南昌大学软件学院

实验报告书

课 程 名 ： 网络安全技术

题　　目： 企业级防火墙实验

实验类别 【验证】

班　　级： 信息安全 193 班

学　　号： 8003119100

姓　　名： 丁俊

评语：

实验态度：认真（　）　一般（　）　较差（　）
实验结果：正确（　）　部分正确（　）错（　）
实验理论：掌握（　）　熟悉（　）　了解（　）生疏（　）
操作技能：较强（　）　一般（　）　较差（　）
实验报告：较好（　）　一般（　）　较差（　）

成绩：＿＿＿＿＿＿　　指导教师： 鄢志辉

一、实验目的

1、熟悉飞塔企业级防火墙的基本配置命令
2、通过安全策略的设置验证防火墙的状态检测功能

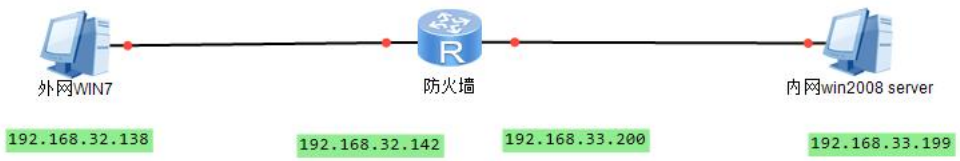
二、实验环境（本次上机实践所使用的平台和相关软件）

3台设备 :Microsoft Windows 2000虚拟机，物理PC win7,飞塔企业级防火墙虚拟机版

网络平台： TCP/IP网络，vmware workstation

三、实验步骤

1、实验拓扑图



实验环境说明：3 个设备，防火墙为虚拟机，2 块网卡，一块接外网，一块接内网。外网为 win10,内网电脑为 win2003server 虚拟机，做 web 和 ftp 服务器。

vmware 环境下网卡设置，需要将防火墙内网端口和 win2000 虚拟机网卡设置到一个独立的网段。

上图将防火墙 port2 端口和内网虚拟机 win2003server 放在同一个网段

2、对虚拟防火墙做初始化，可以通过图形界面进行管理

对防火墙做初始化，设置密码

```
Loading flatkc... ok
Loading /rootfs.gz...ok

Decompressing Linux... Parsing ELF... done.
Booting the kernel.

System is starting...
Serial number is FGVMEV3H3DTM7V48

FortiGate-VM64 login: *ATTENTION*: Admin sessions removed because license regist
ration status changed to 'INVALID'


FortiGate-VM64 login: admin
Password:
You are forced to change your password. Please input a new password.
New Password:
Confirm Password:
Welcome !

FortiGate-VM64 #
```

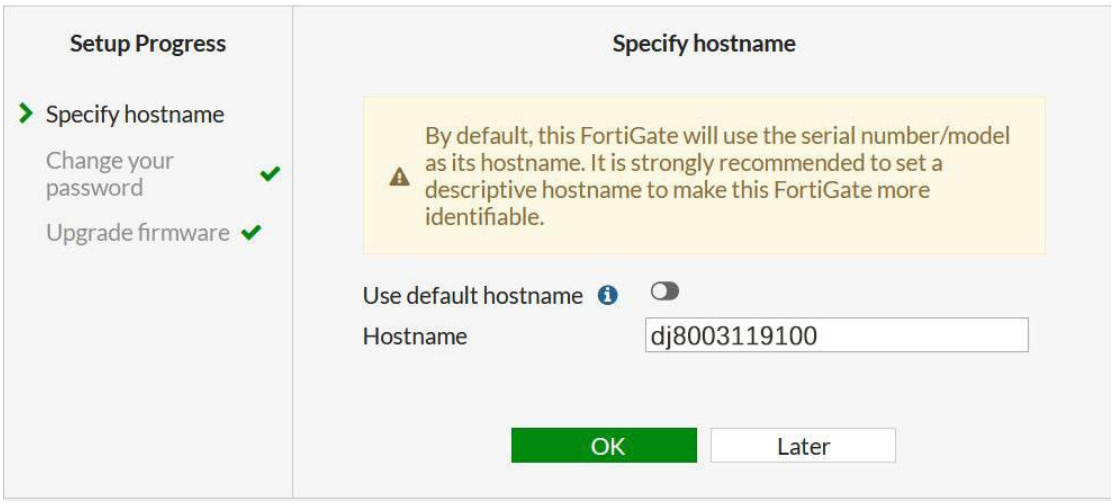
Port1 接 VM8 网卡，获取 IP：192.168.80.156/24 查看 port1

```
FortiGate-VM64 (port1) # get
name                 : port1
vdom                 : root
vrf                  : 0
cli-conn-status      : 2
fortilink            : disable
mode                 : dhcp
client-options:
distance             : 5
priority             : 0
dhcp-relay-service   : disable
ip                   : 192.168.80.156 255.255.255.0
allowaccess          : ping https ssh http fgfm
fail-detect          : disable
arpforward           : enable
broadcast-forward    : disable
bfd                  : global
l2forward            : disable
icmp-send-redirect   : enable
icmp-accept-redirect: enable
vlanforward          : disable
stpforward           : disable
ips-sniffer-mode     : disable
ident-accept         : disable
--More--
```

