

# 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 flatk... ok
Loading /rootfs.gz...ok

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

System is starting...
Serial number is FGUMEV3H3DTM7U48

FortiGate-UM64 login: *ATTENTION*: Admin sessions removed because license registration status changed to 'INVALID'

FortiGate-UM64 login: admin
Password:
You are forced to change your password. Please input a new password.
New Password:
Confirm Password:
Welcome !

FortiGate-UM64 #
```

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

Setup Progress

> Specify hostname

Change your password ✓

Upgrade firmware ✓

Specify hostname

By default, this FortiGate will use the serial number/model as its hostname. It is strongly recommended to set a descriptive hostname to make this FortiGate more identifiable.

Use default hostname ⓘ ☐

Hostname

OK Later

先按要求更改主机名：dj8003119100

然后即可进入主界面

Dashboard

>

Security Fabric

>

Network

>

System

>

Policy & Objects

>

Security Profiles

>

VPN

>

User & Authentication

>

Log & Report

>

FortiGate VM License

Evaluation license. Upload a new license before the evaluation period expires.

Allocated vCPUs

100%

1 / 1

Allocated RAM

49%

1000 MiB / 2 GiB

Expires on

2021/06/16

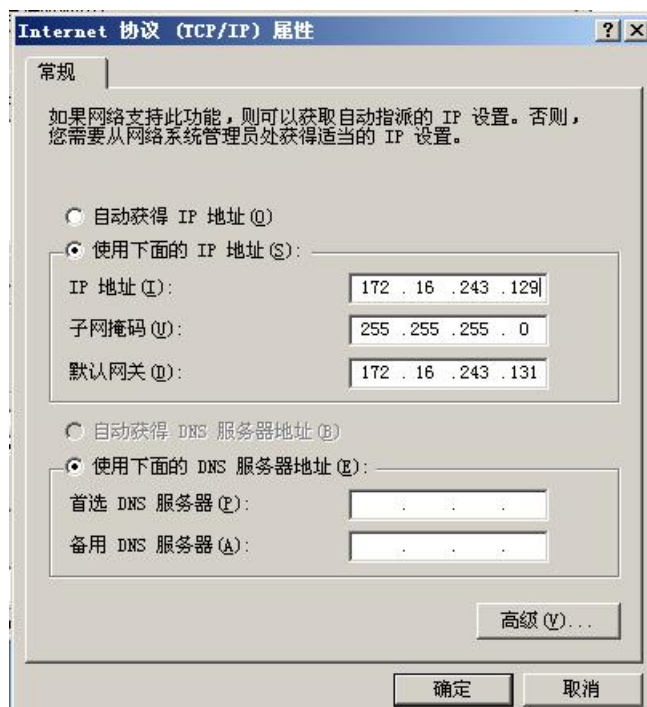
Upload License File

