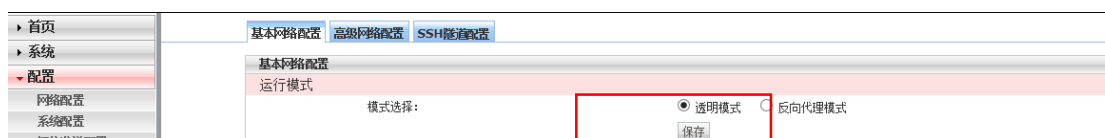
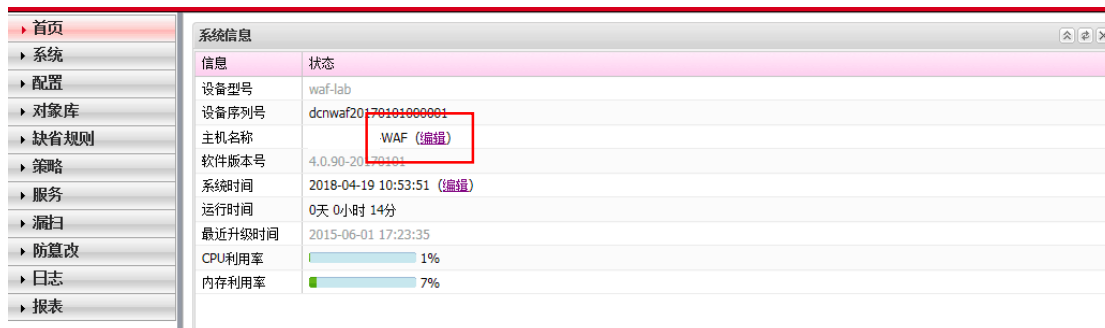


评分标准中参数请以实际题目为准

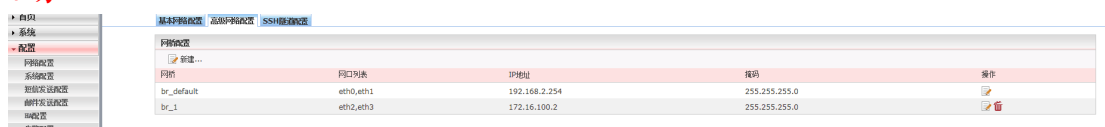
## 一、第一阶段任务一

1、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。(5 分)

2 分



1 分



截图含 IP 地址：匹配参数表 WAF IP 地址 子网掩码 网口列表：eth2 和 eth3

2 分

2、根据网络拓扑图所示，按照 IP 地址参数表，对 DCRS 的名称、各接口 IP 地址进行配置。(5 分)

hostname DCRS 1 分

interface Vlan 1001

ip address 10.0.0.2 255.255.255.252 (匹配参数表) 0.5 分

interface Vlan 1002

ip address 10.0.0.5 255.255.255.0 (匹配参数表) 0.5 分

interface Vlan10

ip address 172.16.10.1 255.255.255.0 (匹配参数表) 0.5 分

interface Vlan20

ip address 172.16.30.1 255.255.255.128 (匹配参数表) 0.5 分

interface Vlan30

ip address 172.168.30.1 255.255.255.192 (匹配参数表) 0.5 分

interface Vlan40

ip address 192.168.40.1 255.255.255.0 (匹配参数表) 0.5 分

interface Vlan100

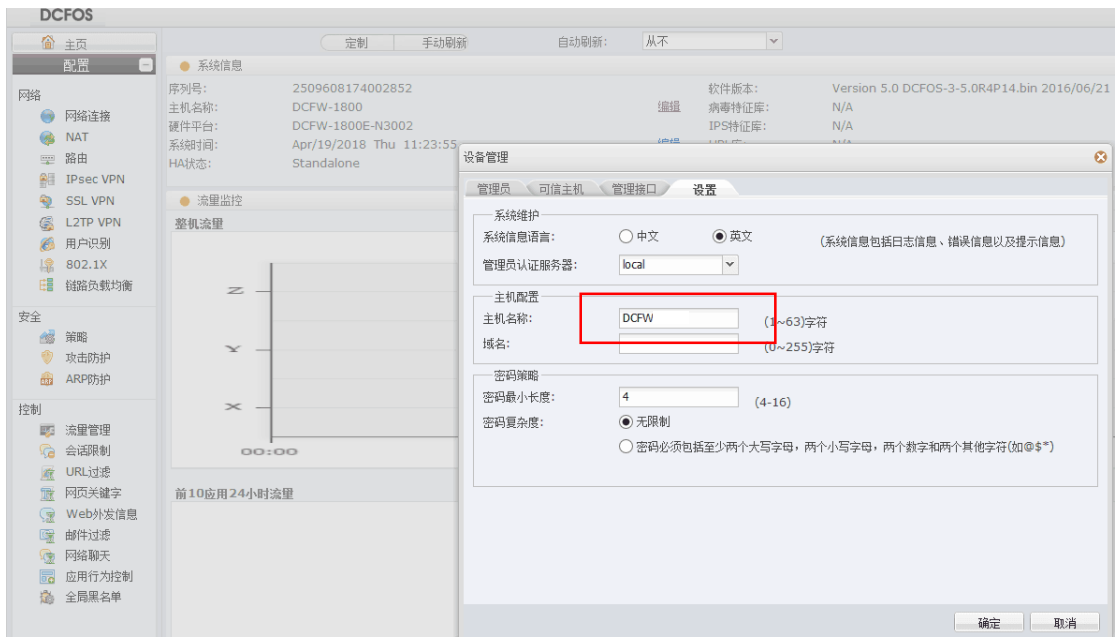
ip address 192.168.100.1 255.255.255.0 (匹配参数表) 0.5 分

interface Vlan200

ip address 172.16.200.1 255.255.255.0 (匹配参数表) 0.5 分

3、根据网络拓扑图所示，按照 IP 地址参数表，对 DCFW 的名称、各接口 IP 地址

进行配置。(5分)



截图含主机名称信息; 2分

<input type="checkbox"/>	ethernet0/1		218.5.18.1/27	0003.0f83.cb11	untrust	0
<input type="checkbox"/>	ethernet0/2		10.0.0.1/30	0003.0f83.cb12	trust	0
<input type="checkbox"/>	ethernet0/3		10.0.0.10/30	0003.0f83.cb13	dmz	0
<input type="checkbox"/>	ethernet0/4		0.0.0.0/0	0003.0f83.cb14	NULL	0
<input type="checkbox"/>	ethernet0/5		0.0.0.0/0	0003.0f83.cb15	NULL	0
<input type="checkbox"/>	ethernet0/6		0.0.0.0/0	0003.0f83.cb16	NULL	0
<input type="checkbox"/>	ethernet0/7		0.0.0.0/0	0003.0f83.cb17	NULL	0
<input type="checkbox"/>	ethernet0/8		0.0.0.0/0	0003.0f83.cb18	NULL	0
<input type="checkbox"/>	tunnel1		192.168.10.254/24	0000.0000.0000	untrust	0

ethernet0/1 接口 IP 正确 1分

ethernet0/2 接口 IP 正确 1分

ethernet0/3 接口 IP 正确 1分

4、根据网络拓扑图所示，按照 IP 地址参数表，对 DCSW 的各接口 IP 地址进行配置。(5分)

