SecPath防火墙通过ASPF实现单向访问的典型配置

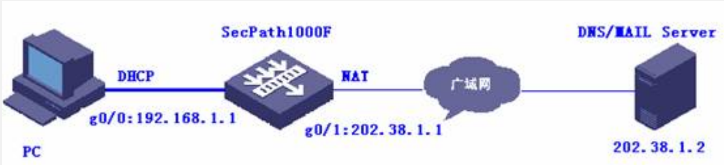
赵彪 2006-10-10 发表

SecPath防火墙通过ASPF实现单向访问的典型配置

一、 组网需求:

实现Trust区域可以访问Untrust区域，但是Untrust区域不可以访问Trust区域。

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。

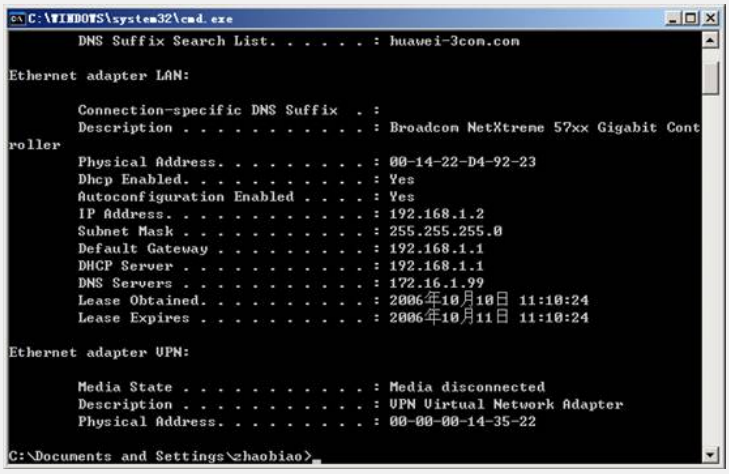
三、 配置步骤

1. SecPath1000F的主要配置

```
#
 sysname Quidway
#
 firewall packet-filter enable
 firewall packet-filter default permit
#
aspf-policy 1      //配置aspf策略
 detect http       //对http协议进行检测
 detect smtp       //对smtp协议进行检测
 detect ftp        //对ftp协议进行检测
 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 172.16.1.99
 domain-name h3c.com
#
acl number 3000   //创建ACL
 rule 0 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 172.16.1.99    //定义DHCP Server分配的DNS
#
interface GigabitEthernet0/1
 ip address 172.16.1.1 255.255.255.0
 firewall packet-filter 3000 inbound    //接口入方向应用ACL，拒绝所有进来的报文
 firewall aspf 1 outbound            //接口出方向应用aspf
#
firewall zone trust
 add interface GigabitEthernet0/0
 set priority 85
#
firewall zone untrust
 add interface GigabitEthernet0/1
 set priority 5
#
```

