마다 역할이 다를 수 있습니다. 사용자는 한 테넌트에 대해서는 읽기 전용 역할을, 다른 테넌트에서는 슈퍼 관리자 역할을 가질 수 있습니다. 인터페이스 또는 설명서에서 읽기 전용 사용자, Admin 사용자 또는 Super Admin 사용자를 언급하는 경우 특정 테넌트에 대한 사용자의 권한 수준을 의미합니다.

멀티 클라우드 방어의 역할

역할은 멀티 클라우드 방어 포털을 통해 멀티 클라우드 방어 테넌트에 액세스할 때 사용자가 수행할 수 있는 작업에서 중요한 역할을 합니다. 역할은 사용자에게 권한 집합을 부여하는 권한입니다.

다음 세 가지 역할을 사용할 수 있습니다.

- 슈퍼 관리자(admin_super)
- 편집 전용 관리자(admin_rw)
- 읽기 전용 관리자(admin_read-only)

두 가지 권한 정의는 다음과 같습니다.

- 수정 - 읽기, 쓰기, 편집 및 삭제
- 읽기 - 읽기 전용

다음 표에는 각 역할과 관련된 각 설정에 대한 권한이 요약되어 있습니다.

설정	슈퍼 관리자 **(admin_super)**	편집 전용**(admin_rw)**	읽기 전용 **(admin_read-only)**
관리			
사용자	수정	수정(슈퍼 관리자 제외)	읽기
MFA 활성/비활성	수정	수정(슈퍼 관리자 제외)	읽기
MFA 재설정	수정	수정(슈퍼 관리자 제외)	읽기
API 키	수정	수정	읽기
역할	읽기	읽기	읽기
계정 / 애플리케이션 태그	수정	수정	읽기
계정 - 이메일 도메인	수정	읽기	읽기
시스템	읽기	읽기	읽기
미터링	읽기	읽기	읽기
알림 프로파일			
서비스	수정	수정	읽기
알림	수정	수정	읽기

멀티 클라우드 방어 테넌트 내 사용자 1명만 슈퍼 관리자 역할을 할당할 수 있습니다. 이 사용자는 계정의 소유자로 간주되며 AWS 계정 또는 Linux 루트 계정의 소유자와 동의어입니다. 다른 모든 사용자에게는 읽기/쓰기 관리자 또는 읽기 전용 관리자 역할이 할당되어야 합니다.

슈퍼 관리자 역할은 멀티 클라우드 방어에 의해 할당되며 멀티 클라우드 방어 테넌트 생성 시 생성된 첫 번째 사용자에게 부여됩니다. 슈퍼 관리자 사용자를 변경해야 하는 경우 멀티 클라우드 방어 지원 팀에 문의하십시오.

33 장

클라우드 어카운트

클라우드 어카운트

다음은 현재 멀티 클라우드 방어에 연결된 클라우드 서비스 제공자에 대한 개요입니다. 다음을 수행할 수 있습니다

어카운트 추가

이 절차를 사용하여 Cloud Accounts(클라우드 어카운트) 페이지에서 클라우드 서비스 제공에 대한 어카운트를 추가할 수 있습니다.

단계 **1** 멀티 클라우드 방어 컨트롤러에 로그인하여 **Manage(**관리**)** > **Cloud Accounts(**클라우드 어카운트**)** > **Accounts(**어카운트**)**로 이동합니다.

단계 **2** **Add Account(**어카운트 추가**)**를 클릭합니다.

단계 **3** Account Type(어카운트유형)의 경우 드롭다운 메뉴를 사용하여 연결할 클라우드 서비스 제공자를 선택합니다.

단계 **4** 연결 마법사를 계속 진행하여 클라우드 서비스 제공자를 연결합니다. 클라우드 서비스 제공자의 유형에 고유할 수 있는 사전 요구 사항 및 항목별 값에 대한 자세한 내용은 어카운트 온보딩, 25 페이지를 참조하십시오.

인벤토리 관리

이 절차를 사용하여 클라우드 서비스 제공자에 대해 할당된 지역의 모니터링된 invotry를 구성하거나 수정합니다.

단계 **1** 멀티 클라우드 방어 컨트롤러에 로그인하여 **Manage(**관리**)** > **Cloud Accounts(**클라우드 어카운트**)** > **Accounts(**어카운트**)**로 이동합니다.

단계 **2** Account(어카운트) 표에서 클라우드 서비스 제공자 어카운트를 하나 선택합니다.

단계 **3** 테이블 위의 옵션에서 **Manage Inventory(**인벤토리 관리**)**를 클릭합니다.

단계 **4** 생성된 창에는 어카운트, 클라우드 서비스 제공자, 현재 모니터링되는 지역에 대한 일반 정보가 표시됩니다.

단계 **5** 다음 작업을 사용하여 영역 선택을 수정합니다.

- 기존 행에 개별 영역을 추가합니다.
- 기존 행에서 개별 영역을 삭제합니다.
- 모니터링 영역의 새 행을 추가합니다. 오른쪽에 있는 파란색 더하기 버튼을 클릭합니다.
- 모니터링 영역의 전체 행을 삭제합니다. 오른쪽의 파란색 빼기 버튼을 클릭합니다.
- **Refresh Interval(**새로 고침 간격**)** 값을 변경합니다. 기본값은 60분마다 새로 고치는 것입니다.
- **Refresh(**새로 고침**)** 아이콘을 사용하여 창을 수동으로 새로 고칩니다.