Hostname DCWS 2分

!

interface Vlan1002

ip address 10.0.0.6 255.255.255.0 252 (匹配参数表) 1分

!

interface Vlan100

ip address 192.168.100.254 255.255.255.0 (匹配参数表) 1分

!

interface Vlan101

ip address 192.168.101.1 255.255.255.0 (匹配参数表) 1分

5、根据网络拓扑图所示，按照 IP 地址参数表，对 DCBI 的名称、各接口 IP 地址进行配置。(5分)



截图含主机名称信息；1分

接口名称	物理地址方式	IP地址	子网掩码	MAC地址	接口状态	监控状态
eth0	静态	192.168.5.254	255.255.255.0	00:16:31:f7:f2:00	启用	未监控
eth1	静态	0.0.0.0	255.255.255.252	00:16:31:f7:f2:00	启用	未监控
eth2	静态	0.0.0.0	0.0.0.0	00:16:31:f7:f2:00	禁用	监控
eth3	静态	0.0.0.0	0.0.0.0	00:16:31:f7:f2:00	禁用	监控
eth4	静态	0.0.0.0	0.0.0.0	00:16:31:f7:f2:00	禁用	未监控
eth5	静态	0.0.0.0	0.0.0.0	00:16:31:f7:f2:00	禁用	未监控

截图含如下信息：

IP 地址 192.168.40.253 子网掩码 255.255.255.0 2分

接口状况： 启用 1分

监控状态： 监控 1分

6、根据网络拓扑图所示,按照 IP 地址参数表,在 DCRS 交换机上创建相应的 VLAN,并将相应接口划入 VLAN。(5分)

DCRS #show vlan

10	VLAN0010	Static	ENET	Ethernet1/0/1 (T)
20	VLAN0020	Static	ENET	Ethernet1/0/1 (T)
30	VLAN0030	Static	ENET	Ethernet1/0/1 (T)
40	VLAN0040	Static	ENET	
	Ethernet1/0/6			
	Ethernet1/0/7			
	Ethernet1/0/8			
	Ethernet1/0/9			
100	VLAN0100	Static	ENET	Ethernet1/0/1 (T)
200	VLAN0200	Static	ENET	Ethernet1/0/10
	Ethernet1/0/11			
	Ethernet1/0/12			
	Ethernet1/0/13			
	Ethernet1/0/14			
	Ethernet1/0/15			
	Ethernet1/0/16			
	Ethernet1/0/17			
	Ethernet1/0/18			
	Ethernet1/0/19			
	Ethernet1/0/20			
	Ethernet1/0/21			
	Ethernet1/0/22			
	Ethernet1/0/23			
	Ethernet1/0/24			
1001	VLAN1001	Static	ENET	Ethernet1/0/2
1002	VLAN1002	Static	ENET	Ethernet1/0/1 (T)

7、采用静态路由的方式,全网络互连。(10分)

DCRS:

ip route 0.0.0.0/0 10.0.0.1 指向外网默认路由 2分

ip route 192.168.101.0/24 10.0.0.6

ip route 192.168.100.0/24 10.0.0.6

DCWS:

ip route 0.0.0.0/0 10.0.0.5 指向外网默认路由 2分

DCFw:

状态	IP/掩码	下一跳	下一跳接口	协议	优先级	度量
	0.0.0.0/0	218.5.18.2	ethernet0/1	静态	1	0
	10.0.0.0/30		ethernet0/2	直连	0	0
	10.0.0.1/32		ethernet0/2	主机	0	0
	172.16.10.0/24	10.0.0.2	ethernet0/2	静态	1	0
	172.16.20.0/25	10.0.0.2	ethernet0/2	静态	1	0
	172.16.100.0/24	10.0.0.2	ethernet0/2	静态	1	0
	192.168.1.0/24		ethernet0/0	直连	0	0
	192.168.1.1/32		ethernet0/0	主机	0	0
	192.168.10.0/24		tunnel1	直连	0	0
	192.168.10.254/32		tunnel1	主机	0	0
	192.168.40.0/24	10.0.0.2	ethernet0/2	静态	1	0
	192.168.100.0/24	10.0.0.2	ethernet0/2	静态	1	0
	192.168.101.0/24	10.0.0.2	ethernet0/2	静态	1	0
	218.5.18.0/27		ethernet0/1	直连	0	0
	218.5.18.1/32		ethernet0/1	主机	0	0

6分错一条扣一分扣完为止

8、防火墙做必要的配置实现内网对外网访问。(20分)

ID	源地址(原始)	目的地址(原始)	服务	出接口 / 下一跳虚拟路由器	转换为	模式	HA组	日志	Track	描述
1	Any	Any	Any	ethernet0/1	出接口IP	动态端口	0	关闭		

Nat 配置正确 10分

ID	名称	状态	有效性	源安全域	目的安全域	源地址	目的地址	源用户/用户组	服务	应用	特征	行为	命中数	描述
2		是	是	trust	untrust	Any(地址组)	Any(地址组)		Any			0	0	
3		是	是	trust	dmz	Any(地址组)	Any(地址组)		Any			0	0	
6		是	是	dmz	dmz	Any(地址组)	Any(地址组)		Any			0	0	

策略配置合理 10分

二、第一阶段任务二

1、在 DCFW 上配置，连接 LAN 接口开启 PING,HTTP,HTTPS, telnet 功能，连接 Internet 接口开启 PING、HTTPS 功能；连接 netlog 接口为 DMZ 区域，合理配置策略，让内网用户能通过网管 netlog。(6分)

接口配置

常规 属性 高级 RIP

名称: ethernet0/2

描述: (0~63)字符

绑定安全域: ☒ 三层安全域 ☐ 二层安全域 ☐ 无绑定

安全域: trust

IP配置

类型: ☒ 静态IP ☐ 自动获取IP ☐ PPPoE

IP地址: 10.0.0.1

网络掩码: 255.255.255.252

☐ 启用DNS代理 ☒ 代理 ☐ 透明代理

高级选项... DHCP... DDNS...

