SecPath安全网关IPSec VPN NAT穿越模板方式典型配置

刘军　2006-09-22 发表

Secpath 1000F防火墙 IPsec VPN NAT穿越模板方式
典型配置

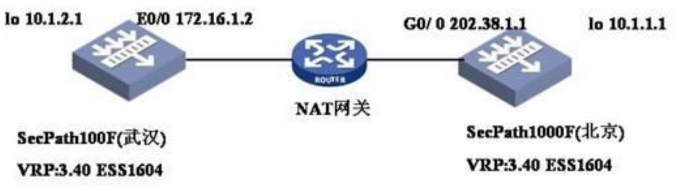
一、组网需求

1.　　实现武汉和北京两个私网的互通。

2.　　北京总部必须是静态地址，武汉分部可以是动态获得也可以是静态配置，为私网地址，去Internet需经过ISP的NAT网关。

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

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
#
 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 3000                                   //定义所保护的数据流

 ike-peer 1                                          //应用的IKE
 proposal p1                                         //应用的安全提议
#
acl number 3000
 rule 0 permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
 rule 1 deny ip
#
interface Aux0
 async mode flow
#
interface Ethernet0/0
 ip address 172.16.1.1 255.255.255.0
#
interface Ethernet0/1
#
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
 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 0.0.0.0 172.16.1.2 preference 60
#
user-interface con 0
```

```
user-interface aux 0
user-interface vty 0 4
#
return
<wuhan>
```

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
#
interface Aux0
 async mode flow
#
interface GigabitEthernet0/0
 ip address 202.38.1.1 255.255.255.0
 ipsec policy policy1
#
interface GigabitEthernet0/1
#
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
 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

```
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
 nat traversal                                     //支持NAT穿越
```

配置重点主要是模板的配置和NAT穿越。