SecPath使用SecKey证书验证建立L2TP+IPSec VPN

巫继雨 2006-10-12 发表

SecPath使用SecKey证书验证建立L2TP+IPSec VPN

一. 组网需求

版本：SecPoint V5.05；SecKey Manager V2.04

设备：Qudiway SecKey 1000；SecPath 100F V3.4 ESS1604

二. 组网图

客户端使用SecKey进行L2TP+IPSec的连接，双方使用数字证书进行IKE协商的身份验证。

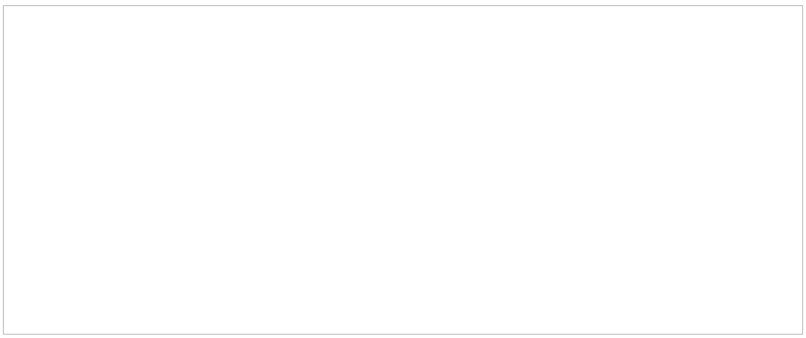
三. 配置步骤

1. 将CA根证书和SecKey本地证书导入SecKey；

SecKey的证书导入有两种实现方式：“手工申请手动导入”和“自动申请自动导入”，下面进行具体说明：

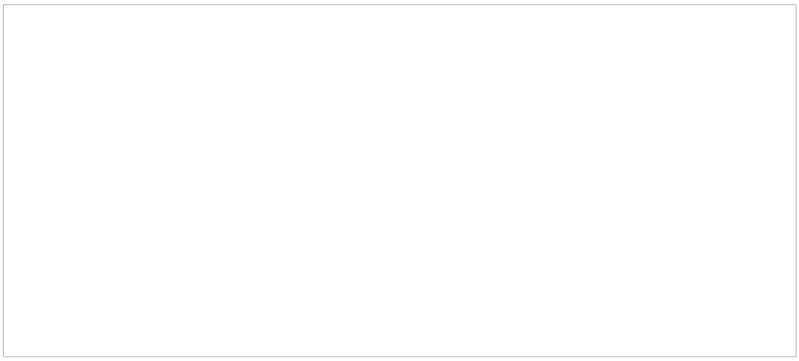
1.1 自动申请自动导入

要使用Seckey Certificate的“申请证书”功能，必须将证书服务器的“证书请求处理”配置为“自动颁发证书”，具体配置如下图：



点选SecKey Certificate的“证书申请”按钮，弹出“证书申请”对话框，填入证书服务器的地址，如下图：

选择“证书申请”对话框的“高级...”，在里面进行本地证书信息的设置，如下图：



完成以上配置后，点击“申请”，即可完成证书的自动申请和自动导入，如下图：

1.2　手工申请手工导入

具体步骤见附件动画：

2.　将CA根证书和SecPath本地证书导入SecPath；

2.1 为SecPath生成本地证书请求

l　PKI实体配置

```
<Quidway>
#
pki entity server                          #PKI实体配置，此处名称应该与PKI Domain中的实体名称一样
 common-name local_ca

l　定义PKI Domain
#
pki domain lns                             #Domain名称
 ca identifier ts-sec                      #指定ca服务器的名称
 certificate request url http://1.1.1.1    #证书请求URL，可任意填写
 certificate request from ra               #向证书注册中心请求注册
 certificate request entity server         #为实体SecPath请求证书
 crl check disable                         #忽略证书撤销列表的检查
```

l　通过RSA生成公、私密钥对

```
[Quidway]rsa local-key-pair create

#设定rsa运算模数为1024位
Input the bits in the modulus[default = 512]:1024
```

l　打印出本地证书请求信息

```
[Quidway]pki request-certificate domain lns pkcs10
```

将整个证书请求复制出来，通过带外方式提交给“证书服务器”，进行证书的申请，具体如参考附件中动画：

2.2 为SecPath颁发证书

登陆证书服务器，为SecPath颁发本地证书。

2.3导入根证书和本地证书到SecPath

l　通过tftp将根证书ca.cer和SecPath的本地证书local.cer上传到SecPath中

l　用import-certificate导入根证书

```
[Quidway]pki import-certificate ca domain lns der filename ca.cer
```

在引入的过程中，需要确认证书的指纹是否正确，选择“Y”，成功导入根证书。

l　导入SecPath的本地实体证书

```
[Quidway]pki import-certificate local domain lns der filename local.cer
```

