# 一、开始

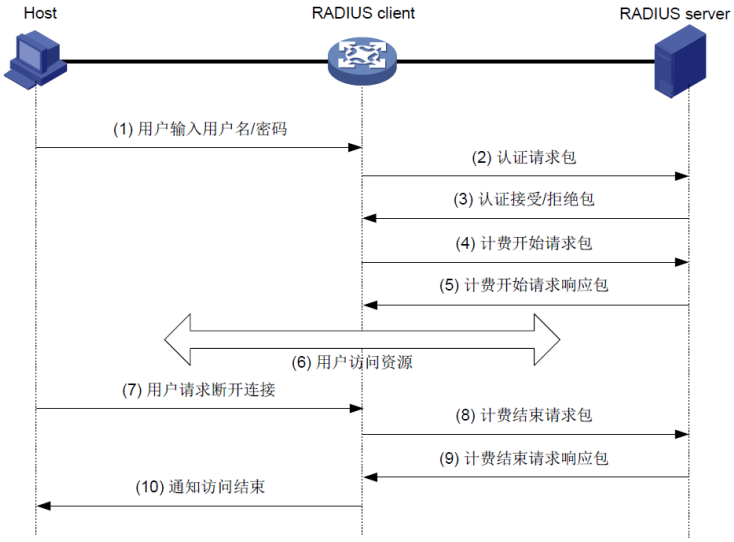
SSL VPN 以 SSL（Secure Sockets Layer，安全套接字层）为基础提供远程的安全连接服务。用户可通过互联网，使用 SSL 协议与远端的 SSL VPN 网关建立安全的连接，同时 SSL VPN 网关负责对 SSL VPN 用户身份进行认证和授权，用户身份认证且授权通过后，便能访问对应的内网资源。用户认证包括：用户名/密码认证、证书认证、用户名/密码和证书的组合认证。其中用户名/密码认证是最常见的，通过配合 AAA（Authentication、Authorization、Accounting，认证、授权、计费）的网络安全管理机制，对 SSL VPN 用户提供认证以及后续授权、计费等安全功能。AAA 可以通过多种协议来实现，这些协议规定了设备与服务器之间如何传递用户信息。目前设备支持 RADIUS（Remote Authentication Dial-In User Service，远程认证拨号用户服务）协议、HWTACACS（HW Terminal Access Controller Access Control System，HW 终端访问控制器控制系统协议）协议和 LDAP（Lightweight Directory Access Protocol，轻量级目录访问协议）协议。本文主要讲述 SSL VPN 结合 RADIUS 服务器进行认证和授权的排错步骤。

RADIUS 是一种分布式的、客户端/服务器结构的信息交互协议，能保护网络不受未授权访问的干扰，常应用在既要求较高安全性、又允许远程用户访问的各种网络环境中。RADIUS 协议合并了认证和授权的过程，它定义了 RADIUS 的报文格式及其消息传输机制，并规定使用 UDP 作为封装 RADIUS 报文的传输层协议，UDP 端口 1812、1813 分别作为认证/授权、计费端口。

RADIUS 的部署模式是**客户端/服务器模式：**

- 客户端：RADIUS 客户端一般位于 NAS 上，可以遍布整个网络，负责将用户信息传输到指定的 RADIUS 服务器，然后根据服务器返回的信息进行相应处理（如接受/拒绝用户接入）。
- 服务器：RADIUS 服务器一般运行在中心计算机或工作站上，维护用户的身份信息和与其相关的网络服务信息，负责接收 NAS 发送的认证、授权、计费请求并进行相应的处理，然后给 NAS 返回处理结果（如接受/拒绝认证请求）。另外，RADIUS 服务器还可以作为一个代理，以 RADIUS 客户端的身份与其它的 RADIUS 认证服务器进行通信，负责转发 RADIUS 认证和计费报文。如下图所示为例，Microsoft Windows Server 系统的网络策略服务器（NPS）组件是一种常用的 RADIUS 服务器平台。


用户、RADIUS 客户端和 RADIUS 服务器之间的交互流程如图所示。




消息交互流程如下：

(1) 用户发起连接请求，向 RADIUS 客户端发送用户名和密码。

(2) RADIUS 客户端根据获取的用户名和密码，向 RADIUS 服务器发送认证请求包（Access-Request），其中的密码在共享密钥的参与下利用 MD5 算法进行加密处理。

(3) RADIUS 服务器对用户名和密码进行认证。如果认证成功，RADIUS 服务器向 RADIUS 客户端发送认证接受包（Access-Accept）；如果认证失败，则返回认证拒绝包（Access-Reject）。由于 RADIUS 协议合并了认证和授权的过程，因此认证接受包中也包含了用户的授权信息。

