

知 某局点GAP2000看不到应用日志经验处理案例

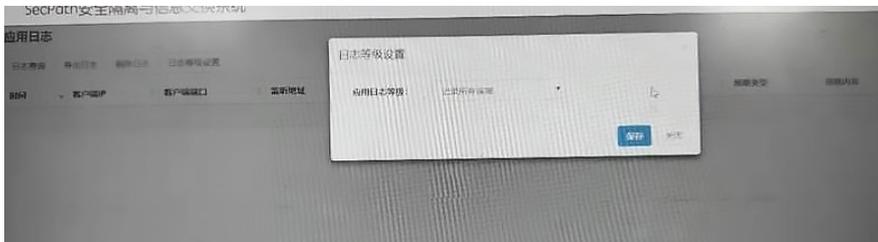
网闸 孙轶宁 2019-03-25 发表

组网及说明

不涉及

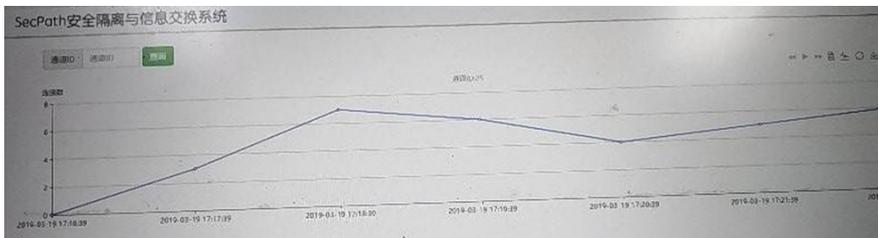
问题描述

客户在网闸上面配置完通道，并且将应用日志的日志等级设置配置为记录所有日志，但是没有任何应用日志的记录。

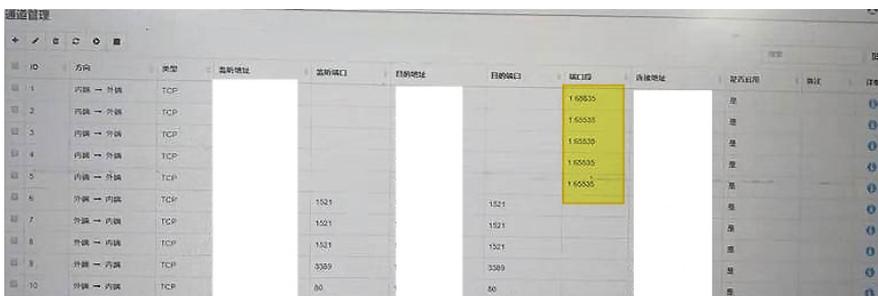


过程分析

1、首先确认是否有通过通道的流量，根据系统连接数来看，确实有流量经过通道。



2、检查通道的配置，发现有不少端口段的配置：

A screenshot of the '通道管理' (Channel Management) interface. It shows a table with columns: ID, 方向 (Direction), 类型 (Type), 源地址 (Source Address), 源端口 (Source Port), 目的地址 (Destination Address), 目的端口 (Destination Port), 端口段 (Port Range), 连接地址 (Connection Address), 是否启用 (Enabled), 备注 (Remarks), and 详情 (Details). The '端口段' column contains values like '1-65535', '1-65534', '1-65533', '1-65532', and '1-65531'.

ID	方向	类型	源地址	源端口	目的地址	目的端口	端口段	连接地址	是否启用	备注	详情
1	内网 -> 外网	TCP					1-65535		是		详情
2	内网 -> 外网	TCP					1-65534		是		详情
3	内网 -> 外网	TCP					1-65533		是		详情
4	内网 -> 外网	TCP					1-65532		是		详情
5	内网 -> 外网	TCP					1-65531		是		详情
6	外网 -> 内网	TCP		1521		1521			是		详情
7	外网 -> 内网	TCP		1521		1521			是		详情
8	外网 -> 内网	TCP		1521		1521			是		详情
9	外网 -> 内网	TCP		3389		3389			是		详情
10	外网 -> 内网	TCP		80		80			是		详情

3、经确认，应用日志存在以下限制：

端口段类型通道，不记录应用日志。

UDP类型通道，只记录拒绝的应用日志。

4、让客户测试TCP类型且非端口段类型的通道，发现有日志记录。

解决方法

应用日志当前实现如下：

端口段类型通道，不记录应用日志。

UDP类型通道，只记录拒绝的应用日志。

因此测试此功能需要用TCP类型且非端口段类型的通道进行测试。