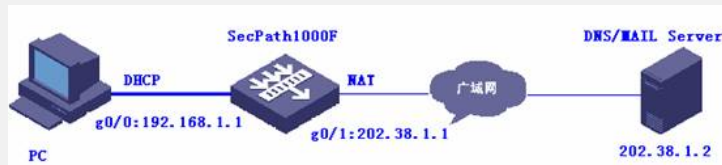


SecPath防火墙邮件收件人过滤的典型组网

一、组网需求:

阻止某些内部员工给内部或外部特定收件人发送垃圾邮件和恶意邮件。

二、组网图



SecPath1000F: 版本为Version 3.40, ESS 1604P01;

DNS/MAIL Server: Windows 2003操作系统;

PC: Windows XP操作系统, DHCP客户端。

三、配置步骤

1. SecPath1000F的主要配置

```
#
sysname Quidway
#
firewall packet-filter enable
firewall packet-filter default permit
#
firewall smtp-filter rcptto enable //启用邮件收件人过滤功能
firewall smtp-filter rcptto load-file flash:/mail-rcptto //指定加载位置和文件
#
aspf-policy 1 //配置aspf策略
detect smtp //对smtp进行检测
detect tcp
detect udp
#
dhcp server ip-pool test //创建DHCP地址池, 定义属性值
network 192.168.1.0 mask 255.255.255.0
gateway-list 192.168.1.1
dns-list 202.38.1.2
domain-name h3c.com
#
acl number 3000 //创建NAT转换的ACL
rule 0 permit ip source 192.168.1.0 0.0.0.255
rule 1 deny ip
#
interface GigabitEthernet0/0
ip address 192.168.1.1 255.255.255.0
dhcp select interface //在接口下启用DHCP
dhcp server dns-list 202.38.1.2 //定义DHCP Server分配的DNS
#
interface GigabitEthernet0/1
ip address 202.38.1.1 255.255.255.0
firewall aspf 1 outbound //接口的出方向应用aspf
nat outbound 3000 //配置nat outbound
#
firewall zone trust
add interface GigabitEthernet0/0
set priority 85
#
firewall zone untrust
add interface GigabitEthernet0/1
set priority 5
```

```

#
ip route-static 0.0.0.0 0.0.0.0 202.38.1.2 //配置默认路由
#
[Quidway]firewall smtp-filter rcptto add deny admin@h3c.com //添加关键字
<Quidway>dis firewall smtp-filter rcptto item-all //显示邮件收件人过滤条目

Firewall smtp-filter rcptto items
item(s) added manually : 1
item(s) loaded from file : 0

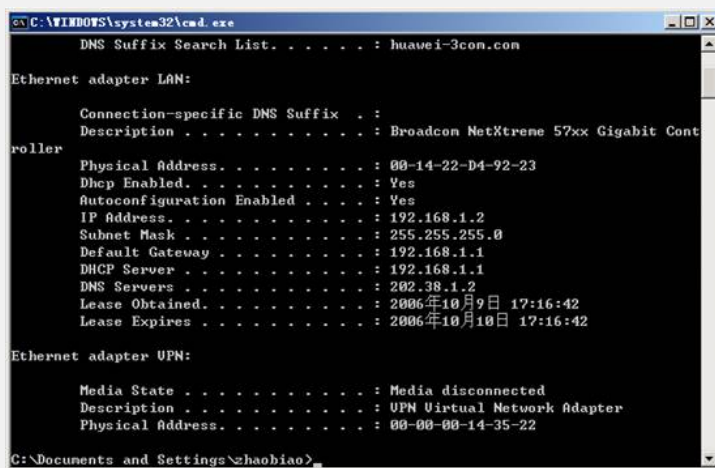
SN Match-Times Keyword
-----
1 1 <deny>admin@h3c.com
<Quidway>dir
Directory of flash:/

1 -rw- 8576044 Sep 30 2006 08:57:31 system
2 -rw- 1021629 Sep 27 2006 10:26:51 http.zip
3 -rw- 1735 Oct 09 2006 17:18:35 config.cfg
4 -rw- 4 Sep 28 2006 21:27:48 snmpboots
5 -rw- 29 Oct 09 2006 20:58:30 mail-rcptto //在flash中保存mail-rcptto
<Quidway>more mail-rcptto //显示“mail-rcptto”文件内容
<deny>admin@h3c.com

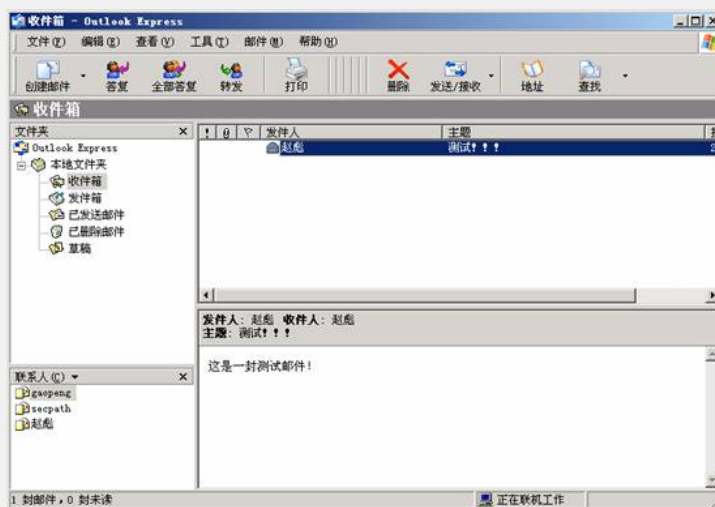
```

