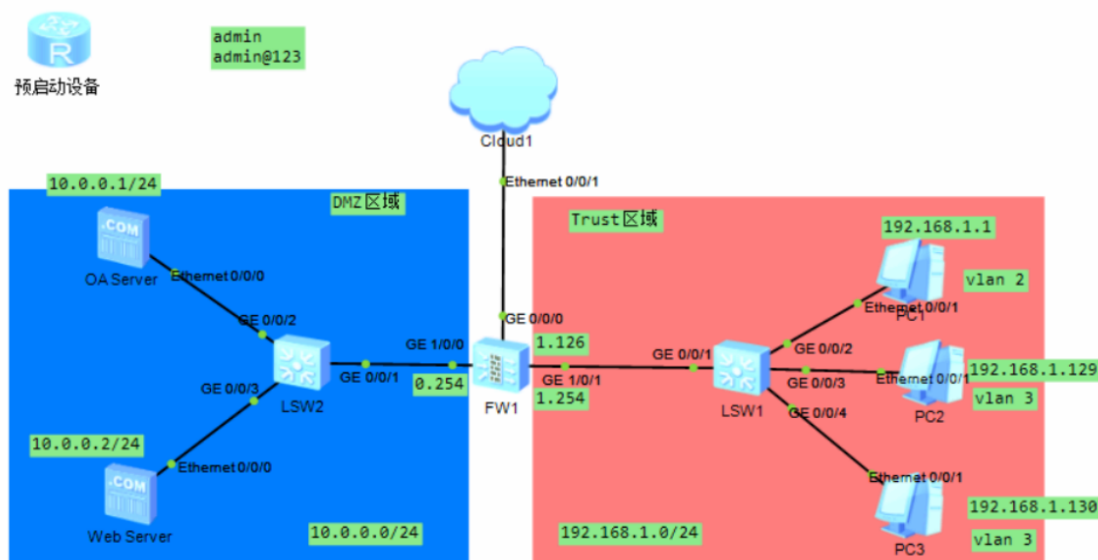


防火墙部署练习

题目及需求：



需求：
1、VLAN 2属于办公区；VLAN 3属于生产区
2、办公区PC在工作日时间（周一至周五，早8到晚6）可以正常访问OA Server，其他时间不允许
3、办公区PC可以在任意时刻访问Web Server
4、生产区PC可以在任意时刻访问OA Server，但是不能访问Web Server
5、特例：生产区PC3可以在每周一早10到早11访问Web Server，用来更新企业最新产品信息

需求分析

- 1.防火墙将网络分为DMZ区域和Trust区域，其中Trust区分为办公区（VLAN2）与生产区（VLAN3），办公区有PC1（192.168.1.1），生产区有PC2（192.168.1.129）和PC3（192.168.1.130）；DMZ区域有OA sever（10.0.1.1/24）和Web sever（10.0.0.2/24）
- 2.办公区在特定时间才可以正常访问OA sever，在任意时刻都可以访问Web sever
- 3.生产区在任意时刻都可以访问OA sever，但不能访问Web sever（PC3除外）

实现思路

1.交换机LSW1

将办公区部署在VLAN2，生产区部署在VLAN3，防火墙和交换机之间允许两种流量通过

2.防火墙

根据需要配置相应安全策略

操作配置

1.根据拓扑图配置各设备IP

PC1

基础配置

命令行

组播

UDP发包工具

串口

主机名:

MAC 地址:

54-89-98-6B-2F-E6

IPv4 配置

☒ 静态

☐ DHCP

☐ 自动获取 DNS 服务器地址

IP 地址:

192 . 168 . 1 . 1

DNS1:

0 . 0 . 0 . 0

子网掩码:

255 . 255 . 255 . 0

DNS2:

0 . 0 . 0 . 0

网关:

192 . 168 . 1 . 126

IPv6 配置

☒ 静态

☐ DHCPv6

IPv6 地址:

::

前缀长度:

128

IPv6 网关:

::

应用

PC2

基础配置

命令行

组播

UDP发包工具

串口

主机名:

MAC 地址:

54-89-98-FB-7C-54

IPv4 配置

☒ 静态

☐ DHCP

☐ 自动获取 DNS 服务器地址

IP 地址:

192 . 168 . 1 . 129

DNS1:

0 . 0 . 0 . 0

子网掩码:

255 . 255 . 255 . 0

DNS2:

0 . 0 . 0 . 0

网关:

192 . 168 . 1 . 254

IPv6 配置

☒ 静态

☐ DHCPv6

IPv6 地址:

::

前缀长度:

128

IPv6 网关:

::

应用

PC3

基础配置

命令行

组播

UDP发包工具

串口

主机名:

MAC 地址:

54-89-98-EF-29-FD

IPv4 配置

☒ 静态

☐ DHCP

☐ 自动获取 DNS 服务器地址

IP 地址:

192 . 168 . 1 . 130

DNS1:

0 . 0 . 0 . 0

子网掩码:

255 . 255 . 255 . 0

DNS2:

