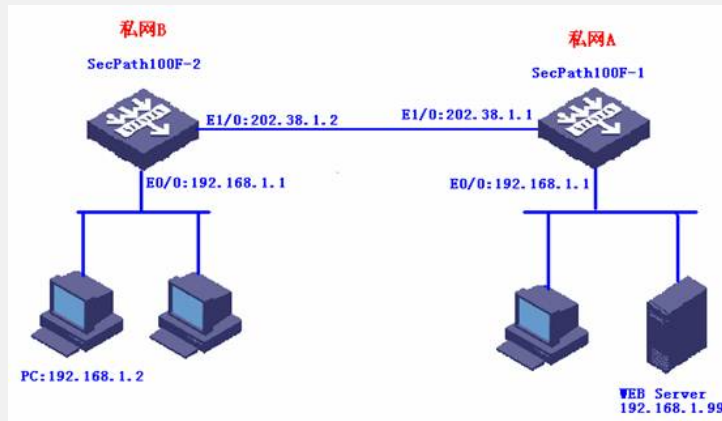


SecPath防火墙静态网段地址转换的典型配置

一、组网需求:

在私网A和私网B的IP地址重复的情况下, 私网B需要访问私网A内的服务器。

二、组网图



SecPath100F: 版本为Version 3.40, ESS 1604P01

三、配置步骤

1. SecPath100F-1的主要配置

配置防火墙默认规则

```
firewall packet-filter enable  
firewall packet-filter default permit
```

配置网段地址静态转换

```
nat static inside ip 192.168.1.1 192.168.1.254 global ip 172.16.1.0 255.255.255.0
```

配置内网口

```
interface Ethernet0/0  
ip address 192.168.1.1 255.255.255.0
```

配置外网口

```
interface Ethernet1/0  
ip address 202.38.1.1 255.255.255.0  
nat outbound static
```

配置区域

```
firewall zone trust  
add interface Ethernet0/0  
firewall zone untrust  
add interface Ethernet1/0  
set priority 5
```

配置路由

```
ip route-static 172.16.2.0 255.255.255.0 202.38.1.2
```

2. SecPath100F-2的主要配置

配置防火墙默认规则

```
firewall packet-filter enable  
firewall packet-filter default permit
```

配置网段地址静态转换

```
nat static inside ip 192.168.1.1 192.168.1.254 global ip 172.16.2.0 255.255.255.0
```

配置内网口

```
interface Ethernet0/0  
ip address 192.168.1.1 255.255.255.0
```

配置外网口

```
interface Ethernet1/0  
ip address 202.38.1.2 255.255.255.0  
nat outbound static
```

配置区域

firewall zone trust

add interface Ethernet0/0

set priority 85

firewall zone untrust

add interface Ethernet1/0

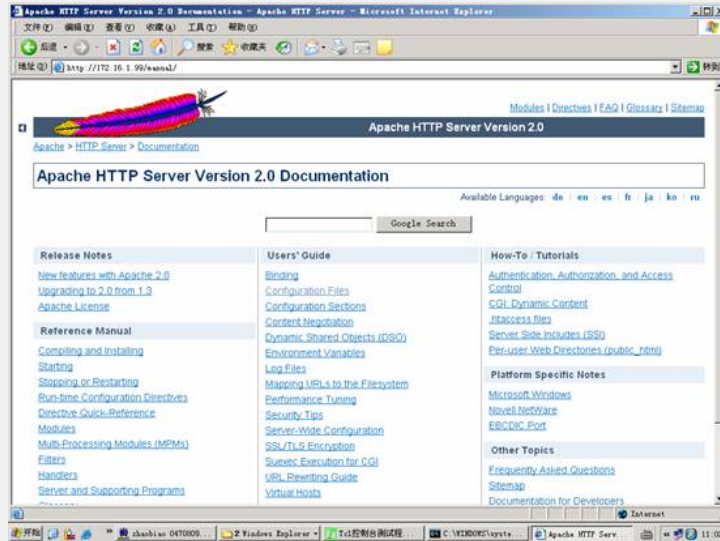
set priority 5

配置路由

ip route-static 172.16.1.0 255.255.255.0 202.38.1.1

3. PC端的验证结果

在私网B中PC的IE中输入：<http://172.16.1.99>就能访问私网A中的WEB服务器



四、配置关键点

1. VRP3.4-1210P01版本以前的静态地址段转换的命令为nat static net-to-net;
2. 保证有到17.16.1.0/24和172.16.2.0/24的路由;
3. 由于做了net static net-to-net, 访问对端私网地址不再是192.168.1.X/24, 而是172.16.1.X/24或172.16.2.X/24, 最后一位地址不变。