流分析

流分析 - 流量摘要

此视图为多云防御从转发或反向网关代理记录的事件提供详细的可视性、过滤和分析。流量摘要事件属于三 (3) 种事件类型之一： 防火墙事件、 网络事件 和 网络攻击。

流量摘要

会话摘要中可用的表和字段如下：

事件详细信息	说明
日期和时间	ISO 8601 格式：YYYY-MM-DD T HH:MM:SS:S 示例：`2020-11-22T10:58:46.820`
CSP 账户	多云防御 CSP 账户
Gateway	多云防御网关
地区	多云防御网关的所在地区
Level	INFO
会话 ID	。

客户端连接	说明
源 IP	源 IP 地址
源端口	源端口
目标 IP	目的 IP 地址
目标端口	目标端口 (Destination Port)
协议 (Protocol)	UDP、TCP

客户端统计信息	客户端与 多云防御网关之间的流量
接收的字节数量	从客户端接收的字节数
已发送的字节数	发送到客户端的字节数
接收的数据包	从客户端接收的数据包数
已发送的数据包数	发送到客户端的数据包数

策略匹配信息	说明
目的地址组	匹配的策略规则中配置的目标地址组
源地址组	在匹配的策略规则中配置的源地址组
请求 SNI	请求中的服务器名称指示
服务类型	服务类型。示例： `PROXY`
源国家/地区	在客户端发出请求的国家/地区
目标国家/地区	请求发往服务器端的国家/地区。例如： 美国

服务器端连接	说明
源 IP	源 IP 地址
源端口	源端口
目标 IP	目的 IP 地址
目标端口	目标端口 (Destination Port)
协议 (Protocol)	UDP、TCP

服务器端统计信息	多云防御网关与服务器之间的流量
接收的字节数量	从服务器收到的字节数

服务器端统计信息	多云防御网关与服务器之间的流量
已发送的字节数	发送到服务器的字节数
接收的数据包	从服务器收到的数据包数
已发送的数据包数	发送到服务器的数据包数

应用信息	说明
客户端应用名称	与会话客户端关联的应用名称。示例： 高级打包工具
负载应用名称	与 Web 服务器主机关联的 HTTP 应用名称。示例：Facebook
服务应用名称	与会话服务器端关联的应用名称。示例： HTTP

操作	说明
操作	允许，拒绝

云服务	说明
云服务	通过请求访问的目标云服务的名称。示例 AMAZON、EC2

源实例信息	说明
实例 ID	实例客户端 ID
实例名称	客户端实例名称（并提供查看标签的功能）
VPC ID	客户端 VPC ID

HTTP 请求	说明
Host	URL 的主机部分
方法	GET, PUT, POST, HEAD, DELETE, PATCH, OPTIONS
URI	URI 标识符 RFC 3986

规则	说明
ID	多云防御 规则的 ID 编号/说明。示例 59 (egress-prod-apt-80)。

FQDN	说明
FQDN	域名名称

FQDN	说明
类别名称 (Category Name)	FQDN 的类别分类。示例： 社交媒体
信誉	FQDN 的信誉得分

流分析 - 所有事件

流分析 - 所有事件 提供对整个 多云防御 解决方案的网络和安全事件的整体可视性。

所有事件中可用的表和字段如下：

事件详细信息	说明
日期和时间	ISO 8601 格式：YYYY-MM-DD T HH:MM:SS:S 示例：`2020-11-22T10:58:46.820`。
类型	APPID、AV、DLP、DPI、FLOW_LOG、FQDNFILTER、L4_FW、L7DOS、MALICIOUS_SRC、SNI、TLS_ERROR、TLS_LOG、URLFILTER。
CSP 账户	多云防御 CSP 账户。
Gateway	多云防御网关。
地区	多云防御网关所在的区域。
Level	紧急, 警报, 关键, 错误, 警告, 通知, 信息, 调试。
会话 ID	。