단계 **6** 모든 변경을 수행한 후에는 **Save**(저장)를 클릭합니다. 또는 변경 사항을 저장하지 않으려면 **Cancel(**취소**)**을 클릭하여 창을 종료합니다.

클라우드 어카운트 편집

다음 절차에 따라 기본 클라우드 서비스 제공자 어카운트 정보를 편집합니다.

단계 **1** 멀티 클라우드 방어 컨트롤러에 로그인하여 **Manage(**관리**)** > **Cloud Accounts(**클라우드 어카운트**)** > **Accounts(**어카운트**)**로 이동합니다.

단계 **2** Account(어카운트) 표에서 클라우드 서비스 제공자 어카운트를 하나 선택합니다.

단계 **3** 표 위에 나열된 옵션에서 **Actions(**작업**)** 드롭다운 메뉴를 확장하고 **Edit(**편집**)**를 클릭합니다. 어카운트에 대한 기본 정보를 생성하는 창입니다.

단계 **4** 채워진 필드(구성 가능)를 편집합니다. 모든 클라우드 서비스 제공자가 동일한 필드를 사용하는 것은 아닙니다.

단계 **5** **Save & Continue(**저장 후 계속**)**를 클릭합니다. 또는 변경 사항을 저장하지 않으려면 **Cancel(**취소**)**을 클릭하여 창을 닫습니다.

단계 **6** 변경 사항을 저장되었습니다.

단계 **7** 창은 현재 모니터링되는 영역을 검토하고 수정할 수 있도록 인벤토리 관리 창으로 자동 전환됩니다. **Save & Continue(**저장 후 계속**)**를 클릭합니다. 또는 변경 사항을 저장하지 않으려면 **Cancel(**취소**)**을 클릭하여 창을 닫습니다. 이 작업은 **Manage Inventory(**인벤토리 관리**)** 창만 닫습니다. 이전 윈도우에서 어카운트에 대한 변경 사항을 되돌리지 않습니다.

클라우드 어카운트에 대한 로그 프로파일 업데이트

다음 절차에 따라 클라우드 서비스 제공자가 현재 로그를 전송하도록 구성된 로그 전달 서비스를 수정합니다.

단계 **1** 멀티 클라우드 방어 컨트롤러에 로그인하여 **Manage(**관리**)** > **Cloud Accounts(**클라우드 어카운트**)** > **Accounts(**어카운트**)**로 이동합니다.

단계 **2** Account(어카운트) 표에서 클라우드 서비스 제공자 어카운트를 하나 선택합니다.

단계 **3** 표 위에 나열된 옵션에서 **Actions(**작업**)** 드롭다운 메뉴를 확장하고 **Update Log Profile(**로그 프로파일 업데이트**)**를 클릭합니다. 어카운트에 대한 기본 정보를 생성하는 창입니다.

단계 **4** 드롭다운 메뉴를 사용하여 로그를 전달할 서비스를 선택합니다. 전송할 로그를 확인하려면 드롭다운 왼쪽에 있는 정보 태그 위에 커서를 놓습니다.

단계 **5** **Save & Continue(**저장 후 계속**)**를 클릭합니다. 또는 변경 사항을 저장하지 않으려면 **Cancel(**취소**)**을 클릭하여 창을 닫습니다.

단계 **6** 변경 사항이 성공적으로 저장되고 **Accounts(**어카운트**)** 페이지로 돌아갑니다.

클라우드 어카운트 내보내기

단계 **1** 멀티 클라우드 방어 컨트롤러에 로그인하여 **Manage(**관리**)** > **Cloud Accounts(**클라우드 어카운트**)** > **Accounts(**어카운트**)**로 이동합니다.

단계 **2** Account(어카운트) 표에서 클라우드 서비스 제공자 어카운트를 하나 선택합니다.

단계 **3** 표 위에 나열된 옵션에서 **Actions(**작업**)** 드롭다운 메뉴를 확장하고 **Export(**내보내기**)**를 클릭합니다. 멀티 클라우드 방어 컨트롤러은 내보내기 마법사를 생성합니다.

단계 **4** Download(다운로드)를 클릭하여 terraform을 로컬로 다운로드하거나 아래로 스크롤하여 Copy Code(코드 복사)를 클릭하여 JSON 리소스를 복사합니다.

단계 **5** Terraform 스크립트에 수동으로 붙여넣습니다.

단계 **6** Terraform 프롬프트에서 창 하단에 있는 명령을 실행합니다.

```
terraform import "ciscomcd_cloud_account"."</cloud service provider>" </cloud service provider>
```

단계 **7** Terraform 프롬프트의 프롬프트에 따라 작업을 완료합니다.

단계 **8** 멀티 클라우드 방어 컨트롤러에서 내보내기 창을 닫습니다. 대시보드에 더 이상 단계가 없습니다.

클라우드 어카운트 삭제

단계 **1** 멀티 클라우드 방어 컨트롤러에 로그인하여 **Manage(**관리**)** > **Cloud Accounts(**클라우드 어카운트**)** > **Accounts(**어카운트**)**로 이동합니다.

단계 **2** Account(어카운트) 표에서 클라우드 서비스 제공자 어카운트를 하나 선택합니다.

단계 **3** 표 위에 나열된 옵션에서 **Actions(**작업**)** 드롭다운 메뉴를 확장하고 **Delete(**삭제**)**를 클릭합니다. 어카운트에 대한 기본 정보를 생성하는 창입니다.