Select file

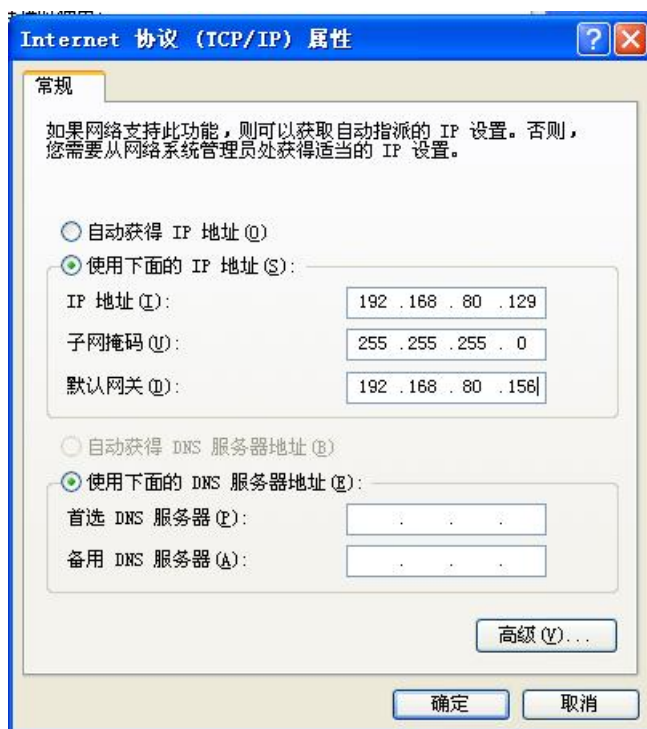
OK Cancel

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

仪表板

Security Fabric

网络

接口

DNS

数据包捕获

SD-WAN接口

SD-WAN规则

SD-WAN状态检查

静态路由

策略路由

RIP

OSPF

BGP

组播路由

系统管理

策略 & 对象

安全配置文件

虚拟专网

用户与认证

日志 & 报表

编辑编辑

名称

别名

类型

角色

地址

端口模式

状态

获取IP/子网掩码

终止日期

已获取的DNS

默认网关

从服务器中重新得到网关

管理距离

改变内部DNS

创建匹配子网的地址对象

访问方式

IPv4

HTTPS

HTTP

PING

FMG-Access

SSH

SNMP

FTM

RADIUS计费

Security Fabric Connection

确认

取消

将防火墙 port2 端口设置为内网区域

仪表板

Security Fabric

网络

接口

DNS

数据包捕获

SD-WAN接口

SD-WAN规则

SD-WAN状态检查

静态路由

策略路由

RIP

OSPF

BGP

组播路由

系统管理

策略 & 对象

安全配置文件

虚拟专网

用户与认证

日志 & 报表

编辑编辑

名称

别名

类型

角色

估算带宽

地址

端口模式

状态

获取IP/子网掩码

终止日期

已获取的DNS

从服务器中重新得到网关

管理距离

改变内部DNS

访问方式

IPv4

HTTPS

SSH

PING

FMG-Access

SNMP

FTM

RADIUS计费

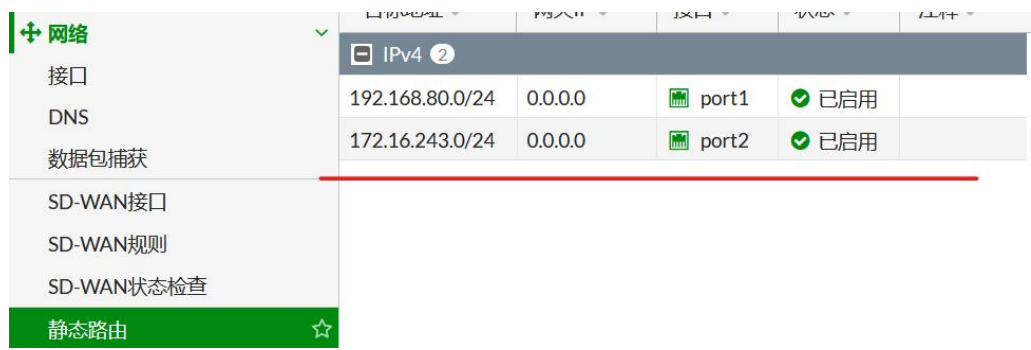
Security Fabric Connection

确认

取消



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

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

Pinging 172.16.243.129 with 32 bytes of data:

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

Ping statistics for 172.16.243.129:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

添加内网、外网 IP 地址范围

New Address

名称

外网

颜色

变更

类型

IP范围

IP 范围

192.168.80.1-192.168.80.255

