クラウドで提供されるファイアウォールログに欠落しているポート情報の理解

内容

はじめに

このドキュメントでは、クラウド配信ファイアウォールログにポート情報が欠落している理由について説明します。

クラウド配信ファイアウォールログにポート情報が欠落しているのはなぜですか。

シスコのマネージドS3バケットまたは自身のS3バケットからCisco Umbrellaログをダウンロードすると、クラウド配信ファイアウォール(CDFW)ログの一部で、「sourcePort」および「destinationPort」の入力に空の値が返されます。

ユーザトラフィックの内部ポート情報を使用できるかどうかは、トラフィックのプロトコルによって異なります。ICMPトラフィックにはポート番号がないため、ポート情報は記録されません。

```
"2020-06-09 18:52:38","[419244240]","raspberrypi","Network Tunnels",
"OUTBOUND","1","84","192.168.64.112","","8.8.8.8","","nyc1.edc",
"1614180","ALLOW"
```

TCPおよびUDPを使用するトラフィックがログに記録されると、ポート情報が表示されます。

```
"2020-06-09 18:53:49","[419244240]","raspberrypi","Network Tunnels",
"OUTBOUND","17","75","192.168.64.112","57405","8.8.8.8","53","nyc1.edc",
"1614180","ALLOW"
```

追加情報

CDFWログの詳細については、Umbrellaのドキュメント「ログ形式とバージョニング：クラウドファイアウォールログ」を参照してください。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。