

信息安全管理与评估

author: leadlife

time: 2022/3/11

微信: Tripse

知识星球: LeadlifeSec

QQ: 482949203

QQ群: 775454947

赛题基本信息

选取赛题

《2021年全国职业院校技能大赛高职组“信息安全管理与评估”赛项任务书4》

搭建部分赛项信息

加上渗透任务总共 🕒 270 分钟

竞赛阶段	任务阶段	竞赛任务	竞赛时间	分值
第一阶段：平台搭建	任务1	网络平台搭建	270分钟	60
第一阶段：安全设备配置防护	任务2	网络安全设备配置与防护	270分钟	240

赛项需注意的内容

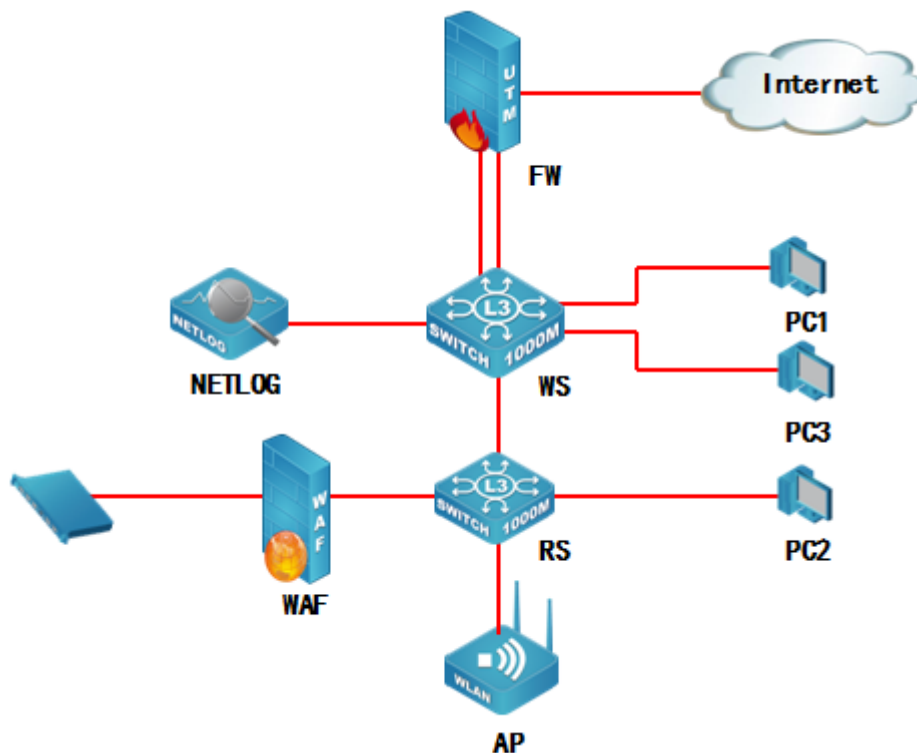
本次大赛，各位选手需要完成三个阶段的任务，其中第一个阶段需要按裁判组专门提供的U盘中的“XXX-答题模板”提交答案。第二、三阶段请根据现场具体题目要求操作。

选手首先需要在U盘的根目录下建立一个名为“GWxx”的文件夹（xx用具体的工位号替代），赛题第一阶段所完成的“XXX-答题模板”放置在文件夹中。

例如：08工位，则需要在U盘根目录下建立“GW08”文件夹，并在“GW08”文件夹下直接放置第一个阶段的所有“XXX-答题模板”文件。

特别说明：只允许在根目录下的“GWxx”文件夹中体现一次工位信息，不允许在其他文件夹名称或文件名称中再次体现工位信息，否则按作弊处理。

网络拓扑图



IP 地址规划表

设备名称	接口	IP 地址	对端设备
防火墙 FW	ETH0/1	9. 0. 0. 1/30 (Trust 安全域)	WS
	ETH0/2	10. 0. 0. 1/30 (untrust 安全域)	
	ETH0/3	11. 0. 0. 1/30 (Trust 安全域)	WS
	ETH0/4	12. 0. 0. 1/30 (Trust 安全域)	WS
	ETH0/5	218. 5. 18. 1/27 (untrust 安全域)	INTERNET
	SSL Pool	192. 168. 10. 1/24 可用 IP 数量为 20	SSL VPN 地址池
三层无线交换机 WS	ETH1/0/1-2	10. 0. 0. 2/30	FW
	VLAN 51 ETH1/0/3	10. 0. 0. 10/30	NETLOG
	VLAN 52 ETH1/0/22	172. 16. 100. 1/24	WAF
	VLAN 10	172. 16. 10. 1/24	无线 1
	VLAN 20	172. 16. 20. 1/25	无线 2
	VLAN 30 ETH1/0/3	172. 16. 30. 1/26	PC1
	VLAN 50 ETH1/0/5	172. 16. 50. 1/26	PC3
	ETH1/0/20 VLAN 100	192. 168. 100. 1/24	RS
三层交换机 RS	ETH1/0/1 VLAN 100	192. 168. 100. 254/24	WS
	无线管理 VLAN VLAN 101 ETH1/0/2	192. 168. 101. 1/24	AP
	VLAN 10		

	ETH1/0/4	172. 16. 40. 1/26	PC2
日志服务器 NETLOG	ETH2	10. 0. 0. 9/30	WS
WEB 应用防火墙	ETH2	172. 16. 100. 2/24	
WAF	ETH3		RS
堡垒服务器	—	—	WAF

设备初始化信息表

设备名称	管理地址	默认管理接口	用户名	密码
防火墙 FW	http://192. 168. 1. 1	ETH0	admin	admin
网络日志系统 NETLOG	https://192. 168. 5. 254	ETH0	admin	123456
WEB 应用防火墙 WAF	https://192. 168. 45. 1	ETH5	admin	admin123
三层交换机 RS	—	Console	—	—
无线交换机 WS	—	Console	—	—
堡垒服务器	—	—	—	
备注	所有设备的默认管理接口、管理 IP 地址不允许修改； 如果修改对应设备的缺省管理 IP 及管理端口，涉及此设备的题目按 0 分处理。			

赛题解析

任务一要求

题号	网络需求
1	根据网络拓扑图所示，按照IP地址参数表，对FW的名称、各接口IP地址进行配置。
2	根据网络拓扑图所示，按照IP地址参数表，对RS的名称进行配置，创建VLAN并将相应接口划入VLAN。
3	根据网络拓扑图所示，按照IP地址参数表，对RS各接口IP地址进行配置。
4	根据网络拓扑图所示，按照IP地址参数表，对WS的各接口IP地址进行配置。
5	根据网络拓扑图所示，按照IP地址参数表，对NETLOG的名称、各接口IP地址进行配置。
6	根据网络拓扑图所示，按照IP地址参数表，对WAF的名称、各接口IP地址进行配置。

任务一操作

FW 端口聚合-WS 端口聚合

题目

- 1 根据网络拓扑图所示，按照IP地址参数表，对FW的名称、各接口IP地址进行配置。

分析

FW 与 WS 存在双接口直连，可以推测出为“端口聚合”

说一下本人观点：不推荐全部使用 Cli 操作 FW 之类的设备，除非 GUI Web 界面实在操蛋

步骤

- 操作 IP 地址
- 修改 FW 名称
- 操作端口聚合
- (对应 WS 也需要操作端口聚合，可以不在该题目要求截图中，若评分标准不涉及)

命令

code	explanation
hostname	设置设备名称
int aggregate[num]	对应端口聚合
lcap enable	开启 lcap 动态协商，否则后期会是强制模式，即使放行策略也无法通信

操作

FW

设备管理

管理员 可信主机 管理接口 **设置**

系统维护

系统信息语言：☐ 中文 ☒ 英文 (系统信息包括日志信息、错误信息以及提示信息)

管理员认证服务器： ▼

主机配置

主机名称： (1~63)字符

域名： (0~255)字符

密码策略

密码最小长度： (4-16)

密码复杂度：☒ 无限制

☐ 密码必须包括至少两个大写字母，两个小写字母，两个数字和两个其他字符(如@*\$)

确定 取消

```
1 DCFW-1800# configure
2 DCFW-1800(config)# hostname FW
3 FW(config)#
4 FW(config)# interface aggregate1
5 FW(config-if-aggl)# ip add 0.0.0.0/0
6 FW(config-if-aggl)# lcap enable
7 FW(config-if-aggl)# no shutdown
8 FW(config-if-aggl)# exit
9 FW(config)# int aggregate1.9
10 FW(config-if-aggl.9)# zone trust
11 FW(config-if-aggl.9)# ip add 9.0.0.1/30
12 FW(config-if-aggl.9)# no shutdown
```

```

13 FW(config-if-aggl.9)# exit
14 FW(config)# interface aggregate1.91
15 FW(config-if-aggl.91)# zone untrust
16 FW(config-if-aggl.91)# no shutdown
17 FW(config-if-aggl.91)# ip add 10.0.0.1/30
18 FW(config-if-aggl.91)# exit
19 FW(config)# interface ethernet0/1
20 FW(config-if-eth0/1)# aggregate aggregate1
21 FW(config-if-eth0/1)# int e0/2
22 FW(config-if-eth0/2)# aggregate aggregate1
23 FW(config-if-eth0/2)# end

```

然后查看 GUI Web 应该是如此

接口名称	状态	IP/掩码	MAC	安全域	接入用户/IP数	流入带宽(bps)	流出带宽(bps)	描述
aggregate1		0.0.0.0/0	0003.0f82.e55e	NULL	0	0	0	
aggregate1.9		9.0.0.1/30	0003.0f82.e55e	trust	0	0	0	
aggregate1.91		10.0.0.1/30	0003.0f82.e55e	untrust	0	0	0	
ethernet0/0		192.168.1.1/24	0003.0f82.e555	trust	0	600	1.26K	
ethernet0/1		0.0.0.0/0	0003.0f82.e556	NULL	0	0	0	
ethernet0/2		0.0.0.0/0	0003.0f82.e557	NULL	0	0	0	
ethernet0/3		0.0.0.0/0	0003.0f82.e558	NULL	0	0	0	
ethernet0/4		0.0.0.0/0	0003.0f82.e559	NULL	0	0	0	
ethernet0/5		218.5.18.1/27	0003.0f82.e55a	untrust	0	0	120	INTERNET

然后我们需要在 FW 上创建任意端口放心通信的一个策略

策略配置

基本配置

高级控制

名称: (0~95)字符

当满足下列条件时——

源安全域:

目的安全域:

源地址: 多个...

目的地址: 多个...

服务簿: 多个...

时间表: 多个...

应用簿: 多个...

源用户: 多个...

做如下控制

行为: ☒ 允许
☐ 拒绝
☐ 安全连接

Web 认证只能工作在trust-vr。

策略描述: (0~255)字符

确定

取消

我们仍然会去 WS 上也开启相对应的 Channel

```
1 DCWS-6028(config)#hostname WS
2 WS(config)#int vlan 9
3 WS(config-if-vlan9)#ip add 9.0.0.2 255.255.255.252
4 WS(config-if-vlan9)#no shutdown
5 WS(config-if-vlan9)#exit
6 WS(config)#int vlan 91
7 WS(config-if-vlan91)#ip add 10.0.0.2 255.255.255.252
8 WS(config-if-vlan91)#no shutdown
9 WS(config-if-vlan91)#exit
10 WS(config)#port-group 1
11 WS(config)#int e1/0/1-2
12 WS(config-if-port-range)#no shutdown
13 WS(config-if-port-range)#switchport mode trunk
14 WS(config-if-port-range)#port-group 1 mode active
15 WS(config-if-port-range)#end
```

最后若完成成功，则能使 WS Ping 通 FW

```
1 WS#ping 9.0.0.1
2 Sending 5 56-byte ICMP Echos to 9.0.0.1, timeout is 2 seconds.
3 !!!
4 Success rate is 100 percent (3/3), round-trip min/avg/max = 0/0/0 ms
5
6 WS#ping 10.0.0.1
7 Sending 5 56-byte ICMP Echos to 10.0.0.1, timeout is 2 seconds.
8 !!!!!
9 Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 m
```

RS VLAN 加入与 Trunk or native

题目

- 1 根据网络拓扑图所示，按照IP地址参数表，对RS的名称进行配置，创建VLAN并将相应的 PC 接口划入 VLAN。
- 2 根据网络拓扑图所示，按照IP地址参数表，对RS各接口IP地址进行配置。

RS 与 WS 互联，我们需要注意无线管理 VLAN 与通信 VLAN

无线管理 VLAN 需要被 Native

步骤

修改 CS6200 交换机名称为 RS

添加对应 VLAN 与 IP add

操作管理 VLAN 与通信 VLAN

命令

code	explanation
switchport trunk native vlan 101	native vlan，使得该 vlan 穿越干道不被 tag 标记