(4) RADIUS 客户端根据接收到的认证结果接入/拒绝用户。如果允许用户接入，则 RADIUS

客户端向 RADIUS 服务器发送计费开始请求包（Accounting-Request）。

(5) RADIUS 服务器返回计费开始响应包（Accounting-Response），并开始计费。

(6) 用户开始访问网络资源。

(7) 用户请求断开连接。

(8) RADIUS 客户端向 RADIUS 服务器发送计费停止请求包（Accounting-Request）。

(9) RADIUS 服务器返回计费结束响应包（Accounting-Response），并停止计费。

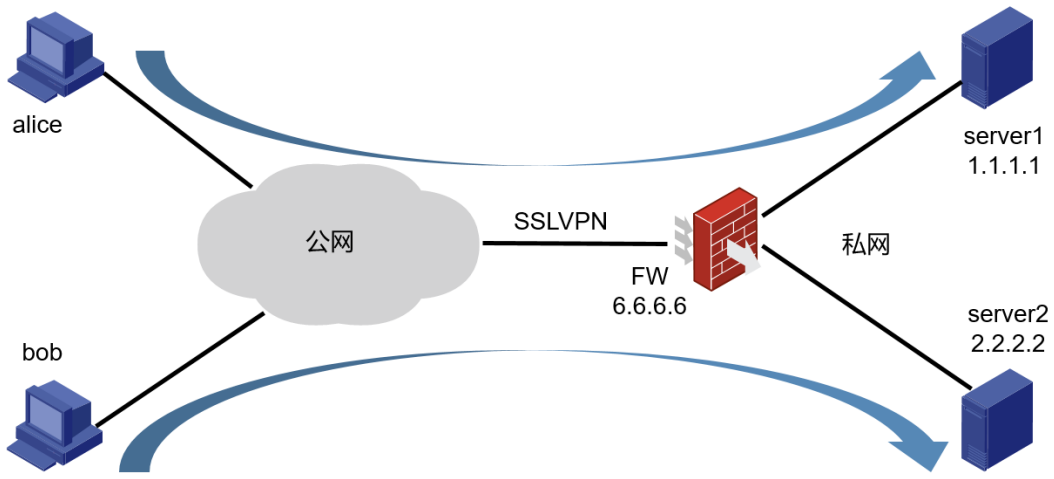
(10) 通知用户结束访问网络资源。

本文致力于 Comware V7 NGFW 系列防火墙 SSL VPN 功能结合 Microsoft Windows Server 系统的网络策略服务器（NPS）组件进行认证和授权的排错步骤。

## 二、流程图说明

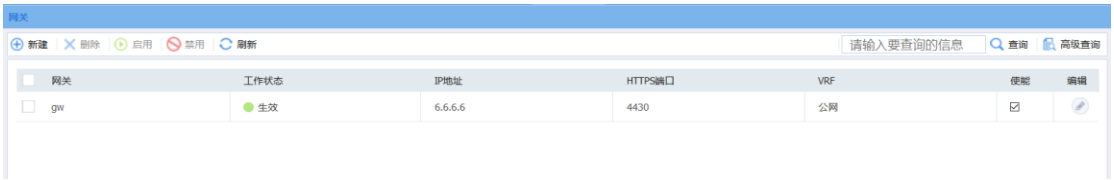
### 1， 检查本地认证和授权是否正常

本文如下图组网为例，用户 alice 和 bob 需要通过 NGFW 系列防火墙提供的 SSL VPN 网关接口来访问内网的服务器资源，且授权规定 alice 只能访问 server1，bob 只能访问 server2。




SSL VPN 本地认证时 Web 界面可以如下配置：

(1) 创建 SSL VPN 网关，使用 FW 公网口地址，修改端口号为 4430。




(2) 创建 SSL VPN 访问实例，ISP 认证域不勾选，缺省对接入用户使用本地认证和本地授权。

(3) 业务选择为 IP 业务，创建两个 IP 接入资源，分别为 server1（1.1.1.1）和 server2（2.2.2.2）。


(4) 创建两个资源组名为 pg1 和 pg2，pg1 调用 server1，pg2 调用 server2。


(5) 创建两个 SSL VPN 用户 alice 和 bob，分别关联 SSL VPN 策略组 pg1 和 pg2。

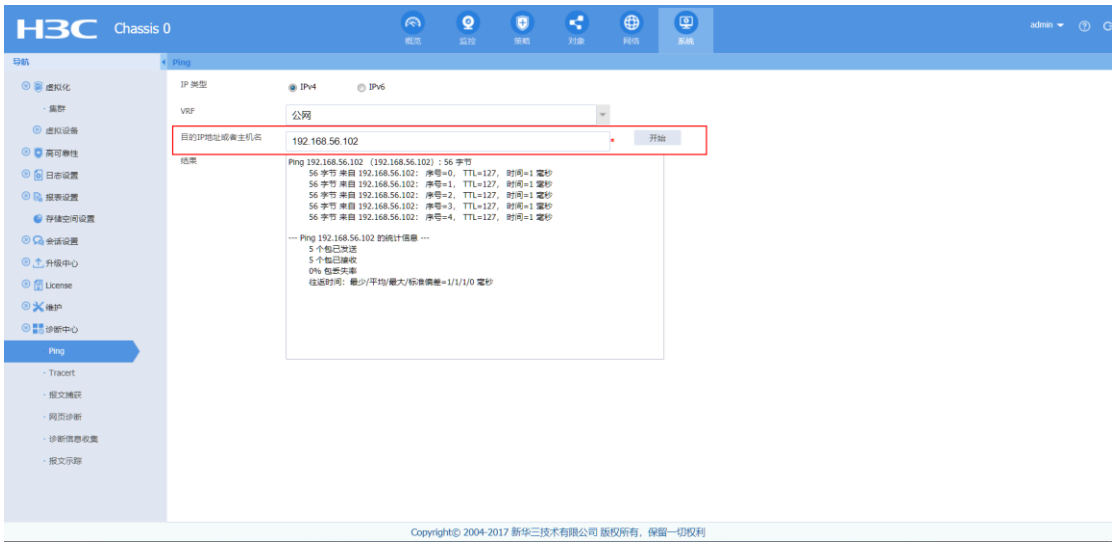

(6) 放通防火墙相关策略并进行拨号测试，以用户 alice 为例，拨号成功后可以正常访问 server1（1.1.1.1），但不能访问 server2（2.2.2.2）。


如果本地认证和授权出现问题，请联系 400 热线进行处理。

## 2， 检查 RADIUS 服务器是否可达

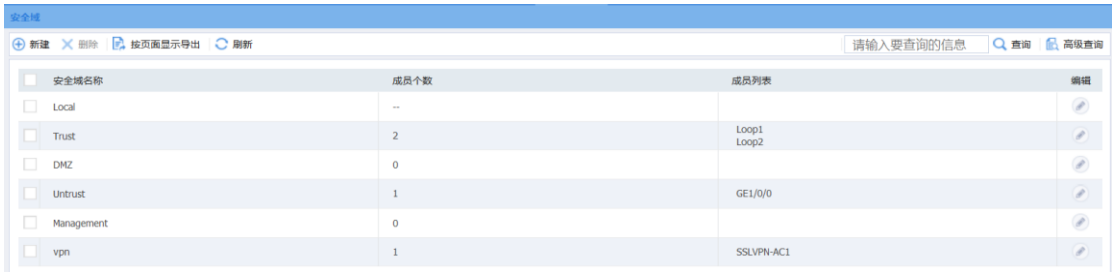
确保本地认证和授权测试无问题后，此时再进行 RADIUS 的相关配置和检查。

首先得确认 RADIUS 两端的网络层是否互通，可以在防火墙上 ping RADIUS 服务器的公网地址测试网络是否可达。如下图所示为例，实验室测试 RADIUS 地址 192.168.56.102。。

