SecPath防火墙IPSec（手工协商）的典型配置

万欣 2008-07-07 发表

SecPath防火墙IPSec（手工协商）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IPSec（手工协商），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
#
firewall packet-filter enable
 firewall packet-filter default permit
#
ipsec proposal wanxin  //创建一个名为“wanxin”的安全提议（全部使用缺省策略）
#
ipsec policy 1 10 manual  //创建安全策略，协商方式为手工协商，不采用IKE的策略协商
security acl 3000  //引用下面设置的acl 3000
 proposal wanxin  //引用上面设置的“ipsec proposal wanxin”
 tunnel local 192.168.1.1  //设置本端地址
 tunnel remote 202.103.1.1  //设置对端地址
 sa spi inbound esp 54321  //设置SPI和密钥（两者分别和对端设置的参数相反）
 sa string-key inbound esp 54321
 sa spi outbound esp 12345
 sa string-key outbound esp 12345
#
acl number 3000  //创建加密数据流（加密的是两LAN的网段，这个很关键）
  rule 0 permit ip source 10.1.1.0 0.0.0.255 destination 10.2.2.0 0.0.0.255
  rule 1 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 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
 set priority 85
#
 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
#
```

```
 firewall packet-filter enable
 firewall packet-filter default permit
#
ipsec proposal wanxin
#
ipsec policy 1 10 manual
security acl 3000
 proposal wanxin
 tunnel local 202.103.1.1
 tunnel remote 192.168.1.1
 sa spi inbound esp 12345
 sa string-key inbound esp 12345
 sa spi outbound esp 54321
 sa string-key outbound esp 54321
#
acl number 3000
 rule 0 permit ip source 10.2.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
 rule 1 deny ip
#
interface GigabitEthernet0/0
 ip address 202.103.1.1 255.255.255.0
 ipsec policy 1
#
interface LoopBack0
 ip address 10.2.2.2 255.255.255.0
#
firewall zone untrust
 add interface GigabitEthernet0/0
set priority 5
#
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 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Ipsec阶段的安全参数必须相同,手工配置的SPI和密钥两Peer间必须相反；

2．其他关键点见注释。