フロー分析

フロー分析：トラフィックの概要

このビューには、フォワードまたはリバース ゲートウェイ プロキシのいずれかから Multicloud Defense によって記録されたイベントについての詳細な可視性、フィルタリング、および分析が表示されます。トラフィックの概要イベントは、ファイアウォールイベント、ネットワークイベント、および Web 攻撃の 3 つのイベントタイプのいずれかに寄与します。

Traffic Summary

[セッションの概要（Session Summary）] で使用可能なテーブルとフィールドは次のとおりです。

イベントの詳細（Event Details）	説明
日付および時刻（Date and Time）	ISO 8601 形式：YYYY-MM-DD T HH:MM:SS:S 例：`2020-11-22T10:58:46.820`
CSP アカウント（CSP Account）	Multicloud Defense CSPアカウント
ゲートウェイ	Multicloud Defense Gateway
地域	Multicloud Defense Gateway のリージョン

イベントの詳細（Event Details）	説明
レベル	INFO
セッション ID	..

クライアント側接続	説明
送信元IP（Src IP）	送信元 IP アドレス
送信元ポート（Src Port）	送信元ポート（Source Port）
宛先 IP	宛先 IP アドレス
宛先ポート	接続先ポート
プロトコル	UDP、TCP

クライアント側の統計	クライアントと Multicloud Defense Gateway 間のトラフィック
受信バイト数	クライアントから受信したバイト数
送信バイト	クライアントに送信されたバイト数
Received Packets	クライアントから受信したパケット数
Transmitted Packets	クライアントに送信されたパケット数

ポリシー一致情報	説明
宛先アドレスグループ（Dest Address Group）	一致するポリシールールで設定された宛先アドレスグループ
送信元アドレスグループ（Src Address Group）	一致するポリシールールで設定された送信元アドレスグループ
要求の SNI（Request SNI）	要求のサーバー名表示
サービス タイプ（Service Type）	[サービスタイプ（Service Type）]。例：`PROXY`
送信元の国（Src Country）	クライアント側の要求の発信元である国
宛先の国（Dest Country）	サーバー側の要求の宛先である国。例：`United States`

サーバー側接続	説明
送信元IP（Src IP）	送信元 IP アドレス

サーバー側接続	説明
送信元ポート（Src Port）	送信元ポート（Source Port）
宛先 IP	宛先 IP アドレス
宛先ポート	接続先ポート
プロトコル	UDP、TCP

サーバー側の統計情報（**Server-side Stats**）	**Multicloud Defense Gateway** とサーバー間のトラフィック
受信バイト数	サーバーから受信したバイト数
送信バイト	サーバーに送信されたバイト数
Received Packets	サーバーから受信したパケット数
Transmitted Packets	サーバに送信されるパケット数。

アプリケーション情報	説明
クライアントアプリケーション名（Client App Name）	セッションのクライアント側に関連付けられたアプリケーション名。例：`Advanced Packaging Tool`
ペイロードアプリケーション名（Payload App Name）	Web サーバーホストに関連付けられている HTTP アプリケーション名。例：`Facebook`
サービスアプリケーション名（Service App Name）	セッションのサーバー側に関連付けられたアプリケーション名。例：`HTTP`

アクション	説明
操作	許可（ALLOW）、拒否（DENY）

クラウドサービス	説明
クラウドサービス	要求によってアクセスされる接続先クラウドサービスの名前。例：`AMAZON`、`EC2`

送信元インスタンス情報	説明
インスタンス ID	クライアントインスタンス ID
インスタンス名（Instance Name）	クライアントインスタンス名（タグも表示可能）
VPC ID	クライアント VPC ID

HTTP リクエスト	説明
ホスト（Host）	URL のホスト部分
方法	GET、PUT、POST、HEAD、DELETE、PATCH、OPTIONS
URI	URI 識別子 RFC 3986

ルール	説明
ID	Multicloud Defense ルールの ID 番号/説明。例：`59 (egress-prod-apt-80)`。

FQDN	説明
FQDN	完全修飾ドメイン名
カテゴリ名（Category Name）	FQDN のカテゴリ分類。例：ソーシャルメディア
レピュテーション	FQDN のレピュテーションスコア

フロー分析：すべてのイベント

[フロー分析：すべてのイベント（Flow Analytics - All Events）] は、Multicloud Defense ソリューション全体のネットワークおよびセキュリティイベントを全体的に可視化します。

