SecPath防火墙位于NAT网关后做IPSEC VPN的典型配置

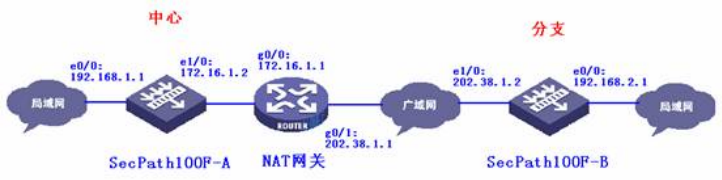
赵彪 2007-03-14 发表

SecPath防火墙位于NAT网关后做IPSEC VPN的典型配置

一、 组网需求：

为了保护中心的VPN网关设备，中心VPN网关设备部署在NAT网关后，通过在NAT网关上做NAT静态映射来实现与分支的互通。

二、 组网图



适合所有版本。

三、 配置信息

1、SecPath100F_A的主要配置

```
#
 sysname zhongxin
#
 ike local-name zhongxin
#
 firewall packet-filter enable
 firewall packet-filter default permit
#
ike peer 1                                          //配置ike peer
 exchange-mode aggressive
 pre-shared-key 123456
 id-type name
 remote-name fenzhi
 nat traversal
#
ipsec proposal 1                                    //配置ipsec proposal
#
ipsec policy-template temp 1                        //配置ipsec policy-template
 ike-peer 1
 proposal 1
#
ipsec policy pol1 1 isakmp template temp            //配置ipsec policy
#
interface Ethernet0/0
 ip address 192.168.1.1 255.255.255.0
#
interface Ethernet1/0
 ip address 172.16.1.2 255.255.255.0
 ipsec policy pol1                                  //启用ipsec policy
#
firewall zone trust
 add interface Ethernet0/0
 set priority 85
#
firewall zone untrust
 add interface Ethernet1/0
 set priority 5
#
 ip route-static 0.0.0.0 0.0.0.0 172.16.1.1 preference 60
#
```

2、SecPath100F_B的主要配置

```
#
 sysname fenzhi
#
 ike local-name fenzhi
#
 firewall packet-filter enable
 firewall packet-filter default permit
#
ike peer 1                                          //配置ike peer
 exchange-mode aggressive
 pre-shared-key 123456
 id-type name
 remote-name zhongxin
 remote-address 202.38.1.100
 nat traversal
#
ipsec proposal 1                                    //配置ipsec proposal
#
ipsec policy pol1 1 isakmp                          //配置ipsec policy
 security acl 3000
 ike-peer 1
 proposal 1
#
acl number 3000                                     //定义保护数据流
 rule 0 permit ip source 192.168.2.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
 rule 1 deny ip
#
interface Ethernet0/0
 ip address 192.168.2.1 255.255.255.0
#
interface Ethernet1/0
 description WAN
 ip address 202.38.1.2 255.255.255.0
 ipsec policy pol1                                  //启用ipsec policy
#
firewall zone trust
 add interface Ethernet0/0
 set priority 85
#
firewall zone untrust
 add interface Ethernet1/0
 set priority 5
#
 ip route-static 0.0.0.0 0.0.0.0 202.38.1.1 preference 60
#
```

3、nat网关的主要配置

```
#
 sysname nat
#
 nat static inside ip 172.16.1.2 global ip 202.38.1.100          //配置静态映射
#
interface GigabitEthernet0/0
 description LAN
 ip address 172.16.1.1 255.255.255.0
#
interface GigabitEthernet0/1
 description WAN
 ip address 202.38.1.1 255.255.255.0
 nat outbound static                                            //启用静态映射
#
 ip route-static 0.0.0.0 0.0.0.0 202.38.1.2 preference 60
 ip route-static 192.168.1.0 255.255.255.0 172.16.1.2 preference 60
#
```

> **四、 配置关键点**
> 见注释。