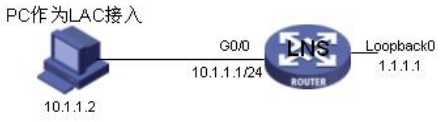
SR66系列路由器与iNode使用证书认证方式L2TP Over IPSec互通功能的配置

L2TP IPsec 证书 张玺 2015-10-22 发表

移动用户通过iNode智能客户端通过L2TP拨号接入LNS以访问总部内网，在PC和LNS之间交互的数据通过IPsec加密后传输。
证书来源：设备端通过手工配置获取CA证书与本地证书；PC端使用USBKEY作为证书。
设备清单：SR66系列路由器1台；PC 1台。



1、设备侧配置：

```
#
sysname LNS
#
l2tp enable      //使能L2TP
#
ike local-name lns        //设置本端IKE名字
#
domain system     //建立域，并配置IP pool
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
 ip pool 1 11.1.1.1 11.1.1.23
#
pki entity aaa     //配置PKI实体名称，并进入该实体视图
 common-name h3c    //配置实体的通用名
#
pki domain aaa      //创建一个PKI域，并进入PKI域视图
certificate request entity aaa    // 指定实体名称
 crl check disable     //不开启CRL校验
#
ike proposal 1      //配置IKE提议，并进入IKE提议视图
 authentication-method rsa-signature  //配置IKE提议所使用的验证算法
#
ike peer pc     //设置IKE邻居
 exchange-mode aggressive       //采用野蛮模式
 id-type name       //采用名字方式识别
 remote-name h3c       //设置IKE PEER的名字
 nat traversal       //开启NAT穿越功能
 certificate domain aaa   //配置采用数字签名验证时证书所属的PKI域
#
ipsec proposal 1      //配置IPSec提议
#
ipsec policy-template temp 1  //建立IPsec虚模板（也可使用ACL代替）
ike-peer pc
 proposal 1
#
ipsec policy pc 10 isakmp template temp//将IPsec Policy与虚模板绑定
#
local-user usera        //创建本地用户usera
 password simple usera
 service-type ppp
#
l2tp-group 1                //创建L2TP组
 allow l2tp virtual-template 0
 tunnel password simple tunnel   //配置隧道验证密码
 tunnel name h3c      //配置隧道名
```

```
#
interface Virtual-Template0        //创建L2TP虚模板
 ppp authentication-mode chap       //采用CHAP的域认证方式
 ppp chap user usera
 remote address pool 1                  //设置地址池
 ip address 11.1.1.111 255.255.255.0
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
interface GigabitEthernet0/0
 ip address 10.1.1.1 255.255.255.0
 ipsec policy pc                //在接口G0/0应用IPSec Policy
#
```

2、在设备端手工配置获取CA证书、获取本地证书、生成密钥对。

（1）使用FTP方式将CA证书文件及本地证书文件导入设备的CF卡中，方法略。

本例中CA证书文件名为hzcaroot.cer，本地证书文件名为vpn.pfx，导入完毕后，敲入如下命令：

cd cfa0:

dir

可以看到证书已经导入到CF卡中。

```
   31    -rw-       1237  Oct 26 2012 08:47:10   aaa_local.cer
   32    -rw-       1068  Oct 24 2012 06:28:24   hzcaroot.cer
   33    -rw-       1050  Oct 26 2012 08:47:40   aaa_ca.cer
   34    -rw-       2129  Oct 26 2012 04:43:20   10.24.cfg
   35    -rw-       2156  Oct 24 2012 02:21:54   vpn.pfx

499444 KB total (182180 KB free)

File system type of cfa0: FAT32

<LNS>
```

（2）生成本地RSA或ECDSA密钥对：

配置命令： [H3C]public-key local create {ecdsa|rsa}

本例中配置： [H3C]public-key local create rsa

```
[LNS]public-key local create rsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
it will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
```

公钥长度可在512-2048选择，默认为1024

输入1024，回车后，生成RSA密钥对成功。

```
Input the bits of the modulus[default = 1024]:1024
Generating Keys...
++
+++++
++++++++
++++++
```

（3）获取CA证书及本地证书：

配置命令：

[H3C]pki import-certificate {ca|local|peer-entity entity-name}domain domain-name {der|p12|pem}[filename filename]

