

SecPath安全网关L2tp+IPSec+证书的典型配置

一、组网需求:

SecPath安全网关实现L2tp+IPSec+证书的典型配置。

二、组网图



PC (Lac客户端)

SecPath V1000-A

适合SecPath安全产品所有版本，PC客户端安装了iNode软件。

三、配置步骤

SecPath V1000-A的主要配置

```
#
l2tp enable //开启L2tp功能
#
ike local-name zhongxin //配置ike本地名称
#
pki entity secpath //配置PKI实体
common-name ipsec_secpath
#
pki domain h3c //配置PKI域
ca identifier ca_server
certificate request url http://ca
certificate request from ra
certificate request entity secpath
crl check disable
#
domain system //配置地址池
ip pool 1 172.16.1.10 172.16.1.100
#
local-user test
password simple test
service-type ppp
#
ike proposal 1 //配置ike安全提议
authentication-method rsa-signature
#
ike peer 1 //配置ike对等体
exchange-mode aggressive
id-type name
remote-name fenzhi
certificate domain h3c
#
ipsec proposal 1 //配置IPSec安全提议
#
ipsec policy-template temp 1 //配置IPsec策略模板
ike-peer 1
proposal 1
#
ipsec policy pol1 1 isakmp template temp //配置IPSec策略
```

```
#
interface Virtual-Template1                //配置虚模板
ppp authentication-mode chap
ip address 172.16.1.1 255.255.255.0
remote address pool 1
#
interface GigabitEthernet0/0
ip address 202.38.1.1 255.255.255.0
ipsec policy pol1                          //应用IPSec策略
#
interface GigabitEthernet0/1
ip address 192.168.1.1 255.255.255.0
#
l2tp-group 1                               //配置L2tp组
undo tunnel authentication
allow l2tp virtual-template 1
#
ip route-static 0.0.0.0 0.0.0.0 202.38.1.2 preference 60
#
```

四、配置关键点
略。