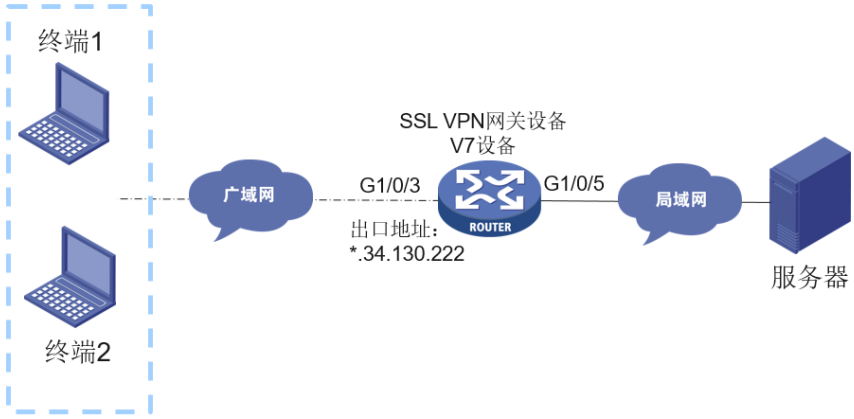
某局点V7型号MSR3610-IE-EAD路由器播入SSL VPN异常的处理案例

SSL VPN　徐猛　2021-12-30 发表

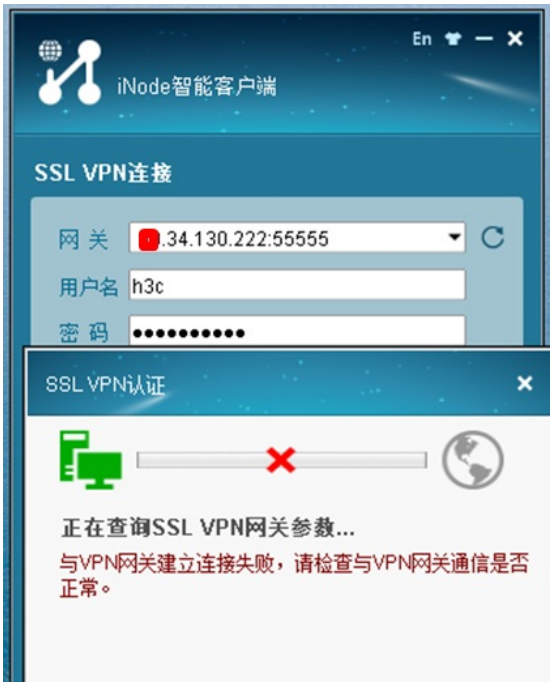
组网及说明



现场拓扑图如上，3口为外网口，同时作为SSL VPN的gateway地址接口。供移动接入人员的SSL VPN接入。

问题描述

组网配置完成后，外网用户播入SSL VPN异常。inode报错提示如下：



过程分析

（1）检查配置无误，使用设备的缺省证书方式方式。

```
#
interface GigabitEthernet0/3
 port link-mode route
 ip address *.34.130.222 255.255.255.252
#
sslvpn ip address-pool ga *.168.50.0 192.168.51.250
#
interface SSLVPN-AC1
 ip address *.168.51.254 255.255.254.0
#
local-user sslvpn class network
 password cipher $c$3$LNNvjy7sDq5d8bfzILTf3nCWjah2bIVrHg==
 service-type sslvpn
 authorization-attribute user-role network-operator
 authorization-attribute sslvpn-policy-group default
#
sslvpn gateway ga
 ip address *.34.130.222 port 55555
 service enable
#
sslvpn context ga
 gateway ga domain system
 ip-tunnel interface SSLVPN-AC1
 ip-tunnel address-pool ga mask 255.255.254.0
 ip-route-list 1
  include *.168.1.0 255.255.255.0
 policy-group default
  filter ip-tunnel acl 3101
  ip-tunnel access-route ip-route-list 1
 default-policy-group default
 aaa domain system
 service enable
#
domain system
#
 domain default enable system
#
```

（2）采集设备的ssl vpn播入过程debug记录。debug中报错bad record mac.，和使用web打开gateway的地址+端口报错内容相同：

```
*Dec 28 20:45:24:884 2021 H3C SSLVPNK/7/SSLVPN_DEBUG_KSSL_HANDSHAKE: Send: TLS 1.0Alert [length 0002], level: fatal, reason: bad_record_mac.
*Dec 28 20:45:24:884 2021 H3C SSLVPNK/7/SSLVPN_KSSL_PACKET:
 02 14
*Dec 28 20:45:24:884 2021 H3C SSLVPNK/7/SSLVPN_DEBUG_KSSL_INFO: SSL3 alert write, level: fatal, reason: bad record mac.
```

发现有**bad record mac.的记录。**

和如下使用电脑直接web访问*.34.130.222:55555网关地址端口的报错SSL_ERROR_BAD_MAC_ALERT相似。

建立安全连接失败

经反馈二线和研发确认：

这款型号设备硬件加密引擎不支持当前的算法，关闭硬件加密引擎，改为软件加密，就正常了。

probe视图下，关闭加密引擎crypto engine accelerator disable。

连接到 59.34.130.222:55555 时发生错误。SSL 对等端报告了不正确的消息认证码。

错误代码：SSL_ERROR_BAD_MAC_ALERT

- 由于不能验证所收到的数据是否可信，无法显示您想要查看的页面。
- 建议向此网站的管理员反馈这个问题。

详细了解...

重试

开始怀疑是设备缺省证书的问题，于是对设备进行了系统的升级重装，但是升级重装了系统后故障依旧。