与“内网”网卡连接，获取 ip 为 172.16.243.131/24，查看 port2

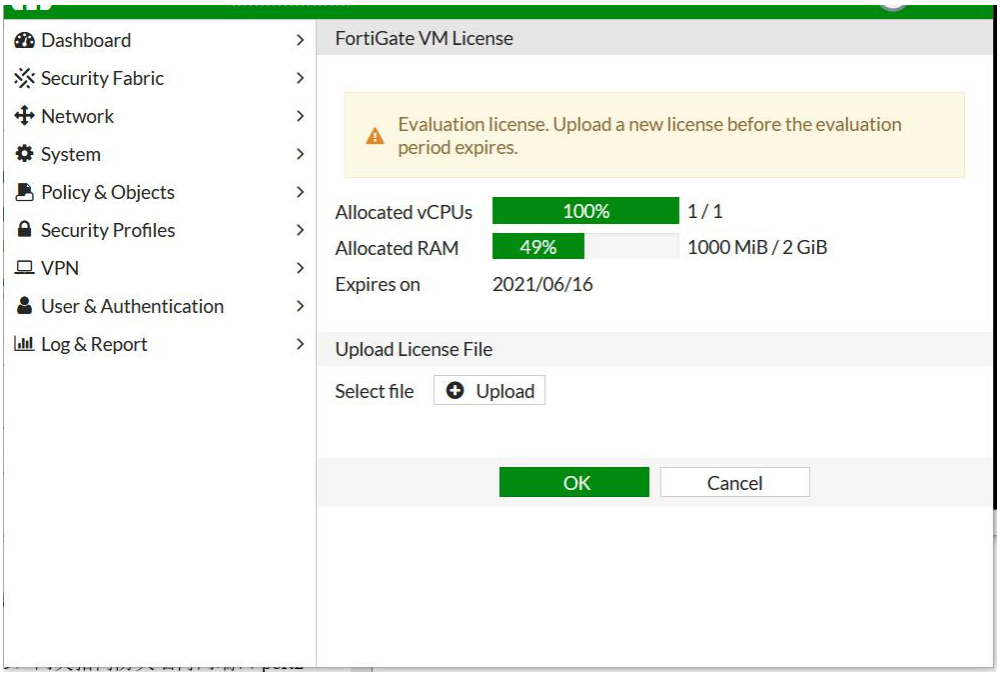
```
FortiGate-VM64 (port2) # get
name                 : port2
vdom                 : root
vrf                  : 0
cli-conn-status      : 2
fortilink            : disable
mode                 : dhcp
client-options:
distance             : 5
priority             : 0
dhcp-relay-service   : disable
ip                   : 172.16.243.131 255.255.255.0
allowaccess          :
fail-detect          : disable
arpforward           : enable
broadcast-forward    : disable
bfd                  : global
l2forward            : disable
icmp-send-redirect   : enable
icmp-accept-redirect: enable
vlanforward          : disable
stpforward           : disable
ips-sniffer-mode     : disable
ident-accept         : disable
--More-- _
```

