

华为防火墙

SSL VPN 故障处理

文档版本 02
发布日期 2021-06-30



版权所有 © 华为技术有限公司 2021。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



HUAWEI和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编： 518129

网址： <https://e.huawei.com>

目录

1 概述	1
2 使用须知	2
3 SSL VPN 支持列表	3
4 SecoClient 拨号 SSL VPN 故障	9
4.1 打开 SecoClient 时出现警告	9
4.1.1 警告：已经有客户端正在运行，不能再运行该程序！	9
4.1.2 警告：请确保已访问过 VPN 的网页或其他 VPN 客户端软件已经关闭	10
4.1.3 警告：当前服务进程已退出或关闭，请尝试重新安装客户端！	11
4.1.4 警告：无法建立 VPN 连接，VPN 服务器可能无法到达	12
4.1.5 警告：获取系统代理失败！	13
4.2 采用用户名/密码方式登录时出现警告	16
4.2.1 警告：不可信的 VPN 服务器证书！	16
4.2.2 警告：认证失败！	17
4.2.3 警告：连接被网关拒绝，请检查网关配置参数！	20
4.2.4 警告：用户连接数已达到上限，请稍后重试！	21
4.2.5 警告：网络扩展启动失败！	23
4.2.6 警告：主机检查失败！	25
4.2.7 警告：接收返回码超时！	26
4.2.8 警告：UDP 隧道建立失败，请选择其它模式登录	27
4.3 采用证书方式登录时出现警告	28
4.3.1 找不到用户证书	29
4.3.2 警告：您的证书验证非法，请提供合法的证书！	30
4.3.3 警告：认证失败！	33
4.4 登录成功后业务出现异常	35
4.4.1 访问内网资源卡顿，Ping 内网延迟大	35
4.4.2 登录成功后，无法访问公网	36
4.4.3 警告：您被强制下线，请重新登录！	37
4.4.4 警告：连接断开，请重新登录！	38
4.4.5 提示：无法建立 VPN 连接，VPN 服务器可能无法到达	38
4.4.6 移动终端启动网络扩展不成功，PC 端可以成功	39
4.4.7 终端加入 AD 域后，SSL VPN 用户接入一段时间后异常掉线	39
4.4.8 新增 SSL VPN 网络扩展可访问网段后，用户无法访问新增网段	41

5 浏览器拨号 SSL VPN 故障	44
5.1 Windows + IE/浏览器兼容模式	44
5.1.1 浏览器提示：无法打开此页面	44
5.1.2 浏览器提示：此网站的安全证书存在问题	46
5.1.3 浏览器提示：您的证书验证非法，请提供合法的证书	47
5.1.4 浏览器提示：应用程序正常初始化（0xc0150002）失败	49
5.1.5 虚拟网关的登录页面停留在转圈画面	50
5.1.6 虚拟网关登录页面无法选择到用户证书	51
5.1.7 用户访问 Web-link 资源失败	53
5.1.8 浏览器启用网络扩展时提示：建立代理环境失败！	54
5.1.9 浏览器启用网络扩展时提示：启动网络扩展服务失败	55
5.1.10 浏览器启用网络扩展后访问内网资源卡顿，Ping 内网延迟大	56
5.1.11 浏览器启用网络扩展访问内网资源，不能命中关联用户/用户组的安全策略	57
5.1.12 浏览器提示：对不起，您的 VPN 会话因为超时或网络原因已断开	57
5.1.13 浏览器提示：访问失败，服务器问题，请与管理员联系	59
5.2 Windows + Chrome/Firefox/浏览器极速模式	60
5.2.1 SSL VPN 虚拟网关登录成功，看不到网络扩展“启动”按钮	60
5.3 Mac OS + Safari 浏览器	61
5.3.1 浏览器登录 SSL VPN，看不到网络扩展“启动”按钮	61
5.4 Android/iOS + 手机浏览器	61
5.4.1 手机使用浏览器登录 SSL VPN，无法看到 Web 代理资源	61
5.5 拨号成功后业务不通	62
5.5.1 网络扩展业务不通	62
5.5.2 Web 代理业务不通	65
5.5.3 端口转发业务不通	67
6 SSL VPN 常见咨询类问题 FAQ	70
6.1 SSL VPN 是否支持双机热备负载分担	70
6.2 SSL VPN 是否支持双机热备主备备份	70
6.3 SSL VPN 用户是否支持不认证登录	70
6.4 SecoClient 是否支持手机终端	70
6.5 SSL VPN 如何实现一个账号多处同时登录	71
6.6 SSL VPN 如何实现用户绑定网络扩展虚拟地址	72
6.7 SSL VPN 网络扩展虚拟 IP 地址分配规则	72
6.8 SecoClient 的日志采集方法	73
6.9 SSL VPN 常见业务日志有哪些	76
6.10 SSL VPN 证书认证相关知识	78
6.11 SSL VPN 和用户管理特性的关联知识点	78
6.12 SSL VPN 角色授权知识点	79
6.13 SSL VPN 是否支持用户和终端绑定	79
6.14 高端防火墙是否支持 SSL VPN 业务	79
6.15 SSL VPN 认证后如何基于用户进行权限管控	79
6.16 SSL VPN 采用 AD/LDAP 认证，如何实现允许指定安全组下的用户登录	80

6.17 SSL VPN 业务报文的域间关系如何确定.....	80
6.18 SSL VPN 是否支持双因子认证.....	81
6.19 SSL VPN 登录之后能否访问防火墙内网接口地址进行管理.....	81
6.20 如何使用 XCA 制作设备证书和用户证书.....	81
6.21 SecoClient 安装和运行是否都需要管理员权限.....	97
6.22 双机场景 SSL VPN 哪些配置可以备份到对端.....	97
6.23 SSL VPN 是否支持 IPv6.....	97
6.24 SSL VPN 控件支持浏览器的情况如何.....	97
6.25 SSL VPN 各子特性的应用范围.....	98
6.26 SSL VPN 是否支持友商 VPN 客户端拨号.....	99
6.27 SVN 和防火墙 SSL VPN 特性区别有哪些.....	99
6.28 SSL VPN 调整网络扩展参数是否强制用户下线.....	99
6.29 使用客户端拨号登录无法生成虚拟网卡，如何解决.....	100
6.30 SSL VPN 有哪些命令可以用来采集调试日志.....	100
6.31 SSL VPN 使用客户端拨号提示返回接收码超时，如何解决.....	100
6.32 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.....	100
6.33 为什么要提前在设备侧上传 ActiveX 控件.....	100
6.34 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.....	101
6.35 SSL VPN 用户接入后对于非法操作如何溯源.....	101
6.36 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.....	101
6.37 SSL VPN 服务器认证场景下的授权规则如何.....	102
6.38 SSL VPN 有哪些常见调试日志.....	104
6.39 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.....	108
6.40 SSL VPN 接入后 Ping 内网延迟大，如何解决.....	111
7 相关资源.....	112

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SecoClient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。

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。

3 SSL VPN 支持列表

SSL VPN 支持接入方式

接入方式	说明
浏览器	用户通过浏览器访问SSL VPN网关（即虚拟网关），在虚拟网关页面上就可以看到企业的资源链接，点击资源链接就可以访问相应资源。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，这4类业务浏览器都支持。
SecoClient	SecoClient是华为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，SecoClient客户端仅支持网络扩展业务。

虚拟网关规格

对于USG6000E的规格，请登录网站，使用[规格查询工具](#)进行查询。其他型号如下所示：

设备型号	最大虚拟网关个数
USG6101/6305/6305-W/6310S/6310S-W/6310S-WL/6510/6510-WL	4
USG6310/6320/6510-SJJ USG6306/6308/6330/6350/6360/6507/6530	64
USG6370/6380/6390/6550/6570 USG6390E/6620/6620-AVE/6630 USG6650/6660/6670	256
NGFW Module	256
USG6680	1024

设备型号	最大虚拟网关个数
USG9500	4096

SSL VPN 用户规格

所有型号的设备都缺省提供了100个最大并发用户数，如果用户想增加最大并发用户数，可以购买License。购买License以后总的最大并发用户数（缺省的100个用户也算在内），不能超过下表中各设备对应的最大并发用户数规格。例如，USG6320支持的最大并发用户数是200个，实际购买License中的最大并发用户数不要超过100个。因为超过100以后，算上缺省的100个，总数就超过了设备规格。

对于USG6000E的规格，请登录网站，使用[规格查询工具](#)进行查询。其他型号如下所示：

设备型号	最大用户数	最大并发用户数
USG6101/6305/6305-W/6310S/6310S-W/6310S-WL/6510/6510-WL	200	100
USG6310/6320/6510-SJJ	400	200
USG6306/6308/6330/6350/6360/6507/6530	1000	500
USG6370/6380/6390/6550/6570	2000	1000
USG6390E/6620/6620-AVE/6630	4000	2000
USG6650/6660/6670/6680	10000	5000
NGFW Module	10000	5000
USG9500	200000	100000

SSL VPN 支持的操作系统和浏览器

SSL VPN业务		支持的操作系统	支持的浏览器及版本
Web代理	<p>Web改写 仅 USG6101/ 6305/6305 -W/6310S/ 6310S-W/ 6310S- WL/ 6510/6510 -WL和 USG6110E /6307E/ 6311E/ 6311E- POE/ 6510E/ 6510E- POE/ 6510E-DK 不支持该 功能。</p>	<p>视浏览器支持的操作系统而定。</p>	<ul style="list-style-type: none"> ● Internet Explorer 6/7/8/9/10/11 (32/64位) ● Firefox 4.0 ~ 30.0 (32位) ● Chrome 10 ~ 20 ● Opera 9.0 ~ 12.0 ● Safari 3.0 ~ 5.1.x
	<p>Web Link</p>	<ul style="list-style-type: none"> ● Windows Server 2003 (32位) ● Windows XP SP1及其以上 (32/64位) ● Windows Vista (32位/64位) ● Windows 7 (32位/64位) ● Windows Server 2008 (32位/64位) ● Windows 8 (32位/64位) ● Windows 8.1 (32位/64位) ● Windows 10 (32位/64位) 	<p>Internet Explorer 6/7/8/9/10/11 (32/64位)</p>

SSL VPN业务	支持的操作系统	支持的浏览器及版本
文件共享	视浏览器支持的操作系统而定。	<ul style="list-style-type: none"> ● Internet Explorer 6/7/8/9/10/11 (32/64位) ● Firefox 4.0 ~ 30.0 (32位) ● Chrome 10 ~ 20 ● Opera 9.0 ~ 12.0 ● Safari 3.0 ~ 5.1.x
端口转发	<ul style="list-style-type: none"> ● Windows Server 2003 (32位) ● Windows XP SP1及其以上 (32/64位) ● Windows Vista (32位/64位) ● Windows 7 (32位/64位) ● Windows Server 2008 (32位/64位) ● Windows 8 (32位/64位) ● Windows 8.1 (32位/64位) ● Windows 10 (32位/64位) 	Internet Explorer 6/7/8/9/10/11 (32/64位)

SSL VPN业务		支持的操作系统	支持的浏览器及版本
网络扩展	浏览器接入	<ul style="list-style-type: none"> Windows Server 2003 (32位) Windows XP SP1及其以上 (32/64位) Windows Vista (32位/64位) Windows 7 (32位/64位) Windows Server 2008 (32位/64位) Windows 8 (32位/64位) Windows 8.1 (32位/64位) Windows 10 (32位/64位) 	<ul style="list-style-type: none"> Internet Explorer 6/7/8/9/10/11 (32/64位) Firefox 38~49 (32位) Firefox 52及以上 (32/64位) Chrome 35及以上 <p>说明 为了满足用户通过Firefox、Chrome浏览器访问网络扩展业务的需要，网络管理员需要在FW的Web界面“系统 > VPN客户端升级”中上传SecoClient软件。同时，在FW的虚拟网关中只允许配置网络扩展业务，且不允许配置证书认证方式。</p> <p>满足以上条件的情况下，用户通过浏览器访问虚拟网关登录页面时，页面上将会提示用户下载并安装SecoClient软件。从V500R005C20和V600R007C00版本开始，设备支持通过Chrome (42及以上)或Firefox (52及以上)访问虚拟网关登录页面，此时用户需要根据浏览器提示安装对应的扩展插件，并安装7.0.2及以上版本的SecoClient软件。SecoClient软件安装完成后，用户刷新登录页面就可以访问网络扩展业务。如果用户当前的操作系统不支持安装SecoClient软件，则用户将无法通过Firefox、Chrome浏览器访问网络扩展业务。</p>
	SecoClient接入	SecoClient客户端支持的操作系统规格由使用的客户端版本决定，如需查询具体规格请使用注册帐号登录网站 http://support.huawei.com/enterprise ，下载最新版本的客户端产品文档。	-

文件共享协议规格

- SMB (CIFS) 协议仅支持32位操作系统。

- NFS协议支持Unix的UID和GID验证。
- NFS v3支持基于UDP的NFS文件共享。
- SMB (CIFS) 协议支持签名特性，即SMB类型的文件共享资源需要输入用户名和密码成功登录后才可以访问。

其他规格

- FW支持的SSL协议版本：TLS 1.0、TLS 1.1、TLS 1.2。
- 一个虚拟网关可以创建63个自定义角色和一个默认角色。
- 一个自定义角色最多关联256个用户和用户组，默认角色无限制。
- 一个自定义角色关联的最大资源数为1024，默认角色可以关联的最大资源数与虚拟网关最大允许资源数相同。
- 一个角色最多关联128条主机检查策略。

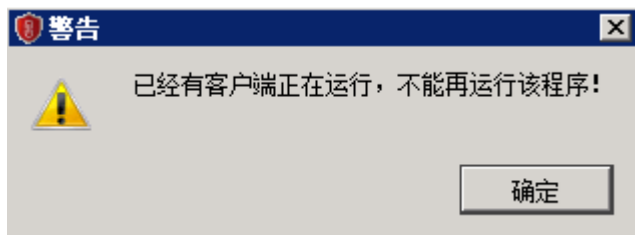
4 SecoClient 拨号 SSL VPN 故障

4.1 打开 SecoClient 时出现警告

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SecoClient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SecoClient在运行。

处理步骤

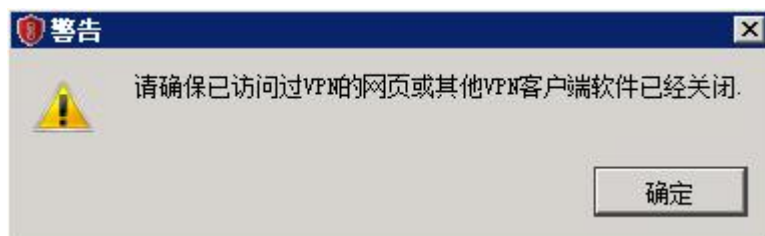
1. 关闭已有的SecoClient运行程序以及使用了SSL VPN业务的浏览器。
2. 检查任务管理器中的SecoClient.exe进程是否已同步关闭，如果没有，请选中SecoClient.exe进程，然后单击“结束进程”。



4.1.2 警告：请确保已访问过 VPN 的网页或其他 VPN 客户端软件已经关闭。

现象描述

打开SecoClient时，系统告警“请确保已访问过VPN的网页或其他VPN客户端软件已经关闭”。



可能原因

1. 终端上已经有IE内核的浏览器登录了SSL VPN。

2. 终端上已经有SVNClient（老的SSL VPN客户端）登录了SSL VPN。

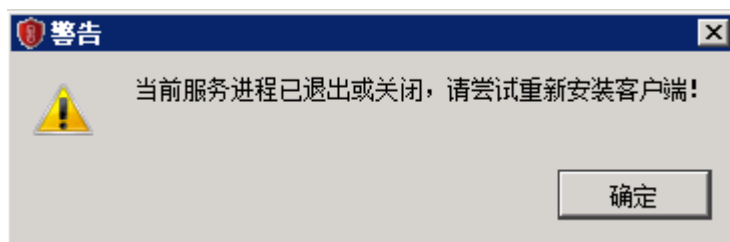
处理步骤

检查终端上是否已经有IE内核的浏览器或SVNClient登录了SSL VPN。如果存在，请从浏览器登录SSL VPN的主页中注销，或退出SVNClient程序，然后再打开SecoClient。

4.1.3 警告：当前服务进程已退出或关闭，请尝试重新安装客户端！

现象描述

打开SecoClient时，系统告警“当前服务进程已退出或关闭，请尝试重新安装客户端！”。



可能原因

SecoClient服务未开启。

处理步骤

1. 在“开始 > 运行”中，输入services.msc命令，单击“确定”，进入“服务”界面。
2. 在“名称”一列中，查看“SecoClientService”的状态，如果对应状态为空白，则表示“SecoClientService”服务未启用。

Remote Procedure Call (RPC)	RPC...	已启动	自动	网络服务
Remote Procedure Call (RPC) ...	在...		手动	网络服务
Remote Registry	使...	已启动	自动	本地服务
Resultant Set of Policy Prov...	提...		手动	本地系统
Routing and Remote Access	在...		禁用	本地系统
RPC Endpoint Mapper	解...	已启动	自动	网络服务
SecoClientService			自动	本地系统
Secondary Logon	在...	已启动	手动	本地系统
Secure Socket Tunneling Prot...	提...	已启动	自动	本地服务
Security Accounts Manager	启...	已启动	自动	本地系统
Server	支...	已启动	自动	本地系统
Shell Hardware Detection	为...	已启动	自动	本地系统
Smart Card	管...		手动	本地服务
Smart Card Removal Policy	允...		手动	本地系统
SNMP Trap	接...		手动	本地服务
Software Protection	启...	已启动	自动 (延...	网络服务

请在该服务上右键单击，在弹出的菜单中选择“启用”。

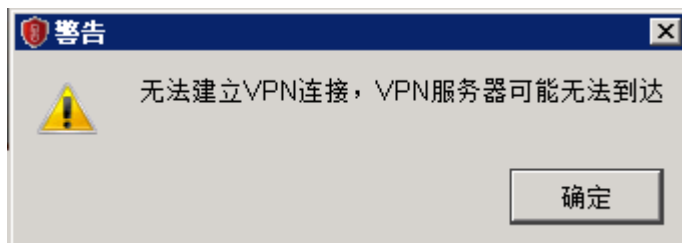


3. 重新打开SecoClient，已无告警。

4.1.4 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. SecoClient到VPN网关的路由不可达。
2. SecoClient上VPN网关的IP地址或端口填写错误。
3. SecoClient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proxy.huawei.com），SecoClient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。
 - a. 在SecoClient所在的终端上Ping VPN网关的IP地址，检查路由是否可达。
 - b. 如果路由不可达，请配置SecoClient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SecoClient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SecoClient配套的VPN网关软件版本有FW V500R001C20、FW V100R001C30SPC900、SVN V200R003C10SPC900，及其它它们之后的版本。它们之前的版本和SecoClient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，SecoClient也需要配置代理参数，如下图。



4.1.5 警告：获取系统代理失败！

现象描述

单击SecoClient主界面上的“代理设置”，选择“代理类型”为“使用系统代理”，系统提示“获取系统代理失败”。



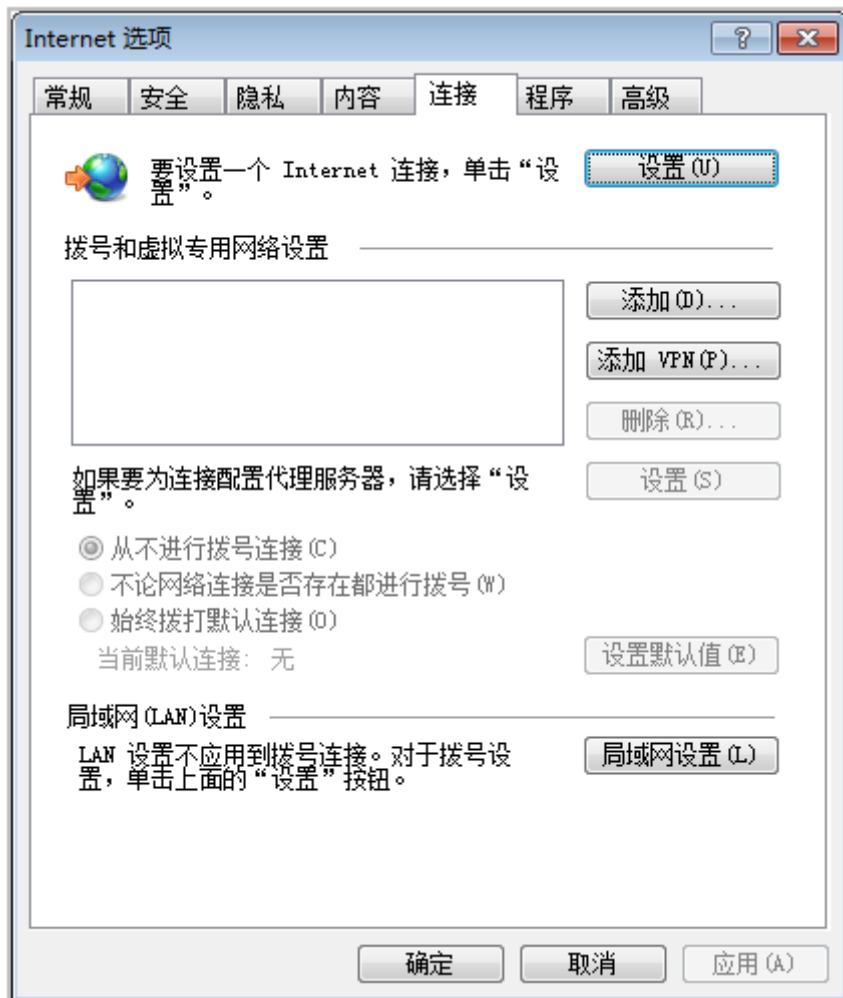
可能原因

用户浏览器中未设置代理。

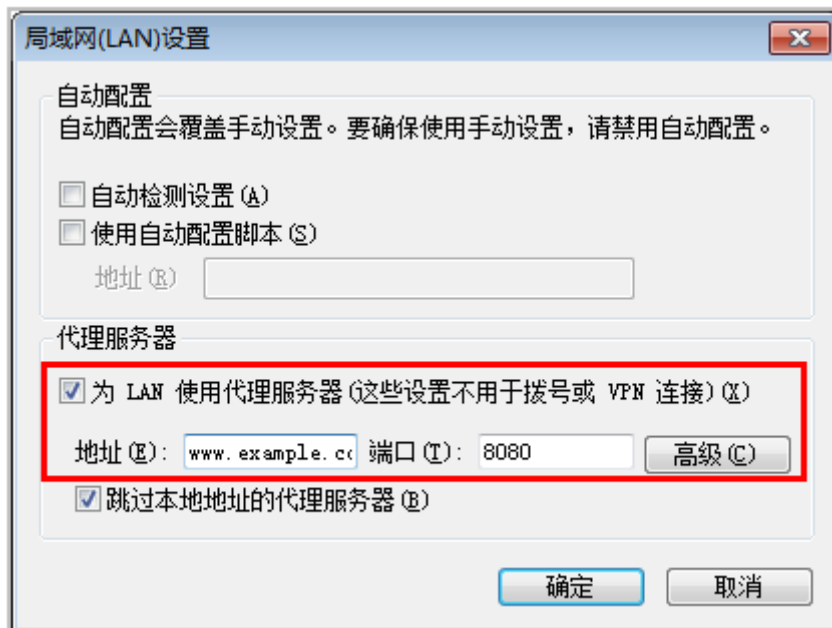
处理步骤

SecoClient在“代理类型”中选择“使用系统代理”，这表示SecoClient的代理配置将使用浏览器中的代理信息。此处出现该提示，则表示用户浏览器中并未设置代理。

1. 打开IE浏览器，在浏览器右上角选择“工具 > Internet选项”，并在弹出的窗口中选择“连接”页签。



2. 单击“局域网设置”，并设置代理服务器。此处假设代理服务器地址为 www.example.com，端口为8080。然后，单击“确定”。



3. 再次打开SecoClient，并选择“代理类型”为“使用系统代理”时，就会看到刚才在浏览器中设置的地址和端口，现在已在SecoClient中显示。这里账号和密码需要向代理服务器管理员获取。

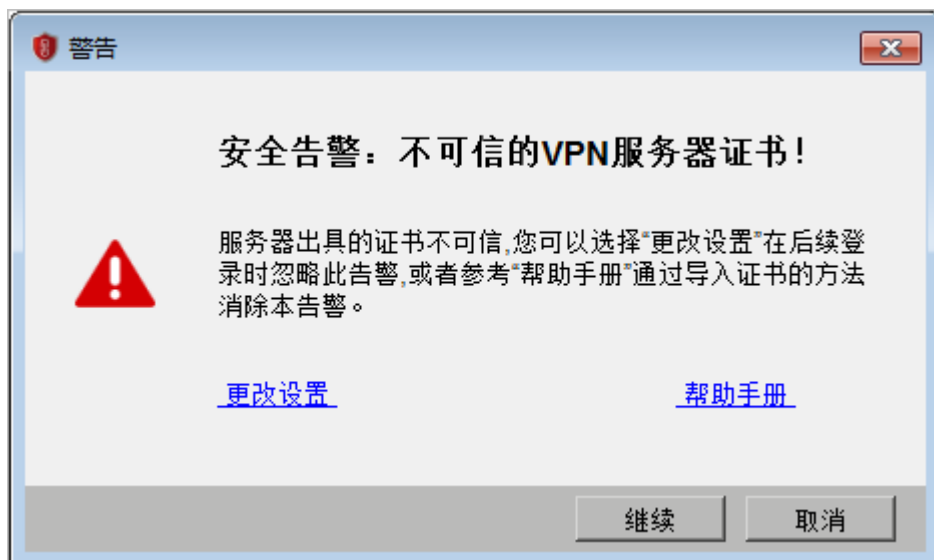


4.2 采用用户名/密码方式登录时出现警告

4.2.1 警告：不可信的 VPN 服务器证书！

现象描述

用户使用SecoClient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

SecoClient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“更改设置”，去勾选“阻塞到不可信服务器的连接”。
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SecoClient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SecoClient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。
SecoClient通过SSL VPN隧道登录虚拟网关时，虚拟网关会向SecoClient推送设备证书，只要SecoClient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](#)。

