SecPath1800F L2TP+IpSec连接方式的配置

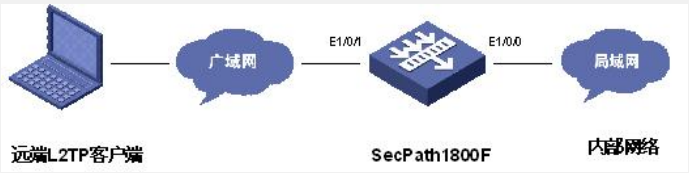
王刚 2006-11-10 发表

SecPath1800F L2TP+IpSec功能的配置

一、 组网需求：

公网用户需要通过公网访问内部网络的资源，同时要保证网络连接数据的安全，采用L2TP + IpSec的方式连接内部网络。

二、 组网图：



三、 配置步骤：

适用版本： SecPath1800F 所有非P2P限流版本。

```
#
acl number 3000
 description untrust-local
 rule 0 permit tcp destination-port eq telnet
 rule 5 permit icmp
 rule 10 permit udp destination-port eq 1701
 rule 15 permit udp destination-port eq 500
acl number 3001
 description vpn-trust
 rule 0 deny tcp destination-port eq 4444
 rule 5 deny udp destination-port eq tftp
 rule 10 deny tcp destination-port eq 135
 rule 15 deny udp destination-port eq 135
 rule 20 deny tcp destination-port eq 139
 rule 25 deny udp destination-port eq netbios-ssn
 rule 30 deny tcp destination-port eq 445
 rule 35 deny udp destination-port eq 445
 rule 40 deny tcp destination-port eq 593
 rule 45 deny udp destination-port eq 593
 rule 50 deny udp destination-port eq 1434
 rule 55 deny tcp destination-port eq 5554
 rule 60 deny tcp destination-port eq 9995
 rule 65 deny tcp destination-port eq 9996
 rule 75 permit ip
acl number 3002
 description vpn-local
 rule 0 permit tcp destination-port eq telnet
 rule 5 permit icmp
acl number 3003
 description untrust-vpn
 rule 0 deny tcp destination-port eq 4444
 rule 5 deny udp destination-port eq tftp
 rule 10 deny tcp destination-port eq 135
 rule 15 deny udp destination-port eq 135
 rule 20 deny tcp destination-port eq 139
 rule 25 deny udp destination-port eq netbios-ssn
 rule 30 deny tcp destination-port eq 445
 rule 35 deny udp destination-port eq 445
```

```
 rule 40 deny tcp destination-port eq 593
 rule 45 deny udp destination-port eq 593
 rule 50 deny udp destination-port eq 1434
 rule 55 deny tcp destination-port eq 5554
 rule 60 deny tcp destination-port eq 9995
 rule 65 deny tcp destination-port eq 9996
 rule 75 permit ip
acl number 3999                    // 定义用以做IpSec的数据流
 rule 5 permit udp destination-port eq 1701
 rule 10 permit udp source-port eq 1701
#
 sysname HA_ErChang_LNS_A
#
 l2tp enable                       // 启用L2TP
#
 ike local-name lns                // 指定IKE 本地名字
#
 firewall packet-filter default permit interzone trust vpn direction inbound
 firewall packet-filter default permit interzone trust vpn direction outbound
#
 bypass switch-back auto
#
 firewall mode route
#
 firewall statistic system enable
#
ike peer peer1                     // 配置用来做IKE协商的信息
 exchange-mode aggressive
 pre-shared-key 234567
 local-id-type name
 remote-name lac
 nat traversal
#
ipsec proposal p1                  // 配置用来做IpSec协商的 proposal （此处使用默认值
)
#
ipsec policy-template template 1   // 配置模板应用相应的acl、ike peer、proposal
 security acl 3999
 ike-peer peer1
 proposal p1
#
ipsec policy l2tp_vpn 1 isakmp template template     // 配置IpSec策略
#
interface Aux0
 async mode flow
 link-protocol ppp
#
interface Ethernet0/0/0
#
interface Ethernet0/0/1
#
interface Ethernet1/0/0
 ip address 192.240.0.3 255.255.255.248
#
interface Ethernet1/0/1            // 在相应接口上绑定IpSec策略
ip address 221.13.223.3 255.255.255.248
ipsec policy l2tp_vpn
#
interface Ethernet1/0/2
#
interface Ethernet1/0/3
#
interface Ethernet1/0/4
#
```

```
interface Ethernet1/0/5
#
interface Ethernet1/0/6
#
interface Ethernet1/0/7
#
interface Virtual-Template1          // 配置用来响应接入的虚模板
 ppp authentication-mode chap
 description test
 ip address 192.239.1.1 255.255.240.0
 remote address pool 1
#
interface Secp3/0/0
#
interface NULL0
#
interface LoopBack0
 ip address 3.3.3.3 255.255.255.255
#
firewall zone local
 set priority 100
#
firewall zone trust
 set priority 85
 add interface Ethernet1/0/0
#
firewall zone untrust
 set priority 5
 add interface Ethernet0/0/0
 add interface Ethernet1/0/1
#
firewall zone dmz
 set priority 50
#
firewall zone name vpn              // 创建一个新的域把虚拟接口加入域
 set priority 30
 add interface Virtual-Template1
#
firewall interzone local trust
#
firewall interzone local untrust
 packet-filter 3000 inbound
 packet-filter 3000 outbound
#
firewall interzone local dmz
#
firewall interzone local vpn
 packet-filter 3002 inbound
 packet-filter 3002 outbound
#
firewall interzone trust untrust
#
firewall interzone trust dmz
#
firewall interzone trust vpn
 packet-filter 3001 inbound
 packet-filter 3001 outbound
#
firewall interzone dmz untrust
#
firewall interzone vpn untrust
 packet-filter 3003 outbound
#
firewall interzone dmz vpn
```

```
#
l2tp-group 1                    // 创建一个L2TP Group 用来相应L2TP的拨入
 allow l2tp virtual-template 1
 tunnel password simple 234567
 tunnel name zhengzhou
#
aaa                             // 创建用户并指定用户使用模式、配置地址池
 local-user hnvpn password simple hnvpn
 local-user hnvpn service-type ppp
 ip pool 1 192.239.1.2 192.239.15.254
#
 authentication-scheme default
#
 authorization-scheme default
#
 accounting-scheme default
#
 domain default
#
#
 ip route-static 0.0.0.0 0.0.0.0 221.13.223.1        // 指定静态路由
 ip route-static 192.240.1.0 255.255.255.0 192.240.0.1
#
user-interface con 0
user-interface aux 0
user-interface vty 0 4
#
return
```

四、 配置关键点：

无