SecPath 1000F防火墙 IPSec VPN NAT穿越模板方式（多分部接入）典型配置

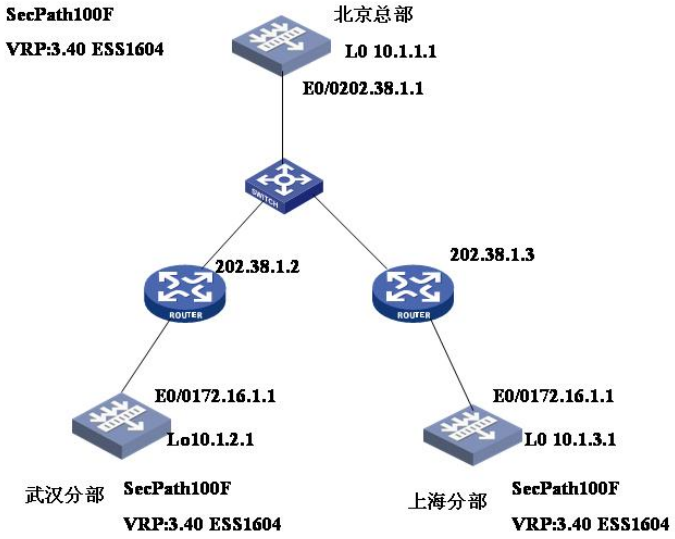
刘军 2006-09-26 发表

SecPath 100F防火墙 IPSec VPN NAT穿越模板方式
（多分部接入）典型配置

一、 组网需求

1． 实现武汉、上海和北京三个私网地址（loopback地址）的互通。
2． 北京总部必须是静态地址，武汉和上海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

北京总部防火墙SecPath 100F最终配置

```
[Quidway]dis cu
#
 sysname Quidway
#
 ike local-name beijing
#
 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 shanghai                    //定义IKE PEER shanghai
 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 shanghai                //对端名字为 shanghai
 nat traversal                       //支持NAT穿越
#
ike peer wuhan                      //定义IKE PEER wuhan
 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_shanghai  //定义安全策略模板
 ike-peer shanghai                   //应用的IKE
 proposal p1                         //应用的安全提议
#
ipsec policy-template temp_wuhan 1
 //定义安全策略模板 temp_wuhan
 ike-peer wuhan                      //应用的IKE
 proposal p1                         //应用的安全提议
#
ipsec policy policy1 1 isakmp template temp_wuhan
//定义安全策略第一条规则应用模板temp_wuhan
#
ipsec policy policy1 2 isakmp template temp_shanghai
//定义安全策略第二条规则应用模板temp_wuhan
#
interface Aux0
 async mode flow
#
interface Ethernet0/0
 ip address 202.38.1.1 255.255.255.0
ipsec policy policy1
#
interface Ethernet0/1
#
interface Ethernet0/2
#
interface Ethernet0/3
#
interface Ethernet1/0
#
interface Ethernet1/1
#
interface Ethernet1/2
#
interface NULL0
#
interface LoopBack0
 ip address 10.1.1.1 255.255.255.0
#
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 10.1.2.0 255.255.255.0 202.38.1.2 preference 60
 ip route-static 10.1.3.0 255.255.255.0 202.38.1.3 preference 60
#
user-interface con 0
user-interface aux 0
user-interface vty 0 4
#
return
[Quidway]
```

武汉防火墙SecPath 100F最终配置

```
Quidway]dis cu
#
 sysname Quidway
#
 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                          //定义IKE PEER
 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           //对端地址
 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                   //定义触发数据流
 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
 ipsec policy policy1
#
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
[Quidway]
```

上海防火墙SecPath 100F最终配置

```
Quidway]dis cu
#
 sysname Quidway
#
 ike local-name shanghai
#
```

```
 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                      //定义IKE PEER
 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      //对端地址
 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              //定义触发数据流
 ike-peer 1                     //应用的IKE
 proposal p1                    //应用的安全提议
#
acl number 3000
 rule 0 permit ip source 10.1.3.0 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
 ipsec policy policy1
#
interface Ethernet0/1
#
interface Ethernet0/2
#
interface Ethernet0/3
#
interface Ethernet1/0
#
interface Ethernet1/1
#
interface Ethernet1/2
#
interface NULL0
#
interface LoopBack0
 ip address 10.1.3.1 255.255.255.0
#
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
[Quidway]
```

四、配置关键点和关键命令

```
ipsec policy-template temp_shanghai 1      //定义安全策略模板 temp_shanghai
 ike-peer shanghai                         //应用的IKE
 proposal p1                               //应用的安全提议
#
ipsec policy-template temp_wuhan 1
//定义安全策略模板 temp_wuhan
 ike-peer wuhan                    //应用的IKE
 proposal p1                       //应用的安全提议
#
ipsec policy policy1 1 isakmp template temp_wuhan
//定义安全策略第一条规则应用模板temp_wuhan
#
ipsec policy policy1 2 isakmp template temp_shanghai
//定义安全策略第二条规则应 用模板temp_wuhan
#
```

配置的关键点就是在北京总部配置两个模版，定义安全策略时定义两条安全策略分别应用两个模板。