4.2.2 警告：认证失败！

现象描述

在SecoClient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

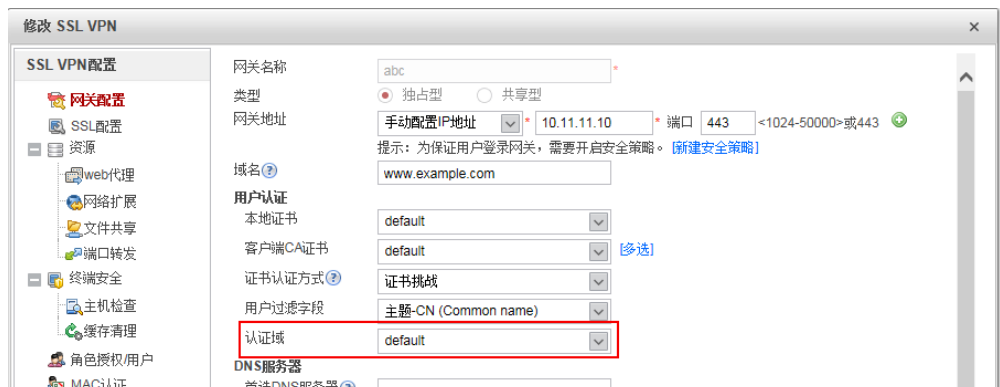
1. 用户名或密码错误，用户过期或用户被锁定。
2. 虚拟网关绑定了不正确的认证域。
3. 认证域未启用SSL VPN接入场景。
4. 虚拟网关未启动网络扩展特性。
5. SSL VPN登录的设备处于双机备状态（HRP_S），而SSL VPN不支持在备设备上登录上线。
6. SSL VPN虚拟网关是共享型，非独占型。
7. 认证域采用服务器认证，新用户认证选项配置了“不允许新用户登录”，但用户在本地不存在。
8. 认证域采用AD/LDAP服务器认证，服务器上配置用户的属性启用了“首次登录必须修改密码”。

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 huawei001
2021-03-30 14:51:04.970 +08:00
Current total number: 1
-----
User Name       : huawei001
Password Config : Yes
Password       : OW7Q30GINMDu2NS8ufuBIAAAAAALKhc4
Parent Group    : /default
Bind Mode      : Unidirectional
State          : Locked
Expiration Time : Unlimited
Multi-IP Login  : Enabled
User Type      : Created By Manager
Vsys           : public
-----
```

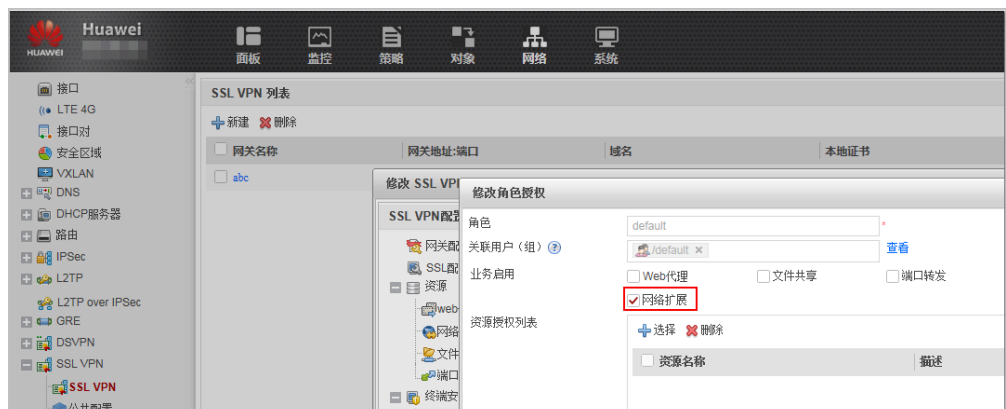
2. 检查虚拟网关是否绑定了认证域，如果有绑定，是否绑定了正确的认证域。



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
```

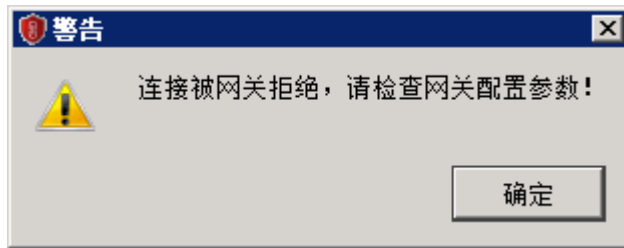
8. 登录AD/LDAP服务器，查看用户的属性是否启用了“首次登录必须修改密码”，如果启用，则去勾选以下红色框选项。



4.2.3 警告：连接被网关拒绝，请检查网关配置参数！

现象描述

在SecoClient登录界面，输入用户名和密码以后，单击“登录”，系统告警“连接被网关拒绝，请检查网关配置参数！”。

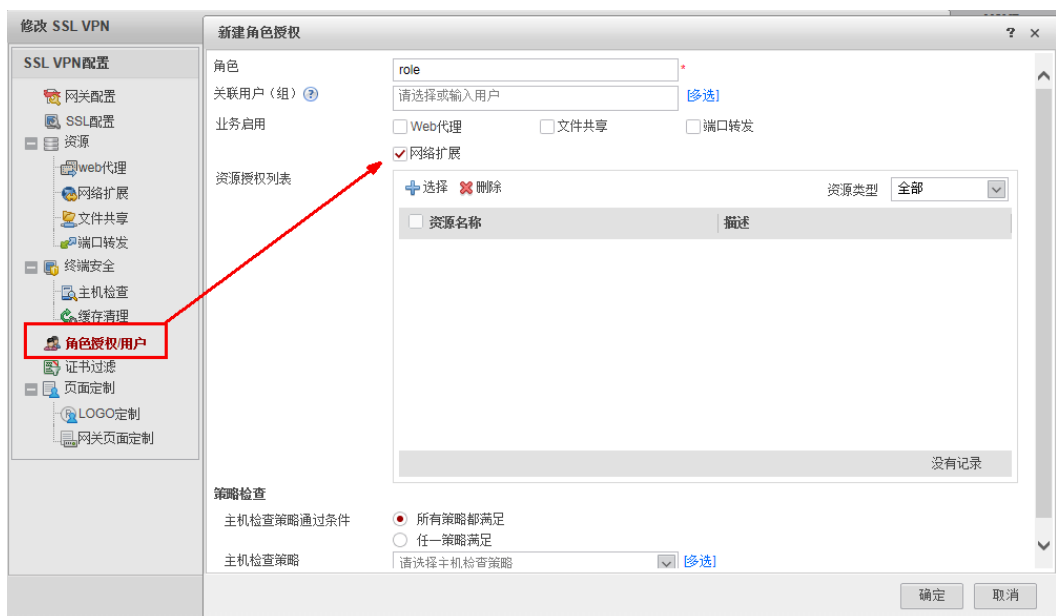


可能原因

虚拟网关网络扩展特性已启用，但是用户所属的角色未启用网络扩展业务。

处理步骤

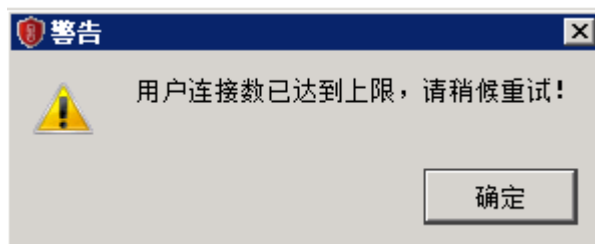
请勾选虚拟网关下“角色授权/用户”中的“网络扩展”业务，然后单击“确定”。



4.2.4 警告：用户连接数已达到上限，请稍后重试！

现象描述

在SecoClient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。

The screenshot shows the 'Modify SSL VPN' configuration window. The 'Maximum concurrent users' field is highlighted with a red box and set to 50. The 'Maximum number of users' field is set to 10. The 'Maximum resources' field is set to 1024. The 'Allow one account to log in at multiple locations simultaneously' checkbox is unchecked.

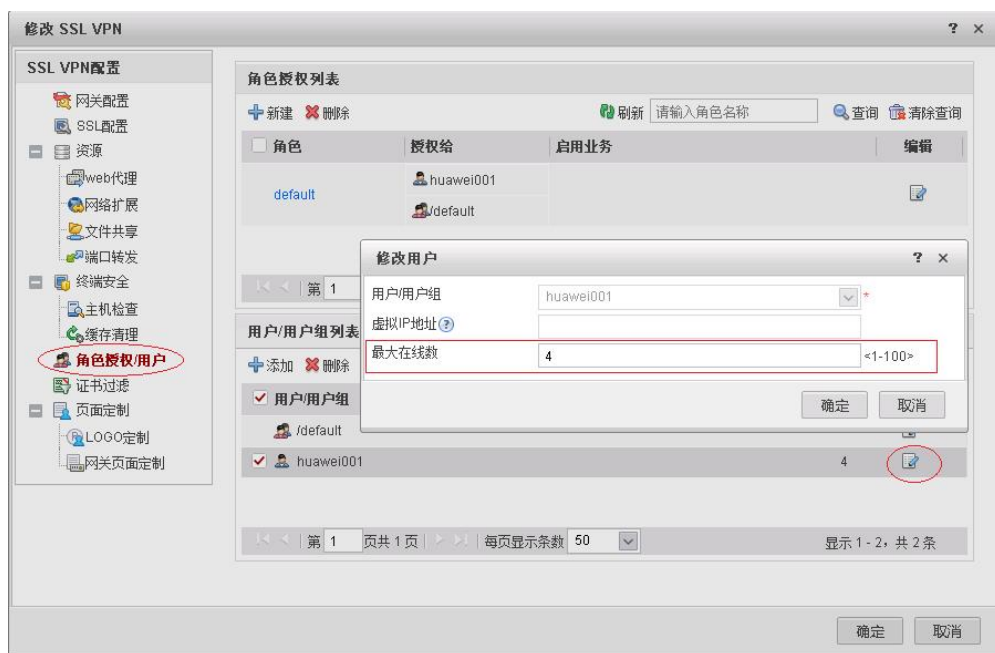
Field	Value	Range
快速通道端口号	443	<1-49999>
最大用户数	10	<1-1000>
最大并发用户数	50	<1-100>
最大资源数	1024	<1-1024> (系统总资源: 12800, 剩余: 11776)

- 原因2的问题定位及解决方法。

检查虚拟网关是否启用了“允许一个账号在多处同时登录”。



如果启用，则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。



4.2.5 警告：网络扩展启动失败！

现象描述

在SecoClient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]**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    huawei002     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
```

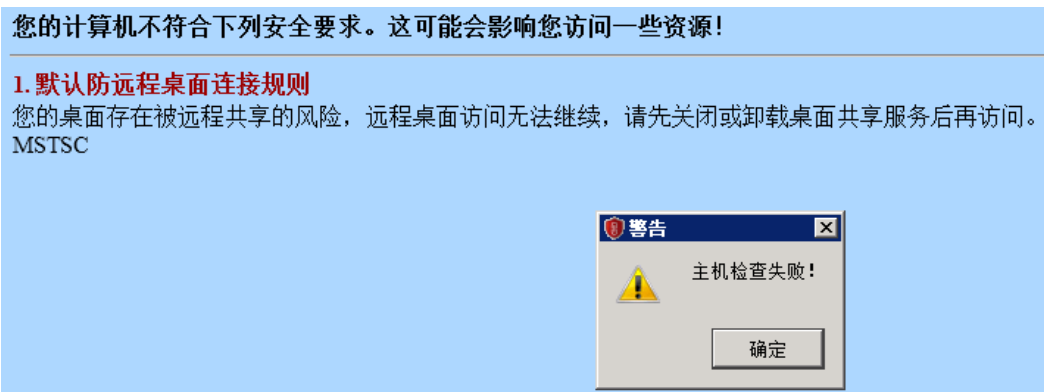
```
Keep Alive State:      enable
Keep Alive Interval:   120(seconds)
Log State:             disable
Point to Point State:  disable
VIP Method:          external server assign
default net pool:      3.3.3.100
Route Mode:           manual
Intranet IP/Mask:     3.3.3.0/255.255.255.0
Intranet IP/Mask:     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]
```

4.2.6 警告：主机检查失败！

现象描述

在SecoClient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。

4.2.7 警告：接收返回码超时！

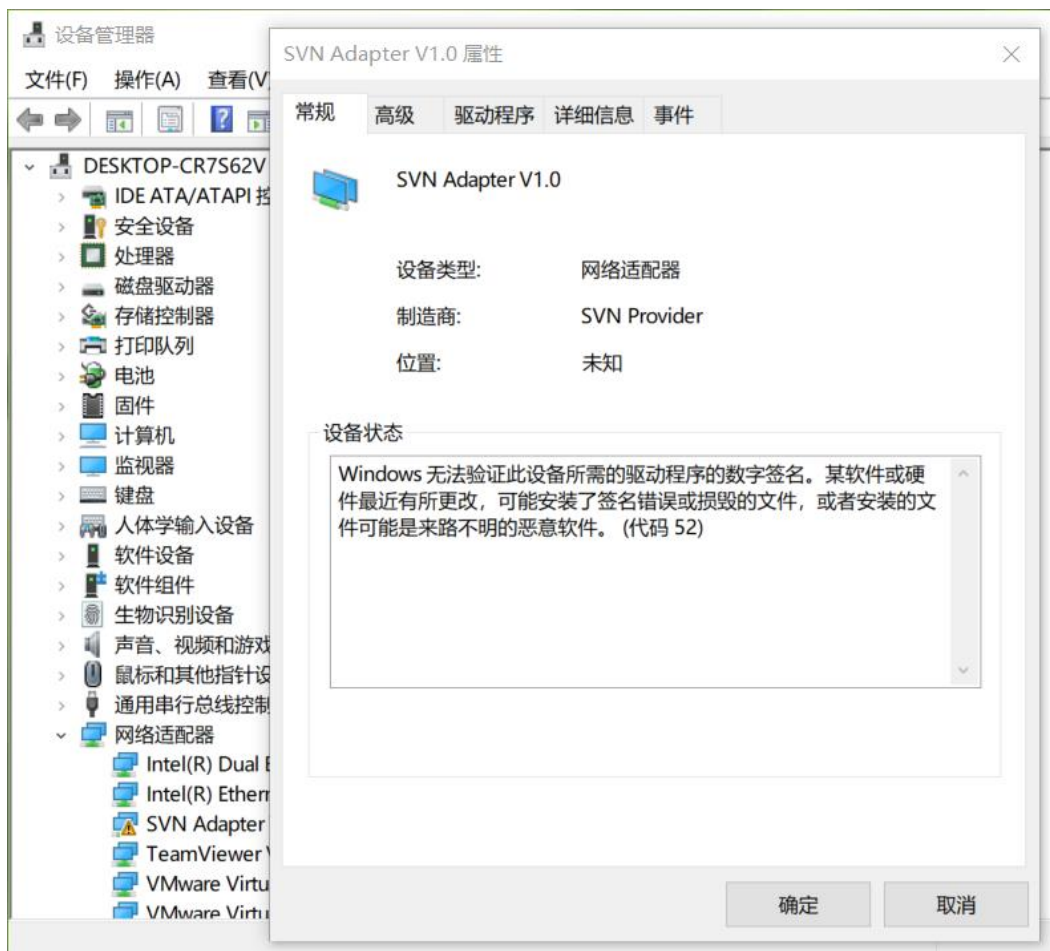
现象描述

在SecoClient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！”。



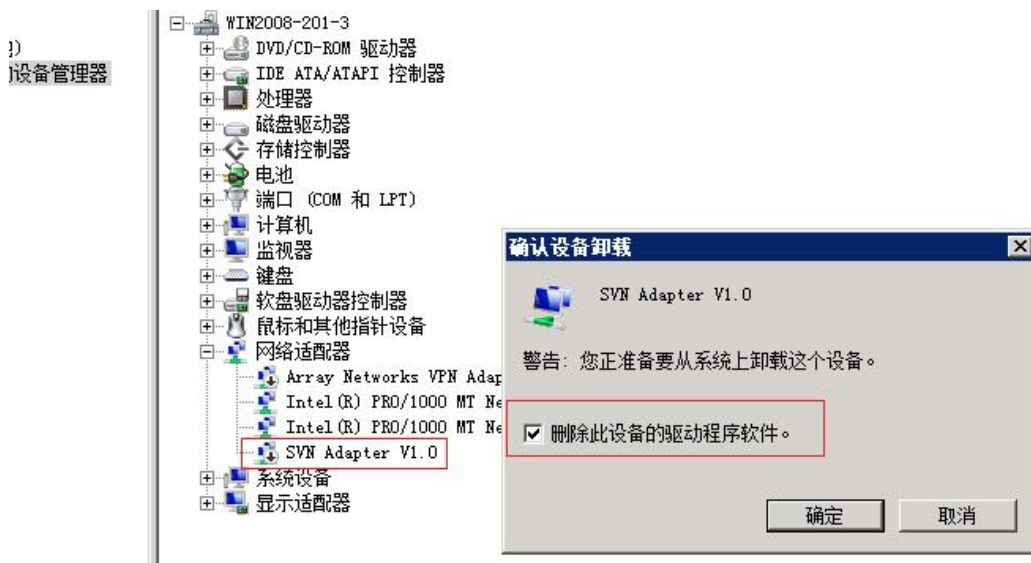
可能原因

虚拟网卡驱动程序安装失败，操作系统不能识别虚拟网卡。



处理步骤

完全卸载SecoClient（含虚拟网卡驱动程序），使用最新版本的SecoClient安装包重新安装。



4.2.8 警告：UDP 隧道建立失败，请选择其它模式登录

现象描述

在SecoClient登录界面，输入用户名和密码以后，单击“登录”，系统告警“UDP隧道建立失败，请选择其它模式登录。”。



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. SecoClient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。

4.3 采用证书方式登录时出现警告

4.3.1 找不到用户证书

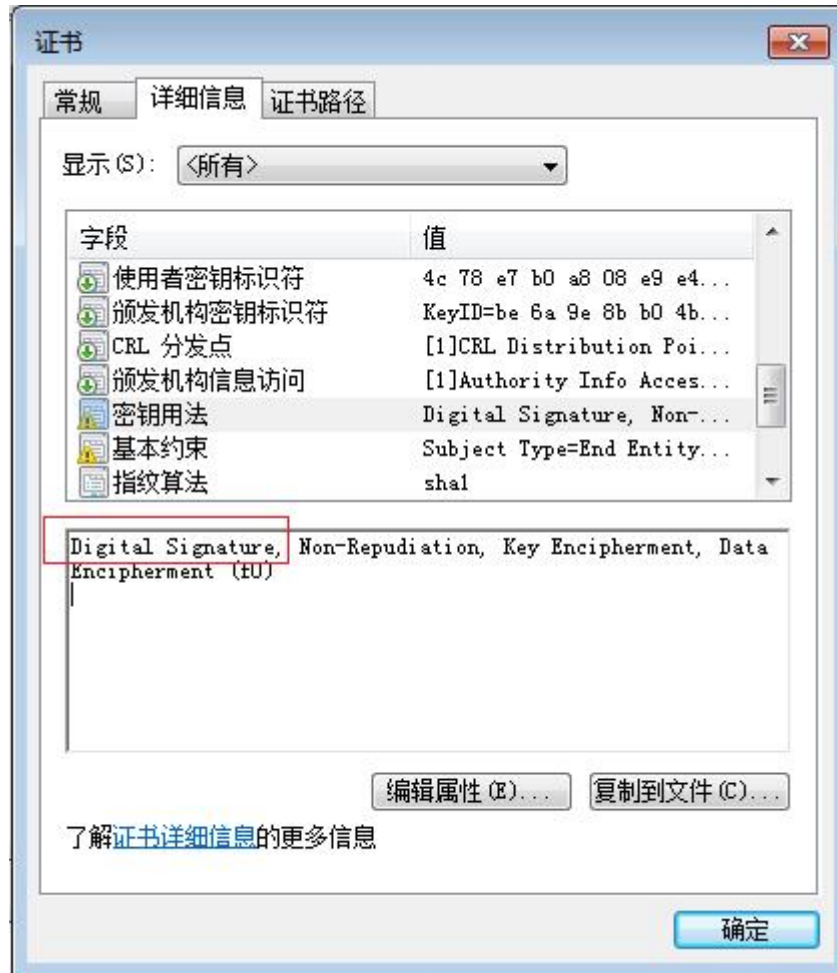
现象描述

在虚拟网关采用证书认证的情况下，在SecoClient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）。



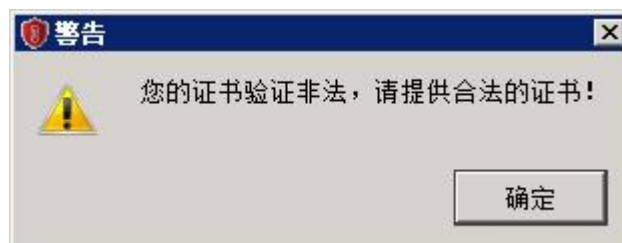
处理步骤

重新制作一本密钥用法带“数字签名”的用户证书。

4.3.2 警告：您的证书验证非法，请提供合法的证书！

现象描述

在SecoClient登录界面，选择用户证书，单击“登录”，系统告警“您的证书验证非法，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限范围之内。



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。

4.3.3 警告：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SecoClient登录界面，选择用户证书，单击“登录”，系统告警“认证失败！”。



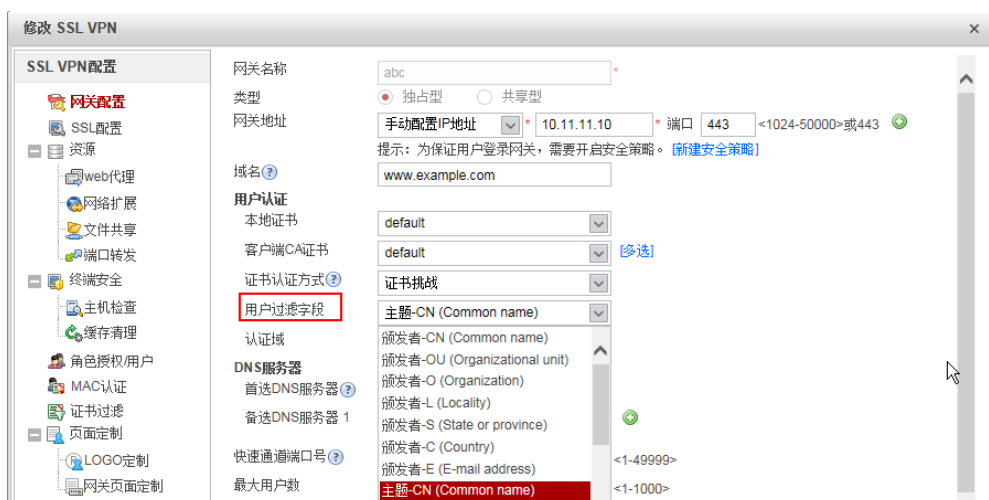
可能原因

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。

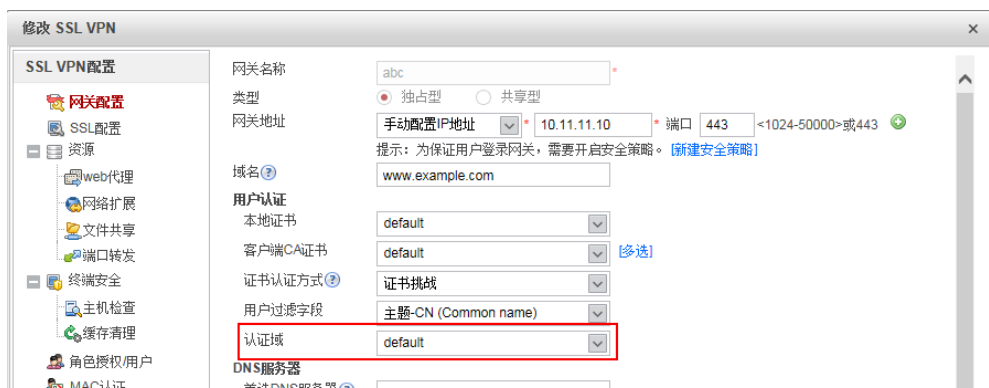
4. 虚拟网关未启动网络扩展特性。
5. SSL VPN登录的设备处于双机备状态（HRP_S），而SSL VPN不支持在备设备上登录上线。

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。



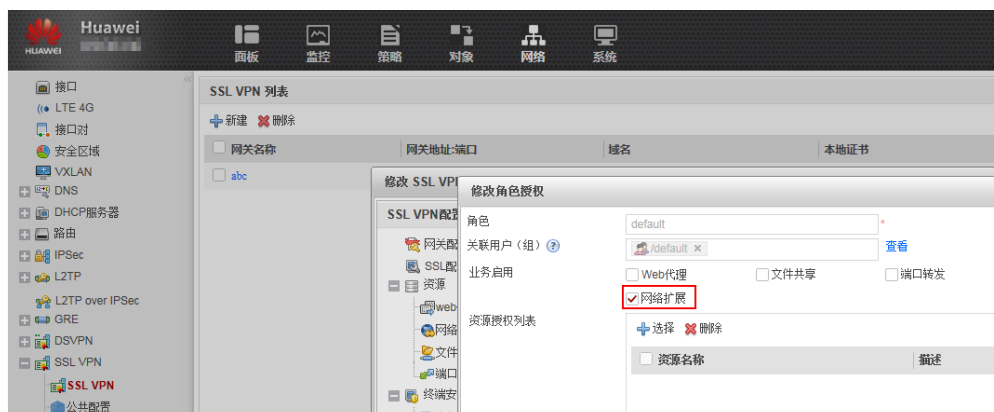
2. 检查虚拟网关是否绑定了认证域，如果有绑定，是否绑定了正确的认证域。



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。



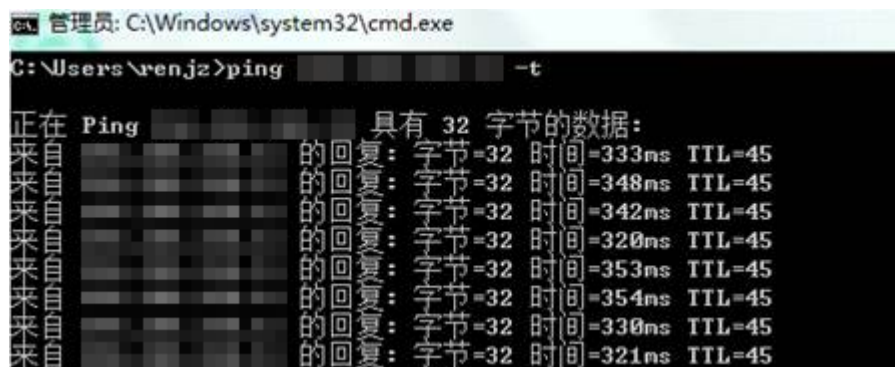
5. 调整配置或组网，确保SSL VPN登录的设备处于双机主状态（HRP_M）。

4.4 登录成功后业务出现异常

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. 将“隧道模式”选择为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，SecoClient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，SecoClient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SecoClient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。



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，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，这个模式通过Web无法配置。

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。



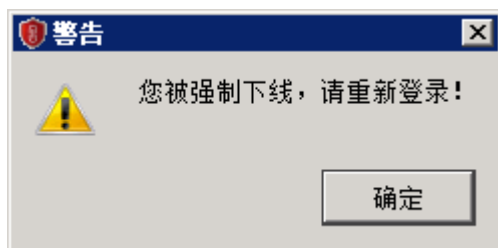
处理步骤

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。

4.4.3 警告：您被强制下线，请重新登录！

现象描述

SecoClient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。

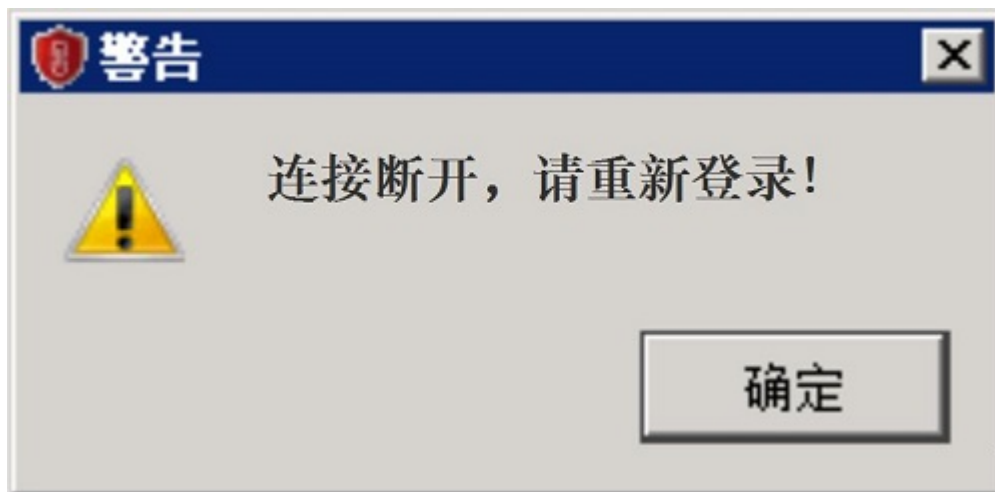
处理步骤

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。

4.4.4 警告：连接断开，请重新登录！

现象描述

SecoClient登录成功，运行一段时间，系统告警“连接断开，请重新登录！”。



可能原因

1. 终端和防火墙中间的链路出现故障。
2. 防火墙或中间链路设备启用了HTTPS攻击防范，且阈值配置低，阻断了真实交互的报文。

处理步骤

1. 排查中间链路。可以尝试换一个拨号环境，测试是否存在相同的问题。
2. 检查防火墙是否配置了HTTPS攻击防范，如果有配置，检查Logbuffer是否有记录丢弃SSL VPN业务报文的日志。

