联软科技
LEAGSOFT

LeagSoft UniVPN 客户端

维护指南

目 录

1 故障处理：SSL VPN 1
1.1 概述 1
1.2 使用须知 1
1.3 SSL VPN 支持列表 1
1.3.1 SSL VPN 支持接入方式 1
1.4 UniVPN 拨号 SSL VPN 故障-V500R005C20 和 V600R007C20 2
1.4.1 打开 UniVPN 时出现警告 2
1.4.1.1 警告：已经有客户端正在运行，不能再运行该程序！ 2
1.4.1.2 警告：无法建立 VPN 连接，VPN 服务器可能无法到达 4
1.4.1.3 超过最大限制，最大限制 16 条 5
1.4.1.4 已达到最大数目，无法新建 6
1.4.2 采用用户名/密码方式登录时出现警告 6
1.4.2.1 警告：不可信的 VPN 服务器证书！ 6
1.4.2.2 认证失败！ 7
1.4.2.3 用户连接数已达到上限，请稍后重试！ 10
1.4.2.4 网络拓展启动失败 11
1.4.2.5 主机检查失败！ 13
1.4.2.6 接受返回码超时！ 13
1.4.2.7 当前连接不支持快速隧道模式，请切换到可靠隧道模式后重试 13
1.4.3 采用证书方式登录时出现警告 14
1.4.3.1 找不到用户证书 15
1.4.3.2 提示：您的用户证书验证非法，请提供合法的证书！ 16
1.4.3.3 提示：认证失败！ 19
1.4.4 登录成功后业务出现异常 23
1.4.4.1 访问内网资源卡顿，ping 内网延迟大 23
1.4.4.2 登录成功后，无法访问公网 24
1.4.4.3 警告：您被强制下线，请重新登录！ 25
1.4.4.4 提示：无法建立 VPN 连接，VPN 服务器可能无法到达 25
1.4.4.5 终端加入 AD 域后，SSL VPN 用户接入一段时间后异常掉线 26
1.4.4.6 新增 SSL VPN 网络拓展可访问网段后，用户无法访问新增网段 28

1.5 SSL VPN 常见咨询类问题 FAQ-V500R005C20 和 V600R007C20 30
1.5.1 SSL VPN 如何实现一个账号多处同时登录 30
1.5.2 连接成功后无法访问资源 31
1.5.3 SSL VPN 证书认证相关知识点 31
1.5.4 SSL VPN 是否支持用户和终端绑定 32
1.5.5 高端防火墙是否支持 SSL VPN 业务 32
1.5.6 如何使用 XCA 制作设备证书和用户证书 32
1.5.7 UniVPN 安装和运行是否都需要管理员权限 48
1.5.8 SSL VPN 使用客户端拨号成功后，终端是否支持自行修改账户密码 48
1.5.9 为什么要提前在设备侧上传 ActiveX 控件 49
1.5.10 虚拟网关服务视图和虚拟网关用户组视图下配置的网络扩展路由模式哪个优先级高 49
1.5.11 SSL VPN 网络扩展三种路由模式下在终端生成的路由有什么区别 49
1.5.11.7 手动路由模式 50
1.5.11.8 分离路由模式 50
1.5.11.9 全路由模式 51
1.5.12 SSL VPN 是否支持双因子认证 51
1.5.13 使用客户端拨号登录无法生成虚拟网卡，如何解决 52
1.5.14 SSL VPN 有哪些命令可以用来采集调试日志 52
1.5.15 SSL VPN 接入后 ping 内网延迟大，如何解决 52
1.5.16 SSL VPN 和用户管理的关联 52
1.5.17 SSL VPN 角色授权知识点 53
1.5.18 SSL VPN 认证后如何基于用户做权限管控 53
1.5.19 SSL VPN 用户接入后对于非法操作如何溯源 53
1.5.20 SSL VPN 服务器认证场景下的授权规则如何 54
1.5.21 UniVPN 的日志采集方法 56
1.5.22 SSL VPN 常见业务日志有哪些 58
1.5.23 SSL VPN 调整网络扩展参数是否强制用户下线 59
1.5.24 SSL VPN 业务报文的域间关系是怎样确定 59
1.5.25 SSL VPN 登录之后能否访问防火墙内网接口地址进行管理 59
1.5.26 双机场景 SSL VPN 哪些配置可以备份到对端 60
1.5.27 SSL VPN 是否支持 IPv6 60
1.5.28 SSL VPN 控件支持浏览器的情况 60
1.5.29 SSL VPN 各子特性的应用范围 61
1.5.30 SSL VPN 是否支持友商 VPN 客户端拨号 61
1.5.31 SVN 和防火墙 SSL VPN 特性区别 61
1.5.32 OSPF 组网下如何发布 SSL VPN 业务地址和网络扩展地址池的路由 62
1.5.33 SSL VPN 是否支持双机热备负载分担 64
1.5.34 SSL VPN 是否支持双机热备主备备份 64
1.5.35 SSL VPN 用户是否支持不认证登录 64

1.5.36 UniVPN 是否支持手机终端 64
1.5.37 SSL VPN 如何实现用户绑定网络扩展虚拟地址 64
1.5.38 SSL VPN 网络扩展虚拟 IP 地址分配规则 65
1.5.39 SSL VPN 有哪些常见调试日志 65
1.5.40 UniVPN 和 SecoClient 是否能同时使用 74
1.5.41 打开 UniVPN 前 PC 主机报错 74
1.5.42 VPN 服务器可以访问公网，内网用户建立 VPN 连接后是否可以访问公网资源 75
1.5.43 MacOS 系统用户使用 UniVPN 建立 VPN 连接后无法访问公网域名，如何解决 75
1.5.44 使用客户端是否要放开某些端口 75
1.6 UniVPN 拨号 SSL VPN 故障-V600R21C10 75
1.6.1 打开 UniVPN 时出现警告 75
1.6.1.1 警告：已经有客户端正在运行，不能再运行该程序！ 75
1.6.1.2 警告：无法建立 VPN 连接，VPN 服务器可能无法到达 77
1.6.1.3 超过最大限制，最大限制 16 条 78
1.6.1.4 已达到最大数目，无法新建 79
1.6.2 采用用户名/密码方式登录时出现警告 79
1.6.2.1 警告：不可信的 VPN 服务器证书！ 79
1.6.2.2 认证失败！ 80
1.6.2.3 用户连接数已达到上限，请稍后重试！ 83
1.6.2.4 网络拓展启动失败 84
1.6.2.5 主机检查失败！ 86
1.6.2.6 接受返回码超时！ 87
1.6.2.7 当前连接不支持快速隧道模式，请切换到可靠隧道模式后重试 87
1.6.3 采用证书方式登录时出现警告 88
1.6.3.1 找不到用户证书 88
1.6.3.2 提示：您的用户证书验证非法，请提供合法的证书！ 90
1.6.3.3 提示：认证失败！ 93
1.6.4 登录成功后业务出现异常 97
1.6.4.1 访问内网资源卡顿，ping 内网延迟大 97
1.6.4.2 登录成功后，无法访问公网 98
1.6.4.3 警告：您被强制下线，请重新登录！ 98
1.6.4.4 提示：无法建立 VPN 连接，VPN 服务器可能无法到达 99
1.6.4.5 终端加入 AD 域后，SSL VPN 用户接入一段时间后异常掉线 99
1.7 移动客户端 FAQ 101
1.7.1 如何导入国密证书 103
1.7.2 如何反馈 iOS 问题 112
1.7.3 取消自动登录（安卓） 118
1.7.4 iOS 异常卡顿的解决方法 118
1.7.5 后台设置国密加证书匿名的情况 119

1.7.6 安卓客户端登录后通知栏显示情况 119
1.7.7 UniConnect 是否支持 MAC 认证 119
1.7.8 IOS 系统是否支持取消自动登录 119
1.7.9 设备熄屏状态掉线 119
1.7.10 多个 VPN 存在同一款手机导致 UniConnect 不可用 119
1.7.11 UniConnect 是否支持多种系统语言 119
1.7.12 VPN 编辑信息界面，连接名称能否输入特殊字符 119
1.7.13 IOS 系统是否支持暗黑模式 119

1 故障处理：SSL VPN

1.1 概述
1.2 使用须知
1.3 SSL VPN 支持列表
1.4 UniVPN 拨号 SSL VPN 故障
1.5 SSL VPN 常见咨询类问题 FAQ

1.1 概述

本文档介绍了 SSL VPN 故障和咨询问题的最常见解决方案，包括 UniVPN 拨号故障、浏览器拨号故障和常见咨询类问题，供您在开始排除故障并致电华为技术支持之前尝试。

1.2 使用须知

使用前建议您了解华为防火墙 SSL VPN 的基本配置。
本文档以华为 USG6000 系列防火墙产品 V5 版本为例。不同产品和版本的实现可能会有差异。
本文档中 FW 是防火墙的缩写。
本文档中使用到的公网 IP 地址均为示意，不指代任何实际意义。

1.3 SSL VPN 支持列表

1.3.1 SSL VPN 支持接入方式

接入方式	说明
UniVPN	UniVPN 是深圳市联软科技公司推出的一款用于 VPN 远程接入的终端软件，主要为移动办公用户远程访问企业内网资源提供安全、便捷的接入服务。SSL VPN 包括 Web 代理、端口转发、文件共享和网络扩展这 4 类业务，UniVPN 客户端仅支持使用网络扩展业务。

1.4 UniVPN 拨号 SSL VPN 故障-V500R005C20 和 V600R007C20

本章节介绍 UniVPN 客户端在接入防火墙设备 V500R005C20 和 V600R007C20 及以后版本时拨号 SSL VPN 的故障处理方式。

1.4.1 打开 UniVPN 时出现警告

警告：已经有客户端正在运行，不能再运行该程序！
警告：无法建立 VPN 连接，VPN 服务器可能无法到达！
警告：当前网关已达到最大限制 16！
警告：已超过最大连接数量，新建失败！

1.4.1.1 警告：已经有客户端正在运行，不能再运行该程序！

现象描述

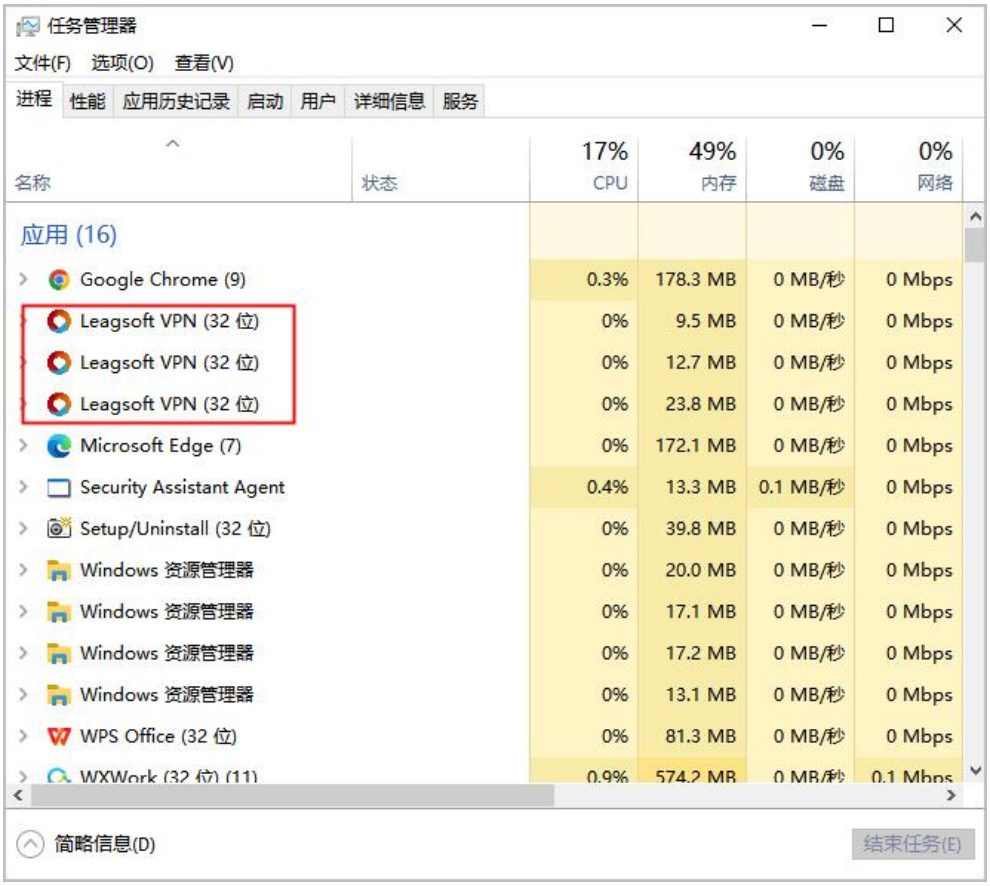
打开 UniVPN 时，系统告警“已经有客户端正在运行，不能再运行该程序！”。

可能原因

终端上已经有 UniVPN 在运行。

处理步骤

关闭已有的 UniVPN 运行程序，并检查任务管理器中的 UniVPN 进程是否同步关闭。


任务管理器
文件(F) 选项(O) 查看(V)
进程 性能 应用历史记录 启动 用户 详细信息 服务
名称 状态 17% CPU 49% 内存 0% 磁盘 0% 网络
应用 (16)
Google Chrome (9) 0.3% 178.3 MB 0 MB/秒 0 Mbps
Leagsoft VPN (32 位) 0% 9.5 MB 0 MB/秒 0 Mbps
Leagsoft VPN (32 位) 0% 12.7 MB 0 MB/秒 0 Mbps
Leagsoft VPN (32 位) 0% 23.8 MB 0 MB/秒 0 Mbps
Microsoft Edge (7) 0% 172.1 MB 0 MB/秒 0 Mbps
Security Assistant Agent 0.4% 13.3 MB 0.1 MB/秒 0 Mbps
Setup/Uninstall (32 位) 0% 39.8 MB 0 MB/秒 0 Mbps
Windows 资源管理器 0% 20.0 MB 0 MB/秒 0 Mbps
Windows 资源管理器 0% 17.1 MB 0 MB/秒 0 Mbps
Windows 资源管理器 0% 17.2 MB 0 MB/秒 0 Mbps
Windows 资源管理器 0% 13.1 MB 0 MB/秒 0 Mbps
WPS Office (32 位) 0% 81.3 MB 0 MB/秒 0 Mbps
简略信息(D)
结束任务(E)

1.4.1.2 警告：无法建立 VPN 连接，VPN 服务器可能无法到达

现象描述

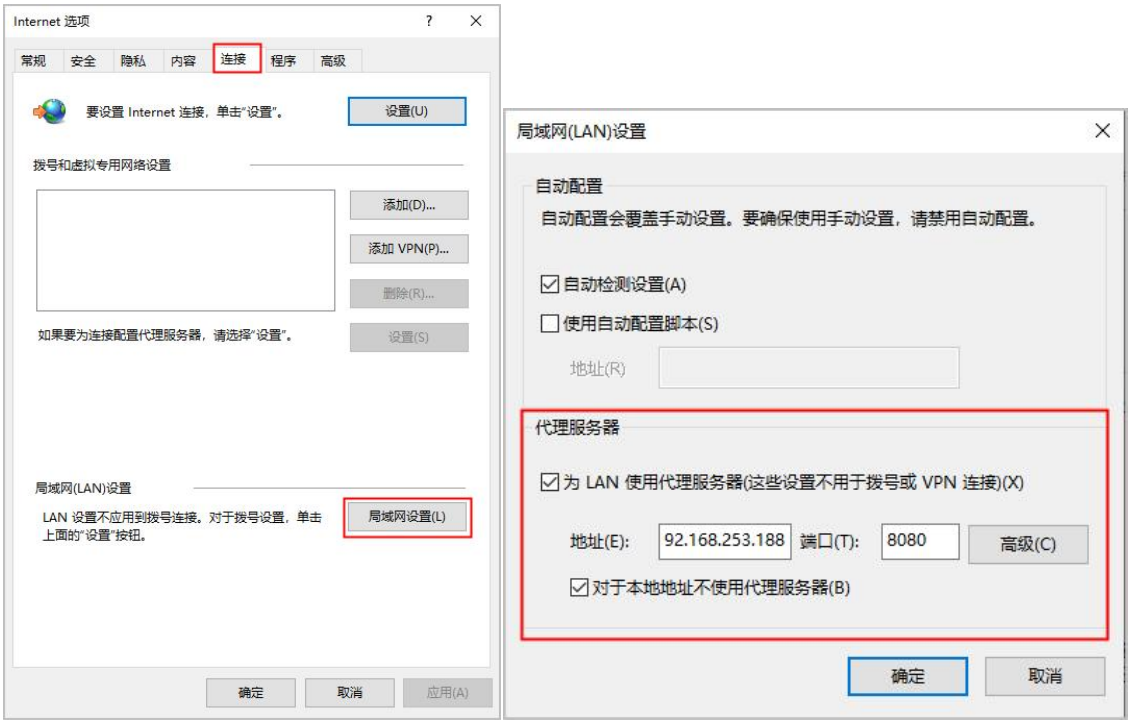
连接 VPN 网关时，系统告警“无法建立 VPN 连接，VPN 服务器可能无法到达”。

可能原因

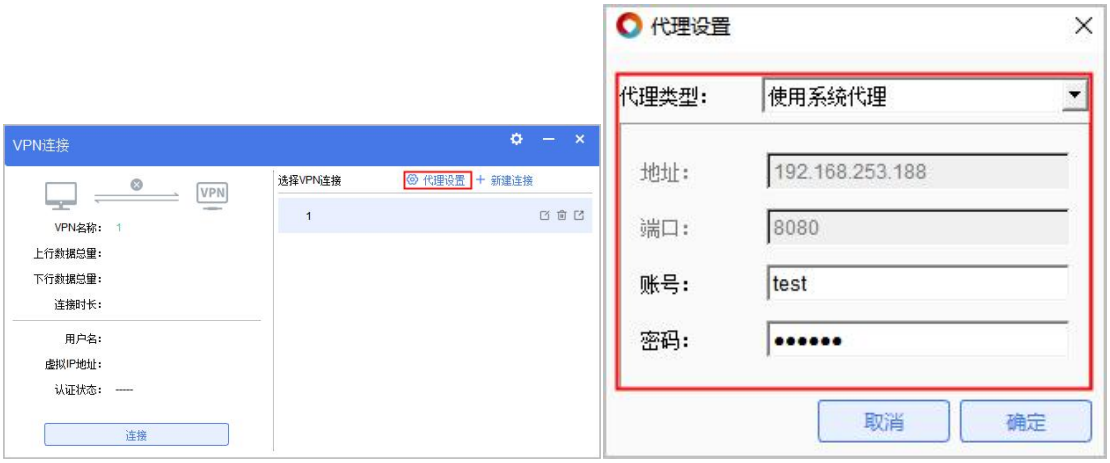
1. UniVPN 到 VPN 网关的路由不可达。
2. UniVPN 上 VPN 网关的 IP 地址或端口填写错误。
3. UniVPN 和 VPN 网关版本不配套。
4. 终端通过代理服务器上网的场景（如 192.168.253.188），UniVPN 未设置代理拨号公网的 VPN 网关。

处理步骤

- 原因 1 的问题定位及解决方法。
  1. 在 UniVPN 所在的终端上 Ping VPN 网关的 IP 地址，检查路由是否可达。
  2. 如果路由不可达，请配置 UniVPN 到 VPN 网关的路由。如果路由可达，表明该问题不是路由原因造成的，请转入分析下一种原因。
- 原因 2 的问题定位及解决方法。
  请检查 UniVPN 上配置的 VPN 网关 IP 地址、端口是否与 VPN 网关侧配置的一致。
- 原因 3 的问题定位及解决方法。
  目前和 UniVPN 配套的 VPN 网关软件版本有 FW V500R005C20SPC500、FW V600R007C20SPC300（SPC301/SPC 302 版本除外）、 V600R021C10，及其它们之后的版本。它们之前的版本，和 UniVPN 并不配套。
- 原因 4 的定位及解决办法。
  检查终端是否通过代理服务器上网。



如果是，UniVPN 也需要配置代理参数，如下图。



1.4.1.3 超过最大限制，最大限制 16 条

现象描述

在 UniVPN 新建连接界面，在远程网关中输入 16 条网关地址以后，单击“添加”，系统告警“超过最大限制，最大限制 16 条”。

可能原因

在客户端新建连接界面中，远程网关已经添加了 16 条，达到了最大可输入网关数。

处理步骤

网关地址达到 16 条后，不再继续添加网关地址。

1.4.1.4 已达到最大数目，无法新建

现象描述

在 UniVPN 主界面，在选择 VPN 连接中添加了 16 个连接配置，单击“+”，系统告警“已达到最大数目，无法新建”。

可能原因

在客户端主界面中，连接配置已经添加了 16 条，达到了最大可添加连接配置数。

处理步骤

连接配置添加 16 条后，不在继续新建

1.4.2 采用用户名/密码方式登录时出现警告

警告：不可信的 VPN 服务器证书！

警告：认证失败！

警告：用户连接数已达到上限，请稍后重试！

警告：网络扩展启动失败！

警告：主机检查失败！

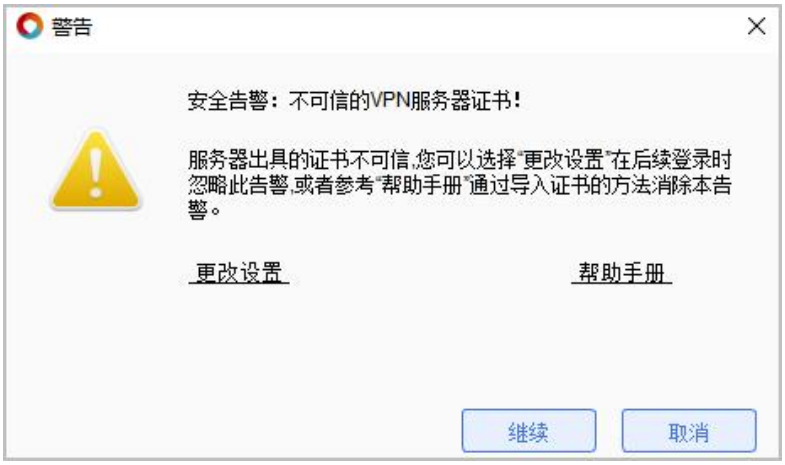
警告：接收返回码超时！

警告：当前连接不支持快速隧道模式，请切换到可靠隧道模式后重试

1.4.2.1 警告：不可信的 VPN 服务器证书！

现象描述

用户使用 UniVPN 通过 SSL VPN 隧道登录 SSL VPN 虚拟网关时，系统弹出如下提示。



可能原因

UniVPN 上缺少认证虚拟网关身份的 CA 证书。

处理步骤

要消除该告警有以下两个方法：

- 单击“设置”，去勾选“VPN 验证服务器可信”。

在用户确定自己登录的虚拟网关身份真实的情况下，可以采用此方法。

- 为 UniVPN 和虚拟网关颁发证书。

用户在无法有效识别虚拟网关身份真实性的情况下，推荐使用此方法。

制作两本证书，一本设备证书放置在虚拟网关上，另一本 CA 证书放置在 UniVPN 所在的主机上。如果用户所在企业已有证书系统，则可以利用自有的系统制作证书。如果没有证书系统，可以使用 XCA 软件制作证书。

UniVPN 通过 SSL VPN 隧道登录虚拟网关时，虚拟网关会向 UniVPN 推送设备证书，只要 UniVPN 上的 CA 证书可以识别虚拟网关的设备证书，系统就不会再提示证书校验非法的告警了。

证书的制作方法请参见如何使用 XCA 制作设备证书和用户证书。

1.4.2.2 认证失败！

现象描述

在 UniVPN 登录界面，输入用户名和密码以后，单击“登录”，系统告警“认证失败！”。

可能原因

1. 用户名或密码错误，用户过期或用户被锁定。
2. 虚拟网关绑定了不正确的认证域。
3. 认证域未启用 SSL VPN 接入场景。
4. 虚拟网关未启动网络扩展特性。
5. SSL VPN 登录的设备处于双机备状态（HRP_S），而 SSL VPN 不支持在备设备上登录上线。
6. SSL VPN 虚拟网关是共享型，非独占型。
7. 认证域采用服务器认证，新用户认证选项配置了“不允许新用户登录”，但用户在本地不存在。
8. 认证域采用 AD/LDAP 服务器认证，服务器上配置用户的属性启用了“首次登录必须修改密码”。
9. 客户端环境通往服务器路由 metric 值（跃点数）超过 1024.

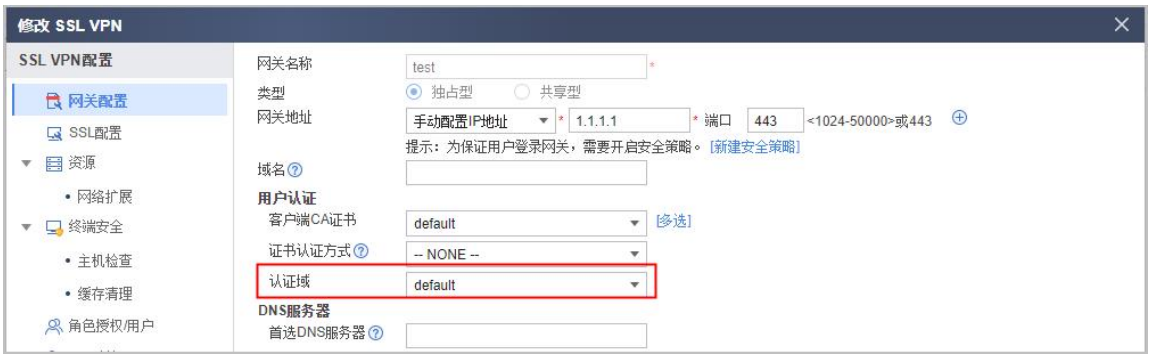
处理步骤

1. 登录设备，检查用户名和密码是否正确，用户是否过期，以及是否处于锁定状态。

```
[sysname]display user-manage user verbose name user001
 2021-03-30 14:51:04.970 +08:00
 Current total number: 1
 ------------------------------------------------------------------------------
   User Name            : user001
   Password Config      : Yes
   Password             : OW7Q30G1NMDu2NS8ufuBIAAAAAALKhc4
   Parent Group         : /default
   Bind Mode            : Unidirectional   State             : Locked
   Expiration Time    : Unlimited
   Multi-IP Login       : Enabled
```

```
  User Type            : Created By Manager
  Vsys                 : public
-------------------------------------------------------------------------------
[sysname]
```

2. 检查虚拟网关是否绑定了认证域，如果有绑定，是否绑定了正确的认证域。



3. 检查认证域配置，是否启用了 SSL VPN 接入场景。

4. 检查是否启用了虚拟网关的网络扩展业务。

5. SSL VPN 不支持负载分担组网。调整配置或组网，确保 SSL VPN 登录的设备处于双机主状态（HRP_M）。

6. 确定 SSL VPN 虚拟网关是否必须是共享型，如果不是，删除该虚拟网关，重新创建独占型虚拟网关。

7. 点击 CLI 控制台，进 AAA 认证域视图，display this 查看该认证域是否存在“new-user deny-authentication”配置，如果存在，执行“undo new-user”删除新用户认证选项的配置。

```
[sysname]aaa
[sysname-aaa]domain default
Info: The domain default is for common users.
[sysname-aaa-domain-default]dis this
2021-04-12 15:05:35.600 +8:00
#
domain default
service-scheme webServerScheme1530599131778
service-type internetaccess ssl-vpn
internet-access mode single-sign-on
reference user current-domain
new-user deny-authentication
#
return
[sysname-aaa-domain default]
```

8. 登录 AD/LDAP 服务器，查看用户的属性是否启用了“首次登录必须修改密码”，如果启用，选择禁用。

9. 检查通往服务器的路由 metric 值是否大于 1024，如果大于 1024，请修改对应路由的 metric 值。

```
sugon@sugon-os:~/桌面$ route -n
内核 IP 路由表
目标            网关            子网掩码        标志  跃点   引用  使用 接口
0.0.0.0         10.18.11.254    0.0.0.0         UG    13392  0        0 enp1s0
10.18.11.0      0.0.0.0         255.255.255.0   U     100    0        0 enp1s0
10.20.2.96      10.18.11.254    255.255.255.255 UGH   100    0        0 enp1s0
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 enp1s0
sugon@sugon-os:~/桌面$ sudo route del default gw 10.18.11.254
sugon@sugon-os:~/桌面$ sudo route add -net 0.0.0.0 gw 10.18.11.254 netmask 0.0.0.0  metric 0 enp1s0
sugon@sugon-os:~/桌面$ route -n
内核 IP 路由表
目标            网关            子网掩码        标志  跃点   引用  使用 接口
0.0.0.0         10.18.11.254    0.0.0.0         UG    0      0        0 enp1s0
10.18.11.0      0.0.0.0         255.255.255.0   U     100    0        0 enp1s0
10.20.2.96      10.18.11.254    255.255.255.255 UGH   100    0        0 enp1s0
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 enp1s0
sugon@sugon-os:~/桌面$
```

1.4.2.3 用户连接数已达到上限，请稍后重试！

现象描述

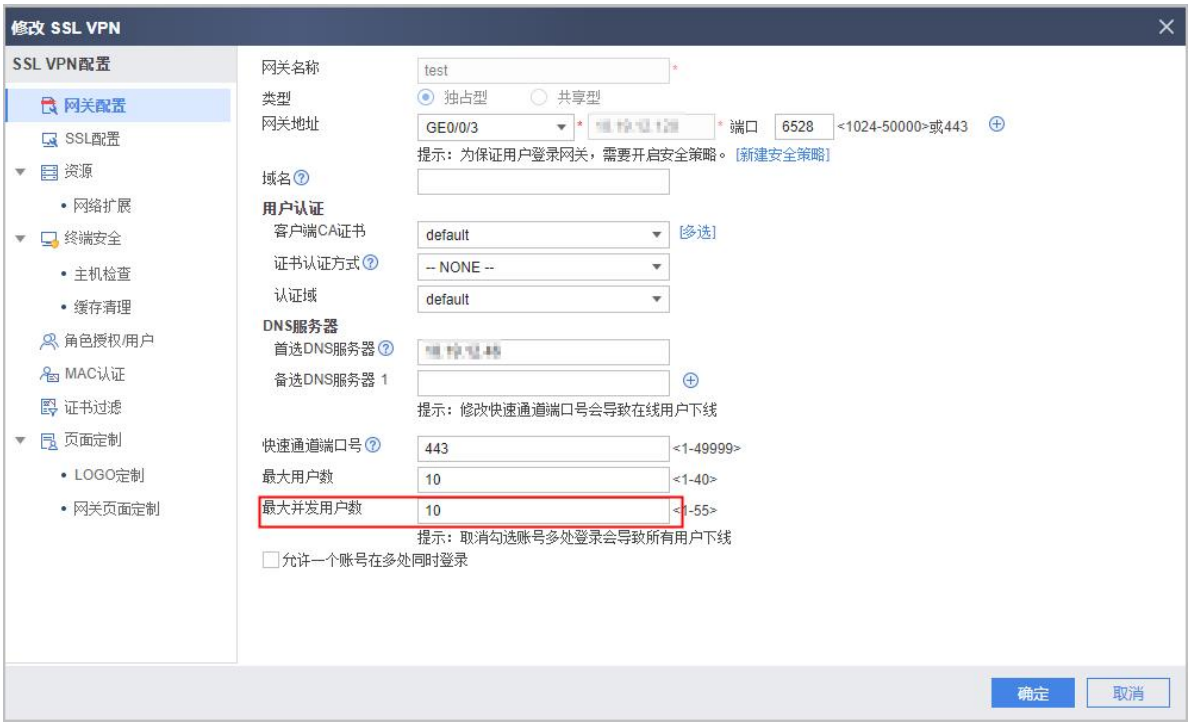
在 UniVPN 登录界面，输入用户名和密码以后，单击“登录”，系统告警“用户连接数已达到上限，请稍后重试！”。

可能原因

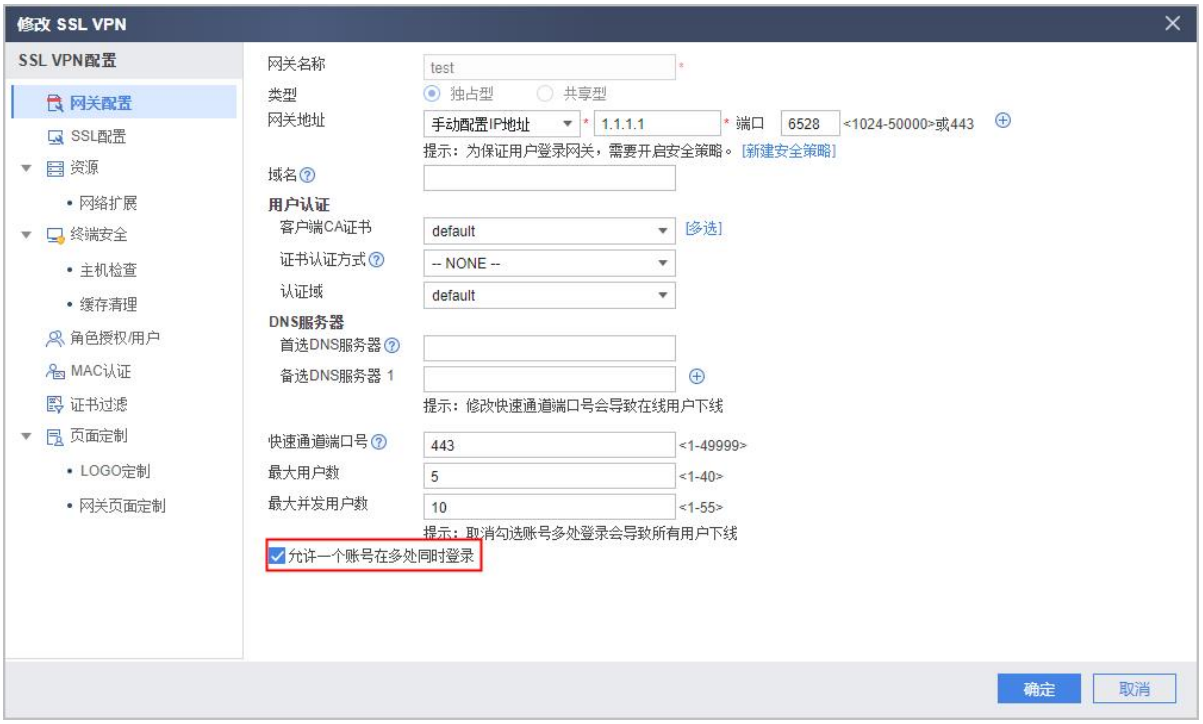
1. 当前 SSL VPN 在线用户数已经达到虚拟网关侧配置的最大并发用户数上限。
2. 虚拟网关启用了公共账号功能，且该用户已登录在线的数目已达到上限。