在物理机 PC 浏览器输入防火墙 port1 地址 http://192.168.80.156/，即可进入图形界面



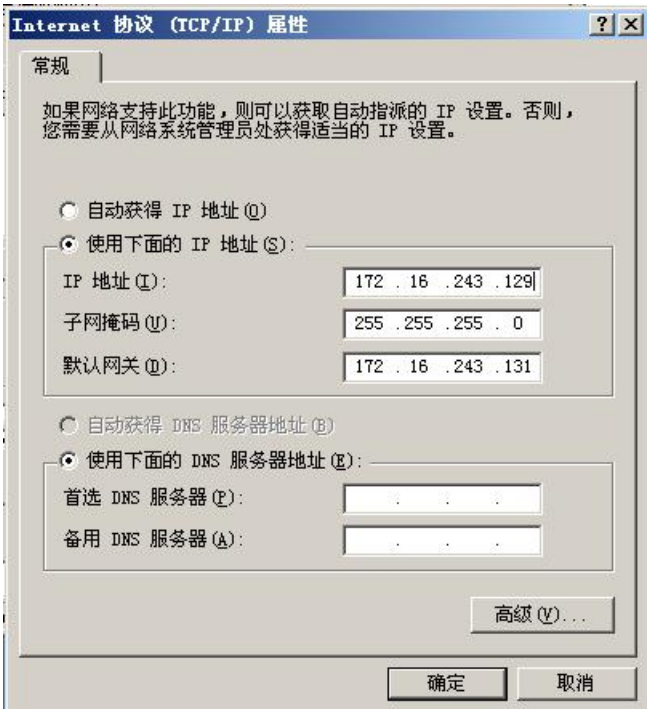
先按要求更改主机名：dj8003119100

然后即可进入主界面

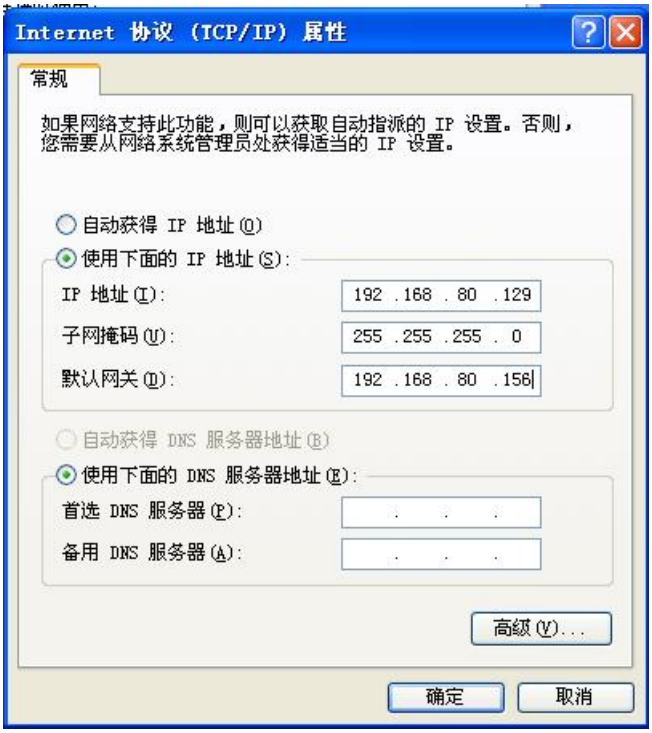


3、如图设置 3 台设备的 IP 地址，win2003 server 虚拟机的网关指向防火墙内网端口，winXP 虚拟机的网关指向防火墙的外网端口。

设置内网 WIn2003 server 虚拟机的 Ip 为 172.16.243.129，网关指向防火墙内网端口 port2