```
[sysname] display logbuffer sec-log | incl x.x.x.x:443 //x.x.x.x表示虚拟网关IP地址
%2018-03-23 12:07:19 SVN5630 %%01SEC/4/ATCKDF(l): AttackType="Https flood attack", slot="0",
receive interface="GE1/0/0 ", proto="TCP", src="1.1.1.1:35042 10.1.1.1:5160 10.1.1.2:41159
10.1.1.3:29902 10.1.1.4:5135 10.1.1.5:27279 10.1.1.6:39425 10.1.1.7:2113 ", dst="x.x.x.x:443 ", begin
time="2018-03-23 12:06:54", end time="2018-03-23 12:07:18", total packets="23", max speed="256",
User="", Action="discard".
```

4.4.5 提示：无法建立 VPN 连接，VPN 服务器可能无法到达

现象描述

移动终端通过SecoClient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

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7.0.2.26及其之后版本的SecoClient才能正常登录虚拟网关。

对于7.0.2.26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。

4.4.6 移动终端启动网络扩展不成功，PC端可以成功

现象描述

移动终端启动网络扩展不成功，PC端可以成功。

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

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7.0.2.26及其之后版本的SecoClient才能正常登录虚拟网关。

对于7.0.2.26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。

4.4.7 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
```

- SecoClient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:239-268435696 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) mquid(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CUT_REQ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，请联系华为技术支持工程师。
2. 在防火墙配置源NAT策略。

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。

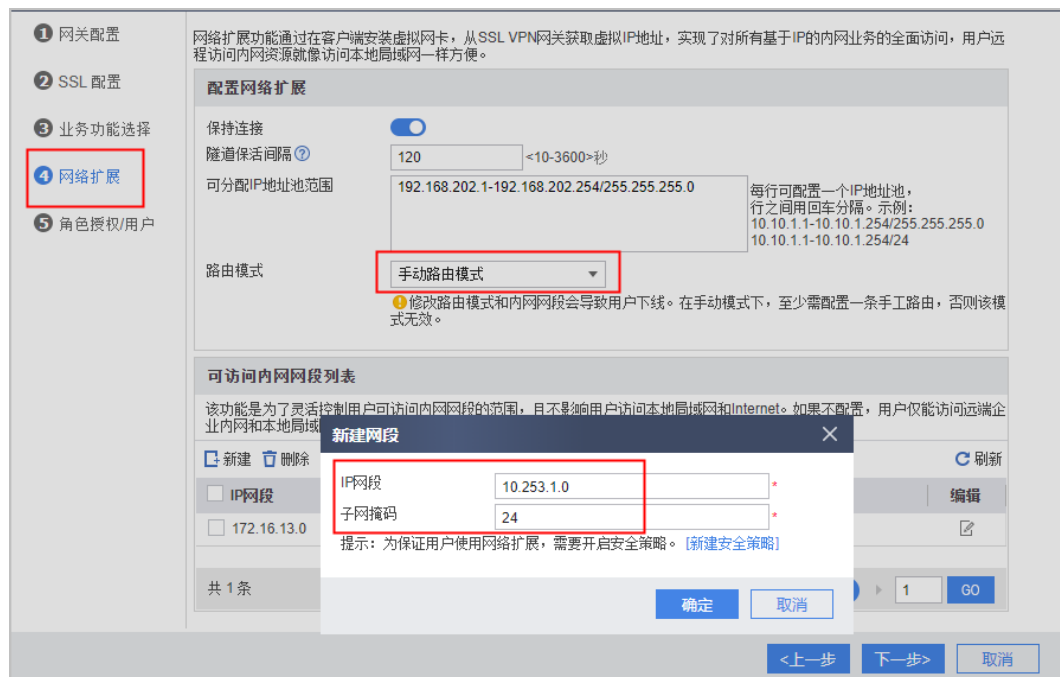
假设SSL VPN用户的虚拟地址为10.2.0.0/16，AD域控制器的地址为10.10.10.3。



4.4.8 新增 SSL VPN 网络扩展可访问网段后，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，如果存在请联系华为技术支持工程师。

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

IPv4路由表

活动路由:

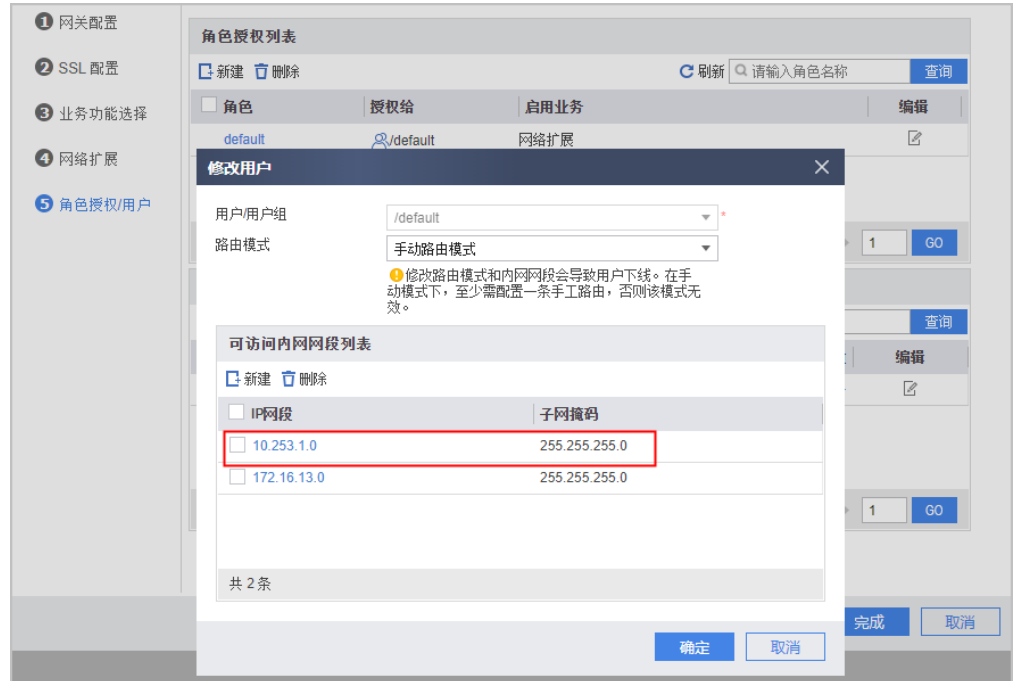
网络目标	网络掩码	网关	接口	跃点数
0.0.0.0	0.0.0.0	10.174.104.1	10.174.105.158	25
10.174.104.0	255.255.252.0	在链路上	10.174.105.158	281
10.174.105.158	255.255.252.255	在链路上	10.174.105.158	281
10.174.105.255	255.255.252.255	在链路上	10.174.105.158	281

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。

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。



3. 在用户组下新增可访问内网网段。



4. 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

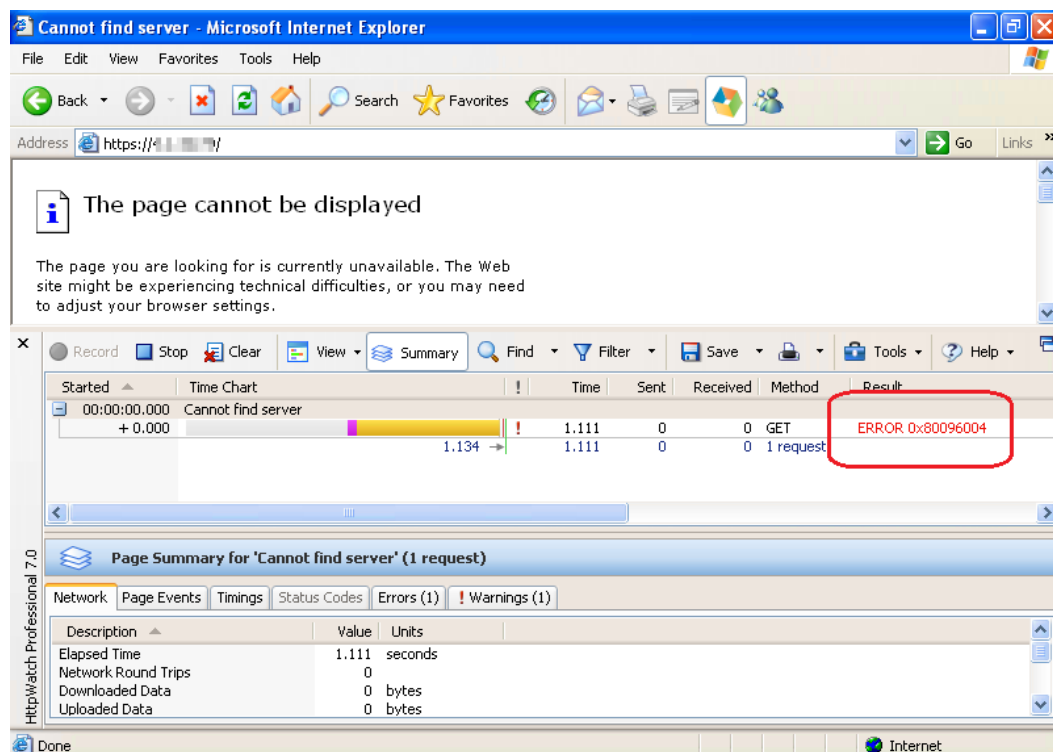
5 浏览器拨号 SSL VPN 故障

5.1 Windows + IE/浏览器兼容模式

5.1.1 浏览器提示：无法打开此页面

现象描述

Windows XP/2003操作系统下，使用浏览器访问SSL虚拟网关时，提示“无法打开此页面”。



可能原因

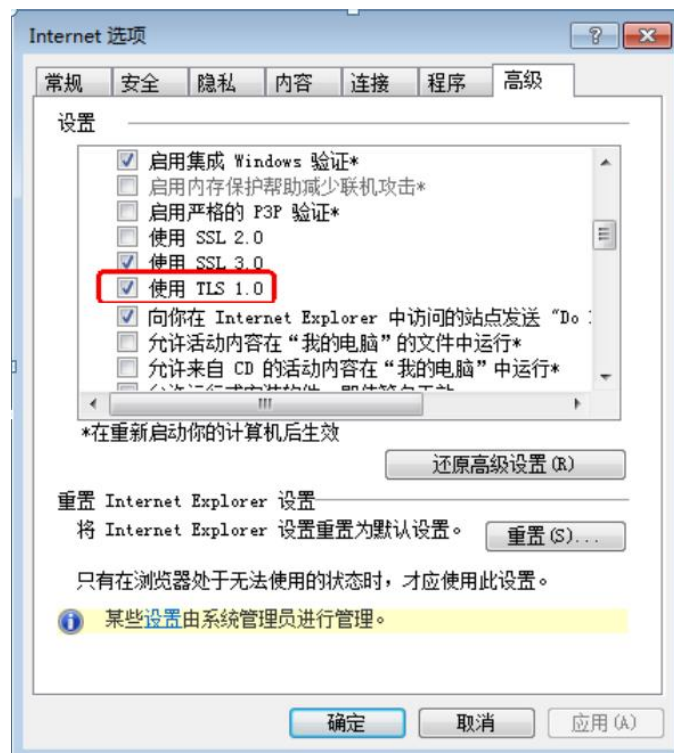
Windows XP/2003操作系统默认不启动TLS协议，也不支持AES加密算法和SHA2认证算法。

处理步骤

1. 对于XP SP3操作系统。

在浏览器上勾选上TLS1.0选项，另外虚拟网关上也要需启用TLS1.0协议，并启用des-cbc3-sha或des-cbc-sha加密套件。

以IE浏览器为例，打开IE浏览器，在浏览器右上角选择“Internet选项”，然后选择“高级”页签。

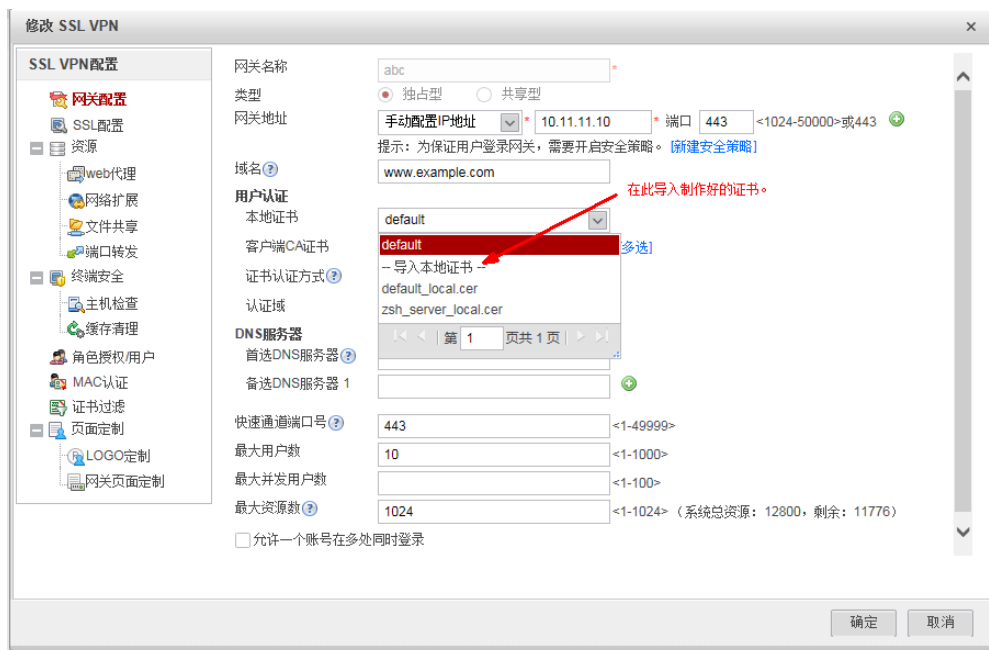


同时，在虚拟网关上也勾选上TLS1.0和对应的加密套件。



2. 对于XP SP2及SP2以下的操作系统。

制作一本sha1WithRSAEncryption签名算法的服务器证书，导入虚拟网关作为设备证书。



5.1.2 浏览器提示：此网站的安全证书存在问题

现象描述

打开浏览器访问SSL VPN网关地址，浏览器提示“此网站的安全证书存在问题”。



可能原因

1. 终端没有安装虚拟网关本地证书对应的CA证书。
2. 虚拟网关本地证书的通用名与访问虚拟网关的IP地址或域名不一致。

处理步骤

可以通过如下两种方法申请或制作本地证书和CA证书，并将本地证书和CA证书导入到防火墙中。

方法一：使用证书制作工具（如xca），制作本地证书和CA证书，在制作本地证书时，必须将Common name字段设置为虚拟网关的IP地址或域名。CA证书需要安装在终端上，才能消除证书安全告警。

方法二：向知名证书颁发机构申请本地证书。可以向证书颁发机构提供虚拟网关的IP地址或域名，用于颁发本地证书，也可以在防火墙上制作证书请求，并拿此证书请求文件去申请本地证书。制作证书请求时，“公用名”必须设置为虚拟网关的IP地址或域名。

5.1.3 浏览器提示：您的证书验证非法，请提供合法的证书

现象描述

虚拟网关配置证书认证。在SSL VPN登录页面选择用户证书，单击“登录”，页面提示“您的证书验证非法，请提供合法的证书！”。

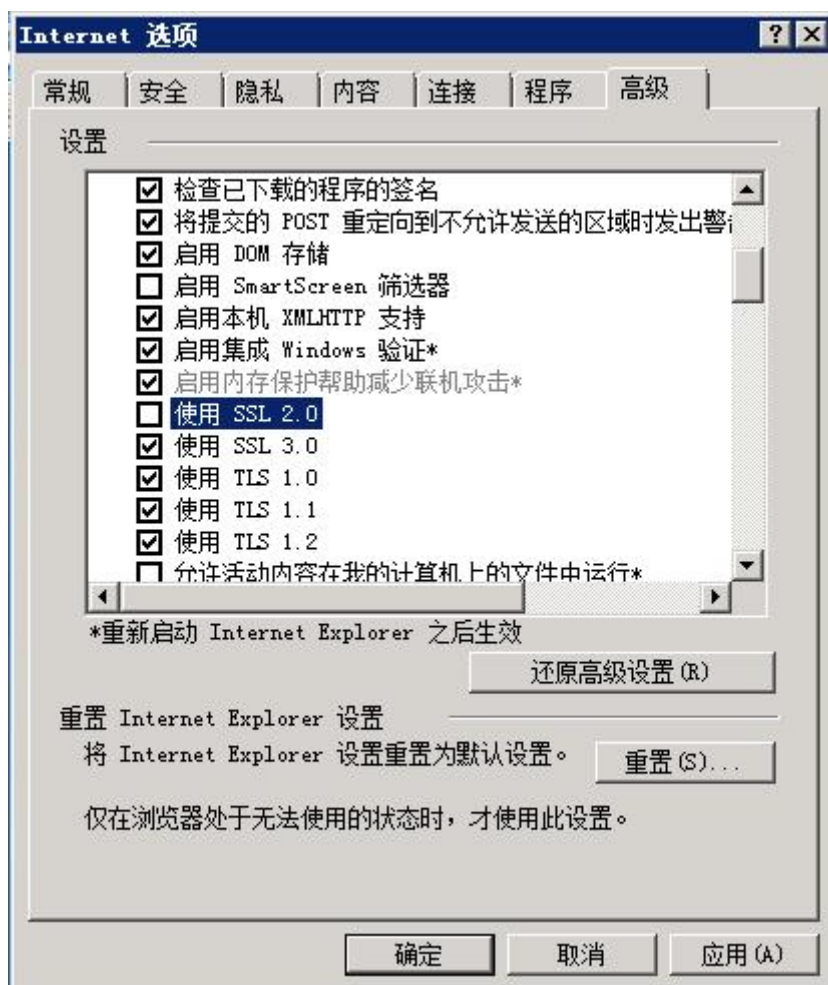


可能原因

1. 用户IE浏览器中的SSL协议启用了SSL 2.0。
2. 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。
3. 安装在终端上的用户证书，没有携带私钥信息。
4. 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。
5. 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. 禁用用户IE浏览器的SSL协议“SSL 2.0”。



2. 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。
3. 检查用户证书，是否有对应的私钥。



4. 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。
5. 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。如果开启了CRL验证功能，但是没有配置CRL，证书认证也会失败。

5.1.4 浏览器提示：应用程序正常初始化（0xc0150002）失败

现象描述

用户在Windows XP/Server 2003/VISTA操作系统下，使用浏览器登录SSL VPN，系统提示“SVNMgr.exe应用程序初始化（0xc0150002）失败”。