服务	说明
源 IP	源 IP 地址。
源端口	源端口。
目标 IP	目标 IP 地址。
目标端口	目的端口。
Protocol	UDP、TCP。

应用信息	说明
客户端应用名称	与会话客户端关联的应用名称。示例： 高级打包工具。
负载应用名称	与 Web 服务器主机关联的 HTTP 应用名称。示例：`Facebook`。

应用信息	说明
服务应用名称	与会话服务器端关联的应用名称。示例： `HTTP`。

操作	说明
操作	允许，拒绝。
状态	ESTABLISHED、CLOSE、CLOSED、CLOSE_WAIT、TIME_WAIT、FIN_WAIT、LAST_ACK。

HTTP 请求	说明
Host	URL 的主机部分。
方法	GET、PUT、POST、HEAD、DELETE、PATCH、OPTIONS。
URI	URI 标识符 RFC 3986。

规则	说明
ID	多云防御 规则的 ID 编号/说明。示例 `59 (egress-prod-apt-80)`。

FQDN	说明
FQDN	完全限定域名。
类别名称 (Category Name)	FQDN 的类别分类。示例： 社交媒体。
信誉	FQDN 的信誉得分。

流分析 - 防火墙事件

此视图提供由 多云防御 防火墙配置记录并在 防火墙事件 类别中汇总的事件的详细可视性、过滤和分析。

防火墙事件中可用的表和字段如下：

事件详细信息	说明
日期和时间	ISO 8601 格式：YYYY-MM-DD T HH:MM:SS:S 示例：`2020-11-22T10:58:46.820`
类型	APPID, L4_FW, MALICIOUS_SRC, SNI
CSP 账户	多云防御 CSP 账户

事件详细信息	说明
Gateway	多云防御网关
地区	多云防御网关的所在地区
Level	紧急, 警报, 关键, 错误, 警告, 通知, 信息, 调试
会话 ID	。

服务	说明
源 IP	源 IP 地址
源端口	源端口
目标 IP	目的 IP 地址
目标端口	目标端口 (Destination Port)
协议 (Protocol)	UDP、TCP

应用信息	说明
客户端应用名称	与会话客户端关联的应用名称。示例： 高级打包工具
负载应用名称	与 Web 服务器主机关联的 HTTP 应用名称。示例：`Facebook`
服务应用名称	与会话服务器端关联的应用名称。示例： `HTTP`

操作	说明
操作	允许，拒绝
状态	ESTABLISHED, CLOSE, CLOSED, CLOSE_WAIT, TIME_WAIT, FIN_WAIT, LAST_ACK

HTTP 请求	说明
Host	URL 的主机部分
方法	GET, PUT, POST, HEAD, DELETE, PATCH, OPTIONS
URI	URI 标识符 RFC 3986

规则	说明
ID	多云防御 规则的 ID 编号/说明。示例 59 (egress-prod-apt-80)

FQDN	说明
FQDN	域名名称
类别名称 (Category Name)	FQDN 的类别分类。示例： 社交媒体
信誉	FQDN 的信誉得分

流分析 - 网络威胁

此视图提供对 多云防御 威胁分析引擎记录并在 网络威胁中汇总的威胁的详细可视性、过滤和分析。

网络威胁

网络威胁中可用的表和字段如下：

事件详细信息	说明
日期和时间	ISO 8601 格式：YYYY-MM-DD T HH:MM:SS:S 示例：`2020-11-22T10:58:46.820`
类型	AV、DLP、DPI
CSP 账户	多云防御 CSP 账户
Gateway	多云防御网关
地区	多云防御网关的所在地区
Level	紧急, 警报, 关键, 错误, 警告, 通知, 信息, 调试
会话 ID	。

服务	说明
源 IP	源 IP 地址
源端口	源端口
目标 IP	目的 IP 地址
目标端口	目标端口 (Destination Port)
协议 (Protocol)	UDP、TCP

应用信息	说明
客户端应用名称	与会话客户端关联的应用名称。示例： 高级打包工具

应用信息	说明
负载应用名称	与 Web 服务器主机关联的 HTTP 应用名称。示例：`Facebook`
服务应用名称	与会话服务器端关联的应用名称示例： `HTTP`