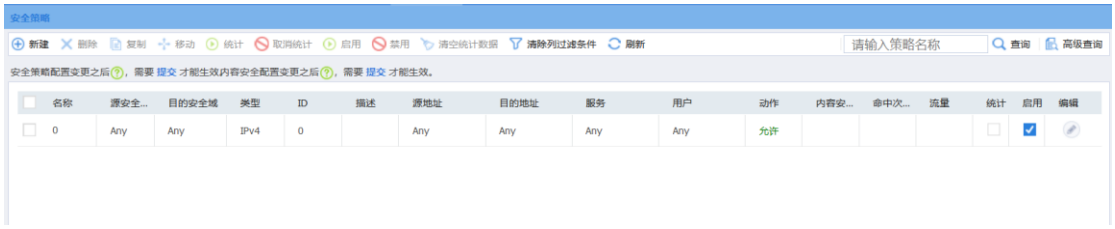



如果 ping 不可达，先排查一下防火墙安全域和安全策略的配置是否正确：

- 安全域的配置：首先需要检查相应的接口是否加入了安全域。



- 安全策略的配置：检查本地域和该安全域之间的安全策略是否放通。



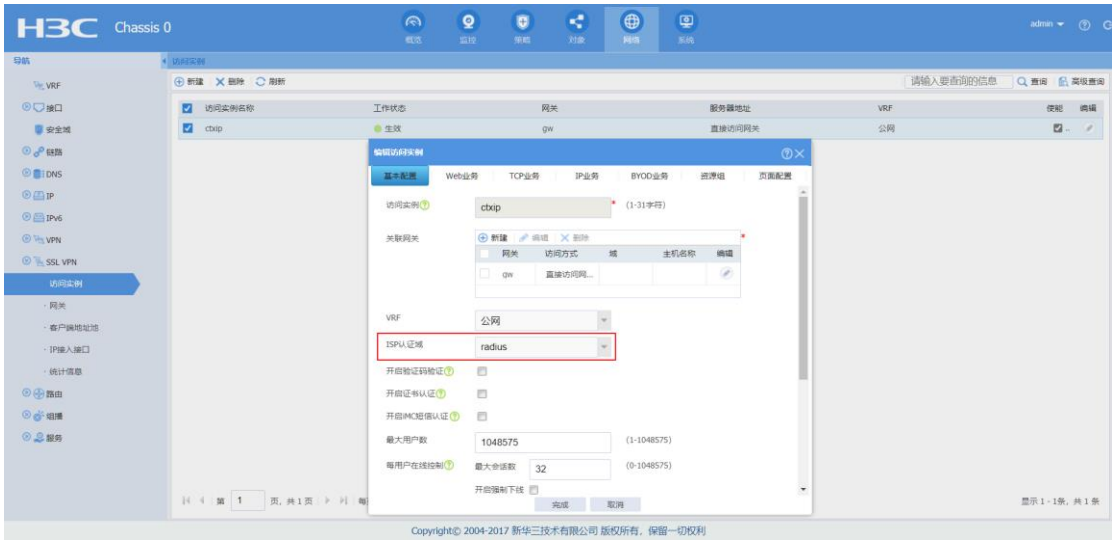

如上图所示，本地测试是全放通策略，所以不存在安全策略阻断的问题。如果现场的安全策略配置十分明细且复杂，建议在 ping 测试结果中打开调试开关。

命令： debugging security-policy packet ip acl XXXX（acl 建议写双向明细规则）

```
<H3C>debugging security-policy packet ip acl 3999
This command is CPU intensive and might affect ongoing services. Are you sure you want to
continue? [Y/N]:Y
<H3C>terminal monitor
The current terminal is enabled to display logs.
<H3C>terminal debugging
The current terminal is enabled to display debugging logs.
```

(1) 如果调试中显示对应的流有 The packet is denied，说明的确是安全策略进行了阻断，需要再仔细检查一下策略的配置。关于防火墙安全策略不通排查，本文不再详细阐述。确认安全策略配置没有问题后，就需要结合防火墙抓包判断中间链路以及 RADIUS 服务器是否存在问题了。

(2) 如果链路连通性没有问题，可以将 SSL VPN 的认证方式修改为已经配置好的 RADIUS 认证方案。如下图所示为例，在 Web 界面进行配置，如下在“网络->SSL VPN->访问实例->编辑访问实例”中将【ISP 认证域】设置为已经配置好的 RADIUS 认证方案，在此实验案例中，方案名称为“RADIUS”。




(3) 如果 RADIUS 认证相关服务存在问题，请按照下面的步骤进行排查。

### 3， 检查 RADIUS 服务器状态是否正常

RADIUS 方案中各服务器的状态（active、block）决定了设备向哪个服务器发送请求报文，以及设备在与当前服务器通信中断的情况下，如何转而与另外一个服务器进行交互。在实际组网环境中，可指定一个主 RADIUS 服务器和多个从 RADIUS 服务器，由从服务器作为主服务器的备份。当 RADIUS 服务器负载分担功能处于开启状态时，设备仅根据当前各服务器承载的用户负荷调度状态为 active 的服务器发送认证请求。当 RADIUS 服务器负载分担功能处于关闭状态时，设备上主从服务器的切换遵从以下原则：

- 当主服务器状态为 active 时，设备首先尝试与主服务器通信，若主服务器不可达，则按照从服务器的配置先后顺序依次查找状态为 active 的从服务器。只要存在状态为 active 的服务器，设备就仅与状态为 active 的服务器通信，即使该服务器不可达，设备也不会尝试与状态为 block 的服务器通信。
- 当主/从服务器的状态均为 block 时，若主服务器状态是自动设置为 block 且已配置主服务器，则采用主服务器进行认证；若主服务器状态是被手工设置为 block 或未配置主服务器，则在自动设置为 block 状态的所有从服务器中按顺序选择从服务器进行认证
- 如果服务器不可达，则设备将该服务器的状态置为 block，并启动该服务器的 quiet 定时器。当服务器的 quiet 定时器超时，或者手动将服务器状态置为 active 时，该服务器将恢复为 active 状态。
- 在一次认证过程中，如果设备在尝试与从服务器通信时，之前已经查找过的服务器状态由 block 恢复为 active，则设备并不会立即恢复与该服务器的通信，而是继续查找从服务器。如果所有已配置的服务器都不可达，则认为本次认证失败。

