SecPath防火墙IPSec over GRE + OSPF典型配置

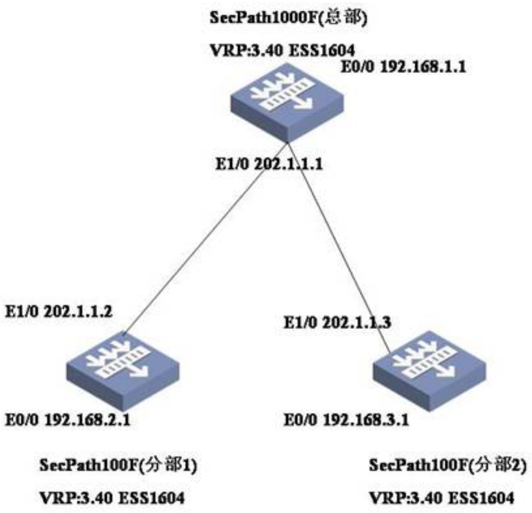
刘军　2006-10-16 发表

SecPath防火墙IPSec over GRE + OSPF
典型配置

一、组网需求

分部1和分部2通过野蛮IPSec的方式连接到中心，采用IPSEC -Over-GRE的方式，在tunnel上运行OSPF协议来实现总部和分部之间的互通。

二、组网图



三、典型配置

总部防火墙SecPath 1000F最终配置

```
center>dis cu
#
 sysname center
#
 ike local-name center                    //中心ike的local-name
#
 router id 1.1.1.1
#
 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 branch1                          //配置到分部1的ike peer
 exchange-mode aggressive                      //设置IPSec为野蛮方式
 pre-shared-key abc                       //预共享密钥为abc
 id-type name                          //选择ID类型为名字/

 remote-name branch1                      //分部1的名字为branch1
 remote-address 10.1.1.2                  //分部1的地址
#
```

```
ike peer branch2                              //配置到分部2的ike peer
 exchange-mode aggressive                    //设置IPSec为野蛮方式
 pre-shared-key abc                          //预共享密钥为abc
 id-type name                                //选择ID类型为名字
 remote-name branch2                         //分部1的名字为branch1
 remote-address 10.1.2.2                     //分部1的地址
#
ipsec proposal 1                              //定义ipsec proposal
#
ipsec policy branch1 10 isakmp                //配置到分部1的ipsec policy
 security acl 3000
 ike-peer branch1
 proposal 1
#
ipsec policy branch2 10 isakmp                //配置到分部2的ipsec policy
 security acl 3001
 ike-peer branch2
 proposal 1
#
acl number 3000
 rule 0 permit ip source 192.168.1.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
acl number 3001
 rule 0 permit ip source 192.168.1.0 0.0.0.255 destination 192.168.3.0 0.0.0.255
#
interface Aux0
 async mode flow
#
interface GigabitEthernet0/0
 ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet0/1
 ip address 202.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0
#
interface GigabitEthernet1/1
#
interface Encrypt2/0
#
interface Tunnel0                        //配置中心和分部1之间的GRE tunnel

 ip address 10.1.1.1 255.255.255.0
 source 202.1.1.1
 destination 202.1.1.2
  ipsec policy branch1                   //应用IPSec策略

#
interface Tunnel1                       //配置中心和分部1之间的GRE tunnel

 ip address 10.1.2.1 255.255.255.0
 source 202.1.1.1
 destination 202.1.1.3
 ipsec policy branch2                    //应用IPSec策略
#
interface NULL0
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
firewall zone local
 set priority 100
#
firewall zone trust
 add interface GigabitEthernet0/0
 add interface GigabitEthernet0/1
 add interface Tunnel0
 add interface Tunnel1
 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
#
ospf 1
 area 0.0.0.10                              //分部1属于area 10
  network 10.1.1.0 0.0.0.255
 #
 area 0.0.0.20                             //分部2属于area 20
  network 10.1.2.0 0.0.0.255
 #
 area 0.0.0.0                              //总部属于area 0
  network 1.1.1.1 0.0.0.0
  network 192.168.1.0 0.0.0.255
#
user-interface con 0
user-interface aux 0
user-interface vty 0 4
#
return
```

