SecPath防火墙aspf典型配置

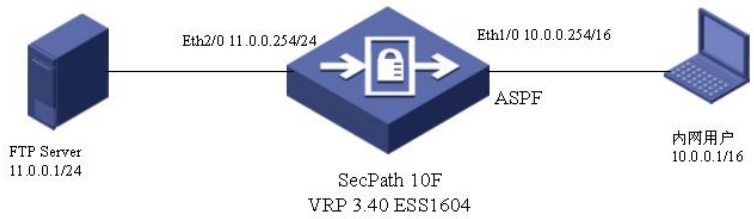
巫继雨 2006-09-25 发表

SecPath防火墙aspf典型配置

一、组网需求

在防火墙上配置一ASPF策略，检测通过防火墙的FTP流量。实现：内部网络用户发起的FTP连接的返回报文，则允许其通过防火墙进入内部网络，其他报文被禁止。

二、组网图



三、配置步骤

```
[DOWN] dis cur
#
 sysname DOWN
#
 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
#
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
#
// 创建ASPF策略，策略号为1，该策略检测应用层的FTP协议，并定义没有任何行为的情况下，FTP协议的超时时间为3000秒。
aspf-policy 1
 detect ftp aging-time 3000
 detect udp
 detect tcp
#
//配置访问控制列表3111，以拒绝所有TCP和UDP流量进入内部网络，ASPF会为允许通过的流量创建临时的访问控制列表。

acl number 3000
 rule 0 deny tcp
 rule 1 deny udp
 rule 2 deny ip
#
interface Ethernet1/0
 ip address 10.0.0.254 255.255.0.0
 //在接口上应用访问控制列表3000
firewall packet-filter 3000 outbound
 //在接口上应用ASPF策略
```

```
firewall aspf 1 inbound
#
interface Ethernet2/0
 speed 10
 duplex full
 ip address 11.0.0.254 255.255.255.0
#
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
 set priority 5
#
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
#
user-interface con 0
user-interface vty 0 4
 authentication-mode scheme
#
return
```

四、配置关键点

1．配置访问控制列表；

2．创建aspf策略；

3．在接口上应用aspf策略。

五、验证结果

在内网10.0.0.1上ping FTP服务器，发现无法ping通；在10.0.0.1上ftp 11.0.0.1，正常。在SecPath10F上查看aspf session，如下：

```
[DOWN]dis aspf session

There is 1 ASPF session:
[Established Sessions]
Session      Initiator        Responder      Application       Status
-----------------------------------------------------------------------------------------------
2A836E4    10.0.0.1:1065    11.0.0.1:21        ftp         FTP_CONXN_UP
```