- 如果在认证过程中删除了当前正在使用的服务器，则设备在与该服务器通信超时后，将会立即从主服务器开始依次查找状态为 active 的服务器并与之进行通信。
- 一旦服务器状态满足自动切换的条件，则所有 RADIUS 方案视图下该服务器的状态都会相应地变化。将认证服务器的状态由 active 修改为 block 时，若该服务器引用了 RADIUS 服务器探测模板，则关闭对该服务器的探测功能；反之，将认证服务器的状态由 block 更改为 active 时，若该服务器引用了一个已存在的 RADIUS 服务器探测模板，则开启对该服务器的探测功能。
- 缺省情况下，设备将配置了 IP 地址的各 RADIUS 服务器的状态均置为 active，认为所有的服务器均处于正常工作状态，但有些情况下用户可能需要通过以下配置手工改变 RADIUS 服务器的当前状态。例如，已知某服务器故障，为避免设备认为其 active 而进行无意义的尝试，可暂时将该服务器状态手工置为 block。

设置的服务器状态不能被保存在配置文件中，可通过在 Web 界面进行查看，如下在“对象->用户->认证管理->RADIUS->修改 RADIUS 方案”中查看认证服务器的状态。


**4， 修改 RADIUS 服务器状态**

可以在 Web 界面进行配置，如下在“对象->用户->认证管理->RADIUS-> RADIUS 方案->修改 RADIUS 方案->修改主认证服务器”中将【状态】设置为“活动”。


此外，设备重启后，各服务器状态将恢复为缺省状态 active。

### 5， 检查 RADIUS 报文源地址是否正确

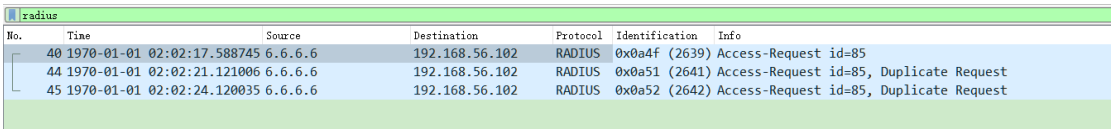
RADIUS 服务器上通过 IP 地址来标识接入设备，并根据收到的 RADIUS 报文的源 IP 地址是否与服务器所管理的接入设备的 IP 地址匹配，来决定是否处理来自该接入设备的认证请求。若 RADIUS 服务器收到的 RADIUS 认证报文的源地址在所管理的接入设备 IP 地址范围内，则会进行后续的认证处理，否则直接丢弃该报文。设备发送 RADIUS 报文时，根据以下顺序查找使用的源 IP 地址：

(1) 当前所使用的 RADIUS 方案中配置的发送 RADIUS 报文使用的源 IP 地址。

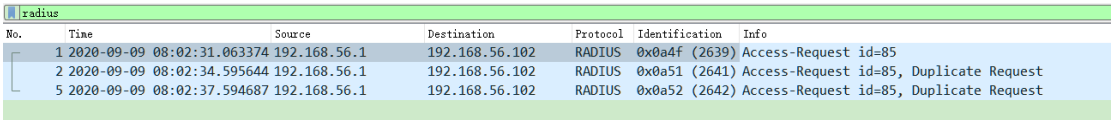
(2) 根据当前使用的服务器所属的 VPN 查找系统视图下通过 RADIUS nas-ip 命令配置的私网源地址，对于公网服务器则直接查找该命令配置的公网源地址。

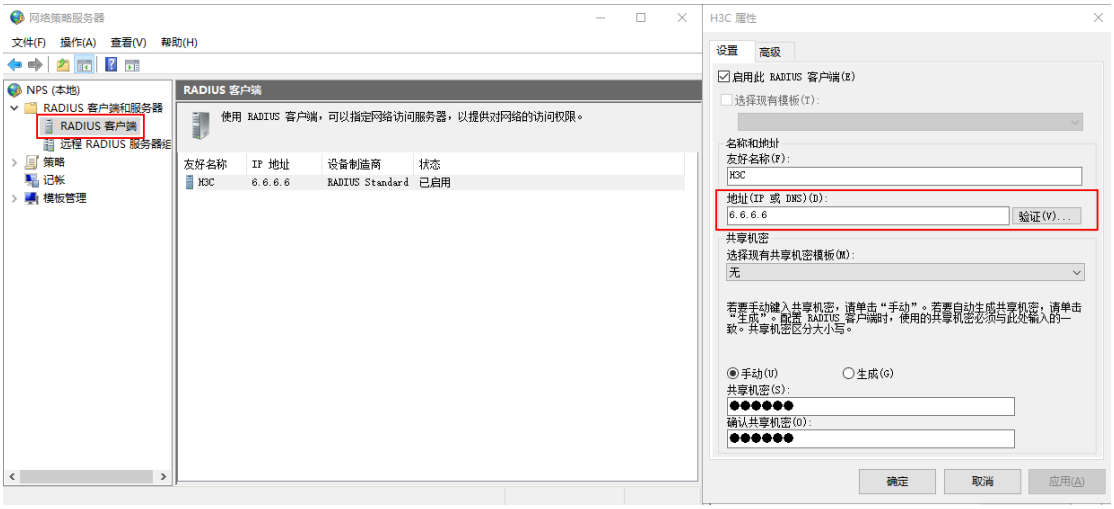
(3) 通过路由查找到的发送 RADIUS 报文的出接口地址

如果防火墙到 RADIUS 服务器之间的设备做了 NAT，将防火墙发出的 RADIUS 报文源地址改变了，但是 RADIUS 服务器上设置的 RADIUS 客户端地址依旧是转换前的地址，那么认证报文就会被 RADIUS 服务器丢弃，且不会有任何报文回应。如下防火墙上抓包的 RADIUS 报文的源地址为 6.6.6.6，目的地址为 192.168.56.102；




