SecPath 防火墙野蛮模式IPSec VRRP典型配置指南

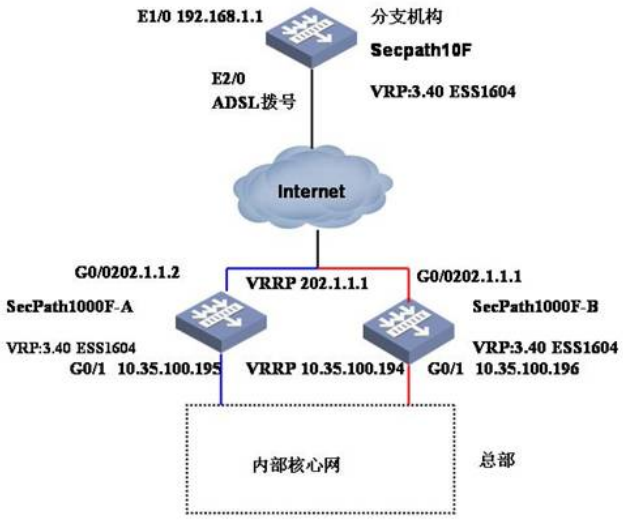
刘军 2006-11-03 发表

SecPath 防火墙野蛮模式IPSec VRRP典型配置指南

一、 组网需求

用户需要总部和分部建立IPSec,总部采用两台防火墙，两台防火墙运行VRRP，分部通过ADSL拨号接入INTERNET，再和总部建立IPSec VPN。

二、 组网图



软件版本如下：

SecPath1000F-A： VRP 3.40 ESS 1604;

SecPath1000F-B： VRP 3.40 ESS 1604;

SecPath10F： VRP 3.40 ESS 1604.