操作	说明
操作	允许，拒绝
状态	ESTABLISHED, CLOSE, CLOSED, CLOSE_WAIT, TIME_WAIT, FIN_WAIT, LAST_ACK

HTTP 请求	说明
Host	URL 的主机部分
方法	GET, PUT, POST, HEAD, DELETE, PATCH, OPTIONS
URI	URI 标识符 RFC 3986

FQDN	说明
FQDN	域名名称
类别名称 (Category Name)	FQDN 的类别分类。示例： 社交媒体
信誉	FQDN 的信誉得分

规则	说明
ID	多云防御 规则的 ID 编号/说明。示例 59 (egress-prod-apt-80)

流分析 - Web 攻击

此视图为 多云防御 Web 保护引擎记录的威胁提供详细的可视性、过滤和分析。 `Web 攻击` 事件类型包括 WAF 和 L7DOS。

Web 攻击

Web 攻击中可用的表和字段如下：

事件详细信息	说明
日期和时间	ISO 8601 格式：YYYY-MM-DD T HH:MM:SS:S 示例：`2020-11-22T10:58:46.820`

事件详细信息	说明
类型	L7DOS、WAF
CSP 账户	多云防御 CSP 账户
Gateway	多云防御网关
地区	多云防御网关的所在地区
Level	紧急, 警报, 关键, 错误, 警告, 通知, 信息, 调试
会话 ID	。

服务	说明
源 IP	源 IP 地址
源端口	源端口
目标 IP	目的 IP 地址
目标端口	目标端口 (Destination Port)
协议 (Protocol)	UDP、TCP

应用信息	说明
客户端应用名称	与会话客户端关联的应用名称。示例： `高级打包工具`
负载应用名称	与 Web 服务器主机关联的 HTTP 应用名称。示例： `Facebook`
服务应用名称	与会话服务器端关联的应用名称示例： `HTTP`

操作	说明
操作	允许，拒绝
状态	ESTABLISHED, CLOSE, CLOSED, CLOSE_WAIT, TIME_WAIT, FIN_WAIT, LAST_ACK

HTTP 请求	说明
Host	URL 的主机部分
方法	GET, PUT, POST, HEAD, DELETE, PATCH, OPTIONS
URI	URI 标识符 RFC 3986

FQDN	说明
FQDN	域名名称
类别名称 (Category Name)	FQDN 的类别分类。示例： 社交媒体
信誉	FQDN 的信誉得分

规则	说明
ID	多云防御 规则的 ID 编号/说明。示例 59 (egress-prod-apt-80)

流分析 - URL 过滤

此视图为 多云防御 URL 过滤配置记录的事件提供详细的可视性、过滤和分析。URL 过滤事件属于三 (3) 种事件类型之一： 防火墙事件、 网络事件 和 网络攻击。

URL 过滤

URL 过滤中可用的表和字段如下：

事件详细信息	说明
日期和时间	ISO 8601 格式：YYYY-MM-DD T HH:MM:SS:S 示例： `2020-11-22T10:58:46.820`
类型	URLFILTER
CSP 账户	多云防御 CSP 账户
Gateway	多云防御网关
地区	多云防御网关的所在地区
Level	紧急, 警报, 关键, 错误, 警告, 通知, 信息, 调试
会话 ID	。

服务	说明
源 IP	源 IP 地址
源端口	源端口
目标 IP	目的 IP 地址
目标端口	目标端口 (Destination Port)
协议 (Protocol)	UDP、TCP

应用信息	说明
客户端应用名称	与会话客户端关联的应用名称。示例： 高级打包工具。
负载应用名称	与 Web 服务器主机关联的 HTTP 应用名称。示例：Facebook
服务应用名称	与会话服务器端关联的应用名称示例： HTTP