단계 **4** 어카운트 삭제를 확인하고 **Yes(**예**)**를 클릭합니다. 어카운트를 삭제하지 않으려면 **No(**아니요**)**를 클릭하여 확인창을 닫습니다.

인벤토리

Inventory(인벤토리**)** 페이지에서 클라우드 서비스 제공자 어카운트와 관련된 검색된 자산을 검토하고 관리할 수 있습니다.

페이지 맨 위의 필터 옵션을 사용하여 클라우드 서비스 제공자 유형별로 어카운트 페이지를 구성합니다. 또는 여러 필드와 값으로 검색을 생성하려면 **Switch to Advanced Search(**고급 검색으로 전환**)**를 클릭할 수도 있습니다.

페이지에 표시된 자산을 클릭하면 자산 및 기본 구성 기록을 볼 수 있습니다. 이 페이지에서는 자산을 편집할 수 없습니다. 필요한 경우 테이블에서 VPC/VNet 값과 자산 ID를 모두 복사할 수 있습니다.

인벤토리 관리, 277 페이지를 선택하면, 멀티 클라우드 방어 내의 해당 페이지로 리디렉션됩니다.

XV 부

어카운트 문제 해결

34 장

어카운트 연결 문제 해결

어카운트 수동으로 온보딩

어카운트 온보딩, 25 페이지에서 제공하는 방법을 사용하여 클라우드 서비스 제공자 계정을 멀티 클라우드 방어에 온보딩하는 경우, 계정을 수동으로 온보딩해야 할 수 있습니다. 대안으로 다음 옵션을 사용합니다.

GCP 프로젝트 수동 온보딩

GCP 개요

GCP 프로젝트 및 GCP 폴더

멀티 클라우드 방어 현재는 GCP 프로젝트 및 GCP 폴더를 모두 지원합니다. 단 이러한 구성 요소는 별도로 지원됩니다. 이러한 두 옵션에 대해 다음과 같은 제한 및 예외를 참고하십시오.

GCP 프로젝트에는 가상 머신, 스토리지 버킷, 데이터베이스 등과 같은 GCP 리소스가 포함되어야 합니다. 모든 Google Cloud 서비스를 생성, 활성화, 사용하는 데 사용할 수 있습니다.

- 프로젝트는 Terraform, 수동 온보딩, 스크립트 온보딩을 통해 온보딩할 수 있습니다.
- 프로젝트는 검색 및 조사 등 오케스트레이션이 필요한 환경에 적합합니다.
- 멀티 클라우드 방어 대시보드를 통해 각 프로젝트와 개별적으로 상호 작용할 수 있습니다.

버전 23.10부터는 GCP 폴더를 Terraform에 연결할 수 있습니다. GCP 폴더에는 프로젝트, 다른 폴더 또는 이 둘의 조합이 포함됩니다. 조직 리소스는 폴더를 사용하여 계층 구조의 조직 리소스 노드 아래에 프로젝트를 그룹화할 수 있습니다.

- `roles/compute.admin` 권한이 활성화되지 않은 폴더는 비어 있는 것으로 간주되어 사용되지 않습니다.

- 온보딩된 폴더와 연결된 프로젝트는 자산 및 트래픽 검색에만 사용됩니다.
- 온보딩된 폴더와 연결된 프로젝트에서는 오케스트레이션 서비스 VPC 또는 게이트웨이 생성을 수용하지 않습니다.
- GCP 콘솔에서 폴더에 만든 권한은 폴더 레벨에서 만들어야 합니다. 따라서 멀티 클라우드 방어 작업은 폴더 레벨에서도 이루어집니다.

GCP 폴더를 온보딩하려는 경우 Terraform 저장소를 참조하십시오.

절차 개요

다음은 GCP 프로젝트를 연결하는 방법에 대한 개요입니다. 셸 스크립트는 멀티 클라우드 방어에서 제공하며 마법사의 일부로 간편한 연결 프로세스를 지원합니다. 스크립트는 다음 단계를 자동화하므로 사용자가 수행할 필요가 없습니다.

1. 2개의 서비스 어카운트를 생성합니다.
2. 다음 API(Compute Engine, Secret Manager)를 활성화합니다.
3. 다음 2개의 VPC(management, datapath)를 생성합니다.
4. 데이터 경로 VPC에서 멀티 클라우드 방어 게이트웨이(앱 트래픽)에 대한 트래픽을 허용하는 방화벽 규칙을 생성합니다.
5. 관리 VPC에서 관리 트래픽이 멀티 클라우드 방어 게이트웨이에서 멀티 클라우드 방어 컨트롤러(으)로 이동할 수 있도록 방화벽 규칙을 생성합니다.

스크립트가 작동하지 않거나 설정을 수동으로 변경해야 하는 경우 GCP 클라우드 콘솔 웹 UI 또는 gcloud CLI를 사용하여 이러한 작업을 실행할 수 있습니다. GCP 프로젝트 수동 온보딩에서 프로젝트를 연결하는 다른 방법를 참조하십시오.

서비스 어카운트

멀티 클라우드 방어에는 GCP 프로젝트에서 2개의 서비스 어카운트를 생성해야 합니다.

- 멀티 클라우드 방어-**controller**: 이 계정은 멀티 클라우드 방어 컨트롤러가 GCP 프로젝트에 액세스하여 멀티 클라우드 방어 게이트웨이에 대한 리소스(멀티 클라우드 방어 게이트웨이), 로드 밸런서를 생성하고 VPC, 서브넷, 보안 그룹 태그 등에 대한 정보를 읽는 데 사용됩니다.
- 멀티 클라우드 방어-**gateway**: 이 계정은 멀티 클라우드 방어 게이트웨이(컴퓨팅 VM 인스턴스)에 할당됩니다. 계정은 Secret Manager(TLS 암호 해독용 개인 키) 및 스토리지에 대한 액세스를 제공합니다.