处理步骤

- 原因 1 的问题定位及解决方法。
  登录虚拟网关，选择“网络 > SSL VPN > SSL VPN”，单击对应虚拟网关的名称，检查该虚拟网关最大并发用户数分配情况是否合理，如果不合理，则调整配置。



- 原因 2 的问题定位及解决方法。
  检查该用户的最大在线数目配置，如果是正常的登录请求，可适当增加该用户的最大在线数目。



1.4.2.4 网络拓展启动失败

现象描述

在 UniVPN 登录界面，输入用户名和密码以后，单击“登录”，系统告警“网络扩展启动失败！”。

可能原因

1. 当前虚拟网关网络扩展地址池内 IP 地址已用完。
2. 虚拟网关网络扩展客户端 IP 分配方式为外部服务器获取，但认证域未配置服务器授权提案。

处理步骤

1. 打开 CLI 控制台，进虚拟网关 service 视图，执行 display network-extension [ip]指令查看网络扩展地址池的配置和分配情况。如果确定地址池已分配完，根据业务需要，适当增加地址池中地址的数目。

```
[sysname-sslvpn-service] display network-extension  VG Network Extension Information
----------------------------                                                Network
Extension State:     enable                                        Keep Alive State:
enable                                                  Keep Alive Interval:        120(seconds)
Log State:                   disable                                              Point to Point
State:        disable                                                  VIP Method:
net pool assign    default net pool:          3.3.3.100                           Route Mode:
manual   Intranet IP/Mask:          3.3.3.0/255.255.255.0   Intranet IP/Mask:
192.168.1.0/255.255.255.0                                   ----------------------------
Virtual  IP Pool:                                                                 NO.
Start-IP                End-IP                Mask                  Alias
----------------------------------------------------------------------------    1
3.3.3.100               3.3.3.200             255.255.255.0         3.3.3.100
----------------------------------------------------------------------------    ----End
[sysname-sslvpn-service] display network-extension ip                               Client IP
Allocation                                                          --------------------
NO.    User                             IP             Time of fetching IP
------------------------------------------------------------------------------  1
usur002                         3.3.3.101       2021-04-16 09:31:56
------------------------------------------------------------------------------
Virtual Gateway:sslvpn
```

2. 认证域配置 RADIUS 服务器认证，且网络扩展客户端 IP 地址分配方式配置为外部服务器获取（network-extension external-server），这时需要为认证域配置 RADIUS 授权提案。

```
[sysname-sslvpn-service] display network-extension  VG Network Extension Information
----------------------------                                                Network
Extension State:     enable                                        Keep Alive State:
enable                                                  Keep Alive Interval:        120(seconds)
Log State:                   disable                                              Point to Point
State:        disable                                                  VIP Method:
external server assign    default net pool:          3.3.3.100                         Route
Mode:                     manual   Intranet IP/Mask:          3.3.3.0/255.255.255.0   Intranet
IP/Mask:              192.168.1.0/255.255.255.0
----End[sysname-sslvpn-service]
```

```
[sysname-aaa] authorization-scheme radius [sysname-aaa-author-radius] dis this 2021-04-16 10:05:35.720 +8:00 # authorization-scheme radius authorization-mode radius # return [sysname-aaa-author-radius] domain default Info: The domain default is for common users. [sysname-aaa-domain-default] dis this 2021-04-12 15:15:35.360 +8:00 # domain default authentication-scheme admin_radius authorization-scheme radius service-scheme webServerScheme1530599131778 radius-server radius service-type internetaccess ssl-vpn internet-access mode single-sign-on reference user current-domain # return [sysname-aaa-domain default]
```

1.4.2.5 主机检查失败！

现象描述

在 UniVPN 登录界面，输入用户名和密码以后，单击“登录”，系统告警“主机检查失败！”。

可能原因

虚拟网关启用了主机检查功能，且终端不符合安全接入的要求。

处理步骤

根据主机检查失败弹出的页面提示排除故障。

1.4.2.6 接受返回码超时！

现象描述

在 UniVPN 登录界面，输入用户名和密码以后，单击“登录”，系统告警“接收返回码超时！”。

可能原因

通信时间是 40s，超过通信时间重启客户端导致系统接收超时

处理步骤

退出 UniVPN，然后重新打开 UniVPN。

1.4.2.7 当前连接不支持快速隧道模式，请切换到可靠隧道模式后重试

现象描述

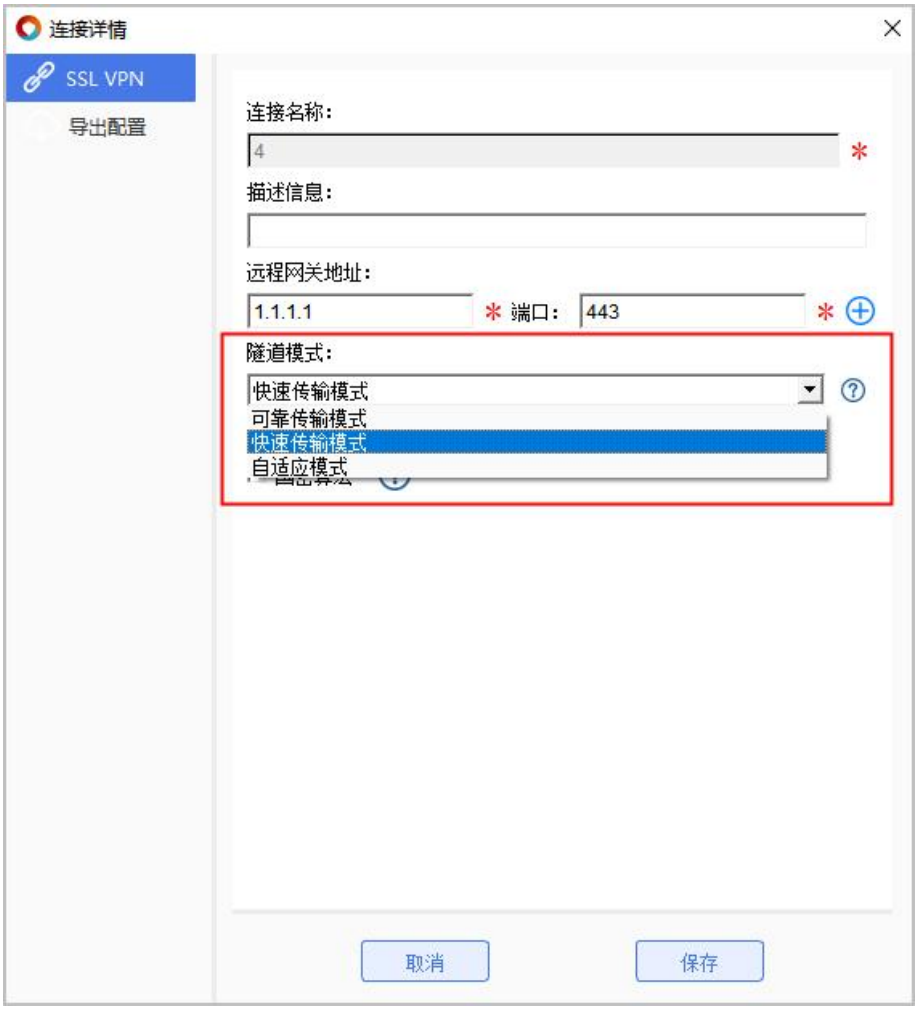
在 UniVPN 登录界面，输入用户名和密码以后，单击“登录”，系统告警“当前连接不支持快速隧道模式，请切换到可靠隧道模式后重试”。

可能原因

终端在拨号 SSL VPN 过程中，会发送 UDP 探测报文，探测建立快速隧道的可行性。如果能收到防火墙的响应，说明快速隧道可以建立。上图中报错，说明该 UDP 链路不通，快速隧道无法建立。

处理步骤

1. UniVPN 配置“自适应模式”拨号，作为临时规避办法。快速隧道无法建立，通过下面步骤继续排查。



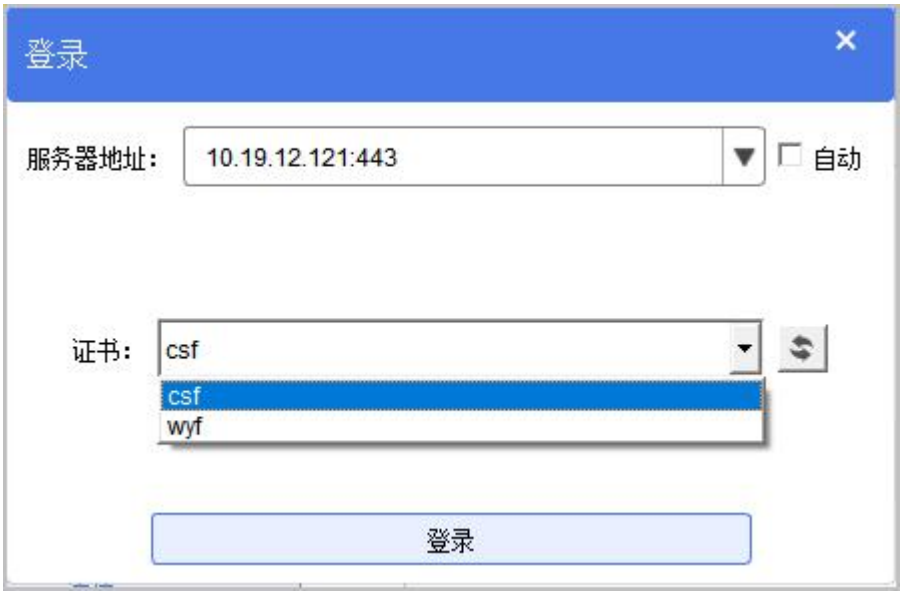
2. 排查防火墙的安全策略，是否放行了终端与 VPN 网关之间建立 UDP 快速链路的数据流。
3. 检查防火墙外层是否存在 NAT 设备，如果存在，需针对 SSL VPN 的 TCP 和 UDP 端口分别做 NAT 映射且安全策略放行；对 UDP 端口做 NAT 映射时，Global 端口和 Inside 端口必须一致。

1.4.3 采用证书方式登录时出现警告

1.4.3.1 找不到用户证书

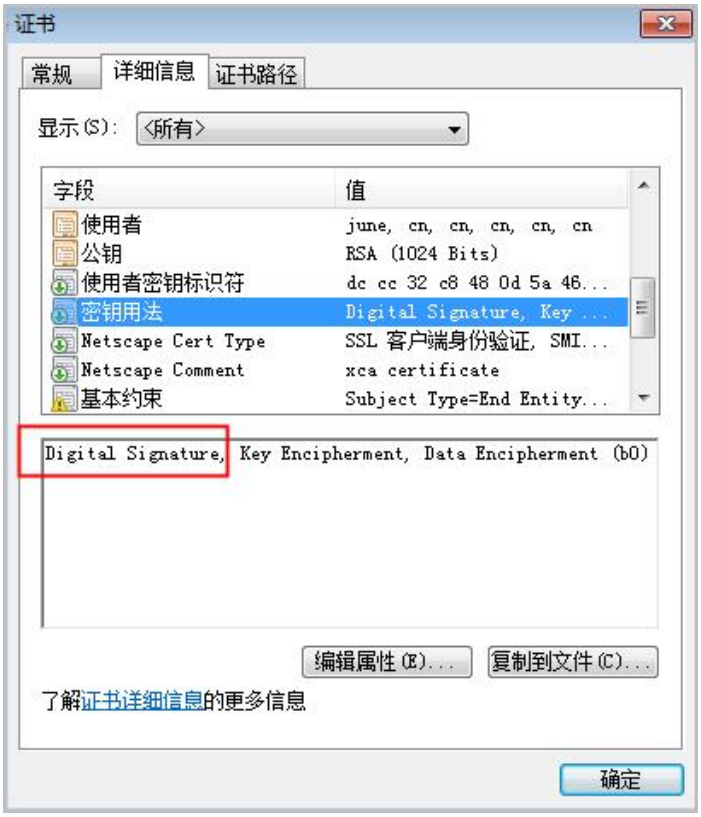
现象描述

在虚拟网关采用证书认证的情况下， 在 UniVPN 登录界面，选择用户证书时，无法找到预期的用户证书。



可能原因

预期的用户证书“密钥用法”没有包含“Digital Signature”（数字签名）。



处理步骤

重新制作一本密钥用法带“数字签名”的用户证书。

说明

如果服务器不支持无数字签名能力的证书，客户端不显示无数字签名能力证书；

如果服务器支持无数字签名能力的证书，但是客户端未显示无数字签名能力证书，可能是服务器开启了密钥用法：必须拥有数字签名能力。

产品名称	产品版本	是否支持无数字签名能力的证书认证
USG6000	V500R005C20SPC500 及以后版本	不支持
USG9500	V500R005C20SPC500 及以后版本	不支持
USG6000E	V600R007C20SPC300 及以后版本（SPC301/SPC 302 版本除外）	不支持
Eudemon200E-N	V500R005C20SPC500 及以后版本	不支持
Eudemon200E-G	V600R007C20SPC300 及以后版本（SPC301/SPC 302 版本除外）	不支持
Eudemon1000E-N	V500R005C20SPC500 及以后版本	不支持
Eudemon1000E-G	V600R007C20SPC300 及以后版本（SPC301/SPC 302 版本除外）	不支持
Eudemon8000E-X	V500R005C20SPC500 及以后版本	不支持
SeMG9811	V500R005C20SPC500 及以后版本	不支持
NGFW Module	V500R005C20SPC500 及以后版本	不支持
USG12000	V600R021C10 及以后版本	支持
USG6000F	V600R021C10 及以后版本	支持
Eudemon9000E-X	V600R021C10 及以后版本	支持
Eudemon9000E-F	V600R021C10 及以后版本	支持
Eudemon1000E-F	V600R021C10 及以后版本	支持

1.4.3.2 提示：您的用户证书验证非法，请提供合法的证书！

现象描述

在 UniVPN 登录界面，选择用户证书，单击“登录”，系统提示“您的用户证书验证非法，请提供合法的证书！”

可能原因

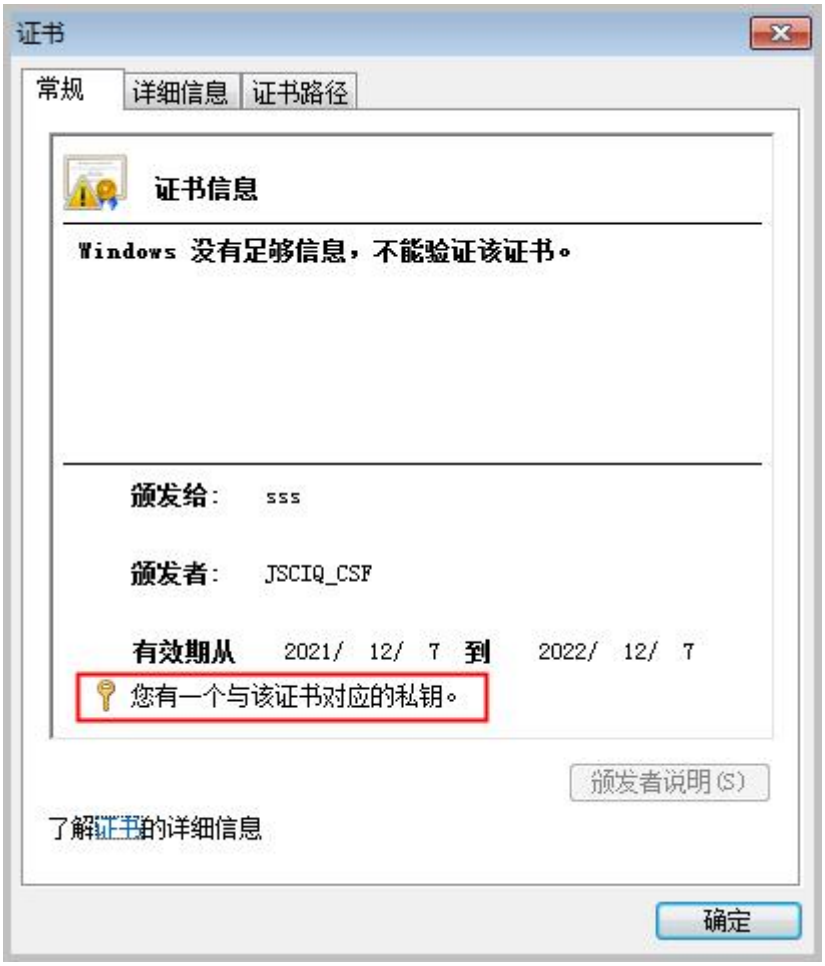
1. 用户证书，不是由防火墙虚拟网关客户端 CA 证书的根证书签名颁发。

2. 安装在终端上的用户证书，没有携带私钥信息。
3. 防火墙设备的系统时间、时区，不在用户证书的有效期范围之内。
4. 用户证书被防火墙配置的 CRL（证书吊销列表）或 OCSP（在线证书状态协议）吊销。

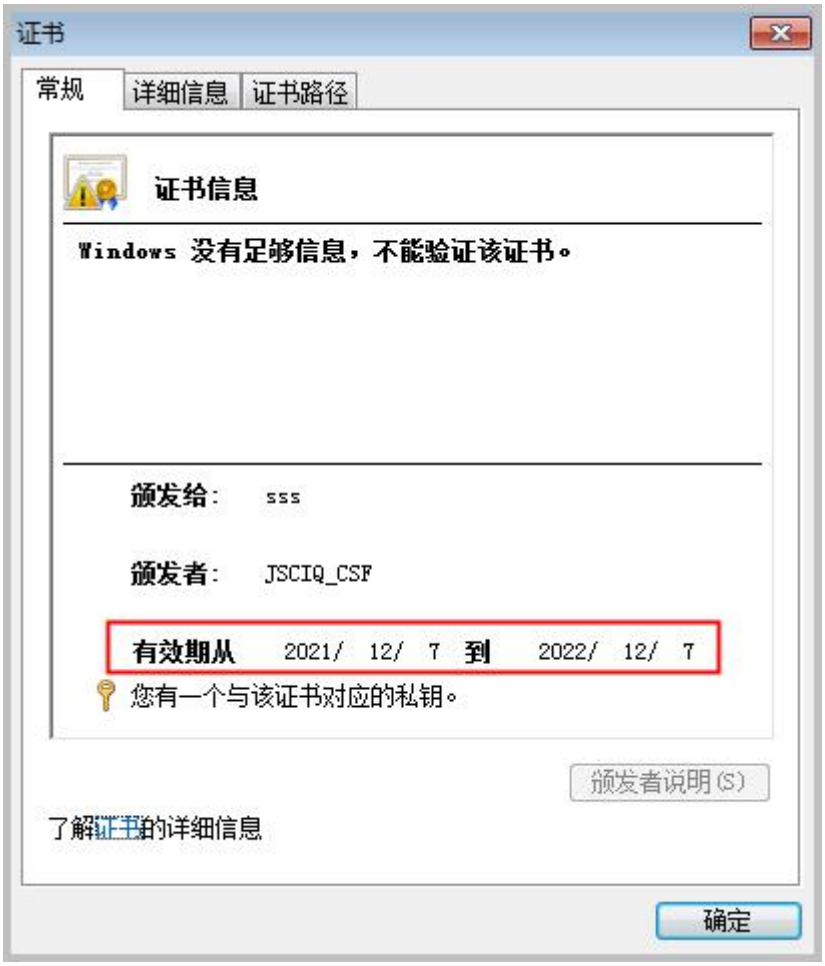
处理步骤

1. 检查用户证书的“颁发者”字段，是否和防火墙虚拟网关客户端 CA 证书的“颁发给”字段一致。

2. 检查用户证书，是否有对应的私钥。



3. 检查防火墙的时间、时区配置是否正确，以及是否在用户证书的有效期范围之内。



4. 检查防火墙是否配置了 CRL 或 OCSP，如果是，取消该配置，观察效果。

1.4.3.3 提示：认证失败！

现象描述

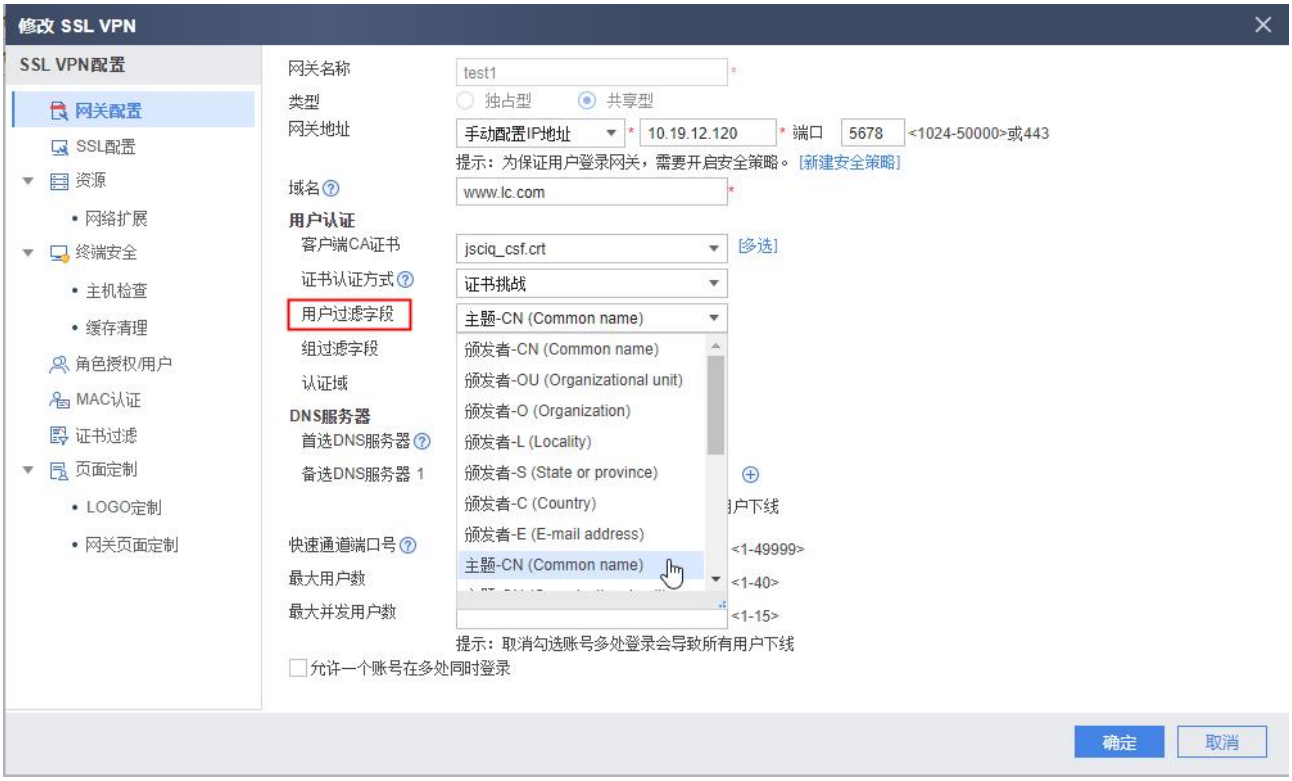
在虚拟网关采用证书挑战认证的情况下，在 UniVPN 登录界面，选择用户证书，单击“登录”，系统提示“认证失败!”。

可能原因

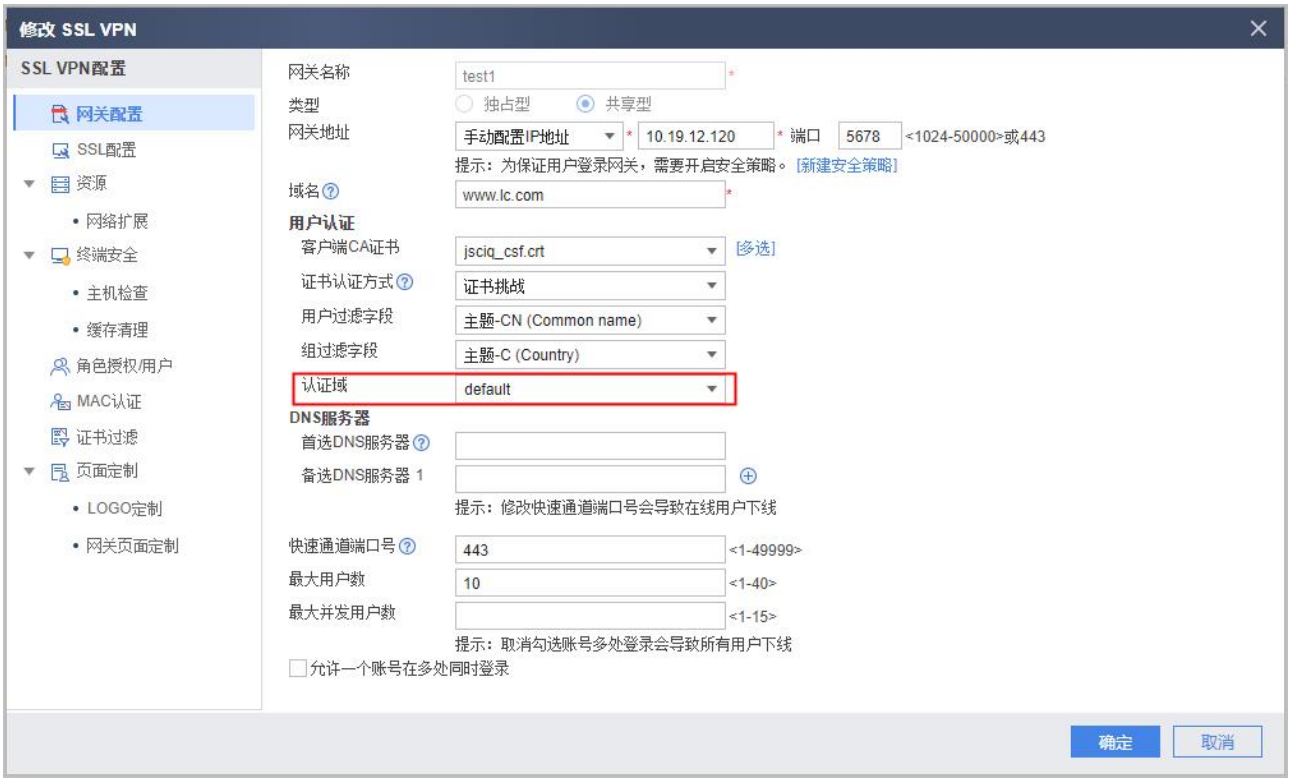
1. 虚拟网关证书认证“用户过滤字段”配置不正确，导致用户登录时设备从用户证书中获取了错误的用户名信息。
2. 虚拟网关绑定了不正确的认证域。
3. 认证域未启用 SSL VPN 接入场景。
4. 虚拟网关未启动网络扩展特性。
5. SSL VPN 登录的设备处于双机备状态（HRP_S），而 SSL VPN 不支持在备设备上登录上线。
6. 证书有效期过期

处理步骤

1. 登录设备，检查虚拟网关证书认证“用户过滤字段”配置，和用户证书中用于认证字段的属性名称是否匹配。



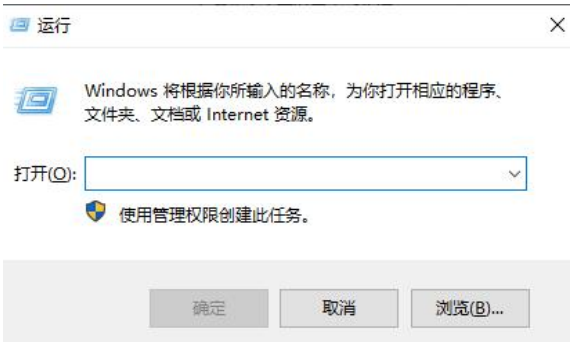
2. 检查虚拟网关是否绑定了认证域，如果有绑定，是否绑定了正确的认证域。



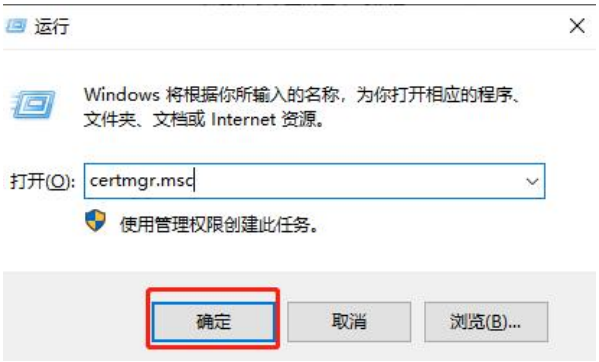
3. 检查认证域配置，是否启用了 SSL VPN 接入场景。

4. 启用虚拟网关的网络扩展特性。

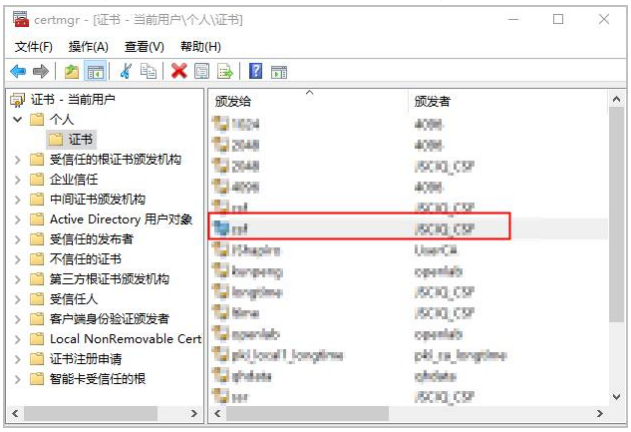
5. 调整配置或组网，确保 SSL VPN 登录的设备处于双机主状态（HRP_M）。
6. 删除已过期证书，重新导入未过期证书。
   1、使用 windows + R 键打开“运行”对话框。



   2、输入 certmgr.msc,单击确定，打开证书管理器

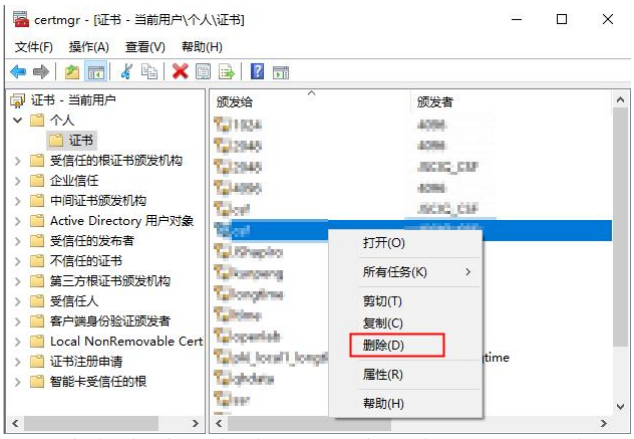


3、选择“个人>证书”，选择用户证书。双击用户证书，查看证书有效期。



4、双击用户证书，查看证书有效期后，单击“确定”返回证书管理器。

5、 右键单击有效期已过期的证书选择“删除”，根据提示删除有效期过期的证书。



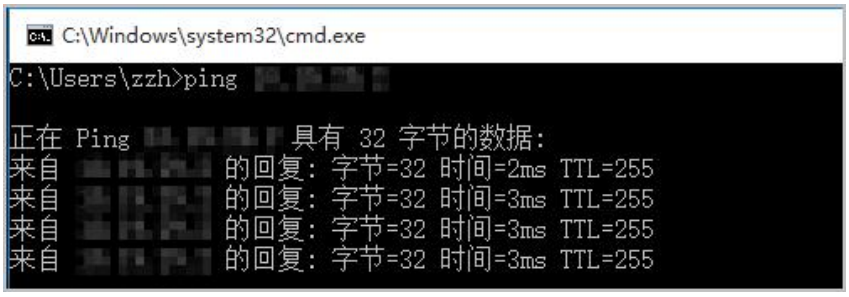
6、 重新安装有效期未过期的用户证书，重新开始 UniVPN 客户端认证。

1.4.4 登录成功后业务出现异常

1.4.4.1 访问内网资源卡顿，ping 内网延迟大

现象描述

SSL VPN 拨号成功，访问内网资源卡顿，Ping 内网延迟大。测试下载速率比 NAT 映射低很多。



可能原因

从技术实现角度来看，NAT 映射只是对报文头做了地址转换，相对简单；而 VPN 技术需要对整个报文做加解密封装，相对复杂。因此，VPN 本身造成的系统消耗和引发的时延就比 NAT 映射大。在跨运营商的场景下，这个延时就更为明显一些。

处理步骤

1. 在隧道模式那里选择快速模式或是自适应模式，快速模式报文传输效率相对较高。当隧道传输模式为“快速传输模式”时，防火墙上要开启 Local 到 Untrust（假设用户处于 Untrust 区域）的域间策略，策略匹配条件中服务类型为 UDP，端口为 443。自适应模式下，UniVPN 会优先以“快速传输模式”与 VPN 网关建立 SSL VPN 隧道；当快速模式建立失败时，UniVPN 会转为使用“可靠传输模式”与 VPN 网关建立 VPN 隧道。
2. 如果企业对外提供了多个 SSL VPN 网关，在 UniVPN 上启用自动优选功能可以保证用户连接到响应最快的那台 VPN 网关，减少延迟。

1.4.4.2 登录成功后，无法访问公网

现象描述

SSL VPN 拨号成功，但是无法访问公网站点了，域名也 Ping 不通。

可能原因

虚拟网关网络扩展配置了分离路由模式或全路由模式。

Web 配置网络扩展时，如果可访问内网网段列表中没有任何网段，网络扩展路由模式则为分离路由模式（network-extension mode split）；如果列表中存在一个或多个网段，网络扩展路由模式为手工路由模式(network-extension mode manual)。在 CLI 控制台下执行 network-extension mode full，可设置网络扩展路由模式为全路由模式。当网络扩展 路由模式为分离路由模式或全路由模式时，用户拨号 SSL VPN 之后无法访问公网。

处理步骤

调整网络扩展路由模式为手工路由模式，终端启用网络扩展成功，仅在访问指定的 VPN 内网网段时，走 VPN 隧道，访问其它网段（含公网），不走 VPN 隧道。

1.4.4.3 警告：您被强制下线，请重新登录！

现象描述

UniVPN 登录成功，运行一段时间，系统告警“您被强制下线，请重新登录！”。

可能原因

1. 管理员强制用户下线。
2. 用户在线老化时间超时下线。

处理步骤

1. 登录 VPN 网关，选择“监控 > 系统日志”，检查防火墙操作日志，确定是否管理员执行了强制用户下线的动作。
2. 检查虚拟网关会话超时时间配置，以及网络扩展保持连接功能是否开启。

1.4.4.4 提示：无法建立 VPN 连接，VPN 服务器可能无法到达

现象描述

UniVPN 登录后，拨号提示：无法建立 VPN 连接，VPN 服务器可能无法到达。

可能原因

出现此现象，大概率是由于客户端侧与网关侧使用加密算法不同导致。

处理步骤

1. 1 从 V600R007C20SPC100 开始，缺省情况下设备去使能虚拟网关的弱加密算法，此时虚拟网关的加 密套件只能使用强加密算法，使用 10781.2.327.1231 及其之后版本的 UniVPN 才能正常登录虚拟网关。
对于 10781.2.327.1231 之前的版本，可在网关侧执行 v-gateway ssl weak-encryption enable 命令使能虚拟网关弱加密算法。
2. 若网关侧和国密侧均配置使用国密算法，出现此提示，若日志打印如下提示:

```
open gmssl lib C:\Program Files (x86)\UniVPN\serviceclient\libgmssl-1_1-x64.dll, failed, reason: 126
[SSL Create failed][load library 2 failed]
```