可能原因

1. XP/Server 2003操作系统没有自带VS2005运行库，需要安装指定的运行库才能运行SVN客户端控件。

2. VISTA操作系统不能运行自带的VS2008运行库，需要安装指定的运行库才能运行SVN客户端控件。

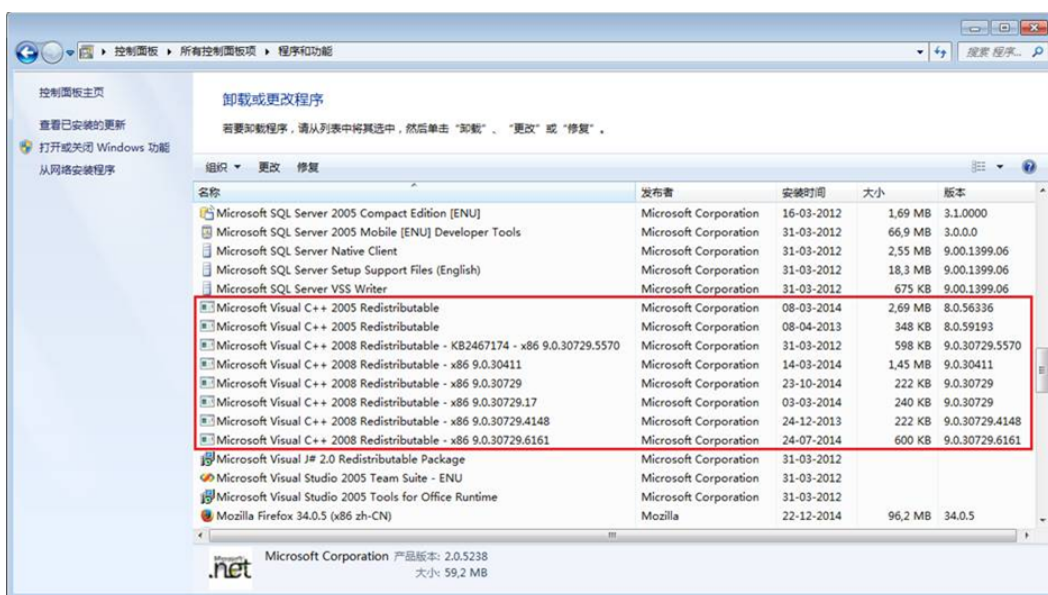
处理步骤

XP/Server 2003 64位操作系统需要安装Microsoft Visual C++ 2005 Redistributable X64运行库。

XP/Server 2003 32位操作系统需要安装Microsoft Visual C++ 2005 Redistributable X86运行库。

VISTA 64位操作系统需要安装Microsoft Visual C++ 2008 Redistributable X64运行库。

VISTA 32位操作系统安装Microsoft Visual C++ 2008 Redistributable X86 运行库。



5.1.5 虚拟网关的登录页面停留在转圈画面

现象描述

用户使用IE浏览器访问SSL VPN虚拟网关，登录页面无法正常显示，停留在转圈画面中，如下图。



可能原因

客户端控件被IE浏览器安全设置阻断。

处理步骤

将虚拟网网关的URL加入“Internet选项 > 安全 > 受信任站点”。



5.1.6 虚拟网关登录页面无法选择到用户证书

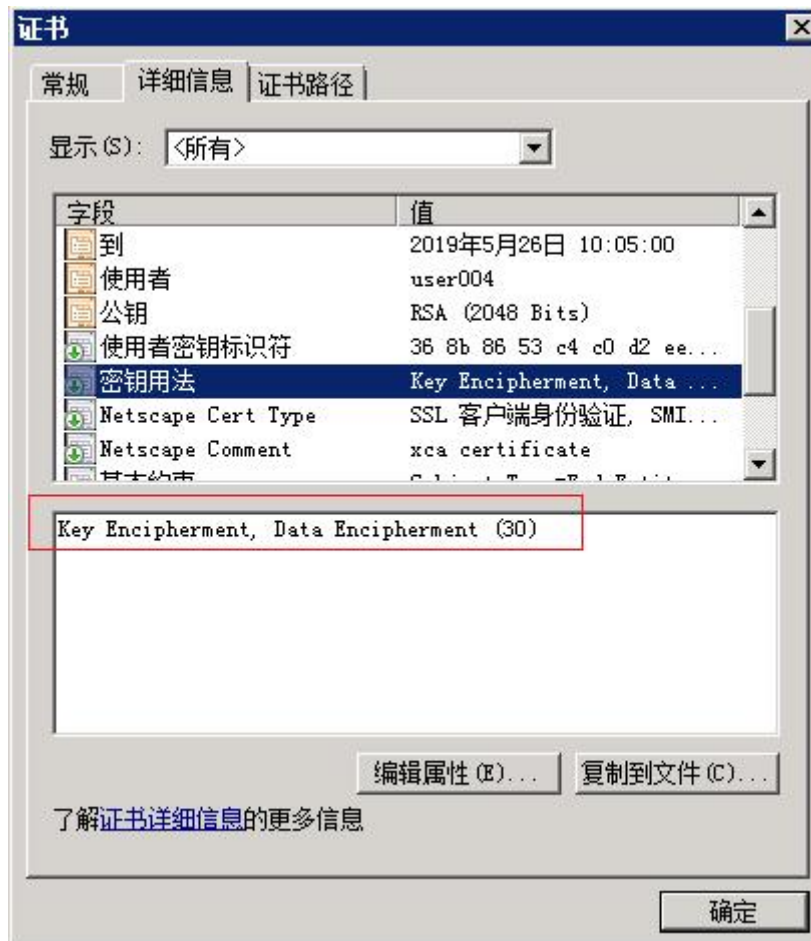
现象描述

在虚拟网关采用证书认证的情况下，用户在 SSL VPN 虚拟网关登录页面，无法找到预期的用户证书。



可能原因

1. 用户证书的密钥用法没有包含“Digital Signature”（数字签名）。



2. USB-Key驱动程序存在问题。
3. 终端系统时间不在用户证书的有效期范围内。
4. 防火墙SSL VPN配置了客户端证书过滤（符合指定条件的用户证书才会显示在SSL VPN登录页面上）。
5. 使用了非IE内核的浏览器访问SSL VPN。

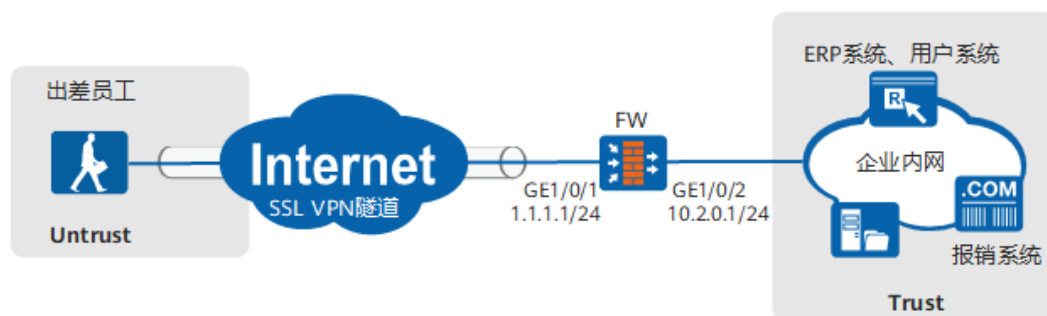
处理步骤

1. 重新制作一本密钥用法带“数字签名”的用户证书。
2. 重装USB-Key驱动程序。
3. 检查终端系统时间，是否在用户证书的有效期范围内。
4. 检查防火墙虚拟网关配置，是否配置了客户端证书过滤。
5. 检查是否使用IE内核的浏览器访问的SSL VPN。

5.1.7 用户访问 Web-link 资源失败

现象描述

企业网络如下图所示，出差员工通过SSL VPN访问公司内部的服务器。ERP系统中存在两个子链接，分别链接到用户系统和报销系统。



在防火墙上配置ERP系统站点的Web-Link资源，测试SSL VPN登录后，能看到这条资源，点击可以打开ERP系统，但点击子链接无法打开用户系统和报销系统。

ERP系统链接：<http://10.2.0.10:8080>

用户系统链接：<http://10.2.0.10:8081>

报销系统链接：<http://10.2.0.11>

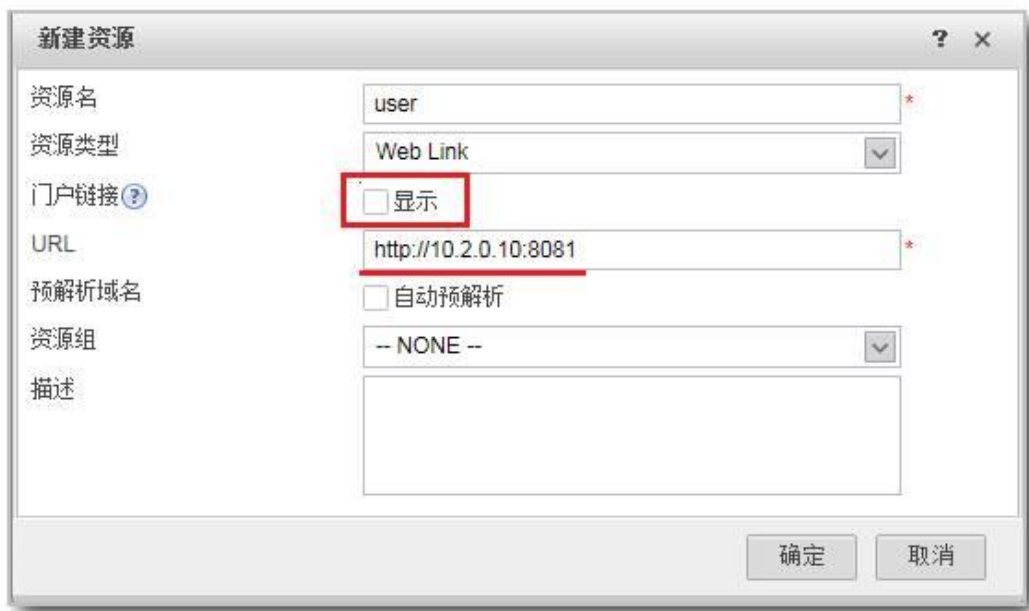
可能原因

Web-link采用端口转发的技术实现，最小限度放行公网对内网服务器的访问权限（保护内网的安全性）。仅当用户访问内网站点的URL和配置Web-Link资源的URL相同或属于其子集时，报文才会被Web-Link控件截获走VPN隧道。例子中配置Web-Link资源的URL为<http://10.2.0.10:8080>，这种情况下访问<http://10.2.0.10:8081>和<http://10.2.0.11>的报文都会因为不匹配Web-Link资源URL而不走VPN隧道。

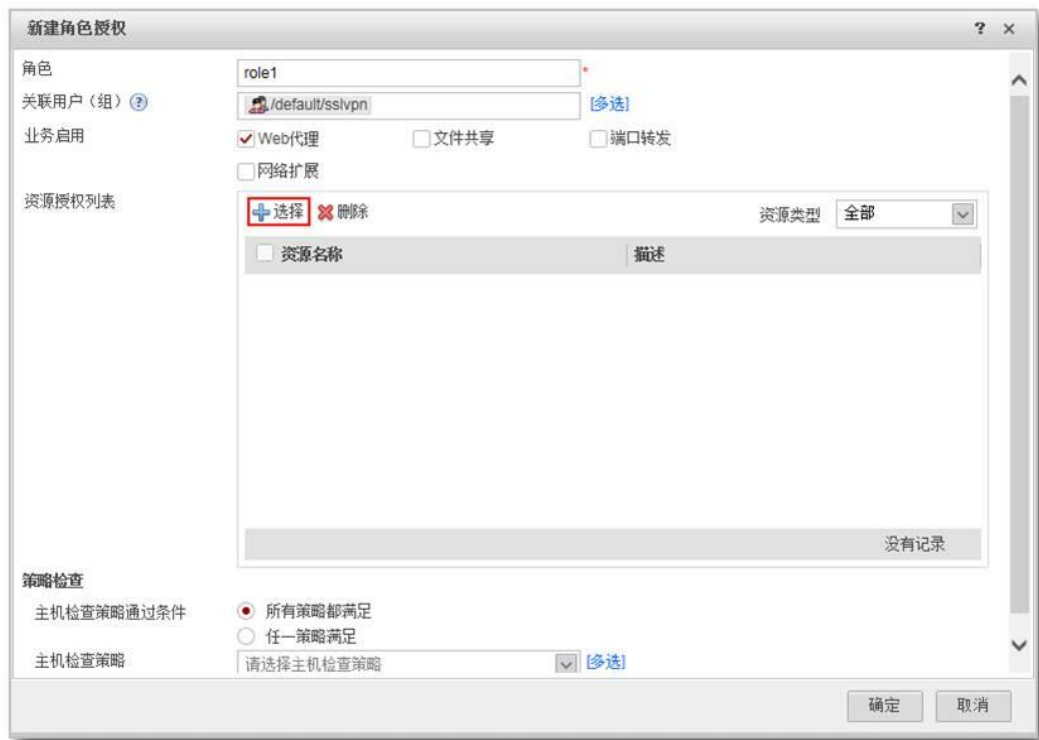
在终端物理网卡上抓包，可看到直接发往10.2.0.10:8081和10.2.0.11的明文报文，而走VPN隧道的报文是加密的，且目的地址是防火墙网关。

处理步骤

为了使用户访问用户系统和报销系统的流量也走SSL VPN隧道访，需要为这些URL配置Web-Link资源。不勾选“门户链接”的“显示”选项，用户在虚拟网关的资源列表中就看不到这个资源，但是通过ERP系统的页面可以访问这个资源。



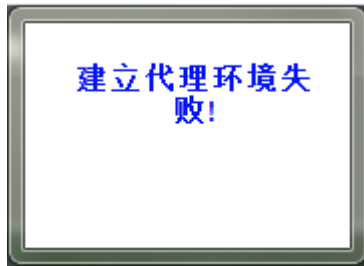
在该角色的资源授权列表中，将上面新建隐藏的Web-Link资源添加进来。



5.1.8 浏览器启用网络扩展时提示：建立代理环境失败！

现象描述

浏览器登录SSL VPN，启用网络扩展失败，提示“建立代理环境失败！”，弹出自动重连提示框。



可能原因

1. PC上安装的防火墙软件阻止网络扩展系统服务程序NemService和虚拟网关/代理服务器之间建立SSL连接。
2. PC上安装的防火墙软件提示用户“允许”或者“阻止”网络扩展系统服务程序NemService连接到网络时，用户没有在指定时间内选择“允许”或者选择了“阻止”。

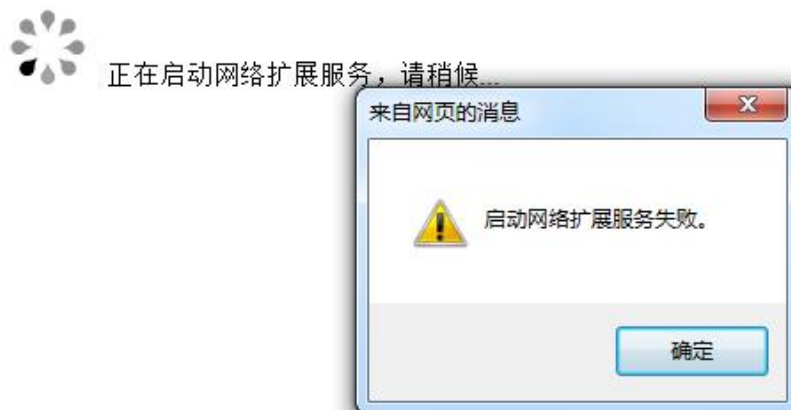
处理步骤

1. 修改PC上防火墙的配置，将“%appdata%\svnclient\NemService.exe” (软件的缺省安装路径)添加到防火墙软件允许连接到网络的软件列表中。
2. 当防火墙软件提示用户“允许”或者“阻止”网络扩展系统服务程序NemService连接到网络时,请在指定时间内选择“允许”。

5.1.9 浏览器启用网络扩展时提示：启动网络扩展服务失败

现象描述

浏览器登录SSL VPN，启动网络扩展失败，提示“启动网络扩展服务失败”。



可能原因

1. 用户PC操作系统的DHCP Client服务未启用。
2. 用户PC操作系统的Interactive Services Detection服务未启用。

处理步骤

1. 打开DHCP Client服务的方法如下：
 - a. 在“开始 > 运行”中，输入services.msc命令，单击“确定”，进入服务窗口。
 - b. 在服务列表中找到DHCP Client服务，右键单击“DHCP Client”，选择“启用”。
2. 启用Interactive Services Detection服务的方法如下：
 - a. 单击“开始”，在运行框中输入services.msc，按回车键。
 - b. 找到Interactive Services Detection服务，然后双击。
 - c. 启动类型选择“启动”，单击“确定”。
 - d. 执行netsh winsock reset，重置winsock。
 - e. 重启电脑生效。

5.1.10 浏览器启用网络扩展后访问内网资源卡顿，Ping 内网延迟大

现象描述

浏览器登录SSL VPN虚拟网关并启用网络扩展成功，访问内网资源卡顿，Ping内网延迟大。



```
管理员: C:\Windows\system32\cmd.exe
C:\Users\renjz>ping 10.10.10.10 -t
正在 Ping 10.10.10.10 具有 32 字节的数据:
来自 10.10.10.10 的回复: 字节=32 时间=333ms TTL=45
来自 10.10.10.10 的回复: 字节=32 时间=348ms TTL=45
来自 10.10.10.10 的回复: 字节=32 时间=342ms TTL=45
来自 10.10.10.10 的回复: 字节=32 时间=320ms TTL=45
来自 10.10.10.10 的回复: 字节=32 时间=353ms TTL=45
来自 10.10.10.10 的回复: 字节=32 时间=354ms TTL=45
来自 10.10.10.10 的回复: 字节=32 时间=330ms TTL=45
来自 10.10.10.10 的回复: 字节=32 时间=321ms TTL=45
```

可能原因

浏览器和SSL VPN网关之间采用的不是快速传输模式。

SSL VPN网络扩展有两种VPN报文封装模式，可靠传输模式和快速传输模式。两者的区别是底层传输协议不同，可靠传输模式采用的是TCP协议，快速传输模式采用的是UDP协议。相比可靠传输协议，快速传输协议传输的速度更快，用户感知也快些。自适应模式，就是在拨号过程中对链路进行探测，决定最终采用快速模式还是可靠模式传输业务数据。使用浏览器登录SSL VPN启用网络扩展，缺省使用“自适应模式”，且不可配置。

处理步骤

为了使浏览器和SSL VPN虚拟网关之间能够采用快速模式传输，需要确保终端访问SSL VPN虚拟网关的UDP协议和443端口被放行。如果SSL VPN虚拟网关是防火墙自身，需放行untrust到local域间的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，则需要在NAT设备上配置UDP协议和443端口的NAT映射。

5.1.11 浏览器启用网络扩展访问内网资源，不能命中关联用户/用户组的安全策略

现象描述

对于命中了安全策略的SSL VPN用户，对应的安全策略动作失效。例如，配置了一条安全策略，禁止SSL VPN用户user1访问10.1.1.1地址，但user1用户仍然可以访问10.1.1.1地址，即安全策略未起作用。

可能原因

SSL VPN用户登录成功后，访问内网资源的数据流进行安全策略匹配时是不带用户信息的。如果要将IP转换成用户信息，实现基于用户/用户组的管控，必须配置认证策略。

处理步骤

配置SSL VPN访问内网资源的认证策略，配置方法如下。



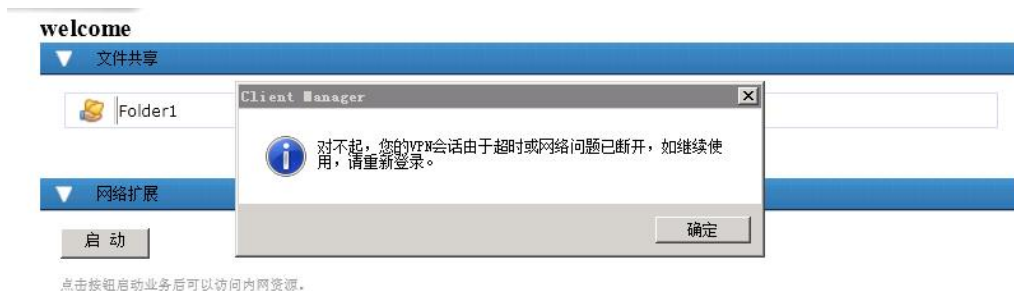
命令行方式：

```
auth-policy
rule name sslvpn_auth
source-zone untrust
destination-zone dmz
source-address 10.0.100.0 mask 255.255.255.0 //SSL VPN用户地址池
action exempt-auth
```

5.1.12 浏览器提示：对不起，您的VPN会话因为超时或网络原因已断开

现象描述

浏览器登录SSL VPN启用网络扩展，一段时间后弹框提示“对不起，您的VPN会话由于超时或网络问题已断开，如继续使用，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。
3. 终端和防火墙之间的链路出现了故障。

处理步骤

排查终端和防火墙之间的链路是否有故障。

如果链路正常，根据客户的业务要求，调整虚拟网关配置。

1. 提高SSL会话超时时间（缺省5分钟）。



2. 启用网络扩展的“保持连接”功能，除非用户生命周期（缺省1440分钟，可修改）到达，否则用户不会空闲下线。

在全路由模式和分离模式下，SSL VPN虚拟网关会发一些广播报文，因为一直有这些广播报文，所以用户不会老化。



5.1.13 浏览器提示：访问失败，服务器问题，请与管理员联系

现象描述

使用浏览器登录SSL VPN虚拟网关，访问文件共享资源，输入用户名/密码登录，系统报错“访问失败，服务器问题，请与管理员联系”。

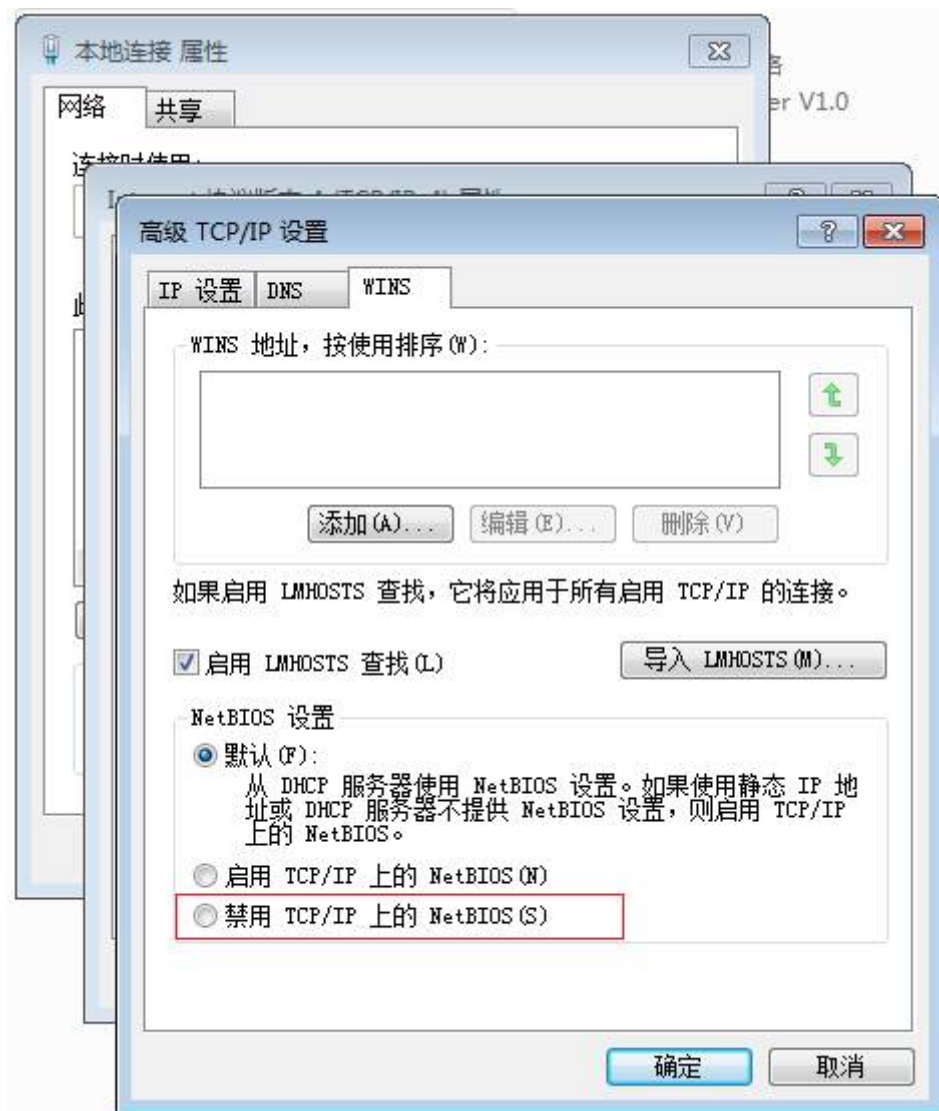


可能原因

1. 输入了SSL VPN的登录账号，而非共享文件夹所在操作系统的登录账号。
2. 共享文件夹所在操作系统限制。

处理步骤

1. 文件共享登录时，输入共享文件夹所在操作系统的登录账号和密码。
2. 调整共享文件夹所在操作系统网卡接口的NetBIOS设置，选择“禁用TCP/IP上的NetBIOS(S)”。



5.2 Windows + Chrome/Firefox/浏览器极速模式

5.2.1 SSL VPN 虚拟网关登录成功，看不到网络扩展“启动”按钮

现象描述

在SSL VPN虚拟网关已经配置了网络扩展，角色也启用了网络扩展业务的情况下，终端用户使用Firefox、Chrome或浏览器极速模式访问登录SSL VPN虚拟网关，看不到网络扩展“启动”按钮。而换成IE浏览器登录，则可以看到。

可能原因

SSL VPN包含Web代理、文件共享、端口转发、网络扩展四个子特性，其中Web代理又细分为Web改写和Web-link两种。这些子特性中，Web-link、端口转发、网络扩展这些子特性依赖于客户端控件，需要浏览器安装运行控件才能使用；而Web改写、文件共享两个子特性不依赖于客户端控件，只要是浏览器就可以使用。

目前，SSL VPN客户端控件仅支持在IE内核的浏览器（多核浏览器兼容模式使用IE内核）上加载。所以Firefox、Chrome这些非IE内核的浏览器登录SSL VPN，仅能看到Web改写资源和文件共享资源，网络扩展资源就看不到。不同浏览器支持的内核请参见[6.24 SSL VPN控件支持浏览器的情况如何](#)。

处理步骤

1. 使用IE内核浏览器登录SSL VPN虚拟网关。
2. 使用SecoClient的SSL VPN拨号。

5.3 Mac OS + Safari 浏览器

5.3.1 浏览器登录 SSL VPN，看不到网络扩展“启动”按钮

现象描述

在SSL VPN虚拟网关已经配置了网络扩展，角色也启用了网络扩展业务的情况下，终端用户使用操作系统自带的Safari浏览器访问登录SSL VPN，页面中看不到网络扩展“启动”按钮。