이러한 서비스 어카운트는 UI에서 제공되는 서비스를 사용하거나 클라우드 서비스 제공자의 CLI를 사용하는 두 가지 방법 중 하나로 생성할 수 있습니다.

GCP 클라우드 콘솔을 사용하여 멀티 클라우드 방어 컨트롤러 서비스 어카운트 생성

멀티 클라우드 방어 컨트롤러 서비스 어카운트는 멀티 클라우드 방어 컨트롤러에서 GCP 프로젝트의 리소스에 액세스하고 관리하는 데 사용됩니다. 계정을 생성하고 키를 생성해야 합니다. 키는 컨트롤러에 계정을 온보딩할 때 컨트롤러에 추가됩니다.

단계 **1** GCP 프로젝트에서 **IAM**을 엽니다.

단계 **2** **Service Accounts(**서비스 어카운트**)**를 클릭합니다.

단계 **3** **Service Account(**서비스 어카운트**)**를 생성합니다.

단계 **4** 이름 및 ID(예: 멀티 클라우드 방어-fcontroller)를 제공하고 **Create(**생성**)**를 클릭합니다.

단계 **5** 컴퓨팅 관리자 및 서비스 어카운트 사용자 역할을 추가합니다.

단계 **6** **Continue(**계속**)**를 클릭합니다.

단계 **7** **Done(**완료**)**을 클릭합니다.

Note 사용자를 추가할 필요는 없습니다.

단계 **8** 새로 생성된 계정을 클릭하고 **Keys(**키**)**가 나올 때까지 아래로 스크롤한 다음 **Add Key(**키 추가**)** 드롭다운에서 **Create New Key(**새 키 생성**)**를 선택합니다.

단계 **9** JSON(기본 옵션)을 선택하고 **Create(**생성**)**를 클릭합니다.

단계 **10** 파일이 컴퓨터에 다운로드됩니다. 이 파일을 저장합니다.

GCP 클라우드 콘솔을 사용하여 멀티 클라우드 방어 방화벽 서비스 어카운트 생성

멀티 클라우드 방어방화벽 서비스 어카운트는 멀티 클라우드 방어 게이트웨이GCP 프로젝트 내부에서 실행 중인 인스턴스에서 사용합니다. 게이트웨이는 (사용자가 구성한 경우) PCAP 파일 등을 저장하기 위해 TLS 암호 해독 및 액세스 스토리지를 위해 SecretManager에 저장된 개인 키에 액세스해야 할 수 있습니다. 또한 여러 게이트웨이에는 (사용자가 구성한 경우) 멀티 클라우드 방어 게이트웨이에서 GCP 기록 인스턴스로 로그를 전송하려면 로그 작성자 권한이 필요합니다.

다음은 이 서비스 어카운트를 생성하는 두(2) 가지 방법입니다.

단계 **1** GCP 프로젝트에서 **IAM**을 엽니다.

단계 **2** **Service Accounts(**서비스 어카운트**)**를 클릭합니다.

단계 **3** **Service Account(**서비스 어카운트**)**를 생성합니다.

단계 **4** 이름 및 ID(예: 멀티 클라우드 방어-firewall)를 제공하고 **Create(**생성**)**를 클릭합니다.

단계 **5** **Secret Manager(**암호 관리자**)**, **Secret Accessor(**암호 접속자**)** 및 **Logs Writer roles(**로그 작성자 역할**)**를 추가합니다.

단계 **6** **Continue(**계속**)**를 클릭합니다.

단계 **7** **Done(**완료**)**을 클릭합니다.

Note 사용자를 추가할 필요는 없습니다.

API 활성화

GCP 콘솔 또는 클라우드 서비스 공급자의 CLI를 사용하여 멀티 클라우드 방어 컨트롤러과(와) GCP 계정 간의 통신에 API를 활성화할 수 있습니다.

API 활성화-GCP 클라우드 콘솔 사용

멀티 클라우드 방어 컨트롤러가 멀티 클라우드 방어 게이트웨이(가상 머신, 로드 밸런서)를 생성할 수 있도록 프로젝트/계정에서 API를 활성화합니다.

단계 **1** 검색 창에서 **Compute Engine API**를 검색합니다.

단계 **2** **Enable(**활성화**)**을 클릭합니다.

단계 **3** 검색 창에서 **Secret Manager API**를 검색합니다.

단계 **4** **Enable(**활성화**)**을 클릭합니다.

단계 **5** 검색 창에서 **Identity and Access Management(IAM) API**를 검색합니다.

단계 **6** **Enable(**활성화**)**을 클릭합니다.

단계 **7** 검색 창에서 **Cloud Resource Manager API**를 검색합니다.

단계 **8** **Enable(**활성화**)**을 클릭합니다.

VPC 설정

멀티 클라우드 방어 게이트웨이 인스턴스는 엣지 또는 허브 모드에서 구축할 수 있습니다. 엣지 모드에서 게이트웨이 인스턴스는 애플리케이션과 동일한 VPC에서 실행됩니다. 이 문서에서는 엣지 모드에서 멀티 클라우드 방어 게이트웨이을 구축하기 위해 준비하는 방법을 중점적으로 설명합니다.

