

SecPath1800F ASPF功能的配置

一、组网需求:

ASPF是应用级网关, 与其他SecPath产品不同, SecPath1800F NAT转换时不会自动打开相应的ASPF功能, 需要在域间手动打开相应的功能。

二、组网图



三、配置步骤:

适用版本: SecPath1800F 3.30 0336 (不包括该版本) 以后所有版本

```
#
acl number 2000           // 设置acl
rule 0 permit source 192.168.1.0 0.0.0.255
#
sysname SecPath
#
// 设置域间规则
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 outbound
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 trust untrust direction inbound
firewall packet-filter default permit interzone trust untrust direction outbound
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 dmz untrust direction inbound
firewall packet-filter default permit interzone dmz untrust direction outbound
#
nat address-group 10 202.96.199.100 202.96.199.110
nat server protocol tcp global 202.96.199.200 ftp inside 192.168.1.200 ftp
// 设置服务映射
#
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
ip address 192.168.1.254 255.255.255.0
#
interface Ethernet1/0/2
#
interface Ethernet1/0/3
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
nat outbound 2000 address-group 10
detect ftp // 在域间做相应的detect功能
#
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:

在域间的可以做多种数据类型的detect的检测。