可能原因

SSL VPN包含Web代理、文件共享、端口转发、网络扩展四个子特性，其中Web代理又细分为Web改写和Web-link两种。这些子特性中，Web-link、端口转发、网络扩展这些子特性依赖于客户端控件，需要浏览器安装运行客户端控件才能使用；而Web改写、文件共享两个子特性不依赖于客户端控件，只要是浏览器就可以使用。

目前，SSL VPN客户端控件仅支持在IE内核的浏览器（多核浏览器兼容模式使用IE内核）上加载运行。Safari浏览器使用非IE内核，所以，登录SSL VPN仅能看到Web改写资源和文件共享资源，其它特性看不到。

处理步骤

安装并使用SecoClient拨号SSL VPN。

5.4 Android/IOS + 手机浏览器

5.4.1 手机使用浏览器登录 SSL VPN，无法看到 Web 代理资源

现象描述

用户使用手机自带的浏览器访问SSL VPN虚拟网关，输入用户名/密码登录成功后，看不到资源列表。使用PC上的浏览器登录，可以看到资源列表。



可能原因

Web代理手机页面使用了旧的Frame框架技术，而新的手机操作系统（Android 4.2之后、iOS 5之后）不再支持该框架技术。

处理步骤

- 使用手机系统自带的L2TP over IPSec功能，代替SSL VPN功能。
- 在手机上安装SecoClient，通过SecoClient网络扩展的方式接入内网。

5.5 拨号成功后业务不通

5.5.1 网络扩展业务不通

现象描述

拨号成功后，无法访问内部服务器网络资源。

可能原因

1. 网络扩展启动后没有正常获取虚拟IP地址。
2. 防火墙与内网服务器的网络连接不正常。
3. 防火墙上配置的安全策略禁止了用户访问内网服务器。
4. 网络扩展路由网段没有包含内网服务器地址。
5. 内网服务器服务没有开启。
6. 防火墙会话表对应表项没有建立。

处理步骤

1. 检查网络扩展启动后是否正常获取虚拟IP地址。
执行**ipconfig /all**查看是否有虚拟网卡和虚IP地址，如果没有获取虚拟IP则网络扩展是没有启动成功，请尝试重新启动。

```
C:\Users\Administrator> ipconfig /all
以太网适配器 本地连接:
    连接特定的 DNS 后缀 . . . . . :
    描述. . . . . : SVN Adapter V1.0 //虚拟网卡名称
    物理地址. . . . . : 00-FF-72-FA-CA-EE
    DHCP 已启用 . . . . . : 否
    自动配置已启用. . . . . : 是
    本地链接 IPv6 地址. . . . . : xxxx-xxxx-xxxx(首选)
    IPv4 地址 . . . . . : 10.100.101.24(首选) //虚拟IP地址
```

```
子网掩码 ..... : 255.255.255.0
默认网关 ..... :
DHCPv6 IAID ..... : 570490738
DHCPv6 客户端 DUID ..... : 00-01-00-01-1B-FB-7F-50-00-0C-29-AD-32-AC
DNS 服务器 ..... : XXXX-XXXX-XXXX
                        XXXX-XXXX-XXXX
                        XXXX-XXXX-XXXX
TCPIP 上的 NetBIOS ..... : 已启用
```

2. 检查防火墙和内网服务器的网络连接是否路由可达。

- a. 在防火墙上Ping内网服务器，在内网服务器未禁Ping的情况下，如果不能Ping通，说明SSL VPN网关和内网服务器之间的网络存在问题，请检查网关和内网服务器之间的连线。

```
[HUAWEI] ping 192.168.11.191
Ping 192.168.11.191: 56 data bytes, press CTRL_C to break
Request time out
Request time out
Request time out
Request time out
Request time out
---192.168.11.191 ping statistics ---
5 packet(s) transmitted
0 packet(s) received
100.00% packet loss //防火墙和内网服务器的线路不通
```

- b. 若连接线路正常，执行命令**display fib 192.168.11.191**检查防火墙是否有到内网服务器的路由。如果没有，添加一条静态路由。

```
[HUAWEI] display fib 192.168.11.191
Route Entry Count: 0 //没有到内网服务器的路由
```

```
[HUAWEI] ip route-static 192.168.11.0 24 172.21.1.1 //配置到内网服务器地址段的静态路由
```

- c. 检查内网服务器、防火墙和内网服务器之间的路由设备，是否有到网络扩展虚拟IP地址的路由。如果没有，请添加。

3. 检查防火墙的安全策略，是否禁止了用户访问服务器资源。

- a. 执行命令**display current-configuration configuration policy-security**检查安全策略的配置，是否放行虚拟IP访问内网服务器资源的请求。如果没有，请参照以下显示添加或修改安全策略。

 说明

虚拟IP地址段所在的安全区域，防火墙自动选择SSL VPN拨号公网接口所在的安全区域作为虚拟IP地址段的安全区域。

```
<HUAWEI> display current-configuration configuration policy-security
security-policy
rule name SSLVPN //配置虚拟IP地址段到内网服务器地址段的安全策略
source-zone untrust //虚拟IP地址段所属的安全区域
destination-zone trust //内网服务器所属的安全区域
source-address address-set source_vip //虚拟IP地址段
destination-address address-set server_ip //内网服务器地址段
action permit
```

- b. 检查安全策略是否关联了用户或用户所属的组。如果已关联，则必须配置认证策略。执行命令**display current-configuration configuration policy-auth**检查是否配置了相应的认证策略，如果没有认证策略，请参照如下显示配置认证策略。

```
<HUAWEI> display current-configuration configuration policy-security
rule name SSLVPN //配置虚拟IP地址段到内网服务器地址段的安全策略
source-zone untrust //虚拟IP地址段所属的安全区域
destination-zone trust //内网服务器所属的安全区域
source-address address-set source_vip //虚拟IP地址段
destination-address address-set server_ip //内网服务器地址段
user /default/group1 //安全策略关联了用户组
user /default/group2/user001 //安全策略关联了用户
action permit
```

```
<HUAWEI> display current-configuration configuration policy-auth
auth-policy
rule name sslvpn //配置虚拟IP地址段到内网服务器地址段的认证策略
source-zone untrust
destination-zone trust
source-address address-set source_vip //虚拟IP地址段
destination-address address-set server_ip //内网服务器地址段
action auth
```

4. 检查SSL VPN网络扩展路由网段，是否包含内网服务器资源的地址。

a. 执行**display network-extension**命令检查网络扩展客户端路由模式。

```
<HUAWEI> system
[HUAWEI] v-gateway gateway
[HUAWEI-gateway] service
[HUAWEI-gateway-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: 10.1.1.1
Route Mode: split
-----
Virtual IP Pool:
NO. Start-IP End-IP Mask Alias
-----
1 10.1.1.1 10.1.1.10 255.255.255.0 10.1.1.1
-----
```

full: 全路由模式; split: 分离模式; manual: 手动模式。

- 全路由模式下，无论是访问什么资源，数据一概被虚拟网卡截获，转发给虚拟网关处理。
- 分离模式下，客户端发送给内网的数据，经系统路由表识别以后，交由虚拟网卡转发，其源IP赋值为虚拟IP。而访问本地子网的数据则交由真实网卡转发，源IP赋值为真实的IP。由此，网络扩展只转发前往内网的数据。同时，分离模式也把不是访问本地子网资源的其他数据经过虚拟网卡转发。
- 手动模式下，在FW端，管理员必须手动配置内网网段静态路由，然后在客户端识别前往该网段的数据，交由虚拟网卡转发。
- 如果客户端路由模式为“手动路由模式”，执行命令**display current-configuration configuration v-gateway**检查手动路由网段是否包含了内网服务器的地址。如果不包含，请执行**network-extension manual-route**命令将内网服务器地址所在的网段添加到手动路由网段内。

```
[HUAWEI] display current-configuration configuration v-gateway
15:41:36 2016/06/16
#
#****BEGIN***tac**1****#
v-gateway tac
service
network-extension enable
network-extension keep-alive enable
network-extension keep-alive interval 120
network-extension netpool 10.100.10.100 10.100.10.200 255.255.255.0 //虚拟IP地址段1
network-extension netpool 10.100.20.1 10.100.20.254 255.255.254.0 //虚拟IP地址段2
netpool 10.100.10.1 default
network-extension mode manual //客户端路由模式
network-extension manual-route 172.16.0.0 255.255.0.0 //手动路由网段1
network-extension manual-route 192.168.11.191 255.255.255.255 //手动路由网段2
```

5. 检查内网服务器服务是否开启。
 - a. 请客户在企业内网尝试访问内网服务器，是否访问正常。如果访问也异常，则检查服务器服务是否开启。
 - b. 请客户确定内网服务器是否对访问来源的IP地址做了限制。如果有限制，则放开虚拟IP地址池的限制。

6. 检查防火墙的会话表，确定对应表项是否建立。

通过**display firewall session table verbose source global 虚拟IP destination global 内网服务器IP**，检查对应的会话表项是否存在。

如果会话表项不存在，可能的原因如下，请根据不同原因排查。

- 访问报文没有到达防火墙。
- 访问报文被防火墙安全策略丢包。
- 防火墙没有到内网服务器的路由。
- 防火墙防攻击策略导致丢包，例如IP spoofing。

如果会话表项存在，但是服务器响应报文数量为0，可能的原因：服务器服务未开启，中间设备没有到虚拟IP地址段的路由。

```
<HUAWEI> display firewall session table verbose source global 10.100.10.100 destination global 192.168.10.100
http VPN:public --> public ID: a48f3fdb655030b65720d507
Zone: untrust--> trust TTL: 24:00:00 Left: 23:59:59
Recv Interface: GigabitEthernet1/0/7
Interface: GigabitEthernet1/0/0 NextHop: 192.168.10.1 MAC: 00-e0-fc-12-34-56
<--packets:9 bytes:8772 -->packets:8 bytes:728 //8表示发送给服务器报文的数量，9表示服务器响应报文数量
10.100.10.100:63334-->192.168.10.100:80 PolicyName: SSLVPN
```

5.5.2 Web 代理业务不通

现象描述

拨号成功后，无法访问内部Web代理资源。

可能原因

1. Web改写配置，没有包含内网服务器资源。
2. 防火墙上配置的安全策略禁止了用户访问服务器资源。
3. 防火墙和内网服务器的网络连接不可达。
4. 内网服务器服务未开启。
5. 防火墙会话表的对应表项没有建立。

处理步骤

1. 检查SSL VPN的Web改写配置，是否包含内网服务器资源。
 - a. 执行**display web-proxy resource**命令检查Web代理资源，查看Web改写或者web-link的资源是否与内网服务器一致，如果内网http服务器的端口号不是80需要在资源配置上加上端口号。如果不一致请修改Web代理配置。

```
<system> system
[HUAWEI] v-gateway gateway
[HUAWEI-gateway] service
[HUAWEI-gateway-service] display web-proxy resource
VG Web Rewrite Resource Lists
-----
```

No.	ResourceAlias	ResourceURL	Link	ResourceDescription
1	http1	http://192.168.10.100	show	-

----End

VG Web Link Resource List

No.	ResourceAlias	ResourceURL	Link	ResourceDescription
1	http2	http://192.168.10.200	show	-

- b. 检查角色是否开启了Web代理功能，执行命令**display current-configuration configuration v-gateway**检查当前绑定的角色是否开启了Web改写资源。

```
[HUAWEI] display current-configuration configuration v-gateway
v-gateway tac
service
web-proxy enable
web-proxy web-link enable
web-proxy proxy-resource http1 http://192.168.1.100 show-link
web-proxy link-resource http2 http://192.168.1.200 show-link
role
role default
role default condition all
role default network-extension enable
role default web-proxy enable //default角色开启了Web改写资源
```

2. 检查防火墙的安全策略，是否禁止了用户访问服务器资源。

执行命令**display current-configuration configuration policy-security**检查安全策略的配置，是否放行虚拟IP访问内网服务器资源的请求。如果没有，则参照以下显示添加或修改安全策略。

```
[HUAWEI] display current-configuration configuration policy-security
security-policy
rule name SSLVPN //配置安全策略
source-zone local //源安全区域固定为local
destination-zone trust //内网服务器所属的安全区域
destination-address address-set server_ip //内网服务器Web代理资源的地址
action permit
```

3. 检查防火墙和内网Web代理服务器的网络连接，是否路由可达。

- a. 在防火墙上Ping内网服务器，在内网服务器未禁Ping的情况下，如果不能Ping通，说明SSL VPN网关和内网服务器之间的网络存在问题，请检查网关和内网服务器之间的连线。

```
[HUAWEI] ping 192.168.11.191
Ping 192.168.11.191: 56 data bytes, press CTRL_C to break
Request time out
Request time out
Request time out
Request time out
Request time out

---192.168.11.191 ping statistics ---
5 packet(s) transmitted
0 packet(s) received
100.00% packet loss //防火墙和内网服务器的线路不通
```

- b. 若连接线路正常，执行命令**display fib**检查防火墙是否有到内网服务器的路由。如果没有，添加一条静态路由。

```
[HUAWEI] display fib 192.168.11.191
Route Entry Count: 0 //没有到内网服务器的路由
[HUAWEI] ip route-static 192.168.11.0 24 172.21.1.1 //配置到内网服务器地址段的静态路由
```

4. 检查内网服务器服务是否开启。

- a. 请客户在企业内网尝试访问内网服务器，是否访问正常。如果访问也异常，则检查服务器服务是否开启。

- b. 请客户确定内网服务器是否对访问来源的IP地址做了限制。如果有限制，则放开限制。
5. 检查防火墙的会话表，确定对应表项是否建立。

通过**display firewall session table verbose destination global** *内网服务器 IP*，检查对应的会话表项是否存在。

如果会话表项不存在，可能的原因：访问报文没有到达防火墙，访问报文被防火墙安全策略丢包，防火墙没有到内网服务器的路由。请根据不同原因排查。

如果会话表项存在，但是服务器响应的后向报文数量为0，可能的原因：服务器服务未开启，中间设备没有到防火墙地址的路由。

```
<HUAWEI> display firewall session table verbose destination global 192.168.10.100
http VPN:public --> public ID: a48f3fdb655030b65720d507
Zone: untrust--> trust TTL: 24:00:00 Left: 23:59:59
Recv Interface: GigabitEthernet1/0/7
Interface: GigabitEthernet1/0/0 NextHop: 192.168.10.1 MAC: 00-e0-fc-12-34-56
<--packets:9 bytes:8772 -->packets:8 bytes:728 //8表示发送给服务器前向报文的数量，9表示服务器响应的后向报文数量
10.100.10.100:63334-->192.168.10.100:80 PolicyName: SSLVPN
```

5.5.3 端口转发业务不通

现象描述

拨号成功后，无法访问内部端口转发资源。

可能原因

1. SSL VPN端口转发配置，没有包含内网服务器资源。
2. 防火墙上配置的安全策略禁止了用户访问服务器资源。
3. 防火墙和内网服务器的网络连接不可达。
4. 内网服务器服务没有开启。
5. 防火墙会话表的对应表项没有建立。

处理步骤

1. 检查SSL VPN端口转发配置，是否包含内网服务器资源。
 - a. 执行**display port-forwarding resource**命令检查端口转发资源。如果不正确请重新配置。

```
<system> system
[HUAWEI] v-gateway gateway
[HUAWEI-gateway] service
[HUAWEI-gateway-service] display port-forwarding resource
VG Port Forwarding Resource Lists
-----
No. ResourceAlias Resource Port ResourceDescription
-----
1 http 192.168.1.100 8080 -
-----
```
 - b. 检查角色是否开启了端口转发功能，执行命令**display current-configuration configuration v-gateway**检查当前绑定的角色是否开启了端口转发资源。

```
[HUAWEI] display current-configuration configuration v-gateway
v-gateway tac
service
port-forwarding enable
```



```
port-forwarding auto-start enable
port-forwarding resource http host-ip 192.168.1.100 8080
role
role default
role default condition all
role default network-extension enable
role default port-forwarding enable //default角色开启了端口转发资源
```

2. 检查防火墙的安全策略，是否禁止了用户访问服务器资源。

执行命令**display current-configuration configuration policy-security**检查安全策略的配置，是否放行虚拟IP访问内网服务器资源的请求。如果没有，则添加或修改安全策略放行。

```
[HUAWEI] display current-configuration configuration policy-security
security-policy
rule name SSLVPN //配置安全策略
source-zone local //源安全区域固定为local
destination-zone trust //内网服务器所属的安全区域
destination-address address-set server_ip //内网服务器端口转发的地址
action permit
```

3. 检查防火墙和内网端口转发服务器的网络连接，是否路由可达。

- a. 在防火墙上Ping内网服务器，在内网服务器未禁Ping的情况下，如果不能Ping通，说明SSL VPN网关和内网服务器之间的网络存在问题，请检查网关和内网服务器之间的连线。

```
[HUAWEI] ping 192.168.11.191
Ping 192.168.11.191: 56 data bytes, press CTRL_C to break
Request time out
Request time out
Request time out
Request time out
Request time out

---192.168.11.191 ping statistics ---
5 packet(s) transmitted
0 packet(s) received
100.00% packet loss //防火墙和内网服务器的线路不通
```

- b. 若连接线路正常，执行命令**display fib**检查防火墙是否有到内网服务器的路由。如果没有，添加一条静态路由。

```
[HUAWEI] display fib 192.168.11.191
Route Entry Count: 0 //没有到内网服务器的路由
[HUAWEI] ip route-static 192.168.11.0 24 172.21.1.1 //配置到内网服务器地址段的静态路由
```

4. 检查内网服务器服务是否开启。

- a. 请客户在企业内网尝试访问内网服务器，是否访问正常。如果访问也异常，则检查服务器服务是否开启。
- b. 请客户确定内网服务器是否对访问来源的IP地址做了限制。如果有限制，则放开限制。

5. 检查防火墙的会话表，确定对应表项是否建立。

通过**display firewall session table verbose destination global 内网服务器IP**，检查对应的会话表项是否存在。

如果会话表项不存在，可能的原因：访问报文没有到达防火墙，访问报文被防火墙安全策略丢包，防火墙没有到内网服务器的路由。请根据不同原因排查。

如果会话表项存在，但是服务器响应的后向报文数量为0，可能的原因：服务器服务未开启，中间设备没有到防火墙地址的路由。

```
<HUAWEI> display firewall session table verbose destination global 192.168.10.100
http VPN:public --> public ID: a48f3fdb655030b65720d507
Zone: untrust--> trust TTL: 24:00:00 Left: 23:59:59
Recv Interface: GigabitEthernet1/0/7
Interface: GigabitEthernet1/0/0 NextHop: 192.168.10.1 MAC: 00-e0-fc-12-34-56
<--packets:9 bytes:8772 -->packets:8 bytes:728 //8表示发送给服务器前向报文的数量，9表示服务器响
```

应的后向报文数量
10.100.10.100:63334-->192.168.10.100:80 PolicyName: SSLVPN

6 SSL VPN 常见咨询类问题 FAQ

6.1 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“主设备”来处理，而不会分担一部分到“从设备”，实现不了双机分担SSL VPN流量的预期效果。

主设备指的是命令行提示符前有HRP_M前缀的那台设备。

从设备指的是命令行提示符前有HRP_S前缀的那台设备。

6.2 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。

6.3 SSL VPN 用户是否支持不认证登录

不支持。

6.4 SecoClient 是否支持手机终端

支持。

SecoClient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。

iOS版SecoClient客户端已上传到苹果应用市场。用户可打开应用市场搜索SecoClient软件，下载安装使用。

Android版SecoClient客户端已上传到华为应用市场和谷歌应用市场。用户可打开应用市场搜索SecoClient软件，下载安装使用。

6.5 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”。

修改用户

登录名: huawei001 *

显示名:

描述:

所属用户组: /default [选择]

所属安全组: [选择]

密码: ***** *

确认密码: ***** *

密码不能和用户名相同，长度为6~16个字符，且密码必须包含数字、大写字母、小写字母、特殊字符中的至少3种，如： Password@或password8#等。

用户属性

账号过期时间: 永不过期 在此时间之后过期

允许多人同时使用该账号登录

警告: 禁用此功能将导致使用此用户帐号登录的所有IP全部下线

IP/MAC绑定: 不绑定 单点绑定 (该用户只能使用指定的地址登录，同时该地址也可被其他用户使用。)

确定 取消

命令行配置方式:

```
[sysname] user-manage user huawei001  
[sysname-localuser-huawei001] multi-ip online enable
```

2. 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。

修改 SSL VPN

SSL VPN配置

网关名称: abc *

类型: 独占型 共享型

网关地址: 手动配置IP地址 10.11.11.10 * 端口 443 <1024-50000>或443

提示: 为保证用户登录网关，需要开启安全策略。 [新建安全策略]

域名: www.example.com

用户认证

本地证书: default

客户端CA证书: default [选择]

证书认证方式: -- NONE --

认证域: 请选择认证域

DNS服务器

首选DNS服务器:

备选DNS服务器 1:

快速通道端口: 443 <1-49999>

最大用户数: 10 <1-1000>

最大并发用户数: <1-100>

最大资源数: 1024 <1-1024> (系统总资源: 12800, 剩余: 11776)

允许一个账号在多处同时登录

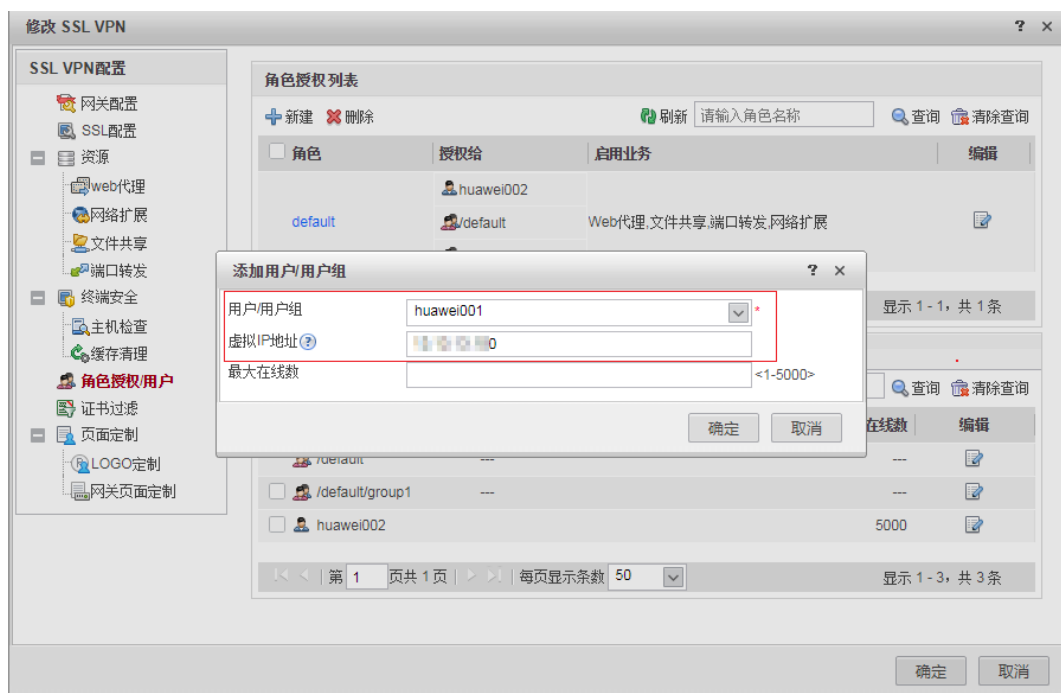
确定 取消

命令行配置方式:

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

6.6 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。



命令行配置方式：

```
[sysname] v-gateway test
[sysname-test] service
// 1.配置地址池
[sysname-test-service] network-extension netpool 20.0.0.2 20.0.0.100 255.255.255.0
[sysname-test-service] network-extension netpool 10.0.100.2 10.0.100.200 255.255.255.0
[sysname-test] vpndb
// 2.1添加用户到虚拟网关
[sysname-test-vpndb] user abc
// 2.2将用户abc与地址10.0.100.100绑定，即用户abc上线的时候分配10.0.100.100这个IP。
[sysname-test-vpndb] user abc virtual-ip 10.0.100.100
```

防火墙也支持用户组和虚拟地址段绑定，但不支持Web界面上配置，只能通过命令行配置。

```
// 3.1添加用户组到虚拟网关
[sysname-test-vpndb] group /default/huawei
// 3.2地址池绑定用户组，即huawei用户组下的用户从地址池20.0.0.2-20.0.0.100分配地址。
[sysname-test-vpndb] group /default/huawei network-extension netpool 20.0.0.2 20.0.0.100 255.255.255.0
```