管理方式

☒ Telnet ☐ SSH ☒ Ping ☒ HTTP ☒ HTTPS ☐ SNMP

路由

逆向路由: ☐ 启用 ☐ 关闭 ☒ 自动

确定 取消

第 1 页, 总页数 1 每页显示条目数 20 显示表项 1 - 8 总数为 8

接口名称	状态	IP/掩码	MAC	安全域	接入用户/IP数	流入带宽(bps)
ethernet0/0		192.168.1.1/24	0003.0fa3.1700	trust	0	2.98K
ethernet0/1		218.5.18.1/27	0003.0fa3.1701	untrust	0	0
ethernet0/2		10.0.0.1/30	0003.0fa3.1702	trust	0	0
ethernet0/3		10.0.0.10/30	0003.0fa3.1703	dmz	0	0
ethernet0/4		0.0.0.0/0	0003.0fa3.1704	NULL	0	0
ethernet0/5		0.0.0.0/0	0003.0fa3.1705	NULL	0	0
ethernet0/6		0.0.0.0/0	0003.0fa3.1706	NULL	0	0
ethernet0/7		0.0.0.0/0	0003.0fa3.1707	NULL	0	0

ID	名称	状态	有效性	源安全域	目的安全域	源地址	目的地址	角色/用户/用户组	服务
7		✓	是	trust	untrust	Any(地址条目)	Any(地址条目)		Any
3		✓	是	trust	untrust	无线用户(地址条目)	Any(地址条目)		DNS
2		✓	是	trust	untrust	无线用户(地址条目)	Any(地址条目)	UNKNOWN(角色)	Any
1		✓	是	trust	untrust	Any(地址条目)	Any(地址条目)		Any
4		✓	是	untrust	trust	Any(地址条目)	Any(地址条目)		TCP-6661
5		✓	是	trust	dmz	Any(地址条目)	Any(地址条目)		Any
6		✓	是	VPNHub	trust	Any(地址条目)	Any(地址条目)		Any

- 1、接口 IP 地址（连接 PC2：匹配参数表、连接 DCRS：匹配参数表）2 分
- 2、接口安全域（连接 PC2：UNTRUST、连接 DCRS：TRUST）1 分
- 3、管理方式（连接 PC2 ping https 打钩 连接 DCRS ping http HTTPS）1 分
- 4、接口状态（连接 PC2：绿色、连接 DCRS：绿色、连接 netlog：绿色）1 分
- 5.策略配置正确得 1 分

2、DCFW 配置 LOG，记录 NAT 会话，Server IP 为 172.16.100.10. 开启 DCFW 上 snmp 服务，server IP 172.16.100.10 团体字符为 public。（6 分）

日志服务器配置

主机名称: 172.16.100.10 (A.B.C.D)/(1~255)字符

绑定方式: ☒ 虚拟路由器: trust-vr ☐ 源接口:

