SecPath1800F虚拟防火墙基本配置（二）

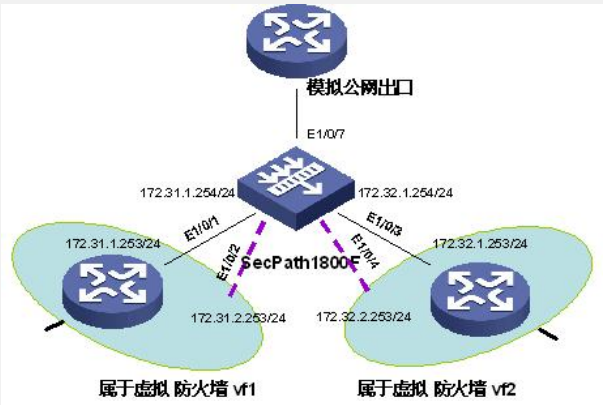
王刚　2007-01-09 发表

SecPath1800F虚拟防火墙功基本配置（二）

一、 组网需求：

SecPath1800F通过不同公网地址映射内部不同虚拟防火墙内的相同私网地址的服务器。

二、 组网图：



三、 配置步骤：

适用版本： SecPath1800F 虚拟防火墙版本

```
#
 ip vpn-instance vf1 vpn-id 1
  route-distinguisher 100:1
#
 ip vpn-instance vf2 vpn-id 2
  route-distinguisher 100:2
#
acl number 2001
 rule 0 permit
acl number 2005  vpn-instance vf1
 rule 0 permit
acl number 2006  vpn-instance vf2
 rule 0 permit
#
 sysname Eudemon
#
 hrp enable
 hrp interface Ethernet1/0/7
#
 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 local vzone direction inbound
 firewall packet-filter default permit interzone local vzone 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 trust vzone direction inbound
```

```
 firewall packet-filter default permit interzone trust vzone 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 untrust vzone direction inbound
 firewall packet-filter default permit interzone untrust vzone direction outbound
 firewall packet-filter default permit interzone dmz vzone direction inbound
 firewall packet-filter default permit interzone dmz vzone direction outbound
 firewall packet-filter default permit interzone vpn-instance vf1 local trust direction inb
ound
 firewall packet-filter default permit interzone vpn-instance vf1 local trust direction out
bound
 firewall packet-filter default permit interzone vpn-instance vf1 local untrust direction i
nbound
 firewall packet-filter default permit interzone vpn-instance vf1 local untrust direction o
utbound
 firewall packet-filter default permit interzone vpn-instance vf1 local dmz direction inb
ound
 firewall packet-filter default permit interzone vpn-instance vf1 local dmz direction out
bound
 firewall packet-filter default permit interzone vpn-instance vf1 local vzone direction in
bound
 firewall packet-filter default permit interzone vpn-instance vf1 local vzone direction o
utbound
 firewall packet-filter default permit interzone vpn-instance vf1 trust untrust direction i
nbound
 firewall packet-filter default permit interzone vpn-instance vf1 trust untrust direction o
utbound
 firewall packet-filter default permit interzone vpn-instance vf1 trust dmz direction inbo
und
 firewall packet-filter default permit interzone vpn-instance vf1 trust dmz direction
outbound
 firewall packet-filter default permit interzone vpn-instance vf1 trust vzone direction in
bound
 firewall packet-filter default permit interzone vpn-instance vf1 trust vzone direction
outbound
 firewall packet-filter default permit interzone vpn-instance vf1 dmz untrust direction
inbound
 firewall packet-filter default permit interzone vpn-instance vf1 dmz untrust direction o
utbound
 firewall packet-filter default permit interzone vpn-instance vf1 untrust vzone direction
inbound
 firewall packet-filter default permit interzone vpn-instance vf1 untrust vzone direction
outbound
 firewall packet-filter default permit interzone vpn-instance vf1 dmz vzone direction in
bound
 firewall packet-filter default permit interzone vpn-instance vf1 dmz vzone direction ou
tbound
 firewall packet-filter default permit interzone vpn-instance vf2 local trust direction inb
ound
 firewall packet-filter default permit interzone vpn-instance vf2 local trust direction out
bound
 firewall packet-filter default permit interzone vpn-instance vf2 local untrust direction i
nbound
 firewall packet-filter default permit interzone vpn-instance vf2 local untrust direction o
utbound
 firewall packet-filter default permit interzone vpn-instance vf2 local dmz direction inb
ound
 firewall packet-filter default permit interzone vpn-instance vf2 local dmz direction out
bound
 firewall packet-filter default permit interzone vpn-instance vf2 local vzone direction in
bound
 firewall packet-filter default permit interzone vpn-instance vf2 local vzone direction o
utbound