6.7 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。

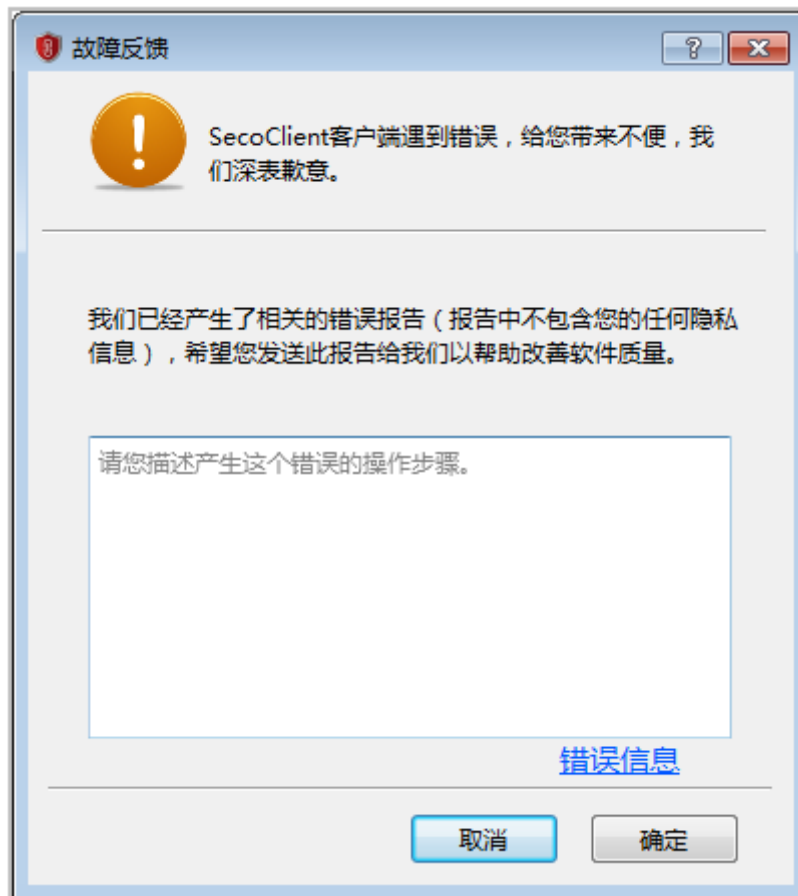
6.8 SecoClient 的日志采集方法

PC 终端的采集方法

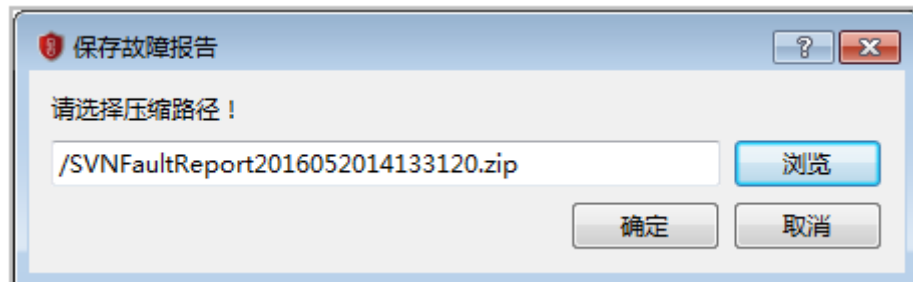
1. 右键单击SecoClient的托盘图标。



2. 选择“错误报告”。



3. 单击“确定”，选择错误报告的存放路径。




4. 单击“确定”。

SecoClient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SecoClient所在PC的网卡信息。
- operate_system_info.txt: 记录SecoClient所在PC的操作系统信息。
- proxy_info.txt: 记录SecoClient所在PC的代理服务器信息。
- route_info.txt: 记录SecoClient所在PC的路由信息。
- SecoClient_SecoClientCS_0.log: 记录SecoClient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。

- SecoClient_SecoClientUI_0.log: 记录SecoClient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。
- SecoClient_SecoClientPromoteService_0.log: SecoClient的服务进程，用于确保SecoClient正常运行。
- 崩溃文件: 当SecoClient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SecoClient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。

移动终端（iOS/Android）的采集方法

1. 单击SecoClient客户端主界面的按钮。



2. 选择“反馈”。



3. 打开“VPN调试日志”开关，重新复现问题后，再单击“反馈日志”，并根据提示操作，日志将以邮件方式反馈。



6.9 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: huawei001 failed to login."
```

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  
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 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  
address 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
```

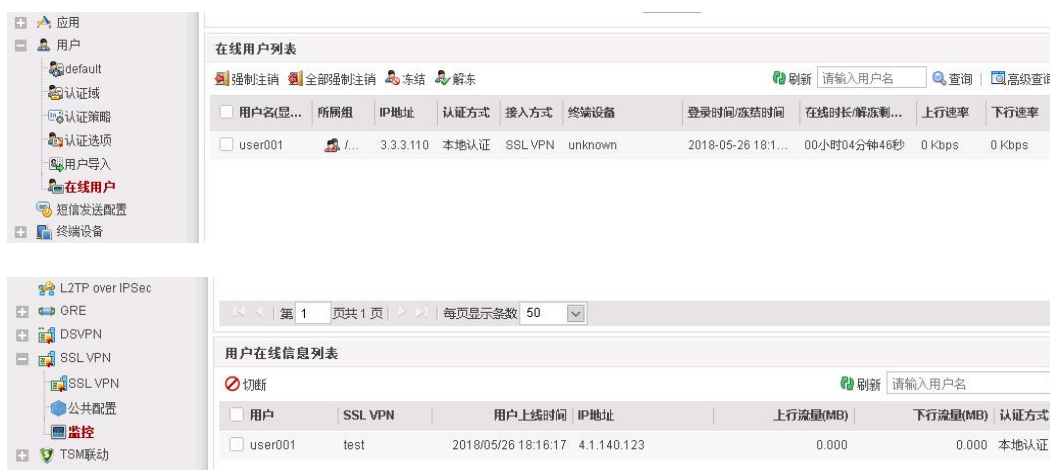
6.10 SSL VPN 证书认证相关知识

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。

6.11 SSL VPN 和用户管理特性的关联知识

用户在使用Web代理、端口转发和文件共享业务时，用户管理特性的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，用户才会上线，才能在用户管理特性的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，一处是在用户管理特性的“在线用户”里查看，另一处是在SSL VPN的“监控”里查看，分别如下图所示。



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。

在用户管理特性的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。

6.12 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。

6.13 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。

6.14 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。

6.15 SSL VPN 认证后如何基于用户进行权限管控

执行如下两个步骤配置基于用户进行权限管控。

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。

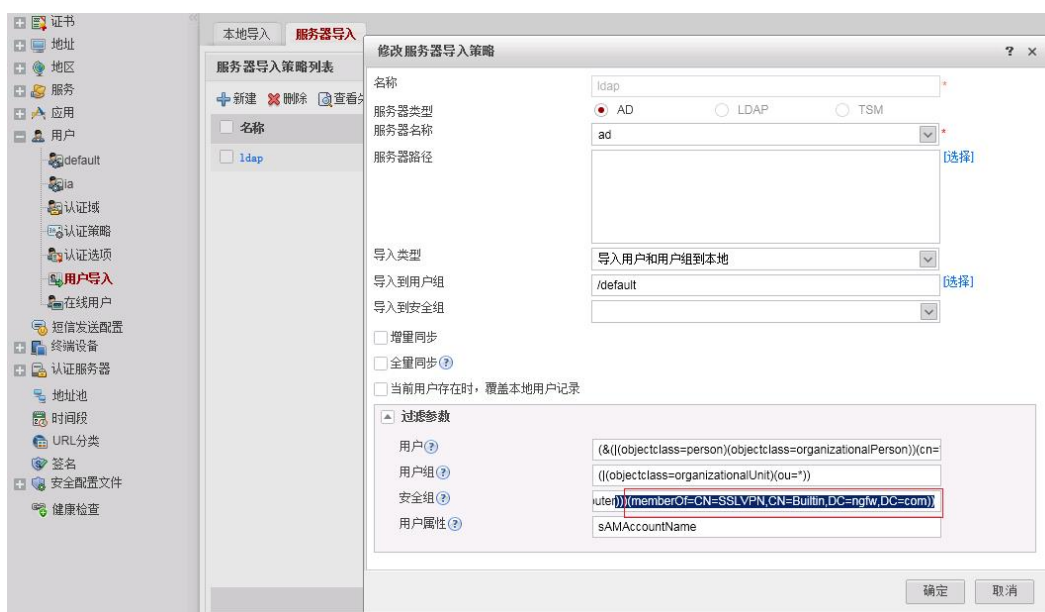
6.16 SSL VPN 采用 AD/LDAP 认证，如何实现允许指定安全组下的用户登录

SSL VPN登录使用AD认证（或LDAP认证），希望某个安全组下的用户允许登录，其他用户不允许登录。

解决办法：修改用户导入策略的用户过滤参数，将用户所属安全组的名称做为匹配条件。这种情况下，属于该安全组的用户，才会被更新到本地，同时配置新用户选项选择“不允许新用户登录”。

修改前：(&((objectclass=person)(objectclass=organizationalPerson))(cn=*)(!(objectclass=computer)))

修改后：(&(&((objectclass=person)(objectclass=organizationalPerson))(cn=*)(!(objectclass=computer)))(memberOf=CN=SSLVPN,CN=Builtin,DC=ngfw,DC=com))



6.17 SSL VPN 业务报文的域间关系如何确定

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。

6.18 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：

- 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。
- 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。

6.19 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。

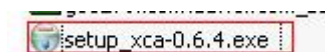
需要注意的是，在双机热备场景下，SSL VPN拨号到主防火墙上，可以使用主墙的内网接口地址对设备进行管理，但是无法通过相同方式对备墙进行管理。要管理备墙，需要通过内网堡垒机或中间设备间接跳转。

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。

6.20 如何使用 XCA 制作设备证书和用户证书

步骤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。

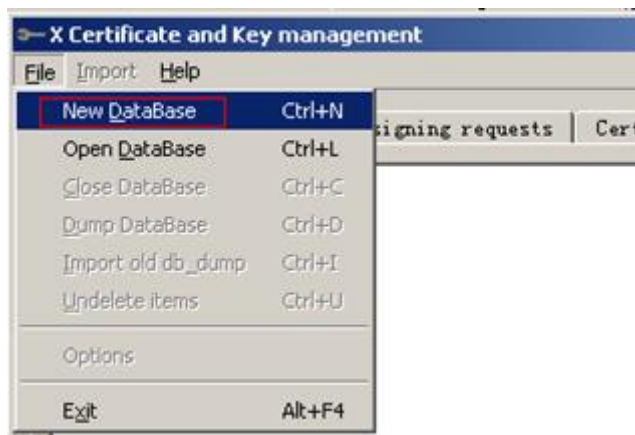


步骤2 运行程序。

1. 单击“开始 > 程序 > xca > xca”运行程序。



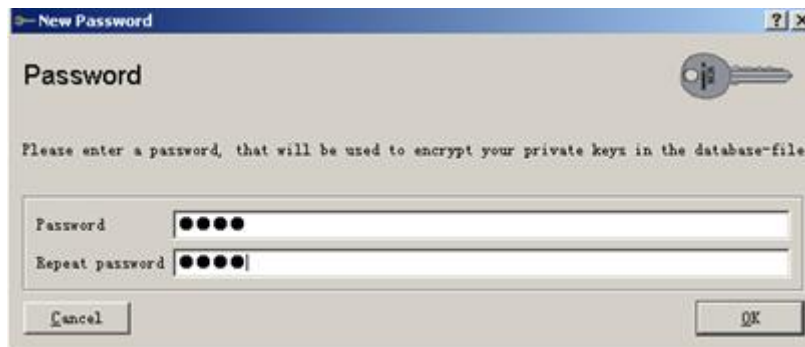
2. 选择“File > New DataBase”创建数据库。



3. 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。



4. 在弹出的对话框中输入密码，并单击“ok”按钮。

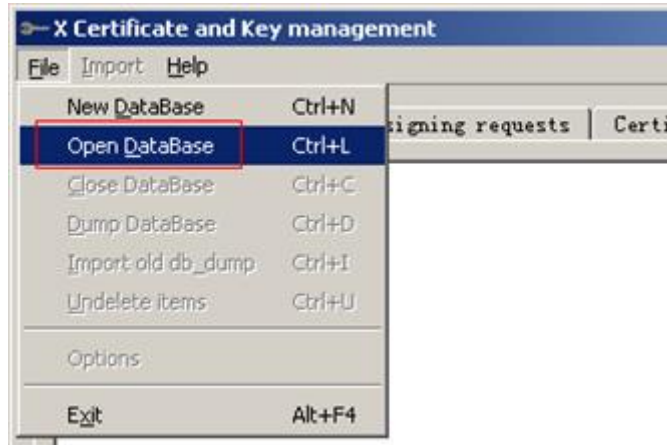


说明

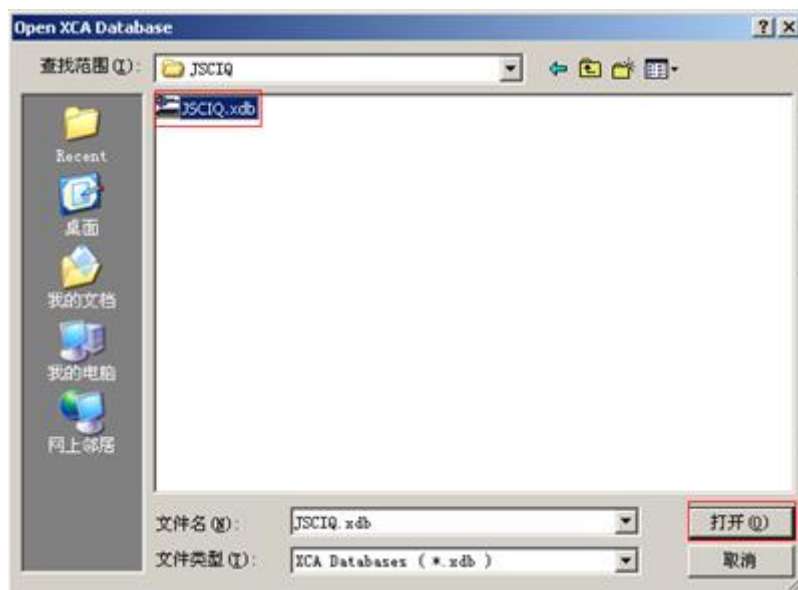
须牢记此密码，再次打开数据库时需要用到该密码。

步骤3 关闭后再次打开xca制作工具。

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



2. 打开上次保存的数据库，单击“打开”按钮。



3. 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。



步骤4 制作根证书。

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



2. 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”。



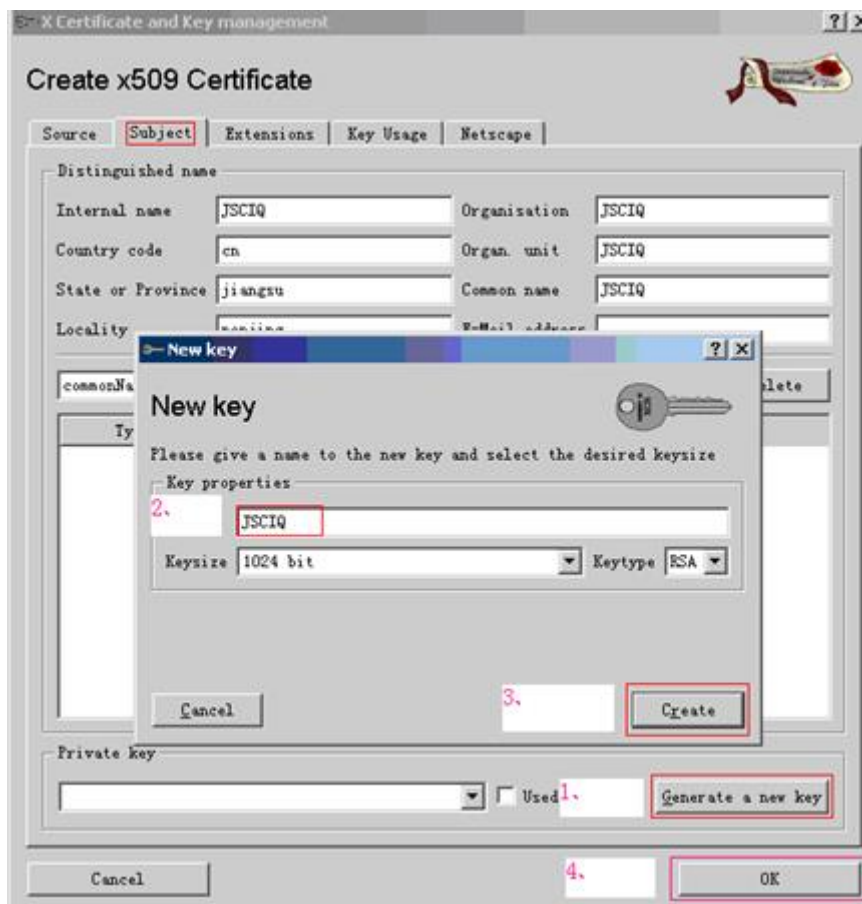
📖 说明

必须选中签名算法为“SHA 1”，然后单击“Apply”按钮。

3. 在“Subject”中填入名称。



4. 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。



5. 最后单击“OK”按钮，就生成了根证书。

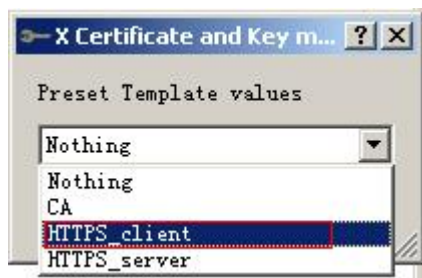


步骤5 制作用户证书。

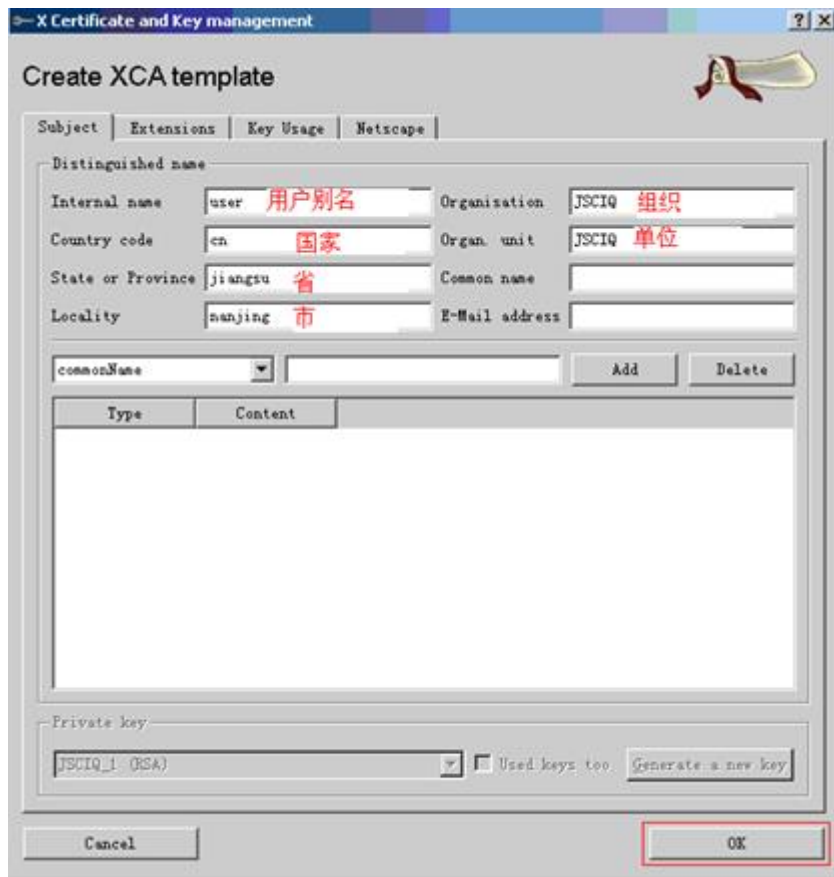
- 制作用户证书模版。
 - a. 选择“Templates”，并单击“New template”按钮制作用户证书。



- b. 选择“HTTPS_client”，单击“OK”。



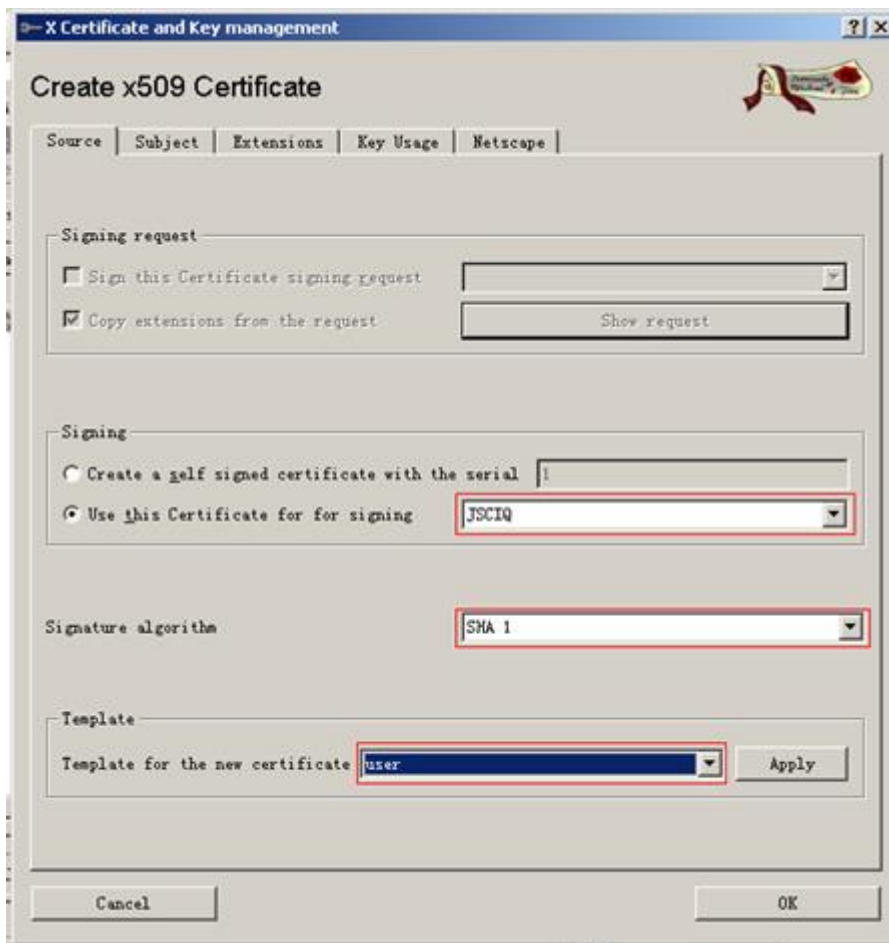
- c. 在用户模版中，设置用户参数（由于每个用户名不同，因此“Common name”不设置），并单击“ok”。



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



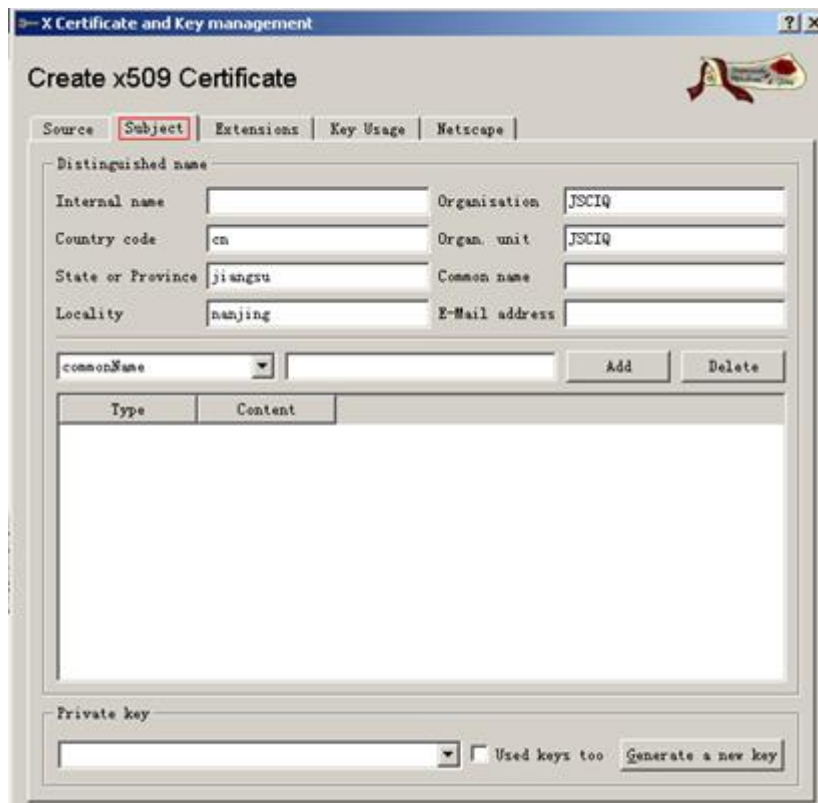
- b. 在“Signing”下选择“Use this Certificate for for signing”为之前的根证书“JSCIQ”，签名算法选择为“SHA-1”，“Template”下选择“user”，单击“Apply”按钮。