设置外网 winXP 虚拟机 Ip 为 192.168.80.129，网关为防火墙外网 port1 端口

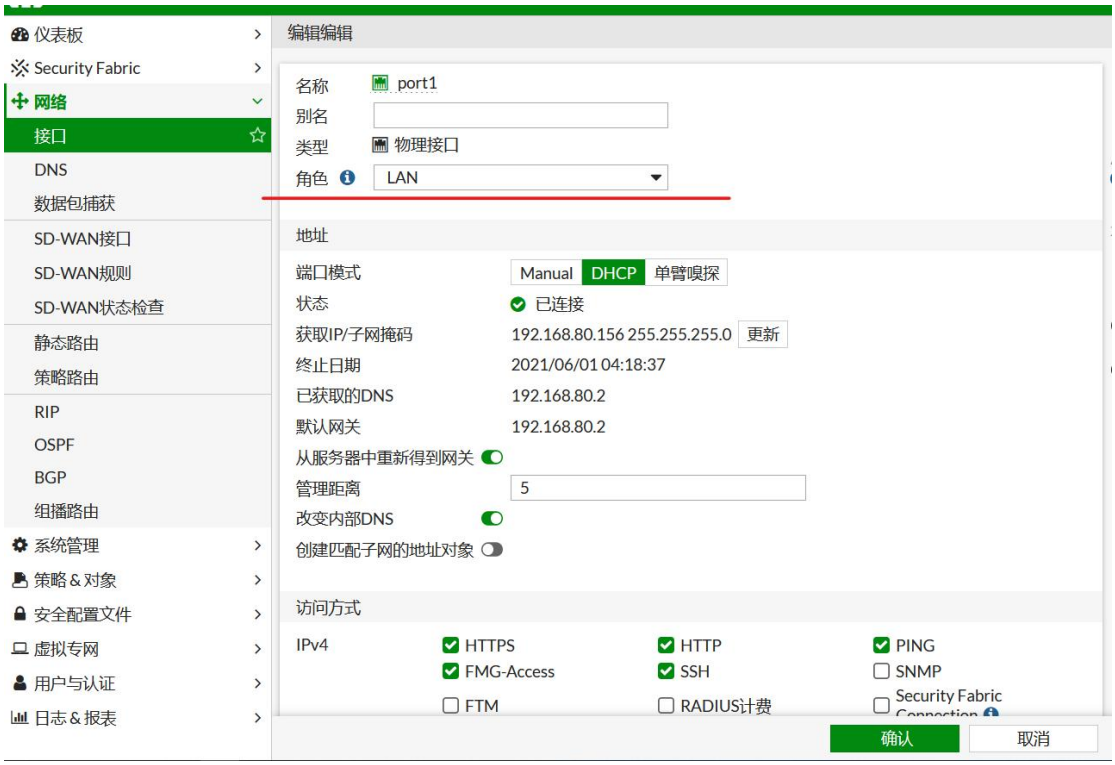


4、添加安全策略，允许外网物理 PC ping 内网 win2000 虚拟机（实验报告要对添加策略前后要做对比测试）

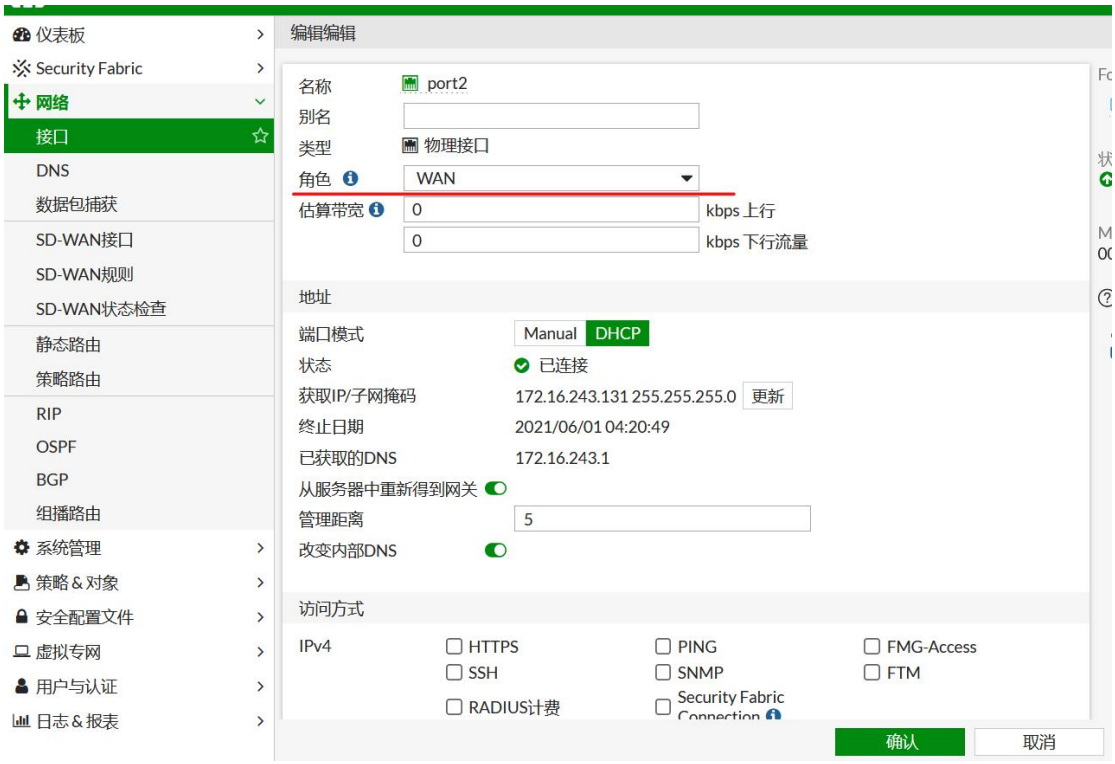
设备	IP	网关
本机	192.168.80.1	\
防火墙 port1	192.168.80.156	\
防火墙 port2	172.16.243.131	\
winXP 虚拟机	192.168.80.129	192.168.80.156