一般是由于缺少某些组件问题导致，可下载 Visual C++ Redistributable for Visual Studio2015 手动安装解决此问题。
微软官方链接：https://www.microsoft.com/zh-CN/download/details.aspx?id=48145&from_wecom=1。

1.4.4.5 终端加入 AD 域后，SSL VPN 用户接入一段时间后异常掉线

现象描述

终端加入 AD 域，SSL VPN 用户接入一段时间后异常掉线，而不加入 AD 域，则不会出现掉线。具体故障现象如下。

- 防火墙上能看到用户下线记录。

在主墙上查看用户下线记录提示如下。

```
HRP_M[HUAWEI] display aaa offline-record username user-name
2020-09-02 11:46:34.219 -03:00
--------------------------------------------------------------------------------
  User name              : test001@domain1
  Domain name            : domain1
  User MAC               : -
  User access type       : SSLVPN
  User IP address        : 10.0.91.89
  User IPV6 address      : -
  User ID                : 65915
  User login time        : 2020/09/02 11:44:27
  User offline time      : 2020/09/02 11:46:21
  User offline reason    : User request to offline
  User name to server    : test001
```

在备墙上查看用户下线记录提示如下。

```
HRP_S[HUAWEI] display aaa offline-record username user-name
--------------------------------------------------------------------------------
  User name              : test001@domain1
  Domain name            : domain1
  User MAC               : -
  User access type       : SSLVPN
  User IP address        : 10.0.91.89
  User IPV6 address      : -
  User ID                : 65915
  User login time        : 2020/09/02 11:44:28
  User offline time      : 2020/09/02 11:46:21
  User offline reason    : Delete backup user
  User name to server    : test001
```

- UniVPN 客户端日志提示用户下线的原因是被网关侧踢下线。

```
FRAME  DEBUG  2020-09-02 12:45:09.000334 ][B00550] [65535][Create event base][eventbase notifyserver notify send ok sock(1256)
FRAME  DEBUG  2020-09-02 12:45:09.000334 ][B00550] [65535][Add event][interval(10:0) tv(10:0) timeout:(1599061519:334423)]
FRAME  DEBUG  2020-09-02 12:45:09.000335 ][B00550] [65535][Insert event][timeoutlist(fd:4 ev_res:268435696 total:0 timer:5 act
FRAME  DEBUG  2020-09-02 12:45:09.000335 ][B00550] [65535][eventlist todo wait][end ok,todo:00000000036A2820 semid:7]
FRAME  DEBUG  2020-09-02 12:45:09.000335 ][B00550] [65535][Unbind channel][unbind channel OK (chid 239 268435695 events(2))]
CNEM   WARN   2020-09-02 12:45:15.000450 ][B00550] [65535][Cnem handle packet from gateway][CMDtype is KICKOUT]
FRAME  DEBUG  2020-09-02 12:45:15.000450 ][B00550] [65535][send message][task(4) mqueid(4) message type:1 send messge addr(000
CNEM   INFO   2020-09-02 12:45:15.000451 ][B00550] [65535][Cnem send status msg to self ok]
```

- 在防火墙上采集调制日志，在用户掉线之前，LAM 模块产生的 CUT_REO 事件。

```
HRP_M<HUAWEI-diagnose> debugging svm error
Sep 14 2020 13:15:49-03:00 FGSTHA00-01 CM/7/DEBUG:
[UCM-MSG] MSG Recv From: (taskName=LAM, Code=ESAP_SRV_MSG_CUT_REQ, Src=0, Dst=-1, Slot=0)WebAuth:0x0 Vrf:0Reason:29 Vlan:0 VPI/VCI:0/0 AccessType:0TimeoutMsg:0 Mac:0000-0000-0000 IPV6: IP:10.0.91.28.
Sep 14 2020 13:15:49-03:00 FGSTHA00-01 CM/7/DEBUG:
```

可能原因

出现上述现象，大概率是由于防火墙上同时配置了 SSL VPN 和 AD 单点登录功能（安装 ADSSO 查询 AD 服务器安全日志）导致。

终端加入 AD 域后，SSL VPN 用户接入网关后需要连接 AD 域控制器进行认证（此时 AD 域控制器会记录安全日志），认证通过后，SSL VPN 用户在防火墙上线，SSL VPN 用户登录成功。当 ADSSO 向 AD 域控制器获取安全日志（内容是 SSL VPN 账号和虚拟 IP 地址的对应关系。）后，将安全日志发送给防火墙，防火墙会根据安全日志再次将此用户上线。也就是在此种场景下，同一个用户（同一个账号对应同一个虚拟 IP）会两次在防火墙上线，第一次是 SSL VPN 用户登录过程，SSL VPN 用户认证通过后在防火墙上线，第二次是防火墙解析 ADSSO 发送的安全日志后将用户上线。

但防火墙不支持上述场景，防火墙解析 ADSSO 发送的安全日志将用户上线时，会将之前已经在线的 SSL VPN 用户踢下线。

处理步骤

1. 请确认防火墙上是否配置了 AD 单点登录功能（安装 ADSSO 查询 AD 服务器安全日志）功能，如果是，请执行后续步骤。如果没有配置 AD 单点登录功能，请联系联软技术支持工程师。
2. 在防火墙配置源 NAT 策略。
3. 针对 SSL VPN 用户请求域控服务器的认证数据流配置源 NAT 策略。配置后，SSL VPN 用户和域控服务器之间没有直接交互。AD 域控制器上产生的安全日志，其用户的源 IP 地址不再是 SSL VPN 拨号获得的虚拟 IP 地址，而是防火墙内网接口 IP 地址。这样防火墙解析 ADSSO 发送的安全日志将用户上线时，不会将之前已经在线的 SSL VPN 用户踢下线。

   a. 选择“策略 > NAT 策略 > NAT 策略”。

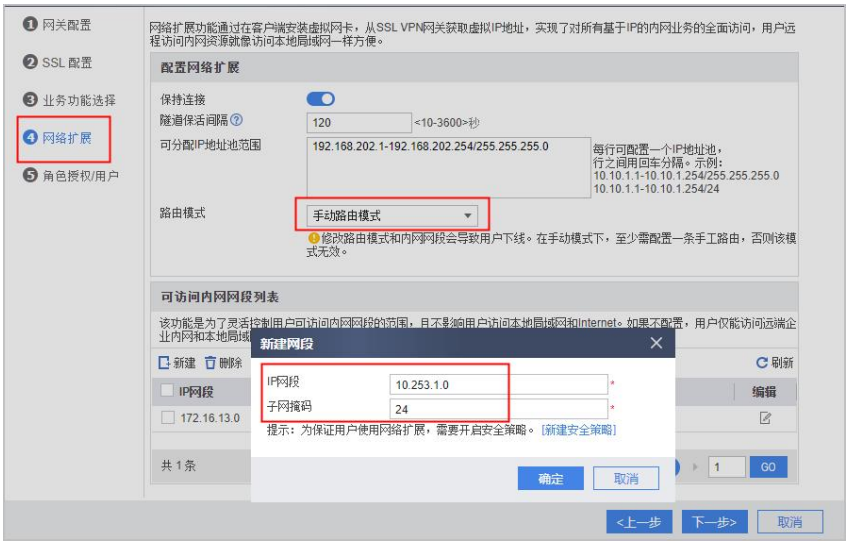
b. 单击“新建”，配置源 NAT 策略。

假设 SSL VPN 用户的虚拟地址为 10.2.0.0/16，AD 域控制器的地址为 10.10.10.3。

1.4.4.6 新增 SSL VPN 网络拓展可访问网段后，用户无法访问新增网段

现象描述

如下图所示，网络扩展下配置“手动路由模式”，在“可访问内网网段列表”中新增网段“10.253.1.0/24”。用户下线并重新拨号后，无法访问新增网段 10.253.1.0/24。



可能原因

出现上述现象，大概率是由于设备没有向终端下发到新增网段的路由导致。

处理步骤

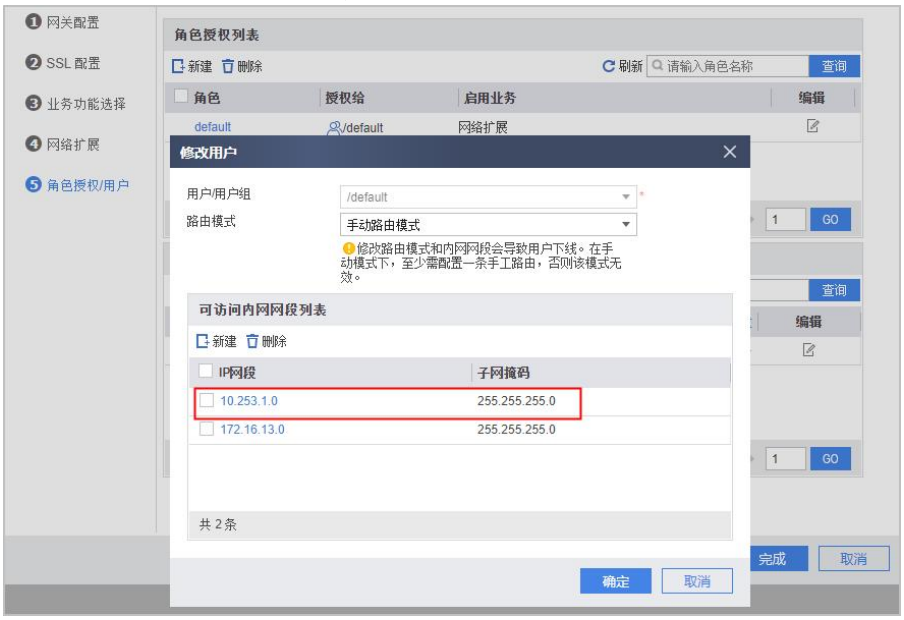
1. 在终端执行 route PRINT 命令检查是否存在到新增网段的路由。如果不存在执行后续步骤，如果存在请联系联软技术支持工程师。

```
C:\Users\XXX> route PRINT

IPv4路由表
===========================================================================
活动路由：
      网路目标          网络掩码          网关          接口      跃点数
        0.0.0.0          0.0.0.0   10.174.104.1   10.174.105.158      25
   10.174.104.0    255.255.252.0      在链路上   10.174.105.158     281
 10.174.105.158  255.255.252.255      在链路上   10.174.105.158     281
 10.174.105.255  255.255.252.255      在链路上   10.174.105.158     281
```

2. 按照如下步骤检查用户组下是否配置了路由模式，新增网段是否包含在“可访问内网网段列表”中，如果配置了路由模式，且新增网段没有包含在“可访问内网网段列表”中，请执行后续步骤。

3. 如下图所示，用户组下配置了路由模式，且新增网段没有包含在“可访问内网网段列表”中。只要用户组下配置了路由模式，则在网络扩展下配置的路由模式无效。

4. 在用户组下新增可访问内网网段。



5. 用户重新登录后检查本地路由，检查到用户组下新增的可访问内网网段已下发到终端，终端用户也能正常访问该网段的资源。

```
IPv4路由表
===========================================================================
活动路由：
    网路目标          网络掩码          网关          接口        跃点数
      0.0.0.0          0.0.0.0        90.x.x.x      90.x.x.x        281
      0.0.0.0          0.0.0.0        17.1.1.1      17.1.1.2        271
  10.253.1.0      255.255.255.0      在链路上    192.168.202.4        1
10.253.1.255     255.255.255.255     在链路上    192.168.202.4      257
```

1.5 SSL VPN 常见咨询类问题 FAQ-V500R005C20 和 V600R007C20

本章节介绍 UniVPN 客户端在接入防火墙设备 V500R005C20 和 V600R007C20 及以后版本时的常见的咨询类问题 FAQ。

1.5.1 SSL VPN 如何实现一个账号多处同时登录

SSL VPN 要实现一个账号多处同时登录，需要设置两处地方。

1. 在创建用户的时候，勾选“允许多人同时使用.该账号登录”。

2. 命令行配置方式：

```
[sysname] user-manage user sslvpn
[sysname-localuser-sslvpn] multi-ip online enable
```

3. 在 SSL VPN 虚拟网关下开启“允许一个账号在多处同时登录”功能。

4. 命令行配置方式：

```
[sysname] v-gateway test1
[sysname-test1] security
[sysname-test-security] public-user enable
```

1.5.2 连接成功后无法访问资源

1. 客户端连接不同的服务器时有功能差异
2. VPN 连接后根据客户端下发的路径决定发送的报文是否要进隧道；服务器可以配置角色授权资源，如果访问的资源根据路由信息进入 VPN 隧道但是不在角色授权资源范围内，则客户端主动拦截并丢弃报文。

1.5.3 SSL VPN 证书认证相关知识点

1. 客户端 CA 证书支持证书链方式，在配置时，需要将链上的所有 CA 证书选中。
2. 客户端 CA 证书可以选择多本没有关联关系的 CA 证书，以支持不同根证书签发的用户证书接入。
3. 用户证书的用户名字段可以携带空格（如“Fang Datong”），但不能包含”和?这两种特殊字符。
4. 双机热备场景下，证书不会进行备份，需要分别在主用设备和备用设备上手动导入客户端 CA 证书。

5. 使用证书匿名认证、证书挑战认证方式进行用户认证时，需要在客户端的浏览器中安装客户端证书，客户端证书的格式必须为.p12、.pem（含密钥）或者.pfx 格式。
6. 证书匿名通过证书提取字段来验证 SSL VPN 用户身份。证书挑战除了使用证书提取字段来验证 SSL VPN 用户身份外，还结合本地或服务器的认证来辅助验证用户身份。

1.5.4 SSL VPN 是否支持用户和终端绑定

V100R001 版本和 V500R001 版本均不支持。

V500R005C00 版本支持虚拟网关对 SSL VPN 用户终端的 MAC 地址进行认证。MAC 认证的 目的在于让用户使用企业指定的合法终端接入网络，避免外来终端给企网络引入潜在危 险。

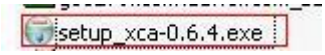
1.5.5 高端防火墙是否支持 SSL VPN 业务

USG9500 高端防火墙型号从 V500R001C50 版本开始支持 SSL VPN 功能，在此之前的版本 （例如 V300R001 版本）不支持 SSL VPN 功能。

1.5.6 如何使用 XCA 制作设备证书和用户证书

1. 安装 XCA 工具。

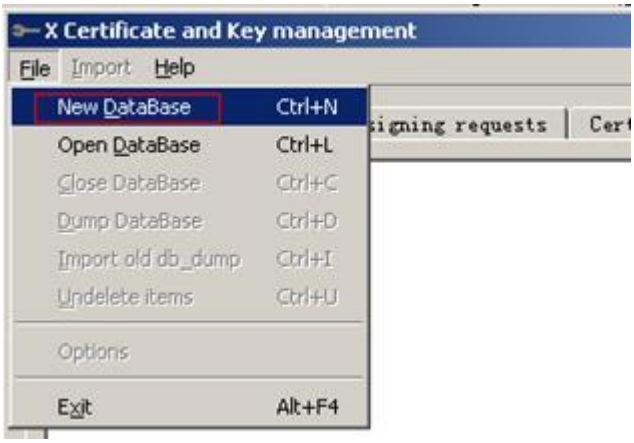
双击“setup_xca-0.6.4.exe”，一直单击“下一步”，直至安装成功。



2. 运行程序。

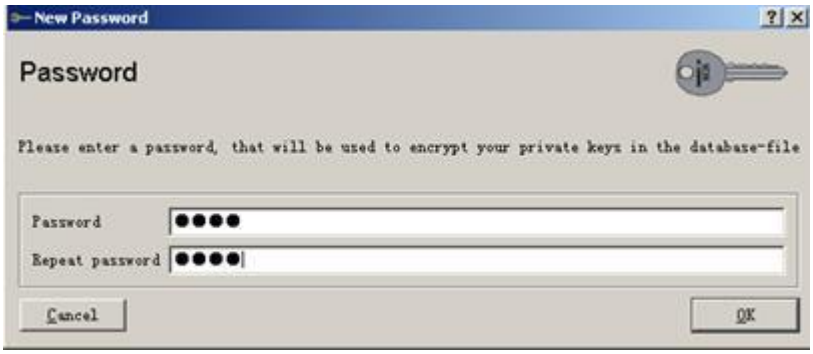
a. 单击“开始 > 程序 > xca > xca”运行程序。

b. 选择“File > New DataBase”创建数据库。



c. 选择数据库文件保存的位置，例如保存在“E:\ca\JSCIQ”中，并给文件进行命名为“JSCIQ”，单击“保存”按钮。

d. 在弹出的对话框中输入密码，并单击“ok”按钮。

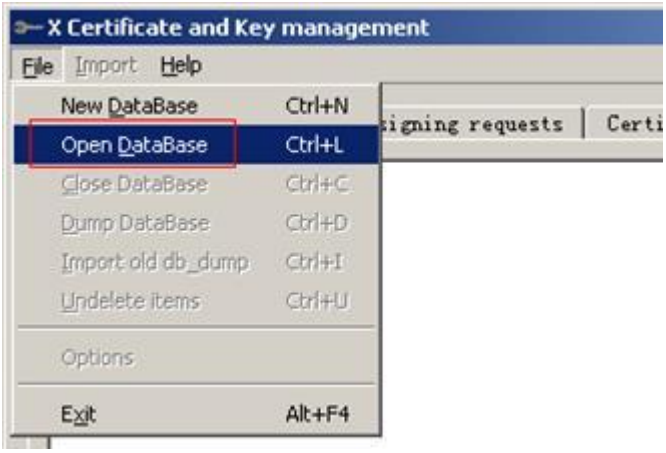


说明

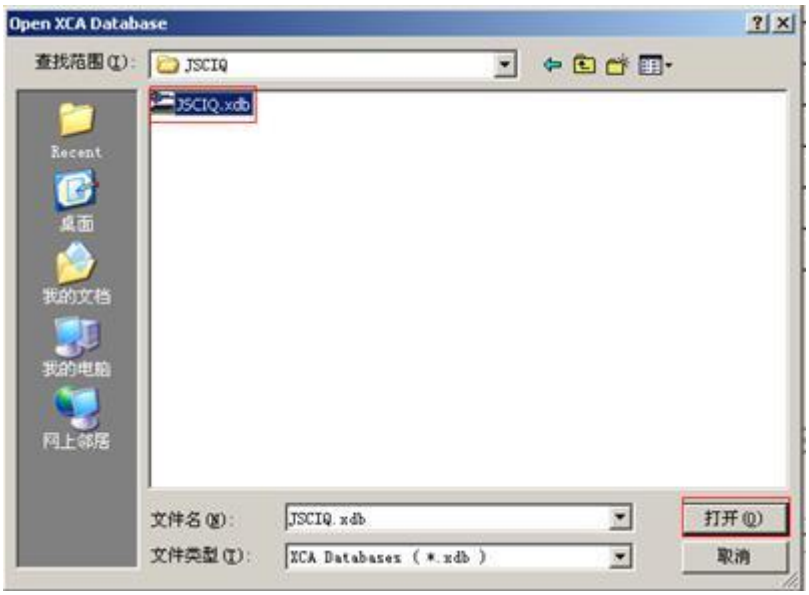
须牢记此密码，再次打开数据库时需要用到该密码。

3. 关闭后再次打开 xca 制作工具。

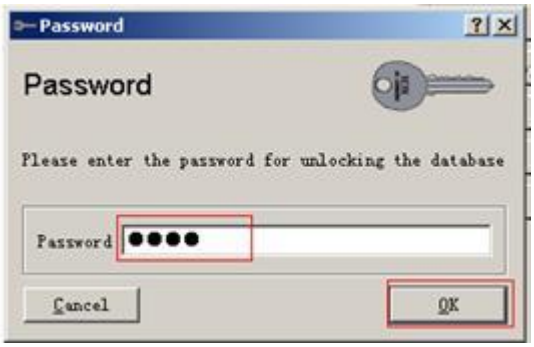
a. 把 xca 关闭，再次打开时，选择“File > Open Datebase”。



b. 打开上次保存的数据库，单击“打开”按钮。



c. 输入上次设置的密码，即可打开之前的数据库，制作用户证书。



4. 制作根证书。

a. 单击“Certificates”下的“New Certificate”。

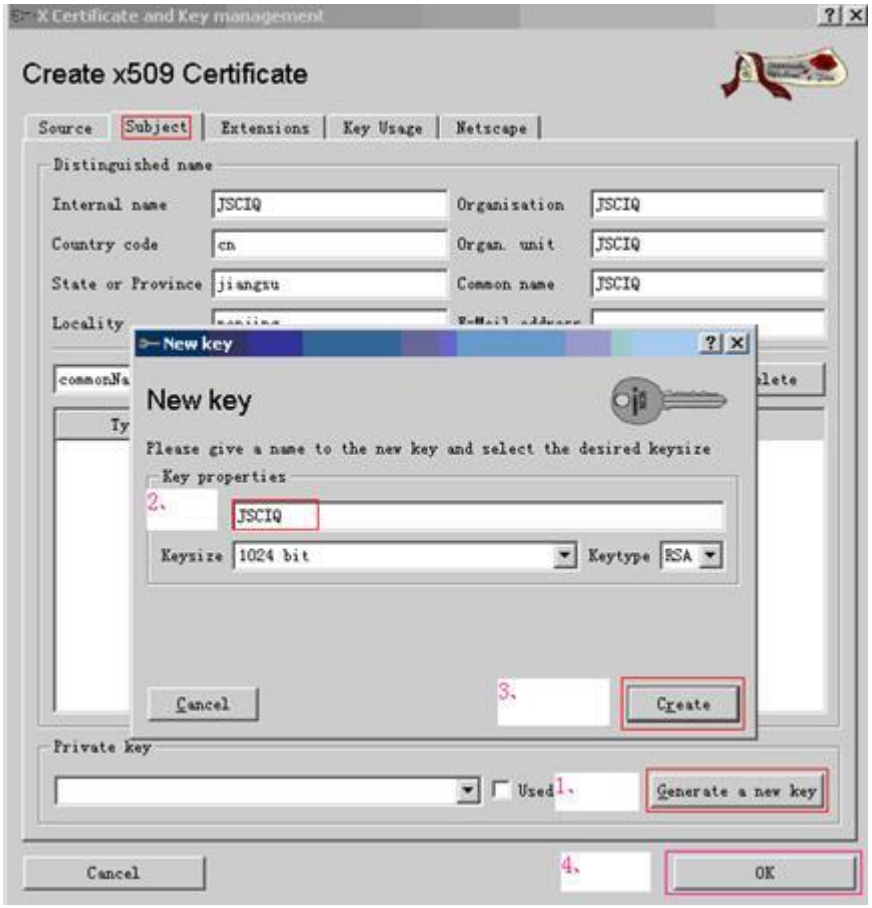
b. 在“Source”的“Signing”中选择加密算法为“SHA 1”，在“Template”中选择“[default]CA”，单击按钮“Apply”。

说明

必须选中签名算法为“SHA 1”，然后单击“Apply”按钮。

c. 在“Subject”中填入名称。

d. 在“Subject”标签下方，选择“Generate a new key”来生成密钥，在弹出的对话框中，给密钥重命名为“JSCIQ”，单击“Create”按钮。



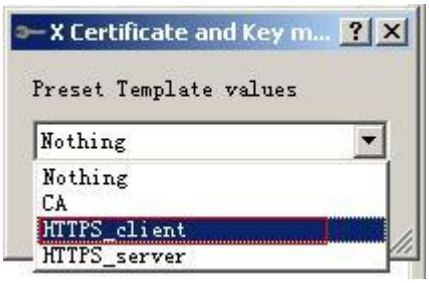
e. 最后单击“OK”按钮，就生成了根证书。

5. 制作用户证书。

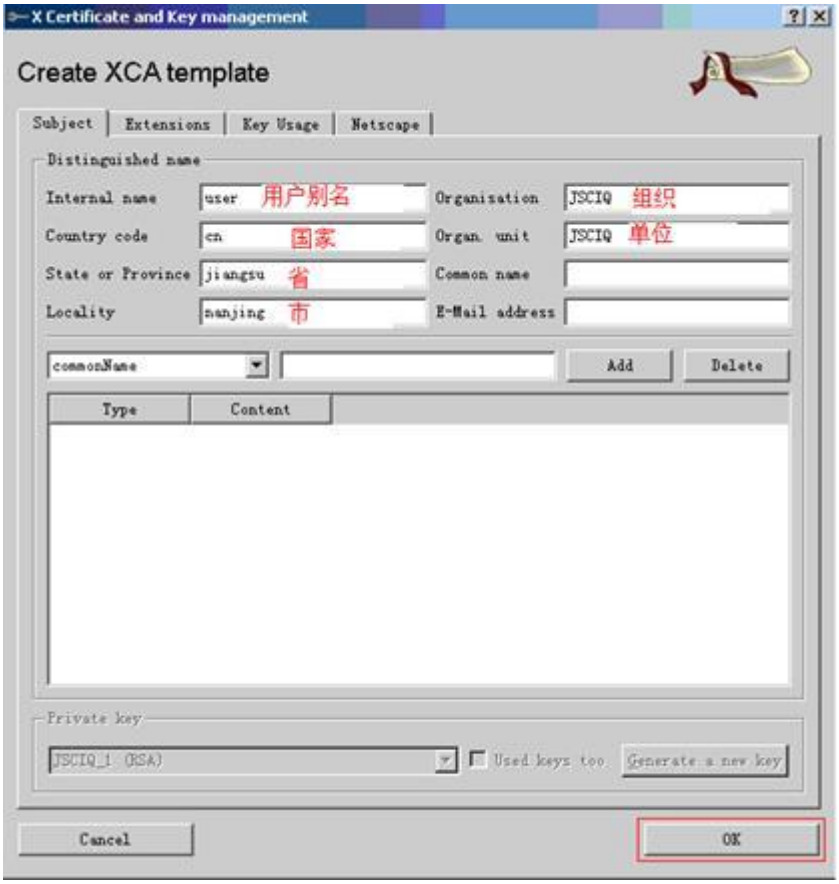
- 制作用户证书模版。

a. 选择“Templates”，并单击“New template”按钮制作用户证书。

b. 选择“HTTPS_client”，单击“OK”。



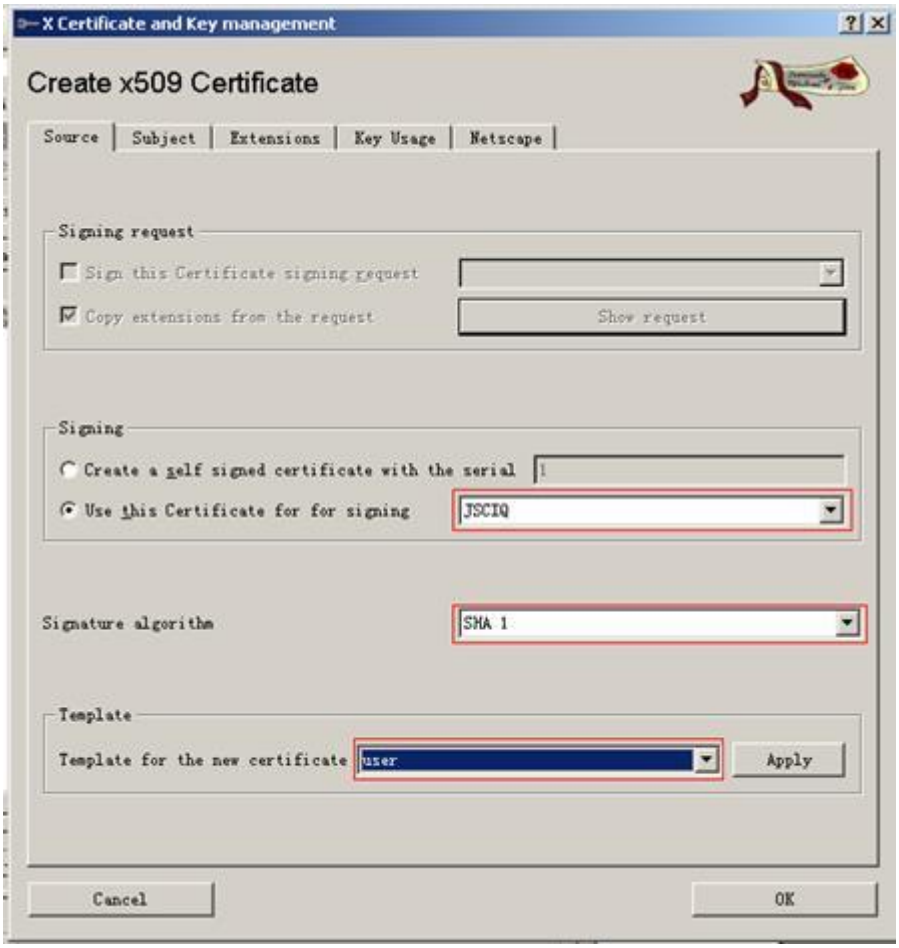
c. 在用户模版中，设置用户参数（由于每个用户名不同，因此 “Common name”不设置），并单击“ok”。



- 制作用户证书。

  a. 选择“Certificate > New Certificate”制作用户证书。

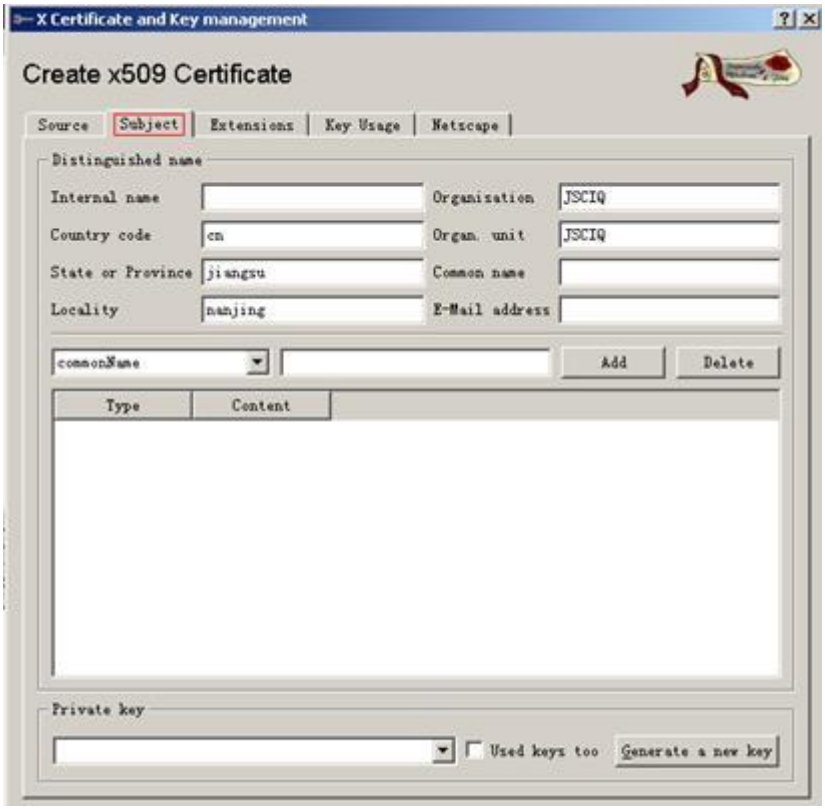
  b. 在“Signing”下选择“Use this Certificate for for signing”为之前的根证书“JSCIQ”，签名算法选择为“SHA-1”，“Template”下选择“user”，单击“Apply”按钮。



说明

必须选择签名算法为“SHA 1”，然后单击 Apply 按钮。

c. 在“subject”标签下可以看到已经有了之前模版中的设置项。



d. 按照下图中所标的顺序进行操作。

i. 在“subject”的“Internal name”中输入用户别名“wangt”。

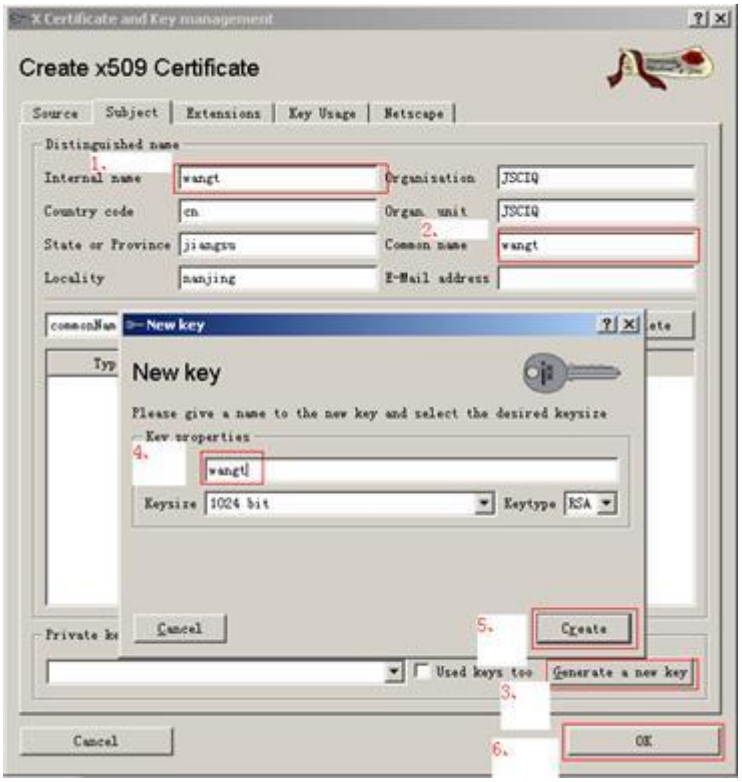
ii. 在“Common name”中输入用户名“wangt”。

iii. 单击右下角的“Generate a new key”。

iv. 在弹出的对话框中输入“wangt”。

v. 单击“create”按钮。

vi. 单击“ok”按扭。



e. 此时可以看到生成的证书。

1.