0 . 0 . 0 . 0

网关:

192 . 168 . 1 . 254

IPv6 配置

☒ 静态

☐ DHCPv6

IPv6 地址:

::

前缀长度:

128

IPv6 网关:

::

应用

OA Sever

基础配置

服务器信息

日志信息

Mac地址:

54-89-98-B3-27-40

(格式:00-01-02-03-04-05)

IPv4配置

本机地址:

10 . 0 . 0 . 1

子网掩码:

255 . 255 . 255 . 0

网关:

10 . 0 . 0 . 254

域名服务器:

0 . 0 . 0 . 0

PING测试

目的IPv4:

192 . 168 . 1 . 126

次数:

5

发送

本机状态:

设备启动

ping 成功: 0 失败: 10

保存

Web Sever

基础配置

服务器信息

日志信息

Mac地址:

54-89-98-79-3D-73

(格式:00-01-02-03-04-05)

IPv4配置

本机地址:

10 . 0 . 0 . 2

子网掩码:

255 . 255 . 255 . 0

网关:

10 . 0 . 0 . 254

域名服务器:

0 . 0 . 0 . 0

PING测试

目的IPv4:

10 . 0 . 0 . 254

次数:

10

发送

本机状态:

设备启动

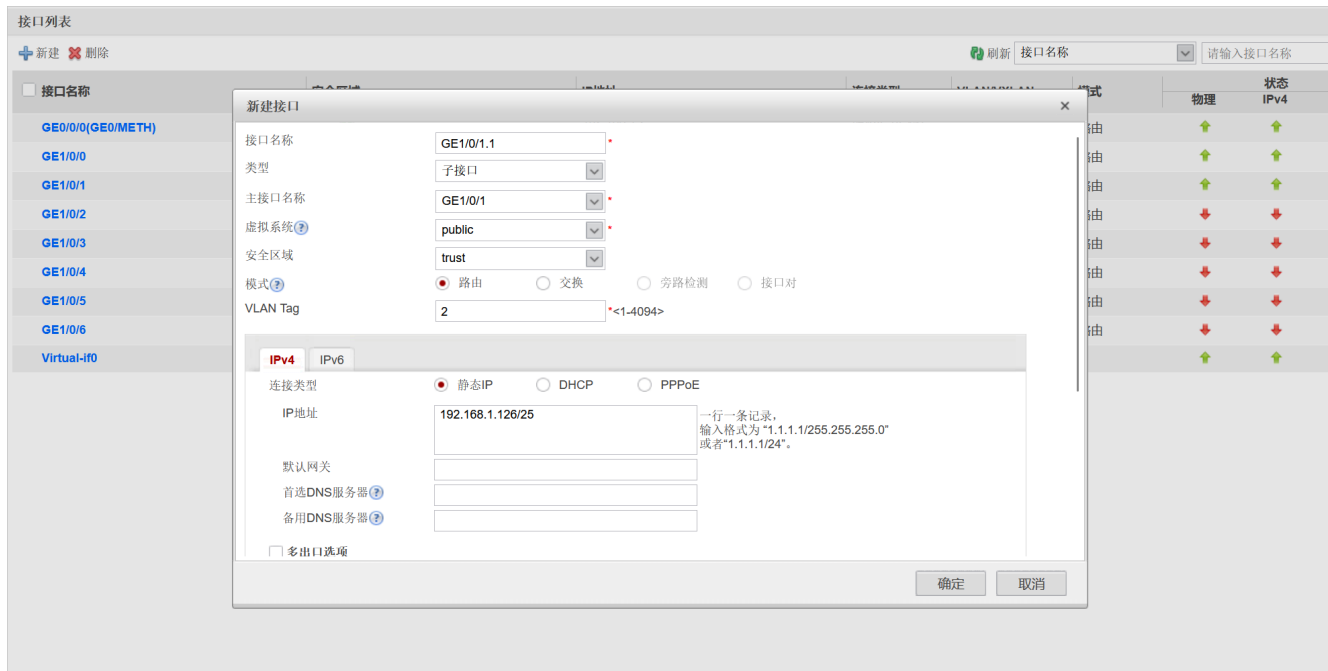
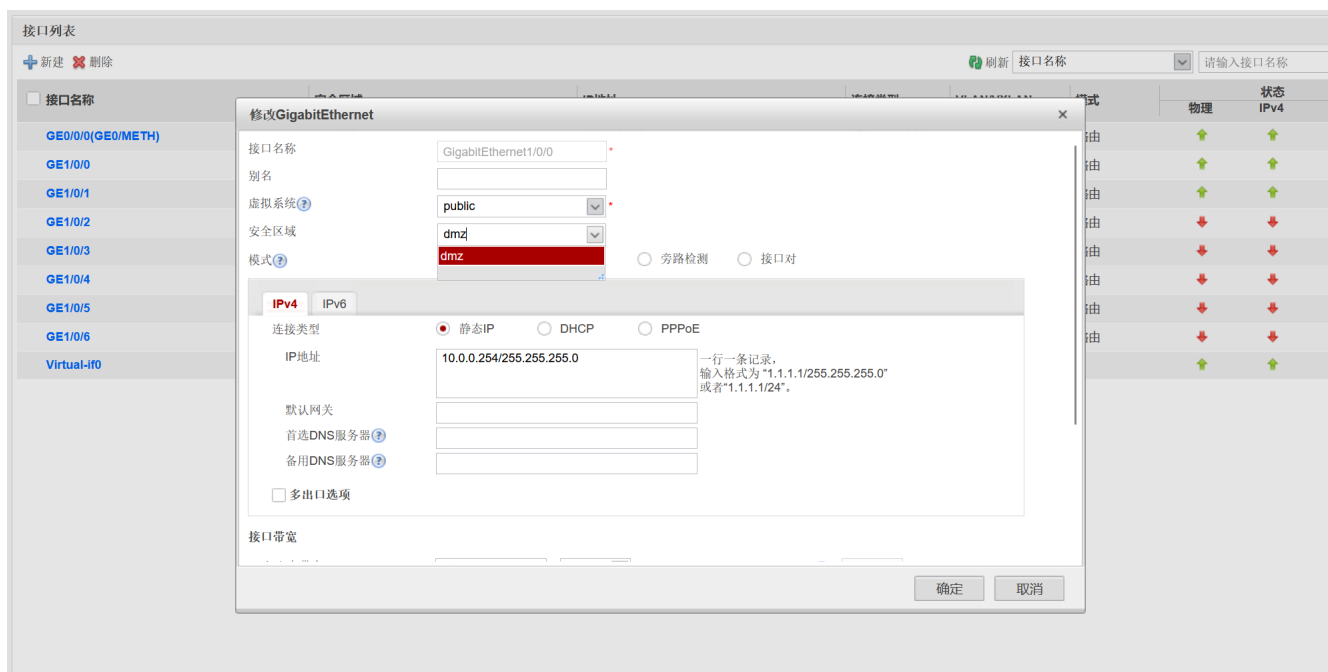
ping 成功: 10 失败: 0