但是在 RADIUS 服务器上抓包来看，相同的报文 Identification 字段相同，源地址已经变成了 192.168.56.1。






## 6， 修改 RADIUS 报文源地址

RADIUS 客户端发送 RADIUS 报文使用的源 IP 地址在系统视图和 RADIUS 方案视图下均可配置，系统视图下的配置将对所有 RADIUS 方案生效，RADIUS 方案视图下的配置仅对本方案有效，并且具有高于前者的优先级。为保证认证报文可被服务器正常接收并处理，接入设备上发送 RADIUS 报文使用的源 IP 地址必须与 RADIUS 服务器上指定的接入设备的 IP 地址保持一致。

通常，该地址为接入设备上与 RADIUS 服务器路由可达的接口 IP 地址，为避免物理接口故障时从服务器返回的报文不可达，推荐使用 Loopback 接口地址为发送 RADIUS 报文使用的源 IP 地址。但在一些特殊的组网环境中，例如在接入设备使用 VRRP（Virtual Router Redundancy Protocol，虚拟路由器冗余协议）进行双机热备应用时，可以将该地址指定为 VRRP 上行链路所在备份组的虚拟 IP 地址。

可以在 Web 界面进行配置，如下在“对象->用户->认证管理->RADIUS-> RADIUS 方案->修改 RADIUS 方案”中将【发送 RADIUS 报文使用的源 IPv4 地址】设置为出接口地址 6.6.6.6。

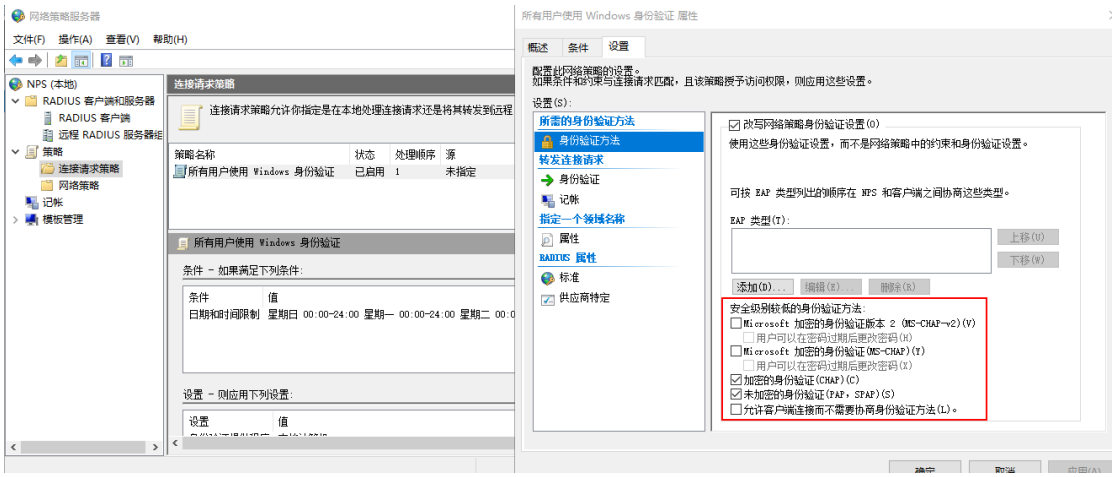

同时 RADIUS 服务器上设置 RADIUS 客户端的 IP 地址为 RADIUS 报文到达服务器的真实源地址，这里为 192.168.56.1。


## 7， 检查 RADIUS 服务器共享密钥是否配置正确

RADIUS 客户端和 RADIUS 服务器之间认证消息的交互是通过共享密钥的参与来完成的，共享密钥是一个带外传输的客户端和服务器都知道的字符串，不需要单独进行网络传输。RADIUS 报文中有一个 16 字节的验证字字段，它包含了对整个报文的数字签名数据，该签名数据是在共享密钥的参与下利用 MD5 算法计算出的，收到 RADIUS 报文的一方要验证该签名的正确性，如果报文的签名不正确，则丢弃它。通过这种机制，保证了 RADIUS 客户端和 RADIUS 服务器之间信息交互的安全性。

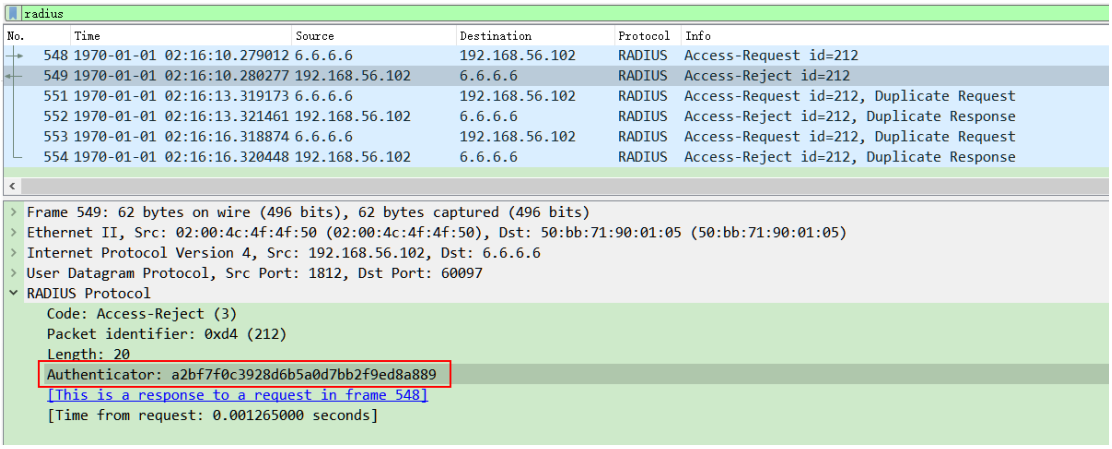
```
> Internet Protocol Version 4, Src: 6.6.6.6, Dst: 192.168.56.102
> User Datagram Protocol, Src Port: 60097, Dst Port: 1812
v RADIUS Protocol
    Code: Access-Request (1)
    Packet identifier: 0x55 (85)
    Length: 225
    Authenticator: 2d141feec7ad32775ec1f2dbb42b0db9
  v Attribute Value Pairs
    > AVP: t=User-Name(1) l=5 val=bob
    > AVP: t=User-Password(2) l=18 val=Encrypted
    > AVP: t=Service-Type(6) l=6 val=Framed(2)
    > AVP: t=NAS-Identifier(32) l=5 val=H3C
    > AVP: t=Calling-Station-Id(31) l=19 val=02-00-4c-4f-4f-50
    > AVP: t=Acct-Session-Id(44) l=40 val=00000011202009091602240000000308100161
    > AVP: t=Vendor-Specific(26) l=30 vnd=H3C(25506)
    > AVP: t=Framed-IP-Address(8) l=6 val=6.6.6.7
    > AVP: t=Vendor-Specific(26) l=33 vnd=H3C(25506)
    > AVP: t=NAS-IP-Address(4) l=6 val=6.6.6.6
    > AVP: t=Vendor-Specific(26) l=25 vnd=H3C(25506)
    > AVP: t=Vendor-Specific(26) l=12 vnd=H3C(25506)
```