操作

这里之所以要 Trunk e1/0/1 口，原因为：与 WS 相互连需要管理 VLAN 通信

```
1 CS6200-28X-EI>enable
2 CS6200-28X-EI#
3 CS6200-28X-EI#config terminal
4 CS6200-28X-EI(config)#hostname RS
5 RS(config)#vlan 100-101
6 RS(config)#vlan 40
7 RS(config-vlan40)#int vlan 100
8 RS(config-if-vlan100)#ip add 192.168.100.254 255.255.255.0
9 RS(config-if-vlan100)#no shutdown
10 RS(config-if-vlan100)#int vlan 101
11 RS(config-if-vlan101)#ip add 192.168.101.1 255.255.255.0
12 RS(config-if-vlan101)#no shutdown
13 RS(config-if-vlan101)#int vlan 40
14 RS(config-if-vlan40)#ip add 172.16.40.1 255.255.255.192
15 RS(config-if-vlan40)#no shutdown
16 RS(config-if-vlan40)#int e1/0/1
17 RS(config-if-ethernet1/0/1)#switchport mode trunk
18 RS(config-if-ethernet1/0/1)#switchport trunk allowed vlan 100;101;40
19 RS(config-if-ethernet1/0/1)#switchport trunk native vlan 101
20 RS(config-if-ethernet1/0/1)#end
```

WS 基础配置

题目

- 1 根据网络拓扑图所示，按照IP地址参数表，对WS的各接口IP地址进行配置。

分析

我们需要注意到相应 PC 业务 VLAN 需要 ACCESS ，并在与 RS 相连接的端口 Trunk 放行所有有关设备的流量

步骤

配置各个 VLAN 与 IP

操作相应 VLAN ACCESS

操作与 RS 相连接的端口 Trunk

操作

```
1 WS#config
2 WS(config)#vlan 51
3 WS(config-vlan51)#vlan 52
4 WS(config-vlan52)#vlan 10
5 WS(config-vlan10)#vlan 20
6 WS(config-vlan20)#vlan 30
7 WS(config-vlan30)#vlan 50
8 WS(config-vlan50)#vlan 100
9 WS(config-vlan100)#int vlan 51
10
11 WS(config)#int vlan 51
12 WS(config-if-vlan51)#ip add 10.0.0.10 255.255.255.252
13 WS(config-if-vlan51)#no shutdown
14 WS(config-if-vlan51)#int vlan 52
15 WS(config-if-vlan52)#ip add 172.16.100.1 255.255.255.0
16 WS(config-if-vlan52)#no shutdown
17 WS(config-if-vlan52)#int vlan 10
18 WS(config-if-vlan10)#ip add 172.16.10.1 255.255.255.0
19 WS(config-if-vlan10)#no shutdown
20 WS(config-if-vlan10)#int vlan 20
21 WS(config-if-vlan20)#ip add 172.16.20.1 255.255.255.128
22 WS(config-if-vlan20)#no shutdown
23 WS(config-if-vlan20)#int vlan 30
24 WS(config-if-vlan30)#ip add 172.16.30.1 255.255.255.192
```

```
25 WS(config-if-vlan30)#no shutdown
26 WS(config-if-vlan30)#int vlan 50
27 WS(config-if-vlan50)#ip add 172.16.50.1 255.255.255.252
28 WS(config-if-vlan50)#no shutdown
29 WS(config-if-vlan50)#int vlan 100
30 WS(config-if-vlan100)#ip add 192.168.100.1 255.255.255.0
31 WS(config-if-vlan100)#no shutdown
32
33 WS(config-if-vlan100)#int e1/0/1
34 WS(config-if-ethernet1/0/1)#switchport mode trunk
35 WS(config-if-ethernet1/0/1)#exit
36 WS(config)#interface e1/0/20
37 WS(config-if-ethernet1/0/20)#switchport mode trunk
38 Set the port Ethernet1/0/20 mode Trunk successfully
39 WS(config-if-ethernet1/0/20)#switchport trunk allowed vlan
    9;10;20;30;50;51;52;91;100
40 WS(config-if-ethernet1/0/20)#end
41 WS#show ip int b
42 Index      Interface      IP-Address      Protocol
43 11009      Vlan9          9.0.0.2         up
44 11010      Vlan10         172.16.10.1     up
45 11020      Vlan20         172.16.20.1     up
46 11030      Vlan30         172.16.30.1     up
47 11050      Vlan50         172.16.50.1     up
48 11051      Vlan51         10.0.0.10       up
49 11052      Vlan52         172.16.100.1    up
50 11091      Vlan91         10.0.0.2        up
51 11100      Vlan100        192.168.100.254 up
52 17500      Loopback       127.0.0.1       up
```

NetLog 基础配置

题目

- 1 根据网络拓扑图所示，按照IP地址参数表，对NETLOG的名称、各接口IP地址进行配置。

分析

我们需要注意，对 NETLOG 的名字要修改，我们需要进入到 Console 控制中操作

```
1 admin[LAB]# hostname NETLOG
```

其他照常操作即可

进入 Netlog Web GUI 界面 **系统信息** → **当前状态** 然后修改名称

其他照常配置

操作

系统信息	
主机名称	NETLOG <input type="text"/>
系统时间	2022-03-11 15:17:10 <input type="button" value="保存"/>
系统版本	v1.0
持续运行时间	2天 19小时 24分
审计数据保存期限	3 月
未读报警信息数量	0 条

使用 IE 浏览器进入 Web 管理界面，操作网络配置 → 网络接入 → 以太网卡接入 配置 IP

详细信息

以太网卡配置

接口名称	eth2
地址获取方式	<input checked="" type="radio"/> 静态 <input type="radio"/> DHCP
IP地址	10.0.0.9
子网掩码	255.255.255.252
MAC地址	00:16:31:e0:d8:66
接口状态	<input checked="" type="radio"/> 启用 <input type="radio"/> 停用
监控状态	<input type="checkbox"/> 监控
阻断发送接口	eth2
阻断目的MAC地址	<input type="radio"/> 指定 <input checked="" type="radio"/> 不指定 00:01:02:03:04:05

保存

WAF 基础配置


与 Netlog 操作差不多这里不多赘述，直接放图

操作

系统配置

时间服务器配置

系统时间: 2022-03-11 18:04:04

☒ 手动设置时间: 2022-03-11 18:04:01  ☐ 与本地时间同步

☐ 时间服务器: 1.pool.ntp.org 如: 1.pool.ntp.org、time.windows.com等

主机名称配置

主机名称: WAF  字母开头，字母、数字、下划线和中划线组成，长度为1到20

配置 → 网络配置 → 高级网络配置

新建网桥

网桥名称: br_23

注: 网桥名称以“br_”开头字母、数字、下划线组成，不超过20个字符

(待选择网口) (已选择网口)

网口列表:

eth4
eth5

>>>
<<<

eth2
eth3

创建好后编辑然后创建 IP

编辑网桥

网桥名称: br_23

(待选择网口) (已选择网口)

网口列表:

eth4
eth5

>>>
<<<

eth2
eth3

IP地址: 172.16.100.2

子网掩码: 255.255.255.0

任务二操作

Telnet Banner

类似题型

- 1 RS和WS开启telnet登录功能，配置使用telnet方式登录终端界面前显示如下授权信息：“WARNING!!! Authorised access only, all of your done will be recorded! Disconnected IMMEDIATELY if you are not an authorised user! Otherwise, we retain the right to pursue the legal responsibility”

注意点

- 关于 Telnet Banner 在比赛中，我们需要注意;
- DCWS-6028 也就是 AC 和 CS6200 三层交换机的 banner 配置不同;

命令

name	code
DCWS-6028	DCWS-6028(config)#banner motd ? LINE 用户字符串, <1-100>字符
DC6200	RS(config)#banner login ? LINE 用户字符串, <1-512>字符

操作

RS

- 1 RS(config)#banner login WARNING!!! Authorised access only, all of your done will be recorded! Disconnected IMMEDIATELY if you are not an authorised user! Otherwise, we retain the right to pursue the legal responsibility

WS

- 1 WS(config)#banner motd WARNING!!! Authorised access only, all of your done will be recorded! Disconnected IMMEDIATELY if you are not an authorised user! Otherwise, we retain the right to pursue the legal responsibility
- 2 %banner string length should be no more than 100

SNMP 网管系统-信息上报

所谓网管系统也就是 SNMP 服务，我们要操作的命令也就是 `snmp-server`

若有关 MAC 地址绑定操作 MAC 即可

类似题型

1 总部部署了一套网管系统实现对核心RS进行管理，网管系统IP为：172.16.100.21，读团体值为：ABC2024，版本为V2C， RS Trap信息实时上报网管，当MAC地址发生变化时，也要立即通知网管发生的变化，每35s发送一次；

注意点

- 开启 snmp-server 服务
- 开启 snmp-server traps 功能
- 需求中有 MAC 地址

命令

code	explanation
snmp-server securityip	设置安全IP地址
snmp-server host	设置接受Trap的管理端
snmp-server trap-source	设置SNMP Trap-source IP地址
snmp-server community	设置团体值
snmp-server enable traps mac-notification	开启 MAC 地址变化信息通告网管
mac-address-table violation-trap-interval 35	操作发送trap信息的时间间隔

操作

```
1 RS#config terminal
2 RS(config)#snmp-server enable
3 RS(config)#snmp-server enable traps
4 RS(config)#snmp-server securityip 172.16.100.21
5 RS(config)#snmp-server host 172.16.100.21 v2c ABC2024
6 RS(config)#snmp-server trap-source 172.16.100.21
7 RS(config)#snmp-server community ro ABC2024
8 RS(config)#snmp-server enable traps mac-notification
9 RS(config)#mac-address-table violation-trap-interval 35
```

流量往返转发 Netlog 跨网段三层镜像

类似题目

- 1 RS出口往返流量发送给NETLOG，由NETLOG对收到的数据进行用户所要求的分析

注意点

我们从题目中可以分析出两个问题；

- 1: RS 与 NETLOG 并不直连
- 2: 要求出口往返流量均转发至 NETLOG

分析以下，我们可以确定两个要点；

- RS 必须拥有与 Netlog 网段 IP 对应的 VLAN，这里为 VLAN 51，由 WS 与 Netlog 通信
- RS 的出口往返流量驻留在 E1/0/1

命令

code	exlanation
remote-span	配置远程镜像Vlan
monitor session 1 source	配置远程镜像源端源端口，以将数据收集并好转发
monitor session 1 remote vlan 51	设置远程镜像给谁
monitor session 1 reflector-port interface e1/0/24	将一个不用的端口用于反射 E1/0/1 流量到 vlan 51 网段 再基于 WS 转发给 NETLOG

操作

```
1 RS(config)#vlan 51
2 RS(config-vlan51)#remote-span
3 RS(config-vlan51)#exit
4 RS(config)#monitor session 1 source interface ethernet 1/0/1
5 RS(config)#monitor session 1 remote vlan 51
6 RS(config)#monitor session 1 reflector-port interface e1/0/24
```


二层隔离-环路检测- DHCP monitor 监听防欺骗-ARP 防欺骗

类似题型

- 1 4. 对RS上VLAN40开启以下安全机制：业务内部终端相互二层隔离，启用环路检测，环路检测的时间间隔为10s，发现环路以后关闭该端口，恢复时间为 30分钟； 如私设DHCP服务器关闭该端口；防止ARP欺骗攻击；

注意点

- 我们需要对指定的安全机制，做发现故障后的动作
- 需要注意 DHCP snooping 在 E1/0/1 口需要 Trust 以发现恶意的私设 DHCP

命令

code	explanation
isolate-port	设置隔离端口属性
loopback-detection	启用环路检测、并设置环路检测时间间隔
loopback-detection specified-vlan 40	绑定 VLAN 40 流量以操作安全机制
loopback-detection control	操作发现环路后的动作
loopback-detection control-recovery timeout 1800	操作关闭端口后的回复时间
ip dhcp snooping binding arp	防止 ARP 欺骗
ip dhcp snooping trust	设置只信任该端口转发的 DHCP 报文，避免恶意 DHCP
ip dhcp snooping binding user-control	启动DHCP Snooping绑定user功能、操作所属 VLNA 40 业务的流量

操作

```
1 RS(config)#vlan 40
2 RS(config-vlan40)#isolate-port apply l2
3 RS(config-vlan40)#exit
4 RS(config)#loopback-detection interval-time 10 10
5
6
7 RS(config)#int e1/0/4
```

```
8 RS(config-if-ethernet1/0/4)#loopback-detection specified-vlan 40

9 RS(config-if-ethernet1/0/4)#loopback-detection control shutdown
10 RS(config-if-ethernet1/0/4)#exit
11 RS(config)#loopback-detection control-recovery timeout 1800
12
13 RS(config)#ip dhcp snooping enable
14 RS(config)#ip dhcp snooping binding enable
15 RS(config)#ip dhcp snooping binding arp
16 RS(config)#int e1/0/1
17 RS(config-if-ethernet1/0/1)#ip dhcp snooping trust
18 RS(config-if-ethernet1/0/1)#exit
19 RS(config)#int e1/0/4
20 RS(config-if-ethernet1/0/4)#ip dhcp snooping binding user-control
```

FW 操作业务流量访问 INTERNET 安全防护-RS VRF VPN

类似题型

- 1 配置使总部VLAN10, 30, 40业务的用户访问INTERNET往返数据流都经过FW进行最严格的安全防护; RS使用相关VPN技术, 模拟INTERNET ,VPN名称为INTERNET地址为218.5.18.2;

注意点

- 我们在操作 FW 的相应匹配流量的地址博时需要对其部署相应的放行策略
- VRF VPN 基于 Loopback 口转发
- 由于基于最严格的安全防护, 我们需要防止恶意路由配置静态路由
- 开机攻击防护

命令

code	explanation
ip vrf INTERNET	创建 VPN路由/转发实例
ip vrf forwarding INTERNET	转发实例

FW

创建业务地址簿

右上角的用户对象 → 地址簿

配置地址簿

名称：

总部VLAN10, 30, 40业务

(1~95)字符

成员：

IP/掩码

IP地址

/

网络掩码

<input type="checkbox"/>	类型	成员
<input type="checkbox"/>	IP地址	172.16.40.0/26
<input type="checkbox"/>	IP地址	172.16.30.0/26
<input type="checkbox"/>	IP地址	172.16.10.0/24

添加

删除

描述：

(0~255)字符

确定

取消

创建 **INTERNET** 地址簿

右上角的用户对象 → 地址簿

配置地址簿

名称: (1~95)字符

成员: /

<input type="checkbox"/>	类型	成员
<input type="checkbox"/>	IP地址	218.5.18.0/27

描述: (0~255)字符

创建相应放行策略

安全 → 策略

- 题目要求最严格的防护，但没说具体操作，为此我们需要考虑的是：相应业务 VLAN 流向 INTERNET 的流量安全性 **避免 INTERNET 可直接访问内网的业务**
- 所以可分析出策略部署应该为 untrust 流向 trust，INTERNET 流向业务 VLAN，那么相反 业务流量向 INTERNET 也必须操作

策略配置

基本配置

高级控制

名称：(0~95)字符

当满足下列条件时

源安全域：

untrust

到

目的安全域：

trust

源地址：

INTERNET

多个...