3.　使用SecKey Manager配置VPN；

3.1 登录SecKey Manager

PIN码默认为六个零。

3.2 生成配置文件

```
[Quidway]pki request-certificate domain lns pkcs10
-----BEGIN CERTIFICATE REQUEST-----
MIIBUjCBvAIBADATMREwDwYDVQQDFAhsb2NhbF9jYTCBnzANBgkqhkiG9w0BAQEF
AAOBjQAwgYkCgYEAmiXUNt7D/llOPbFo+P63rrPGtIpOnTCiRMSR2/MqkXqMMb4A
MOtNkZzirrsmyT7FV7wUSRLTUQb/Ua+EN14b6MvHS0EWHA/MdZq6xZ31p1C0blcc
cQIoBYbdiVhzoGJ/3DghQIbjnFeQMuoErRfgPRroGCuJCfFQXwgEgUo9f9MCAwEA
AaAAMA0GCSqGSIb3DQEBBAUAA4GBAA3TNoXotgxLJfM2yK4PZ1HBXyYrcUdww22F
a7uzx4OB2W/GRAfps+oFNGw0Rsqx3lenltpfkbNjHFdmjoI71Mhfh/FVGP67AFcS
bgmOl8B+enQRvSwkMYpwgWgc9zHJN2i/Jz5OcXD+GXsNXsTMxx+1JK6D105WWy4U
dAfDrSt2
-----END CERTIFICATE REQUEST-----
```

点击“文件生成”，进入到VPN的设置页面，对照SecPath上的配置进行设置就可以了，其中注意将IPSec的验证方法设置为“RSA-SIGNATURE”，如下图：

4. 使用SecPoint建立VPN连接

打开SecPoint，选择“SecKey专有连接”，如上图。在提示输入PIN码后，SecKey中的VPN配置文件将会被读出，我们不需要再输入VPN连接的用户名和密码，只需要点击“登录”就可以了，如下图：

四. 配置总结

基本的配置步骤总结为下面四点：

1. 获取CA根证书，将其导入到SecKey和SecPath中；

说明：CA属于权威的第三方，需要认证的双方都信任这个结构。CA根证书用来验证对方设备证书的签名有效性。

2. 为SecKey和SecPath申请本地证书，并将其导入到设备中；

说明：本地证书即指设备自己的证书，它用来表明设备身份。假如A要向B来证明自己的身份，其基本过程如下：A将自己的本地证书传送给B，然后B使用CA根证书来验证A的本地证书的签名有效性。如果验证通过，则A向B证明了自己的身份。

3. 使用SecKey Manager生成VPN配置文件；

说明：在配置过程中，注意将IPSec的验证方法设置为“RSA-SIGNATURE”。

4. 使用SecPoint进行VPN连接。

五. 附录：

1. SecPath配置

```
[Quidway]dis cur
#
 sysname Quidway
```

```
#
 l2tp enable
#
 ike local-name lns
#
 firewall packet-filter enable
 firewall packet-filter default permit
#
 insulate
#
 undo connection-limit enable
 connection-limit default deny
 connection-limit default amount upper-limit 50 lower-limit 20
#
 firewall statistic system enable
#
pki entity server
  common-name local_ca
#
pki domain lns
  ca identifier ts-sec
  certificate request url http://1.1.1.1
  certificate request from ra
  certificate request entity server
  crl check disable
#
radius scheme system
#
domain system
 ip pool 1 192.168.0.2 192.168.0.10
#
local-user ftp
 password simple ftp
 service-type ftp
local-user test
 password simple 1234
 level 3
 service-type ppp
local-user wujiyu
 password simple 1234
 service-type ppp
#
ike proposal 1
 authentication-method rsa-signature
#
ike peer lac
 exchange-mode aggressive
 remote-name lac
 certificate domain lns
#
ipsec proposal 1
#
ipsec policy-template temp 1
 ike-peer lac
 proposal 1
#
ipsec policy lns 1 isakmp template temp
#
interface Virtual-Template0
 ppp authentication-mode pap
 ip address 192.168.0.1 255.255.255.0
#
interface Aux0
 async mode flow
```

```
#
interface Ethernet0/0
 ip address 1.0.0.1 255.0.0.0
 ipsec policy lns
#
interface Ethernet0/1
#
interface Ethernet0/2
#
interface Ethernet0/3
#
interface Ethernet1/0
#
interface Ethernet1/1
#
interface Ethernet1/2
#
interface Encrypt2/0
#
interface NULL0
#
interface LoopBack1
#
firewall zone local
 set priority 100
#
firewall zone trust
 add interface Ethernet0/0
 add interface Virtual-Template0
 set priority 85
#
firewall zone untrust
 set priority 5
#
firewall zone DMZ
 set priority 50
#
firewall interzone local trust
#
firewall interzone local untrust
#
firewall interzone local DMZ
#
firewall interzone trust untrust
#
firewall interzone trust DMZ
#
firewall interzone DMZ untrust
#
l2tp-group 1
 allow l2tp virtual-template 0 remote lac
 tunnel password simple 12345
 tunnel name lns
#
user-interface con 0
user-interface aux 0
user-interface vty 0 4
#
return
[Quidway]
```

2. VPN配置文件

见附件

说明：此配置文件为使用“文件导出”功能从SecKey Manager中导出的VPN配置文件，已经经过加密处理，需要使用时利用SecKey Manager的“文件导入”即可。