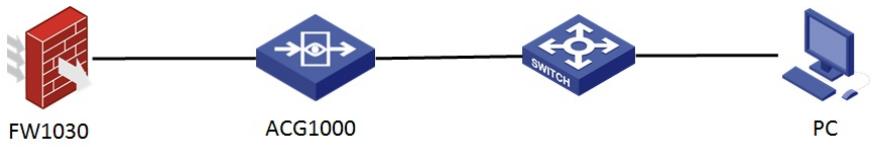
某局点使用ACG1000部署HTTPS解密失败案例

ACG1000 证书 王鸿渐 2018-09-24 发表

组网及说明

拓扑如下：

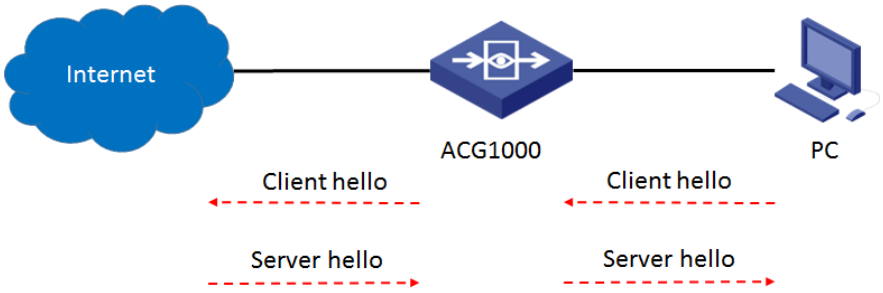


问题描述

某局点ACG1000透明部署https解密用于访问网站审计和邮件审计，但是配置后发现开启https解密，内网PC无法正常访问https网页，关闭https解密后正常，开启邮箱解密配置则无法正常审计到邮箱内容。

过程分析

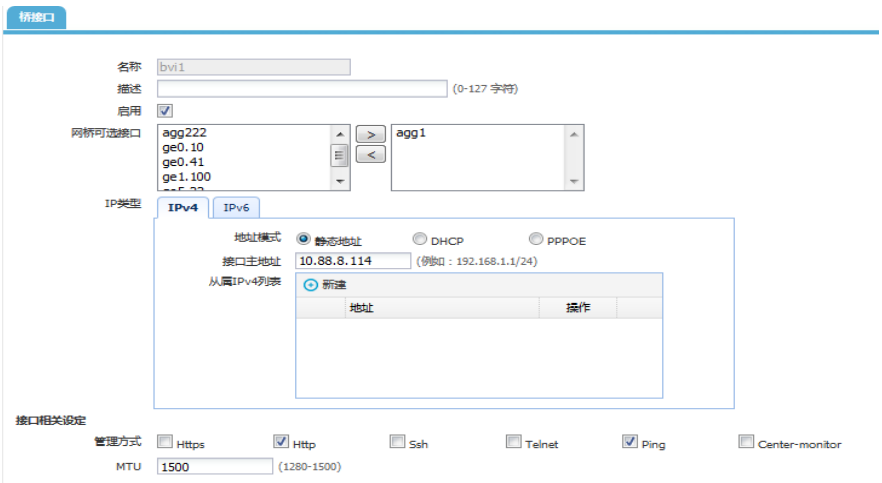
首先我们先理解一下ACG透明模式下HTTPS解密的原理：



.....

1.主机访问https的hello 报文经过ACG时被替换了源地址，以网桥接口地址继续向外网发送SSL请求。
2.外网向ACG的网桥接口回应Server hello时，里面携带的服务器证书信息被替换为ACG本地证书进行解析。
所以整个HTTPS解密过程中，主机的DNS需要指向设备的入接口，以保证DNS流量过ACG，并且ACG上的网桥接口地址必须与外网互通，按照以上两点思路即可。

检查主机和ACG的相关配置



描述	Intel(R) Dual Band Wireless-AC 8265
物理地址	F8-94-C2-9F-F4-39
已启用 DHCP	否
IPv4 地址	192.168.3.10
IPv4 子网掩码	255.255.255.0
IPv4 默认网关	192.168.3.1
IPv4 DNS 服务器	10.88.8.114
IPv4 WINS 服务器	
已启用 NetBIOS over Tcpip	是
连接-本地 IPv6 地址	fe80::fc81:9445:9116:a3ec%18

在ACG出口上抓包查看，服务器端未回应server hello报文。

```
 766 45.638604  10.88.8.114     172.25.14.130   TLSv1.2    571 Client Hello
 767 45.642034  10.88.8.114     172.25.14.130   TLSv1.2    571 Client Hello

 769 45.645424  10.88.8.114     172.25.14.130   TLSv1.2    571 Client Hello
 770 45.648362  10.88.8.114     172.25.14.130   TLSv1.2    571 Client Hello
```

在主机上解析外网DNS，解析失败。

```
C:\Users\     >nslookup baidu.com
DNS request timed out.
    timeout was 2 seconds.
服务器:  UnKnown
Address:  10.88.8.114

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** 请求 UnKnown 超时
```

最后在ACG使用网桥接口IP地址PING外网DNS地址时，发现无法PING通，我们怀疑问题在出口防火墙上。

解决方法

经排查发现出口防火墙上NAT未放通网桥接口地址，添加后问题解决。