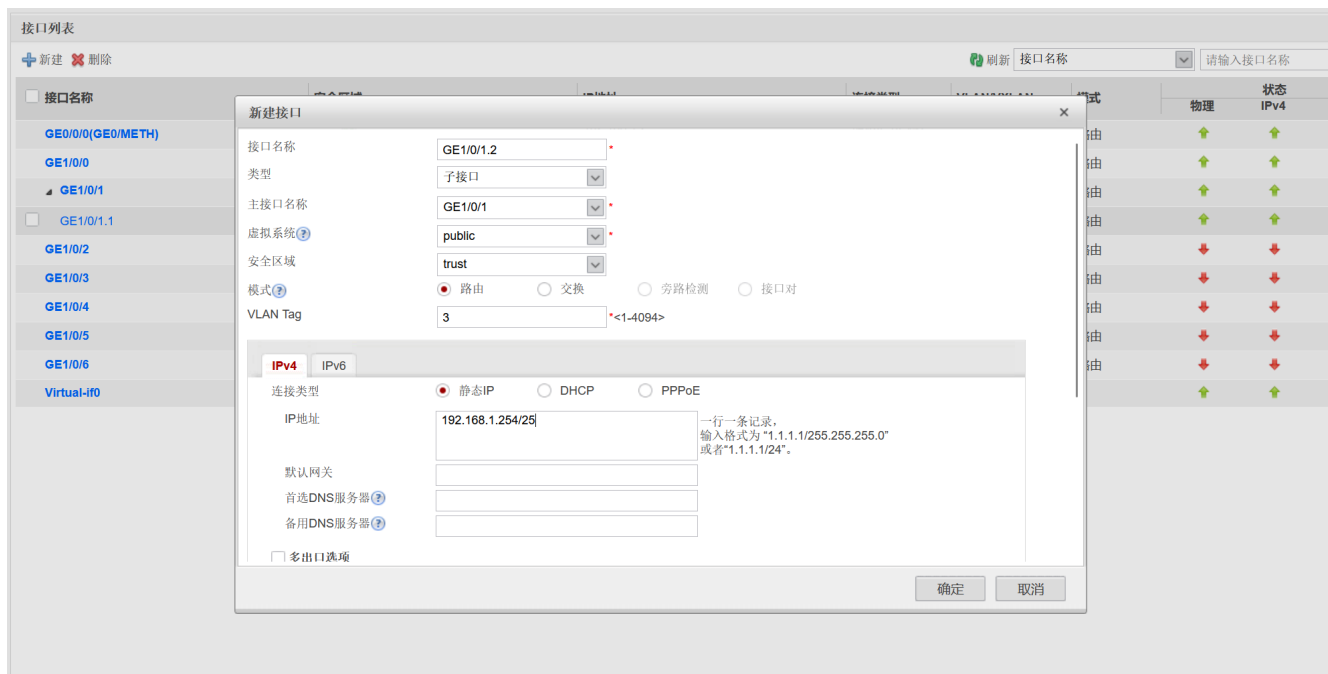
保存

2.建立防火墙与Cloud的连接

```
[USG6000V1]interface GigabitEthernet 0/0/0
[USG6000V1-GigabitEthernet0/0/0]ip address 192.168.1.2[需将网卡网关改为192.168.1.0] 24
[USG6000V1-GigabitEthernet0/0/0]service-manage all permit
```