接口

port1

静态路由配置

☐

注释

输入注释... 0/255

确认

取消



New Address

名称

内网

颜色

变更

类型

IP范围

IP 范围

172.16.243.1-172.16.243.255

接口

port2

静态路由配置

☐

注释

输入注释... 0/255

确认

取消

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

新建策略

名称

外网2内网

流入接口

port1

流出接口

port2

源地址

外网

目标地址

内网

时间表

always

服务

PING

动作

☒ 接受

☐ 拒绝

检测模式

基于流

基于代理

防火墙 / 网络选项

启用NAT

☒

IP池配置

使用流出接口地址

动态IP池

保持源端口

☐

协议选项

PRX

default

安全配置文件

确认

取消



再次尝试外网 ping 内网，成功 ping 通

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

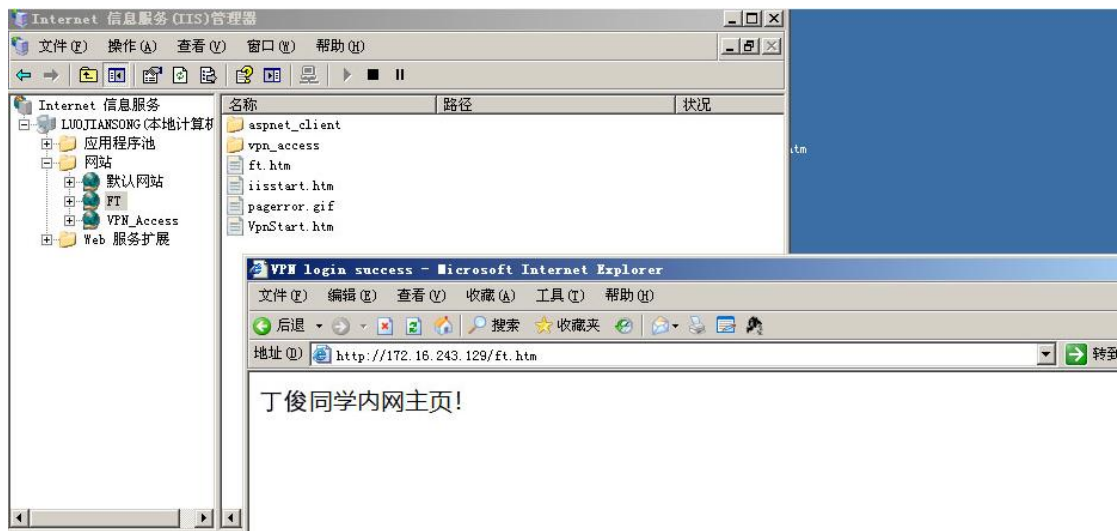
Pinging 172.16.243.129 with 32 bytes of data:

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

新建策略

名称 ⓘ

外网2内网Web

流入接口

port1

流出接口

port2

源地址

外网

目标地址

内网

时间表

always

服务

HTTP

动作

接受

拒绝

检测模式

基于流

基于代理

防火墙/网络选项

启用NAT

IP池配置

使用流出接口地址

动态IP池

保持源端口

协议选项

PRX

default

安全配置文件

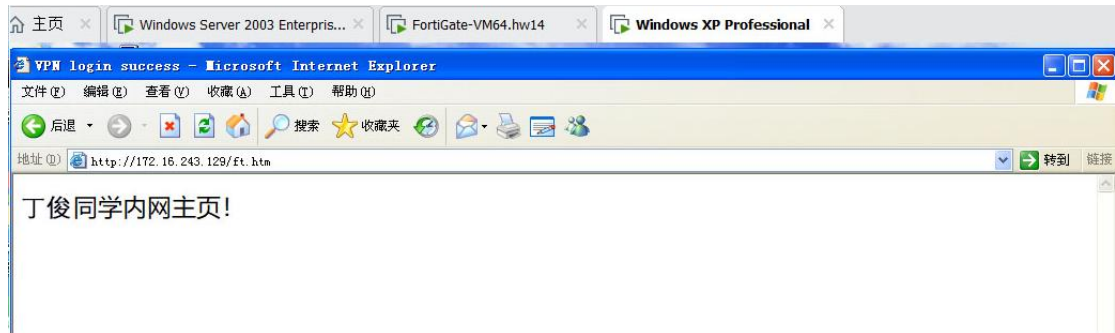
确认

取消

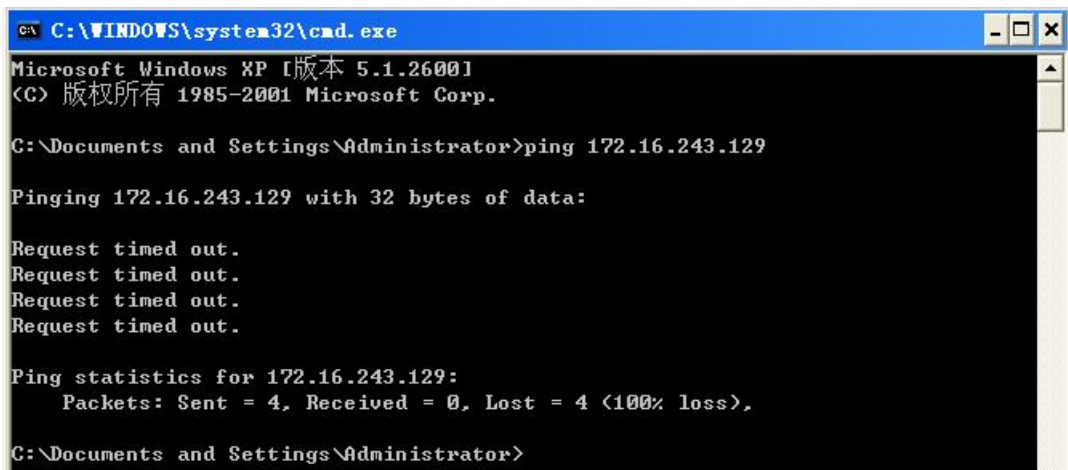
同时关闭外网 ping 内网的策略

外网2内网	外网	内网	always	PING	拒绝		已禁用	480 B
外网2内网Web	外网	内网	always	HTTP	接受	已启用	SSL no-inspection UTM	0 B

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



名称	源地址	目的地址	时间表	服务	动作	NAT	安全配置	流量日志
port1 → port2 2								
外网ping内网	外网计算机	内网计算机	always	PING	接受	已启用	SSL no-inspection	UTM
允许web访问	外网计算机	内网计算机	always	HTTP	拒绝			已禁用

