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 ***1:*** 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.

번역에 관하여
Cisco는 일부 지역에서 본 콘텐츠의 현지 언어 번역을 제공할 수 있습니다. 이러한 번역은 정보 제공의 목적으로만 제공되며, 불일치가 있는 경우 본 콘텐츠의 영어 버전이 우선합니다.