Compreender as informações de porta ausentes dos logs de firewall fornecidos pela nuvem

Contents

Introdução

Este documento descreve por que as informações de porta estão ausentes nos logs de firewall fornecidos pela nuvem.

Por que as informações de porta estão ausentes dos logs de firewall fornecidos na nuvem?

Quando você faz download dos logs do Cisco Umbrella do bucket de S3 gerenciado da Cisco ou do seu próprio bucket de S3, alguns dos logs do Cloud Delivered Firewall (CDFW) estão retornando um valor vazio para entradas "sourcePort" e "destinationPort".

A disponibilidade ou não das informações de porta interna do tráfego do usuário depende do protocolo do tráfego. Como o tráfego ICMP não tem números de porta, nenhuma informação de porta é registrada.

```
"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"
```

Quando o tráfego que usa TCP e UDP é registrado, as informações da porta são exibidas.

```
"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"
```

Informações adicionais

Leia mais sobre os registros de CDFW na documentação do Umbrella: Formato e versão de registro - registros de firewall de nuvem

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.