本例中配置：

[H3C]pki import-certificate ca domain aaa pem filename hzcaroot.cer

（获取根证书，应在本地证书之前获取）

```
[LNS]
[LNS]pki import-certificate ca domain aaa pem filename hzcaroot.cer
The trusted CA's finger print is:
    MD5  fingerprint:0EA6 F65D 2669 E4BE CD41 68C3 88A1 84C4
    SHA1 fingerprint:447A F683 9F3C 4581 4140 DD9E 694E E356 9175 A896

Is the finger print correct?(Y/N):Y

%Oct 28 11:12:29:326 2012 LNS PKI/6/PKI_CA_CERT_TRUSTED: Root CA certificate of the domain aaa is trusted.
Import CA certificate successfully.
[LNS]
%Oct 28 11:12:29:613 2012 LNS PKI/6/PKI_IMPORT_CA_CERT_SUCC: Imported CA certificates of the domain aaa successfully.
[LNS]
```

[H3C]pki import-certificate local domain aaa p12 filename vpn.pfx （获取本地证书）

在Please input challenge password的提示语后，输入本地证书PIN码。

这样CA证书与本地证书即导入成功。

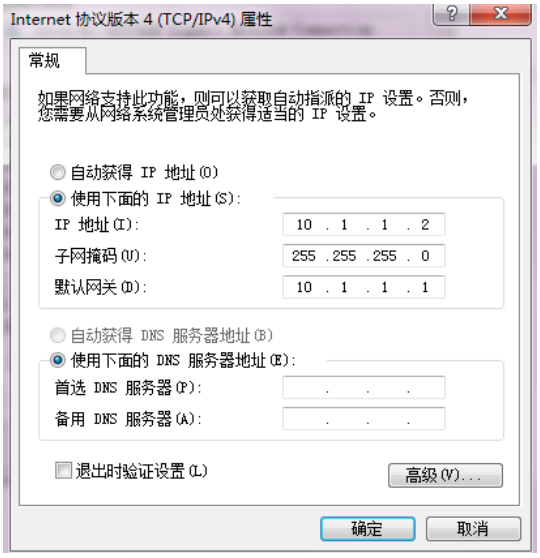
```
[LNS]pki import-certificate local domain aaa p12 filename vpn.pfx
Please input challenge password:
%Oct 28 11:14:21:750 2012 LNS PKI/6/PKI_VERIFY_CERT_SUCC: Verified the certificate CN=SNep\xOOV\xOOP\xOON,CN=10.255.255.13
ss=wangw@hzca.org.cn,OU=O\xO1N\x1A|{,L=gm]\xDE,ST=mYl_,C=CN of domain aaa successfully.
Import local certificate successfully.
Import key pair successfully.
[LNS]
%Oct 28 11:14:22:005 2012 LNS PKI/6/PKI_IMPORT_LOCAL_CERT_SUCC: Imported local certificate of the domain aaa successfully.
[LNS]
```