[すべてのイベント（All Events）] で使用可能なテーブルとフィールドは次のとおりです。

イベントの詳細（Event Details）	説明
日付および時刻（Date and Time）	ISO 8601 形式：YYYY-MM-DD T HH:MM:SS:S 例：`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 アカウント（CSP Account）	Multicloud Defense CSP アカウント。
ゲートウェイ	Multicloud Defense Gateway。
地域	Multicloud Defense Gateway のリージョン。
レベル	[デバッグ（DEBUG）]、[情報（INFO）]、[通知（NOTICE）]、[警告（WARNING）]、[エラー（ERROR）]、[重大（CRITICAL）]、[アラート（ALERT）]、[緊急（EMERGENCY）]。

イベントの詳細（**Event Details**）	説明
セッション ID	..

サービス	説明
[送信元IP（Src IP）]	送信元 IP アドレス。
[送信元ポート（Src Port）]	Source Port：
宛先 IP	宛先 IP アドレス。
宛先ポート	Destination Port：
プロトコル	UDP、TCP。

アプリケーション情報	説明
クライアントアプリケーション名（Client App Name）	セッションのクライアント側に関連付けられたアプリケーション名。例：`Advanced Packaging Tool`。
ペイロードアプリケーション名（Payload App Name）	Web サーバーホストに関連付けられている HTTP アプリケーション名。例：`Facebook`。
サービスアプリケーション名（Service App Name）	セッションのサーバー側に関連付けられたアプリケーション名。例：`HTTP`

アクション	説明
操作	許可（ALLOW）、拒否（DENY）。
状態（State）	確立済み（ESTABLISHED）、クローズ（CLOSE）、クローズ済み（CLOSED）、CLOSE_WAIT、TIME_WAIT、FIN_WAIT、LAST_ACK。

HTTP リクエスト	説明
ホスト（Host）	URL のホスト部分。
方法	GET、PUT、POST、HEAD、DELETE、PATCH、OPTIONS。
URI	URI 識別子 RFC 3986。

ルール	説明
ID	Multicloud Defense ルールの ID 番号/説明。例：`59 (egress-prod-apt-80)`。

FQDN	説明
[FQDN]	完全修飾ドメイン名。
カテゴリ名（Category Name）	FQDN のカテゴリ分類。例：ソーシャルメディア。
レピュテーション	FQDN のレピュテーションスコア。

イベント ログ

イベントログには、Multicloud Defense Gateway を通過するすべてのトラフィックの詳細情報が含まれます。

インスペクション後、Multicloud Defense は、パケットの内容とポリシーで定義されている内容に基づいてセッションとイベントを生成します。分析、イベントに関連する詳細、および実行されたアクションはすべてログの形式でキャプチャされ、**[調査（Investigate）] > [フロー分析（Flow Analytics）] > [すべてのイベント（All Events）]**で使用できます。システムは、これらのログを 30 日間保持します。

ログがキャプチャするイベントタイプ：

表 *1:* イベントタイプと説明

イベントタイプ	イベント名	説明
FQDN フィルタ	完全修飾ドメイン名（FQDN）のフィルタリング	関連するログが、FQDN、送信元、宛先 IP などの詳細情報とともに生成されます。FQDN フィルタリングイベントは、ポリシーに FQDN フィルタリングプロファイルがある場合にのみ生成されます。
SNI	サーバー名表示（SNI）	SNI を使用すると、複数のホスト名を HTTPS 経由で処理できます。これは、Multicloud Defense が TLS ハンドシェイクで SNI を観察したときに生成されます。
APPID	アプリ ID（APPID）	APPID はネットワークトラフィックを分析して、L7 アプリケーションを決定します。APPID ログは、イベントがデータベース内の既知のアプリケーションと一致した場合に生成されます。
L4_FW	L4 ファイアウォール	L4 ファイアウォールイベントは、イベントがルールセットのポリシーと一致した場合に生成されます。

