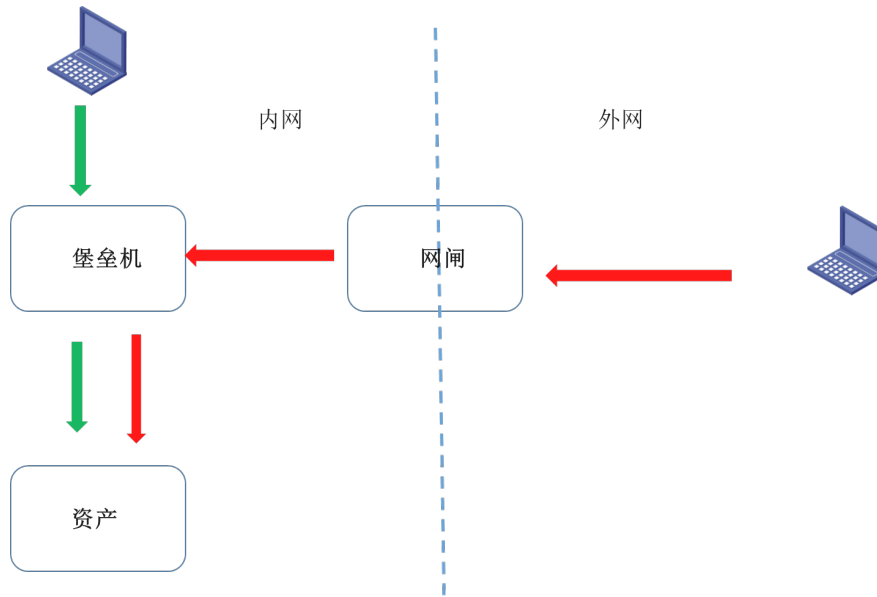


知 堡垒机过网闸访问资产异常问题分析

运维审计 网闸 孔凡安 2022-03-04 发表

组网及说明

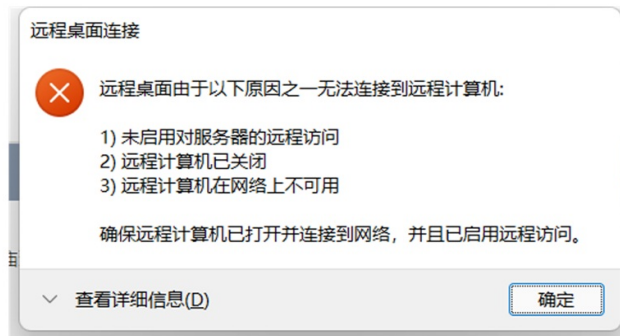


如图所示：内网环境，通过堡垒机可以正常访问资产，在网闸上做了对内网堡垒机地址的映射，希望通过公网也能正常使用堡垒机。结果堡垒机web界面可以正常访问，但是访问资产异常。

问题描述

在内网环境内使用堡垒机可以正常访问资产（RDP、SSH等方式）。

在网闸上做了对内网堡垒机地址的映射，希望通过公网也能正常使用堡垒机。结果堡垒机web界面可以正常访问，但是访问资产异常。



过程分析

首先，内网环境可以通过堡垒机访问资产，说明堡垒机的配置基本没问题。

其次，查看网闸侧对堡垒机地址的映射情况，发现对所有的端口都进行了映射，也没有问题。



外端机抓包发现只有访问堡垒机443端口的报文：

The screenshot shows a Wireshark packet capture window with the filter 'ip.addr eq 10.127.90.252 && tcp'. The packet list table is as follows:

| No. | Time | Source | Destination | Protocol | Time to Live | Identification | DD Sequence | Info |
|-----|-----------|---------------|---------------|----------|----------------|----------------|-------------|--|
| 75 | 1.881375 | | | 61 | 0x6d6e (28014) | | | 36456 → 443 [ACK] Seq=1 Ack=1 Win=254 Len=0 |
| 76 | 1.920555 | 10.127.90.252 | 10.127.90.252 | TCP | 252 | 0x4eac (20140) | | [TCP ACKed unsegmented] 443 → 36456 [ACK] Seq=1 |
| 636 | 10.561447 | | | 61 | 0x6d6f (28015) | | | 37582 → 443 [S] Seq=0 Win=29200 Len=0 MSS=1460 S |
| 637 | 10.577368 | | | 56 | 0x0000 (0) | | | 443 → 37582 [S] Seq=0 Ack=1 Win=29200 Len=0 |
| 638 | 10.577330 | | | 61 | 0x6d70 (28016) | | | 37582 → 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0 |
| 639 | 10.585848 | | | 61 | 0x6d71 (28017) | | | Client Hello |
| 640 | 10.588398 | | | 56 | 0xb88a (45194) | | | 443 → 37582 [ACK] Seq=1 Ack=518 Win=30336 Len=0 |
| 646 | 10.596010 | | | 56 | 0xb88b (45195) | | | Server Hello, Certificate, Server Key Exchange, Se |
| 647 | 10.596580 | | | 61 | 0x6d72 (28018) | | | 37582 → 443 [ACK] Seq=518 Ack=1392 Win=32128 Len=0 |
| 648 | 10.604689 | | | 61 | 0x6d73 (28019) | | | Alert (Level: fatal, Description: Certificate Unkn |
| 649 | 10.604716 | | | 61 | 0x6d74 (28020) | | | 37582 → 443 [FIN, ACK] Seq=525 Ack=1392 Win=32128 |
| 650 | 10.607300 | | | 56 | 0xb88c (45196) | | | 443 → 37582 [FIN, ACK] Seq=1392 Ack=526 Win=30336 |
| 651 | 10.607680 | | | 61 | 0x6d75 (28021) | | | 37582 → 443 [ACK] Seq=526 Ack=1393 Win=32128 Len=0 |
| 667 | 10.716406 | | | 61 | 0x6d76 (28022) | | | 37584 → 443 [S] Seq=0 Win=29200 Len=0 MSS=1460 S |
| 668 | 10.719325 | | | 56 | 0x0000 (0) | | | 443 → 37584 [S] Seq=0 Ack=1 Win=29200 Len=0 |
| 669 | 10.719802 | | | 61 | 0x6d77 (28023) | | | 37584 → 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0 |

怀疑访问资产的报文没到网闸，发现pc到网闸地址3389和22端口都是不通的。

解决方法

PC到网闸设备之间有安全设备拦截了访问网闸地址3389、22端口的报文，放通后访问资产业务正常。涉及开放的端口具体可以参考官网配置指导。