操作	说明
操作	允许，拒绝
状态	ESTABLISHED, CLOSE, CLOSED, CLOSE_WAIT, TIME_WAIT, FIN_WAIT, LAST_ACK

HTTP 请求	说明
Host	URL 的主机部分
方法	GET, PUT, POST, HEAD, DELETE, PATCH, OPTIONS
URI	URI 标识符 RFC 3986

规则	说明
ID	多云防御 规则的 ID 编号/说明。示例 59 (egress-prod-apt-80)

FQDN	说明
FQDN	域名名称
类别名称 (Category Name)	FQDN 的类别分类。示例： 社交媒体
信誉	FQDN 的信誉得分

流分析 - FQDN 过滤

此视图为从 FQDN 过滤配置中记录的事件提供详细的可视性、过滤和分析选项。FQDN 过滤事件属于三 (3) 种事件类型之一： 防火墙事件、 网络事件 和 Web 攻击。

FQDN 过滤

FQDN 过滤中可用的表和字段如下：

事件详细信息	说明
日期和时间	ISO 8601 格式：YYYY-MM-DD T HH:MM:SS:S 示例：2020-11-22T10:58:46.820。
类型	FQDNFILTER。
CSP 账户	多云防御 CSP 账户。
Gateway	多云防御网关。
地区	多云防御网关所在的区域。
Level	紧急, 警报, 关键, 错误, 警告, 通知, 信息, 调试。
会话 ID	。

服务	说明
源 IP	源 IP 地址。
源端口	源端口。
目标 IP	目标 IP 地址。
目标端口	目的端口。
Protocol	UDP、TCP。

操作	说明
操作	允许，拒绝。
状态	ESTABLISHED、CLOSE、CLOSED、CLOSE_WAIT、TIME_WAIT、FIN_WAIT、LAST_ACK。

HTTP 请求	说明
Host	URL 的主机部分。
方法	GET、PUT、POST、HEAD、DELETE、PATCH、OPTIONS。
URI	URI 标识符 RFC 3986。

FQDN	说明
FQDN	完全限定域名。
类别名称 (Category Name)	FQDN 的类别分类。示例： 社交媒体。

FQDN	说明
信誉	FQDN 的信誉得分。

规则	说明
ID	多云防御 规则的 ID 编号/说明。示例 59 (egress-prod-apt-80)。

流分析 - HTTPS 日志

此视图为从 HTTPS 日志记录的事件提供详细的可视性、过滤和分析选项。HTTPS 日志可能会导致三 (3) 种事件类型之一： 防火墙事件、 网络事件 和 Web 攻击。

HTTPS 日志

HTTPS 日志中可用的表和字段如下：

事件详细信息	说明
日期和时间	ISO 8601 格式：YYYY-MM-DD T HH:MM:SS:S 示例：2020-11-22T10:58:46.820
类型	TLS_ERROR、TLS_LOG。
CSP 账户	多云防御 CSP 账户。
Gateway	多云防御网关。
地区	多云防御网关所在的区域。
Level	紧急, 警报, 关键, 错误, 警告, 通知, 信息, 调试。
会话 ID	。

服务	说明
源 IP	源 IP 地址。
源端口	源端口。
目标 IP	目标 IP 地址。
目标端口	目的端口。
Protocol	UDP、TCP。

应用信息	说明
客户端应用名称	与会话客户端关联的应用名称。示例： 高级打包工具。
负载应用名称	与 Web 服务器主机关联的 HTTP 应用名称。示例：Facebook。
服务应用名称	与会话服务器端关联的应用名称示例： HTTP。

操作	说明
操作	允许，拒绝。
状态	ESTABLISHED、CLOSE、CLOSED、CLOSE_WAIT、TIME_WAIT、FIN_WAIT、LAST_ACK。

HTTP 请求	说明
Host	URL 的主机部分。
方法	GET、PUT、POST、HEAD、DELETE、PATCH、OPTIONS。
URI	URI 标识符 RFC 3986。

FQDN	说明
FQDN	完全限定域名。
类别名称 (Category Name)	FQDN 的类别分类。示例： 社交媒体。
信誉	FQDN 的信誉得分。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。