SecPath防火墙透明模式典型配置

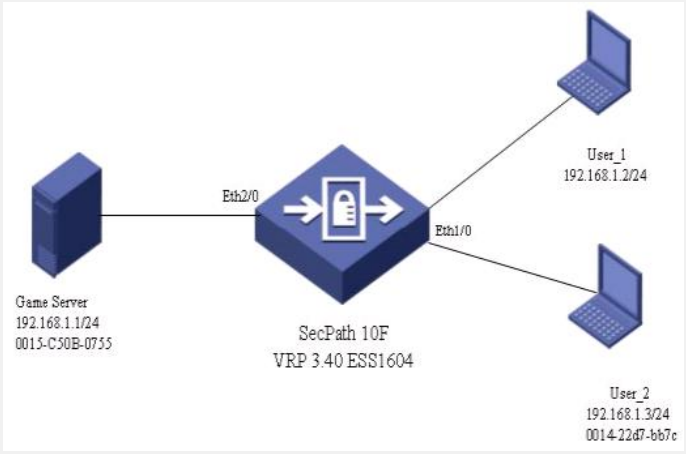
巫继雨 2006-09-26 发表

SecPath防火墙透明模式典型配置

一、组网需求

防火墙工作在透明模式下，平时使用web网管进行管理。192.168.1.1/24为游戏服务器，允许User_1访问游戏服务器，禁止User_2访问游戏服务器。

二、组网图



三、配置步骤

```
[SecPath10F]dis cur
#
 sysname SecPath10F
#
 dvpn service enable
#
 firewall packet-filter enable
 firewall packet-filter default permit
#
 undo firewall arp-learning enable                    //禁止防火墙ARP表项学习功能

 firewall mode transparent
 firewall system-ip 192.168.1.254 255.255.255.0     //为防火墙设置管理地址
 firewall unknown-mac flood                          //对未知目的MAC地址的报文进行泛洪处理
#
 firewall transparent-mode aging-time 600            //配置MAC地址转发表的老化时间为600秒
 firewall transparent-mode transmit ipx              //配置允许通过ipx协议报文

#
 firewall statistic system enable
#
radius scheme system
#
domain system
#
local-user h3c                                       //配置web网管的用户
 password simple h3c
 service-type telnet
 level 3
#
//配置基于MAC的访问控制列表,对源mac为User_2的数据帧进行阻断
```

```
acl number 4000
 rule 0 deny source-mac 0014-22d7-bb7c ffff-ffff-ffff dest-mac 0015-c50b-0755 ffff-ffff-
ffff
#
interface Ethernet1/0
 promiscuous
 firewall ethernet-frame-filter 4000 inbound          //在接口的inbound方向上应用访问
控制列表
#
interface Ethernet2/0
 speed 10
 duplex half
 promiscuous
#
interface NULL0
#
interface LoopBack0
 ip address 192.168.1.254 255.255.255.0
#
firewall zone local
 set priority 100
#
firewall zone trust
 add interface Ethernet1/0
 set priority 85
#
firewall zone untrust
 set priority 5
#
firewall zone DMZ
 add interface Ethernet2/0
 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 smurf                                //开启smurf攻击防范

 firewall defend arp-flood                            //开启arp-flood攻击防
范
#
user-interface con 0
user-interface vty 0 4
 authentication-mode scheme
#
return
```

四、配置关键点

1．透明模式下主要配置见上面蓝色字体部分。