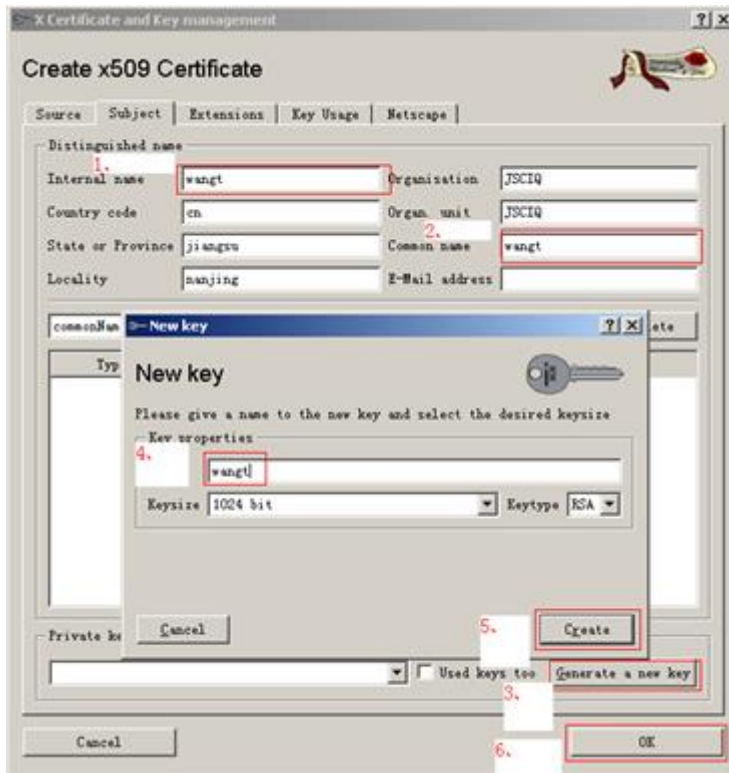
说明

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。
- 在“subject”的“Internal name”中输入用户别名“wangt”。
 - 在“Common name”中输入用户名“wangt”。
 - 单击右下角的“Generate a new key”。
 - 在弹出的对话框中输入“wangt”。
 - 单击“create”按钮。
 - 单击“ok”按钮。



e. 此时可以看到生成的证书。

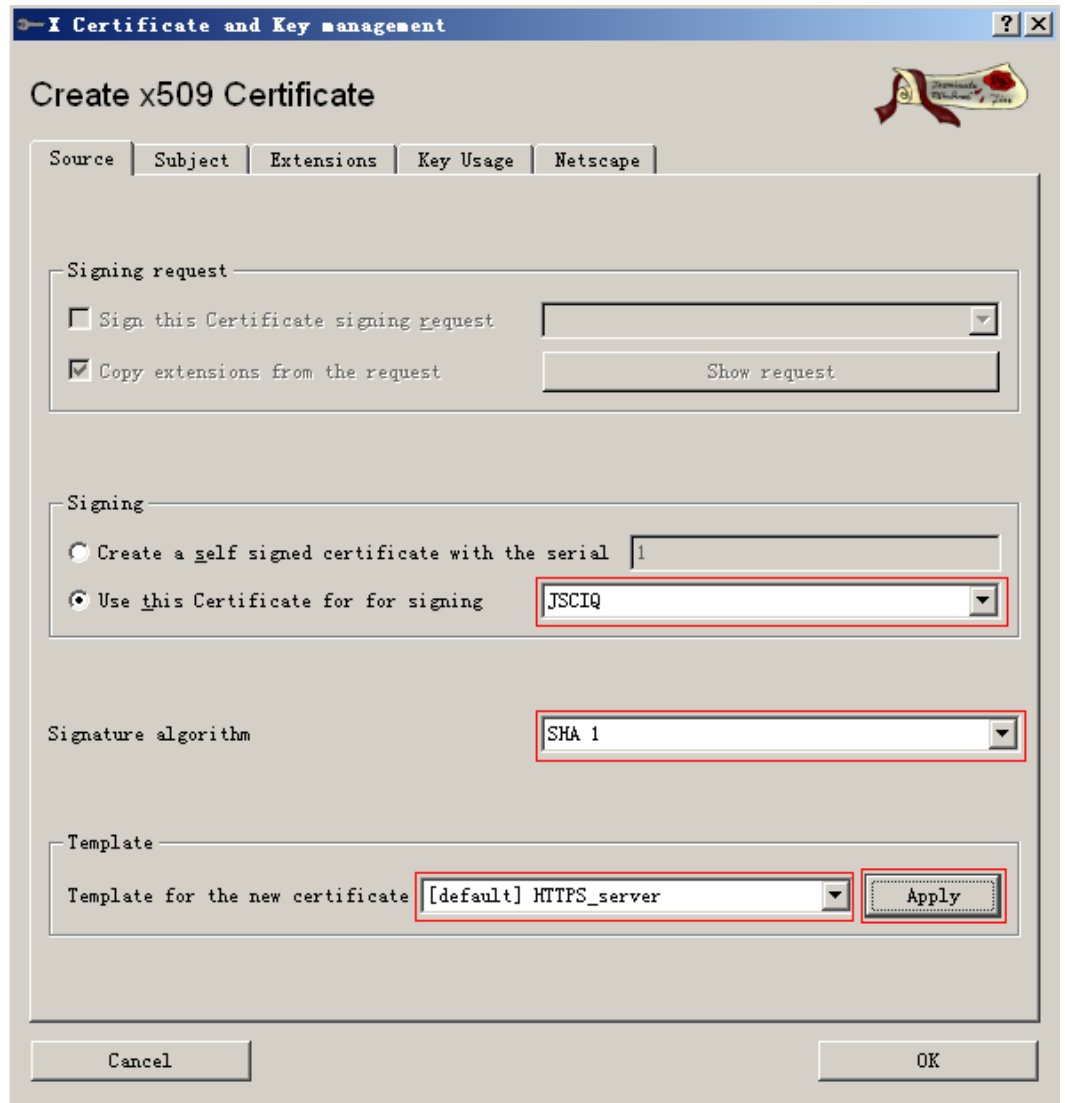


步骤6 制作设备证书。

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



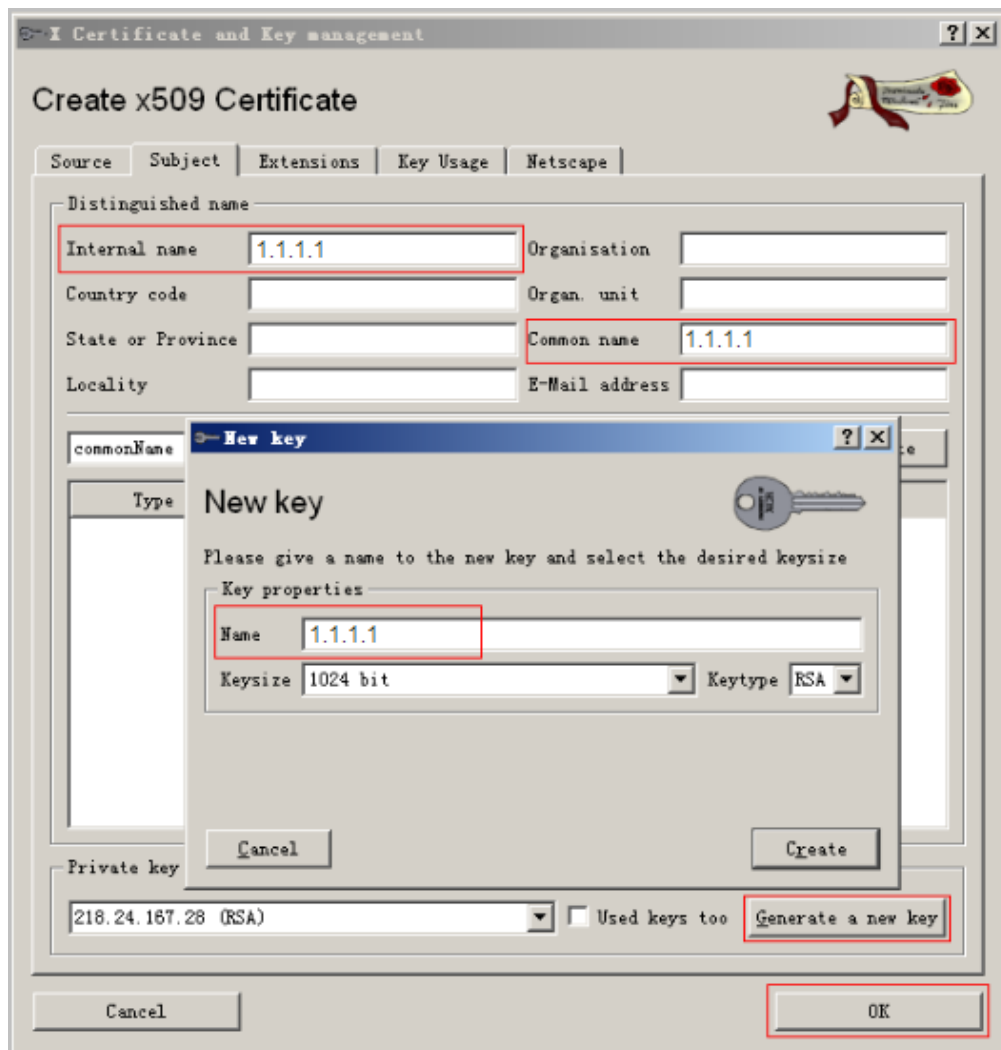
2. 在“Signing”下选择“Use this Certificate for for signing”为之前的根证书“JSCIQ”，签名算法选择为“SHA-1”，“Template”下选择“[default] HTTPS_server”，单击“Apply”按钮。



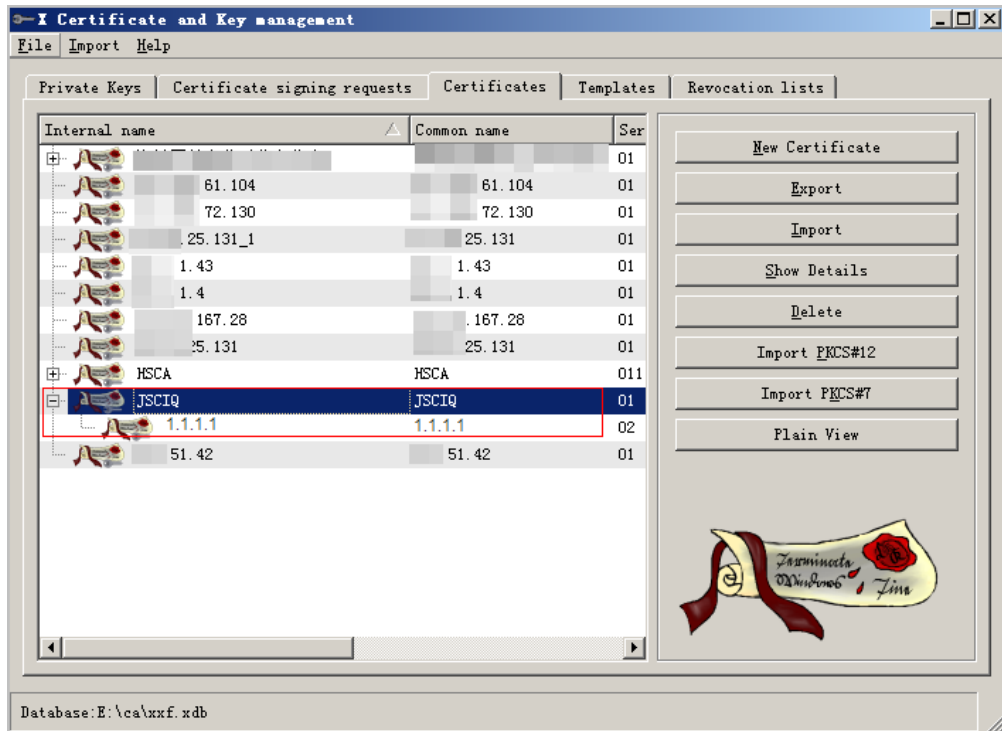
说明

必须选择签名算法为“SHA 1”，然后单击“Apply”按钮。

3. 在“subject”标签页中按照以下顺序进行操作。
 - a. 在“Internal name”中输入虚拟网关IP“1.1.1.1”（必须为虚拟网关IP）。
 - b. 在“Common name”中输入虚拟网关IP“1.1.1.1”（必须为虚拟网关IP）。
 - c. 单击右下角的“Generate a new key”。
 - d. 在弹出的对话框中输入“1.1.1.1”。
 - e. 单击“create”按钮。
 - f. 单击“ok”按钮。



4. 此时可以看到生成的证书。



步骤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。

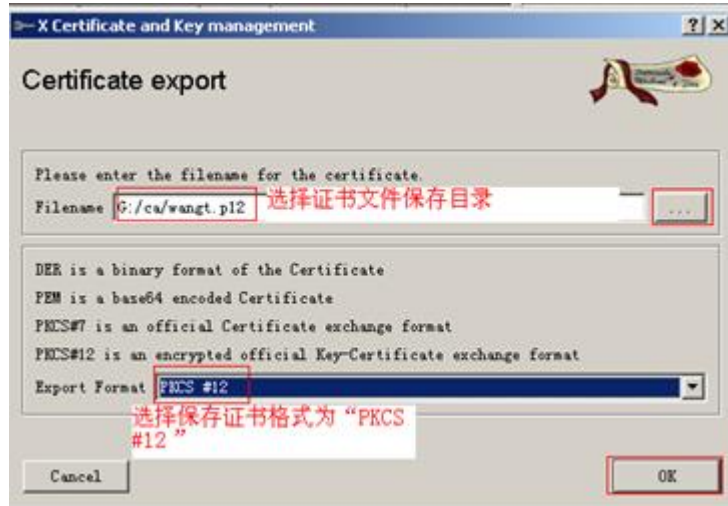


- 导出用户证书。

- 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”。



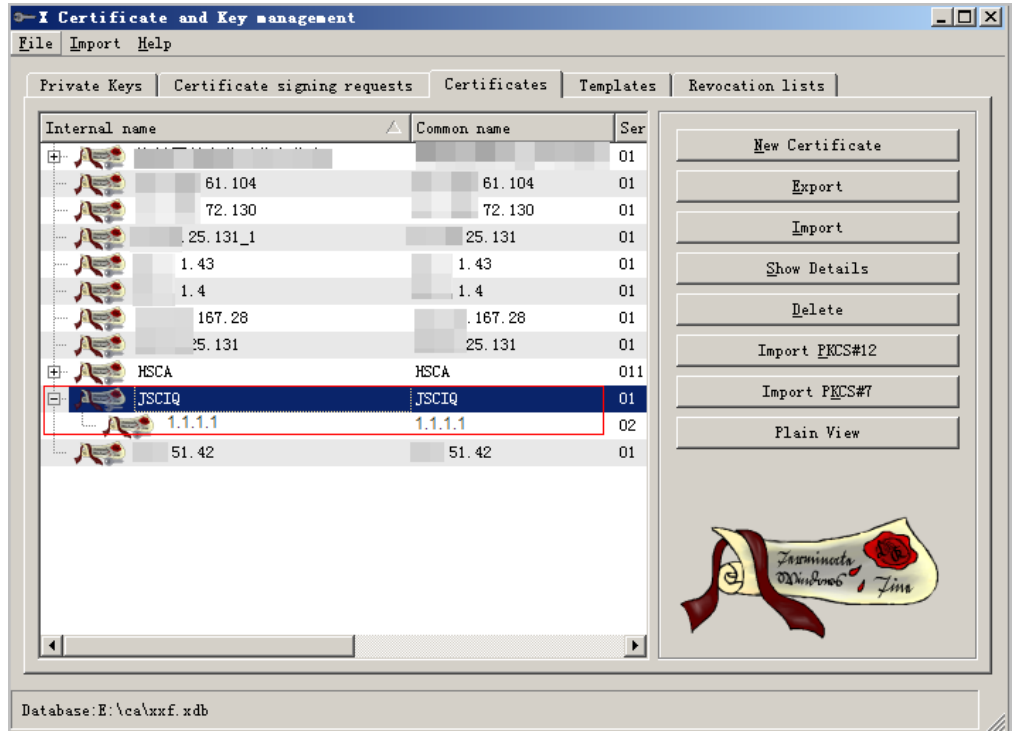
- c. 在弹出的对话框中，密码为空即可，直接单击“ok”。



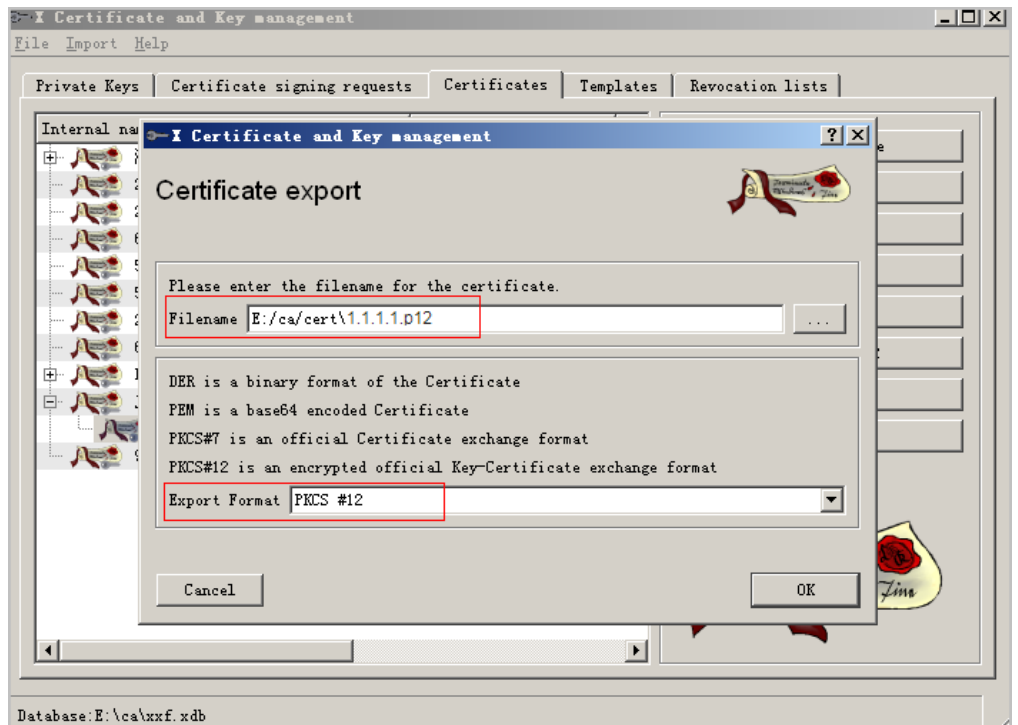
- d. 此时，G:\ca下出现用户证书wangt。



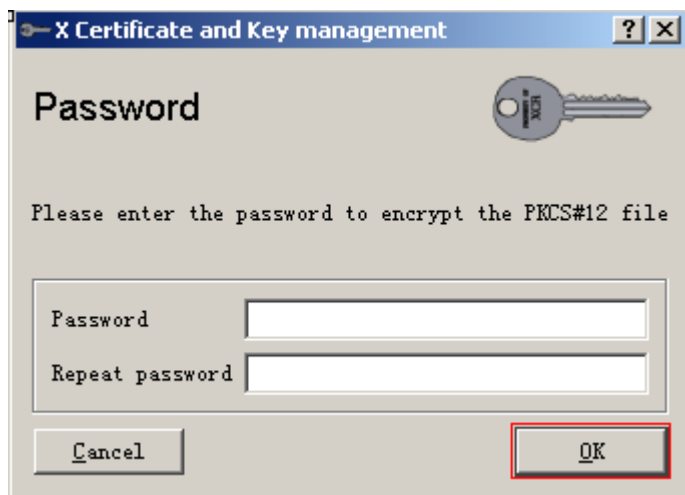
- 导出设备证书。
 - a. 选择“Certificate”下设备证书“1.1.1.1”，单击“Export”。



- 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。

----结束

6.21 SecoClient 安装和运行是否都需要管理员权限

安装SecoClient，需要有管理员权限。

运行SecoClient，不需要有管理员权限，普通用户即可。

6.22 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。

6.23 SSL VPN 是否支持 IPv6

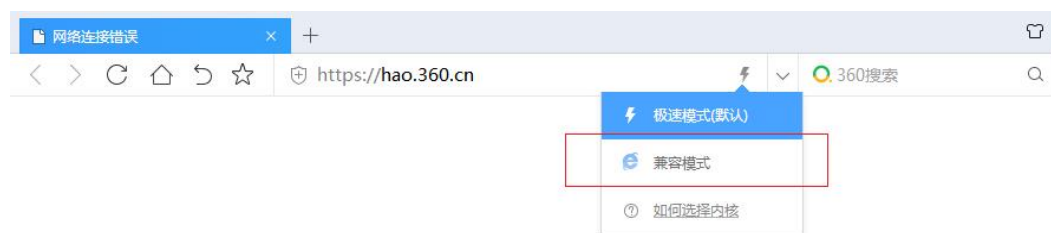
不支持。

6.24 SSL VPN 控件支持浏览器的情况如何

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。

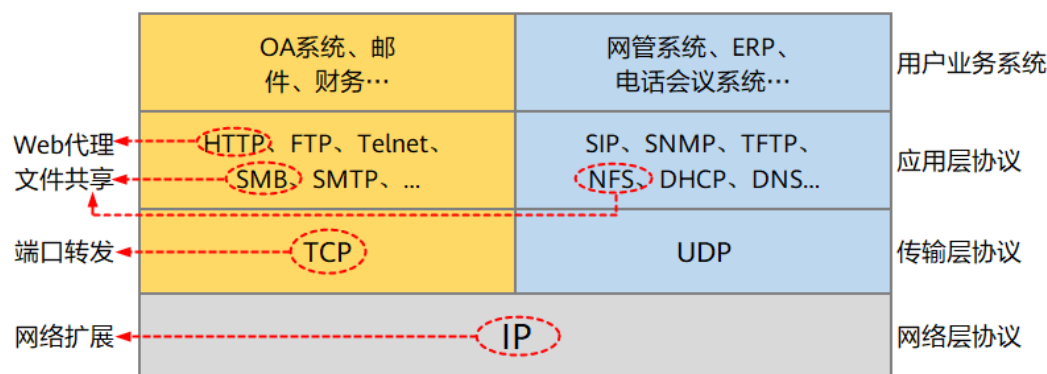


“双核”浏览器大致有以下几种：

- 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。

6.25 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。

6.26 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。

6.27 SVN 和防火墙 SSL VPN 特性区别有哪些

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

6.28 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。

6.29 使用客户端拨号登录无法生成虚拟网卡，如何解决

老版本SecoClient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7.0.5.1及其后续版本的SecoClient解决。

6.30 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。

6.31 SSL VPN 使用客户端拨号提示返回接收码超时，如何解决

老版本SecoClient部分驱动程序与操作系统不兼容，可能导致此问题，请安装7.0.5.1及其后续版本的SecoClient解决。

6.32 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，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SecoClient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。

6.33 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。

6.34 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。

6.35 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。

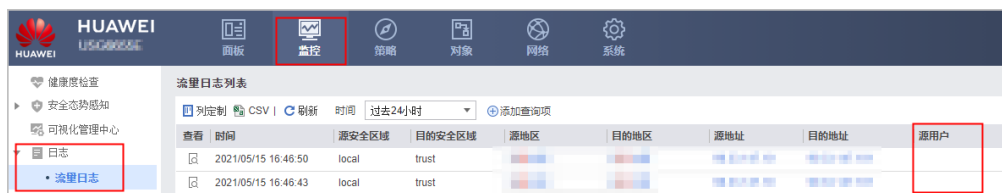
用户登录SSL VPN，启用网络扩展成功，记录日志：

```
%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。



3. 通过分析防火墙在故障时间点的流量日志及系统日志，找到执行非法操作的用户及其源IP地址。

6.36 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
```

