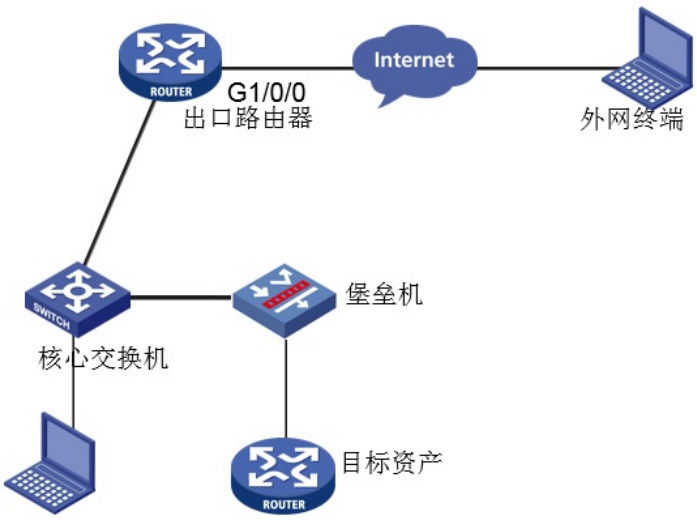
某局点SecPath A2000-V(二代) 外网终端通过堡垒机无法访问资产故障排查经验案例

运维审计 王周华 2020-05-31 发表

组网及说明

客户将堡垒机设备部署在内网，内外网终端均通过堡垒机访问资产，实现资产的安全访问和便捷管理，大致拓扑如下：



本次涉及设备的型号以及版本：A2000-V(二代) E6112

问题描述

反馈内网终端可以通过堡垒机访问资产设备，外网终端可以登录到堡垒机上，但是无法通过堡垒机访问资产设备。

过程分析

1、内网终端可以通过堡垒机访问资产设备。那么说明堡垒机到资产设备的连通性以及账号等的设置没有问题。

2、外网终端可以登录到堡垒机上。说明外网终端到设备的连通性正常并且出口设备的nat server映射功能正常。

3、那么就要分析外网终端通过堡垒机访问资产设备的过程。运维人员通过堡垒机运维设备时，堡垒机拉起客户端程序，客户端通过堡垒机和资产设备建立连接，也就是客户端和堡垒机建立连接，堡垒机再和资产设备建立连接。比如运维人员通过堡垒机用telnet方式访问资产设备，telnet属于字符服务，运维人员电脑拉起客户端程序后通过22端口到堡垒机（端口可以更改，如下），堡垒机再通过23端口和资产设备建立连接。

和现场工程师确认出口设备上的nat server配置，反馈是映射了堡垒机的443端口以及资产设备的telnet的23端口，而堡垒机的字符服务是22端口，所以应该映射的不是资产设备的23端口而是要映射堡垒机的22端口。

解决方法

让现场映射堡垒机的服务端口后问题解决。