外网PC墙使用RemoteApp方式访问内网服务器的应用程序不成功（防火墙）

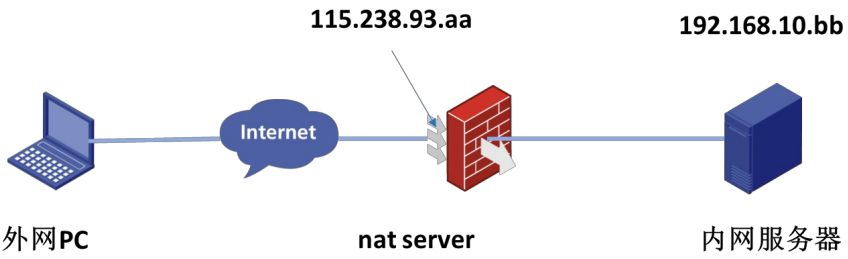
NAT 彭钦 2021-11-20 发表

组网及说明

防火墙出口做了nat server

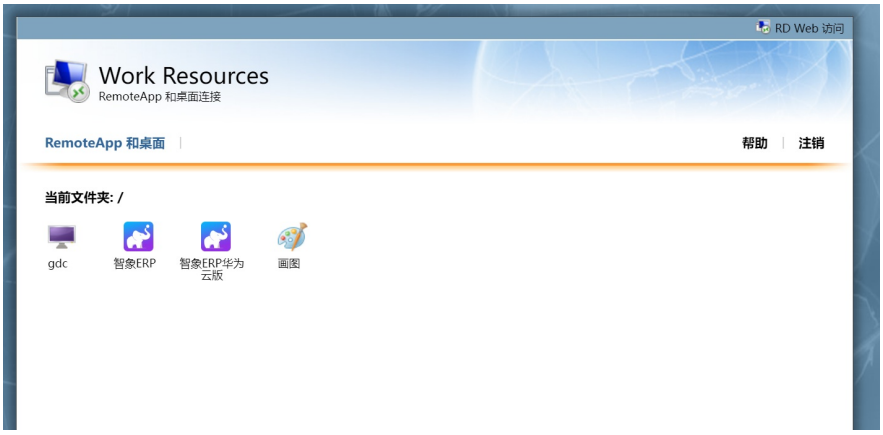
nat server protocol tcp global 115.238.93.aa xxxx inside 192.168.10.bb 443 //用于网页访问

nat server protocol tcp global 115.238.93.aa yyyy inside 192.168.10.bb 3389 //用于远程桌面



问题描述

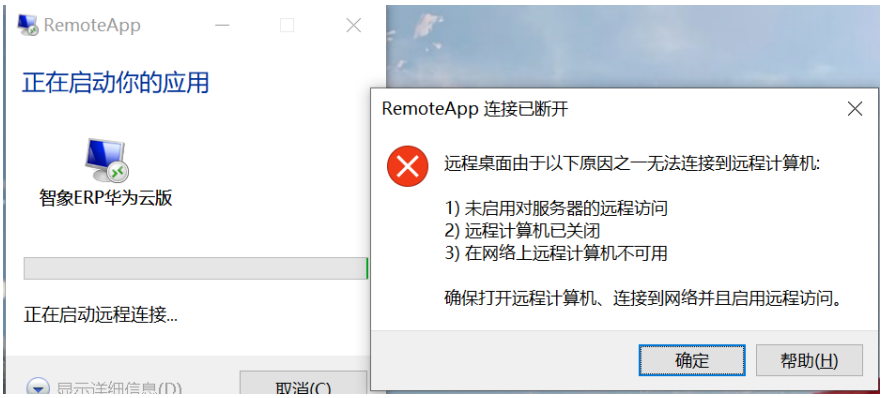
外网PC通过浏览器进入内网服务器的RD Web**访问的**https网页，内网服务器发布了四个应用（gdc、智象ERP、智象ERP华为云版、画图）以供用户可以通过rdp文件（点击图中发布的应用，以“画图”为例）直接访问。



rdp文件:

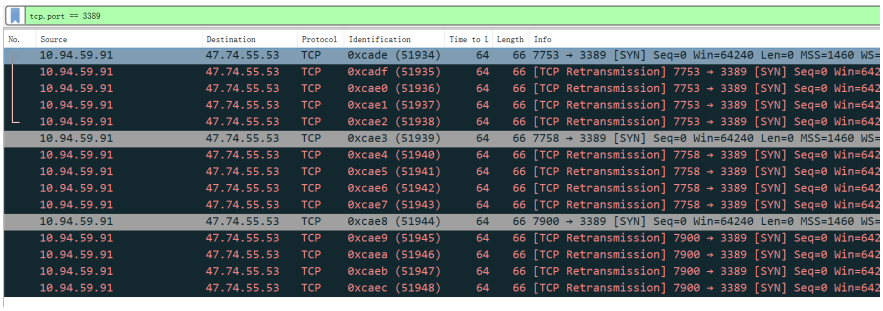
cpub-mspaint-farm-CmsRdsh.rdp

外网PC远程进入内网服务器的画图程序失败:



过程分析

（1）点击rdp文件后，在外网PC抓包，发现外网PC一直在给47.74.55.53的3389端口重传SYN包。该地址并不是内网地址，也不是防火墙地址。怀疑这是在和某个服务器交互报文。



tcp.port == 3389

No.	Source	Destination	Protocol	Identification	Time to l	Length	Info
	10.94.59.91	47.74.55.53	TCP	0xcade (51934)	64	66	7753 → 3389 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=
	10.94.59.91	47.74.55.53	TCP	0xcadf (51935)	64	66	[TCP Retransmission] 7753 → 3389 [SYN] Seq=0 Win=642
	10.94.59.91	47.74.55.53	TCP	0xcae0 (51936)	64	66	[TCP Retransmission] 7753 → 3389 [SYN] Seq=0 Win=642
	10.94.59.91	47.74.55.53	TCP	0xcae1 (51937)	64	66	[TCP Retransmission] 7753 → 3389 [SYN] Seq=0 Win=642
	10.94.59.91	47.74.55.53	TCP	0xcae2 (51938)	64	66	[TCP Retransmission] 7753 → 3389 [SYN] Seq=0 Win=642
	10.94.59.91	47.74.55.53	TCP	0xcae3 (51939)	64	66	7758 → 3389 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=
	10.94.59.91	47.74.55.53	TCP	0xcae4 (51940)	64	66	[TCP Retransmission] 7758 → 3389 [SYN] Seq=0 Win=642
	10.94.59.91	47.74.55.53	TCP	0xcae5 (51941)	64	66	[TCP Retransmission] 7758 → 3389 [SYN] Seq=0 Win=642
	10.94.59.91	47.74.55.53	TCP	0xcae6 (51942)	64	66	[TCP Retransmission] 7758 → 3389 [SYN] Seq=0 Win=642
	10.94.59.91	47.74.55.53	TCP	0xcae7 (51943)	64	66	[TCP Retransmission] 7758 → 3389 [SYN] Seq=0 Win=642
	10.94.59.91	47.74.55.53	TCP	0xcae8 (51944)	64	66	7900 → 3389 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=
	10.94.59.91	47.74.55.53	TCP	0xcae9 (51945)	64	66	[TCP Retransmission] 7900 → 3389 [SYN] Seq=0 Win=642
	10.94.59.91	47.74.55.53	TCP	0xcaea (51946)	64	66	[TCP Retransmission] 7900 → 3389 [SYN] Seq=0 Win=642
	10.94.59.91	47.74.55.53	TCP	0xcaeb (51947)	64	66	[TCP Retransmission] 7900 → 3389 [SYN] Seq=0 Win=642
	10.94.59.91	47.74.55.53	TCP	0xcaec (51948)	64	66	[TCP Retransmission] 7900 → 3389 [SYN] Seq=0 Win=642

（2）下载已由管理员创建并分发的远程桌面协议 (.rdp) 文件，使用notepad编辑rdp文件，发现存在一个full address。查看微软的受支持的远程桌面 RDP 文件设置，发现full address是指定要连接到的远程计算机的名称或 IP 地址，这是 RDP 文件中唯一需要的设置。

RDP文件内容：

```
use multimon:i:1
remoteapplicationmode:i:1
server port:i:3389
allow font smoothing:i:1
promptcredentialonce:i:0
gatewayusagemethod:i:2
gatewayprofileusagemethod:i:0
gatewaycredentialssource:i:0
full address:s:REMOSERVER.AOZHAN.COM
alternate shell:s:||mspaint
remoteapplicationprogram:s:||mspaint
gatewayhostname:s:
remoteapplicationname:s:画图
remoteapplicationcmdline:s:
workspace id:s:remoserver.aozhan.com
use redirection server name:i:1
loadbalanceinfo:s:tsv://MS Terminal Services Plugin.1.farm
```

https://docs.microsoft.com/zh-cn/windows-server/remote/remote-desktop-services/clients/rdp-files /

/参考微软网站上的 受支持的远程桌面 RDP 文件设置

RDP 设置	说明	值
full address:s:value	电脑名称： 此设置指定要连接到的远程计算机的名称或 IP 地址。 这是 RDP 文件中唯一需要的设置。	有效的名称、IPv4 地址或 IPv6 地址。

解决方法

将full address修改成了full address:s:115.238.93.cc:yyyy,再次打开rdp文件，此时可正常访问内网服务器的“画图”程序。