协议: UDP

端口: 514 (1~65535),缺省值: 514

日志类型: ☐ 事件日志 ☐ 配置日志 ☐ 安全日志 ☒ NAT日志 ☐ 网络日志 ☐ 会话日志 ☐ 上网日志 ☐ 调试日志 ☐ NBC日志

确定 取消

日志服务器配置正确 2 分

DCFS

系统管理 对象

事件日志 安全日志 配置日志 网络日志 会话日志 NAT日志 上网日志 NBC日志

☒ 启用 ☐ 记录主机名

☒ 缓存 最大缓存大小: 2097152 (4096~2097152) 字节

☐ 日志服务器 查看日志服务器

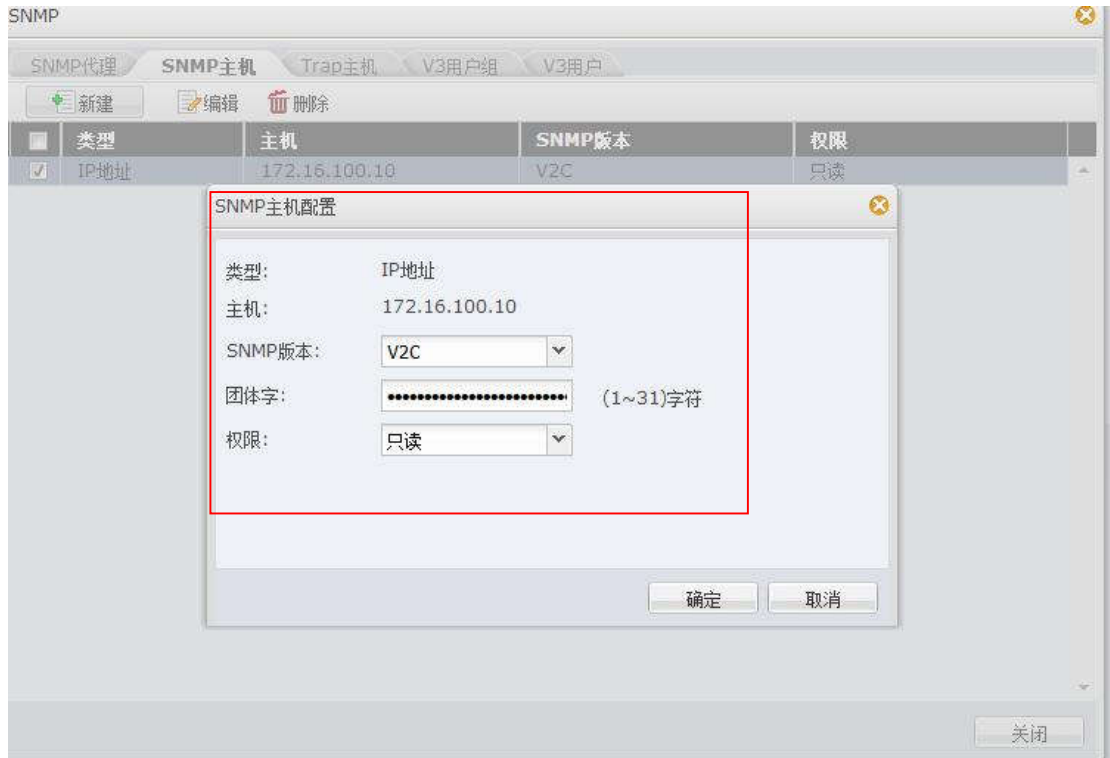
日志分发方式: 明文日志

☐ 使用分布式日志

☒ 轮询方式外发 ☐ 按源IP Hash方式外发

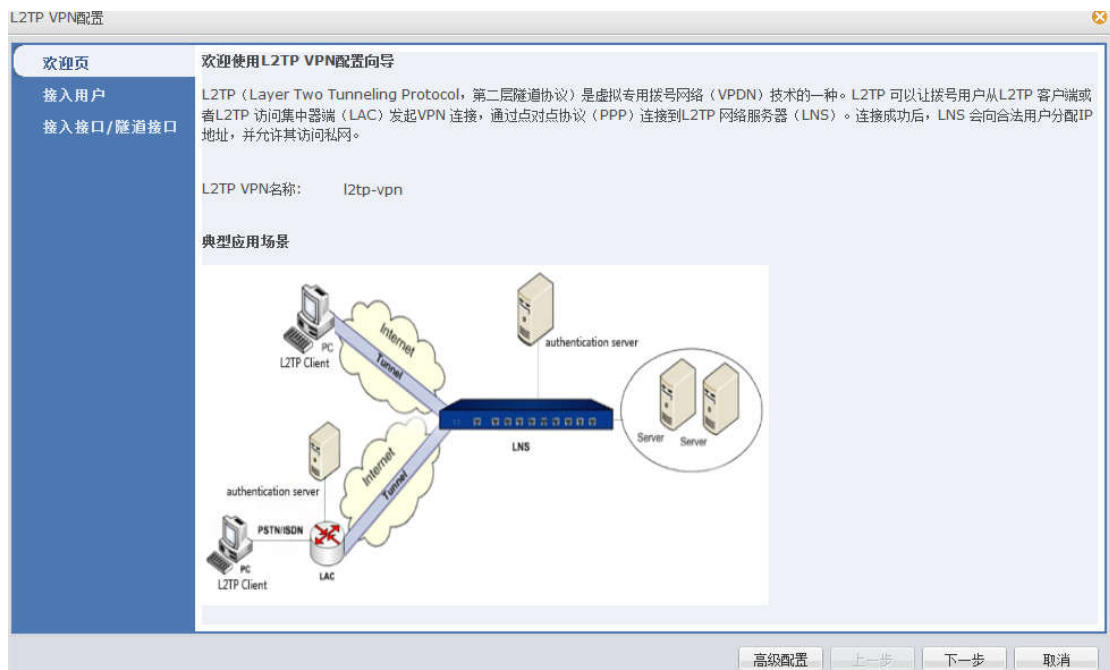
确定 取消

开启 nat 日志记录 2 分



Snmp 服务配置正确 2 分

3、DCFW 做相应配置,使用 l2tp 方式让外网移动办公用户能够实现对内网的访问,用户名密码为 **dcn2018**, VPN 地址池参见地址表;合理配置安全策略。(6 分)





L2TP VPN配置

欢迎页

接入用户

接入接口/隧道接口

选择用于用户认证的AAA服务器

请添加用户认证所需的AAA服务器，列表中AAA服务器上的用户均可进行登录。

L2TP VPN配置只支持认证，不支持计费，即使选择了支持计费功能的AAA服务器。

AAA服务器: local 域名: (1~31)字符 ☐ 用户域名验证

添加

AAA服务器	域	用户域名验证
local		no

删除

高级配置 上一步 下一步 取消

## 账号、AAA 服务器配置 2 分

L2TP VPN配置

欢迎页

接入用户

接入接口/隧道接口

接入接口

出接口: ethernet0/1

隧道接口和地址池

隧道接口

隧道接口: tunnel1 配置...

所属安全域: untrust

IP地址: 192.168.10.254

网络掩码: 255.255.255.0

地址池

地址池: vpn 配置...

起始IP: 192.168.10.1

终止IP: 192.168.10.20

引用IPsec隧道

L2TP over IPsec:

高级配置 上一步 完成 取消

	tunnel1		192.168.10.254/24		0000.0000.0000	untrust	0	0	0
--	---------	--	-------------------	--	----------------	---------	---	---	---

L2TP VPN

新建

删除

刷新

清除

名称	用户数	接口	隧道接口	地址池
l2tp-vpn	1	ethernet0/1	tunnel1	vpn

主页

配置

网络

网络连接

NAT

路由

IPsec VPN

SSL VPN

L2TP VPN

用户识别

Web认证参数配置

SSO代理

在线用户

在线用户: 所有

用户名	类型	角色/用户组	IP	接口/虚拟路由器	在线时长	操作
dcn2018			192.168.10.1	tunnel1	0 天 0 小时 4 分 37 秒	退出



ID	名称	状态	有效性	源安全域	目的安全域	源地址	目的地址	角色/用户/用户组	服务	应用	特征	行为	命中数	备注
8		✓	是	trust	untrust	Any(地址条目)	Any(地址条目)	CNS				✓	115	
9		✓	是	trust	untrust	wifi(地址条目)	Any(地址条目)	UNKNOWN(黄色)	Any			⚠	0	
2		✓	是	trust	untrust	Any(地址条目)	Any(地址条目)	Any				✓	255	
3		✓	是	trust	dmz	Any(地址条目)	Any(地址条目)	Any				✓	0	
6		✓	是	dmz	trust	Any(地址条目)	Any(地址条目)	Any				✓	0	
7		✓	是	dmz	untrust	Any(地址条目)	Any(地址条目)	Any				✓	0	
10		✓	是	untrust	trust	192.168.100.0/24(地址条目)	Any(地址条目)	Any				✓	0	
11		✓	是	untrust	trust	Any(地址条目)	ipv4-ethernet0/1(地址条目)	tcp6666				✓	0	

隧道接口-地址池配置 2 分 192.168.10.0

用户	用户组	账户到期日
dcn2018		-

策略配置 2 分

4、出于安全考虑，无线用户移动性较强，无线用户访问 Internet 是需要采用实名认证，在防火墙上开启 web 认证，账号密码为 2018web。（6 分）

**Web认证参数配置** SSO代理 在线用户

**认证模式**

认证模式: ☒ HTTP ☐ HTTPS ☐ SSO-NTLM ☐ 关闭

HTTP端口:  (1~65535),缺省值:8181

HTTPS端口:  (1~65535),缺省值:44433

**用户登录**

同一用户: ☒ 只允许在一个客户端登录 ☐ 允许多个客户端同时登录

某用户已登录: ☐ 踢出已登录用户 ☒ 禁止同名用户再次登录

**更多设置**

空闲超时时间:  (0~24\*60) 分钟

客户端心跳超时:  (10~3600\*24)秒

☐ 重认证时间间隔:  (10~60\*24)分钟

☐ 强制重登录间隔:  (10~60\*24\*100)分钟

重定向URL:  (1~127)字符

支持通过在URL中指定关键字来传送用户名和密码,对应的关键字为\$USER, \$PWD或\$HASHPWD(通常\$PWD和\$HASHPWD参数二选一即可)。

例如 example.com/oa/login.do?username=\$USER&password=\$HASHPWD

### Web 认证参数配置 2 分

ID	名称	状态	有效性	源安全域	目的安全域	源地址	目的地址	角色/用户/用户组	服务	应用	特征	行为	命中率
8		是	是	trust	untrust	Any(默认全部)	Any(默认全部)		DNS			115	
9		是	是	trust	untrust	wifi(默认全部)	Any(默认全部)	UNKNOWN(黑色)	Any			0	
2		是	是	trust	untrust	Any(默认全部)	Any(默认全部)		Any			235	

