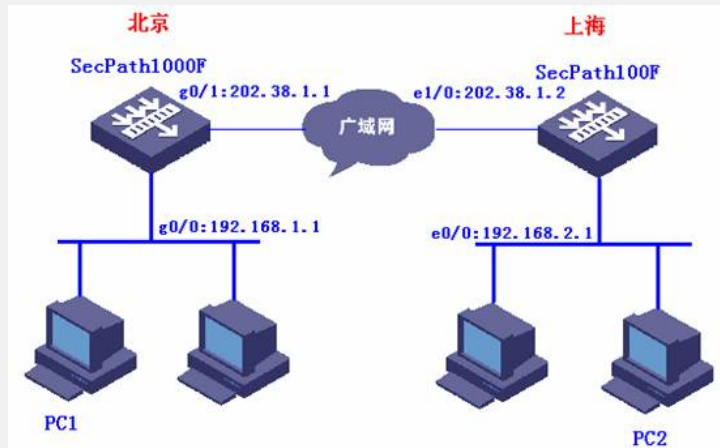


SecPath防火墙GRE VPN典型组网配置

一、组网需求:

北京总部和分支上海之间需要进行互通, PC1与PC2之间需要进行互访。

二、组网图



SecPath1000F: 版本为Version 3.40, ESS 1604P01;

SecPath100F: 版本为Version 3.40, Release 1210P01.

三、配置步骤

1. SecPath1000F的主要配置

```
[beijing]dis cu
#
sysname beijing
#
firewall packet-filter enable
firewall packet-filter default permit
#
firewall statistic system enable
#
radius scheme system
#
domain system
#
acl number 3000 //创建ACL
rule 0 permit tcp source 192.168.1.0 0.0.0.255
rule 1 permit udp source 192.168.1.0 0.0.0.255
rule 2 permit icmp
rule 3 permit gre source 202.38.1.1 0 destination 202.38.1.2 0 //允许gre协议通过
rule 4 deny ip
#
interface GigabitEthernet0/0
ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet0/1
ip address 202.38.1.1 255.255.255.0
firewall packet-filter 3000 outbound //应用ACL
#
interface Tunnel1 //创建隧道接口
ip address 10.0.0.1 255.255.255.0
source 202.38.1.1
destination 202.38.1.2
gre key 123 //指定gre key
#
```

```
firewall zone trust
add interface GigabitEthernet0/0
set priority 85
#
firewall zone untrust
add interface GigabitEthernet0/1
add interface Tunnel1
set priority 5
#
ip route-static 192.168.2.0 255.255.255.0 10.0.0.2 //配置去往对端私网的路由
#
```

2. SecPath100F的主要配置

```
[shanghai]dis cu
#
sysname shanghai
#
firewall packet-filter enable
firewall packet-filter default permit
#
insulate
#
firewall statistic system enable
#
acl number 3000 //创建ACL
rule 0 permit tcp source 192.168.2.0 0.0.0.255
rule 1 permit udp source 192.168.2.0 0.0.0.255
rule 2 permit icmp
rule 3 permit gre source 202.38.1.2 0 destination 202.38.1.1 0 //允许gre协议通过
rule 4 deny ip
#
interface Ethernet0/0
ip address 192.168.2.1 255.255.255.0
#
interface Ethernet1/0
ip address 202.38.1.2 255.255.255.0
firewall packet-filter 3000 outbound
#
interface Tunnel1 //创建隧道接口
ip address 10.0.0.2 255.255.255.0
source 202.38.1.2
destination 202.38.1.1
gre key 123 //指定gre key
#
firewall zone trust
add interface Ethernet0/0
set priority 85
#
firewall zone untrust
add interface Ethernet1/0
add interface Tunnel1
set priority 5
#
ip route-static 192.168.1.0 255.255.255.0 10.0.0.1 //配置去往对端私网的路由
#
```

四、配置关键点

1. 两端的gre key必须保持一致;
2. 必须有去往对端私网的路由;
3. ACL 3000 中必须允许gre协议通过。