SecPath防火墙GRE over IPSec+ospf的典型配置

万欣 2008-07-07 发表

SecPath防火墙GRE over IPSec+ospf的典型配置

一、 组网需求：

两个Peer分别使用的是SecPath1000F，中间公网使用一台SecPath100F起连接作用，两局域网分别使用的是SecPath1000F的LoopBack0口来模拟。在两个Peer上配置GRE over IPSec，使两个局域网能够穿越公网进行通信，并且保护一切传输的数据。

二、 组网图

SecPath1000F：版本为Version 3.40, ESS 1622;

三、 配置步骤

1．SecPath1000F（左）的主要配置：

```
sysname fw1
#
 router id 10.1.1.1
#
 firewall packet-filter enable
 firewall packet-filter default permit
#
ike proposal 10   //设置IKE的策略
 authentication-algorithm md5  //选择md5算法来进行验证（验证方式为预共享密钥，密钥交换为DH:gr
oup1,因为此两项均为缺省设置，故没有显示在dis cu 中，特此说明）
 sa duration 1500  //设置IKE的生存周期为1500s
#
ike peer wanxin  //设置预共享密钥的认证字
 pre-shared-key h3c   //密钥为：h3c（对端也必须一样）
 remote-address 202.103.1.1  //设置对端地址
#
ipsec proposal wanxin  //创建一个名为“wanxin”的安全提议
encapsulation-mode transport   //报文封装采用传输模式(安全协议采用esp,认证算法采用sha1，此两
项均为缺省设置，故也没有显示在dis cu 中)
#
ipsec policy 1 10 isakmp   //创建安全策略，协商方式为自动协商，也就是采用IKE的策略协商
 security acl 3000  //引用下面设置的acl 3000
 ike-peer wanxin   //引用上面设置的“ike peer wanxin”
 proposal wanxin   //引用上面设置的“ipsec proposal wanxin”
 sa duration time-based 1500  //设置基于时间的生存周期为1500s
#
acl number 3000  //创建加密数据流（加密的是两Peer出口的网段，这个很关键）
 rule 1 permit gre source 192.168.1.0 0.0.0.255 destination 202.103.1.0 0.0.0.255
 rule 2 deny ip
#
interface GigabitEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 ipsec policy 1  //在出接口上应用安全策略（只有应用了IPSec才能生效）
#
interface Tunnel0  //创建GRE隧道
 ip address 1.1.1.1 255.255.255.0
 source 192.168.1.1
 destination 202.103.1.1
#
```

```
interface LoopBack0  //用一个回环口地址带模拟一个LAN地址
 ip address 10.1.1.1 255.255.255.0
#
firewall zone untrust
 add interface GigabitEthernet0/0
 add interface Tunnel0  //切记隧道接口也需要加入某一个域
 set priority 85
#
ospf 1  //使用OSPF来保证两LAN之间能路由
 area 0.0.0.0
  network 1.1.1.0 0.0.0.255
  network 10.1.1.0 0.0.0.255
#
 ip route-static 0.0.0.0 0.0.0.0 192.168.1.2 preference 60  //保证两Peer之间能够通信，从而协商IPSec
参数，同时也触发加密流量
```

2．SecPath1000F（Peer2）的主要配置：

```
注：Peer2的配置与Peer1基本相同，故注释同上
sysname fw2
#
 router id 10.2.2.2
#
 firewall packet-filter enable
 firewall packet-filter default permit
#
ike proposal 10
 authentication-algorithm md5
 sa duration 1500
#
ike peer wanxin
 pre-shared-key h3c
 remote-address 192.168.1.1
#
ipsec proposal wanxin
encapsulation-mode transport
#
ipsec policy 1 10 isakmp
 security acl 3000
 ike-peer wanxin
 proposal wanxin
 sa duration time-based 1500
#
acl number 3000
 rule 1 permit gre source 202.103.1.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
 rule 2 deny ip
#
interface GigabitEthernet0/0
 ip address 202.103.1.1 255.255.255.0
 ipsec policy 1
#
interface Tunnel0
 ip address 1.1.1.2 255.255.255.0
 source 202.103.1.1
 destination 192.168.1.1
#
interface LoopBack0
 ip address 10.2.2.2 255.255.255.0
#
firewall zone untrust
 add interface GigabitEthernet0/0
 add interface Tunnel0
 set priority 5
#
```

```
ospf 1
 area 0.0.0.0
  network 1.1.1.0 0.0.0.255
  network 10.2.2.0 0.0.0.255
#
 ip route-static 0.0.0.0 0.0.0.0 202.103.1.2 preference 60
```

3．验证结果：

ping –a 10.1.1.1 10.2.2.2 //测试两LAN之间是否能通信

dis ike sa //查看IKE是否建立完成

dis ipsec sa //查看安全联盟的信息

dis ipsec statistica //查看安全报文的统计信息

四、 配置关键点

1．Peer1与Peer2的IKE，Ipsec两阶段的安全参数必须相同；

2．配置顺序一般为：

（1）两Peer之间能够相互Ping通

（2）隧道建立UP

（3）路由（本例为OSPF）配置完成，确保两LAN之间能够Ping通

（4）配置IPSec

3．其他关键点见注释。