6.37 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。

6.38 SSL VPN 有哪些常见调试日志

在调试业务过程中常见如下调试日志。

- 终端校验设备证书失败，弹出证书安全告警。
[NETC WARN 2021-03-31 00:32:42.000548][SSL Create failed][ErrorCode:19][reason:Verify first error,self signed certificate in certificate chain]
[NETC WARN 2021-03-31 00:32:42.000548][65535][SSL Create failed][reason:connect ssl error connectfd, return number is -1]
[CAUTH WARN 2021-03-31 00:32:42.000554][65535][Auth send failed][reason:netc connect error, code 1]
[NETC WARN 2021-03-31 00:32:42.000554][65535][Socket close failed][errorcode is 10038] //表示证书验证失败
[CAUTH WARN 2021-03-31 00:32:42.000554][65535][Master auth failed][reason:send auth pack to gateway error]
[CAUTH WARN 2021-03-31 00:32:42.000554][65535][Auth login process failed][auth master error]
[CADM INFO 2021-03-31 00:32:42.000554][65535][Normal Msg][biztype is 3 ,msgtype is 3 ,msgcode is 0x3000b]
- 用户登录，因为用户名/密码错误，提示“认证失败”。
[CAUTH INFO 2021-03-29 16:21:09.000423][65535][Auth send][auth package send to gateway successful]
[CAUTH INFO 2021-03-29 16:21:09.000423][65535][Master auth][send auth message to gateway ok]
[CAUTH WARN 2021-03-29 16:21:09.000424][65535][Auth login process][auth master ok]
[CAUTH INFO 2021-03-29 16:21:09.000430][65535][Auth receive ok][auth type 0]
[CAUTH INFO 2021-03-29 16:21:09.000431][65535][uiModule = 0 isRejCode= -5 puiCRejCode = 196609 //表示用户认证失败
[CADM INFO 2021-03-29 16:21:09.000432][65535][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 2021-03-29 16:22:00.000406][65535][Auth send][auth package send to gateway successful]
[CAUTH INFO 2021-03-29 16:22:00.000406][65535][Master auth][send auth message to gateway ok]
[CAUTH WARN 2021-03-29 16:22:00.000406][65535][Auth login process][auth master ok]
[CAUTH INFO 2021-03-29 16:22:00.000413][65535][Auth receive ok][auth type 0]
[CAUTH INFO 2021-03-29 16:22:00.000414][65535][uiModule = 0 isRejCode= -16 puiCRejCode = 196609 //表示用户账号被锁定
[CADM INFO 2021-03-29 16:22:00.000415][65535][Normal Msg][biztype is 3 ,msgtype is 3 ,msgcode is 0x30001]
- 用户登录，因为网络扩展功能未开启，提示“认证失败”。
[CAUTH INFO 2021-03-31 20:10:32.000653][65535][Auth send][auth package send to gateway successful]
[CAUTH INFO 2021-03-31 20:10:32.000653][65535][Master auth][send auth message to gateway ok]
[CAUTH WARN 2021-03-31 20:10:32.000653][65535][Auth login process][auth master ok]
[CAUTH INFO 2021-03-31 20:10:32.000907][65535][Auth receive ok][auth type 0]
[CAUTH INFO 2021-03-31 20:10:32.000907][65535][uiModule = 0 isRejCode= -4 puiCRejCode = 196609 //表示设备侧网络扩展功能未开启
[CADM INFO 2021-03-31 20:10:32.000907][65535][Normal Msg][biztype is 3 ,msgtype is 3 ,msgcode is 0x30001]
- 用户登录，因为用户没有网络扩展权限，提示“连接被网关拒绝，请检查网关配置参数”。
[CAUTH INFO 2021-03-31 18:47:03.000510][65535][Auth send][auth package send to gateway successful]
[CAUTH INFO 2021-03-31 18:47:03.000510][65535][Master auth][send auth message to gateway ok]
[CAUTH WARN 2021-03-31 18:47:03.000510][65535][Auth login process][auth master ok]
[CAUTH INFO 2021-03-31 18:47:03.000911][65535][Auth receive ok][auth type 0]
[CAUTH ERROR 2021-03-31 18:47:03.000911][65535][Auth receive failed][reason:receive error]

- [CADM INFO 2021-03-31 18:47:03.000911][65535][Normal Msg][biztype is 3 ,msgtype is 3 ,msgcode is 0x3000c] //表示用户没有网络扩展功能权限
- 虚拟网卡启动失败（一般由于数字签名不给操作系统识别导致）。

[VNIC WARN 2021-03-25 16:54:31.000316][Not find VNIC when get index
[VNIC INFO 2021-03-25 16:54:31.000317][VNIC state:2]
[VNIC ERROR 2021-03-25 16:54:31.000317][VNIC close failed][reason:timeout][Times :22][Line:581]
[VNIC ERROR 2021-03-25 16:54:31.000318][Close VNIC failed][Line :631]
[VNIC ERROR 2021-03-25 16:54:31.000318][Open VNIC failed][Line :848]
[CNEM ERROR 2021-03-25 16:54:31.000318][Cnem start failed][reason:Start VNIC Failed] //表示启用虚拟网卡失败
[CNEM ERROR 2021-03-25 16:54:31.000319][Cnem asyncmsg ioctl failed][reason:cnem start failed]
 - 终端主动退出登录。

[CAUTH INFO 2021-03-31 00:57:40.000023][65535][CAUTH_Module_Proc][in to CAUTH_Module_Proc]
[CAUTH ERROR 2021-03-31 00:57:40.000023][65535][Service cert failed][reason:Invalid parameter]
[CADM INFO 2021-03-31 00:57:40.000023][65535][Auth send][no need to set certinfo]
[CADM INFO 2021-03-31 00:57:40.000023][65535][Auth send][proxy info :0, user name:, proxy type: 0]
[NETC INFO 2021-03-31 00:57:40.000272][65535][SSL Connect][begin ssl create]
[NETC INFO 2021-03-31 00:57:40.000272][65535][SSL Create][Flag_Algorithm is 0]
[NETC INFO 2021-03-31 00:57:40.000272][65535][Print Cert aucCertIssuerName]
[aucCertIssuerName<>]
[NETC INFO 2021-03-31 00:57:41.000204][65535][SSL Create][Success]
[CAUTH INFO 2021-03-31 00:57:41.000204][65535][Auth send][biz type 9, code 0 logType 1]
[CAUTH INFO 2021-03-31 00:57:41.000204][65535][Auth send][auth package send to gateway successful]
[CADM INFO 2021-03-31 00:57:41.000204][65535][cadm bizctl process][entery bizctl proc srcbiz 3 and bizctl 40]
[CADM INFO 2021-03-31 00:57:41.000204][65535][cadm bizctl process][the biz start to exit biztype 5]
[CADM INFO 2021-03-31 00:57:41.000204][65535][cadm bizctl process][the biztype 5 exit msg is sending. notice_biz 20]
[CNEM INFO 2021-03-31 00:57:41.000204][65535][Cnem module proc][Enter]
[CADM INFO 2021-03-31 00:57:41.000204][65535][cadm bizctl process][the biz start to exit biztype 8]
[CNEM INFO 2021-03-31 00:57:41.000204][65535][Cnem module proc][Cnem moudle stop]
[CADM INFO 2021-03-31 00:57:41.000204][65535][cadm bizctl process][the notice has been send to src biz 3--EXIT WAIT] //表示用户主动退出
[ROUTE INFO 2021-03-31 00:57:41.000204][65535][Route Recovery][start]
[ROUTE INFO 2021-03-31 00:57:41.000220][65535][Route Recovery][Finish]
 - 设备侧踢用户下线。

[CNEM WARN 2021-03-31 01:01:03.000788][65535][Cnem handle packet from gateway][CMDtype is KICKOUT] //表示收到了设备侧踢用户下线的请求
[CNEM INFO 2021-03-31 01:01:03.000803][65535][Cnem send status msg to self ok]
[CNEM INFO 2021-03-31 01:01:03.000803][65535][Cnem module proc][Enter]
[CNEM INFO 2021-03-31 01:01:03.000803][65535][Cnem AsyncMsg BizNem Proc][Enter]
[CNEM INFO 2021-03-31 01:01:03.000803][65535][Cnem run][Enter]
[CNEM INFO 2021-03-31 01:01:03.000803][65535][Cnem run][the current status 145 and msgtype 13]
[CNEM ERROR 2021-03-31 01:01:03.000803][65535][Cnem receive or send packet failed][goto ERR Handle]
[ROUTE INFO 2021-03-31 01:01:03.000803][65535][Route Recovery][start]
[ROUTE INFO 2021-03-31 01:01:03.000819][65535][Route Recovery][Finish]
 - 保活超时，重连失败，退出登录。

[CNEM INFO 2021-03-31 01:12:17.000912][65535][Cnem reconnect][connect not exist,so RECONNECT]
[NETC INFO 2021-03-31 01:12:17.000912][65535][netc connect][connect 26dcdf0a :443 succeed]
[CNEM INFO 2021-03-31 01:12:17.000912][65535][Cnem UDPS create ok][2980]
[CNEM INFO 2021-03-31 01:12:17.000912][65535][Cnem SSL reconnect][get_proxy :0, name is:, type is:0]
[NETC INFO 2021-03-31 01:12:17.000912][65535][SSL Connect][set TCP NODELAY flag ok]
[NETC WARN 2021-03-31 01:12:22.000912][65535][SSL Connect failed][reason:ssl time out, reconnect] //表示重连超时
[NETC WARN 2021-03-31 01:12:27.000927][65535][SSL Connect failed][reason:ssl time out, reconnect]
[NETC WARN 2021-03-31 01:12:32.000943][65535][SSL Connect failed][reason:ssl time out, reconnect]

```
[ NETC ERROR 2021-03-31 01:12:32.000943 ][65535][SSL Connect failed][reason:reach max reconnect time]
[ CNEM ERROR 2021-03-31 01:12:32.000943 ][65535][Cnem SSL reconnect failed][reason:socket connect failed]
[ CNEM INFO 2021-03-31 01:12:32.000943 ][65535][Cnem reconnect][current reconnect times = 0]
[ CNEM INFO 2021-03-31 01:12:37.000943 ][65535][Cnem reconnect][connect not exist,so RECONNECT]
[ NETC INFO 2021-03-31 01:12:37.000943 ][65535][netc connect][connect 26dcaf0a :443 succeed]
[ CNEM INFO 2021-03-31 01:12:37.000943 ][65535][Cnem UDPS create ok][2980]
[ CNEM INFO 2021-03-31 01:12:37.000943 ][65535][Cnem SSL reconnect][get_proxy :0, name is:, type is:0]
[ NETC INFO 2021-03-31 01:12:37.000943 ][65535][SSL Connect][set TCP NODELAY flag ok]
[ NETC WARN 2021-03-31 01:12:42.000943 ][65535][SSL Connect failed][reason:ssl time out, reconnect]
[ NETC WARN 2021-03-31 01:12:47.000943 ][65535][SSL Connect failed][reason:ssl time out, reconnect]
[ NETC WARN 2021-03-31 01:12:52.000943 ][65535][SSL Connect failed][reason:ssl time out, reconnect]
[ NETC ERROR 2021-03-31 01:12:52.000943 ][65535][SSL Connect failed][reason:reach max reconnect time] //达到重连次数上限
```

- 用户登录SSL VPN成功，完整的日志。

```
[ CADM INFO 2021-03-30 22:38:46.000900 ][65535][Proxy info][ConnectType is <1>,Proxy type is <0>] //1表示SSL VPN, 0表示无代理
[ CADM INFO 2021-03-30 22:38:46.000901 ][65535][Proxy info][proxy is :0, user name is , proxy type is 0]
[ PREF INFO 2021-03-30 22:38:46.000902 ][65535][Link pref proc][Enter]
[ PREF INFO 2021-03-30 22:38:46.000902 ][65535][Link backup not open][Return choice site] //没有开启链路备份
[ CADM INFO 2021-03-30 22:38:46.000903 ][65535][Normal Msg][biztype is 1 ,msgtype is 1 ,msgcode is 0x10004]
[ CAUTH INFO 2021-03-30 22:38:46.000915 ][65535][CAUTH_Module_Proc][in to CAUTH_Module_Proc]
[ CAUTH INFO 2021-03-30 22:38:46.000916 ][65535][cauth][get the gateway ip is 10.175.220.38 and port is 443 from domain name]
[ CAUTH INFO 2021-03-30 22:38:46.000916 ][65535][cauth][get the gateway ip is 10.175.220.38 and port is 443 from domain name]
[ AUTH INFO 2021-03-30 22:38:46.000917 ][65535][Addr info][ip address is valid]
[ CAUTH INFO 2021-03-30 22:38:46.000918 ][65535][CAUTH_CTX_SetOPT][aucCertName<>]
[ CAUTH INFO 2021-03-30 22:38:46.000919 ][65535][Master auth][start]
[ ROUTE INFO 2021-03-30 22:38:46.000927 ][65535][mac Address = [0000-0000-0000]
[ NETC INFO 2021-03-30 22:38:47.000177 ][65535][SSL Connect][begin ssl create]
[ NETC INFO 2021-03-30 22:38:47.000177 ][65535][SSL Create][Flag_Algorithm is 0]
[ NETC INFO 2021-03-30 22:38:47.000178 ][65535][Print Cert aucCertIssuerName ] [aucCertIssuerName<>]
[ NETC INFO 2021-03-30 22:38:48.000070 ][65535][SSL Create][Success] //SSL握手成功
[ NETC ERROR 2021-03-30 22:38:48.000329 ][65535][NETC_Check_Domain][The number is not equal]
[ NETC WARN 2021-03-30 22:38:48.000946 ][65535][SSL Create failed][ErrorCode:19][reason:Verify first error,self signed certificate in certificate chain]
[ NETC WARN 2021-03-30 22:38:48.000947 ][65535][SSL Create failed][reason:connect ssl error connectfd, return number is -1]
[ CAUTH WARN 2021-03-30 22:38:48.000949 ][65535][Auth send failed][reason:netc connect error, code 1]
[ NETC WARN 2021-03-30 22:38:48.000950 ][65535][Socket close failed][errorcode is 10038] //证书校验失败, 弹出证书安全告警
[ CAUTH WARN 2021-03-30 22:38:48.000951 ][65535][Master auth failed][reason:send auth pack to gateway error]
[ CAUTH WARN 2021-03-30 22:38:48.000951 ][65535][Auth login process failed][auth master error]
[ CADM INFO 2021-03-30 22:38:48.000953 ][65535][Normal Msg][biztype is 3 ,msgtype is 3 ,msgcode is 0x3000b]
[ CADM INFO 2021-03-30 22:38:50.000955 ][65535][Proxy info][ConnectType is <1>,Proxy type is <0>] //用户点击忽略证书安全告警
[ CAUTH INFO 2021-03-30 22:38:52.000183 ][65535][Master auth][send auth message to gateway ok] //主认证, 发送认证请求去网关
[ CAUTH WARN 2021-03-30 22:38:52.000184 ][65535][Auth login process][auth master ok] //主认证成功
[ CAUTH INFO 2021-03-30 22:38:52.000923 ][65535][Auth receive ok][auth type 0]
[ CADM INFO 2021-03-30 22:38:52.000925 ][65535][Normal Msg][biztype is 3 ,msgtype is 2 ,msgcode is 0x20000]
```

```
[ CADM INFO 2021-03-30 22:38:52.000934 ][65535][SSL Start Nem][in to SSL_StartNem] //启用网络扩展服务/进程
[ VNIC INFO 2021-03-30 22:38:52.000979 ][65535][Start VNIC][begin] //启用虚拟网卡
[ VNIC INFO 2021-03-30 22:38:52.000983 ][65535][Find the VNIC][success]
[ VNIC INFO 2021-03-30 22:38:52.000998 ][65535][Nic Open][begin]
[ VNIC INFO 2021-03-30 22:38:53.000010 ][65535][Get VNIC name][name:本地连接]
[ VNIC INFO 2021-03-30 22:38:53.000011 ][65535][VNIC Start][open cmd is interface set interface "本地连接" admin=ENABLED]
[ CNEM INFO 2021-03-30 22:38:53.000156 ][65535][Cnem send status msg to self ok]
[ CNEM INFO 2021-03-30 22:38:53.000157 ][65535][Cnem Start OK] //网络扩展服务/进程启用完成
[ CNEM INFO 2021-03-30 22:38:53.000158 ][65535][Cnem module proc][Enter]
[ CADM INFO 2021-03-30 22:38:53.000158 ][65535][SSL Start Nem][exit SSL_StartNem]
[ CNEM INFO 2021-03-30 22:38:53.000160 ][65535][Cnem AsyncMsg BizNem Proc][Enter]
[ CNEM INFO 2021-03-30 22:38:53.000161 ][65535][Cnem run][Enter]
[ CNEM INFO 2021-03-30 22:38:53.000162 ][65535][Cnem run][the current status 0 and msgtype 0]
[ CNEM INFO 2021-03-30 22:38:53.000163 ][65535][Cnem SSL create][uiFd = 1924]
[ CNEM INFO 2021-03-30 22:38:53.000164 ][65535][Cnem SSL create][get proxy url : ,port :0, name is , type is 0]
[ NETC INFO 2021-03-30 22:38:53.000164 ][65535][SSL Connect][set TCP NODELAY flag ok]
[ NETC INFO 2021-03-30 22:38:53.000425 ][65535][SSL Connect][begin ssl create]
[ NETC INFO 2021-03-30 22:38:53.000427 ][65535][SSL Create][Flag_Algorithm is 0]
[ NETC INFO 2021-03-30 22:38:53.000428 ][65535][Print Cert aucCertIssuerName ][aucCertIssuerName<>]
[ NETC INFO 2021-03-30 22:38:54.000346 ][65535][SSL Create][Success] //网络扩展进程建立到网关的SSL连接成功
[ CNEM INFO 2021-03-30 22:38:54.000351 ][65535][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 2021-03-30 22:38:54.000608 ][65535][Cnem send status msg to self ok]
[ CNEM INFO 2021-03-30 22:38:54.000608 ][65535][Cnem module proc][Enter]
[ CNEM INFO 2021-03-30 22:38:54.000610 ][65535][Cnem AsyncMsg BizNem Proc][Enter]
[ CNEM INFO 2021-03-30 22:38:54.000611 ][65535][Cnem run][Enter]
[ CNEM INFO 2021-03-30 22:38:54.000612 ][65535][Cnem run][the current status 126 and msgtype 6]
[ CNEM INFO 2021-03-30 22:38:54.000613 ][65535][Cnem send vip request to gateway ok] //发送VIP请求去VPN网关
[ CNEM INFO 2021-03-30 22:38:54.000912 ][65535][Cnem parse new netcfginfo][Enter]
[ CNEM INFO 2021-03-30 22:38:54.000913 ][65535][Cnem parse new netcfginfo][DNS Server IP Num is 2] //从设备侧获得2个DNS服务器地址
[ CNEM INFO 2021-03-30 22:38:54.000913 ][65535][Cnem parse vip info from gateway ok] //从设备侧获得VIP信息
[ CNEM INFO 2021-03-30 22:38:55.000668 ][65535][Cnem send udp detect request to gateway OK] //发送UDP探测报文去VPN网关
[ CNEM INFO 2021-03-30 22:38:56.000026 ][65535][Cnem handle packet from gateway][CMDType is 15]
[ CNEM INFO 2021-03-30 22:38:56.000027 ][65535][Cnem handle packet from gateway][the UDPS tunnel is available] //UDPS隧道可用，接下来建立快速传输通道
[ CNEM INFO 2021-03-30 22:38:56.000028 ][65535][Cnem send status msg to self ok]
[ CNEM INFO 2021-03-30 22:38:56.000028 ][65535][Cnem module proc][Enter]
[ CNEM INFO 2021-03-30 22:38:56.000030 ][65535][Cnem AsyncMsg BizNem Proc][Enter]
[ CNEM INFO 2021-03-30 22:38:56.000030 ][65535][Cnem run][Enter]
[ CNEM INFO 2021-03-30 22:38:56.000031 ][65535][Cnem run][the current status 141 and msgtype 10]
[ CNEM INFO 2021-03-30 22:38:56.000684 ][65535][Cnem vnic set][astAddr[0].s_addr=13131313] - DNS服务器: 19.19.19.19
[ CNEM INFO 2021-03-30 22:38:56.000684 ][65535][Cnem vnic set][astAddr[1].s_addr=14131313] - DNS服务器: 19.19.19.20
[ CNEM INFO 2021-03-30 22:38:56.000032 ][65535][Cnem vnic set][GatewayIP = 26dcaf0a] //拨号VPN公网地址: 10.175.220.38
[ NETF INFO 2021-03-30 22:38:56.000032 ][65535][netf filter][init Enter]
[ VNIC INFO 2021-03-30 22:38:56.000033 ][65535][Get VNIC handle][begin]
[ VNIC INFO 2021-03-30 22:38:56.000034 ][65535][Get VNIC iofd][handle is 1936]
[ VNIC INFO 2021-03-30 22:38:56.000035 ][65535][Get VNIC Handle][success]
[ VNIC INFO 2021-03-30 22:38:56.000036 ][65535][Active VNIC][begin]
[ VNIC INFO 2021-03-30 22:38:56.000037 ][65535][Active VNIC][success]
[ VNIC INFO 2021-03-30 22:38:56.000039 ][65535][Set IP and MASK][begin]
[ VNIC INFO 2021-03-30 22:38:56.000040 ][65535][VNIC IP is 12.12.12.100] //虚拟IP地址信息
[ VNIC INFO 2021-03-30 22:38:56.000041 ][65535][VNIC mask is 255.255.255.0] //虚拟IP地址掩码信息
[ VNIC INFO 2021-03-30 22:38:56.000134 ][65535][Set IP and MASK][success] //设置虚拟网卡IP地
```



```

地址信息
[ VNIC INFO 2021-03-31 00:39:22.000812 ][65535][Set DNS Server IP][begin]
[ VNIC INFO 2021-03-31 00:39:23.000017 ][65535][VNIC Init][set DNS success] //设备虚拟网卡
DNS信息
[ ROUTE INFO 2021-03-30 22:38:59.000718 ][65535][Route set][Begin]:[63]
[ ROUTE INFO 2021-03-30 22:38:59.000719 ][65535][Route set][Before set route print the
routetable:] //注入VPN路由之前打印路由表
[ ROUTE INFO 2021-03-30 22:38:59.000721 ][65535][Route print
begin=====
=====
[ ROUTE INFO 2021-03-30 22:38:59.000744 ][65535][Route print
end=====
=====
[ ROUTE INFO 2021-03-30 22:38:59.000746 ][65535][Get best route info][Ip :10.47.0.1 Mask :
0x000000ff Nic index :68]
[ ROUTE INFO 2021-03-30 22:38:59.000747 ][65535][gateWay info][Ip :10.175.220.38 ]
[ ROUTE INFO 2021-03-30 22:38:59.000748 ][65535][BroadCast Route Judge ok][DestIP : 0xff0c0c0c]
[ ROUTE INFO 2021-03-30 22:38:59.000749 ][65535][Cleanup VNIC related route][Success] //先
清除旧的虚拟网卡路由
[ ROUTE INFO 2021-03-30 22:38:59.000750 ][65535][Set Mannual route][Begin]
[ ROUTE INFO 2021-03-30 22:38:59.000751 ][65535][manul inner route info][Dest:0x000d0d0d Mask:
0x00ffffff NextHop:0x640c0c0c IfIndex:15]
[ ROUTE INFO 2021-03-30 22:38:59.000752 ][65535][Initialize IP inFortation]
[ ROUTE INFO 2021-03-30 22:38:59.000753 ][65535][Set IP infortation][Success]
[ ROUTE INFO 2021-03-30 22:38:59.000778 ][65535][Unlawful route has been deleted]
[ ROUTE INFO 2021-03-30 22:38:59.000778 ][65535][dest: 12.12.12.0 , mask :255.255.255.0, next hop:
12.12.12.100, if:15, met:281]
[ ROUTE INFO 2021-03-30 22:38:59.000779 ][65535][BroadCast Route Judge ok][DestIP : 0xff0c0c0c]
[ ROUTE INFO 2021-03-30 22:38:59.000780 ][65535][BroadCast Route Judge ok][DestIP : 0xff01a8c0]
[ ROUTE INFO 2021-03-30 22:38:59.000780 ][65535][manul inner route info][Dest:0x00000e0e Mask:
0x0000ffff NextHop:0x640c0c0c IfIndex:15]
[ ROUTE ERROR 2021-03-30 22:38:59.000799 ][65535][Delete route Failed][ErrorCode:0]
[ ROUTE ERROR 2021-03-30 22:38:59.000800 ][65535][Delete Unsafe Route Failed][Line :772]
[ ROUTE INFO 2021-03-30 22:38:59.000800 ][65535][BroadCast Route Judge ok][DestIP : 0xff0c0c0c]
[ ROUTE INFO 2021-03-30 22:38:59.000801 ][65535][BroadCast Route Judge ok][DestIP : 0xff01a8c0]
[ ROUTE INFO 2021-03-30 22:38:59.000825 ][65535][Set manual mode route][Success]
[ ROUTE INFO 2021-03-30 22:38:59.000826 ][65535][After set route][Routetable:] //注入VPN
路由后打印路由表
[ ROUTE INFO 2021-03-30 22:38:59.000828 ][65535][Route print
begin=====
=====
[ ROUTE INFO 2021-03-30 22:38:59.000853 ][65535][Route print
end=====
=====

```

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

```

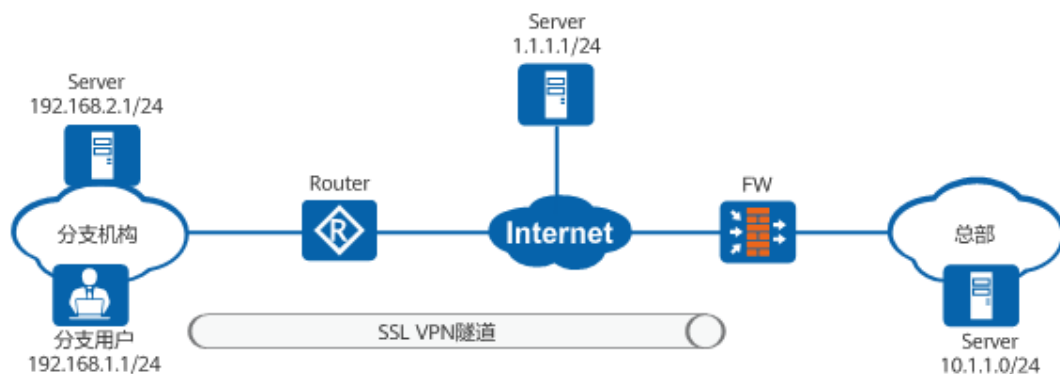
[GLOBAL]
ClientName = SecoClient
ClientVersion = 7.0.9.1
ClientCustomized = false
ClientLogLevel = 1 //修改为0，DEBUG级别日志也会记录

```

6.39 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：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。

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
=====
    
```

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
=====

```

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
=====

```

由	6.6.6.1	255.255.255.255	On-link	6.6.6.1	257	//访问企业内网的路
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
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
路由	192.168.2.255	255.255.255.255	On-link	6.6.6.1	257	//访问企业内网

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）。

6.40 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。

7 相关资源

- [HUAWEI USG6000, USG9500, NGFW Module配置指南-SSL VPN](#)