SecPath防火墙webdata-filter典型组网

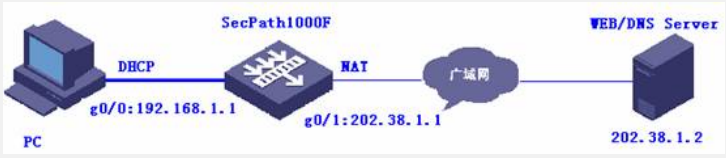
赵彪 2006-10-10 发表

SecPath防火墙webdata-filter典型组网

一、 组网需求：

某公司想限制访问带有某些关键字的网站。

二、 组网图



SecPath1000F：版本为Version 3.40, ESS 1604P01；

WEB/DNS 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 webdata-filter enable    //启用webdata-filter
 firewall webdata-filter load-file flash:/webdata    //指定保存的文件和位置
#
aspf-policy 1     //配置aspf
 detect http      //对http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
```

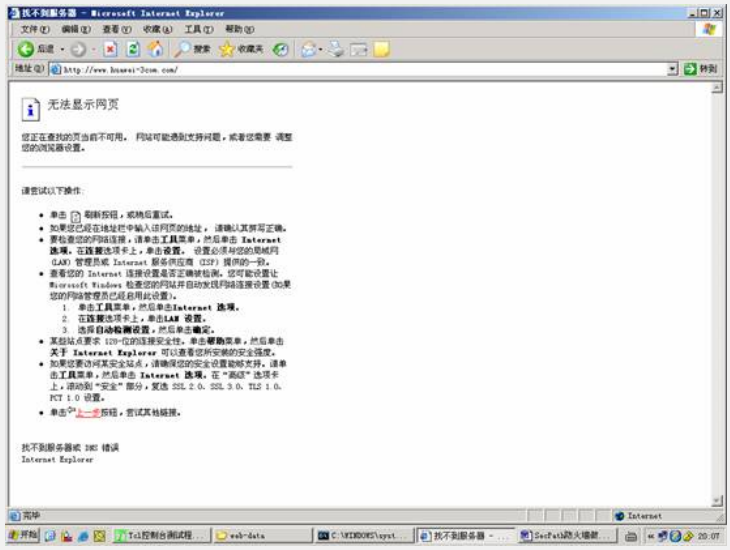
```
#
 ip route-static 0.0.0.0 0.0.0.0 202.38.1.2    //配置默认路由
#
[Quidway]firewall webdata-filter add apache       //添加webdata-filter关键字
      [Quidway]dis firewall webdata-filter item-all         //显示webdata-filter关键字
       Firewall webdata-filter items
         item(s) added manually :   1
         item(s) loaded from file : 0
       SN  Match-Times  Keywords
            -----------------------------------------------
            1          0    apache
<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-        27  Oct 09 2006 17:12:44   webdata    //在flash中保存webdata
<Quidway> more webdata          //显示“webdata”文件内容
apache
```

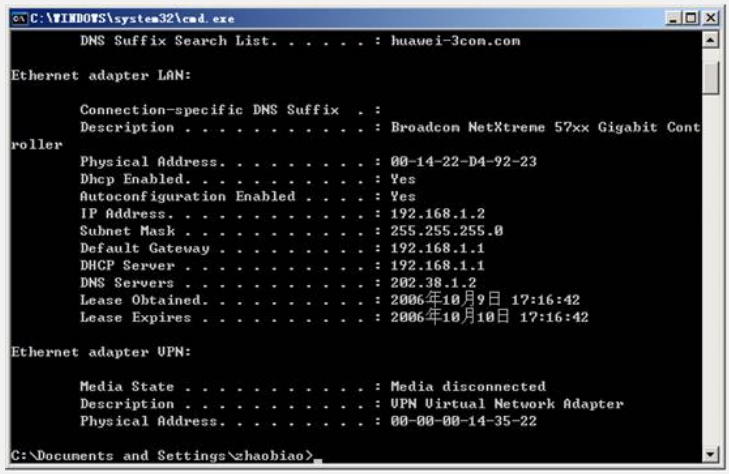
2.　　PC的验证结果

显示自动获取的IP地址：

未启用webdata-filte时，访问Web服务器：



启用webdata-filte后，不能访问Web服务器：



四、 配置关键点

1. 可以通过Tftp程序把*webdata*文件下载到本地，修改完成后再上传到flash中；
2. 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 webdata-filter save-file *webdata*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 webdata-filter load-file *webdata*命令自动加载。