Comprendre les informations de port manquantes dans les journaux de pare-feu fournis dans le cloud

Table des matières

Introduction

Ce document explique pourquoi les informations de port sont manquantes dans les journaux de pare-feu fournis dans le cloud.

Pourquoi les informations de port sont-elles manquantes dans les journaux de mon pare-feu fourni dans le cloud ?

Lorsque vous téléchargez les journaux Cisco Umbrella à partir du compartiment géré S3 de Cisco ou de votre propre compartiment S3, certains journaux du pare-feu fourni dans le cloud (CDFW) renvoient une valeur vide pour les entrées « sourcePort » et « destinationPort ».

Le fait que les informations de port interne du trafic utilisateur soient disponibles ou non dépend du protocole du trafic. Comme le trafic ICMP n'a pas de numéro de port, aucune information de port n'est consignée.

```
"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"
```

Lorsque le trafic utilisant TCP et UDP est consigné, les informations de port s'affichent.

```
"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

Pour en savoir plus sur les journaux CDFW, consultez la documentation Umbrella : Log Format and Versioning - Cloud Firewall Logs

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.