Flow Analytics

Flow Analytics - Traffic Summary

This view provides detailed visibility, filtering and analysis for events recorded by Multicloud Defense from either a forward or reverse gateway proxy. Traffic Summary events contribute to one of three event types: `Firewall Events`, `Network Events` and `Web Attacks`.

The summary page shows both closed and ongoing sessions; select "All events" in the traffic summary page and this selection will list all events including closed and the periodic 5 minute events for long running sessions.

Traffic Summary

Tables and Fields available in Session Summary are as follows:

Event Details	Description
Date and Time	ISO 8601 format: YYYY-MM-DD T HH:MM:SS:S Example: `2020-11-22T10:58:46.820`
CSP Account	Multicloud Defense CSP Account
Gateway	Multicloud Defense Gateway
Region	Region of the Multicloud Defense Gateway

Event Details	Description
Level	INFO
Session ID	..

Client-side Connection	Description
Src IP	Source IP Address
Src Port	Source Port
Dest IP	Destination IP Address
Dest Port	Destination Port
Protocol	UDP, TCP

Client-side Stats	Traffic between client and Multicloud Defense Gateway
Received Bytes	Number of bytes received from client
Transmitted Bytes	Number of bytes sent to client
Received Packets	Number of packets received from client
Transmitted Packets	Number of packets sent to client

Policy Match Info	Description
Dest Address Group	Destination Address Group configured in the matched policy rule
Src Address Group	Source Address Group configured in the matched policy rule
Request SNI	Server Name Indication in the request
Service Type	Service Type. Example: `PROXY`
Src Country	Country that the request originated from on the client-side
Dest Country	Country that the request was destined to on the server-side. Example: `United States`

Server-side Connection	Description
Src IP	Source IP Address
Src Port	Source Port
Dest IP	Destination IP Address
Dest Port	Destination Port

Server-side Connection	Description
Protocol	UDP, TCP

Server-side Stats	Traffic between Multicloud Defense Gateways and server
Received Bytes	Number of bytes received from server
Transmitted Bytes	Number of bytes sent to server
Received Packets	Number of packets received from server
Transmitted Packets	Number of packets sent to server

Application Info	Description
Client App Name	Application name associated with client side of the session. Example: `Advanced Packaging Tool`
Payload App Name	HTTP application name associated with webserver host. Example: `Facebook`
Service App Name	Application name associated with server side of the session. Example: `HTTP`

Action	Description
Action	ALLOW, DENY

Cloud Service	Description
Cloud Service	Name of the destination cloud service accessed with the request. Example `AMAZON, EC2`

Src Instance Info	Description
Instance ID	Client instance ID
Instance Name	Client instance name (and provides ability to see tags)
VPC ID	Client VPC ID

HTTP Request	Description
Host	Host portion of URL
Method	GET, PUT, POST, HEAD, DELETE, PATCH, OPTIONS
URI	URI Identifier RFC 3986

Rule	Description
ID	ID number/description of Multicloud Defense Rule. Example `59 (egress-prod-apt-80).`

FQDN	Description
FQDN	Fully Qualified Domain Name
Category Name	Category classification of the FQDN. Example: `Social Media`
Reputation	Reputation score of the FQDN

Flow Analytics - All Events

Flow Analytics - All Events provides overall visibility into network and security events from the entire Multicloud Defense solution.

Tables and Fields available in All Events are as follows:

Event Details	Description
Date and Time	ISO 8601 format: YYYY-MM-DD T HH:MM:SS:S Example: `2020-11-22T10:58:46.820.`
Type	APPID, AV, DLP, DPI, FLOW_LOG, FQDNFILTER, L4_FW, L7DOS, MALICIOUS_SRC, SNI, TLS_ERROR, TLS_LOG, URLFILTER.
CSP Account	Multicloud Defense CSP Account.
Gateway	Multicloud Defense Gateway.
Region	Region of the Multicloud Defense Gateway.
Level	DEBUG, INFO, NOTICE, WARNING, ERROR, CRITICAL, ALERT, EMERGENCY.
Session ID	..