### 策略配置 2 分

本地服务器	本地用户	用户	用户组	账户到期日
local	所有用户	2018web		-

### 账号配置 2 分

- 5、为了合理利用网络出口带宽,需要对内网用户访问 Internet 进行流量控制,园区总出口带宽为 200M,对除无线用户以外的用户限制带宽,每天上午 9:00 到下午 6:00 每个 IP 最大下载速率为 2Mbps,上传速率为 1Mbps; (6 分)

地址簿

名称

成员IP

描述:

搜索

清空

新建

编辑

删除

	地址簿名称	成员	描述
<input type="checkbox"/>	ipv4.ethernet0/0 subnet	192.168.1.1/24	
<input type="checkbox"/>	ipv4.ethernet0/1	218.5.18.1/32	
<input type="checkbox"/>	ipv4.ethernet0/1 subnet	218.5.18.1/27	
<input type="checkbox"/>	ipv4.ethernet0/2	10.0.0.1/32	
<input type="checkbox"/>	ipv4.ethernet0/2 subnet	10.0.0.1/30	
<input type="checkbox"/>	ipv4.ethernet0/3	10.0.0.10/32	
<input type="checkbox"/>	ipv4.ethernet0/3 subnet	10.0.0.10/30	
<input type="checkbox"/>	ipv4.tunnel1	192.168.10.254/32	
<input type="checkbox"/>	ipv4.tunnel1 subnet	192.168.10.254/24	
<input checked="" type="checkbox"/>	wifi	172.16.20.0/25, 17...	
<input type="checkbox"/>	有线用户	172.16.100.0/24, 1...	

第 1 页, 总页数 1

每页显示条目数 20

显示表项 1 - 14 总数为 14

详情

关联项

地址簿名称:

wifi

地址簿成员:

172.16.20.0/25, 172.16.10.0/24

描述:

## 地址设置 2 分

时间表

新建

编辑

删除

	名称	活跃	周期计划	绝对计划
<input checked="" type="checkbox"/>	days	活跃	每天 09:00 到 18:00	

第 1 页, 总页数 1

每页显示条目数 20

显示表项 1 - 1 总数为 1

时间表详情:

时间表名称:

days

活跃:

活跃

周期计划:

每天 09:00 到 18:00

绝对计划:

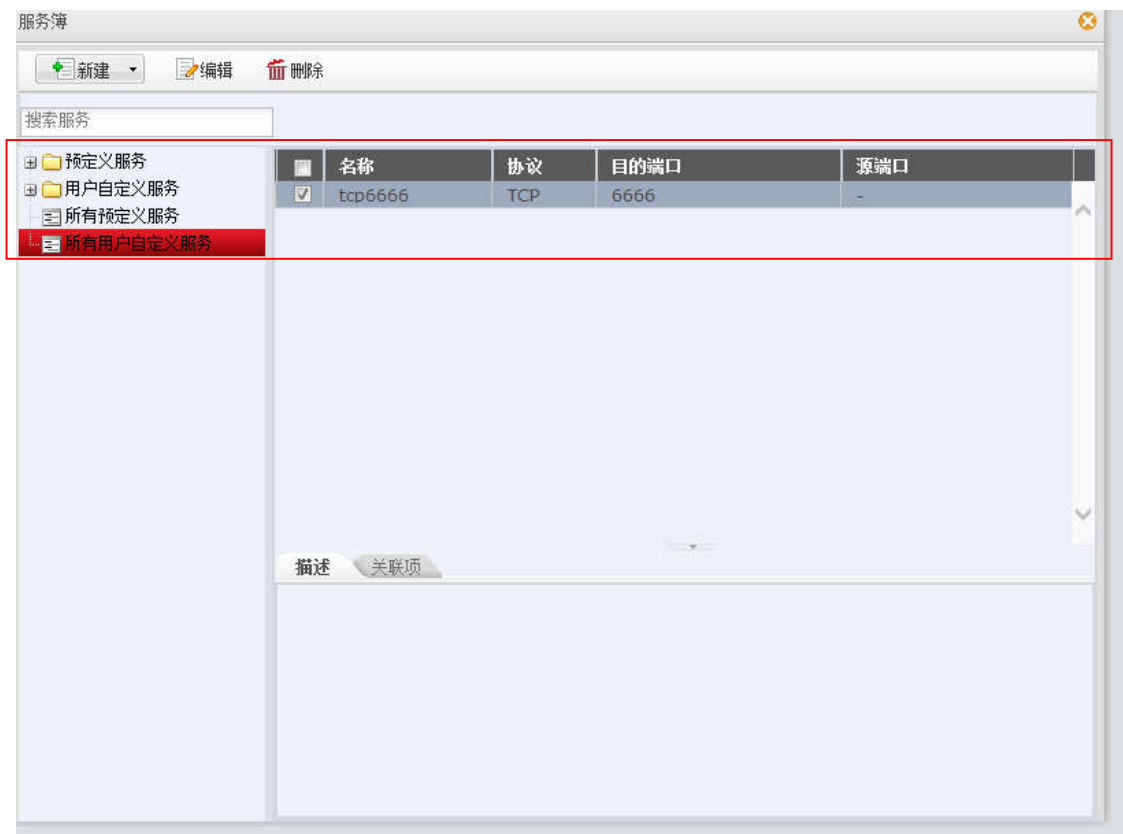
关闭

## 时间设置 2 分



## Ip qos 设置 2 分

- 6、DCFW 上配置 NAT 功能，使 PC3 能够通过 WEB 方式正常管理到 AC，端口号使用 6666;) 合理配置安全策略。(6 分)