三、 典型配置

SecPath1000F-A的最终配置

```
sysname Secpath1000F-A
#
super password level 3 cipher OUM!K%F<+$[Q=^Q`MAF4<1!!
#
l2tp enable
#
ike local-name zongbu
#
firewall packet-filter enable
firewall packet-filter default permit
#
undo connection-limit enable
connection-limit default deny
connection-limit default amount upper-limit 50 lower-limit 20
#
vrrp ping-enable                    //允许ping VRRP的虚拟地址
#
firewall statistic system enable
#
radius scheme system
#
domain system
ip pool 1 172.16.1.3 172.16.1.254
#
local-user telnet
password simple telnet
service-type telnet
```

```
local-user test
password simple test
service-type ppp
#
ike dpd 1                    //启用ike dpd（death peer dection）功能

#
ike peer fenbu                    //创建ike peer，名为fenbu
exchange-mode aggressive          // 使用野蛮模式
pre-shared-key 123456             //预共享密钥为123456
id-type name                      //使用名字方式
remote-name fenbu                 //分支机构的ike名为分部
local-address 202.1.1.1           //设置本地建立ike时使用的地址
nat traversal                     //使能NAT穿越功能
dpd 1                             //引用dpd 1

#
ipsec card-proposal 1             //创建一个名字为1采用加密卡的安全提议（默
//认是采用ESP协议、DES加密算法、MD5验
//证算法。）

use encrypt-card 2/0
#
ipsec policy-template fenbu 1          //创建名字为fenbu的安全策略模板
ike-peer fenbu                    //引用ike对等体fenbu
proposal 1                        //引用安全提议1
#
//创建名为zongbu并引用模板fenbu的安全策略
ipsec policy zongbu 1 isakmp template fenbu
#
acl number 3500                   //创建防病毒访问控制列表
rule 0 deny tcp source-port eq 3127
rule 1 deny tcp source-port eq 1025
rule 2 deny tcp source-port eq 5554
rule 3 deny tcp source-port eq 9996
rule 4 deny tcp source-port eq 1068
rule 5 deny tcp source-port eq 135
rule 6 deny udp source-port eq 135
rule 7 deny tcp source-port eq 137
rule 8 deny udp source-port eq netbios-ns
rule 9 deny tcp source-port eq 138
rule 10 deny udp source-port eq netbios-dgm
rule 11 deny tcp source-port eq 139
rule 12 deny udp source-port eq netbios-ssn
rule 13 deny tcp source-port eq 593
rule 14 deny tcp source-port eq 4444
rule 15 deny tcp source-port eq 5800
rule 16 deny tcp source-port eq 5900
rule 18 deny tcp source-port eq 8998
rule 19 deny tcp source-port eq 445
rule 20 deny udp source-port eq 445
rule 21 deny udp source-port eq 1434
rule 30 deny tcp destination-port eq 3127
rule 31 deny tcp destination-port eq 1025
rule 32 deny tcp destination-port eq 5554
rule 33 deny tcp destination-port eq 9996
rule 34 deny tcp destination-port eq 1068
rule 35 deny tcp destination-port eq 135
rule 36 deny udp destination-port eq 135
rule 37 deny tcp destination-port eq 137
rule 38 deny udp destination-port eq netbios-ns
rule 39 deny tcp destination-port eq 138
rule 40 deny udp destination-port eq netbios-dgm
rule 41 deny tcp destination-port eq 139
```

```
runy udp destination-port eq netbios-ssn
rule 43 deny tcp destination-port eq 593
rule 44 deny tcp destination 4444
rule 45 deny tcp destination-port eq 5800
rule 46 deny tcp destination-port eq 5900
rule 48 deny tcp destination-port eq 8998
rule 49 deny tcp destination-port eq 445
rule 50 deny udp destination-port eq 445
rule 51 deny udp destination-port eq 1434
rule 52 permit ip
#
interface Virtual-Template1
ppp authentication-mode pap
ip address 172.16.1.1 255.255.255.0
remote address pool 1
#
interface Aux0
async mode flow
#
interface Ethernet1/0
#
interface GigabitEthernet0/0
descriptiont to WAN"
ip address 202.1.1.2 255.255.255.0
undo ip fast-forwarding                    //关掉快转
vrrp vrid 1 virtual-ip 202.1.1.1      // 启用VRRP协议号1，虚拟ip为：202.1.1.1
vrrp vrid 1 priority 110            //VRRP协议号1的优先级为110
// VRRP协议号1跟踪GigabitEthernet 0/1的状态，如果down了，则优先级降为90（110 - 20）
vrrp vrid 1 track GigabitEthernet0/1 reduced 20
ipsec policy zongbu              //在该接口上应用ipsec策略zongbu
#
interface GigabitEthernet0/1
description "Connect to gongsi LAN"
tcp mss 1024
ip address 10.35.100.195 255.255.255.0
undo ip fast-forwarding
vrrp vrid 2 virtual-ip 10.35.100.194  // 启用VRRP协议号2，虚拟ip为：10.35.100.194
vrrp vrid 2 priority 110          //VRRP协议号1的优先级为110
// VRRP协议号2跟踪GigabitEthernet 0/1的状态，如果down了，则优先级降为90（110 - 20）

vrrp vrid 2 track GigabitEthernet0/0 reduced 20
firewall packet-filter 3500 inbound//对入口数据进行3500的检查
#
interface Encrypt2/0
#
interface NULL0
#
firewall zone local
set priority 100
#
firewall zone trust
add interface GigabitEthernet0/0
add interface GigabitEthernet0/1
add interface Virtual-Template1
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
undo tunnel authentication
allow l2tp virtual-template 1 remote lac
#
ip route-static 0.0.0.0 0.0.0.0 202.1.1.254 preference 60
ip route-static 10.0.0.0 255.0.0.0 10.35.100.193 preference 60
ip route-static 192.168.1.0 255.255.255.0 202.1.1.254 preference 60
#
SecPath1000F-B的最终配置
#
sysname Secpath1000F-B
#
super password level 3 cipher OUM!K%F<+$[Q=^Q`MAF4<1!!
#
l2tp enable
#
ike local-name zongbu
#
firewall packet-filter enable
firewall packet-filter default permit
#
undo connection-limit enable
connection-limit default deny
connection-limit default amount upper-limit 50 lower-limit 20
#
vrrp ping-enable              //允许ping VRRP的虚拟地址
#
firewall statistic system enable
#
radius scheme system
#
domain system
ip pool 1 172.16.1.3 172.16.1.254
#
local-user telnet
password simple telnet
service-type telnet
local-user test
password simple test
service-type ppp
#
ike dpd 1                  //启用ike dpd（death peer dection）功能
#
ike peer fenbu          //创建ike peer，名为fenbu
exchange-mode aggressive   // 使用野蛮模式