Service	Description
Src IP	Source IP Address.
Src Port	Source Port.
Dest IP	Destination IP Address.
Dest Port	Destination Port.
Protocol	UDP, TCP.

Application Info	Description
Client App Name	Application name associated with client side of the session. Example: `Advanced Packaging Tool`.
Payload App Name	HTTP application name associated with webserver host. Example: `Facebook`.
Service App Name	Application name associated with server side of the session. Example: `HTTP`.

Action	Description
Action	ALLOW, DENY.
State	ESTABLISHED, CLOSE, CLOSED, CLOSE_WAIT, TIME_WAIT, FIN_WAIT, LAST_ACK.

HTTP Request	Description
Host	Host portion of URL.
Method	GET, PUT, POST, HEAD, DELETE, PATCH, OPTIONS.
URI	URI Identifier RFC 3986.

Rule	Description
ID	ID number/description of Multicloud Defense Rule. Example `59 (egress-prod-apt-80)`.

FQDN	Description
FQDN	Fully Qualified Domain Name.
Category Name	Category classification of the FQDN. Example: `Social Media`.
Reputation	Reputation score of the FQDN.

Event Logs

Event logs contain details of all traffic that flows through the Multicloud Defense Gateway.

After inspection, Multicloud Defense generates sessions and events that are based on what is in the packet and what is defined in the policy. The analysis, related details of events, and actions that are taken are all captured in the form of logs, available under **Investigate** > **Flow Analytics** > **All Events**. The system retains these logs for 30 days.

Event types that the logs capture:

Table 1: Event Types and Descriptions

Event Type	Event Name	Description
FQDN FILTER	Fully Qualified Domain Name (FQDN) Filtering	The related logs generate with details of the FQDN, source, destination IP and so on. The FQDN filtering event only generates in case the policy has an FQDN filtering profile.
SNI	Server Name Indication (SNI)	SNI allows multiple host names to be served over HTTPS. This generates when Multicloud Defense observes the SNI in the TLS handshake.
APPID	App ID (APPID)	APPID analyzes the network traffic to determine the L7 application. APPID logs generate when the event matches known applications in the database.
L4_FW	L4 Firewall	An L4 Firewall event generates when the event matches the policy in the ruleset.
URL FILTER	URL Filtering	URL filtering is used to filter out network traffic based on the URL. This event log generates when it matches the URL filtering profile.
IPS	Intrusion Prevention System (IPS)	An IPS event generates when the network traffic matches the IPS ruleset.
DLP	Data Loss Protection (DLP)	A DLP event generates when the network traffic matches the DLP profile that is configured. The logs record these incidents, along with details of transmission such as endpoint, domain, username, rules, source, destination, action taken, and so on.
WAF	Web Application Firewall	A WAF event generates when the network traffic matches the WAF profile that is configured.
L7_DOS	Layer 7 Denial of Service (DoS)	A Layer 7 DoS event generates when the network traffic matches the L7 DoS profile that is configured. These logs contain event details, time of attack, requests, mitigations, and so on.
AV	Antivirus (AV)	An AV event generates when the event matches an AV ruleset in the network traffic.
DPI	Deep Packet Inspection (DPI)	A DPI event generates when the network traffic matches a rule that has an advanced security configured.
MALICIOUS_SRC	Malicious Source	A Malicious Source generates when the network traffic matches a malicious IP.

Event Type	Event Name	Description
TLS_ERROR	TLS Error	A TLS error generates when there is an error during the TLS handshake.
TLS_LOG	TLS Log	A TLS log generates when the network traffic uses TLS. This captures the TLS handshake information such as cipher suites and TLS version.

Firewall Events

This view provides detailed visibility, filtering and analysis for events recorded by the Multicloud Defense Firewall configuration and summarized in `Firewall Events` category.