3.进入防火墙Web界面 (<https://192.168.1.2:8443>), 进行防火墙接口配置





```
[USG6000V1-GigabitEthernet1/0/1.1]service-manage all permit
[USG6000V1-GigabitEthernet1/0/1.2]service-manage all permit
[USG6000V1-GigabitEthernet1/0/0]service-manage all permit
[USG6000V1]firewall zone trust
[USG6000V1-zone-trust]add interface GigabitEthernet 1/0/1.1
[USG6000V1-zone-trust]add interface GigabitEthernet 1/0/1.2
[USG6000V1]firewall zone dmz
[USG6000V1-zone-dmz]add interface GigabitEthernet 1/0/0
```

4.配置路由器LSW1

```
[LSW1]vlan batch 2 3
[LSW1]interface GigabitEthernet 0/0/2
[LSW1-GigabitEthernet0/0/2]port link-type access
[LSW1-GigabitEthernet0/0/2]port default vlan 2
[LSW1]interface GigabitEthernet 0/0/3
[LSW1-GigabitEthernet0/0/3]port link-type access
[LSW1-GigabitEthernet0/0/3]port default vlan 3
[LSW1]interface GigabitEthernet 0/0/4
[LSW1-GigabitEthernet0/0/4]port link-type access
[LSW1-GigabitEthernet0/0/4]port default vlan 3
[LSW1]interface GigabitEthernet 0/0/1
[LSW1-GigabitEthernet0/0/1]port link-type trunk
[LSW1-GigabitEthernet0/0/1]port trunk allow-pass vlan 2 3
```

5.测试VLAN流量流通性

PC1

基础配置 命令行 组播 UDP发包工具 串口

```
Request timeout!
Request timeout!
Request timeout!
Request timeout!

--- 192.168.1.126 ping statistics ---
 5 packet(s) transmitted
 0 packet(s) received
100.00% packet loss

PC>ping 192.168.1.126

Ping 192.168.1.126: 32 data bytes, Press Ctrl_C to break
From 192.168.1.126: bytes=32 seq=1 ttl=255 time=47 ms
From 192.168.1.126: bytes=32 seq=2 ttl=255 time=31 ms
From 192.168.1.126: bytes=32 seq=3 ttl=255 time=47 ms
From 192.168.1.126: bytes=32 seq=4 ttl=255 time=31 ms
From 192.168.1.126: bytes=32 seq=5 ttl=255 time=47 ms

--- 192.168.1.126 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 31/40/47 ms

PC>
```