3、 PC端设置。

（1） 将网线一端与路由器的G0/0口相连，另一端与主机的网卡相连。

（2） 插入USBKEY，安装根证书及其驱动。

（3） 进行IP地址的配置，如下图所示：

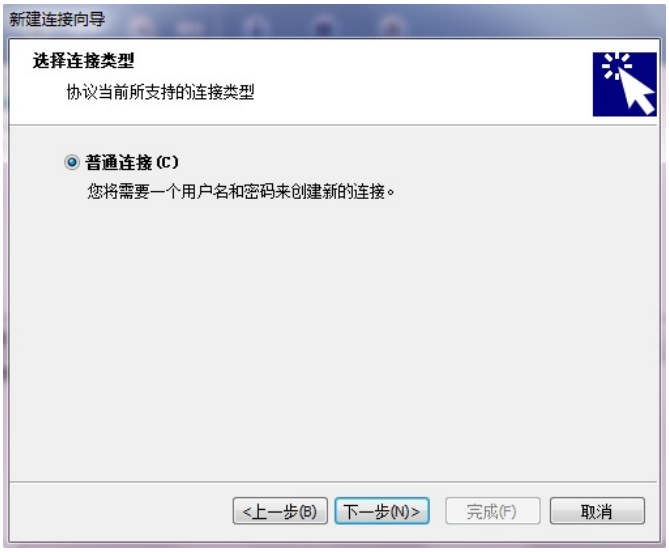


4、iNode智能客户端设置。

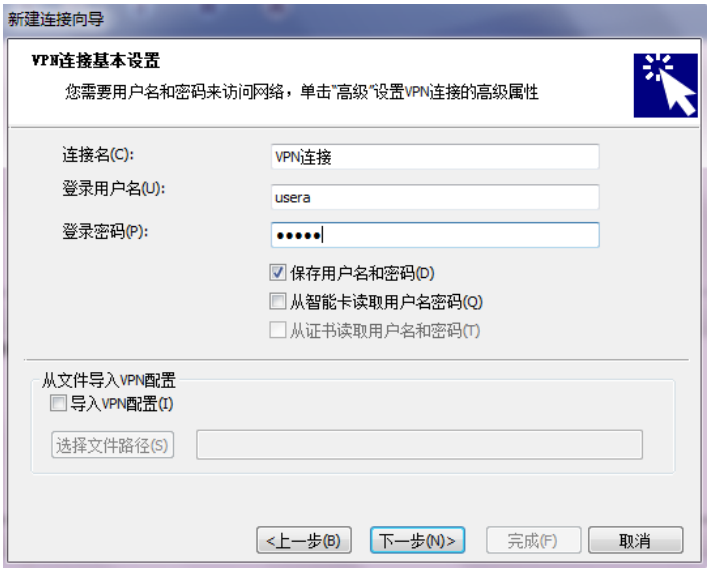
（1） 打开iNode智能客户端，点击左上角“新建”图标，弹出窗口如下：

(2) 选择“有线网络”，点击“下一步”，弹出窗口如下：

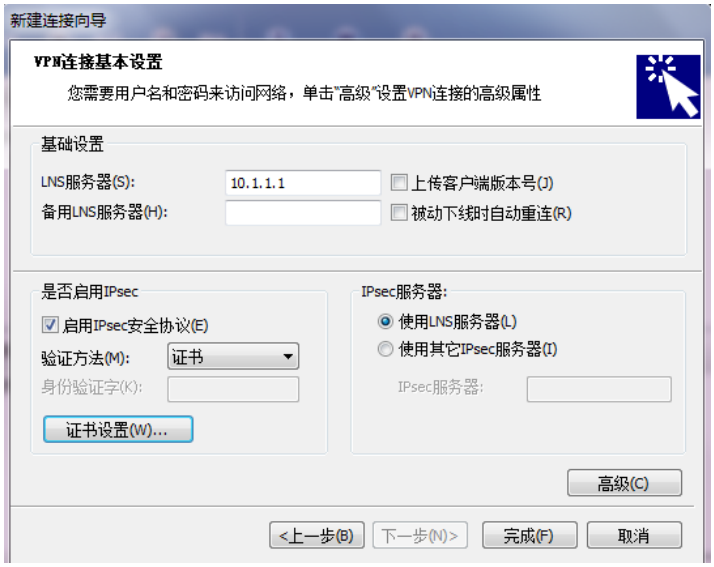
(3)选择“L2TP IPsec VPN协议”，点击“下一步”，弹出窗口如下：



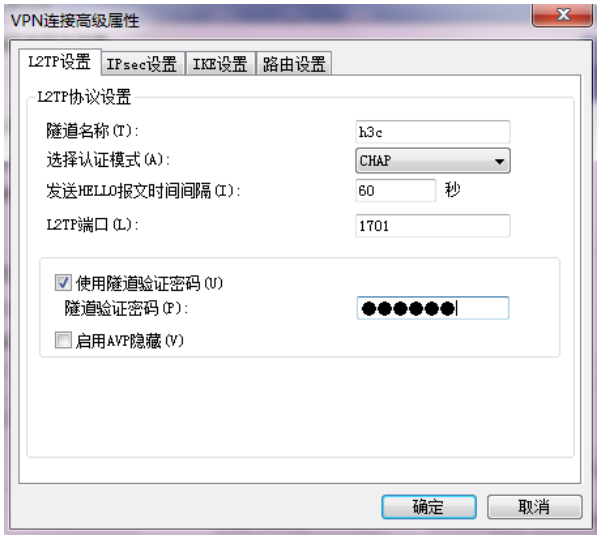
(4) 选择“普通连接”，点击“下一步”，弹出窗口如下：



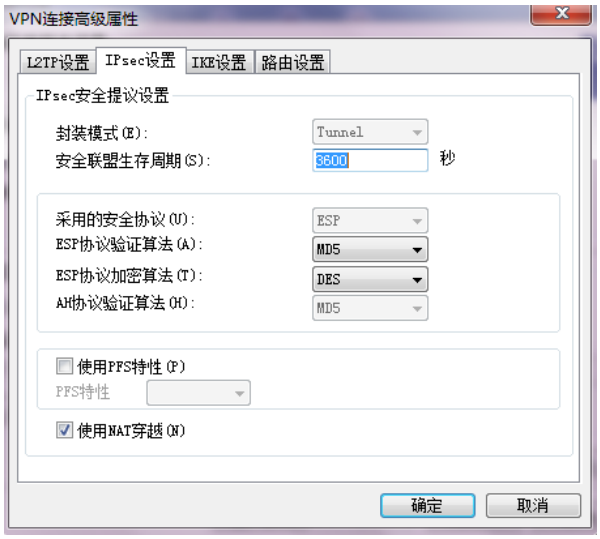
(5)　“连接名”可任意输入，本例为“VPN连接”；本例中“登陆用户名”为“usera”，“登陆密码”为“usera”。点击“下一步”，弹出窗口如下：



