SecPath防火墙常见flood攻击防范典型配置

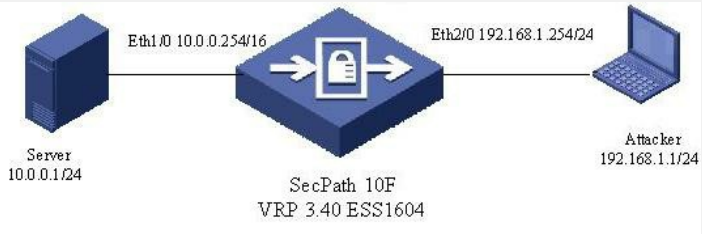
巫继雨 2006-09-23 发表

SecPath防火墙常见flood攻击防范典型配置

一、组网需求

SecPath开启syn-flood、icmp-flood和udp-flood的攻击防范,防止对Server的flood攻击。

二、组网图



软件版本如下:

SecPath10F:VRP 3.40 ESS 1604;

三、配置步骤

```
[Quidway]dis cur
#
 sysname Quidway
#
 firewall packet-filter enable
 firewall packet-filter default permit
#
 undo connection-limit enable
 connection-limit default deny
 connection-limit default amount upper-limit 50 lower-limit 20
#
 firewall statistic system enable          //开启报文全局统计
#
radius scheme system
#
domain system
#
local-user admin
 password cipher .]@USE=B,53Q=^Q`MAF4<1!!
 service-type telnet terminal
 level 3
 service-type ftp
#
acl number 3000
 rule 1 permit ip source 192.168.1.0 0.0.0.255
#
interface Ethernet1/0
 ip address 10.0.0.254 255.255.0.0
#
interface Ethernet2/0
 speed 10
 duplex full
 ip address 192.168.1.254 255.255.255.0
#
interface NULL0
#
firewall zone local
 set priority 100
#
firewall zone trust
 add interface Ethernet2/0
```

```
 set priority 85
#
firewall zone untrust
 add interface Ethernet1/0                //服务器加入非信任域
 set priority 5
 statistic enable ip inzone               //开启所在域入方向的报文统计

#
firewall zone DMZ
 set priority 50
#
firewall interzone local trust
#
firewall interzone local untrust
#
firewall interzone local DMZ
#
firewall interzone trust untrust
#
firewall interzone trust DMZ
#
firewall interzone DMZ untrust
#
 FTP server enable
#
 firewall defend land
 firewall defend smurf
 firewall defend winnuke
 firewall defend syn-flood enable         //使能syn-flood攻击范
 firewall defend icmp-flood enable        //使能mcp-flood攻击防范
                                    //设置受保护主机和启用tcp代理
firewall defend syn-flood ip 10.0.0.1 max-rate 100 tcp-proxy
 firewall defend icmp-flood ip 10.0.0.1    //设置受保护的主机
#
user-interface con 0
user-interface vty 0 4
 authentication-mode scheme
#
return
```

四、配置关键点

1．在全局下开启报文统计；

2．开启受保护主机所在域的入方向的报文统计；

3．使能相应的flood攻击防范；

4．设置受保护主机。

五、验证结果

在攻击机Attacker：192.168.1.1上对10.0.0.1进行syn-flood和icmp-flood攻击，防火墙告警。

```
[Quidway]
%Jan1 08:01:06:125 2000 Quidway SEC/5/ATCKDF:atckType(1016)=(6)ICMP-flood;
rcvIfNa
me(1023)=Ethernet2/0;srcIPAddr(1017)=192.168.1.1;srcMacAddr(1021)=;destIPAddr(
1019)=10.0.0.1;destMacAddr(1022)=;atckSpeed(1047)=1000;atckTime_cn(1048)=200
00101080102
[Quidway]
%Jan1 08:01:36:125 2000 Quidway SEC/5/ATCKDF:atckType(1016)=(5)SYN-flood;r
cvIfNam
e(1023)=Ethernet2/0;srcIPAddr(1017)=192.168.1.1;srcMacAddr(1021)=;destIPAddr(10
19)=10.0.0.1;destMacAddr(1022)=;atckSpeed(1047)=100;atckTime_cn(1048)=200001
01080117
```