

某局点GAP2000业务不通问题处理经验案例

网闸 部署方式 zhilliao_l6nhL 2018-09-24 发表

组网及说明

不涉及

问题描述

客户现场想通过在办公区和隔离区中间部署一台GAP2000网闸设备，来实现办公区PC可以通过域名的方式访问隔离区的服务器。现场反馈添加完通道之后通过域名无法实现正常访问。

过程分析

1、核对网闸内外端机地址、路由及通道配置

IP地址管理

内端机

SLOT0/0

SLOT0/1

SLOT0/2

+

ID	IP	掩码
5	10.198.28.253	255.255.255.0

路由配置

内端机

外端机

IP地址管理

外端机

+

SLOT0/0	ID	IP	掩码
SLOT0/1	2	172.30.1.252	255.255.255.0

路由配置

内端机

外端机

搜索

ID	目的子网	子网掩码	网卡名称	网关
4	0.0.0.0	0.0.0.0	SLOT0/0	172.30.1.254

通道管理

+										搜索	
ID	方向	类型	监听地址	监听端口	目的地址	目的端口	端口段	空闲超时时间(s)	FIN超时时间(s)	连接地址	是否
1	外端 → 内端	TCP	172.30.1.252	80	59.215.233.89	80		0	30	10.198.28.253	是

根据上面的配置，结合现场的实际情况，办公区的PC用的是公网DNS服务器地址，所以无法解析到隔离区的服务器域名对应的真实IP地址，于是建议现场直接用监听地址进行访问，现场反馈还是无法正常访问，网页提示连接超时。

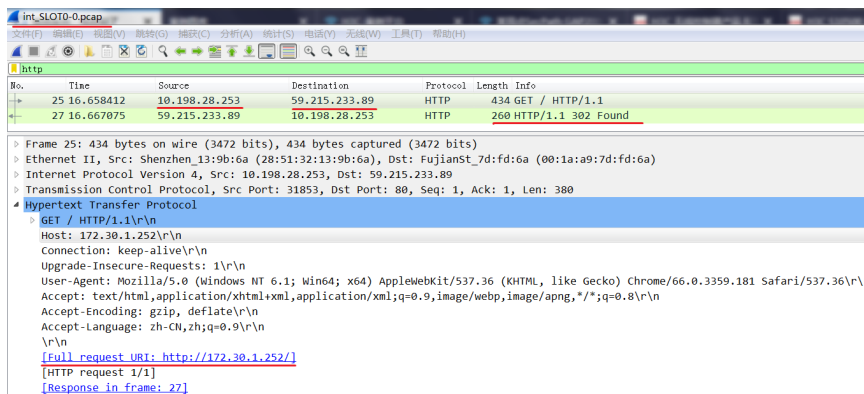
通过在内外端机同时抓包分析，如下图所示：

外端机收到http的报文，目的地址是监听地址172.30.1.252，同时Full request URI填充为：172.30.1.252

No.	Time	Source	Destination	Protocol	Length	Info
1012	10.800317	172.30.10.244	172.30.1.252	HTTP	434	GET / HTTP/1.1
1014	10.850658	172.30.1.252	172.30.10.244	HTTP	260	HTTP/1.1 302 Found

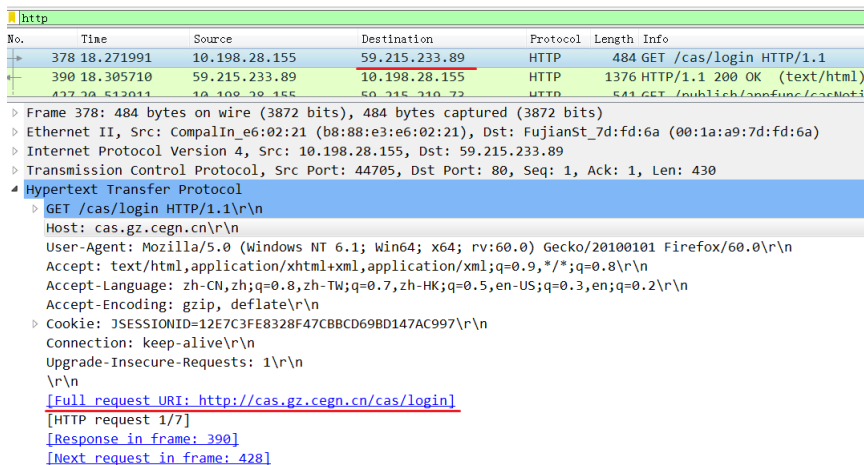
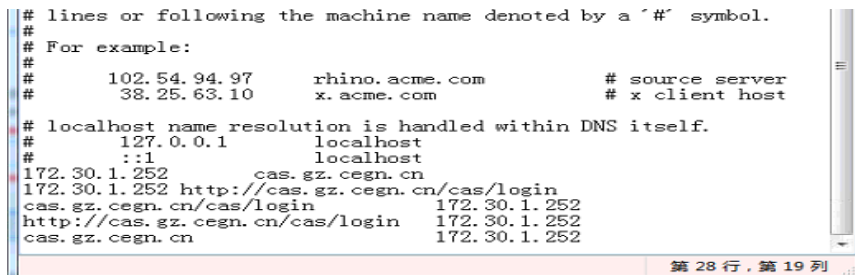
```
> Frame 1012: 434 bytes on wire (3472 bits), 434 bytes captured (3472 bits) on 0
> Ethernet II, Src: HuaweiTe_58:0f:a5 (00:25:9e:58:0f:a5), Dst: Shenzhen_13:9a:ba (28:51:32:13:9a:ba)
> Internet Protocol Version 4, Src: 172.30.10.244, Dst: 172.30.1.252
> Transmission Control Protocol, Src Port: 57660, Dst Port: 80, Seq: 1, Ack: 1, Len: 380
> Hypertext Transfer Protocol
  > GET / HTTP/1.1\r\n
    Hosts: 172.30.1.252\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.181 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: zh-CN,zh;q=0.9\r\n
    \r\n
    [Full request URI: http://172.30.1.252/]
    [HTTP request 1/1]
    [Response in frame: 1014]
```

内端机对报文同时做源目的地址转换并且发送出去，目的地址为59.215.233.89，同时Full request URI还是172.30.1.252



2、跟现场了解到服务器对URL请求标识有校验，必须和真实服务器的地址一致才会响应，但是网闸不会修改HTTP报文中的荷载内容，只是修改报文的地址，所以服务器响应了302的报错，网页无法正常访问。

为了进一步验证，让客户修改主机hosts文件，手动添加监听地址和域名的映射关系，然后使用域名访问，是可以正常访问的。



解决方法

针对上述这种情况，如果是少量终端可以通过修改终端hosts文件的方式解决。

如果终端数量较多，需要配合DNS服务器解析WEB服务器的真实地址解决。