イベントタイプ	イベント名	説明
URL FILTER	URL フィルタリング	URL フィルタリングは、URL に基づいてネットワークトラフィックをフィルタ処理するために使用されます。このイベントログは、URL フィルタリングプロファイルと一致した場合に生成されます。
IPS	侵入防御システム（IPS）	IPSイベントは、ネットワークトラフィックがIPSルールセットに一致した場合に生成されます。
DLP	データ損失防止（DLP）	DLPイベントは、ネットワークトラフィックが設定されている DLP プロファイルと一致した場合に生成されます。ログには、エンドポイント、ドメイン、ユーザー名、ルール、送信元、宛先、実行されたアクションなどの詳細な伝送情報とともに、以下のインシデントが記録されます。
WAF	Webアプリケーションファイアウォール	WAFイベントは、ネットワークトラフィックが設定されている WAF プロファイルと一致した場合に生成されます。
L7_DOS	レイヤ 7 サービス拒否（DoS）	レイヤ7DoSイベントは、ネットワークトラフィックが設定されている L7 DoS プロファイルと一致した場合に生成されます。これらのログには、イベントの詳細、攻撃時刻、要求、緩和策などが含まれます。
AV	ウイルス対策（AV）	AV イベントは、イベントがネットワークトラフィックのAVルールセットと一致した場合に生成されます。
DPI	ディープ パケット インスペクション（DPI）	DPIイベントは、高度なセキュリティが設定されているルールにネットワークトラフィックが一致した場合に生成されます。
MALICIOUS_SRC	悪意のある送信元	悪意のある送信元は、ネットワークトラフィックが悪意のあるIP と一致した場合に生成されます。
TLS_ERROR	TLS エラー	TLSハンドシェイク中にエラーが発生すると、 TLSエラーが生成されます。

イベントタイプ	イベント名	説明
TLS_LOG	TLS ログ	ネットワークトラフィックが TLS を使用すると、TLSログが生成されます。これにより、暗号スイートや TLS バージョンなどのTLSハンドシェイク情報がキャプチャされます。

ファイアウォールイベント

このビューには、Multicloud Defenseファイアウォール設定によって記録されたイベントについての詳細な可視性、フィルタリング、および分析が表示され、その情報は [ファイアウォールイベント（Firewall Events）] カテゴリにまとめられています。

ファイアウォールイベントで使用可能なテーブルとフィールドは次のとおりです。

イベントの詳細（Event Details）	説明
日付および時刻（Date and Time）	ISO 8601 形式：YYYY-MM-DD T HH:MM:SS:S 例：`2020-11-22T10:58:46.820`
Type	APPID、L4_FW、MALICIOUS_SRC、SNI
CSP アカウント（CSP Account）	Multicloud Defense CSP アカウント
ゲートウェイ	Multicloud Defense Gateway
地域	Multicloud Defense Gateway のリージョン
レベル	[デバッグ（DEBUG）]、[情報（INFO）]、[通知（NOTICE）]、[警告（WARNING）]、[エラー（ERROR）]、[重大（CRITICAL）]、[アラート（ALERT）]、[緊急（EMERGENCY）]
セッション ID	..

サービス	説明
[送信元IP（Src IP）]	送信元 IP アドレス
[送信元ポート（Src Port）]	送信元ポート（Source Port）
宛先 IP	宛先 IP アドレス
宛先ポート	接続先ポート
プロトコル	UDP、TCP

アプリケーション情報	説明
クライアントアプリケーション名（Client App Name）	セッションのクライアント側に関連付けられたアプリケーション名。例：`Advanced Packaging Tool`
ペイロードアプリケーション名（Payload App Name）	Web サーバーホストに関連付けられている HTTP アプリケーション名。例：`Facebook`
サービスアプリケーション名（Service App Name）	セッションのサーバー側に関連付けられたアプリケーション名。例：`HTTP`

アクション	説明
操作	許可（ALLOW）、拒否（DENY）
状態（State）	確立済み（ESTABLISHED）、クローズ（CLOSE）、クローズ済み（CLOSED）、CLOSE_WAIT、TIME_WAIT、FIN_WAIT、LAST_ACK

HTTP リクエスト	説明
ホスト（Host）	URL のホスト部分
方法	GET、PUT、POST、HEAD、DELETE、PATCH、OPTIONS
URI	URI 識別子 RFC 3986

ルール	説明
ID	Multicloud Defense ルールの ID 番号/説明。例：59（egress-prod-apt-80）

FQDN	説明
[FQDN]	完全修飾ドメイン名
カテゴリ名（Category Name）	FQDN のカテゴリ分類。例：ソーシャルメディア
レピュテーション	FQDN のレピュテーションスコア

ネットワーク脅威

このビューには、Multicloud Defense 脅威分析エンジンによって記録された脅威についての詳細な可視性、フィルタリング、および分析が提供され、その情報は[ネットワーク脅威（Network Threats）] にまとめられています。