VPC 및 서브넷

멀티 클라우드 방어 게이트웨이 구축 시 멀티 클라우드 방어 컨트롤러에서 관리 및 데이터 경로 VPC 정보를 입력하라는 메시지가 표시됩니다. 멀티 클라우드 방어 게이트웨이 인스턴스에는 2개의 네트워크 인터페이스가 필요합니다. GCP에서 VM 인스턴스의 네트워크 인터페이스는 다른 서브넷에만 있을 수 있는 다른 클라우드 제공자와 달리 다른 VPC에 있어야 합니다. 애플리케이션이 실행 중인 VPC가 이미 있는 경우에는 데이터 경로 VPC 및 서브넷이 있습니다. 관리를 위해 다른 VPC를 생성하거나 다른 기존 VPC를 사용해야 합니다. 자동 생성된 서브넷을 사용하거나 수동으로 생성할 수 있습니다.

*datapath vpc*는 애플리케이션이 실행 중인 *VPC*이며 다음 섹션에서 지칭합니다.

각 VPC에서 멀티 클라우드 방어에는 데이터 경로용 서브넷 1개와 관리용 서브넷 1개가 필요합니다.

관리 서브넷은 인터넷에 대한 기본 경로가 있는 라우트 테이블과 연결해야 하는 퍼블릭 서브넷입니다. 멀티 클라우드 방어 게이트웨이 인스턴스에 멀티 클라우드 방어 컨트롤러과(와)의 통신에 사용하는 이 서브넷에 연결된 인터페이스가 있습니다. 이 인터페이스는 멀티 클라우드 방어 컨트롤러 및 멀티 클라우드 방어 게이트웨이 인스턴스 간의 정책 푸시와 기타 관리, 텔레메트리 활동에 사용됩니다. 고객 애플리케이션 트래픽은 이 인터페이스 및 서브넷을 통과하지 않습니다. 인터페이스는 아래의

네트워크 태그 섹션에서 설명하는멀티 클라우드 방어**-management** 네트워크 태그(또는 팀 요구 사항에 기반한 모든 태그)와 연결되어 있습니다.

데이터 경로 서브넷은 인터넷에 대한 기본 경로가 있는 라우트 테이블과 연결해야 하는 퍼블릭 서브넷입니다. 멀티 클라우드 방어 컨트롤러은(는) 이 서브넷에 네트워크 로드 밸런서(NLB)를 생성합니다. 또한, 멀티 클라우드 방어 게이트웨이 인스턴스에 이 서브넷에 연결된 인터페이스가 있습니다. 고객 애플리케이션 트래픽은 이 인터페이스를 통해 흐릅니다. 이 인터페이스를 통해 인그레스하는 트래픽에 보안 정책이 적용됩니다. 인터페이스는 아래의 네트워크 태그 섹션에서 설명하는멀티 클라우드 방어**-datapath** 네트워크 태그(또는 팀 요구 사항에 기반한 모든 태그)와 연결되어 있습니다.

*CLI*를 사용하여 샘플 *VPC* 및 서브넷

다음 명령을 예로 들어 고유한 명령을 실행하여 GCP 어카운트에 대한 VPC를 생성하겠습니다. 다음 특정 명령에 대해 Google Cloud Shell 창을 엽니다.

단계 **1** VPC 앱 및 서브넷 **apps-us-east1**을 생성합니다.

단계 **2** VPC `멀티 클라우드 방어-mgmt` 및 서브넷 `멀티 클라우드 방어-mgmt-us-east1`을 생성합니다.

단계 **3** 대상 태그가 `멀티 클라우드 방어-mgmt`인 VPC `멀티 클라우드 방어-mgmt`용 방화벽 규칙을 2개 이상 생성합니다.

1. 모든 아웃바운드 트래픽을 허용하는 이그레스 규칙.
2. 방화벽 인스턴스에 대한 SSH를 허용하는 인그레스 규칙.

단계 **4** VPC 앱에 대한 방화벽 규칙을 3개 이상 생성합니다. 다음의 사례를 예로 들 수 있습니다.

1. target-tags가 `멀티 클라우드 방어datapath`인 모든 아웃바운드 트래픽을 허용하는 하나의 이그레스 규칙.
2. target-tags가 `멀티 클라우드 방어-datapath`인 게이트웨이 인스턴스로의 HTTP 및 HTTPS를 허용하는 하나의 인그레스 규칙.
3. target-tags가 `app-instance`인 모든 아웃바운드 트래픽을 허용하는 하나의 이그레스 규칙.
4. `target-tags`가 `app-instance`인 `tcp:8000`을 허용하는 하나의 인그레스 규칙.

```
gcloud config set project <project-name> # incase the project is not set in the gcloud cli shell
gcloud compute networks create apps --subnet-mode custom
gcloud compute networks subnets create apps-us-east1 --network apps --range 10.0.0.0/24 --region us-east1
gcloud compute networks create ciscomcd-mgmt --subnet-mode custom
gcloud compute networks subnets create ciscomcd-mgmt-us-east1 --network ciscomcd-mgmt --range 172.16.0.0/24
 --region us-east1
gcloud compute firewall-rules create ciscomcd-mgmt-out --direction EGRESS --network ciscomcd-mgmt \
    --target-tags ciscomcd-mgmt --allow tcp,udp
gcloud compute firewall-rules create ciscomcd-mgmt-in --direction INGRESS --network ciscomcd-mgmt \
    --target-tags ciscomcd-mgmt --allow tcp:22
gcloud compute firewall-rules create ciscomcd-datapath-out --direction EGRESS --network apps \
    --target-tags ciscomcd-datapath --allow tcp,udp
gcloud compute firewall-rules create ciscomcd-datapath-in --direction INGRESS --network apps \
    --target-tags ciscomcd-datapath --allow tcp:80,tcp:443
gcloud compute firewall-rules create app-instance-out --direction EGRESS --network apps \
    --target-tags app-instance --allow tcp,udp
gcloud compute firewall-rules create app-instance-in --direction INGRESS --network apps \
    --target-tags app-instance --allow tcp:8000,tcp:22
```