2. PC的验证结果

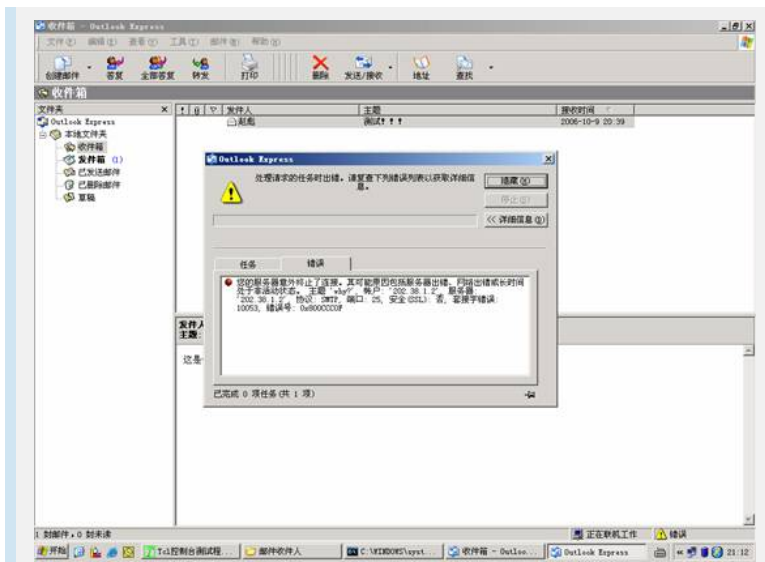
显示自动获取的IP地址:



未配置邮件收件人过滤时，通过客户端OE发送邮件:



配置邮件收件人过滤后，通过客户端OE发送邮件:



四、配置关键点

1. 添加完关键字后，如果重启设备，配置的关键字会丢失，需要通过firewall smtp-filter rcptto save-file mail-rcptto命令保存关键字到flash中；此外，如果重启设备后，还需要重新加载已经保存在flash中的文件，可以通过firewall smtp-filter rcptto load-file mail-rcpttot命令自动加载；
2. 可以通过Tftp程序把mail-rcptto文件下载到本地，修改完成后再上传到flash中。