6. 制作设备证书。

a. 选择“Certificate > New Certificate”制作用户证书。

b. 在“Signing”下选择“Use this Certificate for for signing”为之前的根证书“JSCIQ”，签名算法选择为“SHA-1”，“Template”下选择“[default] HTTPS_server”，单击“Apply”按钮。

说明

必须选择签名算法为“SHA 1”，然后单击“Apply”按钮。

c. 在“subject”标签页中按照以下顺序进行操作。

i. 在“Internal name”中输入虚拟网关 IP“1.1.1.1”(必须为虚拟网关 IP)。

ii. 在“Common name”中输入虚拟网关 IP“1.1.1.1”(必须为虚拟网关 IP)。

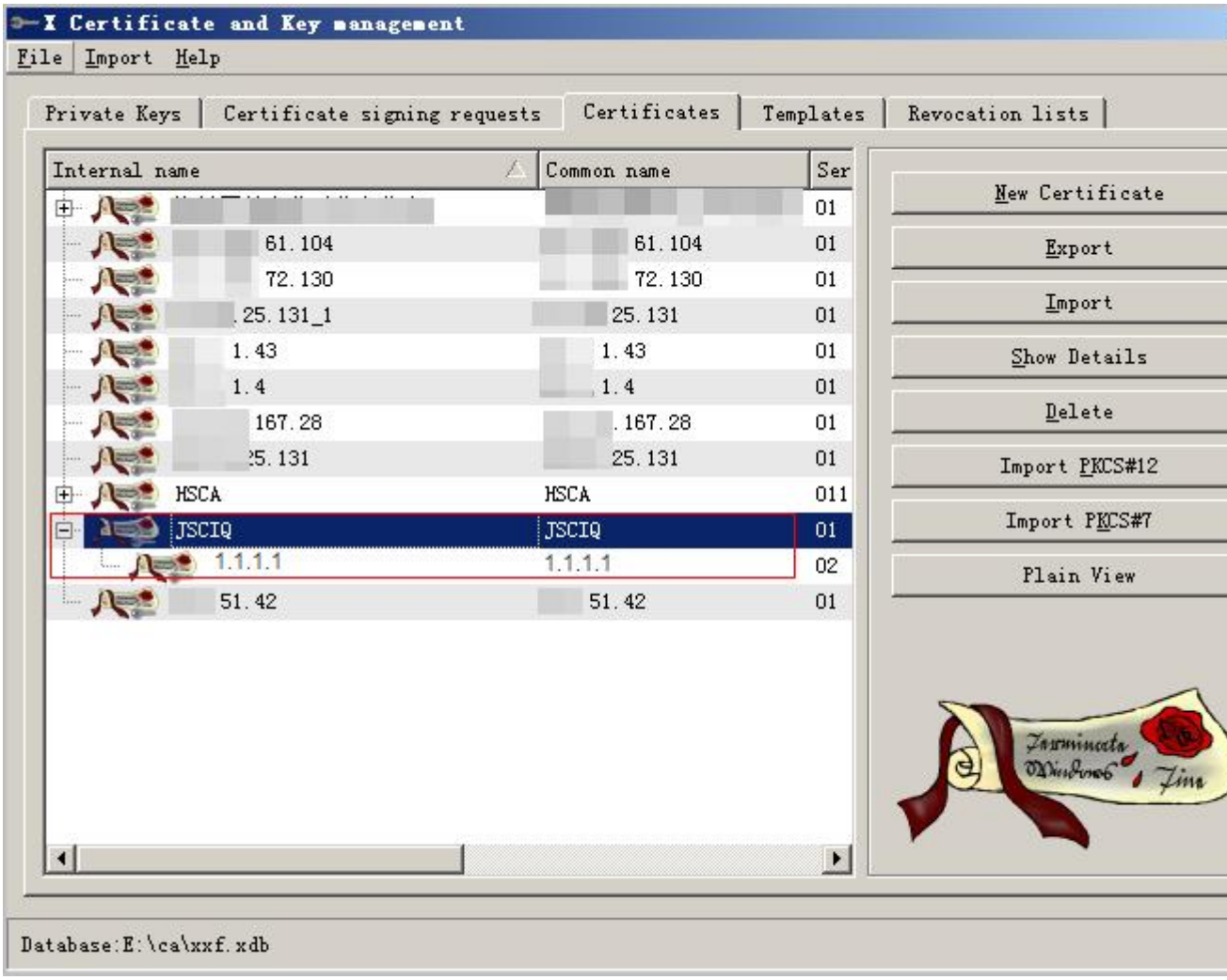
iii. 单击右下角的“Generate a new key”。

iv. 在弹出的对话框中输入“1.1.1.1”。

v. 单击“create”按钮。

vi. 单击“ok”按扭。

d. 此时可以看到生成的证书。



7. 导出证书。

- 导出根证书。

a. 选中根证书“JSCIQ”，单击“Export”。

b. 弹出如下对话框。

c. 单击上图中选择的按钮选择目录，然后单击“ok”即可。

说明

目录中不能包含中文字符。

d. 此时，在“G:/ca”下可以看到 JSCIQ.crt 证书。

1.

- 导出用户证书。

  a. 选择“Certificate”下用户证书“wangt”，单击“Export”。

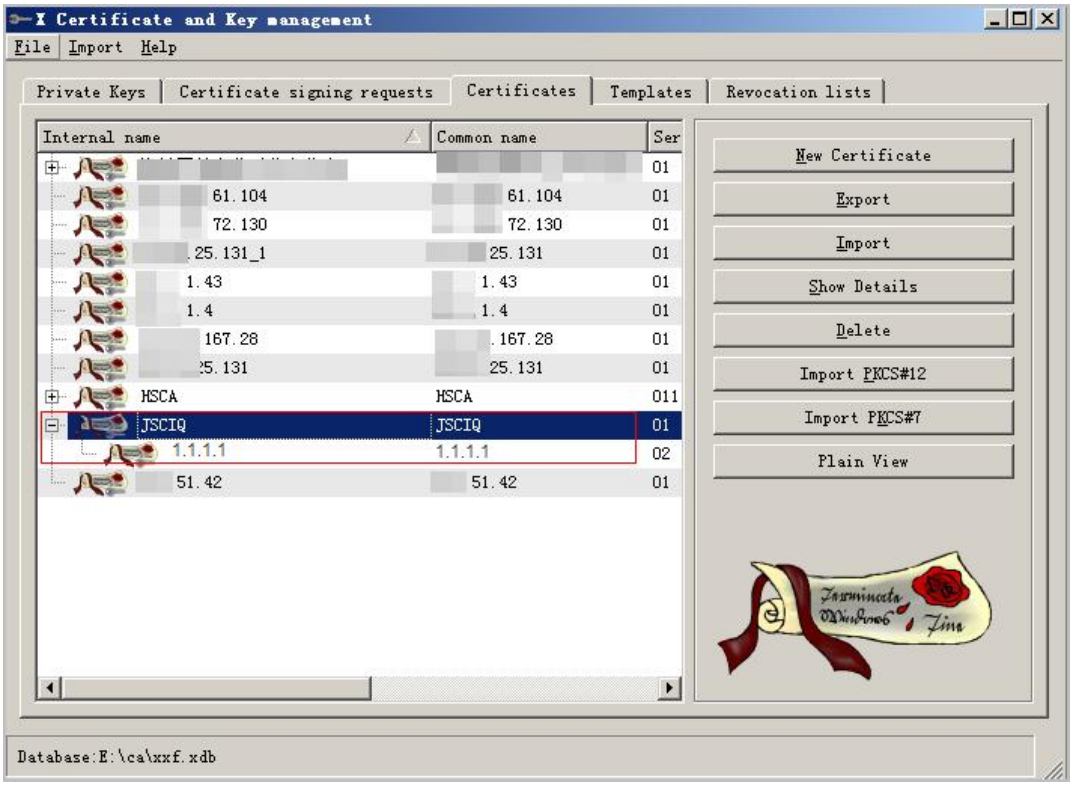
  b. 选择用户证书保存目录及保存类型选择为“PKCS #12”，单击“ok”。

  c. 在弹出的对话框中，密码为空即可，直接单击“ok”。

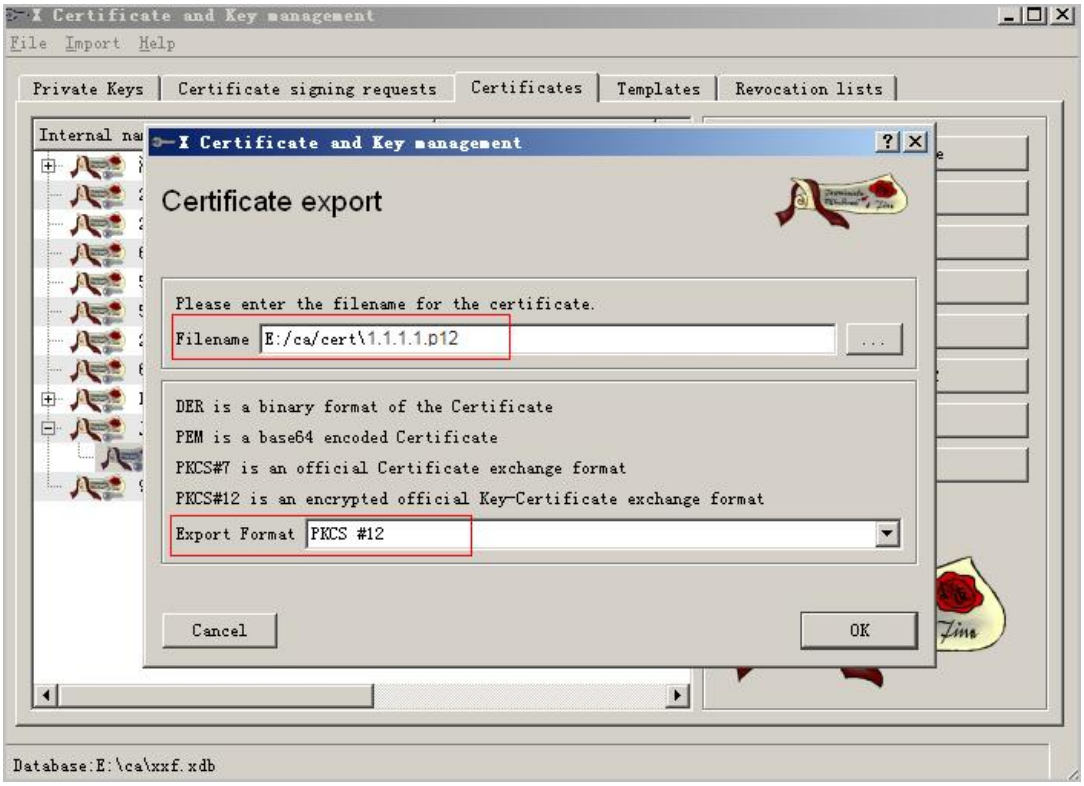
  d. 此时，G:\ca 下出现用户证书 wangt。

- 导出设备证书。

  a. 选择“Certificate”下设备证书“1.1.1.1”，单击“Export”。



b. 选择用户证书保存目录，保存类型选择为“PKCS #12”，单击“ok”。



c. 在弹出的对话框中，密码为空即可，直接单击“ok”。

d. 此时，“E:\ca\cert”下出现用户证书 1.1.1.1.p12。

说明

服务器开启证书过滤，使用颁发者作为条件过滤客户端证书时，在 Macos 和 Linux 系统用户证书的颁发者过滤字段为颁发者证书的 OU 或 CN 字段，Windows 系统无此限制。即在 Macos 和 Linux 系统，用户证书的颁发者 CN 或 OU 的值与服务器设置的相同时，用户证书才可以在客户端显示。否则不显示。

1.5.7 UniVPN 安装和运行是否都需要管理员权限

安装 UniVPN，需要有管理员权限。

运行 UniVPN，不需要有管理员权限，普通用户就行。

1.5.8 SSL VPN 使用客户端拨号成功后，终端是否支持自行修改账户密码

支持，请按照如下方式修改。

1. 右键单击客户端的托盘图标或客户端主界面单击设置，在弹出的菜单中选择“修改密码”。
2. 在弹出的“修改密码”窗口中修改登录密码。

说明

只有当 UniVPN 客户端与对端网关已经建立 VPN 连接的时候才能修改密码。

修改密码成功后，客户端将中断当前的 VPN 连接，需要您使用新密码重新登录。

1.5.9 为什么要提前在设备侧上传 ActiveX 控件

终端用户通过 IE 内核浏览器登录虚拟网关使用 SSL VPN 业务时，需要下载并安装 ActiveX 控件才能正常使用。老版本防火墙将 ActiveX 控件打包在网关的软件包中，故不需要提前上传。

从如下版本开始，ActiveX 控件单独发布，故需要提前在设备侧上传 ActiveX 控件。

- V600R007C00：除 USG6630E/6650E、USG6680E、USG6712E/6716E 外的款型需由管理员提前单独上传 ActiveX 控件至设备。
- V600R007C20：对于 V600R007C20SPC300 之前版本，除 USG6391E/6610E/6620E、USG6630E/6650E、USG6680E 和 USG6712E/6716E 外的款型需由管理员提前上传 ActiveX 控件至设备。对于 V600R007C20SPC300 及后续版本，所有款型都需由管理员提前上传 ActiveX 控件至设备。
- V500R005C20：仅 USG9500 需由管理员提前单独上传 ActiveX 控件至设备。

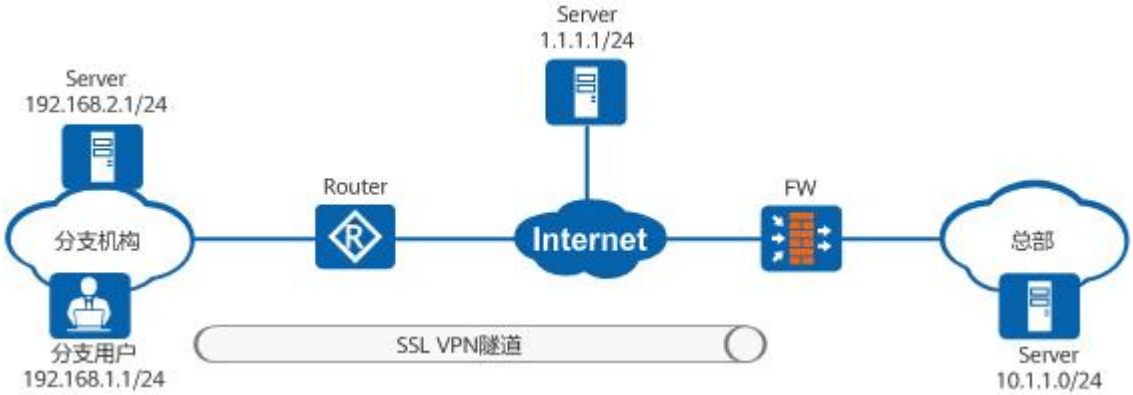
1.5.10 虚拟网关服务视图和虚拟网关用户组视图下配置的网络扩展路由模式哪个优先级高

如果同时在虚拟网关服务视图、虚拟网关用户组视图下配置了路由模式，则虚拟网关用户组视图下配置的路由模式优先。

1.5.11 SSL VPN 网络扩展三种路由模式下在终端生成的路由有什么区别

SSL VPN 的网络扩展服务提供三种路由模式：自适应（手动路由）模式、分离路由模式和全路由模式。

启用网络扩展后，防火墙根据配置的路由模式向分支机构的用户推送路由。路由模式决定了用户可以访问的资源范围。



假设用户从防火墙获取的 IP 地址为 6.6.6.1/24（虚拟网卡的 IP 地址），路由的下一跳地址为 192.168.1.2。

1.5.11.7 手动路由模式

路由模式	命令	用户侧生成的路由	接入服务
手动路由模式	network-extension mode manual network-extension manual-route 10.1.1.0 255.255.255.0 选择手动路由模式时，必须指定用户访问的 Intranet 网段。	只有到总部（10.1.1.0/24）的流量进入虚拟网卡 6.6.6.1，并进入 SSL VPN 隧道。到 Internet 和 LAN 的路由保持不变。	用户可以同时访问 LAN、Internet 和企业内网。

```
IPv4 Route Table
===========================================================================================
Active Routes:
Network Destination        Netmask          Gateway          Interface      Metric
        0.0.0.0            0.0.0.0      192.168.1.2      192.168.1.2          10    //访问Internet的路由
        6.6.6.1      255.255.255.255        On-link            6.6.6.1         257
       10.1.1.0      255.255.255.0        On-link            6.6.6.1           1    //访问企业内网的路由
     10.1.1.255      255.255.255.255        On-link            6.6.6.1         257
   192.168.2.0       255.255.255.0    192.168.1.2      192.168.1.2          11    //访问局域网的路由
===========================================================================================
```

1.5.11.8 分离路由模式

路由模式	命令	用户侧生成的路由	接入服务
分离路由模式	network-extension mode split	默认路由的出接口 IP 地址被修改为虚拟网卡的 IP 地址，用户无法访问 Internet。由于到 LAN 的路由保持不变，用户仍然可以访问 LAN。	用户只能访问 LAN 和企业内网，不能访问 Internet。

```
IPv4 Route Table
===========================================================================================
Active Routes:
Network Destination        Netmask          Gateway          Interface      Metric
        0.0.0.0            0.0.0.0        On-link            6.6.6.1           1    //访问企业内网的路由
        6.6.6.0      255.255.255.0        On-link            6.6.6.1         257
        6.6.6.1      255.255.255.255        On-link            6.6.6.1         257
      6.6.6.255      255.255.255.255        On-link            6.6.6.1         257
   192.168.2.0       255.255.255.0    192.168.1.2      192.168.1.2          11    //访问局域网的路由
===========================================================================================
```

1.5.11.9 全路由模式

路由模式	命令	用户侧生成的路由	接入服务
全路由模式	network-extension mode full	几乎所有路由的出接口 IP 地址都修改为虚拟网卡的 IP 地址，这意味着所有来自用户的流量都进入 SSL VPN 隧道。路由表中仍然存在到 192.168.2.0（本地 LAN）的路由。由于此路由的开销为 11，但防火墙下发的路由开销为 1。因此，到 192.168.2.0 的路由不生效。	用户只能访问企业内网，不能访问 LAN 和 Internet。

```
IPv4 Route Table
===========================================================================================================
Active Routes:
Network Destination        Netmask          Gateway          Interface      Metric
          0.0.0.0          0.0.0.0          On-link            6.6.6.1          1    //访问企业内网的路由
          6.6.6.0    255.255.255.0          On-link            6.6.6.1        257    //访问企业内网的路由
          6.6.6.1  255.255.255.255          On-link            6.6.6.1        257    //访问企业内网的路由
        6.6.6.255  255.255.255.255          On-link            6.6.6.1        257    //访问企业内网的路由
      192.168.2.0    255.255.255.0    192.168.1.2        192.168.1.2         11    //访问企业内网的路由
      192.168.2.0    255.255.255.0          On-link            6.6.6.1          1    //访问企业内网的路由
    192.168.2.255  255.255.255.255          On-link            6.6.6.1        257    //访问企业内网的路由
===========================================================================================================
```

SSL VPN 的网络扩展服务提供三种路由模式总结如下：

- 在手动路由模式下，必须明确定义总部网络子网，并且可以通过 SSL VPN 的虚拟网络适配器访问它，同时内部网和互联网访问也可以保持在可访问的情况下。
- 在分离路由模式下，内部 LAN 访问继续可访问，因为本地 LAN 网关未更改。但是互联网和 HQ 子网可以通过虚拟网络适配器访问，这就是为什么 SSL VPN 客户端失去了互联网访问，应在 HQ 中配置代理服务器，为他们提供互联网访问。
- 在全路由模式下，所有流量路由（互联网、内部网、HQ 子网）都通过 SSL VPN 的虚拟网络适配器路由，这就是为什么在该模式下只有 HQ 子网可以访问，内部网和互联网将无法访问（互联网可以在总部再次提供代理服务器，如拆分隧道场景）。

说明

客户端在不同类型的操作系统上，相同的路由模式下发的路由也会有所差异，以实际下发路由为准。

1.5.12 SSL VPN 是否支持双因子认证

支持。SSL VPN 支持如下两类双因子认证：

1. RADIUS 双因子认证：防火墙和 RADIUS 服务器配合，对 SSL VPN 用户进行身份认证。认证时，除了验证用户名和静态 PIN 码，还要求用户输入动态验证码。动态验证码可以是短信验证码或硬件令牌生成的动态密码。
2. 证书挑战认证：将验证客户端证书与本地认证或服务器认证结合起来。

1.5.13 使用客户端拨号登录无法生成虚拟网卡，如何解决

老版本 UniVPN 部分驱动程序与操作系统不兼容，可能导致无法生成虚拟网卡，请安装最新版本的 UniVPN 解决。

1.5.14 SSL VPN 有哪些命令可以用来采集调试日志

建议使用 debugging sslvpn-user all v-gateway-name user-name 命令来采集调试日志，此命令可以打开所有业务访问调测开关。

1.5.15 SSL VPN 接入后 ping 内网延迟大，如何解决

SSL VPN 接入后 Ping 内网延迟大，可能原因如下。

- 防火墙配置的安全策略，没有放行 untrust 到 local 的 UDP 协议和 443 端口的报文。

终端采用快速传输模式访问 SSL VPN 虚拟网关时，采用 UDP 协议和 443 端口，因此需要在防火墙上配置安全策略以放行 untrust 到 local 的 UDP 协议和 443 端口的报文。如果 SSL VPN 虚拟网关在内网，外层有 NAT 设备，还需要在 NAT 设备上配置 UDP 协议和 443 端口的 NAT 映射。

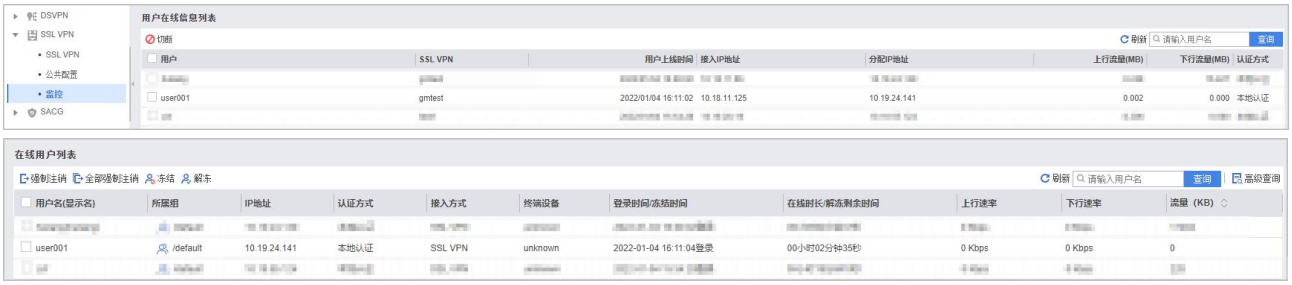
- 防火墙配置了 HTTPS-Flood 攻击防范，且阈值过低。

执行 display anti-ddos defend information system 命令查看是否开启 HTTPS-Flood 攻击防范及其阈值，可以尝试执行 anti-ddos https-flood source-detect alert-rate alert-rate 命令重新配置阈值。

1.5.16 SSL VPN 和用户管理的关联

用户在使用 Web 代理、端口转发和文件共享业务时，用户管理在线用户列表中是不显示用户信息的。只有在使用网络扩展业务时，用户管理用户才会上线，才能在在线用户列表中看到此用户信息。

Web 界面查看 SSL VPN 用户上线的地方有两处，一处是在用户的“在线用户”那里看，另一处是在 SSL VPN 的“监控”那里看，如下图。



命令行查看方法：

- 在虚拟网关 basic 视图下执行 display onlineuser 命令也可以查看。
- 在系统视图下执行 display user-manage online-user 命令也可以查看。

在用户管理在线用户列表中将某用户注销，效果同在 SSL VPN 监控在线用户列表中切断用户一样，用户都会被强制下线。

1.5.17 SSL VPN 角色授权知识点

虚拟网关默认角色 default 只能编辑不能删除，且缺省不可以访问内网任何资源。

USG6000 V1 版本默认角色 default 缺省可以访问内网任何资源，从 V1 版本升级到 V5 版本，这点需关注。

用户登录 SSL VPN 虚拟网关，如果用户/用户组没有加入任何自定义角色，缺省属于 default 角色。

如果 SSL VPN 拨号使用的认证域配置了服务器授权，授权组的认定方式如下：

1. 如果本地存在同名用户，则授权时本地同名用户的父组有效。
2. 如果不存在同名用户，则查看是否配置新用户选项。

   a. 未配置新用户选项

   授权时授权服务器中该用户的父组有效。

   b. 配置新用户选项

   不允许新用户登录：该用户被拒绝登录，授权终止。
   添加到指定的用户组或安全组中：授权时此处指定的用户的父组有效。
   仅作为临时用户，不添加到本地用户列表中：授权时此处指定的用户的父组有效。

1.5.18 SSL VPN 认证后如何基于用户做权限管控

执行如下两个步骤配置基于用户做权限管控。

1. 针对网络扩展地址池访问内网资源的数据流配置“免认证”认证策略。
2. 配置安全策略绑定用户/用户组。

1.5.19 SSL VPN 用户接入后对于非法操作如何溯源

某个时间点，用户通过 SSL VPN 接入内网后获得一个虚拟 IP 地址，并使用该虚拟 IP 地址和内网服务器交互。如果 SSL VPN 用户对内网服务器进行了某种非法操作，此时需要溯源找到操作的用户。

请按照如下方法溯源。

1. 查看系统日志，获得虚拟 IP 地址和用户账号的对应关系。
   a. 选择“监控 > 日志 > 系统日志”。
   b. 查找“USERS/5/NESRV”打头的日志，类似如下。

```
用户登录 SSL VPN，启用网络扩展成功，记录日志：
%2000-04-02 01:35:41 USG6300 %%01USERS/5/NESRV(l): id=USG6320 time="2000-04-02 01:35:40"
fw=USG6300 pri=5 vsys=root vpn=gateway user="huawei001" src=11.11.11.2 dst=11.11.11.1
duration=0s rcvd=0byte(s) sent=0byte(s) type=vpn service=1 msg="Network Extension: Service
startup, the virtual IP address is 13.13.13.102."

用户登录 SSL VPN，关闭网络扩展成功，记录日志：
%2000-04-02 01:35:59 USG6300 %%01USERS/5/NESRV(l): id=USG6320 time="2000-04-02 01:35:40"
fw=USG6300 pri=5 vsys=root vpn=gateway user="huawei001" src=11.11.11.2 dst=11.11.11.1
duration=18s rcvd=0byte(s) sent=715byte(s) type=vpn service=1 msg="Network Extension: Service
shutdown, the virtual IP address is 13.13.13.102."
```

2. 检查防火墙是否配置了认证策略，如果已针对 SSL VPN 用户访问内网服务器的流量配置了“免认证”的认证策略，则这部分流量产生的流量日志就会携带用户信息。

1.5.20 SSL VPN 服务器认证场景下的授权规则如何

服务器认证场景下的授权规则主要存在本地授权、服务器授权两种方式。

本地授权

假设本地授权的配置如下。

```
#
domain icf.local
  authentication-scheme admin_ldap
  authorization-scheme local
  service-scheme webServerScheme
  ldap-server ldapserver2
  service-type internetaccess ssl-vpn l2tp
  internet-access mode password
  reference user current-domain
#
```

当用户 test001@icf.local 存在时，授权规则如下。
用户 test001@icf.local 绑定 virtual-ip 地址，生效。
用户 test001@icf.local 绑定某自定义角色，命中该角色。
用户 test001@icf.local 本地所属的直接父组绑定某自定义角色，命中该角色。
用户 test001@icf.local 本地所属的间接父组绑定某自定义角色，不命中该角色。
用户 test001@icf.local 在认证服务器上所属的直接父组绑定某自定义角色，不命中该角色。
用户 test001@icf.local 在认证服务器上所属的间接父组绑定某自定义角色，不命中该角色。
用户 test001@icf.local 不存在，授权规则如下。
用户 test001@icf.local 在认证服务器上所属的直接父组绑定某自定义角色，不命中该角色。
用户 test001@icf.local 在认证服务器上所属的间接父组绑定某自定义角色，不命中该角色。
找绑定根组 icf.local 的角色，如果没有角色绑定根组 icf.local，则命中 default 缺省角色。

服务器授权

假设服务器授权的配置如下。

```
#
 domain icf.local
  authentication-scheme admin_ldap
  authorization-scheme ldap
  service-scheme webServerScheme
  ldap-server ldapserver2
  service-type internetaccess ssl-vpn l2tp
  internet-access mode password
  reference user current-domain
#
```

当用户 test001@icf.local 存在时，授权规则如下。
用户 test001@icf.local 绑定 virtual-ip 地址，不生效。
用户 test001@icf.local 绑定某自定义角色，不命中该角色。
用户 test001@icf.local 本地所属的直接父组绑定某自定义角色，命中该角色。
用户 test001@icf.local 本地所属的间接父组绑定某自定义角色，不命中该角色。
用户 test001@icf.local 在认证服务器上所属的直接父组绑定某自定义角色，不命中该角色。

用户 test001@icf.local 在认证服务器上所属的间接父组绑定某自定义角色，不命中该角色。
当用户 test001@icf.local 不存在时，授权规则如下。
用户 test001@icf.local 在认证服务器上所属的直接父组绑定某自定义角色，命中该角色。
用户 test001@icf.local 在认证服务器上所属的间接父组绑定某自定义角色，不命中该角色。

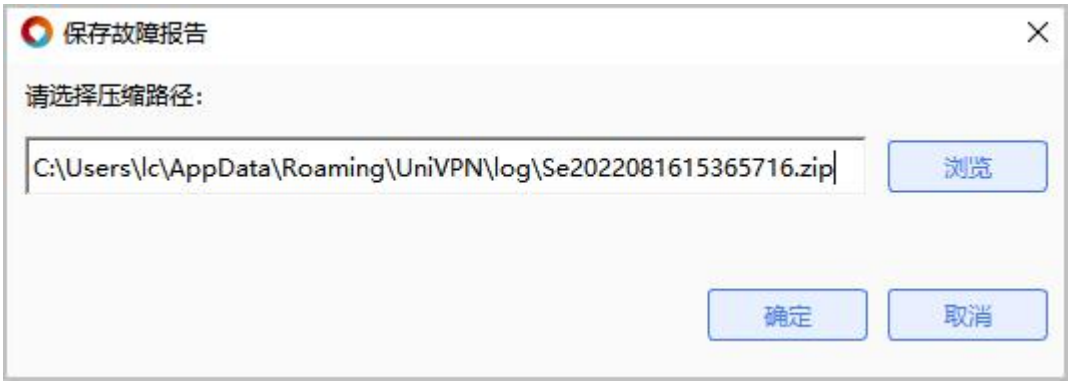
1.5.21 UniVPN 的日志采集方法

PC 终端的采集方法

1. 右键单击 UniVPN 的托盘图标。

2. 选择“错误报告”。

3. 根据提示输入故障标题和操作步骤
4. 单击“确定”，等待日志压缩包生成。



5. 单击“浏览”打开文件位置。

UniVPN 生成错误报告时会收集客户端软件的使用信息，请采取足够的措施以确保以下信息受到严格保护。

- error_detail.txt：记录用户手动输入的对产生该错误的操作步骤的描述，以及所用客户端的版本号信息。
- netcard_info.txt：记录 UniVPN 所在 PC 的网卡信息。
- operate_system_info.txt：记录 UniVPN 所在 PC 的操作系统信息。
- proxy_info.txt：记录 UniVPN 所在 PC 的代理服务器信息。
- route_info.txt：记录 UniVPN 所在 PC 的路由信息。
- UniVPN_UniVPNCS_0.log：记录 UniVPN 业务配置产生的日志信息，例如用户登录成功或失败、VPN 隧道建立正常或异常等信息。

- UniVPN_UniVPNUI_0.log：记录 UniVPN 配置界面产生的日志信息，例如 VPN 连接配置和中英文界面切换所产生的日志信息。
- UniVPN_UniVPNPromoteService_0.log：UniVPN 的服务进程，用于确保 UniVPN 正常运行。
- 崩溃文件：当 UniVPN 在出现异常关闭的情况下将生成崩溃文件，不同原因造成的 UniVPN 异常关闭所生成的崩溃文件名称不一样。在 Windows 操作系统下崩溃文件的后缀是*.dmp，在 MAC 操作系统下生成的崩溃文件后缀为*.core。

1.5.22 SSL VPN 常见业务日志有哪些

在网络发生异常时，网络管理员需要根据日志溯源，下面列出了 SSL VPN 业务常用的日志，以帮助网络管理员溯源使用。

用户登录 SSL VPN 失败，记录日志。

%2000-04-02 01:27:17 sysname %%01USERS/4/USRPWDERR(l): id=sysname time="2000-04-02 01:27:13" fw=sysname pri=4 vsys=root vpn=gateway user="huawei001" src=11.11.11.2 dst=0.0.0.0 duration=3s rcvd=0byte(s) sent=0byte(s) type=vpn service=5 msg="Session:

用户登录 SSL VPN 成功，记录日志。

%2000-04-02 01:35:34 sysname %%01USERS/5/LOGINSUC(l): id=sysname time="2000-04-02 01:35:33" fw=sysname pri=5 vsys=root vpn=gateway user="huawei001" src=11.11.11.2 dst=0.0.0.0 duration=0s rcvd=0byte(s) sent=0byte(s) type=vpn service=5 msg="Session: huawei001 logged in."

用户注销 SSL VPN，记录日志。

%2000-04-02 01:36:00 sysname %%01USERS/5/LOGOUT(l): id=sysname time="2000-04-02 01:35:59" fw=sysname pri=5 vsys=root vpn=gateway user="huawei001" src=11.11.11.2 dst=0.0.0.0 duration=26s rcvd=0byte(s) sent=715byte(s) type=vpn service=5 msg="Session: huawei001 logged out."

用户登录 SSL VPN，启用网络扩展成功，记录日志。

%2000-04-02 01:35:41 sysname %%01USERS/5/NESRV(l): id=sysname time="2000-04-02 01:35:40" fw=sysname pri=5 vsys=root vpn=gateway user="huawei001" src=11.11.11.2 dst=11.11.11.1 duration=0s rcvd=0byte(s) sent=0byte(s) type=vpn service=1 msg="Network Extension StartUp, The virtual IP adddress is 13.13.13.102."

用户登录 SSL VPN，关闭网络扩展成功，记录日志。

%2000-04-02 01:35:59 sysname %%01USERS/5/NESRV(l): id=sysname time="2000-04-02 01:35:40" fw=sysname pri=5 vsys=root vpn=gateway user="huawei001" src=11.11.11.2 dst=11.11.11.1 duration=18s rcvd=0byte(s) sent=715byte(s) type=vpn service=1 msg="Network Extension: The virtual IP adddress is 13.13.13.102."

用户登录 SSL VPN，修改密码成功，记录日志。

%2000-04-02 01:35:21 sysname %%01USERS/5/CHGPWDKICK(l): id=sysname time="2000-04-02 01:35:20" fw=sysname pri=5 vsys=root vpn=gateway user="huawei001" src=11.11.11.2 dst=0.0.0.0 duration=36s rcvd=0byte(s) sent=636byte(s) type=vpn service=5 msg="User huawei001 was forcibly logged out, for the password was successfully modified."