Tables and Fields available in Firewall Events are as follows:

Event Details	Description
Date and Time	ISO 8601 format: YYYY-MM-DD T HH:MM:SS:S Example: `2020-11-22T10:58:46.820`
Type	APPID, L4_FW, MALICIOUS_SRC, SNI
CSP Account	Multicloud Defense CSP Account
Gateway	Multicloud Defense Gateway
Region	Region of the Multicloud Defense Gateway
Level	DEBUG, INFO, NOTICE, WARNING, ERROR, CRITICAL, ALERT, EMERGENCY
Session ID	..

Service	Description
Src IP	Source IP Address
Src Port	Source Port
Dest IP	Destination IP Address
Dest Port	Destination Port
Protocol	UDP, TCP

Application Info	Description
Client App Name	Application name associated with client side of the session. Example: `Advanced Packaging Tool`

Application Info	Description
Payload App Name	HTTP application name associated with webserver host. Example: `Facebook`
Service App Name	Application name associated with server side of the session. Example: `HTTP`

Action	Description
Action	ALLOW, DENY
State	ESTABLISHED, CLOSE, CLOSED, CLOSE_WAIT, TIME_WAIT, FIN_WAIT, LAST_ACK

HTTP Request	Description
Host	Host portion of URL
Method	GET, PUT, POST, HEAD, DELETE, PATCH, OPTIONS
URI	URI Identifier RFC 3986

Rule	Description
ID	ID number/description of Multicloud Defense Rule. Example 59 (egress-prod-apt-80)

FQDN	Description
FQDN	Fully Qualified Domain Name
Category Name	Category classification of the FQDN. Example: `Social Media`
Reputation	Reputation score of the FQDN

Network Threats

This view provides detailed visibility, filtering and analysis for threats recorded by the Multicloud Defense threat analysis engine and summarized in `Network Threats`.

Network Threats

Tables and Fields available in Network Threats are as follows:

Event Details	Description
Date and Time	ISO 8601 format: YYYY-MM-DD T HH:MM:SS:S Example: `2020-11-22T10:58:46.820`
Type	AV, DLP, DPI

Event Details	Description
CSP Account	Multicloud Defense CSP Account
Gateway	Multicloud Defense Gateway
Region	Region of the Multicloud Defense Gateway
Level	DEBUG, INFO, NOTICE, WARNING, ERROR, CRITICAL, ALERT, EMERGENCY
Session ID	..

Service	Description
Src IP	Source IP Address
Src Port	Source Port
Dest IP	Destination IP Address
Dest Port	Destination Port
Protocol	UDP, TCP

Application Info	Description
Client App Name	Application name associated with client side of the session. Example: `Advanced Packaging Tool`
Payload App Name	HTTP application name associated with webserver host. Example: `Facebook`
Service App Name	Application name associated with server side of the session Example: `HTTP`

Action	Description
Action	ALLOW, DENY
State	ESTABLISHED, CLOSE, CLOSED, CLOSE_WAIT, TIME_WAIT, FIN_WAIT, LAST_ACK

HTTP Request	Description
Host	Host portion of URL
Method	GET, PUT, POST, HEAD, DELETE, PATCH, OPTIONS
URI	URI Identifier RFC 3986

FQDN	Description
FQDN	Fully Qualified Domain Name
Category Name	Category classification of the FQDN. Example: `Social Media`
Reputation	Reputation score of the FQDN

Rule	Description
ID	ID number/description of Multicloud Defense Rule. Example 59 (egress-prod-apt-80)

Web Attacks

This view provides detailed visibility, filtering and analysis for threats recorded by the Multicloud Defense web protection engine. The `Web Attacks` event types include WAF and L7 DOS.