pre-shared-key 123456     //预共享密钥为123456
id-type name              //使用名字方式
remote-name fenbu        //分支机构的ike名为分部
local-address 202.1.1.1  //设置本地建立ike时使用的地址
nat traversal            //使能NAT穿越功能
dpd 1                    //引用dpd 1
#
ipsec card-proposal 1    //创建一个名字为1采用加密卡的安全提议（默
//认是采用ESP协议、DES加密算法、MD5验
//证算法。）
```

```
use encrypt-card 1/0
#
ipsec policy-template fenbu 1  //创建名字为fenbu的安全策略模板
ike-peer fenbu                 //引用ike对等体fenbu

proposal 1                     //引用安全提议1
#
//创建名为zongbu并引用模板fenbu的安全策略
ipsec policy zongbu 1 isakmp template fenbu//
#
acl number 3500                //创建防病毒访问控制列表
rule 0 deny tcp source-port eq 3127
rule 1 deny tcp source-port eq 1025
rule 2 deny tcp source-port eq 5554
rule 3 deny tcp source-port eq 9996
rule 4 deny tcp source-port eq 1068
rule 5 deny tcp source-port eq 135
rule 6 deny udp source-port eq 135
rule 7 deny tcp source-port eq 137
rule 8 deny udp source-port eq netbios-ns
rule 9 deny tcp source-port eq 138
rule 10 deny udp source-port eq netbios-dgm
rule 11 deny tcp source-port eq 139
rule 12 deny udp source-port eq netbios-ssn
rule 13 deny tcp source-port eq 593
rule 14 deny tcp source-port eq 4444
rule 15 deny tcp source-port eq 5800
rule 16 deny tcp source-port eq 5900
rule 18 deny tcp source-port eq 8998
rule 19 deny tcp source-port eq 445
rule 20 deny udp source-port eq 445
rule 21 deny udp source-port eq 1434
rule 30 deny tcp destination-port eq 3127
rule 31 deny tcp destination-port eq 1025
rule 32 deny tcp destination-port eq 5554
rule 33 deny tcp destination-port eq 9996
rule 34 deny tcp destination-port eq 1068
rule 35 deny tcp destination-port eq 135
rule 36 deny udp destination-port eq 135
rule 37 deny tcp destination-port eq 137
rule 38 deny udp destination-port eq netbios-ns
rule 39 deny tcp destination-port eq 138
rule 40 deny udp destination-port eq netbios-dgm
rule 41 deny tcp destination-port eq 139
rule 42 deny udp destination-port eq netbios-ssn
rule 43 deny tcp destination-port eq 593
rule 44 deny tcp destination-port eq 4444
rule 45 deny tcp destination-port eq 5800
rule 46 deny tcp destination-port eq 5900
rule 48 deny tcp destination-port eq 8998
rule 49 deny tcp destination-port eq 445
rule 50 deny udp destination-port eq 445
rule 51 deny udp destination-port eq 1434
rule 52 permit ip
#
interface Virtual-Template1
ppp authentication-mode pap
ip address 172.16.1.2 255.255.255.0
remote address pool 1
#
interface Aux0
async mode flow
#
interface GigabitEthernet0/0
```

```
description "Connect to WAN"
ip address 202.1.1.3 255.255.255.0
undo ip fast-forwarding                    //关掉快转
vrrp vrid 1 virtual-ip 202.1.1.1        // 启用VRRP协议号1，虚拟ip为：202.1.1.1
vrrp vrid 1 track GigabitEthernet0/1 reduced 20//VRRP协议号1的优先级为110
// VRRP协议号1跟踪GigabitEthernet 0/1的状态，如果down了，则优先级降为90（110 - 20）
ipsec policy zongbu        //在该接口上应用ipsec策略zongbu
interface GigabitEthernet0/1
description "Connect to gongsi LAN"
tcp mss 1024
ip address 10.35.100.196 255.255.255.248
undo ip fast-forwarding              //关掉快转
vrrp vrid 2 virtual-ip 10.35.100.194  // 启用VRRP协议号1，虚拟ip为：202.1.1.1
vrrp vrid 2 track GigabitEthernet0/0 reduced 20/VRRP协议号1的优先级为110
// VRRP协议号1跟踪GigabitEthernet 0/1的状态，如果down了，则优先级降为90（110 - 20）
firewall packet-filter 3500 inbound//对入口数据进行3500的检查
#

interface Encrypt2/0
#
interface NULL0
#
firewall zone local
set priority 100
#
firewall zone trust
add interface GigabitEthernet0/0
add interface GigabitEthernet0/1
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
undo tunnel authentication
allow l2tp virtual-template 1 remote lac
#
ip route-static 0.0.0.0 0.0.0.0 202.1.1.254 preference 60
ip route-static 10.0.0.0 255.0.0.0 10.35.100.193 preference 60
ip route-static 192.168.1.0 255.255.255.0 202.1.1.254 preference 60
#
snmp-agent
snmp-agent local-engineid 000007DB7F00000100001631
snmp-agent community read huawei
snmp-agent sys-info version all
#
ntp-service unicast-server 10.16.100.238
#
user-interface con 0
```

```
user-interface aux 0
user-interface vty 0
authentication-mode scheme
user-interface vty 1 4
set authentication password cipher 0.Z%C_.$8>K9IIU(@"<GB!!!
#
return
SecPath10F-JIANGXI的最终配置
sysname secpath10-jiangxi
#
ike local-name fenbu
#
firewall packet-filter enable
firewall packet-filter default permit
#
undo connection-limit enable
connection-limit default deny
connection-limit default amount upper-limit 50 lower-limit 20
#
dialer-rule 1 ip permit
#
firewall statistic system enable
#
radius scheme system
#
domain system
#
local-user admin
password cipher .]@USE=B,53Q=^Q`MAF4<1!!
service-type telnet terminal
level 3
service-type ftp
#
ike dpd 1          //启用ike dpd（death peer dection）功能

#
ike peer zongbu  //创建ike peer，名为zongbu
exchange-mode aggressive//使用野蛮模式
pre-shared-key 123456//预共享密钥为123456
id-type name       //使用名字方式
remote-name zongbu  //中心端的名字为zongbu
remote-address 202.1.1.1//中心端建立ipsec的地址为202.1.1.1
nat traversal     //使能NAT穿越功能
dpd 1              //引用dpd 1
#
ipsec proposal 1  //创建一个名字为1的安全提议（默认是采用ESP协议、DES加密算法、MD5验证算
法。）
#
ipsec policy fenbu 1 isakmp//创建名为fenbu的安全策略
security acl 3000    //引用安全流量为acl 3000定义的流量
ike-peer zongbu      //引用ike对等体zongbu
proposal 1           //引用安全提议1

#
dhcp server ip-pool 1
network 192.168.1.0 mask 255.255.255.248
gateway-list 192.168.1.1
dns-list 202.96.128.68
#
acl number 3000   //创建访问控制列表3000
rule 0 permit ip source 192.168.1.0 0.0.0.7 destination 10.0.0.0 0.255.255.255
rule 1 deny ip
acl number 3005
rule 0 deny ip source 192.168.1.0 0.0.0.7 destination 10.0.0.0 0.255.255.255
```