위 명령을 실행한 후에는 앱 VPC에서 VM 인스턴스를 만들고 포트 8000에서 테스트 웹 애플리케이션을 시작할 수 있습니다.

```
gcloud compute instances create app-instance1 \
  --zone=us-east1-b \
  --image-project=ubuntu-os-cloud \
  --image-family=ubuntu-2004-lts \
  --network apps \
  --subnet=apps-us-east1 \
  --tags=app-instance
gcloud compute ssh app-instance1 --zone us-east1-b
echo hello world > index.html
python3 -m http.server 8000
```

네트워크 태그(**GCP** 게이트웨이용)

관리 및 데이터 경로 네트워크 태그는 위의 서브넷 섹션에서 설명한 대로 멀티 클라우드 방어 게이트웨이 인스턴스의 각 인터페이스와 연결됩니다.

관리 VPC에서 게이트웨이 규칙을 생성하고 이를 멀티 클라우드 방어**-management** 네트워크 태그와 연결합니다. 이렇게 하면 게이트웨이 인스턴스가 컨트롤러와 통신하도록 하는 모든 아웃바운드 트래픽을 허용해야 합니다. 선택적으로, 인바운드 규칙의 경우 포트 22(SSH)를 활성화하여 게이트웨이 인스턴스에 대한 SSH 액세스를 허용합니다. 멀티 클라우드 방어 방화벽이 제대로 작동하기 위해 SSH가 반드시 필요한 것은 아닙니다.

데이터 경로 VPC에서 게이트웨이 규칙을 생성하고 이를 멀티 클라우드 방어**-datapath** 네트워크 태그와 연결합니다. 이렇게 하면 활성화한(활성화할 예정) 모든 서비스에 대한 멀티 클라우드 방어 게이트웨이의 트래픽을 허용해야 합니다.

예를 들어 애플리케이션이 포트 3000에서 실행 중이며 포트 443에서 멀티 클라우드 방어 게이트웨이에 의해 프록시되는 경우, 멀티 클라우드 방어-datapath 네트워크 보안 태그에서 포트 443을 열어야 합니다.

게이트웨이 생성

멀티 클라우드 방어 게이트웨이 생성 페이지에서 다음 매개변수를 사용합니다.

1. 데이터 경로 VPC: **apps**.
2. 데이터 경로 네트워크 태그: 멀티 클라우드 방어**-datapath**.
3. 관리 VPC: 멀티 클라우드 방어**-mgmt**.
4. 관리 네트워크 태그: 멀티 클라우드 방어**-mgmt**.
5. **us-east1-b** 영역을 사용합니다.
6. 관리 서브넷: 멀티 클라우드 방어**-mgmt-us-east1**.
7. 데이터 경로 서브넷: **apps-us-east1**.

다른 지역에 서브넷을 생성하여 멀티 클라우드 방어 게이트웨이을 다중 가용성 영역 모드에서 테스트할 수 있습니다.

Azure 구독 수동 온보딩

멀티 클라우드 방어 컨트롤러 대시보드에서 제공되는 스크립트를 사용하여 Azure 구독을 직접 연결할 수 없는 경우 아래 워크플로우를 사용하여 구독을 수동으로 연결합니다.

(선택 사항) 키 저장소 및 Blob 저장소 액세스를 위해 사용자가 할당하는 관리 ID

멀티 클라우드 방어 게이트웨이은(는) 선택적으로 Azure 키 저장소와 통합하여 TLS 인증서를 검색하고, PCAP(패킷 캡처) 파일을 저장하기 위해 Blob 저장소와 통합할 수 있습니다. 사용자가 할당하는 관리형 ID는 이러한 서비스에 대한 액세스 권한을 부여하는 데 사용됩니다.

Azure Portal에서 **Managed Identities(**관리되는 **ID)**로 이동하여 ID를 생성합니다.

또는 Azure Cloud Shell에서 다음 명령을 실행합니다.

```
az identity create -g <RESOURCE GROUP> -n <USER ASSIGNED IDENTITY NAME>
```

Azure 키 저장소에서 TLS 인증서 암호를 생성하는 방법에 대한 자세한 내용은 Azure 키 저장소, on page 127의 내용을 참조하십시오.

Azure Active Directory에 애플리케이션 등록

단계 **1** **Azure Active Directory**로 이동합니다.

단계 **2** **App registrations(**앱 등록**)**를 선택합니다.

단계 **3** **New registration(**새 등록**)**을 클릭합니다.

단계 **4** 새 앱 등록을 참조할 이름을 제공합니다. 예를 들어 멀티 클라우드 방어 컨트롤러. *Supported account types(*지원되는 계정 유형*)*에서 두 번째 옵션인 *Accounts in any organizational directory(*조직 디렉터리의 계정*)*를 선택합니다.