## 服务簿设置 2 分

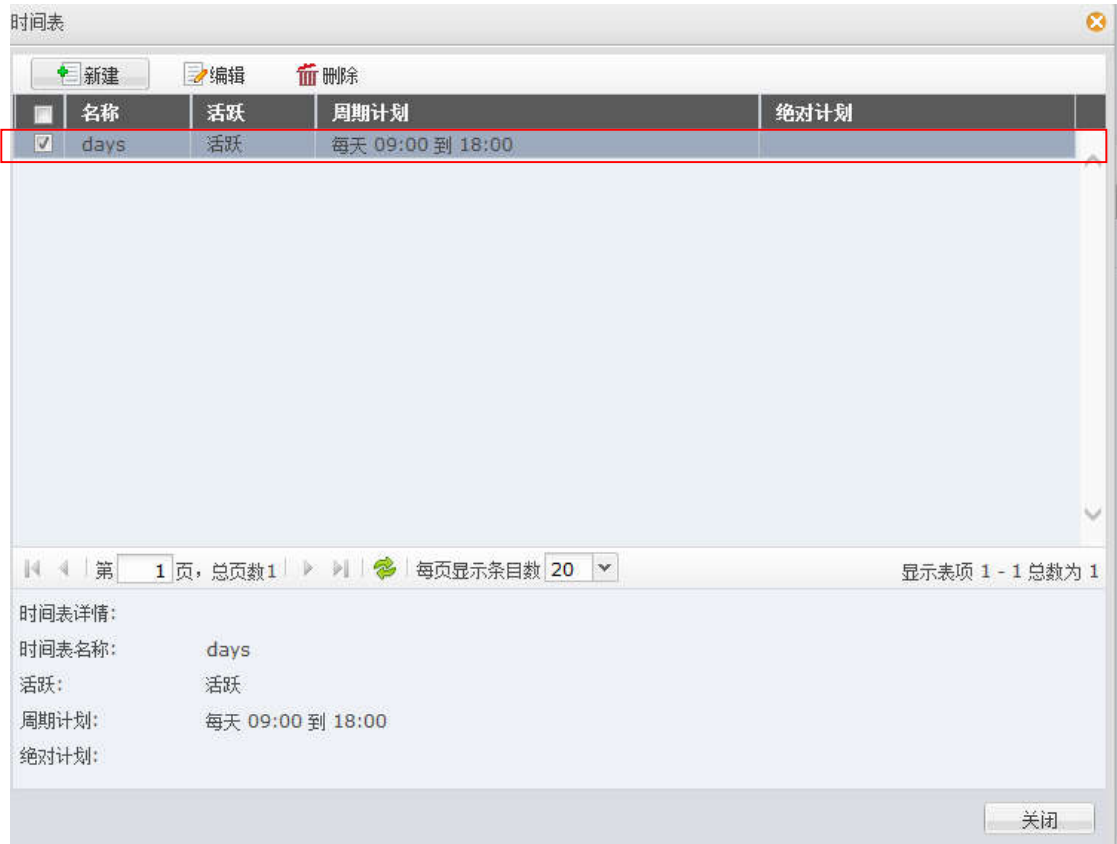


## 目的 nat 2 分



## 策略 2 分

7、在 DCFW 做相关配置要求防火墙能够记录每天 9:00-18:00 内网用户访问外网的 URL，保存在日志服务器；（6 分）



时间表 2 分



应用行为控制规则配置

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

FTP控制

HTTP控制

GET

类型	域名	动作	日志
GET	-	允许	记录日志

HTTP阻止下载

行为规则配置 2 分

日志服务器配置

主机名称: 172.16.100.10

绑定方式: 虚拟路由器: trust-vr

协议: UDP

端口: 514

日志类型:

☐ 事件日志
☐ 配置日志
☐ 安全日志

☐ 网络日志
☒ 会话日志
☐ NAT日志

☒ 上网日志
☐ 调试日志
☒ NBC日志

日志服务器配置 2 分

- 8、配置防火墙 Web 外发信息控制策略，禁止内网无线用户到所有网站的 Web 外发信息控制；内网有线用户到外网网站 Web 外发信息控制，禁止外发关键字“攻击”“病毒”，信任值为 1，并记录相关日志。（6 分）



配置有线、无线地址簿 1 分



Web外发信息规则配置

名称: 无线用户WEB外发 (1~31)字符

当满足以下条件时

目的安全域: untrust

用户: 无线用户

时间表:

配置

配置

做如下控制

控制范围: 所有网站

控制内容: 所有Web外发信息

☒ 阻止外发 ☒ 记录日志

指定的关键字

新建 编辑

关键字类别	<input type="checkbox"/> 阻止外发	<input type="checkbox"/> 记录日志

确定 取消

Web 外发规则配置无线 1 分



关键字配置 2 分



Web 外发规则配置有线 2 分

9、DCFW 做相关配置要求内网用户不能登录 QQ 和 MSN；（6 分）

网络聊天规则配置

名称: deny-QQMSN (1~31)字符

当满足以下条件时

目的安全域: untrust

用户: Any

时间表:

配置

做如下控制

MSN QQ 雅虎通

账号:

添加

账号	阻止使用	记录日志
	<input type="checkbox"/>	<input type="checkbox"/>

删除

列表外的所有MSN账号:

☒ 阻止使用 ☐ 记录日志

确定 取消

网络聊天规则 MSN 配置 1.5 分

网络聊天规则配置

名称: deny-QQMSN (1~31)字符

当满足以下条件时

目的安全域: untrust

用户: Any

时间表:

配置

做如下控制

MSN QQ 雅虎通

账号:

添加

账号	<input type="checkbox"/> 阻止使用	<input type="checkbox"/> 记录日志

删除

列表外的所有QQ账号:

☒ 阻止使用 ☐ 记录日志

确定 取消

网络聊天

新建 编辑 删除 启用 禁用 优先级

名称	目的安全域	用户	时间表	MSN	QQ	雅虎通
deny-QQMSN	untrust	Any		Any	Any	

网络聊天规则 QQ 配置 1.5 分

安全域配置

基本设置

安全域名称: untrust (1~31)字符

描述: (0~63)字符

类型: ☐ 二层安全域 ☒ 三层安全域 ☐ Tap域

虚拟路由器: trust-vr

接口选择:

可绑定接口

- ethernet0/0
- ethernet0/2
- ethernet0/3
- ethernet0/4
- ethernet0/5
- ethernet0/6
- ethernet0/7
- ethernet0/8

已绑定接口

- ethernet0/1
- tunnel1

从域中移除接口将删除接口的IP配置。

高级属性

应用识别: ☒ 启用

WAN安全域: ☒ 启用

确定 取消

Untrust 区域启用应用识别 3分

- 10、DCFw 上配置限制内网用户访问 [www.taobao.com](http://www.taobao.com)，限制内网用户访问 URL 中带有 [taobao](http://www.taobao.com) 关键字的所有网站。(6分)

URL过滤规则配置

名称: taobao

当满足以下条件时

目的安全域: untrust

用户: Any

时间表:

配置

做如下控制

URL类别 URL关键字类别 上网日志记录

新建 编辑

URL类别	阻止访问	记录日志
政治	<input type="checkbox"/>	<input type="checkbox"/>
艺术	<input type="checkbox"/>	<input type="checkbox"/>
教育	<input type="checkbox"/>	<input type="checkbox"/>
非盈利组织	<input type="checkbox"/>	<input type="checkbox"/>
儿童	<input type="checkbox"/>	<input type="checkbox"/>
www.taobao.com	<input checked="" type="checkbox"/>	<input type="checkbox"/>

列表外的所有URL: ☐ 阻止访问 ☐ 记录日志

确定 取消

URLU

URL 类别规则 3 分

URL过滤规则配置

名称: taobao

当满足以下条件时

目的安全域: untrust

用户: Any

时间表:

配置

配置

做如下控制

URL类别 URL关键字类别 上网日志记录

新建 编辑

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

列表外的所有URL: ☐ 阻止访问 ☐ 记录日志

确定 取消

安全 策略 攻击防护 ARP防护 控制 流量管理 会话限制

名称	目的安全域	用户	时间表	URL类别
taobao	untrust	Any		www.taobao.com

URL 关键字规则 3 分

- 11、在 DCB-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;要求对内网访问 internet 全部应用进行记录日志; (6 分)

我的导航 常规配置 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 10 % (范围10--50%)

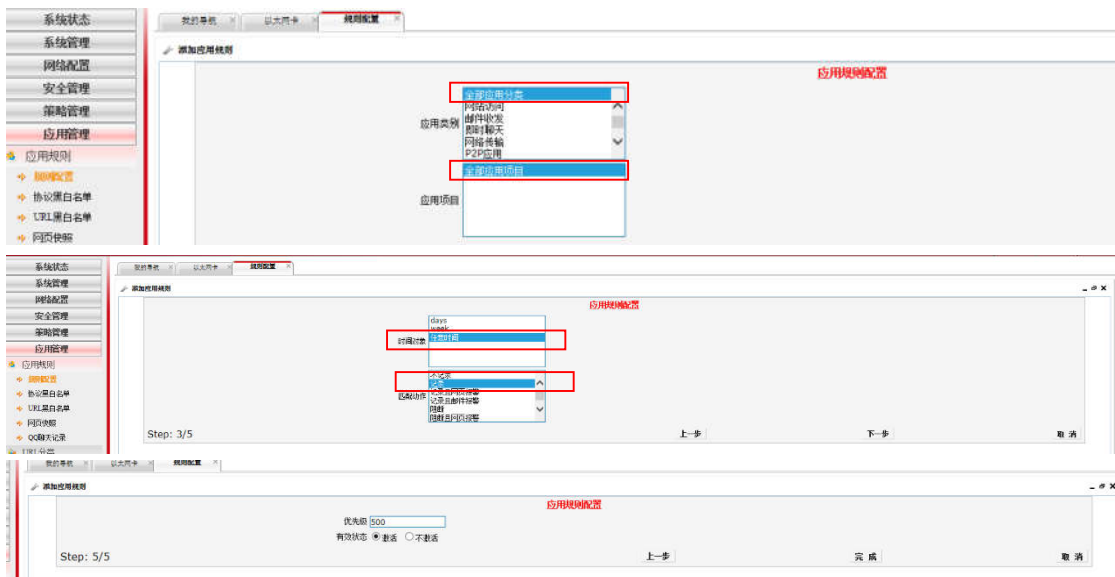
保存

设置旁路模式 2 分

接口名称	地址规划方式	IP地址	子网掩码	MAC地址	接口状态	监控状态
eth0	静态	192.168.5.254	255.255.255.0	00:16:31:f7:f2:08	启用	未监控
eth1	静态	0.0.0.0	0.0.0.0	00:16:31:f7:f2:09	启用	未监控
eth2	静态	0.0.0.0	255.255.255.252	00:16:31:f7:f2:0a	启用	未监控
eth3	静态	0.0.0.0	0.0.0.0	00:16:31:f7:f2:0b	启用	监控
eth4	静态	0.0.0.0	0.0.0.0	00:16:31:e0:6d:7d	启用	未监控
eth5	静态	0.0.0.0	0.0.0.0	00:16:31:e0:6d:7c	启用	未监控

ip 地址 子网掩码: (参照地址规划表) 接口状态 : 启用 监控状态: 监控 2 分





记录全部日志规则 2 分

12、在 DCBI-netlog 上配置，监控周一至周五 9:00-18:00 无线用户所在网段访问的 URL 中包含 **taobao** 的 HTTP 访问记录，并且邮件发送告警；（6 分）



创建时间对象 1 分



应用类别：网站访问

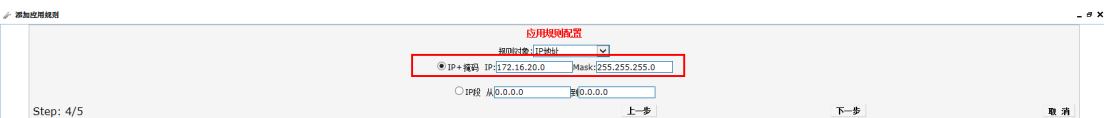
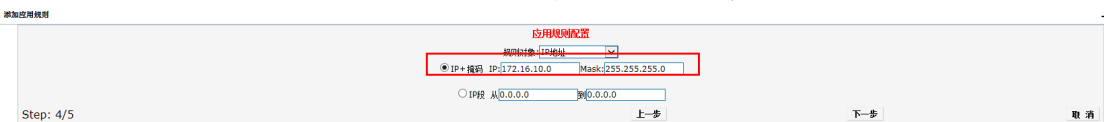
应用项目：网页浏览 1 分



添加 题目要求 URL 地址 1 分



时间对象：上面自定时间范围 匹配动作：记录且邮件报警 1 分

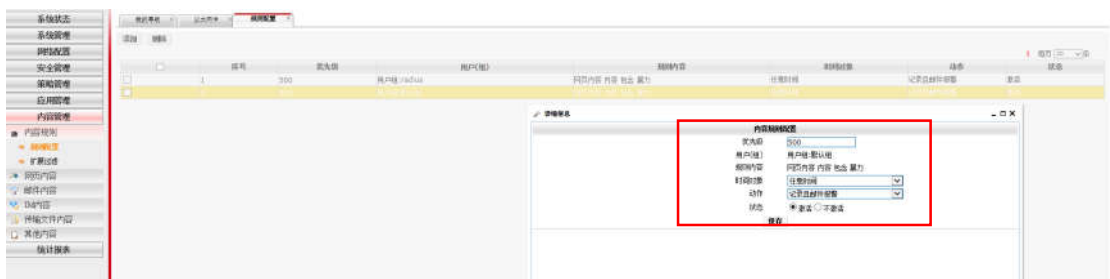


规则对象 无线所在 vlan 网段 1 分

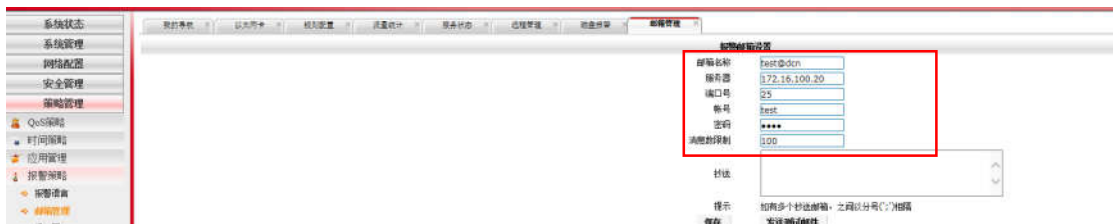


激活 1 分

- 13、在 DCBI 上配置，添加内容规则，对于网站访问关键字包含“暴力”的，记录并邮件报警；（6 分）



- 14、在 DCBI 上配置，使 DCBI 能够通过邮件方式发送告警信息，邮件服务器 ip 172.16.100.20，端口号 25，账号 test@dcn，密码 test，当 DCBI 磁盘使用率超过 80% 时发送一次报警；（6 分）