另外，为防止用户密码在不安全的网络上传递时被窃取，在 RADIUS 报文传输过程中还利用共享密钥对用户密码进行了加密。RADIUS 服务器支持多种方法来认证用户，例如 PAP（Password Authentication Protocol，密码认证协议）、CHAP（Challenge Handshake Authentication Protocol，质询握手认证协议）以及 EAP（Extensible Authentication Protocol，可扩展认证协议）。




为防止数据包中数据被截获被篡改，回应鉴别码采用如下方式生成：RespOnseAuth=MD5(Code+ID+Length+RequestAuth+ Attributes+Secret)，回应鉴别码是对整个数据包进行 MD5 演算产生的 16 字节索引，防止伪造服务器的回应。

如果共享密钥不对，RADIUS 会发送 reject 拒绝报文，RADIUS 客户端会再重复请求两次，相应的，RADIUS 服务器针对每一次请求，都会回应一个拒绝。




同时 debugging RADIUS error 会有“Invalid packet authenticator”报错。

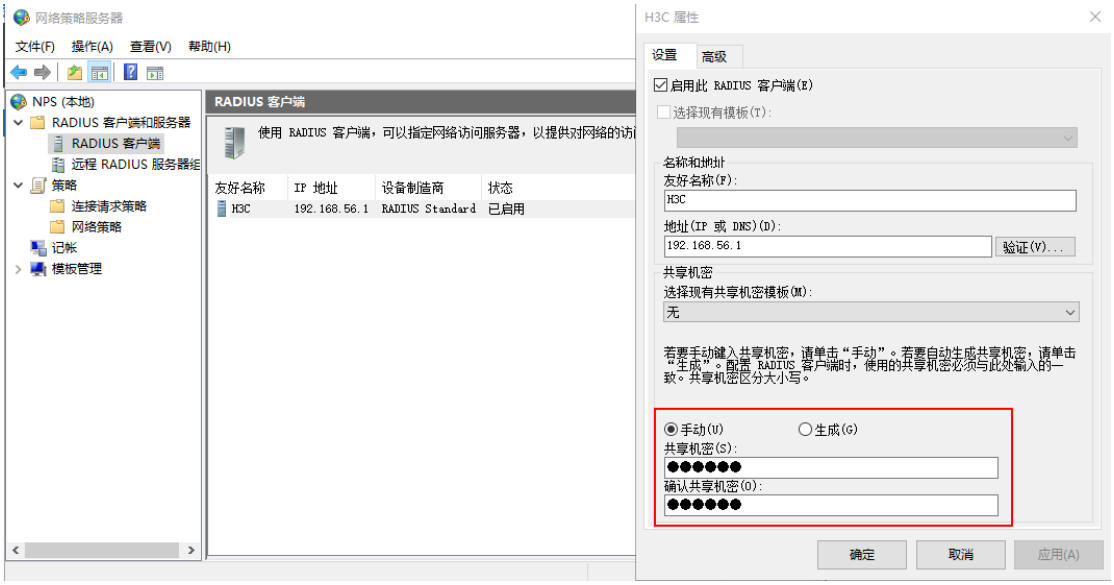
```
*Sep  9 16:17:31:819 2020 H3C RADIUS/7/ERROR: -Context=1;
Reply packet: Invalid packet authenticator.
*Sep  9 16:17:31:819 2020 H3C RADIUS/7/ERROR: -Context=1;
The reply packet is invalid.
*Sep  9 16:17:34:961 2020 H3C RADIUS/7/ERROR: -Context=1;
Reply packet: Invalid packet authenticator.
*Sep  9 16:17:34:962 2020 H3C RADIUS/7/ERROR: -Context=1;
The reply packet is invalid.
*Sep  9 16:17:37:963 2020 H3C RADIUS/7/ERROR: -Context=1;
Reply packet: Invalid packet authenticator.
*Sep  9 16:17:37:963 2020 H3C RADIUS/7/ERROR: -Context=1;
The reply packet is invalid.
```