Tables and Fields available in Web Attacks are as follows:

Event Details	Description
Date and Time	ISO 8601 format: YYYY-MM-DD T HH:MM:SS:S Example: `2020-11-22T10:58:46.820`
Type	L7DOS, WAF
CSP Account	Multicloud Defense CSP Account
Gateway	Multicloud Defense Gateway
Region	Region of the Multicloud Defense Gateway
Level	DEBUG, INFO, NOTICE, WARNING, ERROR, CRITICAL, ALERT, EMERGENCY
Session ID	..

Service	Description
Src IP	Source IP Address
Src Port	Source Port
Dest IP	Destination IP Address
Dest Port	Destination Port
Protocol	UDP, TCP

Application Info	Description
Client App Name	Application name associated with client side of the session. Example: `Advanced Packaging Tool`
Payload App Name	HTTP application name associated with webserver host. Example: `Facebook`
Service App Name	Application name associated with server side of the session Example: `HTTP`

Action	Description
Action	ALLOW, DENY
State	ESTABLISHED, CLOSE, CLOSED, CLOSE_WAIT, TIME_WAIT, FIN_WAIT, LAST_ACK

HTTP Request	Description
Host	Host portion of URL
Method	GET, PUT, POST, HEAD, DELETE, PATCH, OPTIONS
URI	URI Identifier RFC 3986

FQDN	Description
FQDN	Fully Qualified Domain Name
Category Name	Category classification of the FQDN. Example: `Social Media`
Reputation	Reputation score of the FQDN

Rule	Description
ID	ID number/description of Multicloud Defense Rule. Example 59 (egress-prod-apt-80)

URL Filtering

This view provides detailed visibility, filtering and analysis for events recorded by the Multicloud Defense URL Filtering configuration. URL Filtering events contribute to one of three event types: `Firewall Events`, `Network Events` and `Web Attacks`.

Event Details	Description
Date and Time	ISO 8601 format: YYYY-MM-DD T HH:MM:SS:S Example: `2020-11-22T10:58:46.820`
Type	URLFILTER

Event Details	Description
CSP Account	Multicloud Defense CSP Account
Gateway	Multicloud Defense Gateway
Region	Region of the Multicloud Defense Gateway
Level	DEBUG, INFO, NOTICE, WARNING, ERROR, CRITICAL, ALERT, EMERGENCY
Session ID	..

Service	Description
Src IP	Source IP Address
Src Port	Source Port
Dest IP	Destination IP Address
Dest Port	Destination Port
Protocol	UDP, TCP

Application Info	Description
Client App Name	Application name associated with client side of the session. Example: `Advanced Packaging Tool`.
Payload App Name	HTTP application name associated with webserver host. Example: `Facebook`
Service App Name	Application name associated with server side of the session Example: `HTTP`

Action	Description
Action	ALLOW, DENY
State	ESTABLISHED, CLOSE, CLOSED, CLOSE_WAIT, TIME_WAIT, FIN_WAIT, LAST_ACK

HTTP Request	Description
Host	Host portion of URL
Method	GET, PUT, POST, HEAD, DELETE, PATCH, OPTIONS
URI	URI Identifier RFC 3986

Rule	Description
ID	ID number/description of Multicloud Defense Rule. Example 59 (egress-prod-apt-80)

FQDN	Description
FQDN	Fully Qualified Domain Name
Category Name	Category classification of the FQDN. Example: `Social Media`
Reputation	Reputation score of the FQDN

FQDN Filtering

This view provides detailed visibility, filtering and analytical options for events recorded from the FQDN Filtering configuration. FQDN Filtering events contribute to one of three event types: `Firewall Events`, `Network Events` and `Web Attacks`.

Event Details	Description
Date and Time	ISO 8601 format: YYYY-MM-DD T HH:MM:SS:S Example: `2020-11-22T10:58:46.820`.
Type	FQDNFILTER.
CSP Account	Multicloud Defense CSP Account.
Gateway	Multicloud Defense Gateway.
Region	Region of the Multicloud Defense Gateway.
Level	DEBUG, INFO, NOTICE, WARNING, ERROR, CRITICAL, ALERT, EMERGENCY.
Session ID	..