단계 **5** 조직에 적절한 옵션을 선택합니다. **Redirect URI(**리디렉션 **URI)**는 앱 등록을 생성하는 데 필요하지 않습니다.

단계 **6** **Register(**등록**)**를 클릭합니다.

단계 **7** 새로 생성된 애플리케이션 아래의 왼쪽 탐색 모음에서 **Certificates and secrets(**인증서 및 암호**)**를 클릭합니다.

단계 **8** **+ New client secret(+** 새 클라이언트 비밀번호**)**를 클릭한 다음 *Add client secret(*클라이언트 비밀번호 추가*)* 대화 상자에 필요한 정보를 입력합니다.

- **Description(**설명**)**- 설명을 추가합니다(예: 멀티 클라우드 방어-controller-secret1).
- **Expires(**만료**) - Never(**안 함**)**를 선택합니다. 또한 편의에 따라 선택할 수 있습니다. 현재 암호가 만료되면 새 암호를 생성해야 함)를 선택합니다.

단계 **9** **Add(**추가**)**를 클릭합니다. 클라이언트 비밀이 **Value(**값**)** 열에 채워집니다.

단계 **10** 클라이언트 비밀은 한 번만 표시되고 다시 표시되지 않으므로 메모장에 복사합니다.

단계 **11** 왼쪽 내비게이션 바에서 **Overview(**개요**)**를 클릭합니다.

단계 **12** 애플리케이션**(**클라이언트**) ID** 및 디렉터리**(**테넌트**) ID**를 메모장에 복사합니다.

애플리케이션에 할당할 사용자 지정 역할 생성

멀티 클라우드 방어 컨트롤러를 위해 생성된 애플리케이션에 할당할 맞춤형 역할을 생성합니다. 사용자 지정 역할은 인벤토리 목록 정보를 읽고 리소스(예: VM, 로드 밸런서 등)를 생성할 수 있는 애플리케이션 권한을 제공합니다. 사용자 지정 역할은 여러 방법으로 생성할 수 있습니다.

단계 **1** **Subscription(**구독**)**으로 이동하여 **Access Control (IAM)(**액세스 제어**(IAM))**을 클릭합니다.

단계 **2** **Roles(**역할**)**를 클릭하고 상단 메뉴 모음에서 **+Add(+**추가 **)** > **Add Custom Role(**맞춤형 역할 추가**)**로 이동하여 클릭합니다.

단계 **3** 맞춤형 역할에 이름을 지정합니다(예: `멀티 클라우드 방어-controller-role`).

단계 **4** JSON 편집 화면이 표시될 때까지 **Next(**다음**)**를 계속 클릭합니다.

단계 **5** 화면에서 **Edit(**편집**)**를 클릭하고 JSON 텍스트에서 **permissions(**권한**) > Action(**작업**)** 섹션 아래의 다음 내용을 복사하여 대괄호 사이에 붙여넣습니다(들여쓰기는 유지할 필요 없음).

```
"Microsoft.ApiManagement/service/*",
"Microsoft.Compute/disks/*",
"Microsoft.Compute/diskEncryptionSets/read",
"Microsoft.Compute/images/read",
"Microsoft.Compute/sshPublicKeys/read",
"Microsoft.Compute/virtualMachines/*",
"Microsoft.ManagedIdentity/userAssignedIdentities/read",
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
"Microsoft.Network/loadBalancers/*",
"Microsoft.Network/locations/serviceTags/read",
"Microsoft.Network/networkinterfaces/*",
"Microsoft.Network/networkSecurityGroups/*",
"Microsoft.Network/publicIPAddresses/*",
"Microsoft.Network/routeTables/*",
"Microsoft.Network/virtualNetworks/*",
"Microsoft.Resources/subscriptions/resourcegroups/*",
"Microsoft.Storage/storageAccounts/blobServices/*",
"Microsoft.Storage/storageAccounts/listkeys/action",
"Microsoft.Network/networkWatchers/*",
"Microsoft.Network/applicationSecurityGroups/*",
"Microsoft.Compute/diskEncryptionSets/read",
"Microsoft.Insights/Metrics/Read"
```

단계 **6** 선택 사항 - 여러 구독을 멀티 클라우드 방어과(와) 함께 사용하려는 경우 `assignableScopes`에서 JSON을 편집하여 다른 구독 라인을 추가하거나 모든 구독에 사용자 지정 역할을 사용할 수 있도록 *****(별표)로 변경해야 합니다.

단계 **7** 텍스트 상자 맨 위에서 **Save(**저장**)**를 클릭합니다.

단계 **8** **Review + Create(**검토 + 생성**)**를 클릭하고 역할을 생성합니다.

단계 **9** Custom Role(사용자 지정 역할)이 생성되면 **Access Control(IAM)(**액세스 제어**(IAM))**으로 돌아갑니다.

단계 **10** 상단 메뉴 모음에서 **Add(**추가**)** > **Add role assignment(**역할 할당 추가**)**를 클릭합니다.

단계 **11** **Role(**역할**)** 드롭다운에서 위에서 생성한 Custom Role(사용자 지정 역할)을 선택합니다.

단계 **12** **Assign access to(**액세스 권한 할당 대상**)** 드롭다운에서 이를 기본값(Azure AD 사용자, 그룹, 서비스 주체)으로 유지합니다.

단계 **13** **Select(**선택**)** 텍스트 상자에 이전에 생성한 애플리케이션 이름(예: `멀티 클라우드 방어controllerapp`)을 입력하고 **Save(**저장**)**를 클릭합니다.