win2003server 虚拟机	172.16.243.129	172.16.243.131

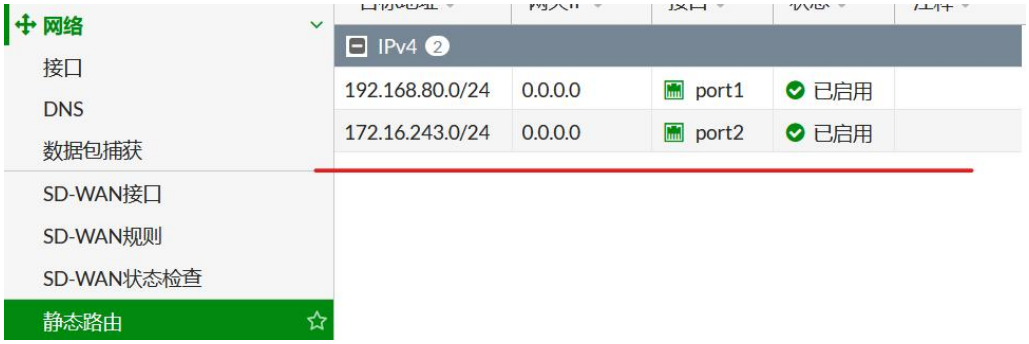
将防火墙 port1 端口设置为外网区域



将防火墙 port2 端口设置为内网区域



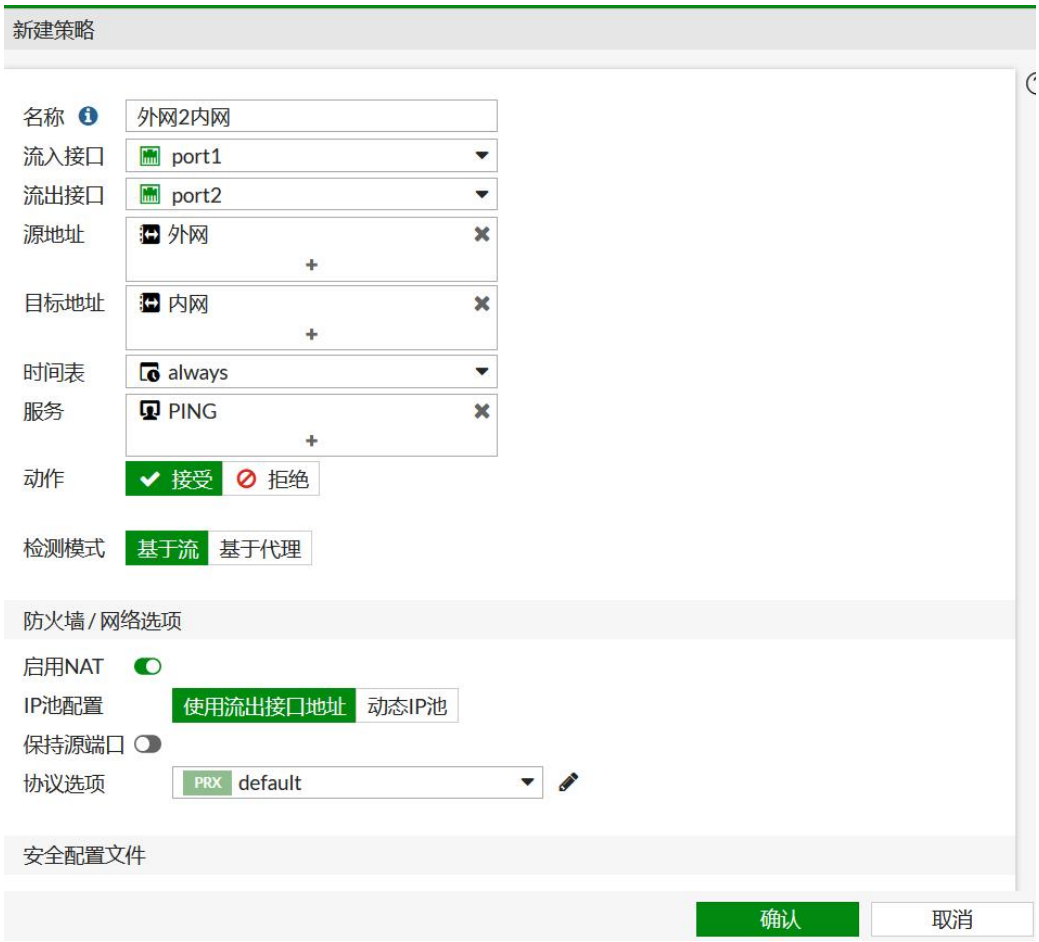
设置防火墙静态路由，使数据包能够转发



在未添加策略时，使用外网虚拟机 Ping 内网失败

添加内网、外网 IP 地址范围

添加安全策略，使外网 winXP 虚拟机能够 ping 内网 win2003server 虚拟机

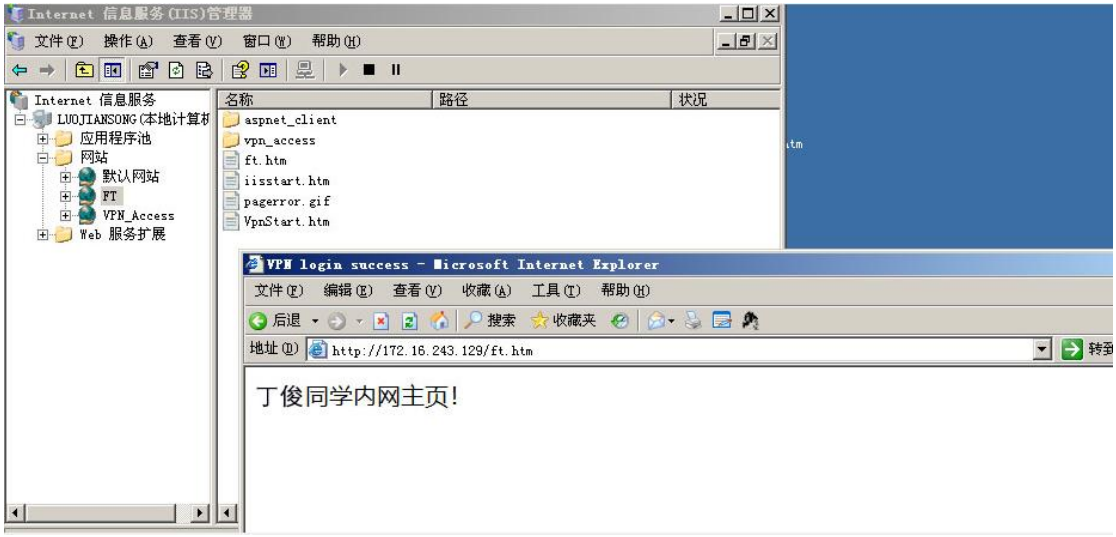


再次尝试外网 ping 内网，成功 ping 通

```
C:\Documents and Settings\Administrator>ping 172.16.243.129

Pinging 172.16.243.129 with 32 bytes of data:

Reply from 172.16.243.129: bytes=32 time=4ms TTL=127
Reply from 172.16.243.129: bytes=32 time=1ms TTL=127
Reply from 172.16.243.129: bytes=32 time<1ms TTL=127
Reply from 172.16.243.129: bytes=32 time<1ms TTL=127

Ping statistics for 172.16.243.129:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 4ms, Average = 1ms
```

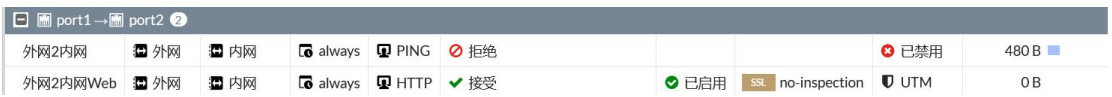
5、添加安全策略，允许外网物理 PC 访问内网 win2003 虚拟机的网站（网站内容要体现自己的名字，测试时只能访问 win2003 服务器的网站，无法访问 ftp 服务）