Service	Description
Src IP	Source IP Address.
Src Port	Source Port.
Dest IP	Destination IP Address.
Dest Port	Destination Port.
Protocol	UDP, TCP.

Action	Description
Action	ALLOW, DENY.

Action	Description
State	ESTABLISHED, CLOSE, CLOSED, CLOSE_WAIT, TIME_WAIT, FIN_WAIT, LAST_ACK.

HTTP Request	Description
Host	Host portion of URL.
Method	GET, PUT, POST, HEAD, DELETE, PATCH, OPTIONS.
URI	URI Identifier RFC 3986.

FQDN	Description
FQDN	Fully Qualified Domain Name.
Category Name	Category classification of the FQDN. Example: `Social Media`.
Reputation	Reputation score of the FQDN.

Rule	Description
ID	ID number/description of Multicloud Defense Rule. Example 59 (egress-prod-apt-80).

HTTPS Logs

This view provides detailed visibility, filtering and analytical options for events recorded from HTTPS Logs. HTTPS logs may contribute to one of three event types: `Firewall Events`, `Network Events` and `Web Attacks`.

Event Details	Description
Date and Time	ISO 8601 format: YYYY-MM-DD T HH:MM:SS:S Example: `2020-11-22T10:58:46.820`
Type	TLS_ERROR, TLS_LOG.
CSP Account	Multicloud Defense CSP Account.
Gateway	Multicloud Defense Gateway.
Region	Region of the Multicloud Defense Gateway.
Level	DEBUG, INFO, NOTICE, WARNING, ERROR, CRITICAL, ALERT, EMERGENCY.
Session ID	..

Service	Description
Src IP	Source IP Address.
Src Port	Source Port.
Dest IP	Destination IP Address.
Dest Port	Destination Port.
Protocol	UDP, TCP.

Application Info	Description
Client App Name	Application name associated with client side of the session. Example: `Advanced Packaging Tool`.
Payload App Name	HTTP application name associated with webserver host. Example: `Facebook`.
Service App Name	Application name associated with server side of the session Example: `HTTP`.

Action	Description
Action	ALLOW, DENY.
State	ESTABLISHED, CLOSE, CLOSED, CLOSE_WAIT, TIME_WAIT, FIN_WAIT, LAST_ACK.

HTTP Request	Description
Host	Host portion of URL.
Method	GET, PUT, POST, HEAD, DELETE, PATCH, OPTIONS.
URI	URI Identifier RFC 3986.

FQDN	Description
FQDN	Fully Qualified Domain Name.
Category Name	Category classification of the FQDN. Example: `Social Media`.
Reputation	Reputation score of the FQDN.

VPN Logs

Virtual Private Network (VPN) logs are records of activities and events that occur within a VPN and can provide detailed information about the usage, performance, and security of the connection. VPN logs include connection, usage, activity, error, and security logs. Note that the display shown on this page is directly

dependent on the selected event details. Click the **Edit** icon to modify the display and select from the following options:

Event Details	Description
Date and Time	ISO 8601 format: YYYY-MM-DD T HH:MM:SS:S Example: 2020-11-22T10:58:46.820.
CSP Account	Name of your cloud service account.
Region	Region of the Multicloud Defense Gateway.
Gateway	The Multicloud Defense Gateway involved in the event.
Text	A preview of the text included in the event message. Click an individual message to expand.
Gateway Security Type	Designation of the Multicloud Defense Gateway.
Instance Name	Identifier for a VPN session or connection instance.

EndUser Logs

An EndUser log is a record of interactions and activities performed by end users within an application or service. These logs act as a snapshot of valuable information about user behavior, system usage, and application performance. Implementing this within your network can create insight as to how users interact with their applications, can track application performance from the user's perspective, and has the potential to help detect suspicious activities with proper investigation.

