Ontbrekende poortinformatie uit door de cloud geleverde firewalllogboeken begrijpen

Inhoud

Inleiding

In dit document wordt beschreven waarom de poortinformatie ontbreekt in de door de cloud geleverde firewalllogboeken.

Waarom ontbreekt de poortinformatie in mijn door de cloud geleverde firewalllogboeken?

Wanneer u de Cisco Umbrella-logs downloadt van de beheerde S3-bucket van Cisco of uw eigen S3-bucket, retourneren sommige van de Cloud Delivered Firewall (CDFW) -logs een lege waarde voor "sourcePort"- en "destinationPort" -ingangen.

Of de interne poortinformatie van het gebruikersverkeer beschikbaar is, hangt af van het protocol van het verkeer. Aangezien ICMP-verkeer geen poortnummers heeft, wordt er geen poortinformatie vastgelegd.

```
"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"
```

Wanneer het verkeer met TCP en UDP wordt geregistreerd, wordt de poortinformatie weergegeven.

```
"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"
```

Aanvullende informatie

Lees meer over CDFW-logs in de overkoepelende documentatie: Logformaat en Versioning - Logboeken van Cloud Firewall

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.