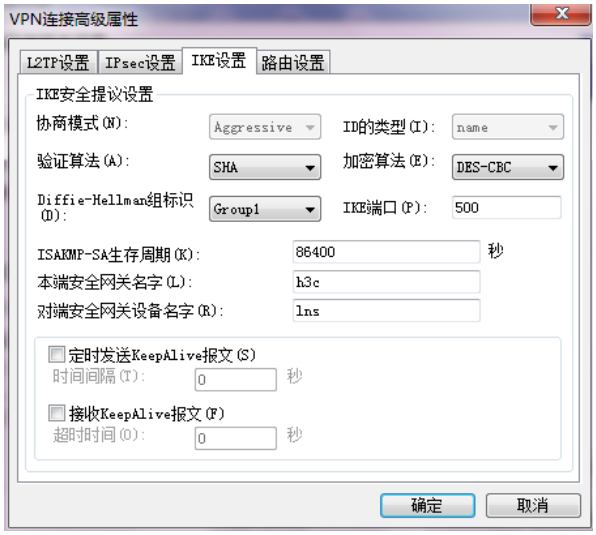
（6） "LNS服务器"设为路由器的G0/0接口地址10.1.1.1；在"启用IPSec安全协议"的选项上打勾，并将验证方法设为"证书"。点击"高级"，弹出窗口如下：



上图中，将"隧道名称"设为"h3c"，将"选择认证模式"设为"CHAP"，勾选"使用隧道验证密码"选项，将隧道验证密码设为"tunnel"。



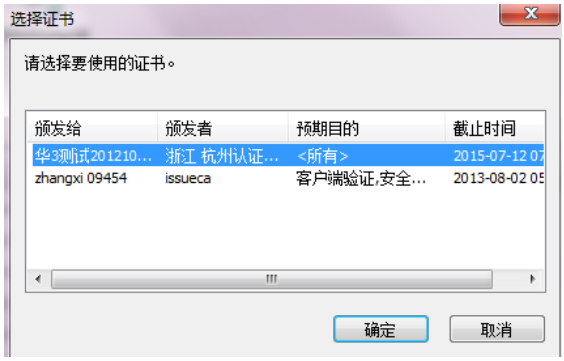
上图中，勾选"使用NAT穿越"选项，其它选项按设备端配置来选择。本例中"ESP协议验证算法"为"MD5"，"ESP协议加密算法"为"DES"。



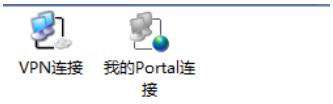
上图中，配置“本段安全网关名字”为“h3c”，“对端安全网关设备名字”为“lns”，其它选项按设备端配置来选择。本例中“验证算法”为“SHA”，“加密算法”为“DES-CBC”。

5、拨号操作：
在iNode主界面上双击“VPN连接”，弹出窗口如下：

点击“连接”，弹出窗口如下：



选择证书“华3测试201210...”，点击“确定”。
首次连接成功如下图所示：



1、首次连接时，会弹出对话框提示输入USBKEY的PIN码，以后只要不将USBKEY拔出，则再次连接不需要输入PIN码。

2、在配置获取本地证书时，可能会碰到以下情况：

```
[LNS]pki import-certificate local domain aaa p12 filename vpn.pfx
Please input challenge password:
Both local device and import file has a key, please choose one of them.
[LNS]
```

此时应进行如下配置：

```
[LNS]
[LNS]_h
Now you enter a hidden command view for developer's testing, some commands may
affect operation by wrong use, please carefully use it with our engineer's
direction.
[LNS-hidecmd]
[LNS-hidecmd]
[LNS-hidecmd]
[LNS-hidecmd]
[LNS-hidecmd]
[LNS-hidecmd]attrib hostkey -h
% Change file attributes successfully.
[LNS-hidecmd]quit
[LNS]quit
<LNS>
```

在用户模式下使用dir命令查看CF卡中文件，发现多了一个hostkey文件：

```
   31    -rw-      1050  Oct 28 2012 11:19:16   aaa_ca.cer
   32    -rw-      1068  Oct 24 2012 06:28:24   hzcaroot.cer
   33    -rw-      1237  Oct 28 2012 11:24:56   aaa_local.cer
   34    -rw-      2129  Oct 26 2012 04:43:20   10.24.cfg
   35    -rw-      2156  Oct 24 2012 02:21:54   vpn.pfx
   36    -rw-       735  Oct 28 2012 11:24:56   hostkey
```

使用detele /unreserved hostkey命令，将其删除。

此时即可重新配置获取本地证书。