到

目的地址：

总部VLAN10, 30, 4

多个...

服务簿：

Any

多个...

时间表：

多个...

应用簿：

多个...

源用户：

多个...

做如下控制

行为：

允许

拒绝

安全连接

Web 认证只能工作在trust-vr。

WEB认证

local

策略描述：(0~255)字符

确定

取消

策略配置

基本配置

高级控制

名称：(0~95)字符

当满足下列条件时

源安全域：

trust

到

目的安全域：

untrust

源地址：

总部VLAN10, 30, 4

多个...

到

目的地址：

INTERNET

多个...

服务簿：

Any

多个...

时间表：

多个...

应用簿：

多个...

源用户：

多个...

做如下控制

行为：

允许

拒绝

安全连接

Web 认证只能工作在trust-vr。

WEB认证

local

策略描述：(0~255)字符

确定

取消

启用静态路由以防止恶意动态路由

	状态	IP/掩码	下一跳	下一跳接口	协议	优先级
		0.0.0.0/0	218.5.18.2		静态	1
		9.0.0.0/30		aggregate1.9	直连	0
		9.0.0.1/32		aggregate1.9	主机	0
		10.0.0.0/30		aggregate1.91	直连	0
		10.0.0.1/32		aggregate1.91	主机	0
		172.16.10.0/24	10.0.0.2	aggregate1.91	静态	1
		172.16.10.0/24	10.0.0.2	aggregate1.91	OSPF	110
		172.16.20.0/25	10.0.0.2	aggregate1.91	OSPF	110
		172.16.30.0/26	10.0.0.2	aggregate1.91	静态	1
		172.16.30.0/26	10.0.0.2	aggregate1.91	OSPF	110
		172.16.40.0/26	10.0.0.2	aggregate1.91	静态	1
		172.16.50.0/30	10.0.0.2	aggregate1.91	OSPF	110
		172.16.100.0/24	10.0.0.2	aggregate1.91	OSPF	110
		192.168.1.0/24		ethernet0/0	直连	0
		192.168.1.1/32		ethernet0/0	主机	0
		192.168.30.0/24		tunnel1	直连	0
		192.168.30.254/32		tunnel1	主机	0
		192.168.100.0/24	10.0.0.2	aggregate1.91	OSPF	110

开启攻击防护

该截图并不完整，勾选全部启用即可

● 攻击防护

选择安全域

安全域: trust

白名单

配置

全选

☒ 全部启用 行为: 丢弃

Flood防护

☒ ICMP洪水攻击防护

警戒值: 1500 (1~50,000) 行为: 丢弃

☒ UDP洪水攻击防护

源警戒值: 1500 (0~300,000) 行为: 丢弃

目的警戒值: 1500 (0~300,000)

☒ ARP欺骗攻击防护

每个MAC最大IP数: 0 (0~1,024) 行为: 丢弃

免费ARP包发送速率: 0 (0~10) ☒ 反向查询

☒ SYN洪水攻击防护

源警戒值: 1500 (0~50,000) 行为: 丢弃

目的警戒值: ☒ 基于IP 1500 (0~50,000) ☐ 基于端口 1500 (0~50,000)

最后策略截图因如此

	2			是	untrust	trust	INTERNET(地址条目)	总部VLAN10, 30, 40 业务(地址条目)		Any	
	3			是	trust	untrust	总部VLAN10, 30, 40 业务(地址条目)	INTERNET(地址条目)		Any	

RS

```
1 RS>enable
2 RS#
3 RS#config terminal
4 RS(config)#ip vrf INTERNET
5 RS(config)#int l1
6 RS(config-if-loopback1)#ip vrf forwarding INTERNET
7 RS(config-if-loopback1)#ip address 218.5.18.2 255.255.255.255
8 RS(config-if-loopback1)#no shutdown
9 RS(config-if-loopback1)#end
```

RIPng 路由 IPv6 协议通信

类似题目

- 1 WS与RS之间配置RIPng,是VLAN30与VLAN50可以通过IPv6通信;
- 2 IPv6业务地址规划如下,其它IPv6地址自行规划:

业务	IPV6**地址**
VLAN30	2001:30::254/64
VLAN50	2001:50::254/64

注意点

- WS 和 RS 之间在网络配置规划中, 没有要求 RS 开启 vlan 30 和 50 , 这里就需要开启然后操作 ipv6 路由;
- 然后我们想想, 以前的 RIP 路由, 是不是都需要宣告邻居路由?
- 那么这里就同时需要将 vlan 100 加入到该 IPv6 的业务规划中与 WS 通信, 以维持 vlan 30 vlan 50 之间的 ipv6 业务通信
- 记住, 所有宣告给予 IPv6 协议

操作

RS

```
1 RS#config terminal
2 RS(config)#ipv6 enable
3 RS(config)#router ipv6 rip
4
5 RS(config-router)#exit
6 RS(config)#int vlan 100
7 RS(config-if-vlan100)#ipv6 address 2001:100::254/64
8 RS(config-if-vlan100)#no shutdown
9 RS(config-if-vlan100)#ipv6 router rip
10 RS(config-if-vlan100)#end
```

WS

```
1 WS(config)#ipv6 enable
2 WS(config)#router ipv6 rip
3
4 WS(config)#int vlan 30
5 WS(config-if-vlan30)#ipv6 address 2001:30::254/64
6 WS(config-if-vlan30)#no shutdown
7 WS(config-if-vlan30)#ipv6 router rip
8 WS(config-if-vlan30)#int vlan 50
9 WS(config-if-vlan50)#ipv6 address 2001:50::254/64
10 WS(config-if-vlan50)#no shutdown
11 WS(config-if-vlan50)#ipv6 router rip
12 WS(config-if-vlan50)#int vlan 100
13 WS(config-if-vlan100)#ipv6 address 2001:100::1/64
14 WS(config-if-vlan100)#no shutdown
15 WS(config-if-vlan100)#ipv6 router rip
```

最后 RS 结果应能 ping6 通信这三个地址

```
1 RS#ping6 2001:30::254
2 Sending 5 56-byte ICMP Echos to 2001:30::254, timeout is 2 seconds.
3 !!!!!
4 Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
5
6 RS#ping6 2001:50::254
7 Sending 5 56-byte ICMP Echos to 2001:50::254, timeout is 2 seconds.
8 !!!!!
9 Success rate is 100 percent (5/5), round-trip min/avg/max = 0/3/16 ms
10
11 RS#ping6 2001:100::1
12 Sending 5 56-byte ICMP Echos to 2001:100::1, timeout is 2 seconds.
13 !!!!!
14 Success rate is 100 percent (5/5), round-trip min/avg/max = 0/10/50 ms
```


OSPF MD5 安全认证

类似题型

- 1 FW、RS、WS之间配置OSPF area 0 开启基于链路的MD5认证，密钥自定义

FW 与 WS 之间连接，在 DCN 设备上需要额外上 vlan，因为设备特定如此，以上我们在前期任务一已经完成不在赘述：

ETH0/1	9.0.0.1/30 （Trust安全域）	WS	
ETH0/2	10.0.0.1/30 （untrust安全域）	WS	

注意点

- 需要注意在 OSPF 协议中声明发送 MD5 消息 key 验证
- 关于 FW 的 OSPF 操作要注意先声明 router-id

命令

code	explanation
ip vrouter trust-vr	FW 进入路由配置模式
ip ospf authentication message-digest	操作 OSPF 认证模式为消息
ip ospf message-digest-key 1 md5 admin	操作 OSPF 认证模式为 MD5 Hash admin

操作

FW

```
1 FW(config)# ip vrouter trust-vr
2 FW(config-vrouter)# router ospf
3 FW(config-router)# router-id 1.1.1.1
4 FW(config-router)# network 9.0.0.1/30 area 0
5 FW(config-router)# network 10.0.0.1/30 area 0
6 FW(config-router)# network 11.0.0.1/30 area 0
7 FW(config-router)# network 12.0.0.1/30 area 0
8 FW(config-router)# network 218.5.18.1/27 area 0
9 FW(config-router)# area 0 authentication message-digest
10
11 FW(config-router)# exit
12 FW(config-vrouter)# exit
```

```
13 FW(config)# int aggregate1.9
14 FW(config-if-aggl.9)# ip ospf authentication message-digest
15 FW(config-if-aggl.9)# ip ospf message-digest-key 1 md5 admin
16 FW(config)# int aggregate1.91
17 FW(config-if-aggl.91)# ip ospf authentication message-digest
18 FW(config-if-aggl.91)# ip ospf message-digest-key 1 md5 admin
```

这里谈及以下，可直接再 agg1 中配置 OSPF MD5 认证，也可组播 OSPF 的 LSA 认证信息

RS

```
1 CS6200-28X-EI>enable
2 CS6200-28X-EI#config terminal
3 CS6200-28X-EI(config)#router ospf 1
4 CS6200-28X-EI(config-router)#network 192.168.100.0/24 area 0
5 CS6200-28X-EI(config-router)#network 192.168.101.0/24 area 0
6 CS6200-28X-EI(config-router)#network 172.16.40.1/26 area 0
7 CS6200-28X-EI(config-router)#area 0 authentication message-digest
8 CS6200-28X-EI(config-router)#exit
9 CS6200-28X-EI(config)#int vlan 100
10 CS6200-28X-EI(config-if-vlan100)#
11 CS6200-28X-EI(config-if-vlan100)#ip ospf authentication message-digest
12 CS6200-28X-EI(config-if-vlan100)#ip ospf message-digest-key 1 md5 admin
13 CS6200-28X-EI(config-if-vlan100)#exit
```

WS

```
1 WS(config)#router ospf 1
2 WS(config-router)#network 10.0.0.0/30 area 0
3 WS(config-router)#network 172.16.100.0/24 area 0
4 WS(config-router)#network 172.16.10.1/24 area 0
5 WS(config-router)#network 172.16.20.1/25 area 0
6 WS(config-router)#network 172.16.30.1/26 area 0
7 WS(config-router)#network 172.16.50.1/26 area 0
8 WS(config-router)#network 192.168.100.0/24 area 0
9 CS6200-28X-EI(config-router)#area 0 authentication message-digest
10 WS(config-router)#exit
11 WS(config)#int vlan 9
12 WS(config-if-vlan9)#ip ospf authentication message-digest
13 WS(config-if-vlan9)#ip ospf message-digest-key 1 md5 admin
14 WS(config-if-vlan9)#exit
15 WS(config)#int vlan 100
16 WS(config-if-vlan100)#ip ospf authentication message-digest
17 WS(config-if-vlan100)#ip ospf message-digest-key 1 md5 admin
18 WS(config-if-vlan100)#exit
```

操作完成后 WS 应有两个 OSPF 邻居

```
1 WS(config)#show ip ospf neighbor
2
3 OSPF process 1:
4 Neighbor ID      Pri   State           Dead Time   Address        Interface
5 1.1.1.1          1     Full/DR         00:00:37   10.0.0.1       Vlan91
6 192.168.101.1    1     Full/DR         00:00:35   192.168.100.254 Vlan100
```

限制吞吐量-收发数据大小

类似题型

- 1 为了有效减低能耗，要求每天晚上20:00到早上07:00把RS端口指示灯全部关闭；如果RS的11端口的收包速率超过30000则关闭此端口，恢复时间5分钟，并每隔10分钟对端口的速率进行统计；为了更好地提高数据转发的性能，RS交换中的数据包大小指定为1600字节；

