【MVS】F5 BIG-IP系列命令行抓包方法

设备管理 **胡伟** 2024-06-13 发表

问题描述

【MVS】F5 BIG-IP系列命令行抓包方法

解决方法

F5 BIG-IP如果不方便登录Web界面进行抓包，可以登录设备后台命令行使用Linux tcpdump工具进行抓包。相关方法如下：

1. 使用root账号SSH登录F5后台命令行
2. 使用Linux tcpdump工具用如下命令进行报文捕获

> tcpdump -s0 -nni 0.0:nnnp host 192.168.1.1 and port 443 -vw /var/tmp/hostname.pcap

- -s0 无限制的数据包截断长度，可以捕获最大的数据量。
- -nn 禁止将主机地址转换为名称，避免进行DNS查询。
- -i 0.0 在接口0.0上捕获流量，表示用于捕获所有接口的“任意”接口。
- :nnnp 使用了'p'标志和'nnn'，这将创建F5以太网尾部的信息及双向代理的流量。
- host 虚拟服务器或源IP的IP地址。如果虚拟服务器的目的地是0.0.0.0:0（称为任意：任意），则需要源IP。
- port 虚拟服务器使用的特定端口，有助于减小捕获文件的大小。虚拟IP地址可以多次使用，但必须与端口号结合使用以形成websocket。
- -v 添加冗长输出，提供屏幕计数器以显示捕获的数据包数量及速率。
- -w 将捕获的数据包保存到文件位置。
- /var/tmp/hostname 文件保存路径和名称。可以随意命名，但需要遵守Linux系统的命名规则。在开始捕获时无需手动创建文件，系统会自动创建。
- .pcap 文件类型，一种捕获文件格式（.cap仍在使用，但不如pcapng格式高效，pcapng是最新的格式，在大多数情况下都可以使用）。