用户启用网络扩展后，被管理员剔除下线，记录日志。

%2000-04-02 01:36:00 sysname %%01USERS/5/LOGOUT(l): id=sysname time="2000-04-02 01:35:59" fw=sysname pri=5 vsys=root vpn=gateway user="huawei001" src=11.11.11.2

dst=0.0.0.0 duration=26s rcvd=0byte(s) sent=715byte(s) type=vpn service=5 msg="Session: huawei001 logged out with virtual IP address 13.13.13.102."
用户会话老化下线，记录日志。
%2000-04-02 02:10:00 sysname %%01USERS/5/EXPIREUSER (l): id=sysname time="2000-04-02 01:09:59" fw=sysname pri=5 vsys=root vpn=gateway user="huawei001" src=11.11.11.2 dst=0.0.0.0 duration=26s rcvd=0byte(s) sent=715byte(s) type=vpn service=5 msg="User huawei001 was forcibly logged out for the user ages."
查看 SSL VPN 用户访问资源的日志。
[sysname] v-gateway test
[sysname-test] service
注意：开启网络扩展日志功能后，每次客户端通过网络扩展与内网服务器建立 TCP 连接时，网关侧都会记录一条连接日志。在 TCP 连接很频繁时，会在网关侧生成很多的日志信息，这样会影响其他日志信息的查看。
[sysname-test-service] network-extension log enable //开启网络扩展的日志开关

1.5.23 SSL VPN 调整网络扩展参数是否强制用户下线

管理员变更（增加、修改、删除）网络扩展手工路由网段，该虚拟网关已在线的用户会被强制踢下线。
管理员添加网络扩展地址池网段，该虚拟网关已在线的用户不会被踢下线。
管理员删除或修改网络扩展地址池网段，该虚拟网关从这个网段里分配 IP 地址上线的用户会被踢下线，不从这个网段中分配 IP 地址上线的用户不会被踢下线。

1.5.24 SSL VPN 业务报文的域间关系是怎样确定

SSL VPN 包含 Web 代理、文件共享、端口转发、网络扩展四个业务。Web 代理、文件共享、端口转发三个业务对应的流量经过的域间关系是 local->trust。Trust 表示防火墙连接企业内网的接口对应的安全区域。
SSL VPN 用户通过网络扩展业务访问企业内网资源，防火墙会以该用户的公网 IP 地址作为目的地址反查路由，找到一个到达该公网 IP 地址的路由出接口。这个出接口所在的安全区域，就是网络扩展业务流量的源安全区域。在多出口场景中，反查路由可能存在多个出接口，则需要将这些出接口所在的安全区域都作为源安全域。防火墙根据网络扩展业务流量的目的 IP 地址查找路由，将出接口所在的安全区域作为目的安全区域。

1.5.25 SSL VPN 登录之后能否访问防火墙内网接口地址进行管理

可以。
需要注意的是，在双机热备场景下，SSL VPN 拨号到主防火墙上，可以使用主墙的内网接口地址对设备进行管理，但是无法通过相同方式对备墙进行管理。要管理备墙，需要通过内网堡垒机或中间设备间接跳转。

对于管理接口绑定 VPN 实例的场景，SSL VPN 拨号后无法访问该管理接口对设备进行管理。这时需要通过内层设备中转来访问管理接口，或者通过访问没有绑定 VPN 实例的内网接口规避。

1.5.26 双机场景 SSL VPN 哪些配置可以备份到对端

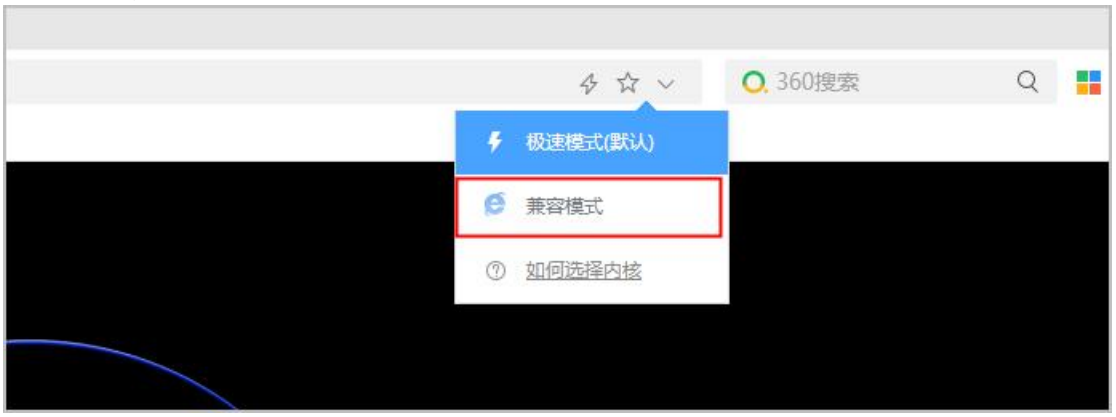
SSL VPN 的一部分配置以 Buildrun 方式展示，另外一部分配置保存在数据库里，如虚拟网关最大用户数、虚拟网关最大资源数、虚拟网关设备证书、虚拟网关角色绑定用户/用户组等，这些配置在配置文件中看不到，需要登录设备才能查看。
双机热备场景下，SSL VPN 的配置可以实现备份，包括 SSL VPN 角色授权中添加用户/用户组、创建角色、角色绑定用户/用户组、角色去绑定用户/用户组、删除角色、SSL VPN 角色授权中删除用户/用户组。

1.5.27 SSL VPN 是否支持 IPv6

不支持。

1.5.28 SSL VPN 控件支持浏览器的情况

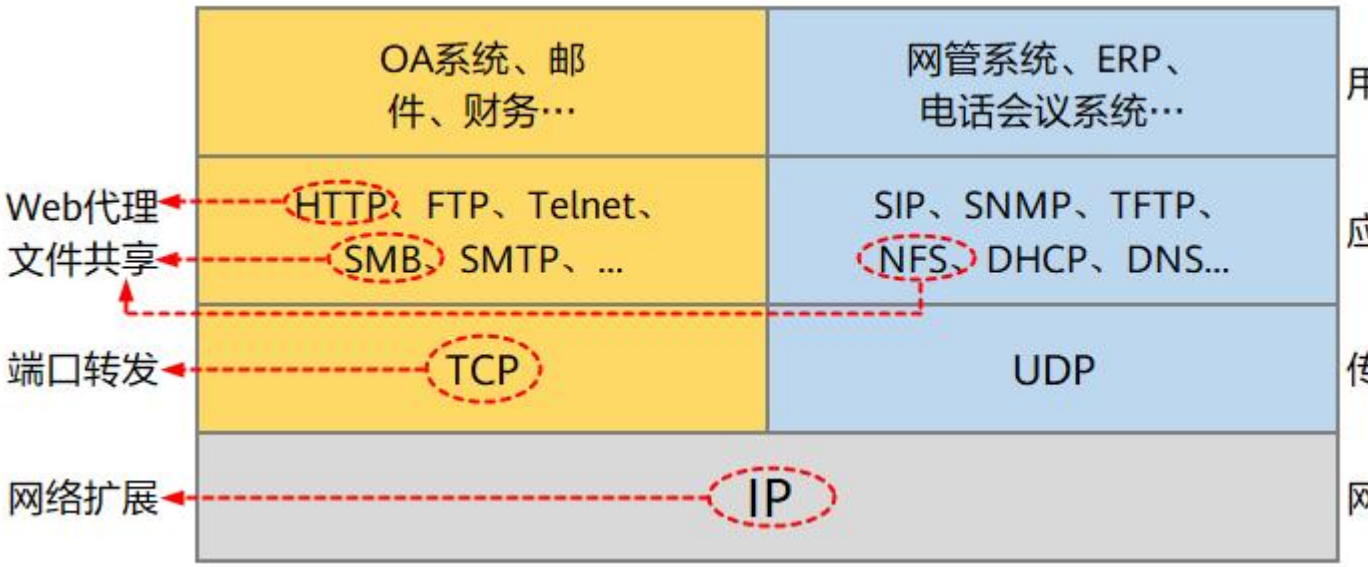
目前，主流的浏览器内核有以下五种：
Trident 内核：常见浏览器有 IE
Gecko 内核：常见浏览器有 Mozilla Firefox
Webkit 内核：常见浏览器有 Apple Safari (Win/Mac/iPhone/iPad)、傲游浏览器 3
Blink 内核：常见浏览器有 Chrome、Opera
Edge 内核：常见浏览器有 Edge
国内厂商浏览器的新版本大多是“双核”甚至是“多核”，其中一个内核是 Trident，然后再增加一个其他内核。一般把其他内核叫做“高速浏览模式”，而 Trident 内核则是“兼容浏览模式”，用户可以来回切换。



360 安全浏览器（Trident+Blink）
360 极速浏览器（Trident+Blink）

猎豹安全浏览器（Trident+Blink）
傲游浏览器（Trident+Webkit）
世界之窗浏览器（Trident+Blink）
搜狗高速浏览器（Trident+Webkit）
UC 浏览器（Trident+Blink）
目前，防火墙的 SSL VPN 特性（Web-link、端口转发、网络扩展和主机检查）仅支持在 IE 内核（即 Trident 内核）的浏览器上安装 ActiveX 控件运行，其它浏览器内核暂不支持。

1.5.29 SSL VPN 各子特性的应用范围



Web 代理： 访问内网 Web 资源。
文件共享： 访问内网系统服务器的共享资源。
端口转发： 访问内网 TCP 应用服务开启的资源。
网络扩展： 访问内网所有的 IP 资源。

1.5.30 SSL VPN 是否支持友商 VPN 客户端拨号

每个厂商定义的 SSL VPN 私有头不同，因此，不同厂商的 VPN 客户端和 SSL VPN 网关之间不可访问。

1.5.31 SVN 和防火墙 SSL VPN 特性区别

SSL VPN 总项	SSL VPN 子项	FW 机型	SVN 机型
虚拟网关	虚拟网关是否受 License 控制	不受 License 限制，受设备型号规格限制	受 License 限制，默认赠送 1 个
	支持根系统下创建虚拟网关	支持	不支持，所有虚拟网关均创建在虚拟系统下
认证授权	是否支持多级认证	不支持	支持，最多支持 3 级认证
	认证和授权分离	不支持	支持
	支持多个认证域	支持	不支持
	访问控制策略	不支持	支持
	安全策略与用户/组关联	支持	不支持
	禁止 Web 登录	不支持	支持
辅助认证	终端标识码	不支持	支持
	图形校验码	不支持	支持
桌面云	负载均衡网关	不支持	支持
	安全云网关	不支持	支持
用户锁定	用户锁定时的认证方式	仅本地用户	本地用户或服务器用户
	用户锁定的方式	仅锁定用户名	支持锁定用户名或用户源 IP

1.5.32 OSPF 组网下如何发布 SSL VPN 业务地址和网络扩展地址池的路由

假设存在如下信息。

- 网络扩展地址池：

```
network-extension netpool 10.23.40.1 10.23.47.254 255.255.248.0
network-extension netpool 10.23.116.1 10.23.117.254 255.255.254.0
network-extension netpool 10.23.144.1 10.23.145.254 255.255.254.0
network-extension netpool 10.23.228.1 10.23.231.254 255.255.252.0
network-extension netpool 10.23.232.1 10.23.239.254 255.255.248.0
network-extension netpool 10.23.244.1 10.23.247.254 255.255.252.0
```

- 防火墙与内网交换机互联接口：10.23.249.253
- 防火墙上已配置的缺省路由：ip route-static 0.0.0.0 0.0.0.0 10.23.175.249
- 内网交换机和防火墙互联接口：10.23.249.254

配置通过 OSPF 向内网交换机发布网络扩展地址池网段路由的方法如下。

```
 # 配置到各网络扩展地址池的路由。
ip route-static 10.23.40.1 255.255.248.0 10.23.175.249
```

```
ip route-static 10.23.116.1 255.255.254.0 10.23.175.249
ip route-static 10.23.144.1 255.255.254.0 10.23.175.249
ip route-static 10.23.228.1 255.255.252.0 10.23.175.249
ip route-static 10.23.232.1 255.255.248.0 10.23.175.249
ip route-static 10.23.244.1 255.255.252.0 10.23.175.249

 # 配置地址前缀列表，并指定地址前缀列表的匹配模式为允许，过滤的 IP 地址为网 络扩展地址池网段。
ip ip-prefix prefix-a index 10 permit 10.23.40.1 21
ip ip-prefix prefix-a index 20 permit 10.23.116.1 23
ip ip-prefix prefix-a index 30 permit 10.23.144.1 23
ip ip-prefix prefix-a index 40 permit 10.23.228.1 22
ip ip-prefix prefix-a index 50 permit 10.23.232.1 21
ip ip-prefix prefix-a index 60 permit 10.23.244.1 22

# 配置名为 sslvpn 的 route-policy，其节点号为 1，匹配模式为允许。
route-policy sslvpn permit node 1
if-match ip-prefix prefix-a

# 配置名为 sslvpn 的 route-policy，其节点号为 100，匹配模式为拒绝。
route-policy sslvpn deny node 100

# 配置 ospf 引入静态路由。
ospf 23 router-id 10.23.249.253
bandwidth-reference 100000
import-route static route-policy sslvpn
area 0.0.0.23
#
配置通过 OSPF 向外网发布 Loopback 地址路由的方法如下。SSL VPN 虚拟网关使用此 Loopback 地址。
# 配置 Loopback 地址。
interface Loopback 10
ip address X.X.X.X 32

# 配置 ospf 引入静态路由。
ospf 23 router-id 10.23.249.253
bandwidth-reference 100000
import-route static route-policy sslvpn
area 0.0.0.23
network X.X.X.X 0.0.0.0

# 配置 SSL VPN 虚拟网关使用此 Loopback 地址。
v-gateway ssl_vpn ip address X.X.X.X
```

1.5.33 SSL VPN 是否支持双机热备负载分担

不支持。这里的不支持不是说 SSL VPN 功能与双机负载分担功能互斥，而是指即便双机负载分担模式下配置了 SSL VPN 功能，SSL VPN 流量也只会由“配置主设备”来处理，而不会分担一部分到“配置从设备”，实现不了双机分担 SSL VPN 流量的预期效果。

配置主设备指的是命令行提示符前有 HRP_M 前缀的那台设备。

配置从设备指的是命令行提示符前有 HRP_S 前缀的那台设备。

1.5.34 SSL VPN 是否支持双机热备主备备份

支持。主防火墙 SSL VPN 用户在线会话信息会自动备份到备防火墙上，在双机倒换过程中，SSL VPN 用户不会掉线，无需重新拨号。

1.5.35 SSL VPN 用户是否支持不认证登录

不支持

1.5.36 UniVPN 是否支持手机终端

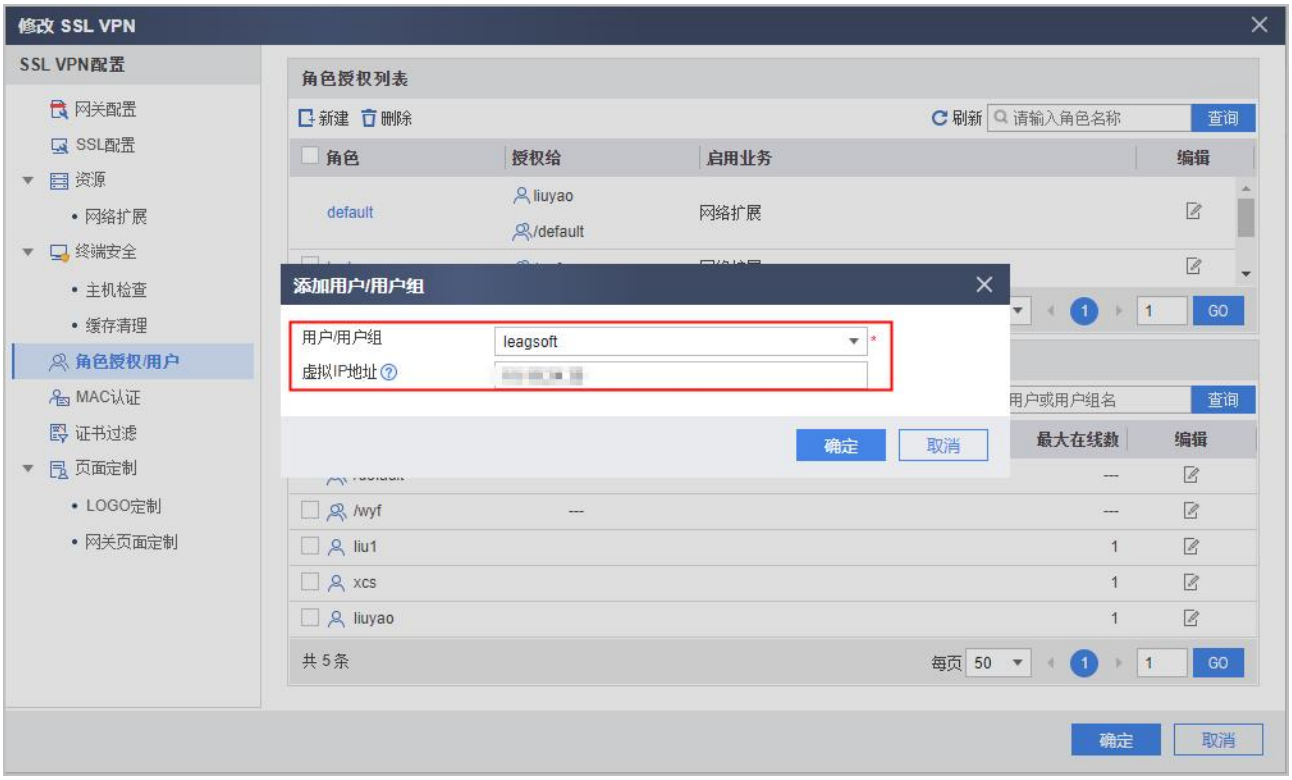
支持。

UniConnect 客户端支持安装在 IOS 系统（10.0 及以上版本）和 Android 系统（5.0 及以上版本）的终端上。

若出现卡顿等问题，请尝试使用操作系统版本较高的手机。

1.5.37 SSL VPN 如何实现用户绑定网络扩展虚拟地址

在“角色授权 > 用户”中的“用户 > 用户组列表”下单击“添加”，然后为用户绑定虚拟 IP 地址



1.5.38 SSL VPN 网络扩展虚拟 IP 地址分配规则

网络扩展业务虚拟 IP 地址分配的优先顺序如下：

当用户只绑定网络扩展虚拟 IP 时，用户将会分配到此虚拟 IP。

当用户组绑定网络扩展虚拟 IP 地址池时，用户组内的用户将会分配到此地址池中的虚拟 IP。

当用户组绑定网络扩展虚拟 IP 地址池时，用户组内的用户同时绑定了网络扩展虚拟 IP 时，该用户将会优先分配到自己绑定的虚拟 IP。

对于没有所属组的用户或所属组没有绑定网络扩展虚拟 IP 地址池时，用户的虚拟 IP 从虚拟网关网络扩展业务中配置的地址池中分配 IP 地址。

当用户组绑定网络扩展虚拟 IP 地址池时，如果该地址池中的 IP 地址被其他用户组外用户所占用，则仍然允许组外用户使用原绑定的地址，不影响在线用户。

将地址池与用户组解绑定时，不影响绑定了固定地址的该组用户及在线用户。

1.5.39 SSL VPN 有哪些常见调试日志

- 终端校验设备证书失败，弹出证书安全警告。

```
[ NETC    INFO    2022-01-04 14:06:36.000399 ][Administrator] [2][SSL
Create][SSLConnect errno: 1, state: error,connectSSL:-1]
```

```
[ NETC   WARN   2022-01-04 14:06:36.000400 ][Administrator] [2][SSL Create
failed][ErrorCode:20][reason:Verify first error,unable to get local  issuer
certificate]
[ NETC   WARN   2022-01-04 14:06:36.000400 ][Administrator] [2]3[xcs SSLFree
begin][reason:connect ssl error connectfd, return number is -1
  pstConInf->psSsl=3792750]
[ CAUTH  WARN   2022-01-04 14:06:36.000514 ][Administrator] [2][CAUTH Auth
SendToGateway failed][reason:netc connect error, code 1]
[ NETC   INFO   2022-01-04 14:06:36.000517 ][Administrator] [2]4[xcs SSLFree
begin][pstConInf->psSsl=0]
[ NETC   WARN   2022-01-04 14:06:36.000517 ][Administrator] [2][Socket close
failed][fd:7404,errorcode is 10035] // 表示证书验证失败
[ CAUTH  WARN   2022-01-04 14:06:36.000518 ][Administrator] [2][Master auth
failed][reason:send auth pack to gateway error]
[ CAUTH  ERROR  2022-01-04 14:06:36.000519 ][Administrator] [2][Auth login process
failed][auth master error]
[ CADM   INFO   2022-01-04 14:06:36.000520 ][Administrator] [2][Normal Msg][biztype
is 3 ,msgtype is 3 ,msgcode is 0x3000b]
```

- 用户登录，因为证书名/密码错误，提示“认证失败”。

```
[ CAUTH  INFO   2022-01-04 13:35:35.000058 ][Administrator] [2][Auth send][auth
package send to gateway successful]
[ CAUTH  INFO   2022-01-04 13:35:35.000058 ][Administrator] [2][Master auth][send
auth message to gateway ok]
[ CAUTH  INFO   2022-01-04 13:35:35.000059 ][Administrator] [2][Auth login
process][auth master ok]
[ CAUTH  INFO   2022-01-04 13:35:35.000059 ][Administrator] [2][Auth receive][auth
type 0]
[ CAUTH  INFO   2022-01-04 13:35:35.000059 ][Administrator] [2]uiModule = 0
iSRejCode= -5 puiCRejCode = 196609 //用户认证失败
[ CAUTH  INFO   2022-01-04 13:35:35.000059 ][Administrator] [2][Auth recv][auth
master failed][reason = 196609]
[ CAUTH  INFO   2022-01-04 13:35:35.000060 ][Administrator] [2][auth master
exit][authType = 0]
[ NETC   INFO   2022-01-04 13:35:35.000060 ][Administrator] [2]4[xcs SSLFree
begin][pstConInf->psSsl=3792750]
[ CADM   INFO   2022-01-04 13:35:35.000060 ][Administrator] [2][Normal Msg][biztype
is 3 ,msgtype is 3 ,msgcode is 0x30001]
```

- 用户登录，因为用户账号被锁定，提示“认证失败”。

```
[ CAUTH  INFO   2022-01-04 14:14:48.000939 ][Administrator] [2][Auth send][auth
package send to gateway successful]
[ CAUTH  INFO   2022-01-04 14:14:48.000940 ][Administrator] [2][Master auth][send
auth message to gateway ok]
[ CAUTH  INFO   2022-01-04 14:14:48.000940 ][Administrator] [2][Auth login
process][auth master ok]
```

```
[ CAUTH  INFO   2022-01-04 14:14:48.000940 ][Administrator] [2][Auth receive][auth
type 0]
[ CAUTH  INFO   2022-01-04 14:14:48.000940 ][Administrator] [2]uiModule = 0
iSRejCode= -16 puiCRejCode = 196609 //表示用户账号被锁定
[ CAUTH  INFO   2022-01-04 14:14:48.000941 ][Administrator] [2][Auth recv][auth
master failed][reason = 196609]
[ CAUTH  INFO   2022-01-04 14:14:48.000941 ][Administrator] [2][auth master
exit][authType = 0]
[ NETC   INFO   2022-01-04 14:14:48.000941 ][Administrator] [2]4[xcs SSLFree
begin][pstConInf->psSsl=37668b0]
[ CADM   INFO   2022-01-04 14:14:48.000941 ][Administrator] [2][Normal Msg][biztype
is 3 ,msgtype is 3 ,msgcode is 0x30001]
```

- 用户登陆，因为用户没有网络扩展权限，提示“认证失败”

```
[ CAUTH  INFO   2022-01-04 14:14:48.000939 ][Administrator] [2][Auth send][auth
package send to gateway successful]
[ CAUTH  INFO   2022-01-04 14:14:48.000940 ][Administrator] [2][Master auth][send
auth message to gateway ok]
[ CAUTH  INFO   2022-01-04 14:14:48.000940 ][Administrator] [2][Auth login
process][auth master ok]
[ CAUTH  INFO   2022-01-04 14:14:48.000940 ][Administrator] [2][Auth receive][auth
type 0]
[ CAUTH  INFO   2022-01-04 14:14:48.000940 ][Administrator] [2]uiModule = 0
iSRejCode= -16 puiCRejCode = 196609 //表示用户账号被锁定
[ CAUTH  INFO   2022-01-04 14:14:48.000941 ][Administrator] [2][Auth recv][auth
master failed][reason = 196609]
[ CAUTH  INFO   2022-01-04 14:14:48.000941 ][Administrator] [2][auth master
exit][authType = 0]
[ NETC   INFO   2022-01-04 14:14:48.000941 ][Administrator] [2]4[xcs SSLFree
begin][pstConInf->psSsl=37668b0]
[ CADM   INFO   2022-01-04 14:14:48.000941 ][Administrator] [2][Normal Msg][biztype
is 3 ,msgtype is 3 ,msgcode is 0x30001]
```

- 终端主动退出登录

```
[ CAUTH  INFO   2022-01-04 15:42:13.000259 ][Administrator] [2][Auth send][auth
package send to gateway successful]
[ NETC   INFO   2022-01-04 15:42:13.000468 ][Administrator] [2]4[xcs SSLFree
begin][pstConInf->psSsl=2b17840]
[ CADM   INFO   2022-01-04 15:42:13.000469 ][Administrator] [2][cadm bizctl
process][entry bizctl proc srcbiz 3 and bizctl 40]
[ CADM   INFO   2022-01-04 15:42:13.000470 ][Administrator] [2][cadm bizctl
process][the biz start to exit biztype 5]
[ CADM   INFO   2022-01-04 15:42:13.000471 ][Administrator] [2][cadm bizctl
process][the biztype 5 exit msg is sending. notice_biz 20]
[ CNEM   INFO   2022-01-04 15:42:13.000472 ][Administrator] [8][Cnem module
proc][Enter]
```

```
[ CADM   INFO   2022-01-04 15:42:13.000474 ][Administrator] [2][cadm bizctl
process][the biz start to exit biztype 8]
[ CNEM   INFO   2022-01-04 15:42:13.000474 ][Administrator] [8][Cnem module
proc][Cnem module stop]
[ CADM   INFO   2022-01-04 15:42:13.000476 ][Administrator] [2][cadm bizctl
process][the biztype 8 exit msg is sending. notice_biz 120]
[ CEPS   INFO   2022-01-04 15:42:13.000476 ][Administrator] [7][hostcheck pro][ceps
module stop start]
[ NETC   INFO   2022-01-04 15:42:13.000478 ][Administrator] [8]4[xcs SSLFree
begin][pstConInf->psSsl=2b010b0]
[ CADM   INFO   2022-01-04 15:42:13.000480 ][Administrator] [2][cadm bizctl
process][the notice has been send to src biz 3--EXIT WAIT]//表示用户主动退出
[ NETC   WARN   2022-01-04 15:42:13.000481 ][Administrator] [8][Socket close
failed][fd:2324,errorcode is 10035]
[ ROUTE  INFO   2022-01-04 15:42:13.000483 ][Administrator] [8][Route
Recovery][start]
[ ROUTE  INFO   2022-01-04 15:42:13.000495 ][Administrator] [8][Route
Recovery][Finish]
```

- 设备侧踢用户下线

```
[ CNEM   WARN   2022-01-04 15:47:32.000364 ][Administrator] [3][Cnem handle packet
from gateway][CMDtype is KICKOUT]//表示收到设备侧踢用户下线的请求
[ CNEM   ERROR  2022-01-04 15:47:32.000366 ][Administrator] [3][Cnem handle packet
from gateway][NEM_CMD_KICKOUT]
[ CNEM   INFO   2022-01-04 15:47:32.000367 ][Administrator] [3][Cnem send status msg
to self ok]
[ CNEM   INFO   2022-01-04 15:47:32.000368 ][Administrator] [8][Cnem module
proc][Enter]
[ CNEM   INFO   2022-01-04 15:47:32.000370 ][Administrator] [8][Cnem AsyncMsg BizNem
Proc][Enter]
[ CNEM   INFO   2022-01-04 15:47:32.000371 ][Administrator] [8][Cnem run][Enter]
[ CNEM   INFO   2022-01-04 15:47:32.000387 ][Administrator] [8][Cnem run][the
current status 145 and msgtype 13]
[ CNEM   ERROR  2022-01-04 15:47:32.000388 ][Administrator] [8][Cnem receive or send
packet failed][goto ERR Handle]
[ NETC   INFO   2022-01-04 15:47:32.000390 ][Administrator] [8]4[xcs SSLFree
begin][pstConInf->psSsl=2b010b0]
[ ROUTE  INFO   2022-01-04 15:47:32.000391 ][Administrator] [8][Route
Recovery][start]
[ ROUTE  INFO   2022-01-04 15:47:32.000404 ][Administrator] [8][Route
Recovery][Finish]
```

- 保活超时，重连失败，退出登录

```
[ CNEM   ERROR  2022-01-04 16:01:48.000444 ][Administrator] [8][Cnem err handle][nem module reconnect fail]
[ CADM   INFO   2022-01-04 16:01:48.000444 ][Administrator] [2][Emergency Msg][biztype:5 msgtype:11 msgcode:0xb0002]
[ CEPS   INFO   2022-01-04 16:01:48.000493 ][Administrator] [7][eps proc][CEPS HostCheck Proc start type 10]
[ CEPS   INFO   2022-01-04 16:01:49.000713 ][Administrator] [7][cacheclean logout][eps start logout cache clean check end]
[ CADM   INFO   2022-01-04 16:01:49.000714 ][Administrator] [2][Normal Msg][biztype is 8 ,msgtype is 5 ,msgcode is 0x50002]
[ CADM   INFO   2022-01-04 16:01:49.000714 ][Administrator] [5][CSDK_Send_Thread][uiMsgSourceMark:0x4000000 -> uiMsgDestMark:0x2000000][uiModuleID:0x8000000][uiMsgType:0x2000500][uiConnetType:0x1000000][uiMsgLength:0x0]
[ CAUTH  INFO   2022-01-04 16:01:49.000718 ][Administrator] [2][CAUTH Module Proc][in to CAUTH Module Proc]
[ CAUTH  WARN   2022-01-04 16:01:49.000719 ][Administrator] [2][Service cert failed][pstCAuthCtx->uiServiceCertCheck =0]
[ CADM   INFO   2022-01-04 16:01:49.000720 ][Administrator] [2][CAUTH Auth SendToGateway][no need to set certinfo]
[ CADM   INFO   2022-01-04 16:01:49.000721 ][Administrator] [2][CAUTH Auth SendToGateway][proxy info :0, user name:, proxy type:0]
[ NETC   WARN   2022-01-04 16:01:54.000722 ][Administrator] [2][SSL Connect failed][reason:ssl time out, reconnect]
[ NETC   WARN   2022-01-04 16:01:59.000723 ][Administrator] [2][SSL Connect failed][reason:ssl time out, reconnect]
[ NETC   WARN   2022-01-04 16:02:04.000724 ][Administrator] [2][SSL Connect failed][reason:ssl time out, reconnect] //表示重连超时
[ NETC   ERROR  2022-01-04 16:02:04.000725 ][Administrator] [2][SSL Connect failed][reason:reach max reconnect time Addr: 10.19.12.120,Port: 5678]  //达到重连次数上限
```

