Understand Missing Port Information from Cloud Delivered Firewall Logs

Contents

Introduction

Why is the Port Information Missing from my Cloud Delivered Firewall Logs?

Additional Information

Introduction

This document describes why the port information is missing from Cloud Delivered Firewall Logs.

Why is the Port Information Missing from my Cloud Delivered Firewall Logs?

When you download the Cisco Umbrella logs from either Cisco's managed S3 bucket or your own S3 bucket, some of Cloud Delivered Firewall (CDFW) logs are returning an empty value for "sourcePort" and "destinationPort" inputs.

Whether or not the internal port information of the user traffic is available depends on the protocol of the traffic. Since ICMP traffic does not have port numbers, no port information is logged.

```
"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"
```

When traffic using TCP and UDP are logged, then the port information is displayed.

```
"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"
```

Additional Information

Read more about CDFW logs in the Umbrella documentation: Log Format and Versioning - Cloud Firewall Logs