SecPath1800F ACL 的配置

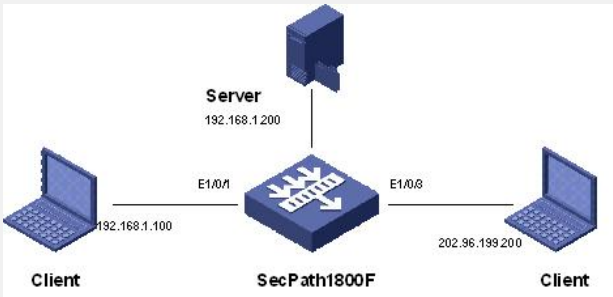
王刚 2006-11-01 发表

SecPath1800F ACL的配置

一、 组网需求：

ACL是防火墙做数据过滤及功能实现的基础。根据用户环境的不同，需要配置不同的ACL满足用户的需求。

二、 组网图：



三、 配置步骤：

适用版本： 适合当前所有防火墙 VRP 版本

```
#
acl number 2001              // 配置基本访问控制列表（只能指定源，目的为any）
 rule 0 permit source 192.168.1.0 0.0.0.255
#
acl number 3001              // 配置扩展的访问控制列表（可以指定目地）
 rule 0 permit ip source 192.168.1.0 0.0.0.255 destination 202.96.199.0 0.0.0.255
acl number 3002              // 配置扩展的访问控制列表
 rule 0 permit ip source 202.96.199.0 0.0.0.255 destination 192.168.1.200 0
#
acl number 5001              // 配置防火墙访问控制列表（该列表不能按照网段指定）
 rule 0 permit tcp source 192.168.1.100 0 destination 202.96.199.100 0 destinatio
n-port eq www
#
 sysname SecPath
#
 nat server global 202.96.199.200 inside 192.168.1.200  // 配置映射服务器
#
 bypass switch-back auto
#
 firewall mode route
#
 firewall statistic system enable
#
interface Aux0
 async mode flow
 link-protocol ppp
#
interface Ethernet0/0/0
#
interface Ethernet0/0/1
#
interface Ethernet1/0/0
#
interface Ethernet1/0/1                  // 设置端口信息
```

```
 ip address 192.168.1.254 255.255.255.0
#
interface Ethernet1/0/2
#
interface Ethernet1/0/3                    // 设置端口信息
 ip address 202.96.199.254 255.255.255.0
#
interface Ethernet1/0/4
#
interface Ethernet1/0/5
#
interface Ethernet1/0/6
#
interface Ethernet1/0/7
#
interface NULL0
#
firewall zone local
 set priority 100
#
firewall zone trust
 set priority 85
 add interface Ethernet1/0/1
#
firewall zone untrust
 set priority 5
 add interface Ethernet1/0/3
#
firewall zone dmz
 set priority 50
#
firewall interzone local trust
#
firewall interzone local untrust
#
firewall interzone local dmz
#
firewall interzone trust untrust                    // 在域间做绑定
 packet-filter 3002 inbound
 packet-filter 3001 outbound
 packet-filter 5001 outbound
#
firewall interzone trust dmz
#
firewall interzone dmz untrust
#
aaa
 authentication-scheme default
#
 authorization-scheme default
#
 accounting-scheme default
#
 domain default
#
#
user-interface con 0
user-interface aux 0
user-interface vty 0 4
#
return
```

四、 配置关键点：

> SecPath1800F的ACl分为基本、高级、防火墙级别，ACL除与防火墙的报文过滤直接相关还有匹配数据流的功能。根据不同的需求要配置不同的ACL。其中基本ACL、高级ACL不能同时在域间的同一个方向上使用，防火墙ACL可以在同时与基本ACL、高级ACL在域间同一个方向上使用。