PC2

基础配置 命令行 组播 UDP发包工具 串口

```
Request timeout!
Request timeout!
Request timeout!
Request timeout!

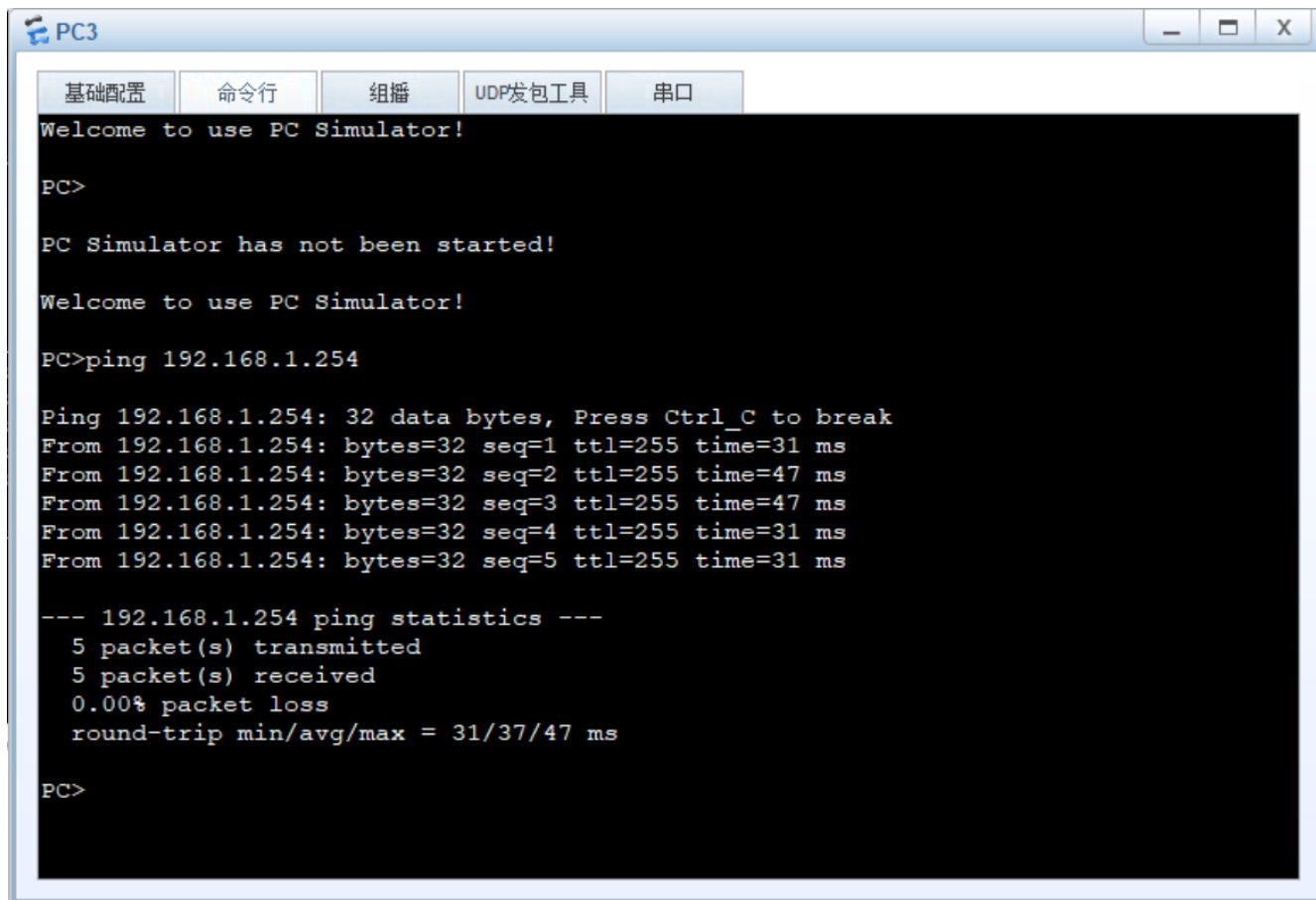
--- 192.168.1.254 ping statistics ---
 5 packet(s) transmitted
 0 packet(s) received
100.00% packet loss

PC>ping 192.168.1.254

Ping 192.168.1.254: 32 data bytes, Press Ctrl_C to break
From 192.168.1.254: bytes=32 seq=1 ttl=255 time=47 ms
From 192.168.1.254: bytes=32 seq=2 ttl=255 time=47 ms
From 192.168.1.254: bytes=32 seq=3 ttl=255 time=47 ms
From 192.168.1.254: bytes=32 seq=4 ttl=255 time=31 ms
From 192.168.1.254: bytes=32 seq=5 ttl=255 time=31 ms

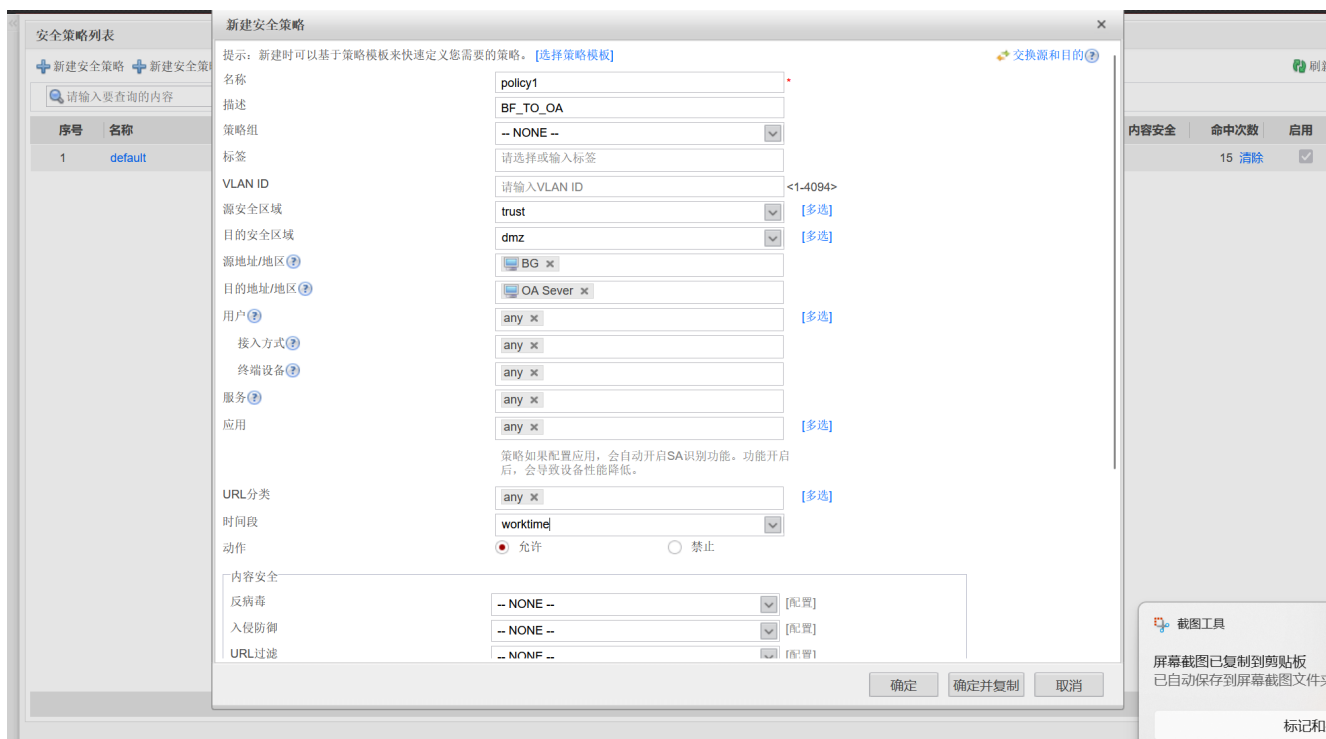
--- 192.168.1.254 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 31/40/47 ms

PC>
```



