SecPath防火墙面向对象的典型配置

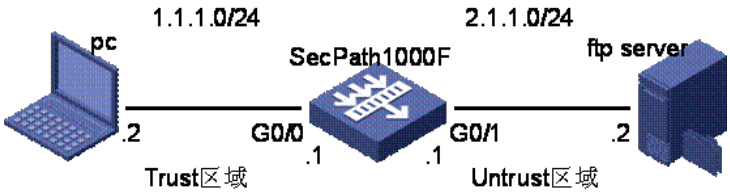
万欣 2008-07-04 发表

SecPath防火墙面向对象的典型配置

一、 组网需求：

利用SecPath防火墙的面向对象特性使内网PC在特定的时间内才能访问外网FTPServer，并且利用NAT隐藏了地址。

二、 组网图



SecPath1000F：版本为Version 3.40, ESS 1622;
FTP Server：Windows XP操作系统；
PC：Windows XP操作系统.

三、 配置步骤

1. SecPath1000F的主要配置：

```
#
 sysname fw
#
 firewall packet-filter enable
#
 firewall statistic system enable
#
radius scheme system
 server-type huawei
#
domain system
#
 object address tr-ip 1.1.1.2 255.255.255.255   //创建地址对象tr-ip
 object address untr-ip 2.1.1.2 255.255.255.255  //创建地址对象untr-ip

#
 object service-group sg   //创建服务对象sg
  add ip
#
acl name  a    //创建流对象a，定义流规则，套用限制时间
 rule 0 permit source tr-ip destination untr-wanxin service sg time-range t-acl
acl name  b    //创建流对象b，定义流规则，套用限制时间
rule 0 permit source untr-ip destination tr-wanxin service sg time-range t-acl
acl name  c    //创建流对象c, 不受限制时间的约束
 rule 0 permit
#
interface GigabitEthernet0/0
 ip address 1.1.1.1 255.255.255.0
 firewall packet-filter a inbound  //接口下应用流规则，下同
 firewall packet-filter c outbound
#
interface GigabitEthernet0/1
 ip address 2.1.1.1 255.255.255.0
 firewall packet-filter b inbound
 firewall packet-filter c outbound
 nat outbound a   //将匹配acl a的流量做NAT，将其地址转换成g0/1的接口地址
```

#
 time-range t-acl 08:00 to 18:00 working-day //设置时间规则，本例设置的时间范围为周一至周五的早上8点到下午6点
#
firewall zone trust
 add interface GigabitEthernet0/0
 set priority 85
#
firewall zone untrust
 add interface GigabitEthernet0/1
 set priority 5
#

2．验证结果：

在设置的时间范围内，PC可以访问FTP服务器，并且PC的地址被转换成了G0/1的接口地址。超出了该时间范围，PC将不能访问FTP服务器。（建议修改clock进行测试）

四、 配置关键点

面向对象设置的对象名称比较的多，在应用的时候应该特别注意对象名称与IP地址以及协议的一一对应关系，不要张冠李戴。