注意点

- 物理要求貌似无法满足(自动关闭指示灯)
- rate 速率
- sflow 恢复
- mtu 指定数据包交换大小

一般数据包如果设置 mtu，若超过阈值则会分块传输，这是 Cisco 的一种特定，DCN 目前未知

命令

code	explanation
rate-violation	操作端口收发速率与违背限定速率后执行的动作
rate-violation control shutdown recovery 300	操作违背执行动作
sflow counter-interval	sflow 协议统计速率

```
1 CS6200-28X-EI(config)#int e1/0/11
2 CS6200-28X-EI(config-if-ethernet1/0/11)#rate-violation all 30000
3 CS6200-28X-EI(config-if-ethernet1/0/11)#rate-violation control shutdown
  recovery 300
4 CS6200-28X-EI(config-if-ethernet1/0/11)#sflow counter-interval 120
5 CS6200-28X-EI(config-if-ethernet1/0/11)#exit
6 CS6200-28X-EI(config)#mtu 1600
```

FW 防火墙安全区域管理-manage

类似题型

- 1 为实现对防火墙的安全管理，在防火墙FW的Trust安全域开启PING,HTTP, SNMP功能，Untrust安全域开启SSH、HTTPS功能

注意点

- 关于这题的注意点在与所有的 Trust 区域开启相应功能
- 所有 Untrust 开启相应功能即可
- 需要注意的是操作 trust 区域后，我们要对应相应功能进入 Web GUI 界面 HTTP

操作

勾选 trust 过滤掉其他非 trust 区域添加 manage 功能即可

untrust 操作一致，不多赘述

<input type="checkbox"/>	安全域名称	类型	虚拟路由器/交换机	接口数	策略数	防病毒
<input checked="" type="checkbox"/>	trust	L3	trust-vr	2	2	
<input type="checkbox"/>	untrust	L3	trust-vr	2	2	
<input type="checkbox"/>	dmz	L3	trust-vr	0	0	
<input type="checkbox"/>	I2-trust	L2	vswitch1	0	0	
<input type="checkbox"/>	I2-untrust	L2	vswitch1	0	0	
<input type="checkbox"/>	I2-dmz	L2	vswitch1	0	0	
<input type="checkbox"/>	VPNHub	L3	trust-vr	0	0	
<input type="checkbox"/>	HA	L3	trust-vr	0	0	

1 页，总页数1

每页显示条目数 20

<input type="checkbox"/>	接口名称	状态	IP/掩码	MAC	安全域
<input type="checkbox"/>	aggregate1.9		9.0.0.1/30	0003.0f82.e55e	trust
<input type="checkbox"/>	ethernet0/0		192.168.1.1/24	0003.0f82.e555	trust

FW 复用公网-NAT 转换

类似题型

1 总部 VLAN 业务用户通过防火墙访问 Internet 时，复用公网IP： 218.5.18.9、218.5.18.10；

注意点

- 需要创建公网地址池簿
- 然后创建地址池：“总部所有业务 VLAN 用户”，将所属 vlan IP 段加入该地址簿
- 然后创建 NAT-- 采用端口复用的方式：指定 IP，动态 IP 多对一
- 是业务用户的 VLAN，防火或者 RS 的通信 VLAN 不要加进去 `vlan 10 20 30 40 50`

操作

添加业务 VLAN 地址池

配置地址簿

名称：

总部所有业务 VLAN

(1~95)字符

成员：

IP/掩码

IP地址

/

网络掩码

<input type="checkbox"/>	类型	成员
<input type="checkbox"/>	IP地址	172.16.40.0/26
<input type="checkbox"/>	IP地址	172.16.50.0/26
<input type="checkbox"/>	IP地址	172.16.30.0/26
<input type="checkbox"/>	IP地址	172.16.20.0/25
<input type="checkbox"/>	IP地址	172.16.10.0/24

添加

删除

描述：

(0~255)字符

确定

取消

配置地址簿

名称：

公网地址池

(1~95)字符

成员：

IP/掩码

IP地址

/

网络掩码

<input type="checkbox"/>	类型	成员
<input type="checkbox"/>	IP地址	218.5.18.10/32
<input type="checkbox"/>	IP地址	218.5.18.9/32

添加

删除

描述：

(0~255)字符

确定

取消

操作源 NAT 配置

源NAT配置

基本配置 更多配置

当IP地址符合以下条件时

虚拟路由器: trust-vr

源地址: 地址条目 Any

目的地址: 地址条目 Any

出流量: 出接口 ethernet0/5

服务:

将地址转换为

转换为: ☐ 出接口IP ☒ 指定IP ☐ 不转换

地址: 地址条目 公网地址池

模式: ☐ 静态(一对一转换)
☒ 动态IP(多对一转换)
☐ 动态端口(多对一转换)

描述: (0~63)字符

确定 取消

FW SSL 链接认证

类似题型

- 1 远程移动办公用户通过专线方式接入总部网络，在防火墙FW上配置，采用SSL方式实现仅允许对内网VLAN 30的访问，用户名密码均为ABC2021，地址池参见地址表；

注意点

- 新建本地用户
- 新建 SSL 向导
- 接入用户-直接添加就行
- 然后配置 "隧道接口和地址池"，"地址池"
- 操作隧道路由配置
- 添加 vlan 30 用户地址博

- 然后配置策略，将 Vlan 30 数据指向 SSL tunnel 隧道

操作

操作点：

右上角对象用户 → 本地用户 → 新建本地用户

配置 → 网络 → SSL VPN

新建本地用户

用户配置

基本配置

PnP VPN配置

名称：

ABC2021

(1~63)字符

密码：

●●●●●●

(0~31)字符

重新输入密码：

●●●●●●|

国家代码(可选)+手机号码：

请输入手机号

(0,6~15)字符

描述：

(0~127)字符

组：

选择...

IKE标识：

☒ None ☐ FQDN ☐ ASN1DN ☐ KEY-ID

账户到期日：

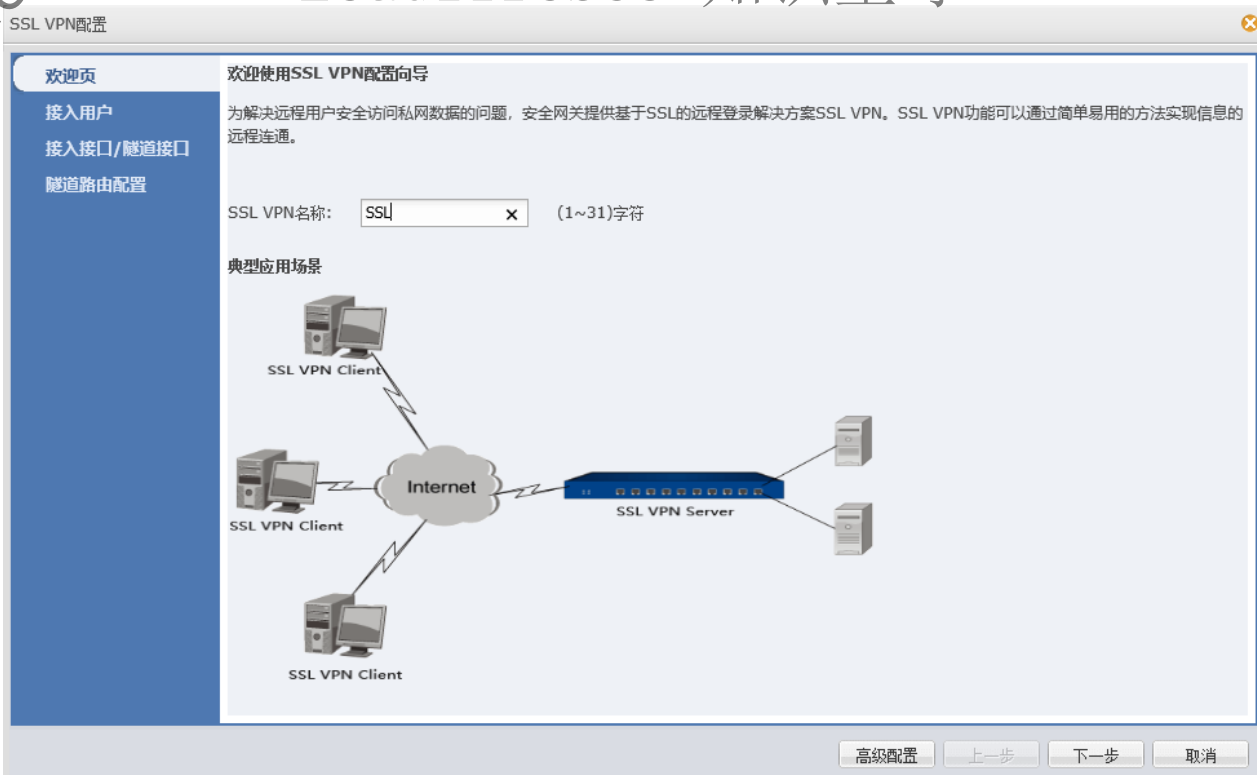
☐ 启用

如果启用了短信认证功能，短信认证码将发送到用户设置的电话号码

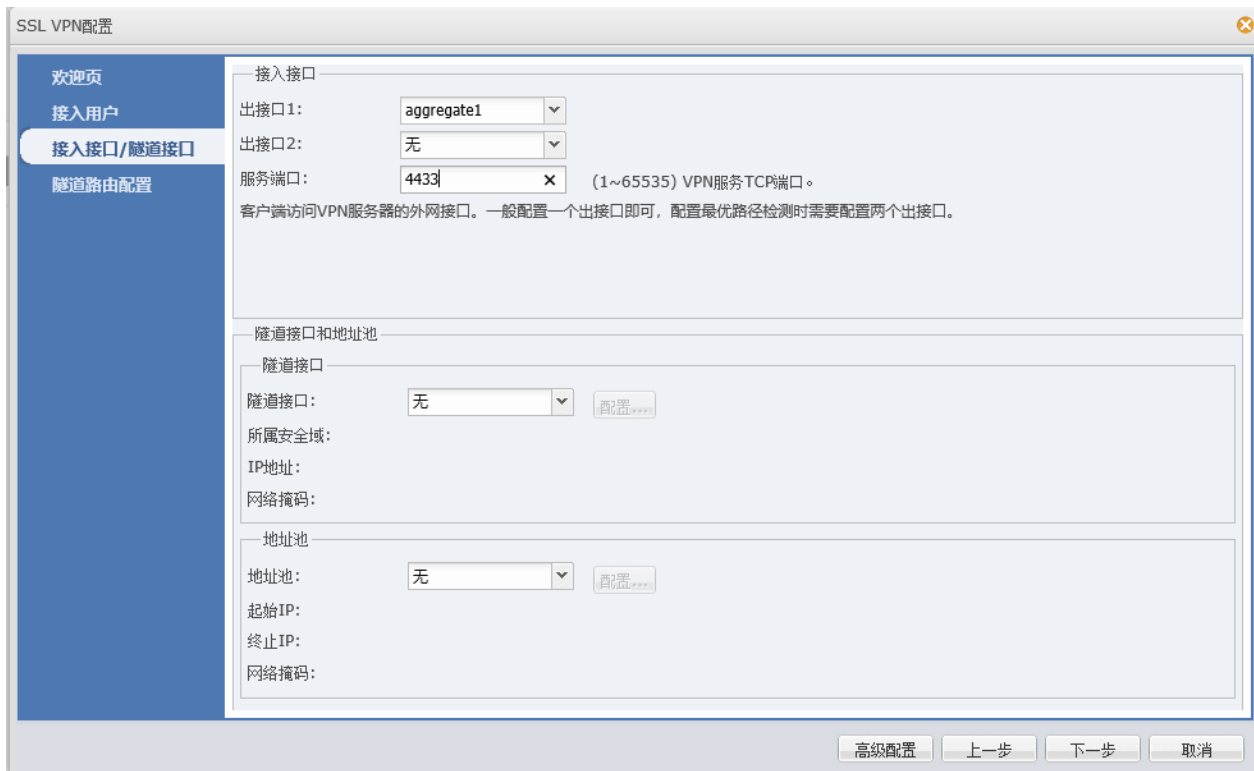
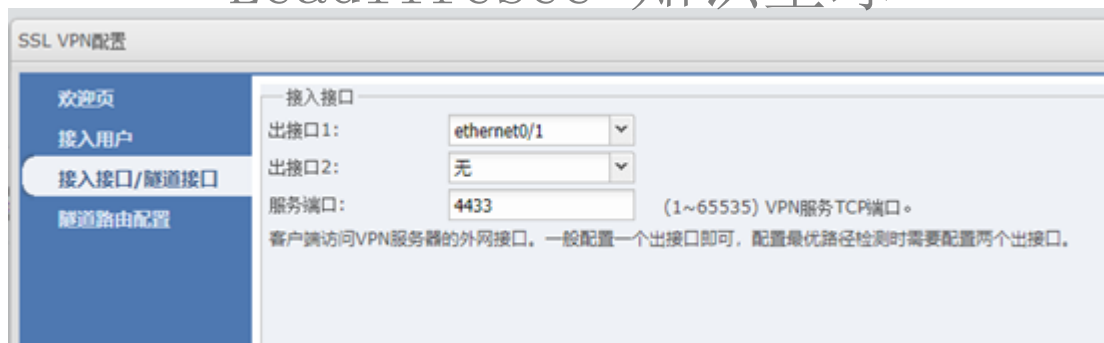
确定