- 用户登陆 SSL VPN 成功，完整的日志。

```
[ CADM   INFO   2022-01-06 13:36:53.000070 ][Administrator] [4][Proxy info][ConnectType is <1>,Proxy type is <0>]//1 表示 SSL VPN，0 表示无代理
[ CADM   INFO   2022-01-06 13:36:53.000071 ][Administrator] [4][Proxy info][proxy is :0, user name is , proxy type is 0]
[ PREF   INFO   2022-01-06 13:36:53.000072 ][Administrator] [2][SetPrefSiteFlag]
[ PREF   INFO   2022-01-06 13:36:53.000073 ][Administrator] [2][Site pref proc][Enter]
[ PREF   INFO   2022-01-06 13:36:53.000074 ][Administrator] [2][Site Pref Preprocess SiteInfo][aucGatewayIP:10.19.12.120][uiGatewayPort:6528]
[ PREF   INFO   2022-01-06 13:36:53.000075 ][Administrator] [2]Number of sites 1
[ PREF   INFO   2022-01-06 13:36:53.000077 ][Administrator] [2][Default getway Index in configuration file is 0]
```

```
[ PREF   INFO   2022-01-06 13:36:53.000078 ][Administrator] [2][Default getway Index
is 0]
[ PREF   INFO   2022-01-06 13:36:53.000096 ][Administrator] [39][Site pref thread
enter][Site order is 0]
[ PREF   INFO   2022-01-06 13:36:53.000097 ][Administrator] [39][Park
RequestPack][pstFirstConnRequest->ucDomain][10.19.12.120]
[ PREF   INFO   2022-01-06 13:36:53.000098 ][Administrator]
[39][SITE_FirstConn_RequestPack over]
[ CAUTH  INFO   2022-01-06 13:36:53.000099 ][Administrator]
[ CAUTH  INFO   2022-01-06 13:36:53.000099 ][Administrator] [39][cauth][get the
gateway ip is 10.19.12.120 and port is 6528 from domain name]
[ CAUTH  INFO   2022-01-06 13:36:53.000099 ][Administrator] [39][Addr info][ip
address is valid]
[ CAUTH  INFO   2022-01-06 13:36:53.000099 ][Administrator] [39][cauth][get the
gateway ip is 10.19.12.120 and port is 6528 from domain name]
[ CAUTH  INFO   2022-01-06 13:36:53.000100 ][Administrator]
[ CAUTH  INFO   2022-01-06 13:36:53.000100 ][Administrator] [39][cauth][get the
gateway ip is 10.19.12.120 and port is 6528 from domain name]
[ CAUTH  INFO   2022-01-06 13:36:53.000100 ][Administrator] [39][Addr info][ip
address is valid]
[ PREF   INFO   2022-01-06 13:36:53.000100 ][Administrator] [39][SITE FirstConn
SendAndRecv][aucDomainName:10.19.12.120:6528]
[ PREF   INFO   2022-01-06 13:36:53.000100 ][Administrator] [39][SITE FirstConn
SendAndRecv][aucDstDomain:10.19.12.120:6528]
[ PREF   INFO   2022-01-06 13:36:53.000101 ][Administrator] [39][SITE FirstConn
SendAndRecv][!!!!!!!!!!]
[ PREF   INFO   2022-01-06 13:36:53.000101 ][Administrator] [39][SITE FirstConn
SendAndRecv][conn->aucHostName:10.19.12.120]
[ PREF   INFO   2022-01-06 13:36:53.000101 ][Administrator]
[39][NETC_Socket_Connect] Begin!
[ NETC   INFO   2022-01-06 13:36:53.000102 ][Administrator] [39][SSL
Create][Success]// SSL 握手成功
[ NETC   INFO   2022-01-06 13:36:54.000704 ][Administrator] [2][NETC SSL
Create][connect][connectSSL == -1]
[ NETC   WARN   2022-01-06 13:36:54.000705 ][Administrator] [2][SSL
Create][SSL_ERROR_WANT_READ continue][retry 19999]
[ NETC   INFO   2022-01-06 13:36:54.000706 ][Administrator] [2][SSL
Create][SSLConnect errno: 1, state: error,connectSSL:-1]
[ NETC   WARN   2022-01-06 13:36:54.000706 ][Administrator] [2][SSL Create
failed][ErrorCode:19][reason:Verify first error,self signed certificate in
certificate chain]
[ NETC   WARN   2022-01-06 13:36:54.000706 ][Administrator] [2]3[xcs SSLFree
begin][reason:connect ssl error connectfd, return number is -1
pstConInf->psSsl=2b5b3e0]
[ CAUTH  WARN   2022-01-06 13:36:54.000706 ][Administrator] [2][CAUTH Auth
SendToGateway failed][reason:netc connect error, code 3]
```

```
[ NETC   INFO   2022-01-06 13:36:54.000706 ][Administrator] [2]4[xcs SSLFree
begin][pstConInf->psSsl=0]
[ NETC   WARN   2022-01-06 13:36:54.000707 ][Administrator] [2][Socket close
failed][fd:3668,errorcode is 10035]//证书校验失败，弹出证书安全警告

[ CADM   INFO   2022-01-06 13:36:54.000707 ][Administrator] [2][Normal Msg][biztype
is 3 ,msgtype is 3 ,msgcode is 0x3000b]
[ CADM   INFO   2022-01-06 13:36:54.000708 ][Administrator]
[5][CSDK_Send_Thread][uiMsgSourceMark:0x4000000 ->
uiMsgDestMark:0x2000000][uiModuleID:0x3000000][uiMsgType:0xB000300][uiConnetType:
0x1000000][uiMsgLength:0x0]
[ CADM   INFO   2022-01-06 13:37:15.000450 ][Administrator] [4][Proxy
info][ConnectType is <1>,Proxy type is <0>]
[ CADM   INFO   2022-01-06 13:37:15.000450 ][Administrator] [4][Proxy info][proxy
is :0, user name is , proxy type is 0]
[ PREF   INFO   2022-01-06 13:37:15.000450 ][Administrator] [2][Link pref
proc][Enter]
[ PREF   INFO   2022-01-06 13:37:15.000451 ][Administrator] [2][Link backup not
open][Return choice site] //没有开启链路备份

[ CAUTH  INFO   2022-01-06 13:37:15.000551 ][Administrator] [2][Auth send][auth
package send to gateway successful]
[ CAUTH  INFO   2022-01-06 13:37:15.000551 ][Administrator] [2][Master auth][send
auth message to gateway ok]
[ CAUTH  INFO   2022-01-06 13:37:15.000551 ][Administrator] [2][Auth login
process][auth master ok]//主认证成功
[ CAUTH  INFO   2022-01-06 13:37:15.000552 ][Administrator] [2][Auth receive][auth
type 0]
[ CAUTH  INFO   2022-01-06 13:37:15.000552 ][Administrator] [2][auth master
exit][authType = 0]
[ NETC   INFO   2022-01-06 13:37:15.000552 ][Administrator] [2]4[xcs SSLFree
begin][pstConInf->psSsl=2b5b3e0]
[ CADM   INFO   2022-01-06 13:37:15.000553 ][Administrator] [2][Normal Msg][biztype
is 3 ,msgtype is 2 ,msgcode is 0x20000]
[ CADM   INFO   2022-01-06 13:37:15.000553 ][Administrator]
[5][CSDK_Send_Thread][uiMsgSourceMark:0x4000000 ->
uiMsgDestMark:0x2000000][uiModuleID:0x3000000][uiMsgType:0x200][uiConnetType:0x10
00000][uiMsgLength:0x0]
[ CADM   INFO   2022-01-06 13:37:15.000554 ][Administrator] [4][SSL Start Nem][in to
SSL_StartNem]//启用网络扩展服务
[ VNIC   INFO   2022-01-06 13:37:15.000556 ][Administrator] [8][Start VNIC][begin]
//启用虚拟网卡
[ VNIC   INFO   2022-01-06 13:37:15.000557 ][Administrator] [8][Find the
VNIC][success]
[ VNIC   INFO   2022-01-06 13:37:15.000564 ][Administrator] [8][Nic Open][begin]
[ VNIC   INFO   2022-01-06 13:37:15.000570 ][Administrator] [8][Get VNIC name][name:
本地连接]
```

```
[ VNIC   INFO   2022-01-06 13:37:15.000571 ][Administrator] [8][VNIC Start][open cmd
is interface set interface "本地连接" admin=ENABLED]
[ CNEM   INFO   2022-01-06 13:37:15.000603 ][Administrator] [8][Cnem send status msg
to self ok]
[ CNEM   INFO   2022-01-06 13:37:15.000604 ][Administrator] [8][Cnem Start OK]//
网络扩展启用完成
[ NETC   INFO   2022-01-06 13:37:15.000608 ][Administrator] [8][NETC SSL
Create][pstConInf->aucHostName][10.19.12.120]
[ NETC   INFO   2022-01-06 13:37:15.000608 ][Administrator] [8][NETC SSL
Create][g_gatewayDomain][10.19.12.120]
[ PREF   INFO   2022-01-06 13:37:15.000608 ][Administrator] [8][GetPrefSiteFlag:0]
[ CAUTH  INFO   2022-01-06 13:37:15.000608 ][Administrator]
[8][CAUTH_CheckIsDomain][pucDomain is 10.19.12.120]
[ CAUTH  INFO   2022-01-06 13:37:15.000609 ][Administrator]
[8][CAUTH_CheckIsDomain][pucDomain is IP]
[ NETC   INFO   2022-01-06 13:37:15.000609 ][Administrator] [8][NETC SSL
Create][connect]
[ NETC   INFO   2022-01-06 13:37:15.000619 ][Administrator] [8][NETC SSL
Create][connect][connectSSL == 1]
[ NETC   INFO   2022-01-06 13:37:15.000619 ][Administrator] [8][SSL Create][Success]
//网络扩展建立到网关的 SSL 连接成功
[ CNEM   INFO   2022-01-06 13:37:15.000620 ][Administrator] [8][Cnem SSL create
ok][3656]
[ CNEM   INFO   2022-01-06 13:37:15.000620 ][Administrator] [8][Cnem SSL
create ][reason:channel bind success][sslChannelId<3656>]
[ CNEM   INFO   2022-01-06 13:37:15.000620 ][Administrator] [8][Cnem send status msg
to self ok]
[ CNEM   INFO   2022-01-06 13:37:15.000621 ][Administrator] [8][Cnem module
proc][Enter]
[ CNEM   INFO   2022-01-06 13:37:15.000621 ][Administrator] [8][Cnem AsyncMsg BizNem
Proc][Enter]
[ CNEM   INFO   2022-01-06 13:37:15.000621 ][Administrator] [8][Cnem run][Enter]
[ CNEM   INFO   2022-01-06 13:37:15.000621 ][Administrator] [8][Cnem run][the
current status 20 and msgtype 1]
[ CNEM   INFO   2022-01-06 13:37:15.000621 ][Administrator] [8][Cnem send acl
request to gateway ok]//发送 ACL 请求去网关（和 SVN 设备交互时使用）
[ CNEM   INFO   2022-01-06 13:37:15.000622 ][Administrator] [3][Cnem send status msg
to self ok]

[ CNEM   INFO   2022-01-06 13:37:15.000626 ][Administrator] [8][Cnem send vip
request to gateway ok] //发送 VIP 请求去 VPN 网关
[ CNEM   INFO   2022-01-06 13:37:15.000628 ][Administrator] [3][Cnem handle packet
from gateway][CMDtype is REQVIP]
[ CNEM   INFO   2022-01-06 13:37:15.000628 ][Administrator] [3][Cnem parse new
netcfginfo][Enter]
[ CNEM   INFO   2022-01-06 13:37:15.000628 ][Administrator] [3][Cnem parse new
netcfginfo][DNS Server IP Nums is 1]//从设备侧获得 1 个 DNS 服务器地址
```

```
[ CNEM   INFO   2022-01-06 13:37:15.000628 ][Administrator] [3][Cnem parse vip info
from gateway ok] //从设备侧获得 VIP 信息
[ VNIC   INFO   2022-01-06 13:37:15.000632 ][Administrator] [8][Get VNIC
iofd][handle is 2648]
[ VNIC   INFO   2022-01-06 13:37:15.000632 ][Administrator] [8][Get VNIC
Handle][success]
[ VNIC   INFO   2022-01-06 13:37:15.000632 ][Administrator] [8][Active VNIC][begin]
[ VNIC   INFO   2022-01-06 13:37:15.000632 ][Administrator] [8][Active
VNIC][success]
[ VNIC   INFO   2022-01-06 13:37:15.000633 ][Administrator] [8][Set IP and
MASK][begin]
[ VNIC   INFO   2022-01-06 13:37:15.000633 ][Administrator] [8][VNIC IP is
10.19.15.36]//虚拟 IP 地址信息
[ VNIC   INFO   2022-01-06 13:37:15.000633 ][Administrator] [8][VNIC mask is
255.255.255.0]//虚拟 IP 地址掩码信息
[ VNIC   INFO   2022-01-06 13:37:15.000675 ][Administrator] [8][Set IP and
MASK][success]//设置虚拟网卡 IP 地址信息
[ VNIC   INFO   2022-01-06 13:37:15.000676 ][Administrator] [8][Set DNS Server
IP][begin]
[ VNIC   INFO   2022-01-06 13:37:15.000745 ][Administrator] [8][VNIC Init][set DNS
success]//设置虚拟网卡 DNS 信息
[ ROUTE  INFO   2022-01-06 13:37:19.000059 ][Administrator] [41][Route
set][Begin]:[70]
[ ROUTE  INFO   2022-01-06 13:37:19.000059 ][Administrator] [41][Route set][Before
set route print the routetable:]//注入 VPN 路由之前打印路由表
[ ROUTE  INFO   2022-01-06 13:37:19.000060 ][Administrator] [41][Route print
begin==============================================================================
========
[ ROUTE  INFO   2022-01-06 13:37:19.000068 ][Administrator] [41][Get best route
info][Ip :10.19.28.254 Mask :0x00000000 Nic index :10]
[ ROUTE  INFO   2022-01-06 13:37:19.000068 ][Administrator] [41][gateWay
info][Ip :10.19.12.120 ]
[ ROUTE  INFO   2022-01-06 13:37:19.000069 ][Administrator] [41][BroadCast Route
Judge ok][DestIP : 0xff0f130a]
[ ROUTE  INFO   2022-01-06 13:37:19.000069 ][Administrator] [41][Cleanup VNIC
related route][Success]//先清除旧的虚拟网卡路由
[ ROUTE  INFO   2022-01-06 13:37:19.000084 ][Administrator] [41][manul inner route
info][Dest:0x2e0c130a  Mask:0xffffffff  NextHop:0x240f130a  IfIndex:13]
[ ROUTE  ERROR  2022-01-06 13:37:19.000096 ][Administrator] [41][Delete route
Failed][ErrorCode:0]
[ ROUTE  ERROR  2022-01-06 13:37:19.000097 ][Administrator] [41][Delete Unsafe Route
Failed][Line :787]
[ ROUTE  INFO   2022-01-06 13:37:19.000097 ][Administrator] [41][BroadCast Route
Judge ok][DestIP : 0xff0f130a]
[ ROUTE  INFO   2022-01-06 13:37:19.000097 ][Administrator] [41][BroadCast Route
Judge ok][DestIP : 0xff1c130a]
```

```
[ ROUTE  INFO   2022-01-06 13:37:19.000097 ][Administrator] [41][BroadCast Route
Judge ok][DestIP : 0xff3f1fac]
[ ROUTE  INFO   2022-01-06 13:37:19.000110 ][Administrator] [41][Set manual mode
route][Success]
[ ROUTE  INFO   2022-01-06 13:37:19.000110 ][Administrator] [41][After set
route][Routetable:]//注入 VPN 路由后打印路由表
[ ROUTE  INFO   2022-01-06 13:37:19.000110 ][Administrator] [41][Route print
begin==========================================================================
========
```

- 缺省情况下，UniVPN 只记录 INFO、WARN、ERROR 三个基本日志，如果要记录 DEBUG 级别的日志，　　需要修改 UniVPN 配置文件“sysconfig.ini”

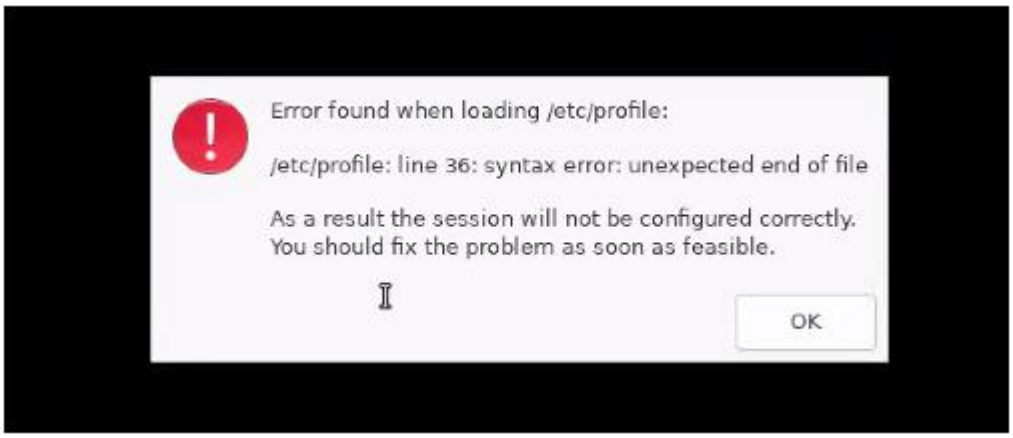
```
[GLOBAL]
ClientName = SecoClient
ClientVersion = 7.0.9.1
ClientCustomized = false
ClientLogLevel = 1      //修改为 0，DEBUG 级别日志也会记录
```

1.5.40 UniVPN 和 SecoClient 是否能同时使用

不能，如果 PC 存在 SecoClient，安装 UniVPN 时会检测并卸载 SecoClient。如果卸载 SecoClient 失败请手动卸载 SecoClient，避免 UniVPN 客户端出现问题。

1.5.41 打开 UniVPN 前 PC 主机报错

1、本地化的 linux 系统如果开机启动出现如下弹窗，会导致 VPN 服务无法自启，需要联系管理员恢复配置文件(/etc/profile)



2、当 VPN 连接成功后，如果出现意外退出程序进程的情况（覆盖安装、电脑断电等），可能导致下发的路由没有被删除。当出现这种情况时可以联系管理员。

1.5.42 VPN 服务器可以访问公网，内网用户建立 VPN 连接后是否可以访问公网资源

可以，但是由于系统特性差异，内网部分用户在使用 UniVPN 客户端建立 VPN 连接后，可能会出现无法通过 VPN 访问公网的现象。

解决方案：内网用户拨号获取地址后需要经过防火墙访问公网，需要对获取到的私网地址做 NAT 转换。

1.5.43 MacOS 系统用户使用 UniVPN 建立 VPN 连接后无法访问公网域名，如何解决

实际使用过程中，Mac OS 系统和 Windows 系统在 DNS 解析方面存在差异。若 Mac OS 用户出现建立 VPN 连接前可访问公网资源，建立 VPN 连接后无法访问公网域名的现象，可手动配置一条不同的公网 dns 服务器。

1.5.44 使用客户端是否要放开某些端口

是的，客户端会绑定特定端口，请允许以下端口通信。
Windows 平台:
promote service 监听端口 29190 如果失败，端口递增绑定
CSDK 监听端口 19060
UI 监听端口 29192
linux 和 MacOS 平台:
promote service 监听端口 29191
监听端口 19060
UI 监听端口 29192

1.6 UniVPN 拨号 SSL VPN 故障-V600R21C10

本章节介绍 UniVPN 客户端在接入防火墙设备 V600R21C10 及以后版本时拨号 SSL VPN 的故障处理方式。

1.6.1 打开 UniVPN 时出现警告

警告：已经有客户端正在运行，不能再运行该程序！
警告：无法建立 VPN 连接，VPN 服务器可能无法到达
警告：无效的 IP 或域名！

1.6.1.1 警告：已经有客户端正在运行，不能再运行该程序！

现象描述

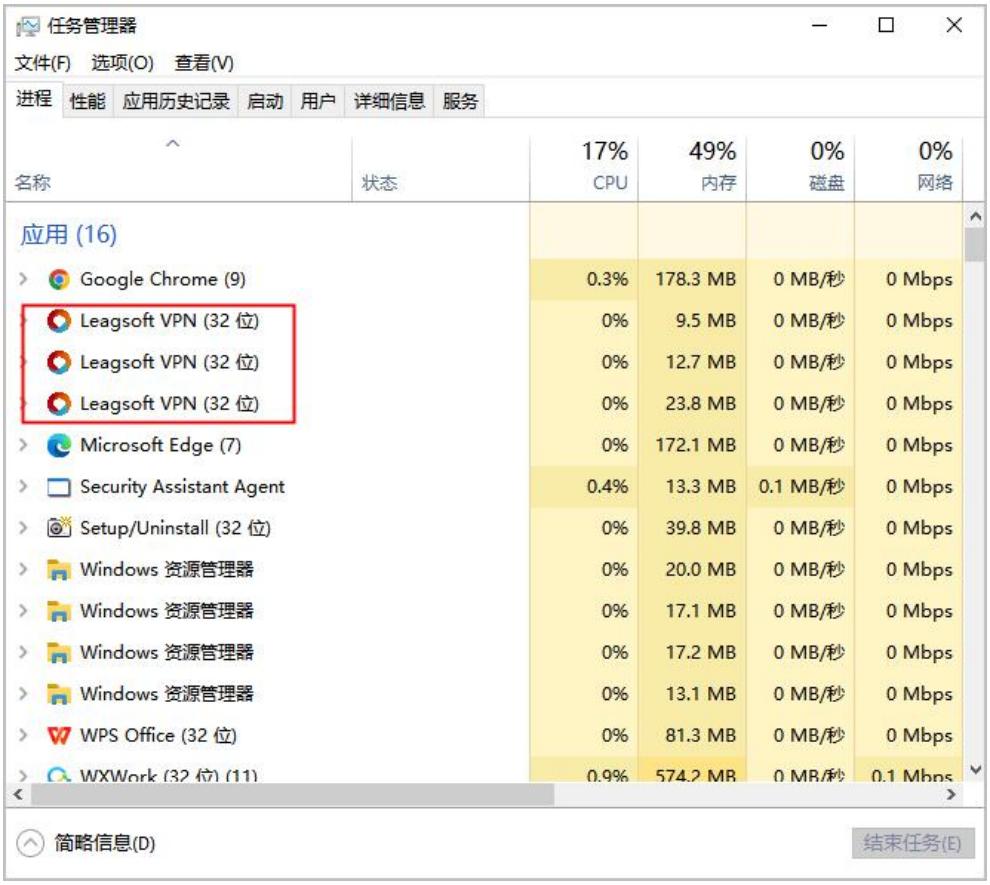
打开 UniVPN 时，系统告警“已经有客户端正在运行，不能再运行该程序！”。

可能原因

终端上已经有 UniVPN 在运行。

处理步骤

关闭已有的 UniVPN 运行程序，并检查任务管理器中的 Security Assisant Agent.exe 进程是否同步关闭。



1.6.1.2 警告：无法建立 VPN 连接，VPN 服务器可能无法到达

现象描述

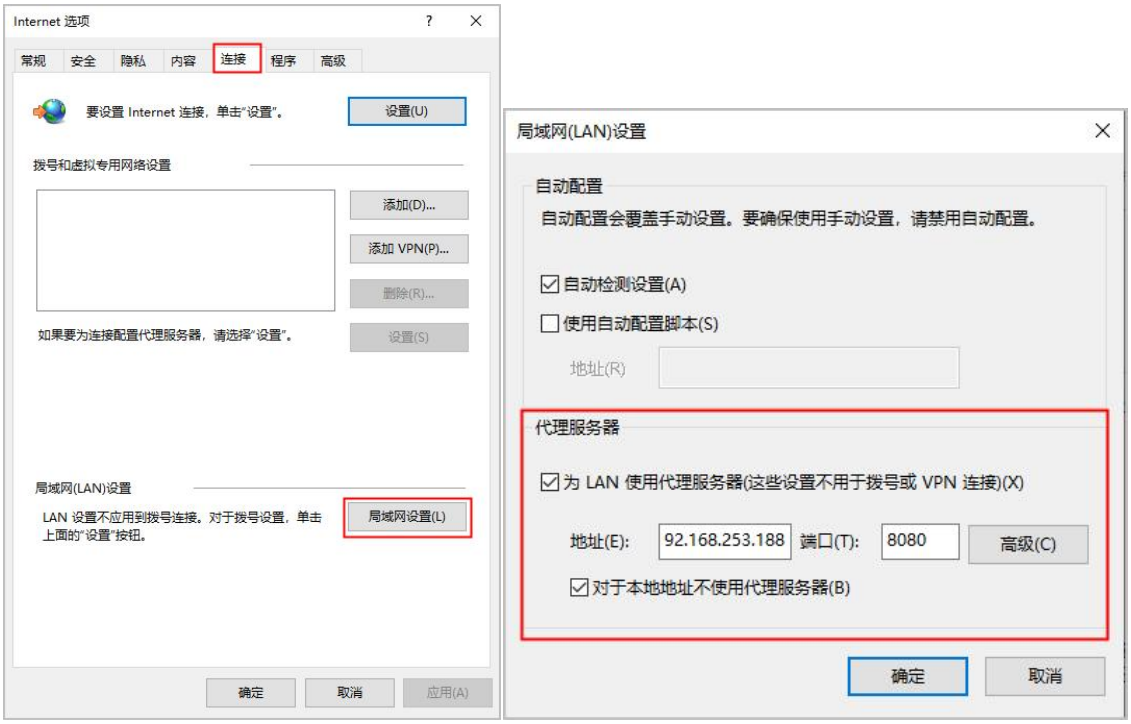
连接 VPN 网关时，系统告警“无法建立 VPN 连接，VPN 服务器可能无法到达”。

可能原因

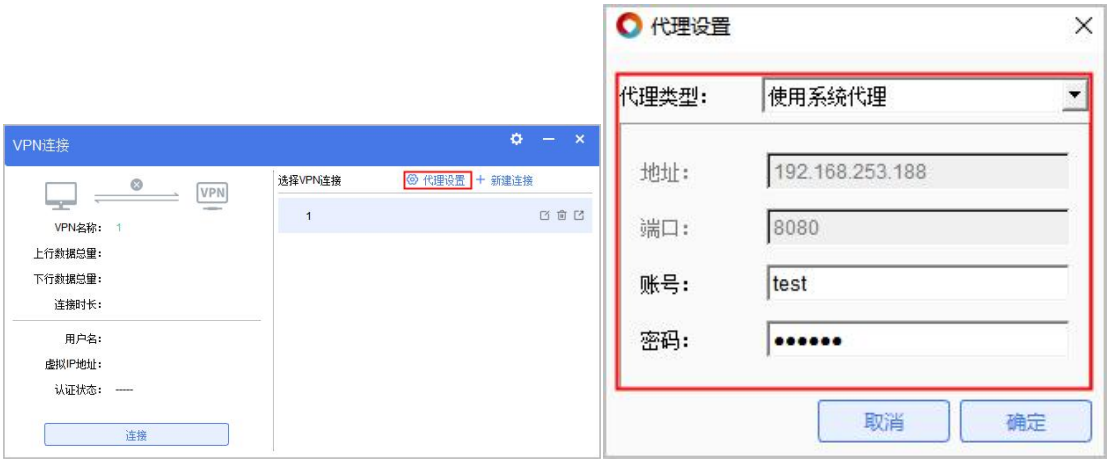
5. UniVPN 到 VPN 网关的路由不可达。
6. UniVPN 上 VPN 网关的 IP 地址或端口填写错误。
7. UniVPN 和 VPN 网关版本不配套。
8. 终端通过代理服务器上网的场景（如 192.168.253.188），UniVPN 未设置代理拨号公网的 VPN 网关。

处理步骤

- 原因 1 的问题定位及解决方法。
  3. 在 UniVPN 所在的终端上 Ping VPN 网关的 IP 地址，检查路由是否可达。
  4. 如果路由不可达，请配置 UniVPN 到 VPN 网关的路由。如果路由可达，表明该问题不是路由原因造成的，请转入分析下一种原因。
- 原因 2 的问题定位及解决方法。
  请检查 UniVPN 上配置的 VPN 网关 IP 地址、端口是否与 VPN 网关侧配置的一致。
- 原因 3 的问题定位及解决方法。
  目前和 UniVPN 配套的 VPN 网关软件版本有 FW V500R005C20SPC500、FW V600R007C20SPC300（SPC301/SPC 302 版本除外）、 V600R021C10，及其它们之后的版本。它们之前的版本，和 UniVPN 并不配套。
- 原因 4 的定位及解决办法。
  检查终端是否通过代理服务器上网。



如果是，UniVPN 也需要配置代理参数，如下图。



1.6.1.3 超过最大限制，最大限制 16 条

现象描述

在 UniVPN 新建连接界面，在远程网关中输入 16 条网关地址以后，单击“添加”，系统告警“超过最大限制，最大限制 16 条”。

可能原因

在客户端新建连接界面中，远程网关已经添加了 16 条，达到了最大可输入网关数。

处理步骤

网关地址达到 16 条后，不再继续添加网关地址。

1.6.1.4 已达到最大数目，无法新建

现象描述

在 UniVPN 主界面，在选择 VPN 连接中添加了 16 个连接配置，单击“+”，系统告警“已达到最大数目，无法新建”。

可能原因

在客户端主界面中，连接配置已经添加了 16 条，达到了最大可添加连接配置数。

处理步骤

连接配置添加 16 条后，不在继续新建

1.6.2 采用用户名/密码方式登录时出现警告

警告：不可信的 VPN 服务器证书！

警告：认证失败！

警告：用户连接数已达到上限，请稍后重试！

警告：网络扩展启动失败！

警告：主机检查失败！

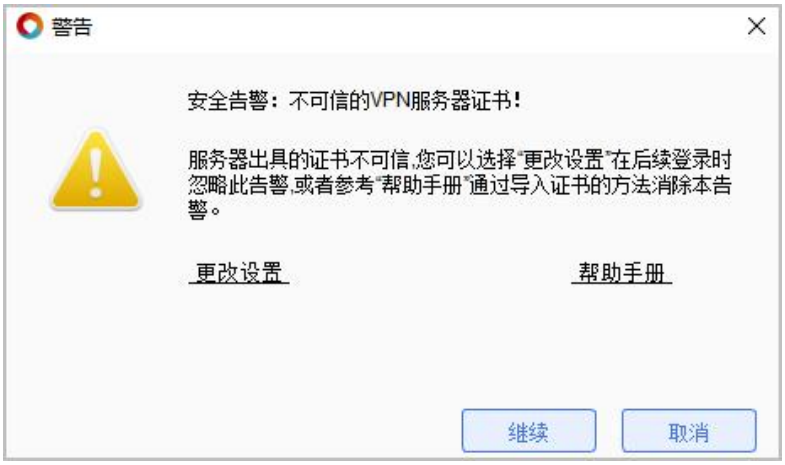
警告：接收返回码超时！

警告：当前连接不支持快速隧道模式，请切换到可靠隧道模式后重试

1.6.2.1 警告：不可信的 VPN 服务器证书！

现象描述

用户使用 UniVPN 通过 SSL VPN 隧道登录 SSL VPN 虚拟网关时，系统弹出如下提示。



可能原因

UniVPN 上缺少认证虚拟网关身份的 CA 证书。

处理步骤

要消除该告警有以下两个方法：

- 单击“设置”，去勾选“VPN 验证服务器可信”。

在用户确定自己登录的虚拟网关身份真实的情况下，可以采用此方法。

- 为 UniVPN 和虚拟网关颁发证书。

用户在无法有效识别虚拟网关身份真实性的情况下，推荐使用此方法。

制作两本证书，一本设备证书放置在虚拟网关上，另一本 CA 证书放置在 UniVPN 所在的主机上。如果用户所在企业已有证书系统，则可以利用自有的系统制作证书。如果没有证书系统，可以使用 XCA 软件制作证书。

UniVPN 通过 SSL VPN 隧道登录虚拟网关时，虚拟网关会向 UniVPN 推送设备证书，只要 UniVPN 上的 CA 证书可以识别虚拟网关的设备证书，系统就不会再提示证书校验非法的告警了。

证书的制作方法请参见如何使用 XCA 制作设备证书和用户证书。

1.6.2.2 认证失败！

现象描述

在 UniVPN 登录界面，输入用户名和密码以后，单击“登录”，系统告警“认证失败！”。

可能原因

1. 用户名或密码错误，用户过期或用户被锁定。
2. 虚拟网关绑定了不正确的认证域。
3. 认证域未启用 SSL VPN 接入场景。
4. 虚拟网关未启动网络扩展特性。
5. SSL VPN 登录的设备处于双机备状态（HRP_S），而 SSL VPN 不支持在备设备上登录上线。
6. 认证域采用 AD/LDAP 服务器认证，服务器上配置用户的属性启用了“首次登录必须修改密码”。
7. 客户端环境通往服务器路由 metric 值（跃点数）超过 1024.

处理步骤

1. 登录设备，检查用户名和密码是否正确，用户是否过期，以及是否处于锁定状态。

```
[HUAWEI-aaa]display local-access-user username user001
2023-04-13 08:58:05.793 +08:00
  The contents of local access user(s):
  Password             : ****************
  State                : block
  Service-type-mask    : V
  Access-limit         : Yes
  Access-limit-max     : 4294967295
  Accessed-num         : 0
  Block-time-left      : 2 Min(s)
  Original-password    : No
  Password-set-time    : 2023-02-23 20:01:17+08:00
  Password-expired     : Yes
  Password-expire-time : 2023-03-15 20:01:17+08:00
```

```
Account-expire-time   : -
Local Access User ID : 17
Service-scheme        : -
UCL group(s)          : -
```

2. 检查虚拟网关是否绑定了认证域，如果有绑定，是否绑定了正确的认证域。

3. 检查用户配置，是否启用了 SSL VPN 接入场景。

4. 检查是否启用了虚拟网关的网络扩展业务。

5. SSL VPN 不支持负载分担组网。调整配置或组网，确保 SSL VPN 登录的设备处于双机主状态（HRP_M）。

6. 登录 AD/LDAP 服务器，查看用户的属性是否启用了“首次登录必须修改密码”，如果启用，选择禁用。

7. 检查通往服务器的路由 metric 值是否大于 1024，如果大于 1024，请修改对应路由的 metric 值。

```
sugon@sugon-os:~/桌面$ route -n
内核 IP 路由表
目标            网关            子网掩码        标志  跃点   引用  使用 接口
0.0.0.0         10.18.11.254    0.0.0.0         UG    13392  0        0 enp1s0
10.18.11.0      0.0.0.0         255.255.255.0   U     100    0        0 enp1s0
10.20.2.96      10.18.11.254    255.255.255.255 UGH   100    0        0 enp1s0
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 enp1s0
sugon@sugon-os:~/桌面$ sudo route del default gw 10.18.11.254
sugon@sugon-os:~/桌面$ sudo route add -net 0.0.0.0 gw 10.18.11.254 netmask 0.0.0.0  metric 0 enp1s0
sugon@sugon-os:~/桌面$ route -n
内核 IP 路由表
目标            网关            子网掩码        标志  跃点   引用  使用 接口
0.0.0.0         10.18.11.254    0.0.0.0         UG    0      0        0 enp1s0
10.18.11.0      0.0.0.0         255.255.255.0   U     100    0        0 enp1s0
10.20.2.96      10.18.11.254    255.255.255.255 UGH   100    0        0 enp1s0
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 enp1s0
sugon@sugon-os:~/桌面$
```

1.6.2.3 用户连接数已达到上限，请稍后重试！

现象描述

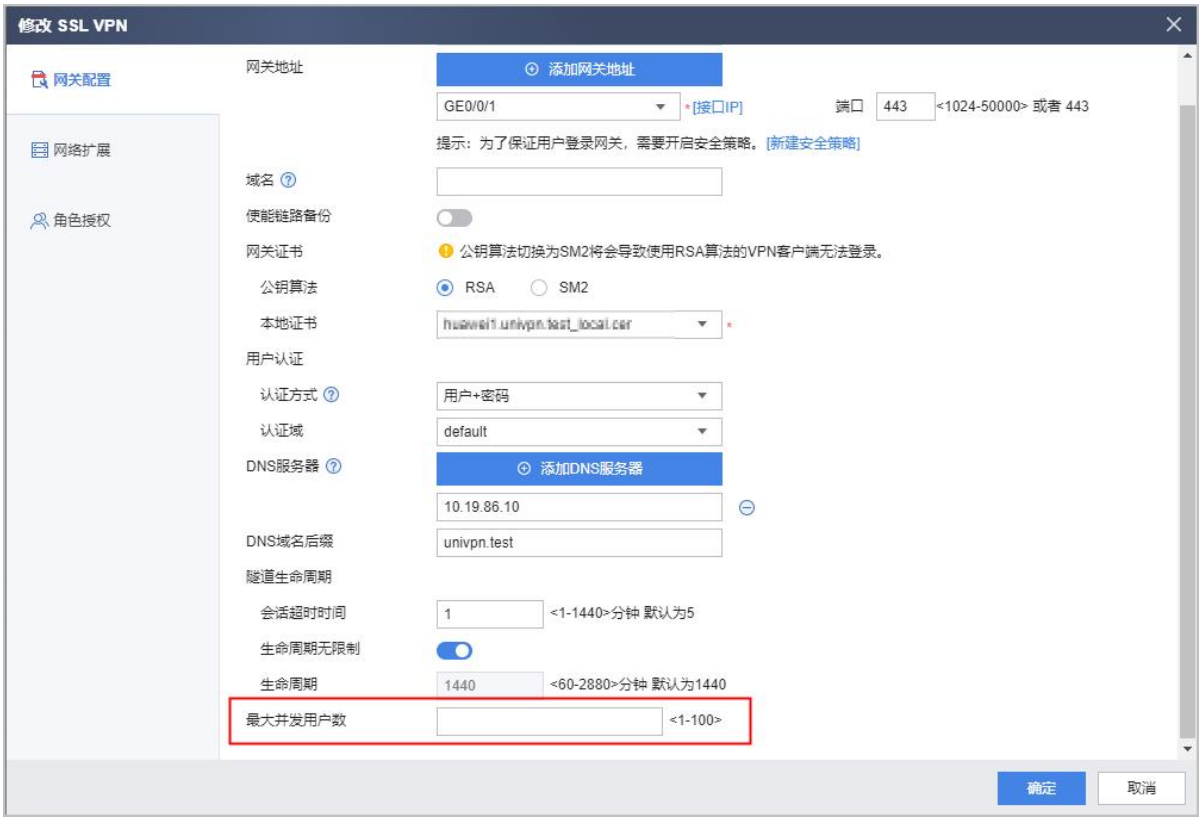
在 UniVPN 登录界面，输入用户名和密码以后，单击“登录”，系统告警“用户连接数已达到上限，请稍后重试！”。

