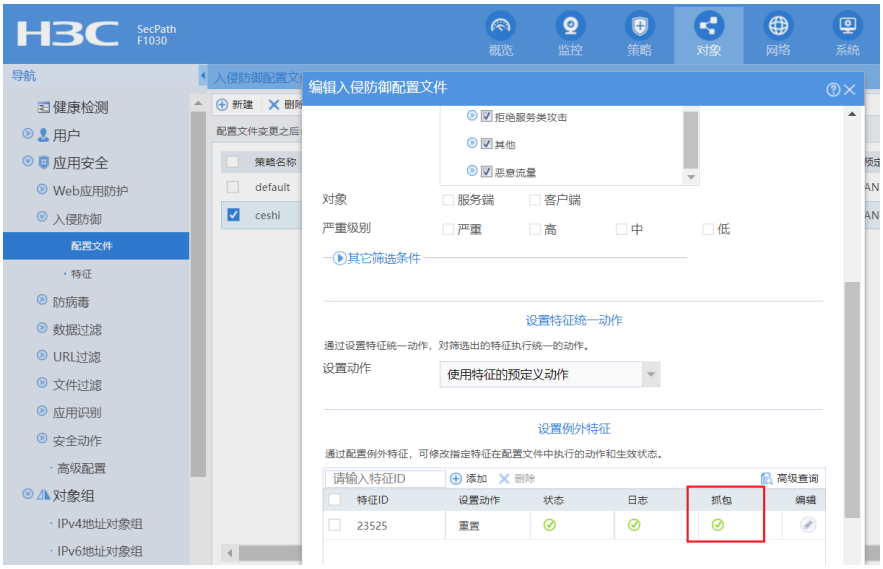
安全设备IPS抓包信息下载查看方法

IPS防攻击　曾招维　2022-05-12 发表

问题描述

安全设备开启IPS抓包后，抓包信息如何？



解决方法

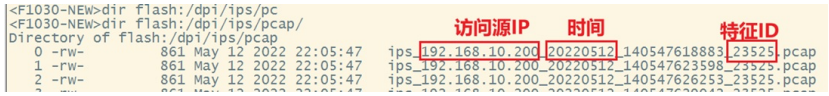
命令行：

<F1030-NEW>dir flash:/dpi/ips/pcap/

Directory of flash:/dpi/ips/pcap

0 -rw- 861 May 12 2022 22:05:47 ips_192.168.10.200_20220512_140547618883_23525.pca p

1 -rw- 861 May 12 2022 22:05:47 ips_192.168.10.200_20220512_140547623598_23525.pca p



FTP/TFTP下载：

<F1030-NEW>ftp 192.168.10.200

Press CTRL+C to abort.

Connected to 192.168.10.200 (192.168.10.200).

220 3Com 3CDaemon FTP Server Version 2.0

User (192.168.10.200:(none)): zzw

331 User name ok, need password

Password:

230 User logged in

Remote system type is UNIX.

Using binary mode to transfer files.

ftp> put flash:/dpi/ips/pcap/ips_192.168.10.200_20220512_140547618883_23525.pcap

227 Entering passive mode (192,168,10,200,165,246)

125 Using existing data connection

.

226 Closing data connection; File transfer successful.

861 bytes sent in 0.001 seconds (1.21 Mbytes/s)