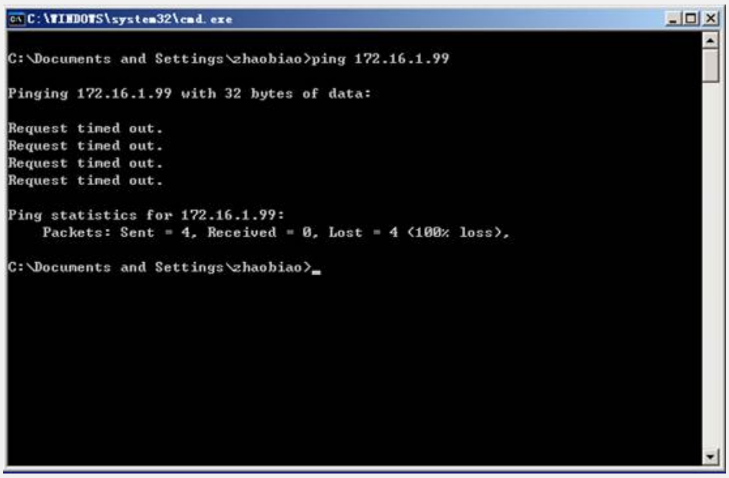
2. PC的验证结果

显示自动获取的IP地址：



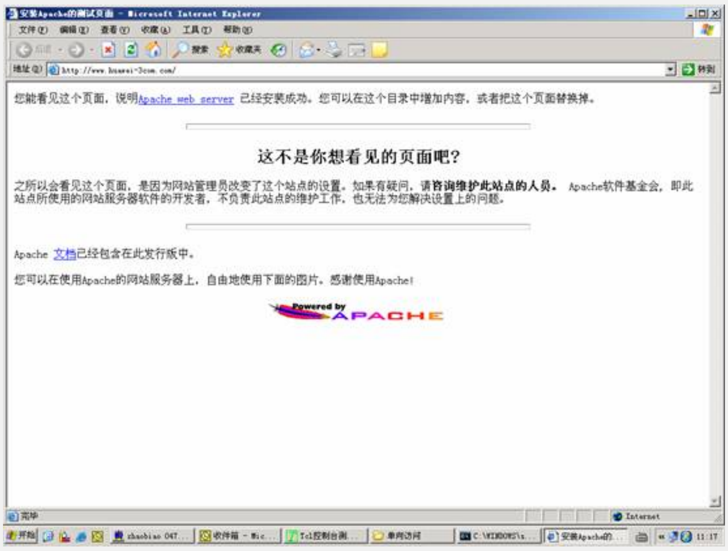
```
        DNS Suffix Search List. . . . . . : huawei-3com.com

Ethernet adapter LAN:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : Broadcom NetXtreme 57xx Gigabit Cont
roller
        Physical Address. . . . . . . . . : 00-14-22-D4-92-23
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 192.168.1.2
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1
        DHCP Server . . . . . . . . . . . : 192.168.1.1
        DNS Servers . . . . . . . . . . . : 172.16.1.99
        Lease Obtained. . . . . . . . . . : 2006年10月10日 11:10:24
        Lease Expires . . . . . . . . . . : 2006年10月11日 11:10:24

Ethernet adapter VPN:

        Media State . . . . . . . . . . . : Media disconnected
        Description . . . . . . . . . . . : VPN Virtual Network Adapter
        Physical Address. . . . . . . . . : 00-00-00-14-35-22

C:\Documents and Settings\zhaobiao>_
```

Ping Web服务器：



```
C:\Documents and Settings\zhaobiao>ping 172.16.1.99

Pinging 172.16.1.99 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.16.1.99:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Documents and Settings\zhaobiao>_
```

访问Web服务器：


安装Apache的测试页面 - Microsoft Internet Explorer
文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)
后退
搜索
收藏夹
地址(D)
转到
完毕
Internet
开始
11:17

http://www.huawei-3com.com/

您能看见这个页面，说明Apache web server 已经安装成功。您可以在这个目录中增加内容，或者把这个页面替换掉。

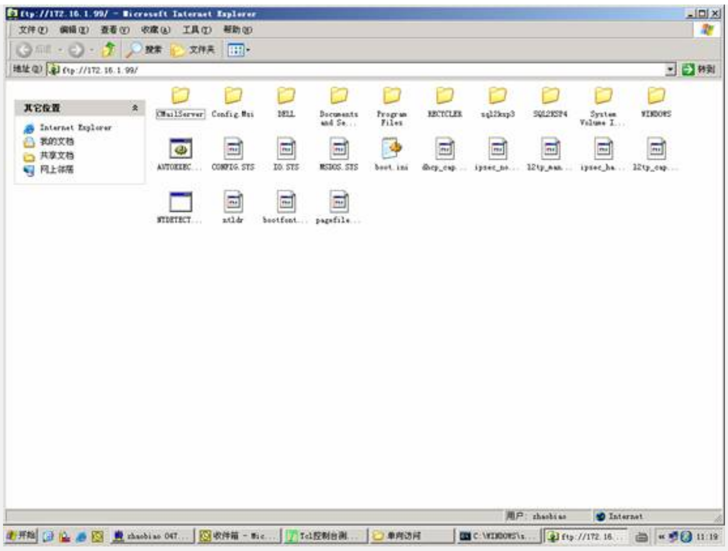
这不是你想看见的页面吧?

之所以会看见这个页面，是因为网站管理员改变了这个站点的设置。如果有疑问，请**咨询维护此站点的人员。** Apache软件基金会，即此站点所使用的网站服务器软件的开发者，不负责此站点的维护工作，也无法为您解决设置上的问题。

Apache 文档已经包含在此发行版中。

您可以在使用Apache的网站服务器上，自由地使用下面的图片。感谢使用Apache!

访问Ftp服务器：


ftp://172.16.1.99/ - Microsoft Internet Explorer
文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)
后退 搜索 文件夹
地址(D) ftp://172.16.1.99/
转到
其它位置
Internet Explorer
我的文档
共享文档
网上邻居
CMailServer
Config.Msi
DELL
Documents and Se...
Program Files
RECYCLER
sql2ksp3
SQL2KSP4
System Volume I...
WINDOWS
AUTOEXEC...
CONFIG.SYS
IO.SYS
MSDOS.SYS
boot.ini
dhcp_cap...
ipsec_no...
l2tp_man...
ipsec_ha...
l2tp_cap...
NTDETECT...
ntldr
bootfont...
pagefile...
用户: zhaobiao
Internet
开始
zhaobiao 047...
收件箱 - Mic...
Tcl控制台测...
单向访问
C:\WINDOWS\s...
ftp://172.16...
11:19

四、 配置关键点

见注释。