可能原因

1. 当前 SSL VPN 在线用户数已经达到虚拟网关侧配置的最大并发用户数上限。
2. 虚拟网关启用了公共账号功能，且该用户已登录在线的数目已达到上限。

处理步骤

- 原因 1 的问题定位及解决方法。
  登录虚拟网关，选择“网络 > SSL VPN > SSL VPN”，单击对应虚拟网关的名称，检查该虚拟网关最大并发用户数分配情况是否合理，如果不合理，则调整配置。



- 原因 2 的问题定位及解决方法。

  检查该用户的最大在线数目配置，如果是正常的登录请求，可适当增加该用户的最大在线数目。

1.6.2.4 网络拓展启动失败

现象描述

在 UniVPN 登录界面，输入用户名和密码以后，单击“登录”，系统告警“网络扩展启动失败！”。

可能原因

1. 当前虚拟网关网络扩展地址池内 IP 地址已用完。
2. 客户端虚拟网卡异常或客户端无权限操作虚拟网卡。

处理步骤

1. 打开 CLI 控制台，进虚拟网关 service 视图，执行 display network-extension [ip]指令查看网络扩展地址池的配置和分配情况。如果确定地址池已分配完，根据业务需要，适当增加地址池中地址的数目。

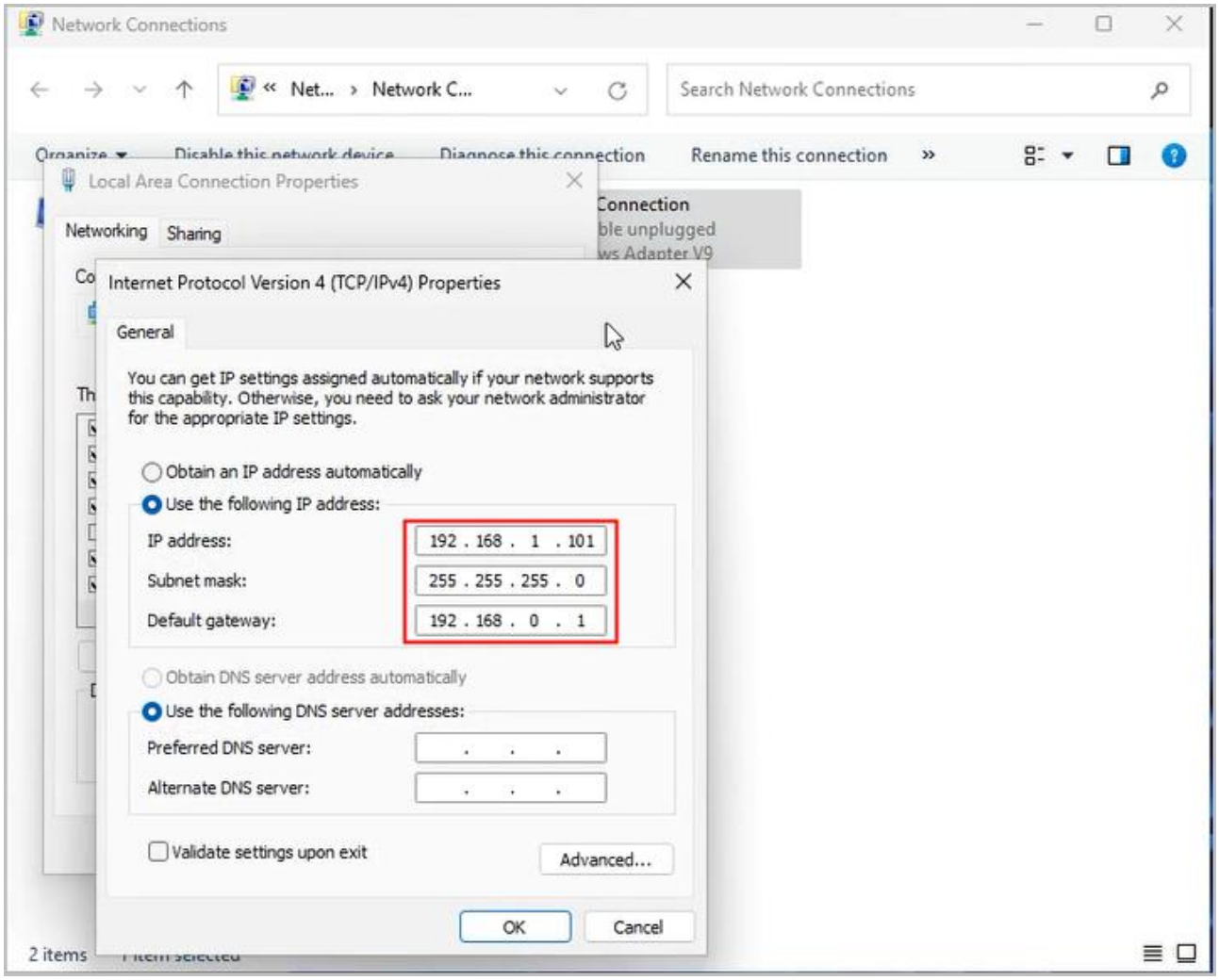
```
<HUAWEI>display ip pool name test
2023-04-21 16:41:26.551 +08:00

 Pool-name        : test
 Pool-No          : 0
```

```
 Lease             : 1 Days 0 Hours 0 Minutes
 Domain-name       : -
 DNS-server0       : -
 NBNS-server0      : -
 Netbios-type      : -
 Position          : Local
 Status            : Unlocked
 Gateway-0         : -
 Network           : -
 Mask              : -
 VPN instance      : --
 Logging           : Disable
 Conflicted address recycle interval: -
 Address Statistic: Total       :100       Used        :0
                    Idle        :100       Expired     :0
                    Conflict    :0         Disabled    :0

-----------------------------------------------------------------------------
 Section ID: 0
        Start           End       Total    Used Idle(Expired) Conflict Disabled
-----------------------------------------------------------------------------
      100.1.1.1     100.1.1.100     100       0        100(0)       0      0
-----------------------------------------------------------------------------
<HUAWEI>
```

2. 查看系统网络适配器是否正确安装虚拟网卡，若虚拟网卡异常请尝试卸载后重新安装；

测试当前用户下是否可以正常操作虚拟网卡，依次执行以下禁用、启用和设置 ip 三条命令查看虚拟网卡是否可以正确设置。若无法正确设置，请查询是否存在策略禁止客户端操作虚拟网卡。

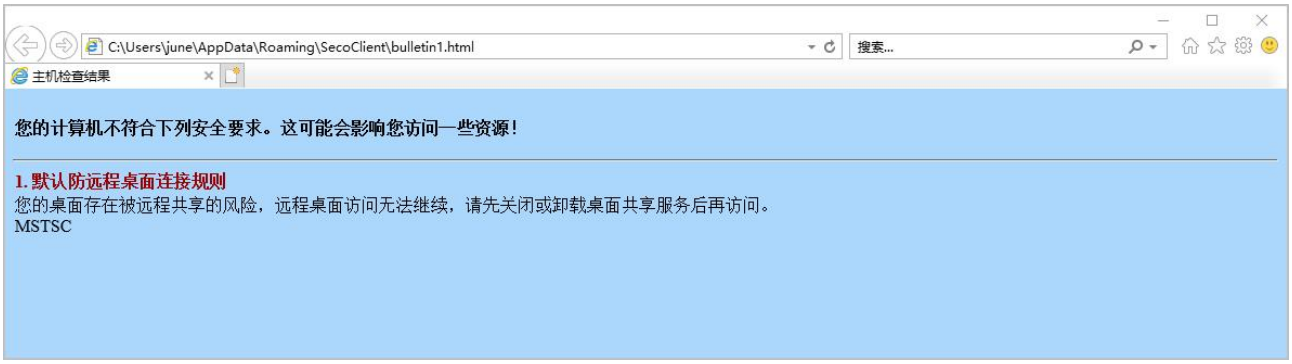
```
C:\Windows\System32>netsh.exe interface set interface "Local Area Connection" admin=DISABLED

C:\Windows\System32>netsh.exe interface set interface "Local Area Connection" admin=ENABLED

C:\Windows\System32>netsh interface ip set address "Local Area Connection" static 192.168.1.101 255.255.255.0
 192.168.0.1 1

C:\Windows\System32>
```



1.6.2.5 主机检查失败！

现象描述

在 UniVPN 登录界面，输入用户名和密码以后，单击“登录”，系统告警“主机检查失败！”。



可能原因

虚拟网关启用了主机检查功能，且终端不符合安全接入的要求。

处理步骤

根据主机检查失败弹出的页面提示排除故障。

1.6.2.6 接受返回码超时！

现象描述

在 UniVPN 登录界面，输入用户名和密码以后，单击“登录”，系统告警“接收返回码超时！”。

可能原因

通信时间是 40s，超过通信时间重启客户端导致系统接收超时

处理步骤

退出 UniVPN，然后重新打开 UniVPN。

1.6.2.7 当前连接不支持快速隧道模式，请切换到可靠隧道模式后重试

现象描述

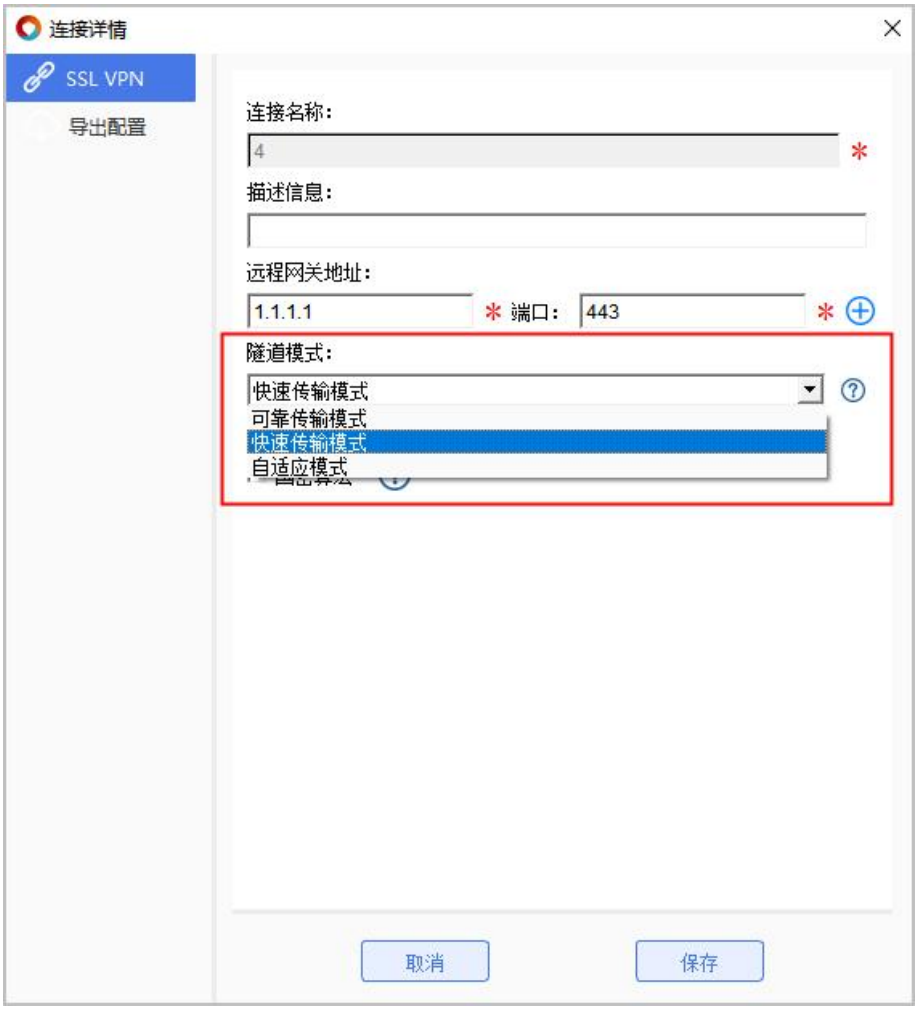
在 UniVPN 登录界面，输入用户名和密码以后，单击“登录”，系统告警“当前连接不支持快速隧道模式，请切换到可靠隧道模式后重试”。

可能原因

终端在拨号 SSL VPN 过程中，会发送 UDP 探测报文，探测建立快速隧道的可行性。如果能收到防火墙的响应，说明快速隧道可以建立。上图中报错，说明该 UDP 链路不通，快速隧道无法建立。

处理步骤

1. UniVPN 配置“自适应模式”拨号，作为临时规避办法。快速隧道无法建立，通过下面步骤继续排查。



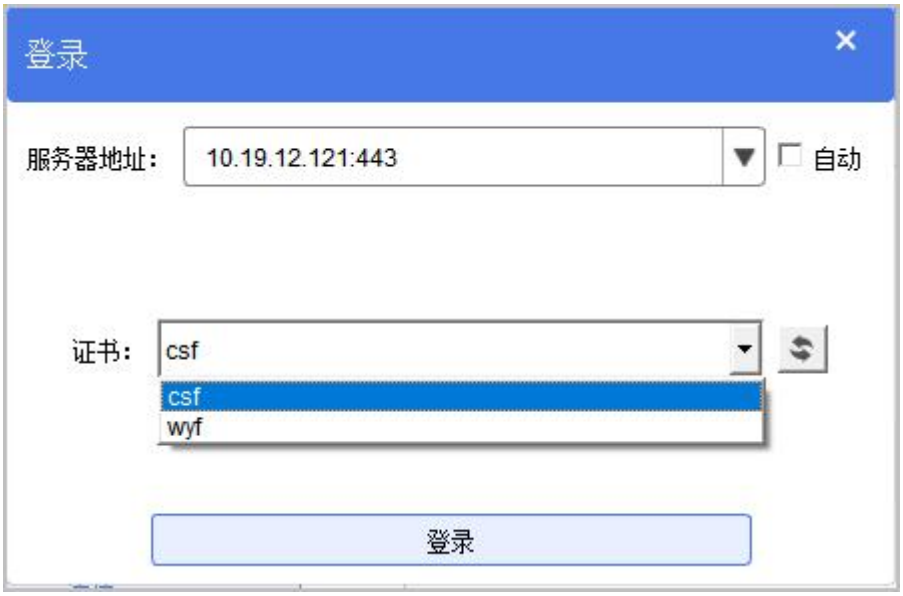
2. 排查防火墙的安全策略，是否放行了终端与 VPN 网关之间建立 UDP 快速链路的数据流。
3. 检查防火墙外层是否存在 NAT 设备，如果存在，需针对 SSL VPN 的 TCP 和 UDP 端口分别做 NAT 映射且安全策略放行；对 UDP 端口做 NAT 映射时，Global 端口和 Inside 端口必须一致。

1.6.3 采用证书方式登录时出现警告

1.6.3.1 找不到用户证书

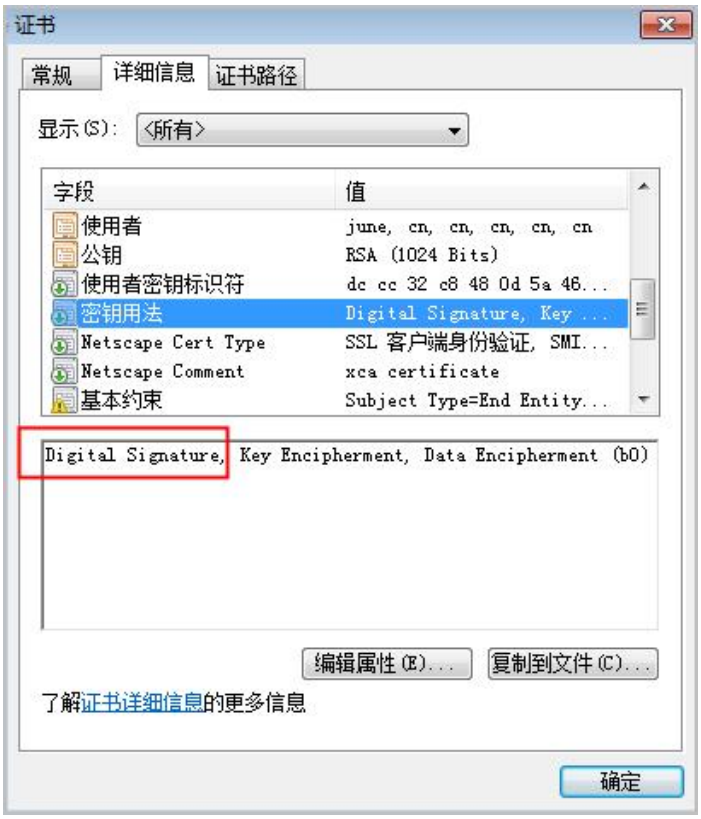
现象描述

在虚拟网关采用证书认证的情况下， 在 UniVPN 登录界面，选择用户证书时，无法找到预期的用户证书。



可能原因

预期的用户证书“密钥用法”没有包含“Digital Signature”（数字签名）。



处理步骤

重新制作一本密钥用法带“数字签名”的用户证书。

说明

如果服务器不支持无数字签名能力的证书，客户端不显示无数字签名能力证书；

如果服务器支持无数字签名能力的证书，但是客户端未显示无数字签名能力证书，可能是服务器开启了密钥用法：必须拥有数字签名能力。

产品名称	产品版本	是否支持无数字签名能力的证书认证
USG6000	V500R005C20SPC500 及以后版本	不支持
USG9500	V500R005C20SPC500 及以后版本	不支持
USG6000E	V600R007C20SPC300 及以后版本（SPC301/SPC 302 版本除外）	不支持
Eudemon200E-N	V500R005C20SPC500 及以后版本	不支持
Eudemon200E-G	V600R007C20SPC300 及以后版本（SPC301/SPC 302 版本除外）	不支持
Eudemon1000E-N	V500R005C20SPC500 及以后版本	不支持
Eudemon1000E-G	V600R007C20SPC300 及以后版本（SPC301/SPC 302 版本除外）	不支持
Eudemon8000E-X	V500R005C20SPC500 及以后版本	不支持
SeMG9811	V500R005C20SPC500 及以后版本	不支持
NGFW Module	V500R005C20SPC500 及以后版本	不支持
USG12000	V600R021C10 及以后版本	支持
USG6000F	V600R021C10 及以后版本	支持
Eudemon9000E-X	V600R021C10 及以后版本	支持
Eudemon9000E-F	V600R021C10 及以后版本	支持
Eudemon1000E-F	V600R021C10 及以后版本	支持

1.6.3.2 提示：您的用户证书验证非法，请提供合法的证书！

现象描述

在 UniVPN 登录界面，选择用户证书，单击“登录”，系统提示“您的用户证书验证非法，请提供合法的证书！”

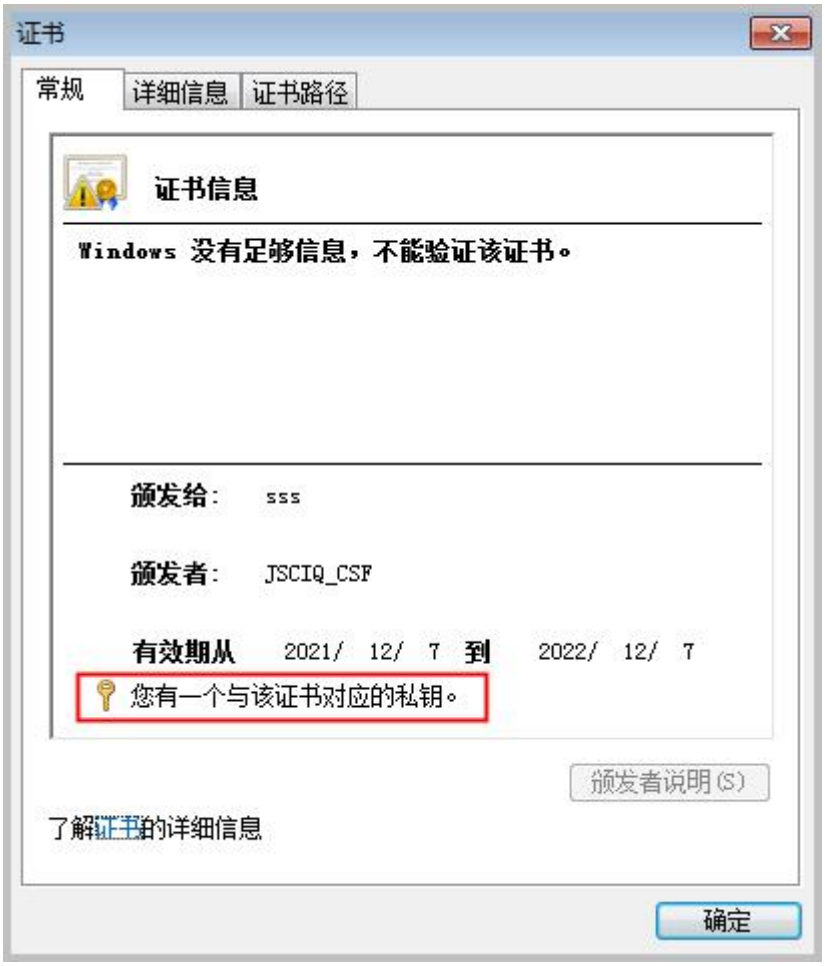
可能原因

1. 用户证书，不是由防火墙虚拟网关客户端 CA 证书的根证书签名颁发。
2. 安装在终端上的用户证书，没有携带私钥信息。
3. 防火墙设备的系统时间、时区，不在用户证书的有效期范围之内。
4. 用户证书被防火墙配置的 CRL（证书吊销列表）或 OCSP（在线证书状态协议）吊销。

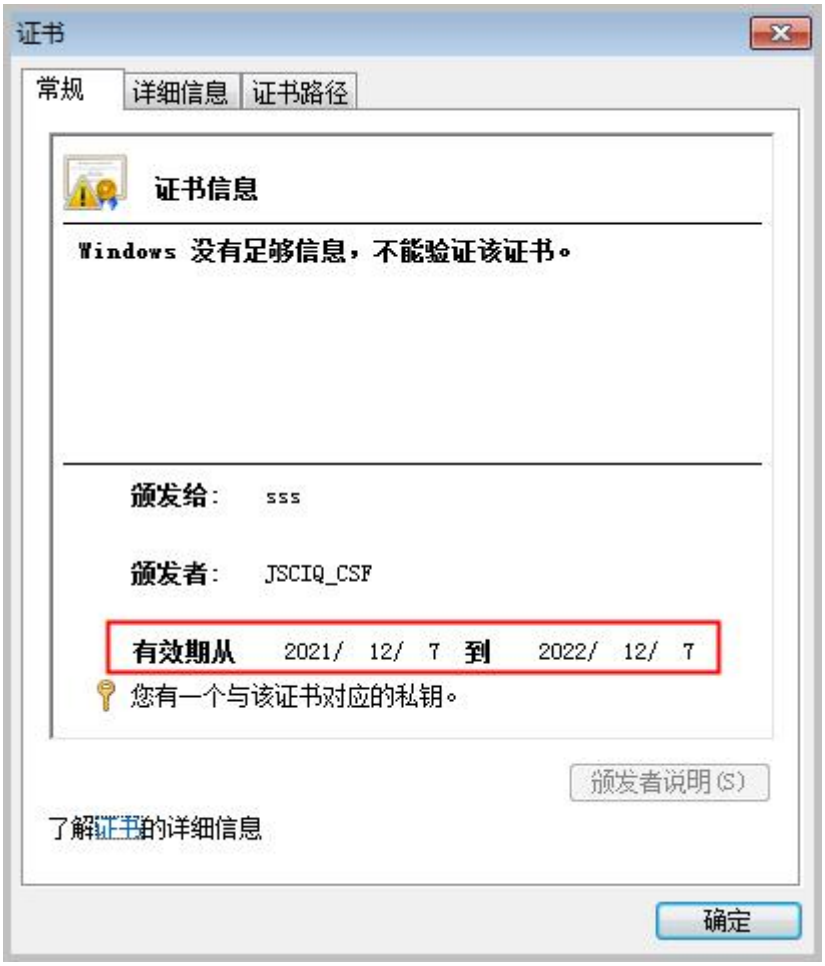
处理步骤

1. 检查用户证书的“颁发者”字段，是否和防火墙虚拟网关客户端 CA 证书的“颁发给”字段一致。

2. 检查用户证书，是否有对应的私钥。



3. 检查防火墙的时间、时区配置是否正确，以及是否在用户证书的有效期范围之内。



4. 检查防火墙是否配置了 CRL 或 OCSP，如果是，取消该配置，观察效果。

1.6.3.3 提示：认证失败！

现象描述

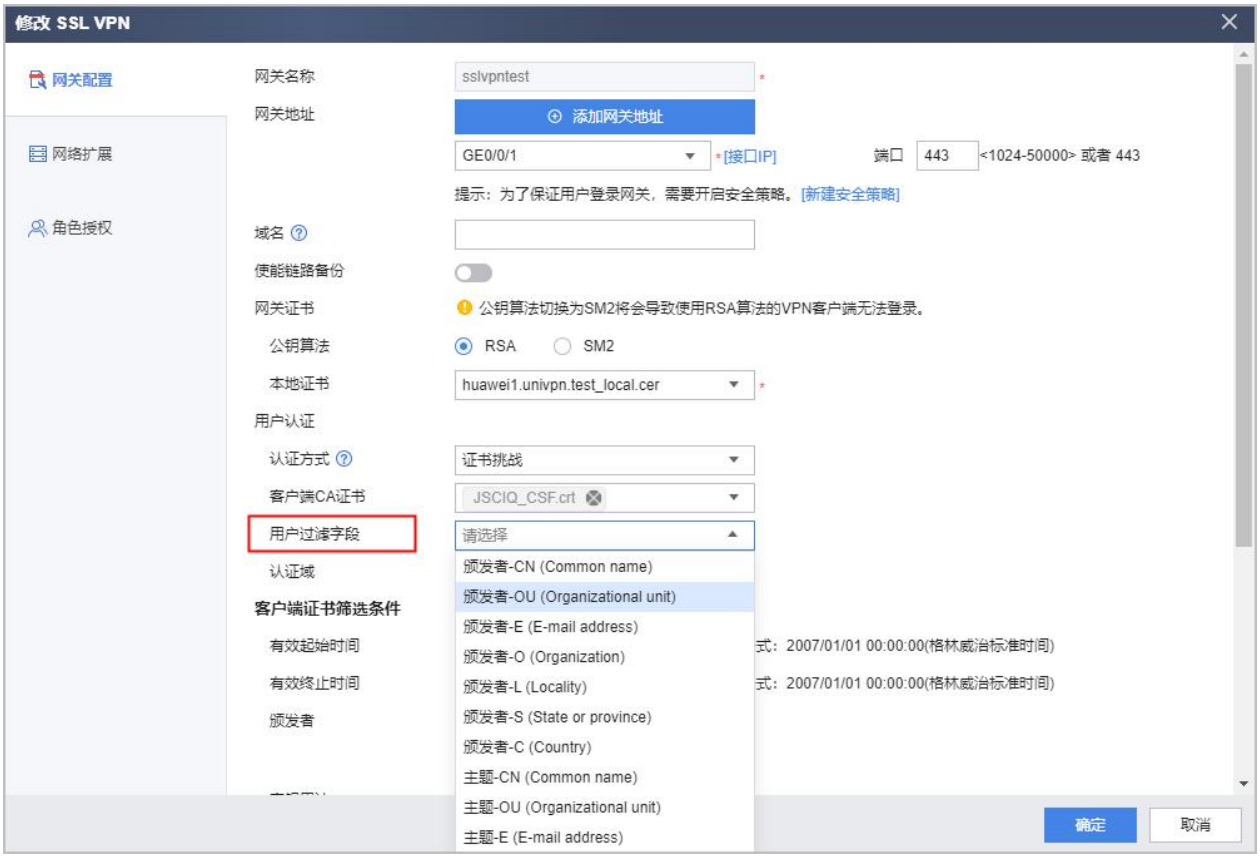
在虚拟网关采用证书挑战认证的情况下，在 UniVPN 登录界面，选择用户证书，单击“登录”，系统提示“认证失败!”。

可能原因

1. 虚拟网关证书认证“用户过滤字段”配置不正确，导致用户登录时设备从用户证书中获取了错误的用户名信息。
2. 虚拟网关绑定了不正确的认证域。
3. 认证域未启用 SSL VPN 接入场景。
4. SSL VPN 登录的设备处于双机备状态（HRP_S），而 SSL VPN 不支持在备设备上登录上线。
5. 证书有效期过期

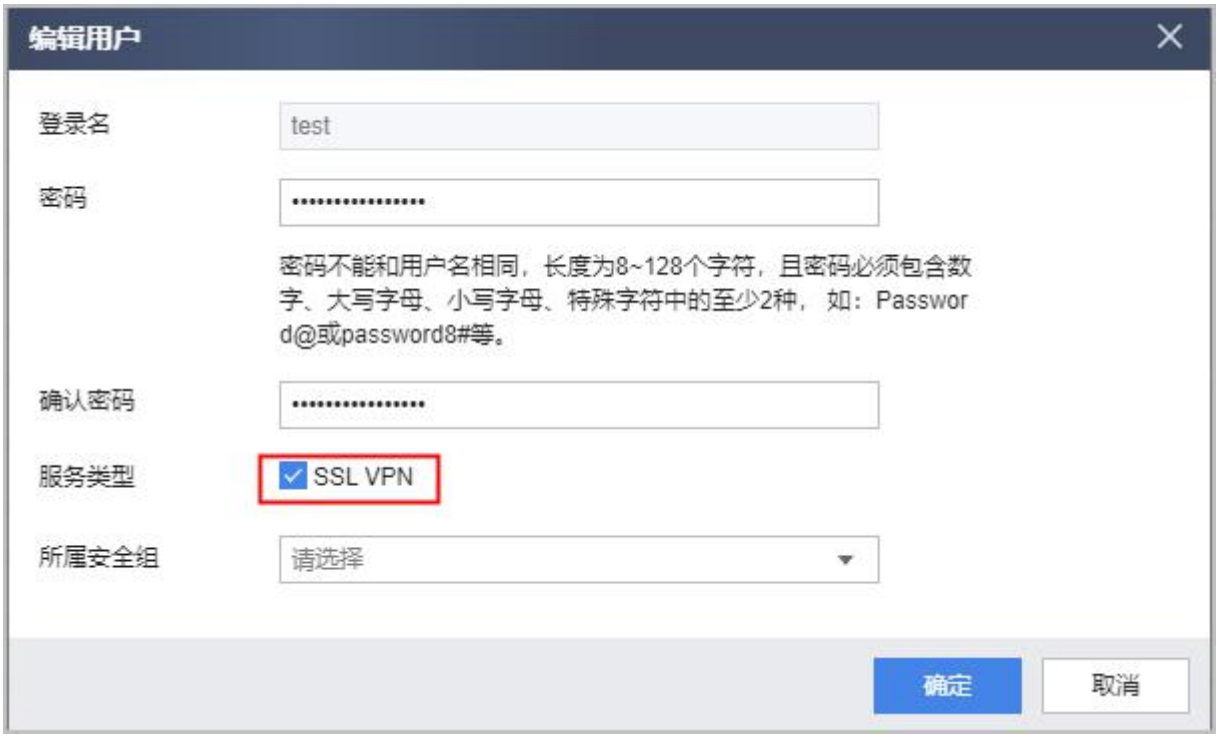
处理步骤

1. 登录设备，检查虚拟网关证书认证“用户过滤字段”配置，和用户证书中用于认证字段的属性名称是否匹配。

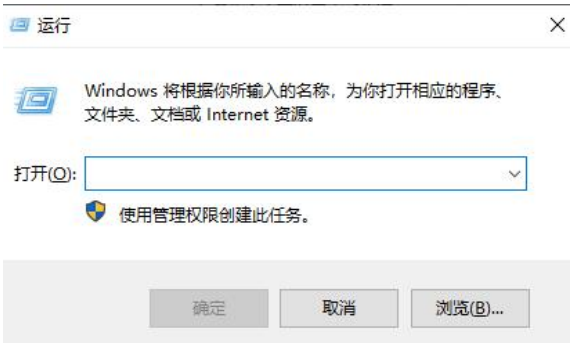


2. 检查虚拟网关是否绑定了认证域，如果有绑定，是否绑定了正确的认证域。

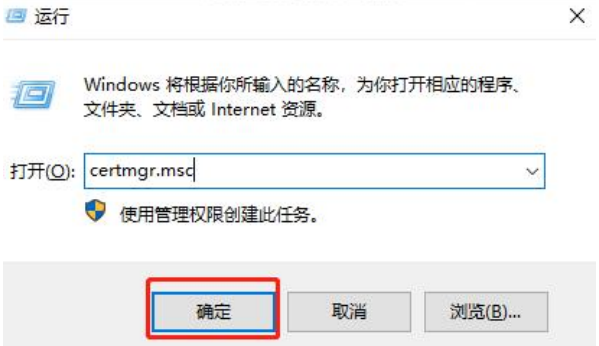
3. 检查用户配置，是否启用了 SSL VPN 接入场景。



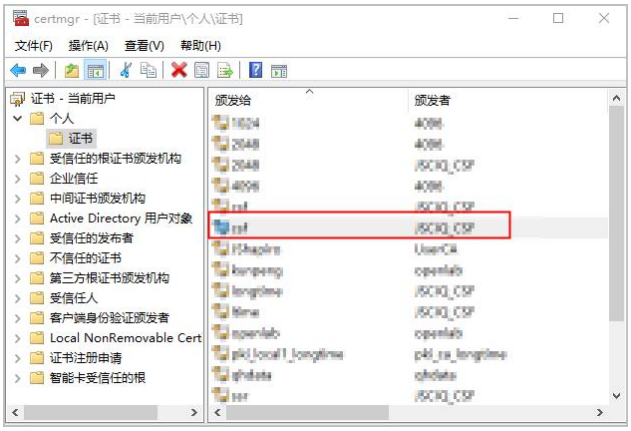
4. 调整配置或组网，确保 SSL VPN 登录的设备处于双机主状态（HRP_M）。
5. 删除已过期证书，重新导入未过期证书。
   1、使用 windows + R 键打开“运行”对话框。