说明 RADIUS 提供的 MD5 加密，设备侧无法验证，可见两端的共享密钥不匹配。

## 8， 修改 RADIUS 服务器共享密钥

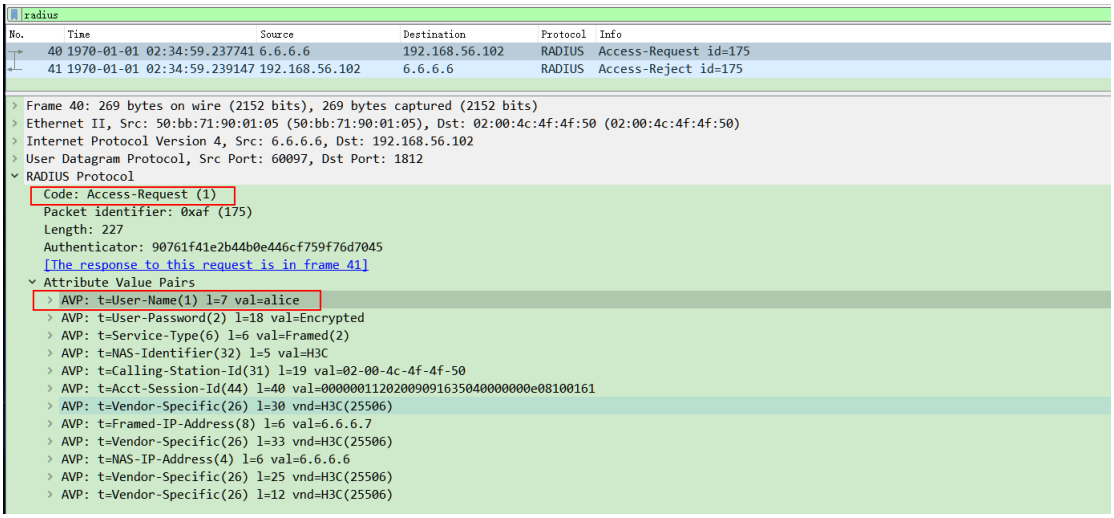
可以在 Web 界面进行配置，如下在“对象->用户->认证管理->RADIUS-> RADIUS 方案->修改 RADIUS 方案->修改主认证服务器”中将【共享密钥】设置为“123456”。

同时在 RADIUS 服务器将对应 RADIUS 客户端的共享密钥设置一致。




## 9， 检查 VPN 用户名和密码是否正确

RADIUS 实现用户认证是其基本功能，如果用户名或者账号密钥不正确，RADIUS 服务器直接返回 Reject 报文。




同时，在 debugging RADIUS all 中可以看到 resultCode 为 1 的打印信息。

```
*Sep  9 16:31:13:493 2020 H3C RADIUS/7/EVENT: -Context=1;
Received reply packet successfully.
*Sep  9 16:31:13:493 2020 H3C RADIUS/7/EVENT: -Context=1;
Found request context, dstIP: 192.168.56.102, dstPort: 1812, VPN instance: --
(public), socketFd: 48, pktID: 207.
*Sep  9 16:31:13:493 2020 H3C RADIUS/7/EVENT: -Context=1;
The reply packet is valid.
*Sep  9 16:31:13:493 2020 H3C RADIUS/7/EVENT: -Context=1;
Decoded reply packet successfully.
*Sep  9 16:31:13:493 2020 H3C RADIUS/7/PACKET: -Context=1;
 03 cf 00 14 56 94 a9 a0 b9 c4 b4 2c d2 49 0b 06
 04 29 7b 55
*Sep  9 16:31:13:493 2020 H3C RADIUS/7/EVENT: -Context=1;
Sent reply message successfully.
*Sep  9 16:31:13:493 2020 H3C RADIUS/7/EVENT: -Context=1;
PAM_RADIUS: Processing RADIUS authentication.
*Sep  9 16:31:13:493 2020 H3C RADIUS/7/EVENT: -Context=1;
PAM_RADIUS: Fetched authentication reply-data successfully, resultCode: 1
```

## 10， 修改 VPN 用户名和密码

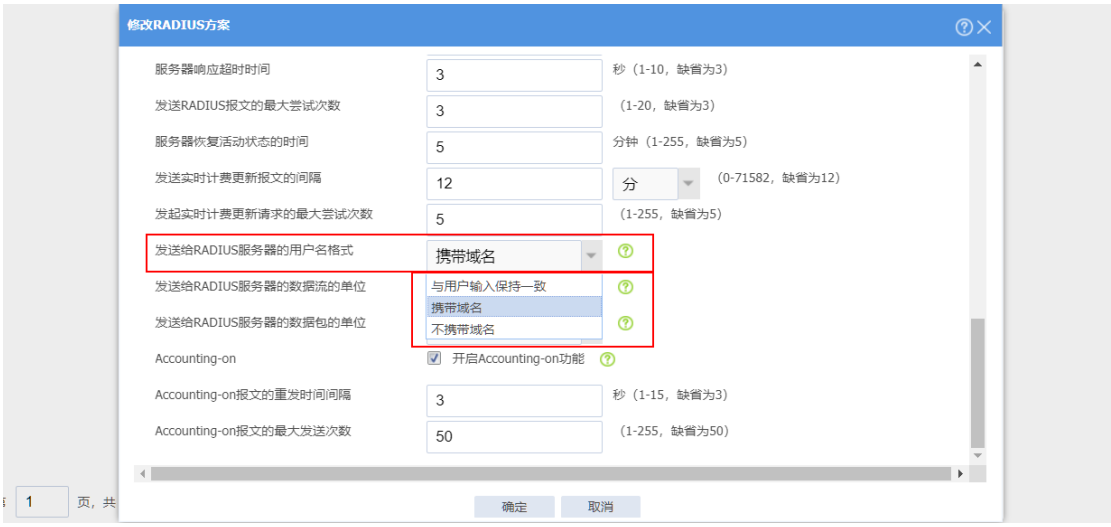
接入用户通常以“userid@isp-name”的格式命名，“@”后面的部分为 ISP 域名，设备通过该域名决定将用户归于哪个 ISP 域。由于有些较早期的 RADIUS 服务器不能接受携带有 ISP 域名的用户名，因此就需要设备首先将用户名中携带的 ISP 域名去除后再传送给该类 RADIUS 服务器。通过设置发送给 RADIUS 服务器的用户名格式，就可以选择发送 RADIUS 服务器的用户名中是否要携带 ISP 域名，以及是否保持用户输入的原始用户名格式。

如果要在两个乃至两个以上的 ISP 域中引用相同的 RADIUS 方案，建议设置该 RADIUS 方案允许用户名中携带 ISP 域名，使得 RADIUS 服务器端可以根据 ISP 域名来区分不同的用户。

如果指定某个 RADIUS 方案不允许用户名中携带有 ISP 域名，那么请不要在两个或两个以上的 ISP 域中同时设置使用该 RADIUS 方案。否则，会出现虽然实际用户不同（在不同的 ISP 域中），但 RADIUS 服务器认为用户相同（因为传送到它的用户名相同）的错误。

设备发送给 RADIUS 服务器的用户名格式有三种方式，如下：

- keep-original：发送给 RADIUS 服务器的用户名与用户的输入保持一致。
- with-domain：发送给 RADIUS 服务器的用户名携带 ISP 域名。
- without-domain：发送给 RADIUS 服务器的用户名不携带 ISP 域名。