ネットワーク脅威

[ネットワーク脅威（Network Threats）] で使用可能なテーブルとフィールドは次のとおりです。

イベントの詳細（Event Details）	説明
日付および時刻（Date and Time）	ISO 8601 形式：YYYY-MM-DD T HH:MM:SS:S 例：`2020-11-22T10:58:46.820`
Type	AV、DLP、DPI
CSP アカウント（CSP Account）	Multicloud Defense CSP アカウント
ゲートウェイ	Multicloud Defense Gateway
地域	Multicloud Defense Gateway のリージョン
レベル	[デバッグ（DEBUG）]、[情報（INFO）]、[通知（NOTICE）]、[警告（WARNING）]、[エラー（ERROR）]、[重大（CRITICAL）]、[アラート（ALERT）]、[緊急（EMERGENCY）]
セッション ID	..

サービス	説明
[送信元IP（Src IP）]	送信元 IP アドレス
[送信元ポート（Src Port）]	送信元ポート（Source Port）
宛先 IP	宛先 IP アドレス
宛先ポート	接続先ポート
プロトコル	UDP、TCP

アプリケーション情報	説明
クライアントアプリケーション名（Client App Name）	セッションのクライアント側に関連付けられたアプリケーション名。例：`Advanced Packaging Tool`
ペイロードアプリケーション名（Payload App Name）	Web サーバーホストに関連付けられている HTTP アプリケーション名。例：`Facebook`
サービスアプリケーション名（Service App Name）	セッションのサーバー側に関連付けられたアプリケーション名（例：`HTTP`）

アクション	説明
操作	許可（ALLOW）、拒否（DENY）

アクション	説明
状態（State）	確立済み（ESTABLISHED）、クローズ（CLOSE）、クローズ済み（CLOSED）、CLOSE_WAIT、TIME_WAIT、FIN_WAIT、LAST_ACK

HTTP リクエスト	説明
ホスト（Host）	URL のホスト部分
方法	GET、PUT、POST、HEAD、DELETE、PATCH、OPTIONS
URI	URI 識別子 RFC 3986

FQDN	説明
[FQDN]	完全修飾ドメイン名
カテゴリ名（Category Name）	FQDN のカテゴリ分類。例：ソーシャルメディア
レピュテーション	FQDN のレピュテーションスコア

ルール	説明
ID	Multicloud Defense ルールの ID 番号/説明。例：59（egress-prod-apt-80）

Web 攻撃

このビューには、Multicloud Defense Web 保護エンジンによって記録された脅威についての詳細な可視性、フィルタリング、および分析が表示されます。[Web攻撃（Web Attack）] のイベントタイプには、WAF と L7DOS があります。

[Web攻撃（Web Attack）] で使用可能なテーブルとフィールドは次のとおりです。

イベントの詳細（Event Details）	説明
日付および時刻（Date and Time）	ISO 8601 形式：YYYY-MM-DD T HH:MM:SS:S 例：`2020-11-22T10:58:46.820`
Type	L7DOS、WAF
CSP アカウント（CSP Account）	Multicloud Defense CSPアカウント
ゲートウェイ	Multicloud Defense Gateway
地域	Multicloud Defense Gateway のリージョン

イベントの詳細（Event Details）	説明
レベル	[デバッグ（DEBUG）]、[情報（INFO）]、[通知（NOTICE）]、[警告（WARNING）]、[エラー（ERROR）]、[重大（CRITICAL）]、[アラート（ALERT）]、[緊急（EMERGENCY）]
セッション ID	..

サービス	説明
[送信元IP（Src IP）]	送信元 IP アドレス
[送信元ポート（Src Port）]	送信元ポート（Source Port）
宛先 IP	宛先 IP アドレス
宛先ポート	接続先ポート
プロトコル	UDP、TCP

アプリケーション情報	説明
クライアントアプリケーション名（Client App Name）	セッションのクライアント側に関連付けられたアプリケーション名。例：`Advanced Packaging Tool`
ペイロードアプリケーション名（Payload App Name）	Web サーバーホストに関連付けられている HTTP アプリケーション名。例：`Facebook`
サービスアプリケーション名（Service App Name）	セッションのサーバー側に関連付けられたアプリケーション名（例：`HTTP`）

アクション	説明
操作	許可（ALLOW）、拒否（DENY）
状態（State）	確立済み（ESTABLISHED）、クローズ（CLOSE）、クローズ済み（CLOSED）、CLOSE_WAIT、TIME_WAIT、FIN_WAIT、LAST_ACK

HTTP リクエスト	説明
ホスト（Host）	URL のホスト部分
方法	GET、PUT、POST、HEAD、DELETE、PATCH、OPTIONS
URI	URI 識別子 RFC 3986

