SecPath防火墙报文统计和连接限制典型配置

巫继雨 2006-09-26 发表

SecPath防火墙报文统计和连接限制典型配置

一、组网需求

192.168.1.0/24网段为内网用户，处于信任域，通过NAT上网。Server服务器部署在dmz区域，对外提供www服务。

要求：

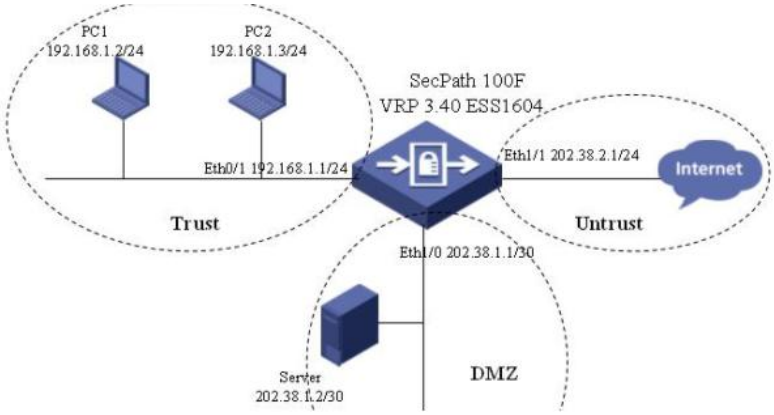
1，内网用户只有在学习时间可以上网，并且限制每个人的对外连接数；

2，对DMZ域入方向的tcp、udp连接进行限制；

3，对Trust域向外发起的IP连接数进行限制；

4，对防火墙总体的TCP连接数和不同协议的流量比例进行限制。

二、组网图



三、配置步骤

```
[SecPath100F]dis cur
#
 sysname SecPath100F
#
 firewall packet-filter enable
 firewall packet-filter default permit
#
 insulate
#
 //使能连接限制
connection-limit enable
 //对不在连接限制acl中的报文不启用连接限制
connection-limit default deny
//连接限制的默认上限为50,下限为20
 connection-limit default amount upper-limit 50 lower-limit 20
#
 //nat转换所用的地址池
nat address-group 1 202.38.2.2 202.38.2.5
#
 firewall statistic system enable
 //设置tcp流量所占的百分比为75％，udp所占的百分比为15％，icmp所占的百分比为5%
 //，并且允许流量在10%范围内波动，每隔10分钟进行一次流量统计
firewall statistic system flow-percent tcp 70 udp 15 icmp 5 alternation 10 time 10

 //设置允许的tcp连接数的上限为45万，下限为40万
 firewall statistic system connect-number tcp high 450000 low 400000
 //对超过流量限制的报文告警并丢弃
 firewall statistic warning-level drop
#
radius scheme system
#
domain system
#
```

```
//在学习时间允许对192.168.1.0/24网段的用户进行nat转换
acl number 2000
 rule 0 permit source 192.168.1.0 0.0.0.255 time-range study
 rule 1 deny
#
 //创建连接限制策略
connection-limit policy 1
//限制192.168.1.0/24网段每个用户的连接数上限为50，下限为30
 limit 1 acl 2000 per-source amount 50 30
#
interface Aux0
 async mode flow
#
interface Ethernet0/0
#
interface Ethernet0/1
 ip address 192.168.1.1 255.255.255.0
#
interface Ethernet0/2
#
interface Ethernet0/3
#
interface Ethernet1/0
 ip address 202.38.1.1 255.255.255.252
#
interface Ethernet1/1
 ip address 202.38.2.1 255.255.255.0
 //进行nat转换
nat outbound 2000 address-group 1
#
interface Ethernet1/2
#
interface Encrypt2/0
#
interface NULL0
#
 //允许上网的时间段
time-range study 08:00 to 17:00 working-day
#
firewall zone local
 set priority 100
#
firewall zone trust
 //将eth0/1加入信任域
 add interface Ethernet0/1
 set priority 85
 //在信任域的出方向使能IP统计功能
statistic enable ip outzone
//使能基于信任域出方向的IP连接数量监控
 statistic connect-speed ip outzone tcp high 3000 low 2500
 statistic connect-speed ip outzone udp high 2500 low 2000
#
firewall zone untrust
 //将eth1/1加入非信任域
 add interface Ethernet1/1
 set priority 5
#
firewall zone DMZ
 //将eth1/0加入DMZ域
 add interface Ethernet1/0
 set priority 50
 //使能域统计功能
statistic enable zone inzone
//使能域连接数量监控
```

```
 statistic connect-number zone inzone tcp high 200000 low 150000
 statistic connect-number zone inzone udp high 150000 low 100000
#
firewall interzone local trust
#
firewall interzone local untrust
#
firewall interzone local DMZ
#
firewall interzone trust untrust
#
firewall interzone trust DMZ
#
firewall interzone DMZ untrust
#
 nat connection-limit-policy 1
#
user-interface con 0
user-interface aux 0
user-interface vty 0 4
 authentication-mode none
 user privilege level 3
#
return
```

四、配置关键点

具体见上面蓝色字体部分

1，连接数限制配置步骤：

- 使能连接数限制功能；
- 创建连接限制策略；
- 在全局下启用nat转换的连接限制。

2，配置域(IP)统计的步骤：

- 使能域(IP)统计功能；
- 使能域(IP)连接数量监控；