取消

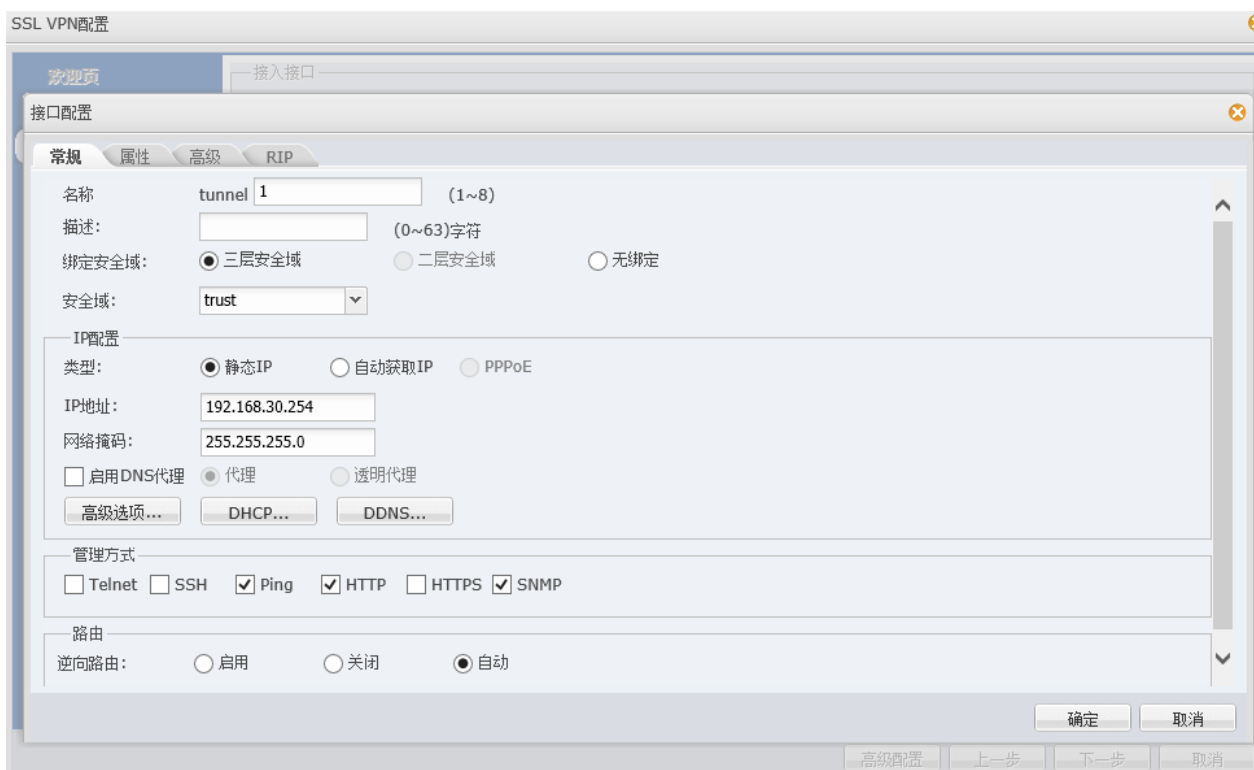
操作 SSL VPN



关于这题正确操作应当是如下，但是我对其做出一种质疑，既然我们已经在 FW 上完成的端口聚合的操作，我们应当在aggregate1 配置为出接口，并非如下，但是如果题目要求一致，可以先取消掉端口聚合再截图



新建隧道接口



建立 SSL VPN 地址池

SSL VPN配置

接入接口

出接口1: aggregate1

地址池配置

基本配置 IP用户绑定 IP角色绑定

地址池名称: SSL Pool (1~31)字符

起始IP: 192.168.10.1

终止IP: 192.168.10.20

保留起始IP:

保留终止IP:

网络掩码: 255.255.255.0 x

DNS1:

DNS2:

DNS3:

DNS4:

WINS1:

WINS2:

确定 取消

高级配置 上一步 下一步 取消

SSL VPN配置

隧道路由

IP:

网络掩码:

度量值: 35 (1~9999)

添加

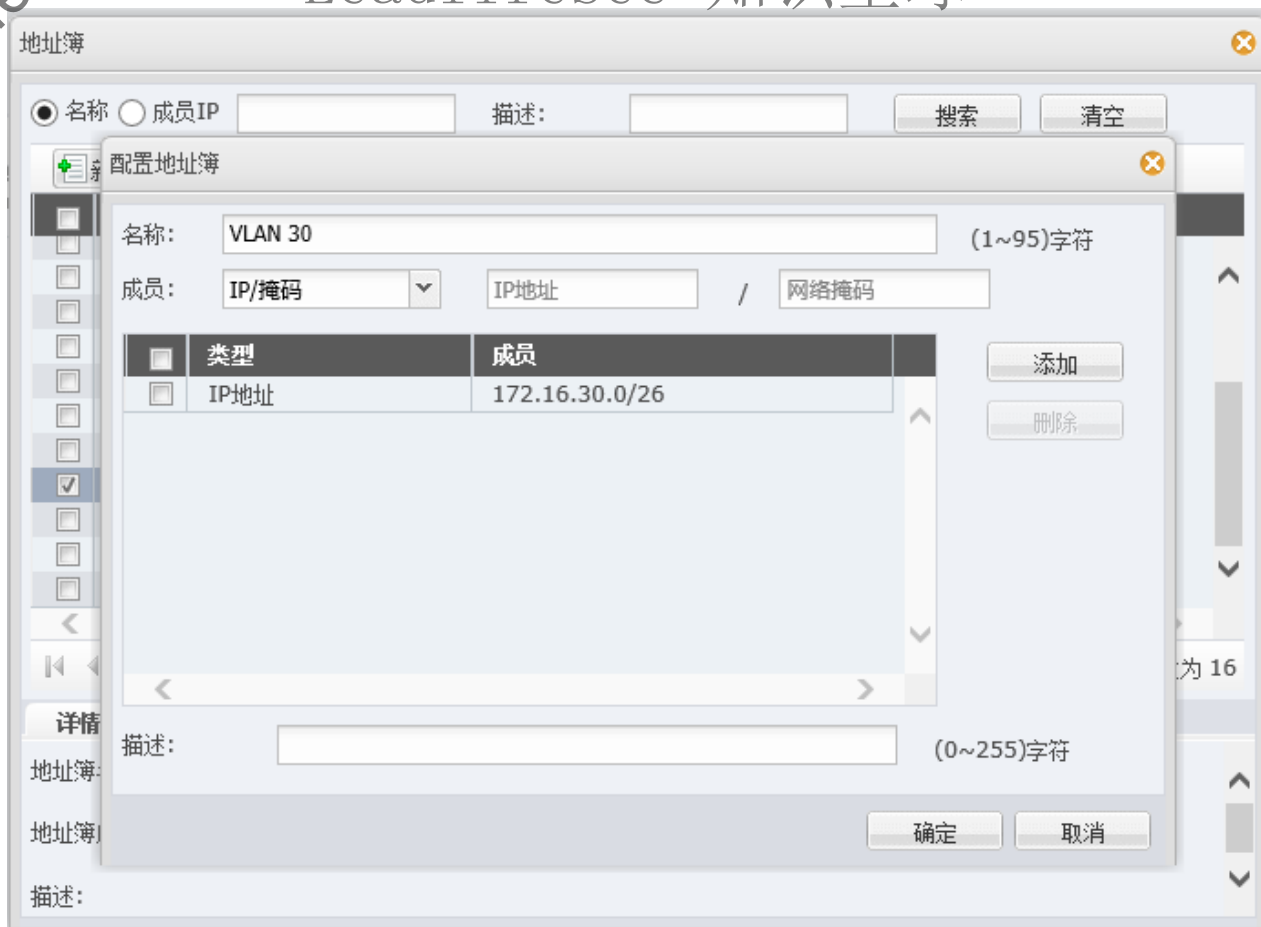
IP	网络掩码	度量值
0.0.0.0	0.0.0.0	1

删除

高级配置 上一步 完成 取消

操作策略

新建 VLAN 30 相关用户地址池



操作 VPN tunnel 策略，允许流量通过



FW Qos 流量控制-关键字过滤

类似题型

- 1 为了保证带宽的合理使用，通过流量管理功能将引流组应用数据流，上行最小带宽设置为2M，下行最大带宽设置为4M；为净化上网环境，要求在防火墙FW做相关配置，禁止无线用户周一至周五工作时间9:00-18:00的邮件内容中含有“病毒”、“赌博”的内容，且记录日志；

注意点

- QOS流量设置 流量管理 >> 应用 Qos 配置
- 无线用户地址池配置
- 时间表配置
- 关键字类别配置
- 过滤配置

操作

Qos 限制通往互联网 INTERNET 流量

应用QoS

基本配置

细粒度控制

高级配置

规则名称:

引流组

(1~31)字符

限流对象:

接口

ethernet0/5

所属安全域为untrust

匹配条件:

引流组

更多

删除

上行带宽:

最小带宽

32~100,000,000 Kbps

时间表

添加

最小带宽:2,024Kbps

删除

高级

下行带宽:

最大带宽

32~100,000,000 Kbps

时间表

添加

最大带宽:4,096Kbps

删除

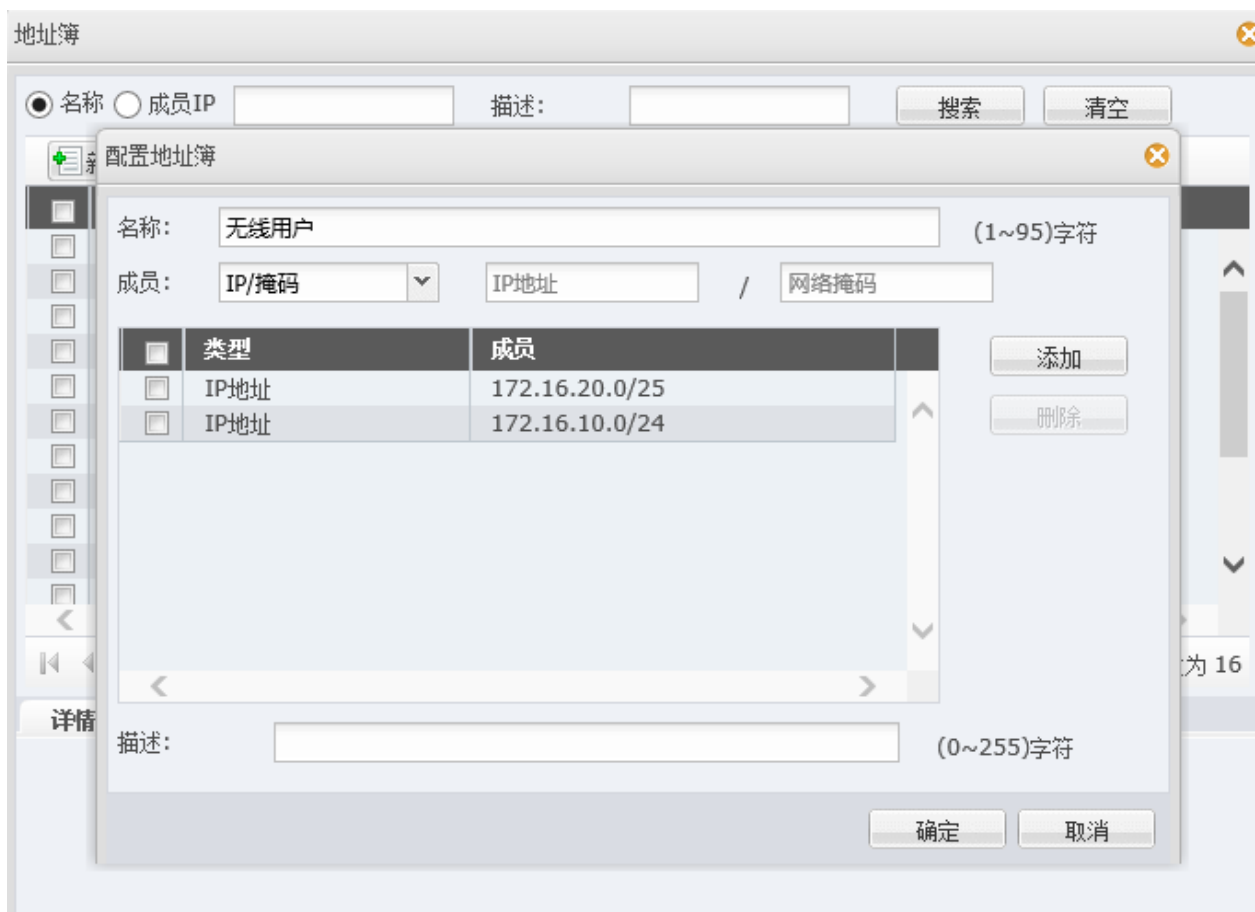
高级

确定

取消

过滤无线用户的邮件关键字内容

先创建无线用户地址簿



创建时间表 对象用户 → 时间表

时间表

新建

名称

时间表配置

时间表名称: 周一至周五 (1~31)字符

添加周期计划

预览: 星期一 星期二 星期三 星期四 星期五 09:00 到 18:00

类型: ☐ 每天 ☒ 每周的某几天 ☐ 每周一段时间

每周计划任务

计划周期: ☒ 星期一 ☒ 星期二 ☒ 星期三 ☒ 星期四
☒ 星期五 ☐ 星期六 ☐ 星期日

起始时间: 09:00

结束时间: 18:00

预览 确定 取消

绝对计划

绝对计划是一个时间范围,周期计划会在绝对计划的时间范围内生效。若不配置绝对计划,周期计划会在被功能模块引用时,立即生效

起始时间:

结束时间:

确定 取消

关闭

控制 → 网页关键字

关键字类别配置

类别名称: DB

新建 删除

关键字	类型	信任值
赌博	完全匹配	100
病毒	完全匹配	100

确定 取消

网页关键字规则配置

名称: (1~31)字符

当满足以下条件时

目的安全域:

用户:

时间表:

做如下控制

关键字类别	<input checked="" type="checkbox"/> 阻止访问	<input checked="" type="checkbox"/> 记录日志
DB	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

关键字控制范围: [所有网站](#)

控制 → 邮件过滤

邮件过滤规则配置

名称: (1~31)字符

当满足以下条件时

目的安全域:

用户:

时间表:

做如下控制

控制类型: ☐ 所有邮件 ☒ 指定邮件控制内容

控制动作:

- ☐ 阻断/审计 [发件人](#)
- ☐ 阻断/审计 [收件人](#)
- ☒ 阻断/审计 [邮件内容](#)

上述配置外邮件: ☒ 阻止发送 ☒ 记录日志

NetLog 时间表注意点参考

有关时间段配置参考说明：

参数	说明
周期时间	表示循环往复按周期生效的策略时间
工作日	配置范围从【周日】到【周六】，点击【全选】将全部选中。
时段	一个时间策略中每项最大可以设置四个具体时段。时段格式为：小时：分钟，例如：15：59 表示 15 时 59 分。时段具体设置要求：时段开始时间不能大于等于终止时间，至少要相差 1 分钟。每项中的四个时段，不能有交集。例如：时段一：12：00-15：00 时段二：13：00-14:00，时段一与 时段二存在交集，不符合时间段策略配置要求。
时间表	记录当前时间列表信息；每项时段要求必须符合如上【时段】设置具体要求；在同一个时间策略中，位于时间列表中的每项中工作日（周日到 周六）不能有重叠。例如： 第一项：周日，周三 00:00-01:00 第二项，周二，周三 02:00-03:00 在这两项中【周三】出现重复设置，尽管他们时段没有重复，但是依然造成冲突。只需修改成： 第一项：周日 00:00-01:00 第二项：周二 02:00-03:00 第三项：周三 00:00-01:00，02:00-03:00 即可消除这样的重叠冲突

NetLog 部署方式-邮件告警-SNMPv3-NTP服务器

类似题型

- 1

在公司总部的NETLOG上配置，设备部署方式为旁路模式，并配置监控接口与管理接口。增加非admin账户NETLOG2024，密码NETLOG2024，该账户仅用于用户查询设备的日志信息和统计信息。使NETLOG能够通过邮件方式发送告警信息，邮件服务器在服务器区，IP地址是172.16.10.200，端口号25，账号test，密码test；NETLOG上配置SNMPv3，用户名admin，MD5秘钥adminABC，配置日志服务器与NTP服务器，两台服务器地址：172.16.10.200；

- 部署方式有一个点，并非一定要操作初装向导来改变部署方式
- 在添加管理员用户 NETLOG2024 时需要建立一个相关用户的管理员组 NETLOG
-

操作

操作部署方式

系统管理 → 基本管理 → 基本信息 → 部署方式

部署和工作方式配置

设备部署方式

☐ 串行连接 ☒ 旁路连接

审计引擎模式

☒ 普通模式

审计服务内存使用比率

% (范围10--50%)

保存

操作监控接口

网络配置 → 网络接入 → 以太网卡

详细信息

以太网卡配置

接口名称

eth2

地址获取方式

☒ 静态 ☐ DHCP

IP地址

子网掩码

MAC地址

00:16:31:e0:d8:66

接口状态

☒ 启用 ☐ 停用

监控状态

☒ 监控

阻断发送接口

阻断目的MAC地址

☐ 指定 ☒ 不指定

保存

操作管理接口

系统管理 → 基本信息 → 管理端口

管理端口配置

认证服务器

网关服务器

认证端口

网关端口

代理端口

认证页面 ☐ 指定

本地自定义页面url:

`http://网关服务器IP:7755/custom_aaa/filename`

页面提交:

1.页面提交时指定的url地址为--`http://认证服务器IP地址:认证端口/login.cgi?act=login`

2.认证页面需要传参数:

(1)认证服务器IP--s

(2)网关端口--p

(3)用户名--username

(4)密码--usrpwd

3.提交方法:调用window.open

添加用户-先添加相应管理员组

系统管理 → 权限管理 → 管理员组

添加	删除	组名	备注
<input type="checkbox"/>		NETLOG	

系统管理 → 权限管理 → 管理员

添加系统管理员

管理员配置

名称

所属组

NETLOG

密码

••••••••

密码重复

••••••••

邮箱(用于找回密码)

IP地址

MAC地址

最大并发数

激活态

不激活

有效期

从 到

角色

配置角色组

系统管理 → 权限管理 → 角色管理

添加角色

配置角色

角色名称

netlog

关联用户组

radius
默认组

关联用户

关联选择

全选

确定

全选

配置该账户权限

系统管理 → 权限管理 → 权限分配

选择角色

netlog

权限列表			<input type="checkbox"/> 全选	<input type="checkbox"/> 全选
<input checked="" type="checkbox"/> 系统状态	⌵	<input type="checkbox"/>	<input type="checkbox"/> 浏览	<input type="checkbox"/> 添加
<input checked="" type="checkbox"/> 系统管理	⌵	<input type="checkbox"/>	<input type="checkbox"/> 浏览	<input type="checkbox"/> 添加
<input checked="" type="checkbox"/> 基本信息	⌵	<input type="checkbox"/>	<input type="checkbox"/> 浏览	<input type="checkbox"/> 添加
<input checked="" type="checkbox"/> 高可用性	⌵	<input type="checkbox"/>	<input type="checkbox"/> 浏览	<input type="checkbox"/> 添加
<input checked="" type="checkbox"/> 备份恢复	⌵	<input type="checkbox"/>	<input type="checkbox"/> 浏览	<input type="checkbox"/> 添加
<input checked="" type="checkbox"/> 系统升级	⌵	<input type="checkbox"/>	<input type="checkbox"/> 浏览	<input type="checkbox"/> 添加
<input checked="" type="checkbox"/> 权限管理	⌵	<input type="checkbox"/>	<input type="checkbox"/> 浏览	<input type="checkbox"/> 添加
<input checked="" type="checkbox"/> 系统日志	⌵	<input type="checkbox"/>	<input checked="" type="checkbox"/> 浏览	<input type="checkbox"/> 添加
<input checked="" type="checkbox"/> 日志查看	⌵	<input type="checkbox"/>	<input checked="" type="checkbox"/> 浏览	<input type="checkbox"/> 添加
<input checked="" type="checkbox"/> 网络配置	⌵	<input type="checkbox"/>	<input type="checkbox"/> 浏览	<input type="checkbox"/> 添加
<input checked="" type="checkbox"/> 安全管理	⌵	<input type="checkbox"/>	<input type="checkbox"/> 浏览	<input type="checkbox"/> 添加
<input checked="" type="checkbox"/> 策略管理	⌵	<input type="checkbox"/>	<input type="checkbox"/> 浏览	<input type="checkbox"/> 添加
<input checked="" type="checkbox"/> 应用管理	⌵	<input type="checkbox"/>	<input type="checkbox"/> 浏览	<input type="checkbox"/> 添加
<input checked="" type="checkbox"/> 内容管理	⌵	<input type="checkbox"/>	<input type="checkbox"/> 浏览	<input type="checkbox"/> 添加
<input checked="" type="checkbox"/> 统计报表	⌵	<input type="checkbox"/>	<input type="checkbox"/> 浏览	<input type="checkbox"/> 添加
<input checked="" type="checkbox"/> 统计报表	⌵	<input type="checkbox"/>	<input checked="" type="checkbox"/> 浏览	<input type="checkbox"/> 添加
<input checked="" type="checkbox"/> 全文检索	⌵	<input type="checkbox"/>	<input type="checkbox"/> 浏览	<input type="checkbox"/> 添加
<input checked="" type="checkbox"/> 报表定制	⌵	<input type="checkbox"/>	<input type="checkbox"/> 浏览	<input type="checkbox"/> 添加
<input checked="" type="checkbox"/> 其他	⌵	<input type="checkbox"/>	<input type="checkbox"/> 浏览	<input type="checkbox"/> 添加

操作邮件警告

策略管理 → 报警策略 → 邮件管理

报警邮箱设置

邮箱名称

default

服务器

172.16.10.200

端口号

25

帐号

test

密码

••••

消息数限制

100

抄送

提示

如有多个抄送邮箱，之间以分号(';')相隔

保存

发送测试邮件

系统管理 → 基本信息 → 远程管理

SNMP V3配置	
用户	<input type="text" value="admin"/>
认证密钥(MD5)	<input type="text" value="adminABC"/>
加密密钥(DES)	<input type="text" value="snmpcrypt"/>
<input type="button" value="保存配置"/>	

系统日志输出设置	
系统日志输出IP地址	<input type="text" value="172.16.10.200"/>
<input type="button" value="保存"/>	

添加 NTP 服务器

系统管理 → 基本信息 → NTP 配置

 添加NTP服务器

NTP配置	
NTP服务器名称	<input type="text" value="NTP"/>
服务器类型	<input type="radio"/> 域名 <input checked="" type="radio"/> IP地址
服务器域名	<input type="text"/>
服务器IP地址	<input type="text" value="172.16.10.200"/> <input type="button" value="x"/>
<input type="button" value="添加保存"/>	

NetLog 监控 URL 记录-HTTP访问记录-网段聊天记录-邮件收发记录

涉及题型

- 1 在公司总部的NETLOG上配置，监控工作日（每周一到周五）期间PC1网段访问的URL中包含xunlei的HTTP访问记录，并且邮件发送告警。监控PC2网段所在网段用户的即时聊天记录。监控内网所有用户的邮件收发访问记录。

leadlife 注意点

- 题目中要操作一个邮件发送警告

操作

配置时间表

策略管理 → 时间策略

详细设置

绝对时间

从0000-00-00到0000-00-00

恢复默认值

格式为:YYYY-MM-DD

按月为周期

从到日

月周期时段

(1)00:00--00:00(2)00:00--00:00(3)00:00--00:00(4)00:00--00:00

设定

重置

按周为周期

周日周一周二周三周四周五周六全选

周周期时段

(1)00:00--23:59(2)00:00--00:00(3)00:00--00:00(4)00:00--00:00

设定

重置

周周期设定的详细时间列表

清空时间列表

自动整合排序

序号	周日	周一	周二	周三	周四	周五	周六	时间段一	时间段二
1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	00:00--23:59	00:00--00:00

操作监控 HTTP

应用管理 → 应用规则 → 规则配置

应用规则配置

应用类别

全部应用分类
网站访问
邮件收发
即时聊天
网络传输
P2P应用

应用项目

全部应用项目
网页浏览
网页提交

添加应用规则

应用规则配置

高级选项

应用选项

匹配内容

应用选项

匹配关系

Step: 2/5

上一步

应用规则配置

时间对象

监控工作日

任意时间

匹配动作

不记录

记录

记录且网页报警

记录且邮件报警

阻断

阻断且网页报警

上一步

下一步

应用规则配置

规则对象: IP地址

IP + 掩码

IP: 172.16.30.0Mask: 255.255.255.192

IP段

从 0.0.0.0到 0.0.0.0

上一步

下一步

操作监控聊天

应用规则配置

应用类别

全部应用分类

网站访问

邮件收发

即时聊天

网络传输

P2P应用

应用项目

全部应用项目

MSN

QQ

Fetion

UC

POPO

应用规则配置

高级选项 ☐

应用选项

无

无

匹配内容

上一步

应用规则配置

时间对象

监控工作日

任意时间

匹配动作

不记录

记录

记录且网页报警

记录且邮件报警

阻断

阻断且网页报警

上一步

应用规则配置

规则对象: IP地址

IP + 掩码

IP: 172.16.40.0

Mask: 255.255.255.192

IP段

从 0.0.0.0

到 0.0.0.0

上一步

操作监控所有内网邮件收发记录

应用规则配置

应用类别

全部应用分类

网站访问

邮件收发

即时聊天

网络传输

P2P应用

应用项目

全部应用项目

SMTP

POP3

IMAP

应用规则配置

高级选项 ☐

应用选项

发件人

包含

匹配内容

上一步

应用规则配置

时间对象

监控工作日

任意时间

匹配动作

不记录

记录

记录且网页报警

记录且邮件报警

阻断

阻断且网页报警

上一步

应用规则配置

规则对象: IP地址

IP+掩码

IP: 0.0.0.0Mask: 0.0.0.0

IP段

从 0.0.0.0 到 0.0.0.0

上一步

最后应有如下三条监控操作

序号	优先级	用户(组)	规则内容	时间对象	动作	状态
1	500	IP用户:0.0.0.0/0.0.0.0	邮件收发	任意时间	记录	激活
2	500	IP用户:172.16.40.0/255.255.255.192	即时聊天	任意时间	记录	激活
3	500	IP用户:172.16.30.0/255.255.255.192	网站访问 URL地址 包含 xunlei	监控工作日	记录且邮件报警	激活