FQDN	説明
[FQDN]	完全修飾ドメイン名
カテゴリ名（Category Name）	FQDN のカテゴリ分類。例：ソーシャルメディア
レピュテーション	FQDN のレピュテーションスコア

ルール	説明
ID	Multicloud Defense ルールの ID 番号/説明。例：59（egress-prod-apt-80）

URL フィルタリング

このビューには、Multicloud Defense URL フィルタリング設定によって記録されたイベントについての詳細な可視性、フィルタリング、および分析が表示されます。URL フィルタリングイベントは、ファイアウォールイベント、ネットワークイベント、および Web 攻撃の 3 つのイベントタイプのいずれかに寄与します。

イベントの詳細（Event Details）	説明
日付および時刻（Date and Time）	ISO 8601 形式：YYYY-MM-DD T HH:MM:SS:S 例：2020-11-22T10:58:46.820
Type	URLFILTER
CSP アカウント（CSP Account）	Multicloud Defense CSPアカウント
ゲートウェイ	Multicloud Defense Gateway
地域	Multicloud Defense Gateway のリージョン
レベル	[デバッグ（DEBUG）]、[情報（INFO）]、[通知（NOTICE）]、[警告（WARNING）]、[エラー（ERROR）]、[重大（CRITICAL）]、[アラート（ALERT）]、[緊急（EMERGENCY）]
セッション ID	..

サービス	説明
[送信元IP（Src IP）]	送信元 IP アドレス
[送信元ポート（Src Port）]	送信元ポート（Source Port）
宛先 IP	宛先 IP アドレス

サービス	説明
宛先ポート	接続先ポート
プロトコル	UDP、TCP

アプリケーション情報	説明
クライアントアプリケーション名（Client App Name）	セッションのクライアント側に関連付けられたアプリケーション名。例：`Advanced Packaging Tool`。
ペイロードアプリケーション名（Payload App Name）	Web サーバーホストに関連付けられている HTTP アプリケーション名。例：`Facebook`
サービスアプリケーション名（Service App Name）	セッションのサーバー側に関連付けられたアプリケーション名（例：`HTTP`）

アクション	説明
操作	許可（ALLOW）、拒否（DENY）
状態（State）	確立済み（ESTABLISHED）、クローズ（CLOSE）、クローズ済み（CLOSED）、CLOSE_WAIT、TIME_WAIT、FIN_WAIT、LAST_ACK

HTTP リクエスト	説明
ホスト（Host）	URL のホスト部分
方法	GET、PUT、POST、HEAD、DELETE、PATCH、OPTIONS
URI	URI 識別子 RFC 3986

ルール	説明
ID	Multicloud Defense ルールの ID 番号/説明。例：59（egress-prod-apt-80）

FQDN	説明
[FQDN]	完全修飾ドメイン名
カテゴリ名（Category Name）	FQDN のカテゴリ分類。例：ソーシャルメディア
レピュテーション	FQDN のレピュテーションスコア

FQDNフィルタリング

このビューには、FQDNフィルタリング設定によって記録されたイベントについての詳細な可視性、フィルタリング、および分析オプションが表示されます。FQDNフィルタリングイベントは、ファイアウォールイベント、ネットワークイベント、および Web 攻撃の 3 つのイベントタイプのいずれかに寄与します。

イベントの詳細（Event Details）	説明
日付および時刻（Date and Time）	ISO 8601 形式：YYYY-MM-DD T HH:MM:SS:S 例：`2020-11-22T10:58:46.820`。
Type	FQDNFILTER。
CSP アカウント（CSP Account）	Multicloud Defense CSP アカウント。
ゲートウェイ	Multicloud Defense Gateway。
地域	Multicloud Defense Gateway のリージョン。
レベル	[デバッグ（DEBUG）]、[情報（INFO）]、[通知（NOTICE）]、[警告（WARNING）]、[エラー（ERROR）]、[重大（CRITICAL）]、[アラート（ALERT）]、[緊急（EMERGENCY）]。
セッション ID	..