<center>

分部1防火墙SecPath 100F最终配置

```
[branch1]dis cu
#
 sysname branch1
#
 ike local-name branch1                   //分部1的ike的local-name
#
 router id 2.2.2.2
#
 firewall packet-filter enable
 firewall packet-filter default permit
#
 insulate
#
 firewall statistic system enable
#
radius scheme system
#
domain system
#
ike peer center                          //配置到中心的ike peer
 exchange-mode aggressive                 //设置IPSec为野蛮方式
 pre-shared-key abc                       //预共享密钥为abc
 id-type name                             //预共享密钥为abc
 remote-name center                       //对端的名字为center
 remote-address 10.1.1.1                  //对端的地址为202.101.1.1
#
ipsec proposal 1                         //定义ipsec proposal
#
ipsec policy brach1 10 isakmp             //配置到中心的ipsec policy
 security acl 3000                        //指定安全策略所引用的访问控制列表号
 ike-peer center                          //引用ike peer
 proposal 1                               //引用ipsec proposal
#
acl number 3000
 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 Ethernet0/0
 ip address 192.168.2.1 255.255.255.0
#
interface Ethernet0/1
#
interface Ethernet0/2
#
interface Ethernet0/3
#
interface Ethernet1/0
 ip address 202.1.1.2 255.255.255.0


#
interface Ethernet1/1
#
interface Ethernet1/2
#
interface Tunnel0
 ip address 10.1.1.2 255.255.255.0
 source 202.1.1.2
 destination 202.1.1.1
 ipsec policy brach1                      //在接口上应用IPSec policy

#
interface NULL0
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
firewall zone local
 set priority 100
#
firewall zone trust
 add interface Ethernet0/0
 add interface Ethernet1/0
 add interface Tunnel0
 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
#
ospf 1
 area 0.0.0.10
  network 2.2.2.2 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 192.168.2.0 0.0.0.255
#
user-interface con 0
user-interface aux 0
user-interface vty 0 4
#
return
[branch1]
```

分部2防火墙SecPath 100F最终配置

```
 <brach2>dis cu
#
 sysname brach2
#
 ike local-name branch2                    //分部2的ike的local-name
#
 router id 3.3.3.3
#
 firewall packet-filter enable
 firewall packet-filter default permit
#
 insulate
#
 firewall statistic system enable
#
radius scheme system
#
domain system
#
ike peer center                          //配置到中心的ike peer
 exchange-mode aggressive                  //设置IPSec为野蛮方式
 pre-shared-key abc                       //预共享密钥为abc
 id-type name                             //选择名字作为ike协商的ID/

 remote-name center                        //对端的名字为center
 remote-address 10.1.2.1                   //对端的名字为center
#
ipsec proposal 1                           //定义ipsec proposal
#
ipsec policy branch2 10 isakmp             //配置到中心的ipsec policy
 security acl 3000                        //指定安全策略所引用的访问控制列表号
 ike-peer center                          //引用ike peer
 proposal 1                               //引用ipsec proposal
#
acl number 3000
 rule 0 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
#
interface Aux0
 async mode flow
#
interface Ethernet0/0
 ip address 192.168.3.1 255.255.255.0
```

```
#
interface Ethernet0/1
#
interface Ethernet0/2
#
interface Ethernet0/3
#
interface Ethernet1/0
 ip address 202.1.1.3 255.255.255.0

#
interface Ethernet1/1
#
interface Ethernet1/2
#
interface Tunnel0
 ip address 10.1.2.2 255.255.255.0
 source 202.1.1.3
 destination 202.1.1.1
ipsec policy branch2                //在接口上应用IPSec policy
#
interface NULL0
#
interface LoopBack0
 ip address 3.3.3.3 255.255.255.255
#
firewall zone local
 set priority 100
#
firewall zone trust
 add interface Ethernet0/0
 add interface Ethernet1/0
 add interface Tunnel0
 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
#
ospf 1
 area 0.0.0.20
  network 3.3.3.3 0.0.0.0
  network 10.1.2.0 0.0.0.255
  network 192.168.3.0 0.0.0.255
#
user-interface con 0
user-interface aux 0
user-interface vty 0 4
#
return
```

```
<brach2>                                  `
```

四、配置关键点和关键命令

1．配置触发IPSec的数据流是私网的地址。

2．配置OSPF不能将公网接口放进去。

3．要在TUNNEL口上应用IPSec policy