NetLog 配置应用及其应用组

涉及题型

- 1

NETLOG 配置应用及应用组“P2P视频下载”，UDP协议端口号范围65551-65651，在周一至周五8：00-20：00监控内网中所有用户的“P2P视频下载”访问记录；

注意点

- 需要注意到 题目中还有时间点 所以我们需要再创建一个时间表

操作

操作策略管理 P2P

策略管理 → 应用管理 → 应用组

添加自定义应用组

自定义应用组

应用组名称 P2P视频下载

保存

添加自定义应用

自定义应用配置

自定义名称

所属应用组 ▼

协议类型 ▼

服务器IP

服务器端口 从 到 ×

保存

操作时间表以监控内网

策略管理 → 时间策略

详细设置

从 到 恢复默认值 格式为:YYYY-MM-DD

按月为周期 ☐ 从 到 日

月周期时段 (1) (2) (3) (4) 设定 重置

按周为周期 ☒ 周日 ☐ 周一 ☒ 周二 ☒ 周三 ☒ 周四 ☒ 周五 ☒ 周六 ☐ 全选 ☐

周周期时段 (1) (2) (3) (4) 设定 重置

周周期设置的详细时间列表

清空时间列表

自动整合排序

序号	周日	周一	周二	周三	周四	周五	周六	时间段一	时间段二
1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="08:00--20:00"/>	<input type="text" value="00:00--00:00"/>

应用管理 → 应用规则 → 规则配置

应用规则配置

应用类别

应用项目

应用规则配置

高级选项 ☒应用选项 等于

<input type="checkbox"/> 浩方游戏	<input type="checkbox"/> 反恐精英	<input type="checkbox"/> 大话西游-上海	<input type="checkbox"/> 大话西游-江苏	<input type="checkbox"/> 泡泡堂1
<input type="checkbox"/> 泡泡堂2	<input type="checkbox"/> 传奇1	<input type="checkbox"/> 传奇2	<input type="checkbox"/> 传奇3	<input checked="" type="checkbox"/> P2P视频下载

应用选项

匹配关系

匹配内容

上一步

下一步

应用规则配置

时间对象

监控工作日

P2P病毒下载

任意时间

匹配动作

不记录

记录

记录且网页报警

记录且邮件报警

阻断

阻断且网页报警

上一步

下一步

应用规则配置

规则对象: IP地址

IP + 掩码

IP: 0.0.0.0

Mask: 0.0.0.0

IP段

从 0.0.0.0

到 0.0.0.0

上一步

下一步

Netlog ARP 数量统计-身份识别

涉及题型

- NETLOG配置对内网ARP数量进行统计，要求30分钟为一个周期；NETLOG配置开启用户识别功能, 对内网所有MAC地址进行身份识别；

操作

ARP 数量统计-操作周期

策略管理 → ARP 策略

ARP统计

ARP统计配置

ARP统计

激活

不激活

统计周期

30

分钟

保存

操作身份识别

用户识别

用户识别

识别接口

默认

DCSM

DCBI

说明

默认审计用户识别方式 (支持PPPOE拨号用户自动识别)

详细配置

方法

按IP识别

按MAC识别

保存

NetLog 报表定制

涉及题型

- 1 NETLOG配置统计出用户请求站点最多前20排名信息，发送到邮箱为bn2024@chinaskills.com

操作

增加定制报表

名称: 请求站点最多前20排名

报表类型: 用户请求站点最多排名

范围: 全部

时间段1: 0时 到 0时

时间段2: 0时 到 0时

TopN排名: 20

生成报表周期: 每天 0时

接收邮箱: bn2024@chinaskills.com

保存

WAF 配置与接入

涉及题型

- 1 公司内部有一台网站服务器直连到WAF，地址是RS上VLAN10网段内的第五个可用地址，端口是8080，配置将服务访问日志、WEB防护日志、服务监控日志信息发送syslog日志服务器，IP地址是服务器区内第六个可用地址，UDP的514端口；

注意点

可能一些同学和我一样，刚见到这题，都不知道这题目在说些什么，那么这里我带着大家一起分析一下

- 地址为 RS 上 VLAN 10 网段内的第五个可用地址：172.16.10.5
- 题目中表示 公司内部有一台网站服务器直连到WAF ：操作 WAF 中的服务-服务管理 来管理服务器

- 又表示需要将日志发送给服务器区内第六个可用地址：172.16.10.6

这样我们再继续解题

操作

WAF 介入服务器操作服务管理

服务 → 服务管理

新建服务

*服务名称:	<input type="text" value="service"/>	字母开头，字母、数字和下划线组成，长度为1到20
*服务类型:	<div>HTTP</div>	
*主机地址:	<input type="text" value="172.16.10.5"/>	点分十进制整数，形如：192.168.23.4
*主机端口:	<input type="text" value="8080"/>	(1~65535)
域名:	<input type="text"/>	
策略集:	<div>无</div>	
*字符集:	<div></div>	
MAC绑定:	<input type="checkbox"/> 启用服务与MAC地址绑定	
*记录访问日志:	<div><input checked="" type="radio"/>是 <input type="radio"/>否</div>	
*记录防护日志:	<div><input checked="" type="radio"/>是 <input type="radio"/>否</div>	
链路绑定:	<div>br_default</div>	

WAF 接入服务器操作日志管理

配置 → 日志配置

基本配置 日志导出 日志清空 日志服务器

日志服务器

*名称:	<input type="text" value="syslog"/>	字母开头，字母、数字和下划线组成，长度为1到20
*服务器IP:	<input type="text" value="172.16.10.6"/>	
*端口:	<input type="text" value="514"/>	(1~65535)
协议类型:	<div>UDP</div>	
*日志类型:	<div><input checked="" type="checkbox"/> 服务访问日志 <input checked="" type="checkbox"/> WEB防护日志 <input checked="" type="checkbox"/> 服务监控日志</div>	

本功能将导出所选日志到syslog日志服务器

确定 取消

涉及题型

- 1 在公司总部的WAF上配置，阻止常见的WEB攻击数据包访问到公司内网服务器，防止某源IP地址在短时间内发送大量的恶意请求，影响公司网站正常服务。

注意点

- 操作基本防护，阻止常见 Web 攻击
- 防止 CC 攻击，开启流量过大访问防护

操作

策略 → 基本攻击防护

基本攻击防护

策略名称: P-xxx

基本攻击防护

状态: ☒ 开启 ☐ 关闭 选择是否开启基本攻击防护。推荐: 是。

应答体检测

状态: ☒ 启用 是否启用应答体检测。此选项对性能有一定影响, 建议在对应答时间没有特殊要求的情况下使用。

防护动作

动作: 阻止 防护动作可以选择允许 (允许继续请求服务器资源), 阻止 (阻止请求, 返回403页面, 或, 相应的错误过滤页面), 重定向 (重定向请求到配置的重定向URL), 阻断 (在设置的阻断时间内, 阻止同源IP的请求)。

默认攻击防护类型

☒ SQL注入攻击防护 ☒ 跨站脚本攻击防护 ☒ 操作系统注入命令 ☒ 远程文件包含攻击防护 ☒ 目录遍历攻击防护 ☒ 其他

策略 → 暴力浏览防护

暴力浏览攻击防护

策略名称: P-xxx

暴力浏览防护

状态: ☒ 开启 ☐ 关闭 选择是否开启暴力浏览防护。

单IP允许的最大请求数: 3000 请求计数的最大值, 计数满足最大值时, 将执行已配置的防护动作, 数值范围: 1-32767

防护动作

动作: 阻止 防护动作可以选择阻止 (阻止请求, 返回403页面, 或, 相应的错误过滤页面)。

确定 重置

WAF 限定请求阈值避免 DDOS 与 缓冲区溢出

涉及题目

- 1 大量请求的确认值是：10秒钟超过3000次请求；编辑防护策略，定义HTTP请求体的最大长度为256，防止缓冲区溢出攻击；

注意点

- 这里与 WAF 基本防护配置有点相似
- 不过需要注意 WAF 有关 HTTP 类似的配置均 属于协议配置

操作

限定请求阈值

策略 → 暴力浏览防护

暴力浏览攻击防护		
策略名称: P-xxx		
暴力浏览防护		
状态:	<input checked="" type="radio"/> 开启 <input type="radio"/> 关闭	选择是否开启暴力浏览防护。
单IP允许的最大请求数:	3000	请求计数的最大值，计数满足最大值时，将执行已配置的防护动作，数值范围：1-32767
防护动作 ^		
动作:	阻止	防护动作可以选择阻止（阻止请求，返回403页面，或，相应的错误过滤页面）。
<div>确定 重置</div>		

限定 HTTP 请求数据最大长度

策略 → 协议规范检测

记得比赛的截图要勾选开启

协议规范检测

策略名称: P-xxx

协议规范检测

状态: ☒ 开启 ☐ 关闭 开启对HTTP协议各组成元素的长度限制功能。这些检查能够有效阻断缓冲溢出等攻击。推荐: 是

请求头域值的最大长度: 8192 定义请求报头值的最大长度。推荐:8192

请求头名称的最大长度: 64 定义报头名称的最大长度。推荐:64

请求头域的最大个数: 20 定义了一个请求能够包含的最多报头个数。推荐: 20

请求体的最大长度: 256 请求body的最大长度。POST请求有一个包含表单参数和值的请求body。推荐: 32768

表单参数值的最大长度: 512 指定表单参数值的最大长度。推荐: 512

表单参数名称的最大长度: 64 指定表单参数名称的最大长度。推荐:64

请求行的最大长度: 4096 请求行是请求中的第一行。包括Method、URL和HTTP版本。最大请求行长度应该与最大URL长度近似。

查询参数值的最大长度: 512 定义请求报头值的最大长度。推荐: 512

查询参数名称的最大长度: 64 指定参数名称的最大长度。推荐:64

查询参数的最大个数: 40 查询参数的最大个数。推荐:40

禁止的请求协议: 指定禁止的请求协议(HTTP/0.9, HTTP/1.0, HTTP/1.1), 多项配置以半角逗号分隔

COOKIE最大个数: 40 所有的Cookie可以被包含在一个"Cookie: "首部中(格式为name=value, 以半角分号隔开)。此项限制了cookie的数量。推荐: 40

禁止的方法: 指定禁止的HTTP方法, 多项配置以半角逗号分隔

禁止的HOST: 指定禁止的host, 多项配置以半角逗号分隔

防护动作

WAF 爬虫防护-文件上传策略-编辑防护策略-禁止访问特殊文件

- 1 WAF上配置开启爬虫防护功能, 当爬虫标识为360Spider, 自动阻止该行为; WAF上配置阻止用户上传ZIP、DOC、JPG、RAR格式文件; WAF上配置编辑防护策略, 要求客户机访问内部网站时, 禁止访问*.bat的文件;

这题没啥注意点, 纯粹操作

操作

标识爬虫

对象库 → 爬虫标识组

先添加 360Spider 的爬虫标识再操作爬虫标识组

爬虫标识组 爬虫标识

爬虫标识组		
爬虫标识组名称: <input type="text"/> 添加 字母开头, 字母、数字和下划线组成, 长度为1到20		
序号	选择	爬虫标识组名称
1	<input type="checkbox"/>	DefaultRobots
2	<input type="checkbox"/>	pe1
全选 <input type="checkbox"/> 删除所选		

爬虫标识

爬虫标识特征:

添加

爬虫标识特征

▼

等于

▼

360Spider

查询

序号	选择	爬虫标识特征
1	<input type="checkbox"/>	360Spider

全选

☐

删除所选

爬虫防护

策略 → 爬虫防护

爬虫防护

策略名称:

P-xxx

▼

爬虫防护

状态:

☒ 开启

☐ 关闭

爬虫标识组:

pe1

▼

防护动作

▲

动作:

阻止

▼

特殊文件格式上传阻止

策略 → 输入参数验证

策略名称：

P-xxx

参数验证

状态：

开启

关闭

选择是否开启输入参数验证。推荐：是。

防护动作

动作：

阻止

防护动作可以选择允许（允许继续请求服务器资源），阻止（阻止请求，返回403页面，或，相应的错误过滤页面），重定向（重定向请求到配置的重定向URL）。

上传文件格式特征检测

DOC

DOCX

GIF

JPG

JPEG

PDF

PNG

RAR

XLSZIP

检测上传文件的格式特征，文件格式不正确，不允许其上传。

未检测文件动作：

允许

若上传文件格式特征检测都不勾选，则默认检测动作为允许。

创建参数

类型	匹配方式	匹配表达式	操作
<div>查询参数名称</div>	<div>正则匹配</div>	<div></div>	<div>添加</div>
表单参数名称	字符串匹配	userName	<div></div>
表单参数值	字符串匹配	admin	<div></div>
表单参数值	正则匹配	admin	<div></div>