サービス	説明
[送信元IP（Src IP）]	送信元 IP アドレス。
[送信元ポート（Src Port）]	Source Port：
宛先 IP	宛先 IP アドレス。
宛先ポート	Destination Port：
プロトコル	UDP、TCP。

アクション	説明
操作	許可（ALLOW）、拒否（DENY）。
状態（State）	確立済み（ESTABLISHED）、クローズ（CLOSE）、クローズ済み（CLOSED）、CLOSE_WAIT、TIME_WAIT、FIN_WAIT、LAST_ACK。

HTTP リクエスト	説明
ホスト（Host）	URL のホスト部分。
方法	GET、PUT、POST、HEAD、DELETE、PATCH、OPTIONS。
URI	URI 識別子 RFC 3986。

FQDN	説明
[FQDN]	完全修飾ドメイン名。
カテゴリ名（Category Name）	FQDNのカテゴリ分類。例：ソーシャルメディア。
レピュテーション	FQDN のレピュテーションスコア。

ルール	説明
ID	Multicloud Defense ルールの ID 番号/説明。例：59 (egress-prod-apt-80)。

HTTPS ログ

このビューでは、HTTPS ログに記録されたイベントの詳細な可視性、フィルタリング、および分析オプションを利用できます。HTTPS ログは、ファイアウォールイベント、ネットワークイベント、および Web 攻撃の 3 つのイベントタイプのいずれかに寄与する可能性があります。

イベントの詳細（Event Details）	説明
日付および時刻（Date and Time）	ISO 8601 形式：YYYY-MM-DD T HH:MM:SS:S 例：`2020-11-22T10:58:46.820`
Type	TLS_ERROR、TLS_LOG。
CSP アカウント（CSP Account）	Multicloud Defense CSP アカウント。
ゲートウェイ	Multicloud Defense Gateway。
地域	Multicloud Defense Gateway のリージョン。
レベル	[デバッグ（DEBUG）]、[情報（INFO）]、[通知（NOTICE）]、[警告（WARNING）]、[エラー（ERROR）]、[重大（CRITICAL）]、[アラート（ALERT）]、[緊急（EMERGENCY）]。
セッション ID	..

サービス	説明
[送信元IP（Src IP）]	送信元 IP アドレス。
[送信元ポート（Src Port）]	Source Port：
宛先 IP	宛先 IP アドレス。
宛先ポート	Destination Port：
プロトコル	UDP、TCP。

アプリケーション情報	説明
クライアントアプリケーション名（Client App Name）	セッションのクライアント側に関連付けられたアプリケーション名。例：`Advanced Packaging Tool`。
ペイロードアプリケーション名（Payload App Name）	Web サーバーホストに関連付けられている HTTP アプリケーション名。例：`Facebook`。
サービスアプリケーション名（Service App Name）	セッションのサーバー側に関連付けられたアプリケーション名（例：`HTTP`）。

アクション	説明
操作	許可（ALLOW）、拒否（DENY）。
状態（State）	確立済み（ESTABLISHED）、クローズ（CLOSE）、クローズ済み（CLOSED）、CLOSE_WAIT、TIME_WAIT、FIN_WAIT、LAST_ACK。

HTTP リクエスト	説明
ホスト（Host）	URL のホスト部分。
方法	GET、PUT、POST、HEAD、DELETE、PATCH、OPTIONS。
URI	URI 識別子 RFC 3986。

FQDN	説明
[FQDN]	完全修飾ドメイン名。
カテゴリ名（Category Name）	FQDN のカテゴリ分類。例：ソーシャルメディア。
レピュテーション	FQDN のレピュテーションスコア。

VPN ログ

仮想プライベートネットワーク（VPN）ログは、VPN内で発生するアクティビティとイベントを記録したものであり、接続の使用状況、パフォーマンス、およびセキュリティに関する詳細情報がわかります。VPNログには、接続、使用状況、アクティビティ、エラー、およびセキュリティログが含まれます。このページに示すディスプレイは、選択したイベントの詳細に直接依存することに注意してください。[編集（Edit）]アイコンをクリックして表示内容を変更し、次の情報オプションから選択します。

イベントの詳細	説明
日付および時刻（Date and Time）	ISO 8601 形式：YYYY-MM-DD T HH:MM:SS:S 例：2020-11-22T10:58:46.820。
CSP アカウント（CSP Account）	クラウドサービスアカウントの名前。
地域	Multicloud Defense Gateway のリージョン。
ゲートウェイ	イベントに関与する Multicloud Defense Gateway。
テキスト（Text）	イベントメッセージに含まれるテキストのプレビュー。個々のメッセージをクリックして展開します。
ゲートウェイ セキュリティ タイプ（Gateway Security Type）	Multicloud Defense Gateway の名称。
[インスタンス名（Instance Name）]	VPN セッションまたは接続インスタンスの識別子。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。