同时设置允许 ftp 并开启第四点的允许 Ping 策略

新建策略

名称 ⓘ

流入接口

流出接口

源地址

目标地址

时间表

服务

动作

检测模式

外网2内网ftp

port1

port2

外网

+

内网

+

always

FTP

+

接受

拒绝

基于流

基于代理

防火墙 / 网络选项

启用NAT

IP池配置

保持源端口

协议选项

使用流出接口地址

动态IP池

PRX

default

安全配置文件

确认

取消

目的地址	时间表	服务	动作	NAT	安全配置	流量日志	字节数
内网	always	PING	接受	已启用	SSL no-inspection	UTM	720 B
内网	always	HTTP	拒绝			已禁用	2.58 kB
内网	always	FTP	接受	已启用	SSL no-inspection	UTM	0 B

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

```
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<1ms TTL=127
Reply from 172.16.243.129: bytes=32 time=1ms TTL=127
Reply from 172.16.243.129: bytes=32 time=2ms TTL=127
Reply from 172.16.243.129: bytes=32 time=2ms 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 = 2ms, Average = 1ms
```

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

---

```
C:\Documents and Settings\Administrator>ping 192.168.80.156

Pinging 192.168.80.156 with 32 bytes of data:

Reply from 192.168.80.156: bytes=32 time<1ms TTL=255
Reply from 192.168.80.156: bytes=32 time<1ms TTL=255
Reply from 192.168.80.156: bytes=32 time<1ms TTL=255
Reply from 192.168.80.156: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.80.156:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

#### 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，对网络安全认识更进一步，对安全知识了解更加全面。