단계 **14** **Subscription(**구독**)** 페이지의 왼쪽 메뉴 모음에서 **Overview(**개요**)**를 클릭하고 구독 ID를 메모장에 복사합니다.

멀티 클라우드 방어 컨트롤러 온보딩에 필요한 값

계속 진행하기 전에 다음 정보가 있는지 확인하십시오.

- 구독 ID(*subscription overview(*구독 개요*)* 페이지)
- 디렉터리(테넌트) ID(*Azure AD app overview(Azure AD* 앱 개요*)* 페이지)
- 애플리케이션(클라이언트) ID(*Azure AD app overview(Azure AD* 앱 개요*)* 페이지)
- 클라이언트 암호(클라이언트 암호 생성 시 복사됨)

마켓플레이스 약관 동의

멀티 클라우드 방어 컨트롤러는 Azure Marketplace에서 멀티 클라우드 방어 VM(가상 머신) 이미지를 사용하여 게이트웨이 인스턴스를 생성합니다. 각 구독에 대해 약관에 동의해야 합니다. Azure 포털 웹사이트(오른쪽 상단 메뉴 모음)에서 Azure Cloud 쉘을 엽니다. Bash 쉘을 선택하거나 전환하고 다음 명령을 실행합니다(subscription-id를 이전 섹션에서 복사한 구독 ID로 대체).

```
az vm image terms accept --publisher valtix --offer datapath --plan valtix_dp_image
--subscription subscription-id
```

클라우드 어카운트용 **Terraform** 온보딩 스크립트

온보딩 마법사 또는 수동 프로세스를 사용하는 대신 terraform 스크립트를 사용하여 클라우드 서비스 제공자 어카운트를 온보딩합니다.

Terraform 정보

멀티 클라우드 방어고객은 **Terraform Provider**를 사용하여 검색 - 퍼블릭 클라우드 어카운트 온보딩, 지속적인 자산 가시성 확보, 침해 지표(IoC) 탐지, 구축 - 멀티 클라우드 방어 게이트웨이에서 인그레스, 이스트-웨스트 트래픽 보호, 방어 - 지속적으로 검색되는 클라우드 자산으로 멀티 클라우드(AWS, Azure, GCP, OCI) 동적 정책으로 방어 등의 작업을 수행할 수 있습니다.

Attention 멀티 클라우드 방어 컨트롤러 버전 23.10부터는 Terraform 제공자를 사용하여 GCP 폴더와 GCP 프로젝트를 연결할 수 있습니다. 자세한 내용은 Terraform 저장소, on page 292를 참조하십시오.

멀티 클라우드 방어 Terraform 제공자는 Terraform 레지스트리에서 제공되는 "확인된" 제공자입니다. 이제 고객은 멀티 클라우드 방어용 Terraform 제공업체를 사용하여 클라우드 어카운트를 멀티 클라우드 방어에 온보딩하고, 멀티 클라우드 방어 게이트웨이를 구축하고, 인터넷으로부터의 인그레스

공격(WAF, IDS/IPS, Geo-IP)을 방어하고, 송신 트래픽의 유출을 차단하고(TLS 암호 해독, IDS/IPS, AV, DLP, FQDN/URL 필터링), VPC/VNet 간의 이스트-웨스트 공격을 방지하기 위한 보안 정책을 지정하여 보안을 운영에 통합할 수 있습니다. 클라우드 자산 태그를 기반으로 보안 정책을 지정할 수 있습니다(예: "dev", "test", "prod", "pci", "web", "app1" 등).

자세한 내용은 다음을 참조하십시오.

- 멀티 클라우드 방어용 Terraform 제공자를 다운로드합니다.
- GitHub의 예.
- Terraform의 멀티 클라우드 방어 블로그.

Terraform 저장소

활용 사례	설명	Github 저장소
AWS 온보딩	Terraform을 사용하여 AWS 계정을 온보딩하기 위한 것입니다.	Github 저장소
AWS 검색 CFT	이 CFT 구축에는 멀티 클라우드 방어의 검색 기능을 사용하는 데 필요한 모든 권한이 포함됩니다. 전체 기능 집합을 보려면 제품 CFT를 사용하십시오.	Github 저장소
AWS 검색	이 모드는 Terraform을 사용하는 검색 전용 모드로 AWS 계정을 온보딩하기 위한 것입니다.	Github 저장소
Azure 온보딩	Terraform을 사용하여 Azure 구독을 온보딩하는 데 사용됩니다.	Github 저장소
GCP 프로젝트 온보딩	Terraform을 사용하여 GCP 프로젝트를 온보딩하기 위한 것입니다.	Github 저장소
GCP 폴더 온보딩	Terraform을 사용하여 GCP 폴더를 온보딩하기 위한 것입니다.	Github 저장소

설정을 Terraform 블록으로 내보내기

고객은 보안 프로파일을 멀티 클라우드 방어 컨트롤러에서 Terraform 리소스 블록으로 내보낼 수 있습니다. 설정을 Terraform 블록으로 내보내려면 원하는 보안 프로파일로 이동하여 선택한 다음 **Export(**내보내기**)** 버튼을 클릭합니다. 이렇게 하면 선택한 개체/보안 프로파일에 대한 Terraform 블록이 포함된 파일이 다운로드됩니다.

다음을 제외한 모든 개체 및 프로파일은 terraform 내보내기를 지원합니다.

- 게이트웨이
- 서비스 VPC/VNet
- 진단