rule 1 permit ip source 192.168.1.0 0.0.0.255
rule 2 deny ip
acl number 3500 *//设置防病毒访问控制列表*
rule 0 deny tcp source-port eq 3127
rule 1 deny tcp source-port eq 1025
rule 2 deny tcp source-port eq 5554
rule 3 deny tcp source-port eq 9996
rule 4 deny tcp source-port eq 1068
rule 5 deny tcp source-port eq 135
rule 6 deny udp source-port eq 135
rule 7 deny tcp source-port eq 137
rule 8 deny udp source-port eq netbios-ns
rule 9 deny tcp source-port eq 138
rule 10 deny udp source-port eq netbios-dgm
rule 11 deny tcp source-port eq 139
rule 12 deny udp source-port eq netbios-ssn
rule 13 deny tcp source-port eq 593
rule 14 deny tcp source-port eq 4444
rule 15 deny tcp source-port eq 5800
rule 16 deny tcp source-port eq 5900
rule 18 deny tcp source-port eq 8998
rule 19 deny tcp source-port eq 445
rule 20 deny udp source-port eq 445
rule 21 deny udp source-port eq 1434
rule 30 deny tcp destination-port eq 3127
rule 31 deny tcp destination-port eq 1025
rule 32 deny tcp destination-port eq 5554
rule 33 deny tcp destination-port eq 9996
rule 34 deny tcp destination-port eq 1068
rule 35 deny tcp destination-port eq 135
rule 36 deny udp destination-port eq 135
rule 37 deny tcp destination-port eq 137
rule 38 deny udp destination-port eq netbios-ns
rule 39 deny tcp destination-port eq 138
rule 40 deny udp destination-port eq netbios-dgm
rule 41 deny tcp destination-port eq 139
rule 42 deny udp destination-port eq netbios-ssn
rule 43 deny tcp destination-port eq 593
rule 44 deny tcp destination-port eq 4444
rule 45 deny tcp destination-port eq 5800
rule 46 deny tcp destination-port eq 5900
rule 48 deny tcp destination-port eq 8998
rule 49 deny tcp destination-port eq 445
rule 50 deny udp destination-port eq 445
rule 51 deny udp destination-port eq 1434
rule 52 permit ip
#
ierface Dialer1 *//该接口用于ADSL拨号*
link-protocol ppp *//封装PPP*
ppp pap local-user test password simple test*//发送ADSL帐号*
mtu 1450
tcp mss 1350
ip address ppp-negotiate
dialer user 1*//使能共享DCC，并设置对端用户名*
dialer-group 1
dialer bundle 1 *//设置该dialer0接口的使用的dialer bundle为1*
nat outbound 3005*//使能NAT，以允许用户上intenet*
firewall packet-filter 3500 inbound*//在接口应用防病毒访问控制列表*
ipsec policy fenbu*//引用安全策略fenbu*

