SecPath防火墙黑名单、MAC绑定和ACL组合测试典型配置指导

巫继雨 2006-09-01 发表

SecPath黑名单、MAC绑定和ACL组合测试典型配置指导

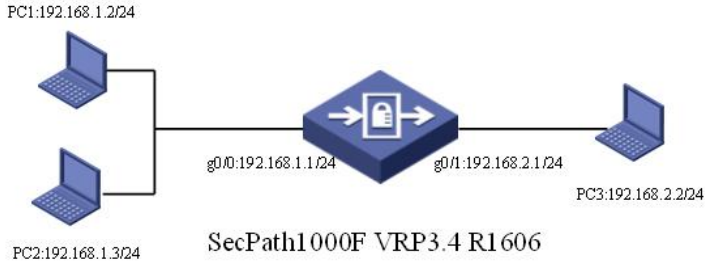
一、组网需求

1，黑名单分为静态和动态两种。静态需要手动将ip地址添加到黑名单表中。动态黑名单是和地址扫描、端口扫描的攻击防范结合到一起的。本例通过静态配置黑名单来防止PC1对网络的访问。

2，对PC2进行mac绑定处理，即PC2的ip地址只有发自PC2才会被防火墙处理。这里假设PC2的MAC地址为0000-0000-0001。

3，只允许PC2对网络进行访问，其他机器不允许访问网络。通过ACL实现。

二、网络拓扑



三、配置步骤

```
[SecPath1000F]firewall packet-filter  default  permit
[SecPath1000F]Interface  GigabitEthernet  0/0
[SecPath1000F-interfaceGigabitEthernet0/0]      ip address 192.168.2.1 24
[SecPath1000F-interfaceGigabitEthernet0/0]      quit
[SecPath1000F]Interface  GigabitEthernet  0/1
[SecPath1000F-interfaceGigabitethernet0/1] ip address 192.168.1.1 24
[SecPath1000F-interfaceGigabitethernet0/1] quit
[SecPath1000F]firewall zone trust
[SecPath1000F-firewall-trust]add interface Gigabitethernet 0/1
[SecPath1000F-firewall-trust]quit
[SecPath1000F]firewall zone untrust
[SecPath1000F-firewall-untrust]add interface Gigabitethernet 0/0
[SecPath1000F-firewall-untrust]quit

[SecPath1000F]firewall blacklist  192.168.1.2          //将PC1的IP地址添加的黑名单表项
[SecPath1000F]firewall blacklist  enable               //使能黑名单功能
//将发现的地址扫描攻击的源地址添加到黑名单中，阻断100分钟
[SecPath1000F]firewall  defend  ip-sweep blacklist-timeout 100
//将发现的端口扫描攻击的源地址添加到黑名单中，阻断200分钟
[SecPath1000F]firewall  defend  port-scan blacklist-timeout  200
[SecPath1000F]firewall blacklist  enable     使能黑名单功能

//ip地址192.168.1.2已经和 MAC地址0-0-1建立了一一对应关系
[SecPath1000F]firewall mac-binding 192.168.1.2 0-0-1
[SecPath1000F]firewall mac-binding enable              //使能MAC绑定

[SecPath1000F]acl number 3000
//允许192.168.1.2主机的数据流通过
[SecPath1000F-acl-adv-3000]rule  permit  ip source  192.168.1.2 0
[SecPath1000F-acl-adv-3000]rule deny ip                //拒绝其他机器的访问
[SecPath1000F-acl-adv-3000]quit
[SecPath1000F]interface  GigabitEthernet  0/0
//将高级ACL应用到防火墙当前接口上的入方向检测
[SecPath1000F-GigabitEthernet0/0]firewall  packet-filter  3000 inbound
```

四、配置要点

1，配置黑名单表项，注意使能黑名单；

2.，配置MAC和IP地址绑定关系，注意使能地址绑定功能；

3，配置ACL；在接口上应用ACL。

五、验证结果

1． 静态黑名单配置后，可以看到如下信息：

PC1和PC3无法ping通。

2．动态黑名单配置后，在PC3使用攻击工具触发防火墙的攻击防范后，在1000F将会提示攻击的源IP地址添加到黑名单中，PC2和PC3无法ping通。

3．配置MAC绑定后，可以看到如下信息：

改变PC2的mac地址为0000-0000-1111，PC2和PC3将会无法ping通

4．删除黑名单和MAC绑定后，配置ACL，可以看到如下信息：

只有PC2可以和PC3互通。