用于检测请求的查询参数和表单参数，可选择正则匹配或字符串匹配。匹配表达式支持中英文字符，最长32字符。

确定

重置

禁止访问特殊文件

策略 → 黑白名单

黑白名单

策略名称：

P-xxx

黑白名单

状态：

开启

关闭

类型	黑白名单种类	匹配模式	值
<div>黑名单</div>	<div>URI</div>	<div>正则匹配</div>	*.bat

- 1 WAF上配置，使用WAF的漏洞立即扫描功能检测服务器（172.16.10.100）的安全漏洞情况，要求包括信息泄露、SQL注入、跨站脚本编制；

操作

漏扫 → 配置

新建“漏洞扫描”任务

基本配置

*任务名称:

service

字母开头，字母、数字和下划线组成，长度为1到20

*任务添加方式:

☒单任务

☐批量任务

*扫描目标:

172.16.10.100

反向代理模式下，请填写服务器真实地址。
IP:port或域名:port，端口可不填（默认为80）

*执行方式:

☒立即执行

☐将来执行

☐周期执行

*扫描内容:

☒信息泄露

☒SQL注入

☐操作系统命令

☒跨站脚本编制

☐认证不充分

☐拒绝服务

高级配置

确定

取消

WAF 邮件-短信上报威胁情报

涉及题型

- 1 在公司总部的WAF上配置， WAF设备的内存使用率超过50%每隔5分钟发送邮件和短信给管理，邮箱bn2024@digitalchina.com，手机13912345678；
- 2 在公司总部的WAF上配置，将设备状态告警、服务状态告警信息通过邮件（发送到bn2024@digitalchina.com）及短信方式(发送到13812345678)发送给管理员；

操作

配置 → 告警配置

告警管理-设备状态告警

日志空间检测:	<input checked="" type="radio"/> 是 <input type="radio"/> 否
设备占用空间:	80 % 请在日志配置模块中编辑, 超过此值则告警
内存检测:	<input checked="" type="radio"/> 是 <input type="radio"/> 否
内存占用空间:	50 % 大小请输入 1 到 95(%), 超过此值则告警
告警开关:	<input checked="" type="radio"/> 开启 <input type="radio"/> 关闭
发送间隔:	5 分钟
告警方式:	<input checked="" type="checkbox"/> 邮件 <input checked="" type="checkbox"/> 短信
接收邮箱:	bn2024@digitalchina.com 邮件之间用半角逗号分隔, 仅允许输入10个邮箱地址
接收手机号码:	13912345678 手机号码之间用半角逗号分隔, 仅允许输入10个手机号码

保存 重置

告警管理-WEB攻击告警

告警开关:	<input checked="" type="radio"/> 开启 <input type="radio"/> 关闭
发送间隔:	5 分钟
告警方式:	<input checked="" type="checkbox"/> 邮件 <input checked="" type="checkbox"/> 短信
接收邮箱:	bn2024@digitalchina.com 邮件之间用半角逗号分隔, 仅允许输入10个邮箱地址
是否发送摘要信息:	<input type="radio"/> 否 <input checked="" type="radio"/> 是
接收手机号码:	13812345678 手机号码之间用半角逗号分隔, 仅允许输入10个手机号码

保存 重置

WS DHCP 下发三层发现 AP 被动上线

涉及题目

- WS上配置DHCP, 管理VLAN为VLAN101, 为AP下发管理地址, 保证完成AP注册; 为无线用户VLAN10,20, 有线用户VLAN 30,40下发IP地址;

注意点

- AP 上需要配置 DHCP 服务, 通过 Option 43 特殊字段下发
- RS 需要配置 DHCP 服务, 为业务用户下发 IP 地址, 同时做 DHCP 中继转发 WS DHCP 报文以 AP 被动发现

WS 配置 DHCP 服务下发 IP

```
1 WS#config
2 WS(config)#service dhcp
3 WS(config)#ip dhcp pool AP
4 WS(dhcp-ap-config)#network-address 192.168.101.0 255.255.255.0
5 WS(dhcp-ap-config)#default-router 192.168.101.1

6 WS(dhcp-ap-config)#option 43 hex 0104C0A86401 `这里注意, 是 AP 的 VLAN 100 管
理地址 hex`
7 WS(dhcp-ap-config)#exit
8
9 WS(config)#ip dhcp pool 10
10 WS(dhcp-10-config)#network-address 172.16.10.0 255.255.255.0
11 WS(dhcp-10-config)#default-router 172.16.10.1
12 WS(dhcp-10-config)#exit
13
14 WS(config)#ip dhcp pool 20
15 WS(dhcp-20-config)#network-address 172.16.20.0 255.255.255.128
16 WS(dhcp-20-config)#default-router 172.16.20.1
17 WS(dhcp-20-config)#exit
18
19 WS(config)#ip dhcp pool 30
20 WS(dhcp-30-config)#network-address 172.16.30.0 255.255.255.192
21 WS(dhcp-30-config)#default-router 172.16.30.1
22 WS(dhcp-30-config)#exit
23
24 WS(config)#ip dhcp pool 40
25 WS(dhcp-40-config)#network-address 172.16.40.0 255.255.255.192
26 WS(dhcp-40-config)#default-router 172.16.40.1
27 WS(dhcp-40-config)#exit
28
29 WS(config)#ip forward-protocol udp bootps
```

RS 开启 DHCP 中继转发 DHCP 服务器 AC VLAN

```
1 CS6200-28X-EI(config)#service dhcp
2 CS6200-28X-EI(config)#ip forward-protocol udp bootps
3 CS6200-28X-EI(config)#int vlan 101
4 CS6200-28X-EI(config-if-vlan101)#ip helper-address 192.168.100.1
5 CS6200-28X-EI(config-if-vlan101)#exit
```

以上操作完毕后, AP 应当获取到 IP 地址, 且 AC 与 AP 可通信

```
1 WS#show ip dhcp binding
2 Total dhcp binding items: 1, the matched: 1
3 IP address           Hardware address       Lease expiration       Type
4 192.168.101.2        00-03-0F-82-2D-B0      Tue Jan 03 01:39:00 2006 Dynami
5
6 WS#ping 192.168.101.2
7 Sending 5 56-byte ICMP Echos to 192.168.101.2, timeout is 2 seconds.
8 !!!!!
```

WS 操刀 AP 三层被动上线

```
1 WS(config)#wireless
2 WS(config-wireless)#enable
3 WS(config-wireless)#no auto-ip-assign
4 WS(config-wireless)#static-ip 192.168.100.1
5 WS(config-wireless)#ap authentication none
6 WS(config-wireless)#discovery ip-list 192.168.101.2
7 WS(config-wireless)#ap database 00-03-0F-82-2D-B0
```

完成上述步骤后，AP 应当成功上线

```
1 WS#show wireless ap status
2
3 (*) Peer Managed IP Address           Profile Status
   Status           Age
4 -----
5 00-03-0f-82-2d-b0 192.168.101.2           1      Managed
   Success          0d:00:00:04
```

WS WLAN SSID 与安全配置

涉及题型

- 1 在NETWORK下配置SSID，需求如下：
- 2 1: NETWORK 1下设置SSID ABC2021, VLAN10, 加密模式为wpa-personal,其口令为ABCE2024;
- 3 2: NETWORK 2下设置SSID GUEST, VLAN20不进行认证加密,做相应配置隐藏该SSID;

注意点

- 加密模式需要注意
- NETWORK 2 需要注意，不进行加密认证，却隐藏

操作

(1)

```
1 WS(config-wireless)#network 1
2 WS(config-network)#ssid ABC2021
3 WS(config-network)#vlan 10
4 WS(config-network)#security mode wpa-personal
5 WS(config-network)#wpa key ABCE2024
```

(2)

```
1 WS(config-network)#network 2
2 WS(config-network)#ssid GUEST
3 WS(config-network)#vlan 20
4 WS(config-network)#hide-ssi
```

WS WLAN 本地认证

涉及题型

```
1 NETWORK 1开启内置portal+本地认证的认证方式，账号为ABC密码为ABCE2024；
```

注意点

- 开启内置 portal
- 开启本地认证

命令

code	explanation
captive-portal	进入 WS 本地认证模块
authentication-type internal	设置认证模式为内置认证(内置本地认证)，需要注意，这里并非本地认证，可以当作一个登录模式
verification local	配置为本地认证
group a	给予绑定用户的用户组
interface ws- network 1	加入绑定无线节点

操作

```
1 WS(config)#captive-portal
2 WS(config-cp)#enable
3
4 WS(config-cp)#authentication-type internal
5 WS(config-cp)#user ABC
6 WS(config-cp-local-user)#password ABCE2024
7 WS(config-cp-local-user)#group a
8 WS(config-cp-local-user)#exit
9
10 WS(config-cp)#configuration 1
11 WS(config-cp-instance)#verification local
12 WS(config-cp-instance)#group a
13 WS(config-cp-instance)#interface ws-network 1
```

WS WLAN 接入控制-用户隔离

涉及题型

- 1 配置SSID GUEST每天早上0点到6点禁止终端接入；GUEST最多接入10个用户，并对GUEST网络进行流控，上行1M，下行2M；配置所有无线接入用户相互隔离；


```
1 WS(config-cp)#exit
2 WS(config)#wireless
3 WS(config-wireless)#network 2
4 WS(config-wireless)#max-clients 10
5 WS(config-network)#time-limit from 00:00 to 06:00 weekday all
6 WS(config-network)#qos max-bandwidth up 1024
7 WS(config-network)#qos max-bandwidth down 2048
8 WS(config-network)#exit
9
10
11 这里需要将无线的用户所处端口加入隔离组
12 WS(config-ap-profile)#station-isolation allowed vlan add 10
13 WS(config-ap-profile)#station-isolation allowed vlan add 20
14 WS(config-ap-profile)#radio 1
15 WS(config-ap-profile-radio)#station-isolation
```

WS WLAN AP 版本检测自动升级-延迟 AP 发送帧时间 -配置 AP 超时状态-AP 脱离 AC 情况自主工作

类似题型

- 1 配置当AP上线，如果AC中储存的Image版本和AP的Image版本号不同时，会触发AP自动升级；配置AP发送向无线终端表明AP存在的帧时间间隔为1秒；配置AP失败状态超时时间及探测到的客户端状态超时时间都为2小时；配置AP在脱离AC管理时依然可以正常工作；

操作

检测 AP 版本不符自动升级操作

- ```
1 WS(config)#wireless
2 WS(config-wireless)#ap auto-upgrade
```

```
1 WS(config-wireless)#ap profile 1
2 WS(config-ap-profile)#radio 1
3 WS(config-ap-profile-radio)#beacon-interval 1000
```

### 操作 AP 超时状态-AP 脱离 AC 情况自主工作

```
1 WS(config-wireless)#wireless ap anti-flood agetime 120 `超时探测时间`
2 WS(config-wireless)#agetime ap-failure 2 `状态失败超时时间`
3
4 WS(config-wireless)#ap profile 1
5 WS(config-ap-profile)#ap ?
6 escape 开启或关闭AP 逃生模式
7
8 WS(config-ap-profile)#ap escape
9 WS(config-ap-profile)#ap escape client-persist
```

### WS WALN 低于 num% 信号值禁止连接-AP 威胁探测

#### 涉及题目

- 1 为防止外部人员蹭网，现需在设置信号值低于50%的终端禁止连接无线信号；为防止非法AP假冒合法SSID，开启AP威胁检测功能；

#### 操作

#### 操作低于阈值禁止链接

```
1 WS(config-wireless)#ap profile 1
2 WS(config-ap-profile)#radio 1
3 WS(config-ap-profile-radio)#client-reject rssi-threshold 50
4 WS(config-ap-profile-radio)#exit
5 WS(config-ap-profile)#exit
```

#### 操作 AP 威胁探测

```
1 WS(config-wireless)#wids-security fakeman-ap-managed-ssid
2
3 WS(config-wireless)#wids-security ap-de-auth-attack
4
5 WS(config-wireless)#wids-security managed-ap-ssid-invalid
6
7 WS(config-wireless)#end
8
9 WS#wireless ap profile apply 1
```

关于这题，我建议这里全打上，多打不扣分

## 罕见赛题的总结

**RS、WS运行静态组播路由和因特网组管理协议第二版本；PC1启用组播，使用VLC工具串流播放视频文件1.mpg，组地址228.10.10.7，端口：3456，实现PC2可以通过组播查看视频播放。**

| VLAN 40 RS ETH1/0/4 | 172.16.40.1/26 | PC2 |
|---------------------|----------------|-----|
| VLAN 30 WS ETH1/0/3 | 172.16.30.1/26 | PC1 |

### 操作

```
1 ip igmp snooping
2 ip igmp snooping vlan 100
3 ip igmp snooping vlan 100 static-group 228.10.10.5 source 192.168.100.1
 interface e1/0/
```

```
1 RS(config)#ip igmp snooping vlan 100
2 RS(config)#ip igmp snooping vlan 100 l2-general-querier-version 2
```

```
1 RS(config)#int vlan 100
2 RS(config-if-vlan100)#ip igmp version 2
```