Event Details	Description
Date and Time	ISO 8601 format: YYYY-MM-DD T HH:MM:SS:S Example: 2020-11-22T10:58:46.820.
CSP Account	Name of your cloud service account.
Region	Region of the Multicloud Defense Gateway.
Gateway	The Multicloud Defense Gateway involved in the event.
Session ID	The unique identifier assigned to a user's session when they interact with an application or system.
Text	A preview of the text included in the event message. Click an individual message to expand.
Level	The severity or importance of a logged event. This can help categorize and prioritize entries for easy analyzing.
Src IP	Identifier for a VPN session or connection instance.

Event Details	Description
Dst IP	The destination IP address of a network connection of communication.
Dst Port	The numerical destination port of a network connection or communication.
Payload App Name	The application or component of a system where the user action took place.
Action	The specific operation or event performed by the user within the system.
Policy Name	The name of the policy matching against the user.
Instance Name	The unique identifier or label assigned to that particular instance within an environment.
First Name	The identified first name of the user performing this action.
Last Name	The identified last name of the user performing this action.
Group	The identified group the user performing this action is associated with.
Department	The identified department of the user performing this action.
Method	The action that a client uses to communicate with a server: **GET**, **POST**, **PUT**, **DELETE**, **HEAD**, and so on.
URI	The identifying string of the resource being requested from the server.
FQDN	The FQDN of where the logged event originates from.
Category Name	The the name of the category the logged event is associated as.

HTTP2 Logs

The HTTP2, or HTTP/2, log refers to logging information specifically related to HTTP/2. It is designed to improve the performance and efficiency of data transfer between clients and servers. When logging HTTP/2 activity, the logs capture details about how HTTP/2 protocol features are utilized. This has the potential to provide insights into the performance and behavior of web applications using this protocol This can help developers and administrators optimize resource usage, troubleshoot issues, and ensure efficient data transmission.

Event Details	Description
Date and Time	ISO 8601 format: YYYY-MM-DD T HH:MM:SS:S Example: 2020-11-22T10:58:46.820.
CSP Account	Name of your cloud service account.
Region	Region of the Multicloud Defense Gateway.
Gateway	The Multicloud Defense Gateway involved in the event.
Session ID	The unique identifier assigned to a session.
Text	A preview of the text included in the event message. Click an individual message to expand.
Src IP	Identifier for a VPN session or connection instance.
Dst IP	The destination IP address of a network connection of communication.
Dst Port	The numerical destination port of a network connection or communication.
Payload App Name	The application or component of a system where the HTTP2 communication took place.
Action	The specific operation or type of event that was logged regarding HTTP2 communication.
Policy Name	The name of the policy matching against the HTTP2 log.
Instance Name	The unique identifier or label assigned to that particular HTTP2 activity.
First Name	The identified first name of the user associated with the HTTP2 activity.
Last Name	The identified last name of the user associated with the HTTP2 activity.
Group	The identified user group associated with this HTTP2 activity.
Department	Wwhich department within an organization is responsible for or associated with the logged activity.
FQDN	The FQDN of the server or host involved in the communication.
Category Name	The the name of the category the logged communication is associated as.

AI Guardrails Logs

An AI Guardrails log is a record of the most recent interactions and events triggered by AI Defense. These logs only generate if you have AI Defense enabled on you tenant and you have at least one AI Guardrail profile attachd to your policy. These logs act as a snapshot of valuable information about user behavior, system usage, and application performance of the past 24 hours.

Event Details	Description
Date and Time	ISO 8601 format: YYYY-MM-DD T HH:MM:SS:S Example: 2020-11-22T10:58:46.820.
CSP Account	Name of your cloud service account.
Region	Region of the Multicloud Defense Gateway.
Gateway	The Multicloud Defense Gateway involved in the event.
Text	A preview of the text included in the event message. Click an individual message to expand.
Action	The specific operation or event performed by the user within the system.
Instance Name	The unique identifier or label assigned to that particular instance within an environment.
FQDN	The FQDN of where the logged event originates from.