   2、输入 certmgr.msc,单击确定，打开证书管理器

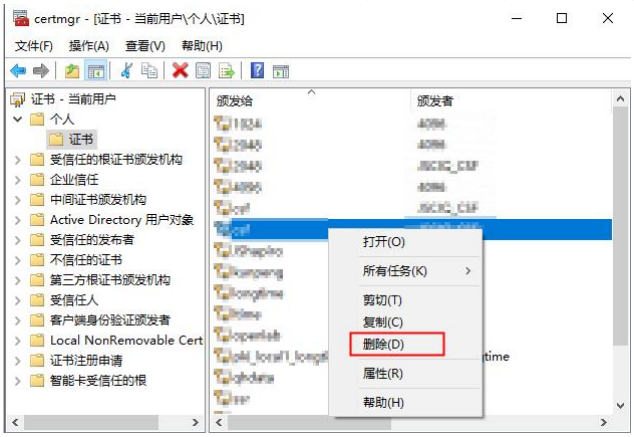


   3、选择“个人>证书”，选择用户证书。双击用户证书，查看证书有效期。



4、双击用户证书，查看证书有效期后，单击“确定”返回证书管理器。

5、右键单击有效期已过期的证书选择“删除”，根据提示删除有效期过期的证书。



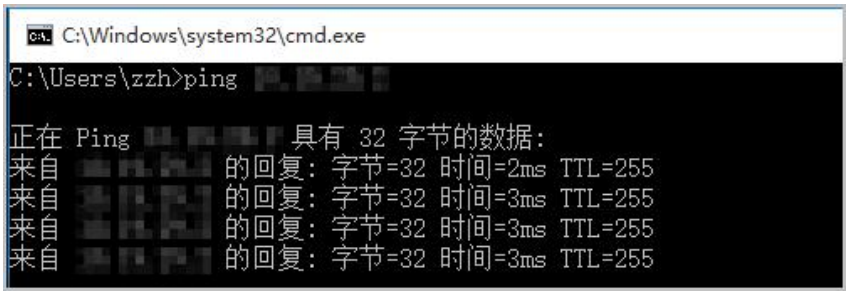
6、重新安装有效期未过期的用户证书，重新开始 UniVPN 客户端认证。

1.6.4 登录成功后业务出现异常

1.6.4.1 访问内网资源卡顿，ping 内网延迟大

现象描述

SSL VPN 拨号成功，访问内网资源卡顿，Ping 内网延迟大。测试下载速率比 NAT 映射低很多。



可能原因

从技术实现角度来看，NAT 映射只是对报文头做了地址转换，相对简单；而 VPN 技术需要对整个报文做加解密封装，相对复杂。因此，VPN 本身造成的系统消耗和引发的时延就比 NAT 映射大。在跨运营商的场景下，这个延时就更为明显一些。

处理步骤

1. 在隧道模式那里选择快速模式或是自适应模式，快速模式报文传输效率相对较高。当隧道传输模式为“快速传输模式”时，防火墙上要开启 Local 到 Untrust（假设用户处于 Untrust 区域）的域间策略，策略匹配条件中服务类型为 UDP，端口为 443。自适应模式下，UniVPN 会优先以“快速传输模式”与 VPN 网关建立 SSL VPN 隧道；当快速模式建立失败时，UniVPN 会转为使用“可靠传输模式”与 VPN 网关建立 VPN 隧道。
2. 如果企业对外提供了多个 SSL VPN 网关，在 UniVPN 上启用自动优选功能可以保证用户连接到响应最快的那台 VPN 网关，减少延迟。

1.6.4.2 登录成功后，无法访问公网

现象描述

SSL VPN 拨号成功，但是无法访问公网站点了，域名也 Ping 不通。

可能原因

1. 虚拟网关网络扩展配置了分离路由模式或全路由模式。
2. 资源未授权

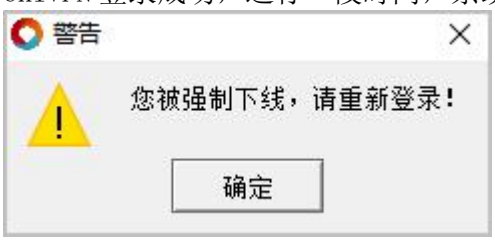
处理步骤

1. 调整网络扩展路由模式为手工路由模式，终端启用网络扩展成功，仅在访问指定的 VPN 内网网段时，走 VPN 隧道，访问其它网段（含公网），不走 VPN 隧道。
2. 将对应的资源授权给 vpn 用户。

1.6.4.3 警告：您被强制下线，请重新登录！

现象描述

UniVPN 登录成功，运行一段时间，系统告警“您被强制下线，请重新登录！”。



可能原因

1. 管理员强制用户下线。
2. 用户在线老化时间超时下线。

处理步骤

3. 登录 VPN 网关，选择“监控 > 系统日志”，检查防火墙操作日志，确定是否管理员执行了强制用户下线的动作。
4. 检查虚拟网关会话超时时间配置，以及网络扩展保持连接功能是否开启。

1.6.4.4 提示：无法建立 VPN 连接，VPN 服务器可能无法到达

现象描述

UniVPN 登录后，拨号提示：无法建立 VPN 连接，VPN 服务器可能无法到达。

可能原因

出现此现象，大概率是由于客户端侧与网关侧使用加密算法不同导致。

处理步骤

1. 从 V600R007C20SPC100 开始，缺省情况下设备去使能虚拟网关的弱加密算法，此时虚拟网关的加密套件只能使用强加密算法，使用 10781.2.327.1231 及其之后版本的 UniVPN 才能正常登录虚拟网关。

   对于 10781.2.327.1231 之前的版本，可在网关侧执行 v-gateway ssl weak-encryption enable 命令使能虚拟网关弱加密算法。

2. 若网关侧和国密侧均配置使用国密算法，出现此提示，若日志打印如下提示：

```
open gmssl lib C:\Program Files (x86)\UniVPN\serviceclient\libgmssl-1_1-x64.dll, failed, reason: 126
[SSL Create failed][load library 2 failed]
```

一般是由于缺少某些组件问题导致，可下载 Visual C++ Redistributable for Visual Studio2015 手动安装解决此问题。

微软官方链接：https://www.microsoft.com/zh-CN/download/details.aspx?id=48145&from_wecom=1。

1.6.4.5 终端加入 AD 域后，SSL VPN 用户接入一段时间后异常掉线

现象描述

终端加入 AD 域，SSL VPN 用户接入一段时间后异常掉线，而不加入 AD 域，则不会出现掉线。

具体故障现象如下。

- 防火墙上能看到用户下线记录。

在主墙上查看用户下线记录提示如下。

```
[HUAWEI]info-center source sslvpn channel logbuffer log level informational
Warning: There is security risk as all logs which level is not less than 6 will be output the logbuffer.
[HUAWEI]display logbuffer service-log
2023-04-23 11:43:46.314 +08:00
Logging buffer configuration and contents : enabled
Allowed max buffer size : 10240
Actual buffer size : 512
Channel number : 4 , Channel name : logbuffer
Dropped messages : 0
Overwritten messages : 1008
Current messages : 11

Apr 23 2023 11:39:02+08:00 HUAWEI %%01SSLVPN/6/USERLOGOUT(l):CID=0x814f0428;The user logged out. (User Name=csf, Vsys=pub
lic, VGName=sslvpntest, Virtual IP= [redacted], Client IP= [redacted], Obverse Packets=9, Obverse Bytes=1110, Reverse Pa
ckets= 76, Reverse Bytes=4596, Logout Reason=The user proactively goes offline.).
Apr 23 2023 11:38:28+08:00 HUAWEI %%01SSLVPN/6/USERLOGINSUCC(l):CID=0x814f0428;User login succeeded. (User Name=csf, Vsys
=public, VGName=sslvpntest, Virtual IP= [redacted], Client IP= [redacted]).
```

在备墙上查看用户下线记录提示如下。

```
[HUAWEI]info-center source sslvpn channel logbuffer log level informational
Warning: There is security risk as all logs which level is not less than 6 will be output the logbuffer.
[HUAWEI]display logbuffer service-log
2023-04-23 11:43:46.314 +08:00
Logging buffer configuration and contents : enabled
Allowed max buffer size : 10240
Actual buffer size : 512
Channel number : 4 , Channel name : logbuffer
Dropped messages : 0
Overwritten messages : 1008
Current messages : 11

Apr 23 2023 11:39:02+08:00 HUAWEI %%01SSLVPN/6/USERLOGOUT(l):CID=0x814f0428;The user logged out. (User Name=csf, Vsys=pub
lic, VGName=sslvpntest, Virtual IP= [redacted], Client IP= [redacted] Obverse Packets=9, Obverse Bytes=1110, Reverse Pa
ckets= 76, Reverse Bytes=4596, Logout Reason=The user proactively goes offline.).
Apr 23 2023 11:38:28+08:00 HUAWEI %%01SSLVPN/6/USERLOGINSUCC(l):CID=0x814f0428;User login succeeded. (User Name=csf, Vsys
=public, VGName=sslvpntest, Virtual IP= [redacted] Client IP= [redacted]).
```

- UniVPN 客户端日志提示用户下线的原因是被网关侧踢下线。

```
FRAME  DEBUG  2020-09-02 12:45:09.000334 ][B00550] [65535][Create event base][eventbase notifyserver notify send ok sock(1256)
FRAME  DEBUG  2020-09-02 12:45:09.000334 ][B00550] [65535][Add event][interval(10:0) tv(10:0) timeout:(1599061519:334423)]
FRAME  DEBUG  2020-09-02 12:45:09.000335 ][B00550] [65535][Insert event][timeoutlist(fd:4 ev_res:268435696 total:0 timer:5 act
FRAME  DEBUG  2020-09-02 12:45:09.000335 ][B00550] [65535][eventlist todo wait][end ok,todo:00000000036A2820 semid:7]
FRAME  DEBUG  2020-09-02 12:45:09.000335 ][B00550] [65535][Unbind channel][unbind channel OK (chid-239-268435695 events(2))]
CNEM   WARN   2020-09-02 12:45:15.000450 ][B00550] [65535][Cnem handle packet from gateway][CMDtype is KICKOUT]
FRAME  DEBUG  2020-09-02 12:45:15.000450 ][B00550] [65535][send message][task(4) mqueid(4) message type:1 send message addr(000
CNEM   INFO   2020-09-02 12:45:15.000451 ][B00550] [65535][Cnem send status msg to self ok]
```

- 在防火墙上采集调制日志，在用户掉线之前，LAM 模块产生的 CUT_REO 事件。

```
HRP_M<HUAWEI-diagnose> debugging swm error
Sep 14 2020 13:15:49-03:00 FGSTHA00-01 CM/7/DEBUG:
[UCM-MSG] MSG Recv From:(taskName=LAM, Code=ESAP_SRV_MSG_CUT_REQ, Src=0, Dst=-1, Slot=0)WebAuth:0x0 Vrf:0Reason:29 Vlan:0 VPI/VCI:0/0 AccessType:0TimeoutMsg:0 Mac:0000-0000-0000 IPV6: IP:10.0.91.28.
Sep 14 2020 13:15:49-03:00 FGSTHA00-01 CM/7/DEBUG:
```

可能原因

出现上述现象，大概率是由于防火墙上同时配置了 SSL VPN 和 AD 单点登录功能（安装 ADSSO 查询 AD 服务器安全日志）导致。

终端加入 AD 域后，SSL VPN 用户接入网关后需要连接 AD 域控制器进行认证（此时 AD 域控制器会记录安全日志），认证通过后，SSL VPN 用户在防火墙上线，SSL VPN 用户登录成功。当 ADSSO 向 AD 域控制器获取安全日志（内容是 SSL VPN 账号和虚拟 IP 地址的对应关系。）后，将安全日志发送给防火墙，防火墙会根据安全日志再次将此用户上线。也就是在此种场景下，同一个用户（同一个账号对应同一个虚拟 IP）会两次在防火墙上线，第一次是 SSL VPN 用户登录过程，SSL VPN 用户认证通过后在防火墙上线，第二次是防火墙解析 ADSSO 发送的安全日志后将用户上线。

但防火墙不支持上述场景，防火墙解析 ADSSO 发送的安全日志将用户上线时，会将之前已经在线的 SSL VPN 用户踢下线。

处理步骤

1. 请确认防火墙上是否配置了 AD 单点登录功能（安装 ADSSO 查询 AD 服务器安全日志）功能，如果是，请执行后续步骤。如果没有配置 AD 单点登录功能，请联系联软技术支持工程师。
2. 在防火墙配置源 NAT 策略。
3. 针对 SSL VPN 用户请求域控服务器的认证数据流配置源 NAT 策略。配置后，SSL VPN 用户和域控服务器之间没有直接交互。AD 域控制器上产生的安全日志，其用户的源 IP 地址不再是 SSL VPN 拨号获得的虚拟 IP 地址，而是防火墙内网接口 IP 地址。这样防火墙解析 ADSSO 发送的安全日志将用户上线时，不会将之前已经在线的 SSL VPN 用户踢下线。

   c. 选择“策略 > NAT 策略 > NAT 策略”。

   d. 单击“新建”，配置源 NAT 策略。

   假设 SSL VPN 用户的虚拟地址为 10.2.0.0/16，AD 域控制器的地址为 10.10.10.3。

1.7 移动客户端 FAQ

除了 PC 版的 **UniConnect** 客户端外，联软科技公司还推出了基于 iOS 及 Android 操作系统的移动版客户端。

获取

- **获取 iOS 操作系统版本的移动版客户端**

  方式一：打开“**APP Store**”APP，搜索“**UniConnect**”字段，即可下载最新版本的 UniConnect iOS 版本客户端。

- **获取 Android 操作系统版本的移动版客户端**

  方式一：下载并打开**应用市场类** APP，搜索“**UniConnect**”字段，即可下载最新版本的 UniConnect Android 版本客户端。

规格

移动版 UniConnect 客户端目前仅支持建立 SSL VPN 连接，具体支持的机型及操作系统版本如下：

表 1-1 移动版 UniConnect 客户端支持的机型及操作系统版本

操作系统	iOS	Android
支持的操作系统版本	支持 iOS 10.0 及以上版本。	支持 Android 5.0 及以上版本。
支持的设备型号	• iPhone X • iPhone 8/8 Plus • iPhone 7/7 Plus • iPhone 6s/6s Plus	-

操作系统	iOS	Android
	• iPhone 6/6 Plus • iPhone 5s • iPad Pro • iPad Air 1/2 • iPad 4 • iPad mini 2/3/4	
支持的设备屏幕分辨率	-	• 720*1280 • 1080*1920 • 1440*2560 • 2160*4096

移动版 UniConnect 客户端的功能规格如下：

表 1-2 移动版 UniConnect 客户端的功能规格

功能名称		iOS	Android
SSL VPN	网络扩展	支持	支持
	终端安全 **说明** 网关侧开启终端安全功能时，移动版 UniConnect 户端可以拨号成功。	支持	支持
	网关优选	支持	支持
	断线重连	支持	支持
	链路备份 **说明** 网关侧开启链路备份功能时，移动版 UniConnect 客户端可以拨号成功。	支持	支持
	证书认证	支持	支持
	MAC 认证	不支持	不支持
	证书筛选	支持	支持
	双因子认证	支持	支持 可通过短信

功能名称		iOS	Android
			验证码进行双因子认证
L2TP VPN		不支持	不支持
L2TP over IPSec VPN		不支持	不支持
NAT 穿越		不支持	不支持
代理穿越		不支持	不支持
隧道分离		支持	支持
基本功能	开机自启动	不支持	不支持
	界面语言切换 **说明** 仅支持中英文切换。	支持	支持
	自动登录	支持	支持
配置文件	导入	不支持	不支持
	导出	不支持	不支持
故障定位		支持	支持
命令行配置		不支持	不支持
非管理员权限用户配置		支持	支持

移动版 UniConnect 客户端的性能规格如下：

表 1-3 移动版 UniConnect 客户端的性能规格

功能名称	规格
VPN 新建连接数	16 个

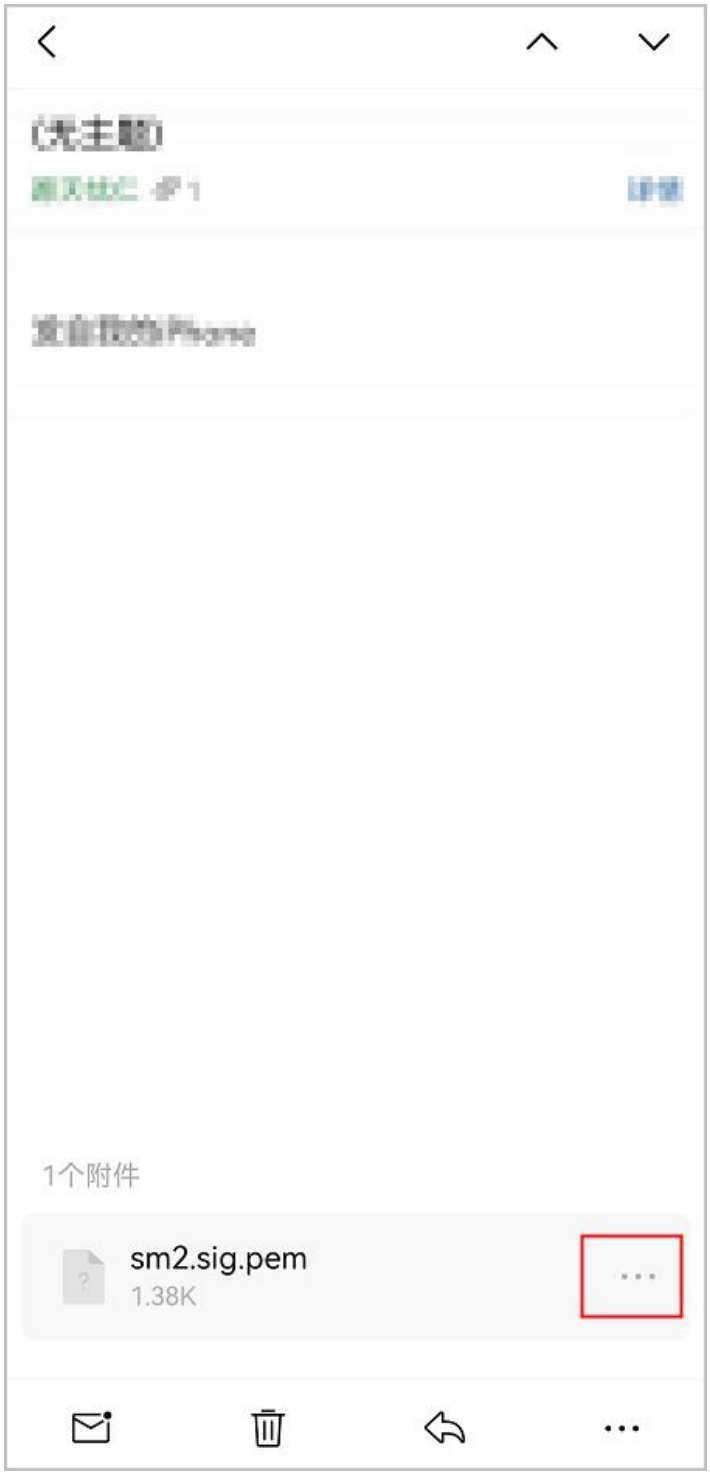
操作

移动版 UniConnect 客户端的具体操作，请参见 APP 内“ > 帮助”节点下的联机帮助。

1.7.1 如何导入国密证书

国密证书和非国密证书导入客户端方法一致，下面以国密证书导入 UniConnect 为例，介绍 UniConnect 导入并使用证书认证。

步骤 1 打开邮箱找到此文件，点击右下角的 。



步骤 2 单击此文件（没有下载就会请求下载）选择**“分享文件”**。

步骤 3 选择 UniConnect。

2:42
(无主题)
愿天忧仁 1
详情
请勿轻信邮件中的密保，汇款，中奖信息
分享文件
转为演示
转为PDF
AI 隐私保护
B612咔叽
EasyConnect
Fleet
Telegram
UniConnect
WLAN 直连
取消

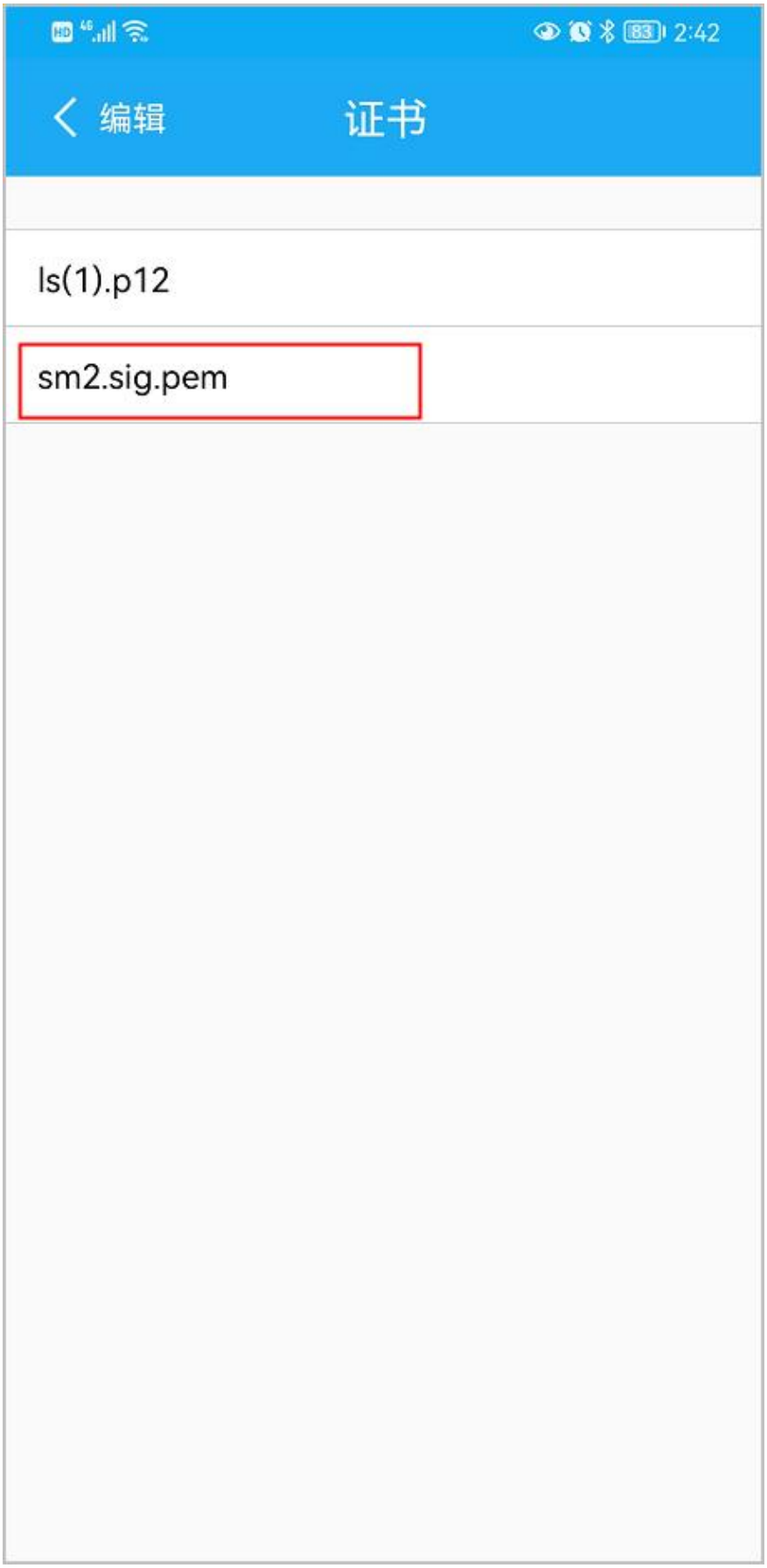
步骤 4 单击**“确定”**。

2:42
返回
保存
提示
确认保存?
取消
确定

步骤 5 导入成功后开启“证书认证”开关。

2:42
主页
编辑
保存
类型
SSL
连接名称
5555
远程网关地址
10.19.12.121
端口
5555
隧道模式
自适应传输模式
自动登录
路由覆盖
国密算法
证书认证
删除VPN连接

步骤 6 单击“证书选择”选择国密证书。

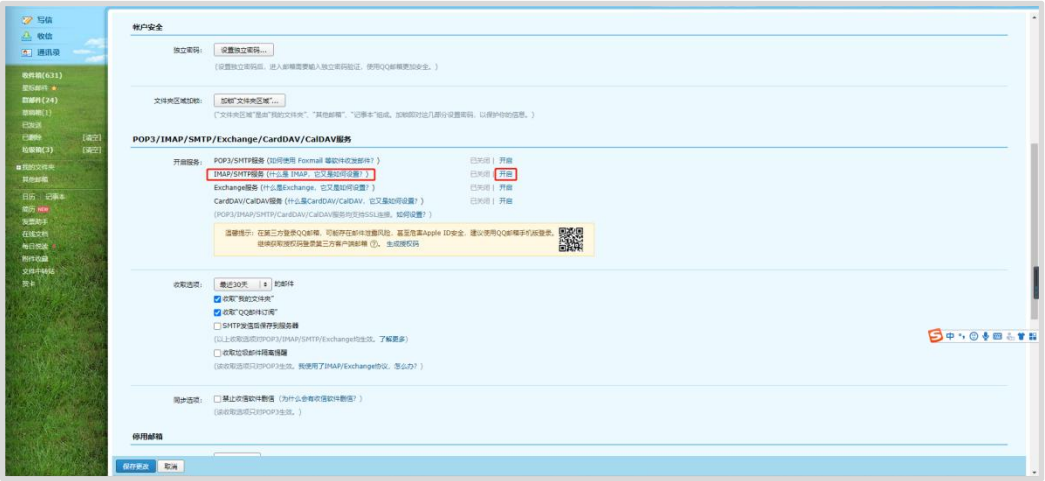

2:42
编辑
证书
ls(1).p12
sm2.sig.pem

1.7.2 如何反馈 iOS 问题

配置邮箱

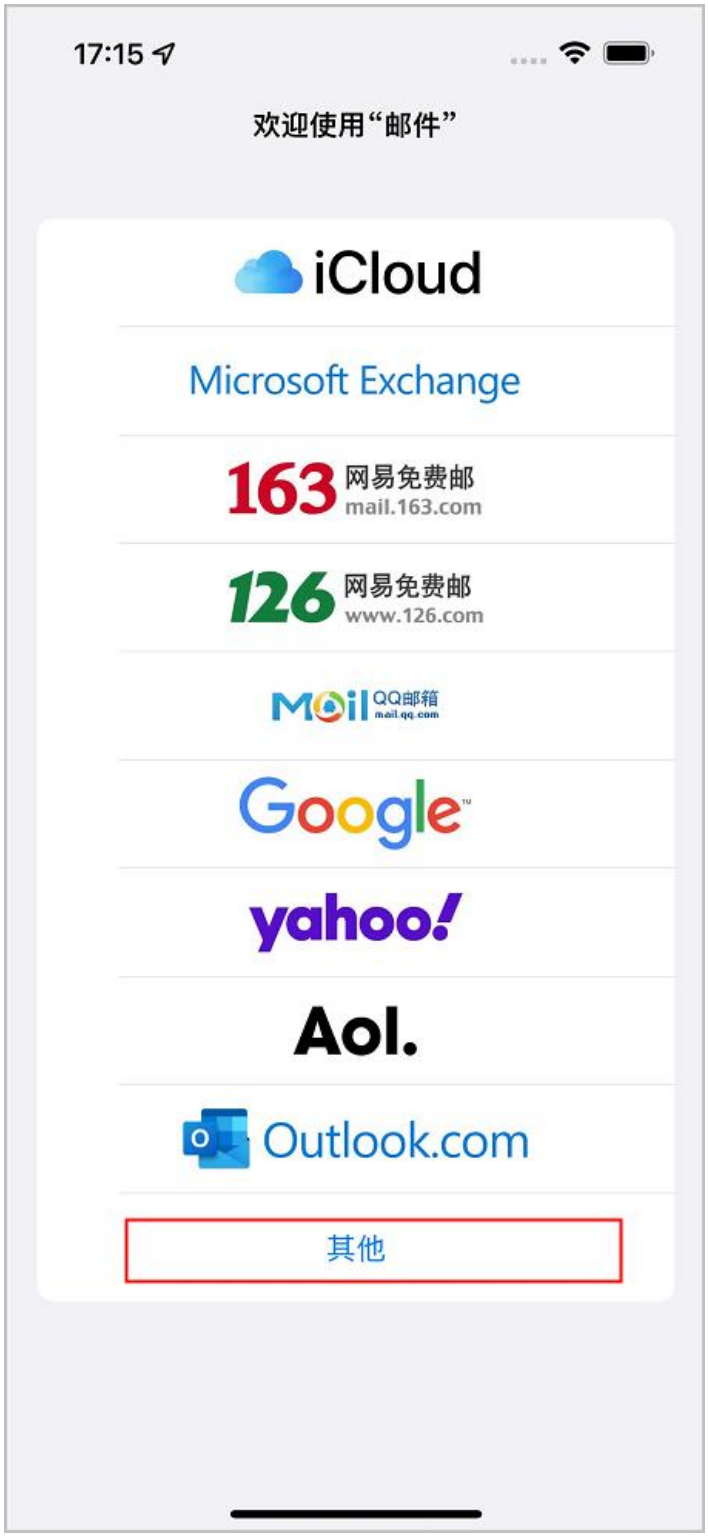
步骤 1 进入 QQ 邮箱，单击左上角“设置”，选择“账户”。

步骤 2 在“账户”页中，单击 IMAP/SMTP 后的“开启”开启 IMAP 服务。



步骤 3 单击 Generate Authorization Code，获得授权码。

步骤 4 打开手机桌面中的邮箱，选择"其他"QQ 邮箱。



步骤 5 将电脑页面显示的授权码填入此密码框。

步骤 6 单击右上角的“下一步”。

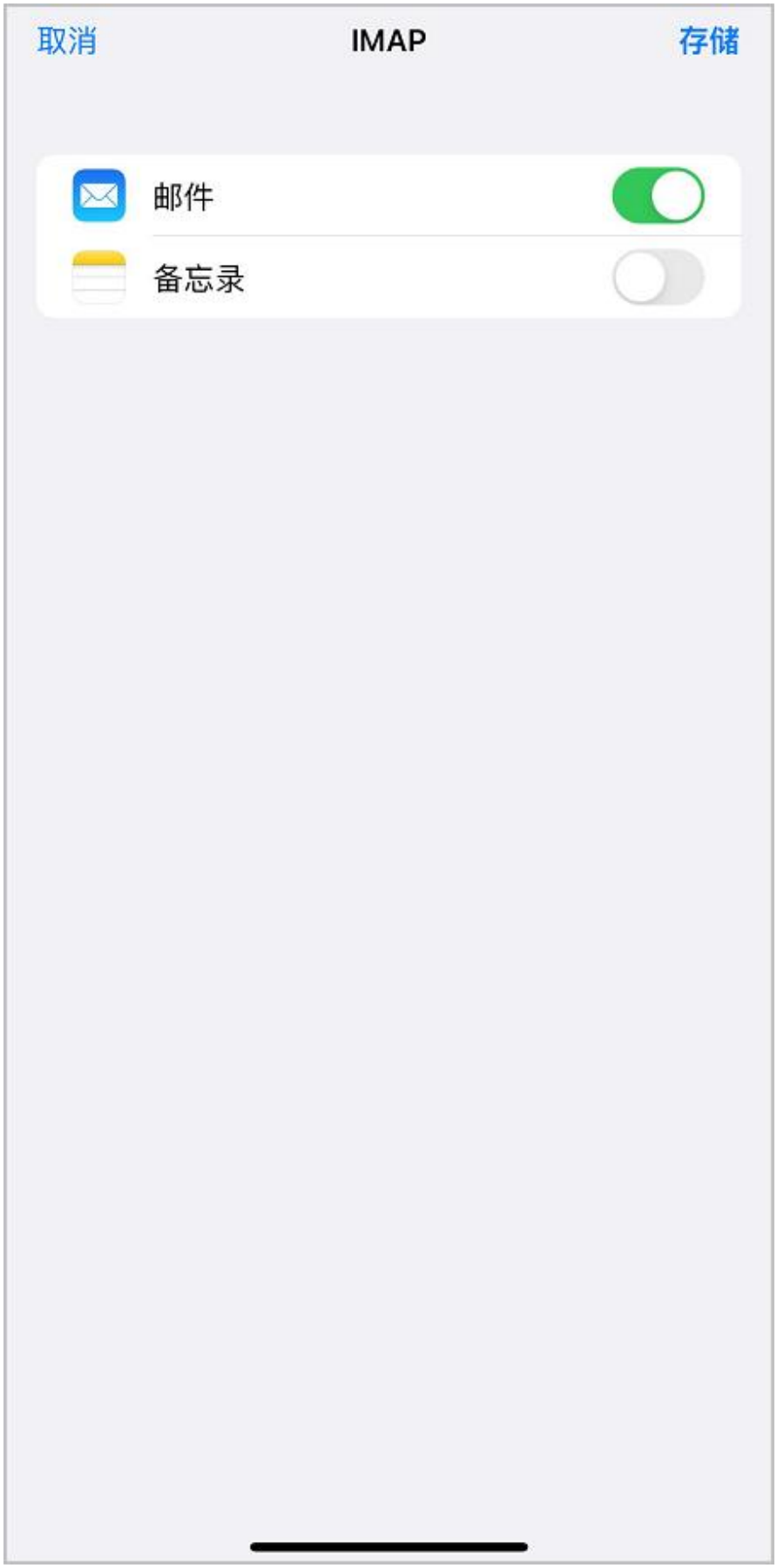
步骤 7 QQ 账户信息填写全名，电子邮件，描述；

收件服务器填写主机名，用户名（为电子邮件），密码（为步骤 3 第二张图片显示的 Authorization Code）；

发件服务器所填写的信息和收集服务器相同（主机名为 smtp.qq.com,密码都是授权码）。

取消
帐户
完成
QQ 帐户信息
全名
电子邮件
描述
收件服务器
主机名
imap.qq.com
用户名
密码
发件服务器
SMTP
smtp.qq.com
高级

步骤 8 单击“存储”。


取消
IMAP
存储
邮件
备忘录

步骤 9 配置成功后，在登录页面选择“ >反馈”开启反馈日志后进行操作。

1.7.3 取消自动登录（安卓）

步骤 1 在登录时用户密码时开启自动登录，然后连接成功。

步骤 2 断开连接后，编辑任一连接将自动登录按钮关闭，单击“保存”即取消自动登录已。

1.7.4 iOS 异常卡顿的解决方法

步骤 1 使用 IOS 客户端时，若因长时间使用、机型版本过旧等原因引起的客户端卡顿，请重启客户端应用后再使用。

1.7.5 后台设置国密加证书匿名的情况

后台设置为国密+证书匿名的配置，App 登录时仅显示一本国密签名证书。

1.7.6 安卓客户端登录后通知栏显示情况

安卓客户端登录后，会在通知栏顶端显示，然而部分手机因为系统自身维护导致其在下拉通知栏中消失。

1.7.7 UniConnect 是否支持 MAC 认证

不支持。

1.7.8 IOS 系统是否支持取消自动登录

不支持。

1.7.9 设备熄屏状态掉线

设备锁屏 2 小时及以上时，可能出现与服务器设备断开连接，此时需打开应用，重新进行连接操作。

1.7.10 多个 VPN 存在同一款手机导致 UniConnect 不可用

恢复操作步骤：1.进入 UniConnect。2.选择 vpn 连接信息。

1.7.11 UniConnect 是否支持多种系统语言

仅支持中英文。

1.7.12 VPN 编辑信息界面，连接名称能否输入特殊字符

特殊字符仅支持下划线“_”和“.”。

1.7.13 IOS 系统是否支持暗黑模式

不支持。