Secpath1800F策略路由功能的配置

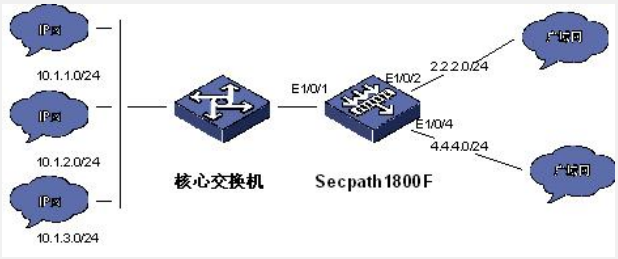
王刚 2006-09-03 发表

Secpath1800F策略路由功能的配置

一、 组网需求：

当防火墙有双公网出口时，根据用户的源地址或者需要访问目的地址来选择防火墙的转发出口，从而实现路由选择。

二、 组网图：



三、 配置步骤：

适用版本：Secpath1800F 所有VRP版本

```
acl number 2001
 rule 0 permit source 10.1.0.0 0.0.255.255
#
acl number 3001                          // 定义与策略路由相关的 acl
 rule 0 deny ip source 10.1.1.0 0.0.0.255    // 10.1.1.0 网段不作策略路由
 rule 5 permit ip source 10.1.2.0 0.0.0.255  // 源地址为10.1.2.0 的网段做策略路由
 rule 10 permit ip destination 202.96.199.0 0.0.0.255
                                          // 目的地址为202.96.199.0 的网段做策略路由
#
 sysname Eudemon
#
 firewall packet-filter default permit interzone local trust direction inbound
 firewall packet-filter default permit interzone local trust direction outbound
 firewall packet-filter default permit interzone local untrust direction inbound
 firewall packet-filter default permit interzone local untrust direction outboun
d
 firewall packet-filter default permit interzone local dmz direction inbound
 firewall packet-filter default permit interzone local dmz direction outbound
 firewall packet-filter default permit interzone local test direction inbound
 firewall packet-filter default permit interzone local test direction outbound
 firewall packet-filter default permit interzone trust untrust direction inbound
 firewall packet-filter default permit interzone trust untrust direction outboun
d
 firewall packet-filter default permit interzone trust dmz direction inbound
 firewall packet-filter default permit interzone trust dmz direction outbound
 firewall packet-filter default permit interzone trust test direction inbound
 firewall packet-filter default permit interzone trust test direction outbound
 firewall packet-filter default permit interzone dmz untrust direction inbound
 firewall packet-filter default permit interzone dmz untrust direction outbound
 firewall packet-filter default permit interzone test untrust direction inbound
 firewall packet-filter default permit interzone test untrust direction outbound
 firewall packet-filter default permit interzone test dmz direction inbound
 firewall packet-filter default permit interzone test dmz direction outbound
```

```
#
 nat address-group 2 2.2.2.10 2.2.2.10
 nat address-group 4 4.4.4.10 4.4.4.10
#
 firewall mode route
#
 firewall statistic system enable
#
traffic classifier test                  // 定义traffic 名字 及感兴趣数据流
  if-match acl 3001
#
traffic behavior test_do                 // 定义策略路由的转发出口及地址
  remark ip-nexthop 4.4.4.2 output-interface Ethernet1/0/4
                                         // 地址 4.4.4.2 为相应的网关地址
#
qos policy po_ro                         // 定义相应的策略路由组
 classifier test behavior test_do
#
interface Aux0
 async mode flow
 link-protocol ppp
#
interface Ethernet0/0/0
#
interface Ethernet0/0/1
#
interface Ethernet1/0/0
#
interface Ethernet1/0/1
 ip address 192.168.1.254 255.255.255.0
#
interface Ethernet1/0/2
 ip address 2.2.2.1 255.255.255.0
#
interface Ethernet1/0/3
#
interface Ethernet1/0/4
 ip address 4.4.4.1 255.255.255.0
#
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
 qos apply policy po_ro outbound        // 在相应的域上绑定策略路由
 add interface Ethernet1/0/1
#
firewall zone untrust
 set priority 5
 add interface Ethernet1/0/2
#
firewall zone dmz
 set priority 50
#
firewall zone name test
 set priority 75
```

```
 add interface Ethernet1/0/4
#
firewall interzone local trust
#
firewall interzone local untrust
#
firewall interzone local dmz
#
firewall interzone local test
#
firewall interzone trust untrust
 nat outbound 2001 address-group 2
#
firewall interzone trust dmz
#
firewall interzone trust test
 nat outbound 2001 address-group 4
#
firewall interzone dmz untrust
#
firewall interzone test untrust
#
firewall interzone test dmz
#
aaa
 authentication-scheme default
#
 authorization-scheme default
#
 accounting-scheme default
#
 domain default
#
#
 ip route-static 0.0.0.0 0.0.0.0 2.2.2.2          // 定义默认路由
 ip route-static 10.1.0.0 255.255.0.0 192.168.1.133
#
user-interface con 0
user-interface aux 0
user-interface vty 0 4
```

四、 配置关键点：

配置策略路由时，主要要打开做相应的策略路由的域之间的规则。特别要注意的是，对于Version 3.30 Release 0336 以前的版本，存在策略路由根据默认路由域之间的规则来决定是否允许转发的问题。