6.策略配置

需求2



需求3

策略列表

新建安全策略 + 新建安全策略

请输入要查询的内容

序号	名称
1	policy1
2	default

新建安全策略

提示：新建时可以基于策略模板来快速定义您需要的策略。[\[选择策略模板\]](#)

名称

policy2

描述

BG_TO_WEB

策略组

-- NONE --

标签

请选择或输入标签

VLAN ID

请输入VLAN ID

<1-4094>

源安全区域

trust

[多选]

目的安全区域

dmz

[多选]

源地址/地区

BG

目的地址/地区

Web Sever

用户

any

[多选]

接入方式

any

终端设备

any

服务

any

[多选]

应用

any

[多选]

策略如果配置应用，会自动开启SA识别功能。功能开启后，会导致设备性能降低。

URL分类

any

[多选]

时间段

any

动作

☒ 允许

☐ 禁止

内容安全

反病毒

-- NONE --

[配置]

入侵防御

-- NONE --

[配置]

URL过滤

-- NONE --

[配置]

确定

确定并复制

取消

需求4

策略对象网络系统

新建安全策略

提示：新建时可以基于策略模板来快速定义您需要的策略。[\[选择策略模板\]](#)

✖ 交换源和目的?

名称

policy3

描述

SC_TO_OA

策略组

-- NONE --

标签

请选择或输入标签

VLAN ID

请输入VLAN ID

<1-4094>

源安全区域

trust

[多选]

目的安全区域

dmz

[多选]

源地址/地区?

SC x

目的地址/地区?

OA Sever x

用户?

any x

[多选]

接入方式?

any x

终端设备?

any x

服务?

any x

应用

any x

[多选]

URL分类

any x

[多选]

时间段

any

动作

☒ 允许

☐ 禁止

内容安全

反病毒

-- NONE --

[配置]

入侵防御

-- NONE --

[配置]

URL过滤

-- NONE --

[配置]

确定

确定并复制

取消

需求5

新建安全策略

提示：新建时可以基于策略模板来快速定义您需要的策略。[选择策略模板]

名称

policy4

描述

SC_TO_WEB

策略组

-- NONE --

标签

请选择或输入标签

VLAN ID

请输入VLAN ID

<1-4094>

源安全区域

trust

[多选]

目的安全区域

dmz

[多选]

源地址/地区

192.168.1.130

x

目的地址/地区

Web Sever

x

用户

any

x

[多选]

接入方式

any

x

终端设备

any

x

服务

any

x

应用

any

x

[多选]

URL分类

any

x

[多选]

时间段

PC3

动作

允许

禁止

内容安全

反病毒

-- NONE --

[配置]

入侵防御

-- NONE --

[配置]

URL过滤

-- NONE --

[配置1]