 firewall packet-filter default permit interzone vpn-instance vf2 trust untrust direction i
```

```
nbound
 firewall packet-filter default permit interzone vpn-instance vf2 trust untrust direction o
utbound
 firewall packet-filter default permit interzone vpn-instance vf2 trust dmz direction inbo
und
 firewall packet-filter default permit interzone vpn-instance vf2 trust dmz direction
outbound
 firewall packet-filter default permit interzone vpn-instance vf2 trust vzone direction in
bound
 firewall packet-filter default permit interzone vpn-instance vf2 trust vzone direction
outbound
 firewall packet-filter default permit interzone vpn-instance vf2 dmz untrust direction
inbound
 firewall packet-filter default permit interzone vpn-instance vf2 dmz untrust direction o
utbound
 firewall packet-filter default permit interzone vpn-instance vf2 untrust vzone direction
inbound
 firewall packet-filter default permit interzone vpn-instance vf2 untrust vzone direction
outbound
 firewall packet-filter default permit interzone vpn-instance vf2 dmz vzone direction in
bound
 firewall packet-filter default permit interzone vpn-instance vf2 dmz vzone direction ou
tbound
#
 nat address-group 123 vf1 172.16.1.8 172.16.1.8 vpn-instance vf1
 nat address-group 124  172.16.1.20 172.16.1.20
 nat address-group 125  172.16.1.21 172.16.1.21 vpn-instance vf2
 nat server  global 172.16.1.202 inside 172.31.1.200 vpn-instance vf1  //配置映射
关系
 nat server  global 172.16.1.203 inside 172.31.1.200 vpn-instance vf2  //配置映射
关系
#
#
 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 binding vpn-instance vf1
 ip address 172.31.1.253 255.255.255.0
#
interface Ethernet1/0/2
#
interface Ethernet1/0/3
 ip binding vpn-instance vf2
 ip address 172.31.1.253 255.255.255.0
#
interface Ethernet1/0/4
#
interface Ethernet1/0/5
#
interface Ethernet1/0/6
 ip address 7.7.7.7 255.255.255.0
#
interface Ethernet1/0/7
 ip address 172.16.1.1 255.255.255.0
```

```
 vrrp vrid 100 virtual-ip 172.16.1.101
 vrrp vrid 200 virtual-ip 172.16.1.102
 vrrp vrid 200 priority 102
#
interface NULL0
#
firewall zone local
 set priority 100
#
firewall zone trust
 set priority 85
 add interface Ethernet1/0/5
#
firewall zone untrust
 set priority 5
 add interface Ethernet1/0/7
#
firewall zone dmz
 set priority 50
#
firewall zone vzone
 set priority 0
#
firewall zone vpn-instance vf1 local
 set priority 100
#
firewall zone vpn-instance vf1 trust
 set priority 85
 add interface Ethernet1/0/1
#
firewall zone vpn-instance vf1 untrust
 set priority 5
 add interface Ethernet1/0/2
#
firewall zone vpn-instance vf1 dmz
 set priority 50
#
firewall zone vpn-instance vf1 vzone
 set priority 0
#
firewall zone vpn-instance vf2 local
 set priority 100
#
firewall zone vpn-instance vf2 trust
 set priority 85
 add interface Ethernet1/0/3
#
firewall zone vpn-instance vf2 untrust
 set priority 5
#
firewall zone vpn-instance vf2 dmz
 set priority 50
#
firewall zone vpn-instance vf2 vzone
 set priority 0
#
firewall interzone vpn-instance vf1 trust vzone     // 配置域间的地址转换
 nat outbound 2005 address-group vf1
#
firewall interzone vpn-instance vf2 trust vzone     // 配置域间的地址转换
 nat outbound 2006 address-group 125
 detect ftp
#
vrrp group 1
```

```
 add interface Ethernet1/0/7 vrrp vrid 100 data
 vrrp-group enable
 vrrp-group priority 102
 vrrp-group preempt delay 0
 undo vrrp-group group-send
vrrp group 2
 add interface Ethernet1/0/7 vrrp vrid 200 data
 vrrp-group enable
 vrrp-group preempt delay 0
 undo vrrp-group group-send
#
aaa
 authentication-scheme default
#
 authorization-scheme default
#
 accounting-scheme default
#
 domain default
#
#
 slb
#
 ip route-static vpn-instance vf1 0.0.0.0 0.0.0.0 Ethernet1/0/7   // 配置默认路由
 ip route-static vpn-instance vf2 0.0.0.0 0.0.0.0 Ethernet1/0/7   // 配置默认路由
#
user-interface con 0
user-interface aux 0
user-interface vty 0 4
#
return
```

四、 配置关键点：

注意路由的配置，当有下一跳时，除指定接口外还要指定下一跳的地址。