先在内网 win2003server 安装 iis，发布网页

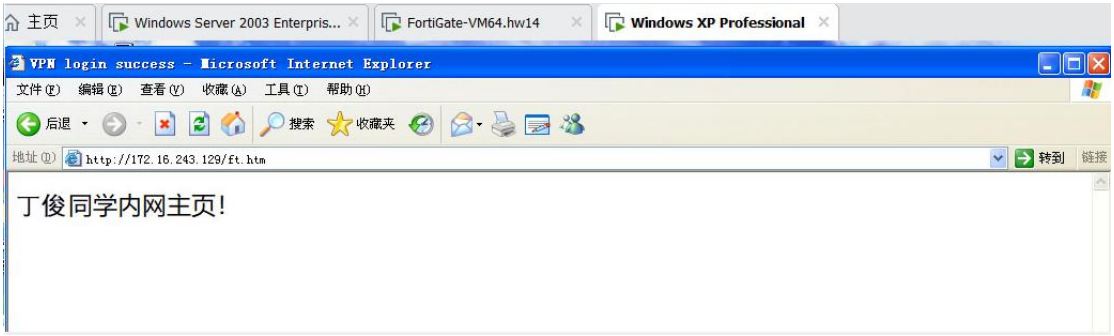


然后设置策略允许外网访问内网的 http 服务

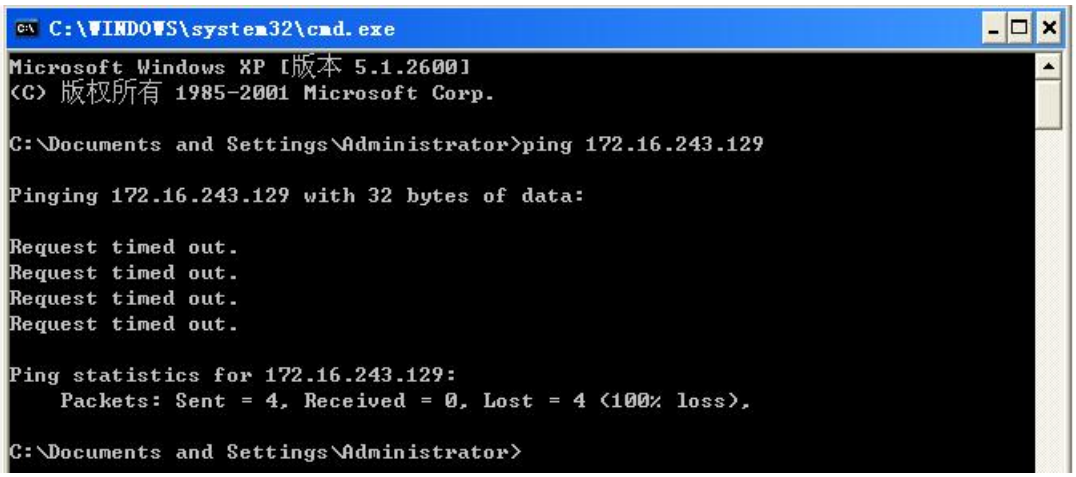
同时关闭外网 ping 内网的策略



使用外网浏览器输入地址访问内网，访问成功



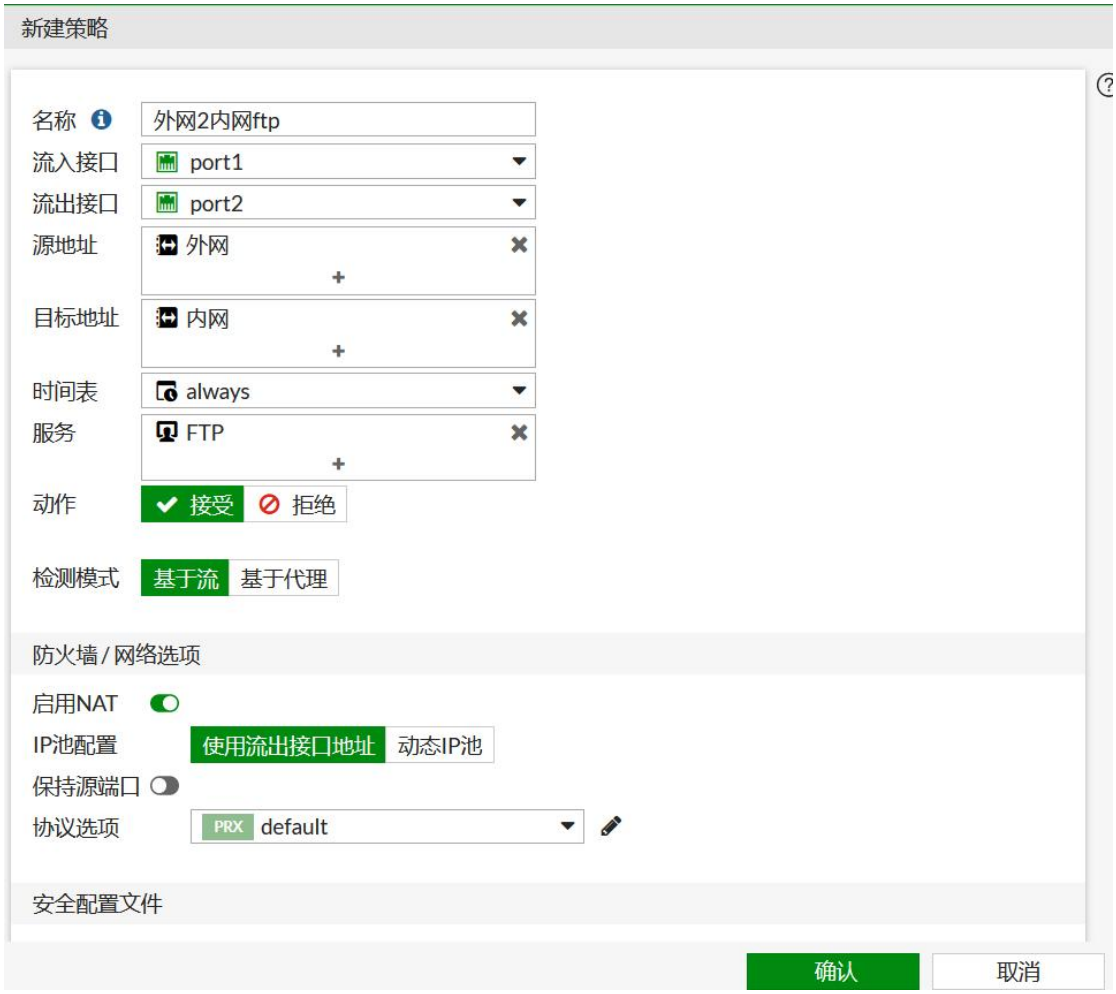
尝试外网 Ping 内网失败



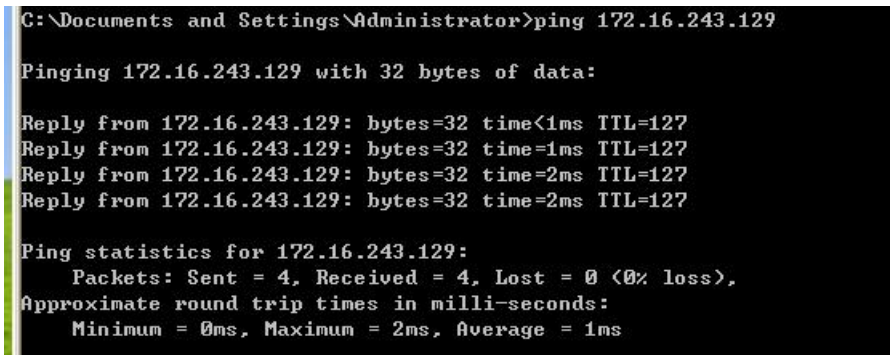
6、修改安全策略，允许外网物理 PC 访问除内网 win2003 虚拟机的网站的其他应用（测试结果无法访问 win2003 服务器的网站，可以访问 ftp 等其他服务）

