SecPath防火墙双机热备+NAT Server的典型配置

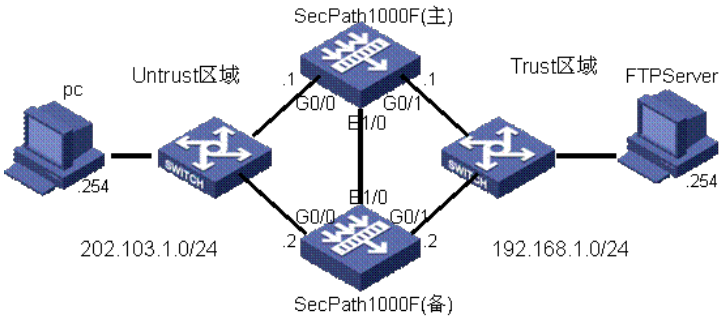
万欣　2008-07-04 发表

SecPath防火墙双机热备+NAT Server的典型配置

一、 组网需求：

SecPath防火墙在主备切换的情况下不影响pc从FTPServer上下载数据。

二、 组网图



SecPath1000F：版本为Version 3.40, ESS 1622;

FTP Server：Windows XP操作系统;

PC：Windows XP操作系统.

三、 配置步骤

1. SecPath1000F（主）的主要配置：

```
#
 sysname fw1
#
 firewall packet-filter enable
 firewall packet-filter default permit
#
interface Ethernet1/0
#
interface GigabitEthernet0/0
 ip address 202.103.1.1 255.255.255.0
 nat server protocol tcp global 202.103.1.88 any inside 192.168.1.254 any     //FTP服务器的地址映射
#
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
#
firewall zone trust
 add interface GigabitEthernet0/1
 set priority 85
#
firewall zone untrust
 add interface GigabitEthernet0/0
 set priority 5
#
firewall zone DMZ   //心跳线接口也同样需要加入某一域
 add interface Ethernet1/0
 set priority 50
#
rdo 1
 priority 105
 ha-interface interface Ethernet1/0 peer-mac ffff-ffff-ffff   //斜体部分为系统自动生成，不用配置，下同
 vif 1 interface GigabitEthernet0/1 virtual-ip 192.168.1.100 virtual-mac 005e-0000-1101 reduce 10
 vif 2 interface GigabitEthernet0/0 virtual-ip 202.103.1.100 virtual-mac 005e-0000-1102 reduce 10
#
```

2. SecPath1000F（备）的主要配置：

```
#
```

```
 sysname fw2
#
 firewall packet-filter enable
 firewall packet-filter default permit
#
interface Ethernet1/0
#
interface GigabitEthernet0/0
 ip address 202.103.1.2 255.255.255.0
 nat server protocol tcp global 202.103.1.88 any inside 192.168.1.254 any
#
interface GigabitEthernet0/1
 ip address 192.168.1.2 255.255.255.0
#
firewall zone local
 set priority 100
#
firewall zone trust
 add interface GigabitEthernet0/1
 set priority 85
#
firewall zone untrust
 add interface GigabitEthernet0/0
 set priority 5
#
firewall zone DMZ
 add interface Ethernet1/0
 set priority 50
#
rdo 1
 ha-interface interface Ethernet1/0 peer-mac ffff-ffff-ffff
 vif 1 interface GigabitEthernet0/1 virtual-ip 192.168.1.100 virtual-mac 005e-0000-1101 reduce 10
 vif 2 interface GigabitEthernet0/0 virtual-ip 202.103.1.100 virtual-mac 005e-0000-1102 reduce 10
#
```

3．验证结果：

当PC从FTP服务器上下载数据的同时，切断主防火墙上的某一接口，使备防火墙变成主，此时观察到下载不会受到影响。

四、 配置关键点

1. 心跳线接口也必须加入到某一域上；
2. 主防火墙上的rdo的优先级要高于备（默认rdo优先级为100）；
3. NAT Server做在出接口上；
4．PC和服务器的网关应该指向虚地址（virtual-ip）