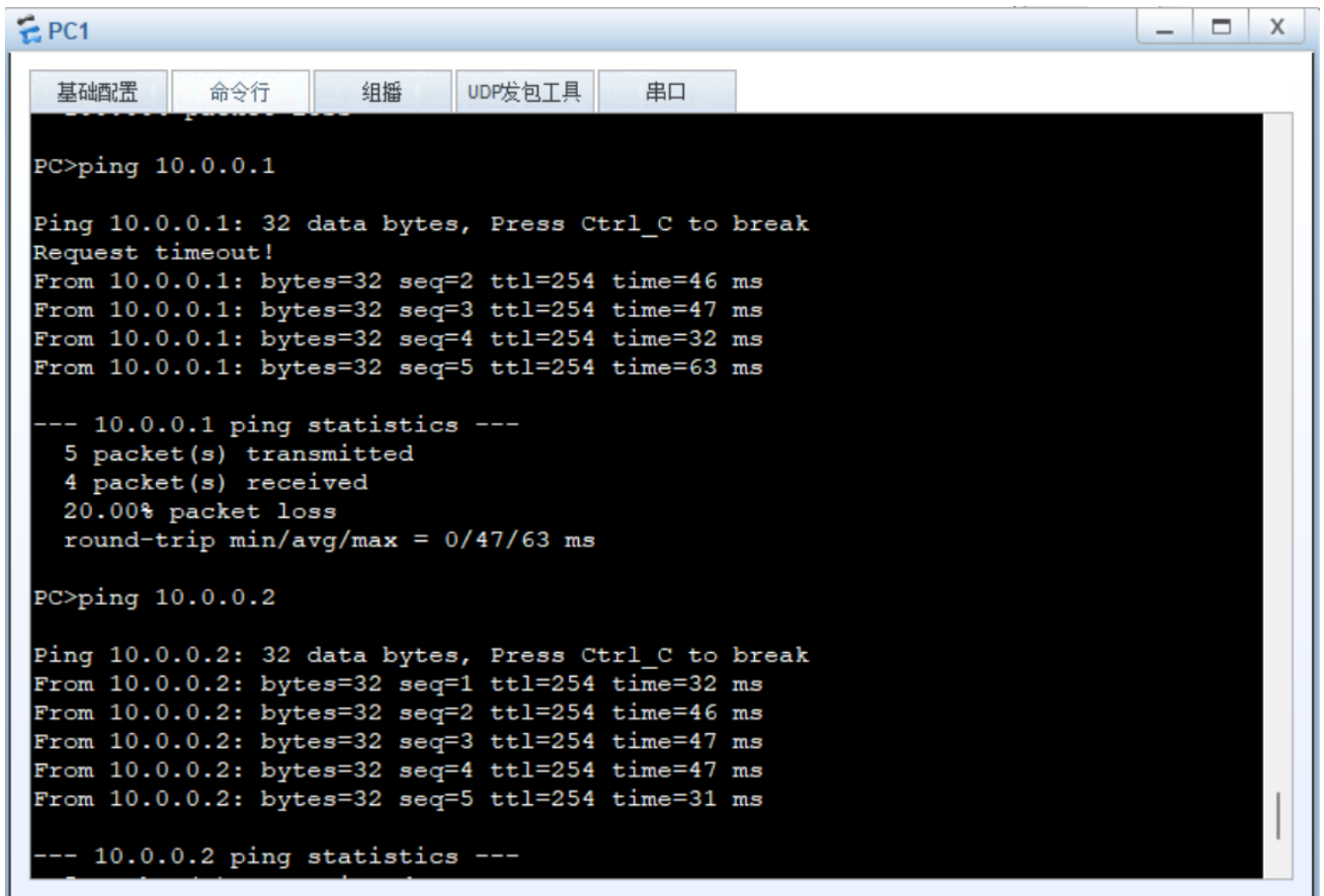
确定

确定并复制

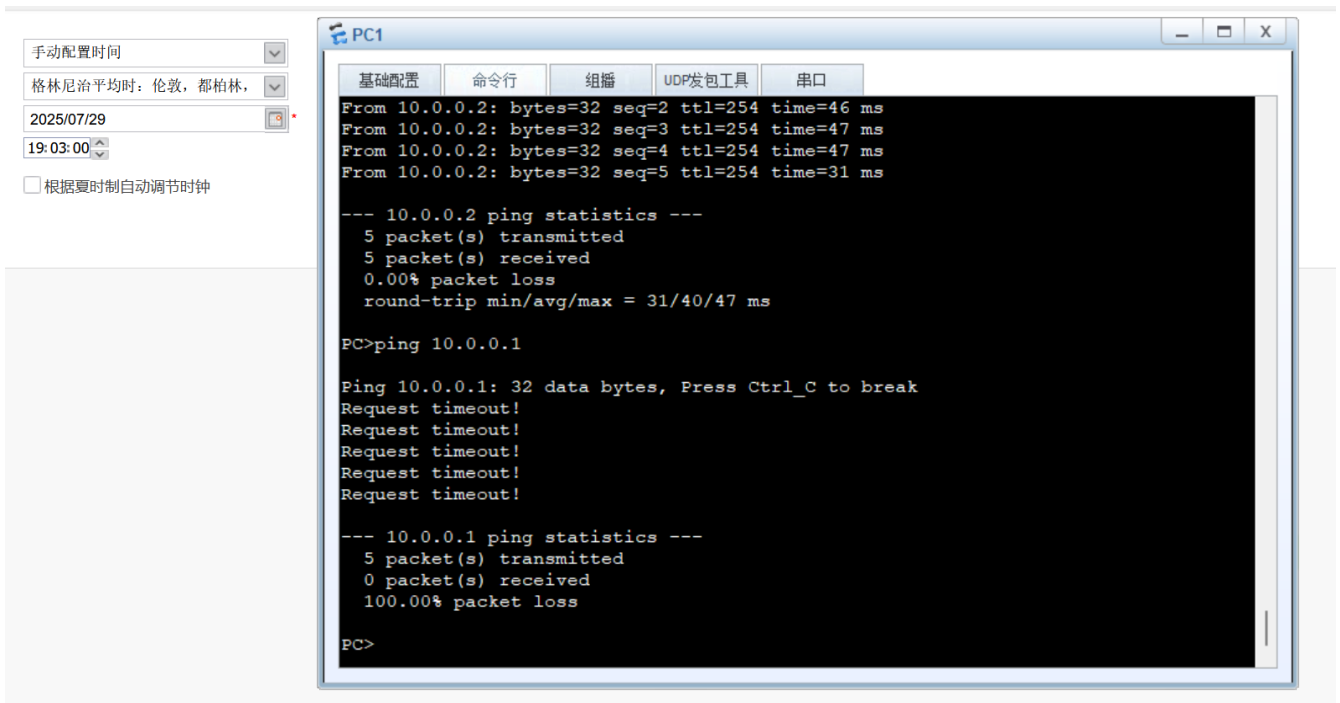
取消

连接测试

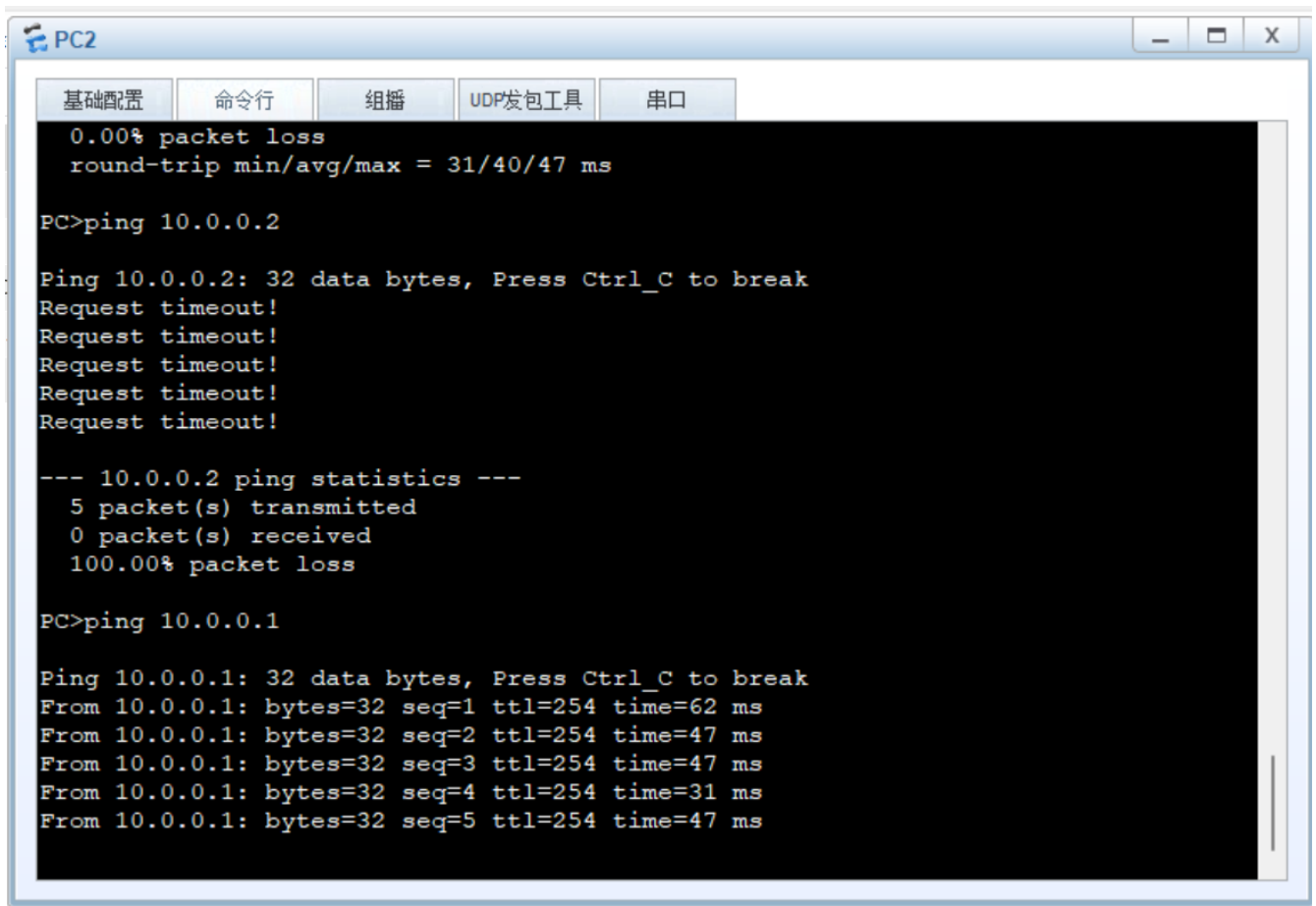
1.将系统时间设置为工作日工作时间，检测办公区能否连接OA服务器和WEB服务器



2.将系统时间设置为工作日非工作时间，检测办公区能否连通OA服务器



3.检测生产区能否连接OA服务器和WEB服务器



4.将系统时间设置为周一上午十点半，检测PC3能否连接WEB服务器