#
interface Ethernet1/0
tcp mss 1350
ip address 192.168.1.1 255.255.255.248

```
firewall packet-filter 3500 inbound//在接口应用防病毒访问控制列表#
interface Ethernet2/0
speed 10
duplex full
pppoe-client dial-bundle-number 1//将dialer0绑定到该接口上
tcp mss 1350
ip address dhcp-alloc
#
interface NULL0
#
firewall zone local
set priority 100
#
firewall zone trust
add interface Ethernet1/0
add interface Ethernet2/0
add interface Dialer1
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
#
FTP server enable
#
dhcp server forbidden-ip 192.168.1.1
#
ip route-static 0.0.0.0 0.0.0.0 Dialer 1 preference 60
#
ntp-service unicast-server 10.16.100.238
#
user-interface con 0
user-interface vty 0 4
authentication-mode scheme
user privilege level 3
set authentication password simple xxxxx
#
return
```

四、 配置关键点

1. IKE第一阶段要配置成野蛮模式。
2. 配置IKE时要配置DPD，便于在发生主备切换，能够重新协商IPSec.
3. 在配置VRRP在接口上，需要跟踪另一个接口的状态，以便能够及时切换。

分部配置NAT上网，应用于NAT的ACL要把分部内网地址访问总部内网地址的数据流拒绝掉，不让其做地址转