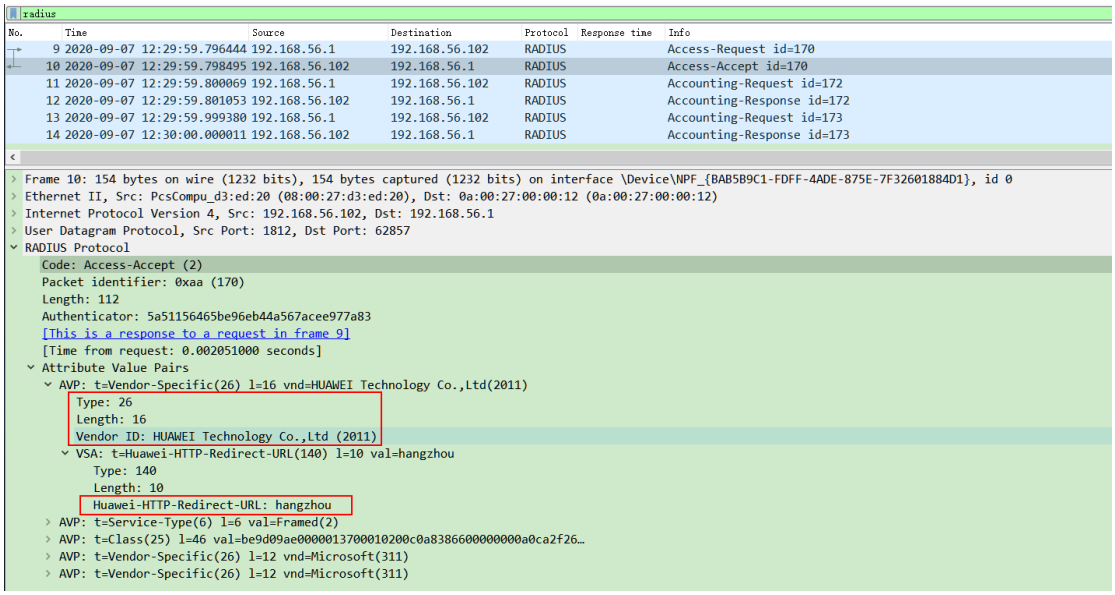



## 11， 检查 RADIUS 属性映射是否正确

H3C SSL VPN 采用的是外部认证服务器授权的方式（这样做的好处就是无需在本地重复创建认证用户），在这种情况下，如果管理员要区分不同用户的访问权限，需要 RADIUS 服务器进行授权用户组的下发。我们规定该授权信息的下发是通过厂商自定义属性中的子属性来下发。RADIUS 协议标准规定第 26 号属性（Vendor-Specific）为厂商自定义属性，通过该属性各个厂商可以在 RADIUS 的认证授权过程中下发自己特有的一些属性。我们就是通过这种方式来下发我们的用户组属性的。厂商自定义属性的格式如下：

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      Type       |  Length       |             Vendor-Id
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     Vendor-Id (cont)            | Vendor type   | Vendor length |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Attribute-Specific...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

要求 Vendor-Id 字段的值为 **2011**，同时 Vendor type 字段的值为 **140**，Atrribute 字段的值为要下发的用户组名如 hangzhou（需要在 SSL VPN 网关上创建和下发用户组名相同的用户组）。下面是一个具体的报文格式，该报文中要下发的用户组名为 hangzhou。




在实际的联动认证中，请参考该指导设定 RADIUS 服务器参数以便能够正确下下发用户组信息。

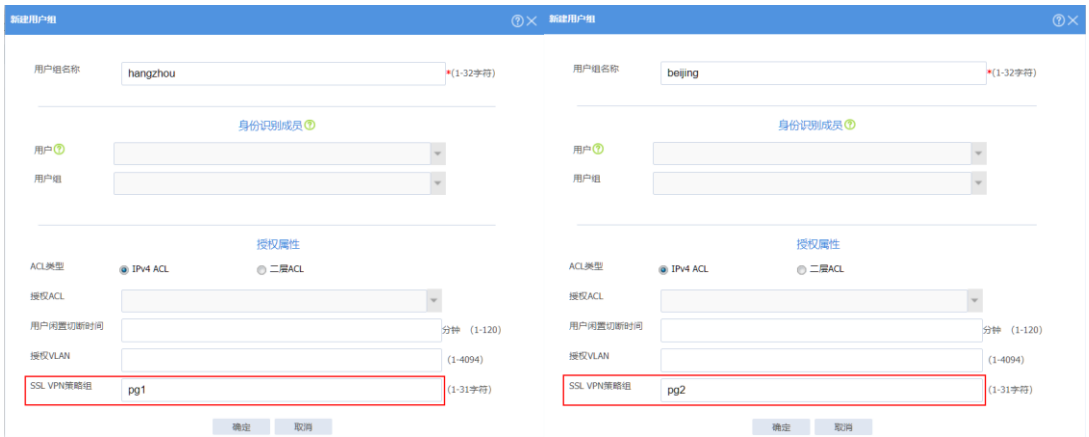
## 12， 修改 RADIUS 属性映射

以 NPS 为例，用户对应的用户组属性通过下述方式进行配置：


比如 alice 和 bob 两个用户分别属于 hangzhou 和 beijing 两个用户组，则在网络策略服务器上要分别设置下发各自的用户组属性。



同时防火墙上也需要设置相同名称的用户组，且此用户组要关联下对应的 SSL VPN 资源组。



使用 iNode SSL VPN 拨入时可以明显的看出，防火墙给两个用户下发的资源不同，这样便可完成对 alice 和 bob 的用户授权功能。


## 13， 拨打热线 400-810-0504 寻求帮助

完成上述排查步骤后，就可以实现 RADIUS 服务器对 SSLVPN 用户的认证和授权操作了，如果按照上述排查思路排查结果仍然存在异常，请收集完整的 DEBUG 信息、设备的完整配置、RADIUS 服务器上对应用户的配置和属性截图以及相关的抓包信息返回总部进行分析，技术支持热线为 400-810-0504。