修改上述第五点的安全策略，将接受改为拒绝

同时设置允许 ftp 并开启第四点的允许 Ping 策略



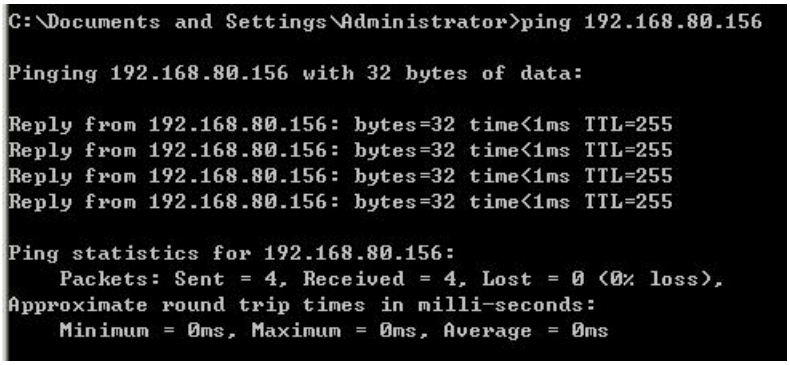
测试 ping 和 ftp，ping 和 ftp 均成功。（ftp 服务器步骤搭建省略）



7、添加安全策略，允许 内网 win2000 虚拟机 ping 外网物理 PC（实验报告要对添加策略前后要做对比测试）

方法和第四点类似，配置策略如下

内网 Ping 外网成功



四、结果分析与实验体会（试验中遇到的问题及解决过程，产生的错误及原因分析，试验体会和收获）

在刚开始 ping 的过程中，我发现无论怎样设置策略都 ping 不通，思考很久后才发现是防火墙没有关闭。这次实验使我初步了解了防火墙的作用、工作原理及其配置方法，对网络安全的认识更进一步，对安全知识的了解更加全面。