SecPath 防火墙 IPSec VPN ADSL拨号NAT穿越模板方式典型配置

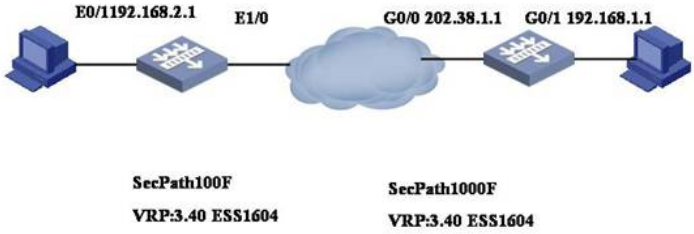
刘军 2006-10-16 发表

SecPath 防火墙 IPSec VPN ADSL拨号NAT穿越模板方式典型配置

一、组网需求

1. 实现武汉和北京两个私网网段的互通。
2. 北京总部必须是静态地址，武汉分部是动态ADSL获得，为公网地址，
   通过SecPath做地址转换上INTERNET,北京总部做地址转换映射内部服务器提供给外部访问。
3. 要求私网两个网段之间的数据流量采用IPSEC隧道加密传输。

二、组网图



三、典型配置

1、防火墙SecPath 100F最终配置

```
 wuhan>dis cu
#
 sysname wuhan
#

 ike local-name wuhan
#
 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
#

 dialer-rule 1 ip permit
 #
 firewall statistic system enable
#
radius scheme system
#
domain system
#
ike peer 1                              //配置IKE参数
 exchange-mode aggressive                    // 配置为野蛮模式
 pre-shared-key 12345                        //配置预共享密钥
```

```
 id-type name                                //ID类型为名字
 remote-name beijing                         //对端名字为beijing
 remote-address 202.38.1.1                   //对端IP
 nat traversal                               //支持NAT穿越
#
ipsec proposal p1                            //定义安全提议
#
ipsec policy policy1 1 isakmp                //定义安全策略
 security acl 3001                           //定义触发数据流
 ike-peer 1                                  //应用的IKE
 proposal p1                                 //应用的安全提议
#
acl number 3000              //定义上网的ACL
 rule 0 deny ip source 192.168.2.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
 rule 1 permit ip source 192.168.2.0 0.0.0.255
acl number 3001              //定义IPSec的ACL
 rule 0 permit ip source 192.168.2.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
#
interface Aux0
 async mode flow
#
 interface Dialer1                           //定义拨号口
 link-protocol ppp
 ppp pap local-user 123 password simple 123      //拨号的用户和密码
 mtu 1450                                    //定义MTU
 ip address ppp-negotiate                    //定义协商地址
 dialer user test
 dialer-group 1
 dialer bundle 1
 nat outbound 3000
 ipsec policy policy1
 #
interface Ethernet0/0
pppoe-client dial-bundle-number 1            //绑定拨号口
#
interface Ethernet0/1
ip address 192.168.2.1 255.255.255.0
#
interface Ethernet0/2
#
interface Ethernet0/3
#
interface Ethernet1/0
#
interface Ethernet1/1
#
interface Ethernet1/2
#
interface NULL0
#
interface LoopBack0
 ip address 10.1.2.1 255.255.255.0
#
firewall zone local
 set priority 100
#
firewall zone trust
 add interface Ethernet0/0
 add interface Ethernet0/1
 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
#
 ip route-static 0.0.0.0 0.0.0.0 Dialer 1 preference 60
#
user-interface con 0
user-interface aux 0
user-interface vty 0 4
#
return
<wuhan>
```

2、防火墙SecPath 1000F最终配置

```
[beijing]dis cu
#
 sysname beijing
#
 ike local-name beijing
#
 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
#
 firewall statistic system enable
#
radius scheme system
#
domain system
#
ike peer 1                                  //配置IKE参数
 exchange-mode aggressive                        // 配置为野蛮模式
 pre-shared-key 12345                        //配置预共享密钥
 id-type name                                //ID类型为名字
 remote-name wuhan                           //对端名字为wuhan
 nat traversal                               //支持NAT穿越
#
ipsec proposal p1                           //定义安全提议
#
ipsec policy-template temp 1                //定义安全策略模板
 ike-peer 1                                 //应用的IKE
 proposal p1                                //应用的安全提议
#
ipsec policy policy1 1 isakmp template temp     //定义安全策略使用安全策略模板
#
acl number 3000                             //定义上网的ACL

 rule 0 deny ip source 192.168.1.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
 rule 1 permit ip source 192.168.1.0 0.0.0.255
```

```
acl number 3001                          //定义NAT SERVER的ACL

 rule 0 deny ip source 192.168.0.0 0.0.255.255 destination 192.168.0.0 0.0.255.2
55
 rule 1 permit ip
#
interface Aux0
 async mode flow
#
interface GigabitEthernet0/0
 ip address 202.38.1.1 255.255.255.0
 nat outbound 3000
 nat server 3001 protocol tcp global current-interface ftp inside 192.168.1.2 ft
p
 ipsec policy policy1
#
interface GigabitEthernet0/1
ip address 192.168.1.1 255.255.255.0

#
interface GigabitEthernet1/0
#
interface GigabitEthernet1/1
#
interface Encrypt2/0
#
interface NULL0
#
interface LoopBack0
 ip address 10.1.1.1 255.255.255.0
#
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
#
 ip route-static 0.0.0.0 0.0.0.0 202.38.1.2 preference 60
#
user-interface con 0
user-interface aux 0
user-interface vty 0 4
#
return
```

[beijing] `

四、配置关键点和关键命令

1.IPSec配置重点主要是模板的配置和NAT穿越.

2.配置重点是定义拨号口，拨号口和以太口的绑定.

3.ACL的制定,上网的ACL和NAT SERVER的ACL要把两个私网网段之间的访问要排除掉.