了解云交付的防火墙日志中缺少的端口信息

目录

简介

本文档说明云交付的防火墙日志中缺少端口信息的原因。

为什么云交付的防火墙日志中缺少端口信息？

当您从思科托管S3存储桶或您自己的S3存储桶下载Cisco Umbrella日志时，一些云交付防火墙(CDFW)日志会为“sourcePort”和“destinationPort”输入返回空值。

用户流量的内部端口信息是否可用取决于流量的协议。由于ICMP流量没有端口号，因此不会记录端口信息。

```
"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"
```

记录使用TCP和UDP的流量时，会显示端口信息。

```
"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

阅读Umbrella文档中有关CDFW日志的更多信息：日志格式和版本控制 — 云防火墙日志

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。