### 创建用户名密码 3 分



### 报警阈值 3 分

- 15、在 DCBI 上配置，将 DCBI 的日志信息发送到日志服务器，日志服务器 ip 172.16.100.10，community 名字 public。(6 分)



- 16、在 DCBI 上配置，增加非 admin 账户 DCN2018，密码 dcbi1234，该账户仅用于用户查询设备的日志信息和统计信息。；(6 分)



### 权限分配 3 分

添加系统管理员

### 管理员配置

名称	DCN2018
所属组	dftgroup
密码	*****
密码重复	*****
邮箱(用于找回密码)	
IP地址	0.0.0.0
MAC地址	00:00:00:00:00:00
最大并发数	0
激活态	激活
有效期	从 0000-00-00 到 0000-00-00 <a href="#">恢复默认值</a>
角色	查询

[确定](#)

### 账号配置 3 分

- 17、DCBI 配置应用及应用组“p2p 下载”，UDP 协议端口号范围 40000-42000，在周一至周五 9:00-18:00 监控 LAN 中所有用户的“p2p 下载”访问记录并告警；（6 分）

详细信息

### 自定义应用配置

自定义名称	p2p下载
所属应用组	P2P下载
协议类型	UDP
服务器IP	0.0.0.0
服务器端口	从 40000 到 42000

[保存](#)

### P2p 下载端口号定义 2 分

添加时间策略

[添加保存](#)

### 基本设置

策略名称: dftname  
策略描述: description

### 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

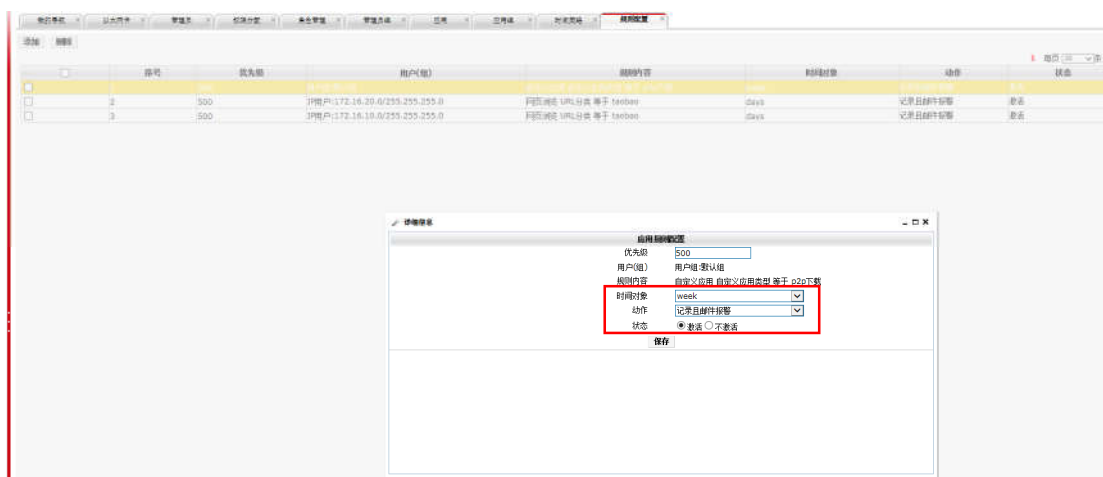
按月为周期 ☐ 从 到 日  
月周期时段: (1) 00:00-00:00 (2) 00:00-00:00 (3) 00:00-00:00 (4) 00:00-00:00 [设定](#) [重置](#)

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) 09:00-18:00 (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](#)

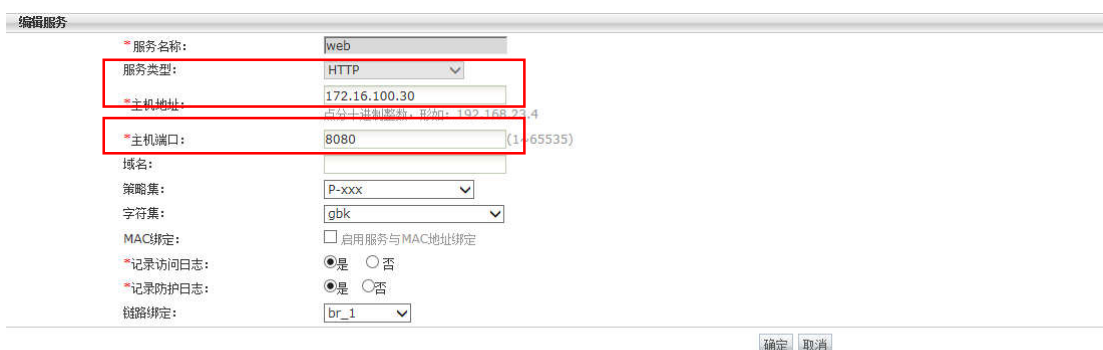
序号	周日	周一	周二	周三	周四	周五	周六	时间段一	时间段二	时间段三	时间段四	移除本项
1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	09:00-18:00	00:00-00:00	00:00-00:00	00:00-00:00	<a href="#">移除</a>

### 时间对象 2 分

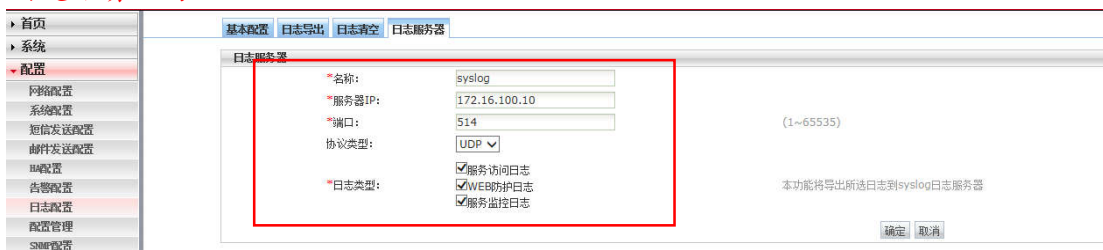


### 应用规则设置 2 分

- 18、在 WAF 上配置，公司内部有一台网站服务器直连到 WAF，IP 地址是 172.16.100.30，端口是 8080，并将服务访问日志、Web 防护日志、服务监控日志发送至 syslog 日志服务器，syslog 日志服务器 IP 地址是 172.16.100.10，UDP 的 514 端口；（6 分）



### 创建服务 3 分

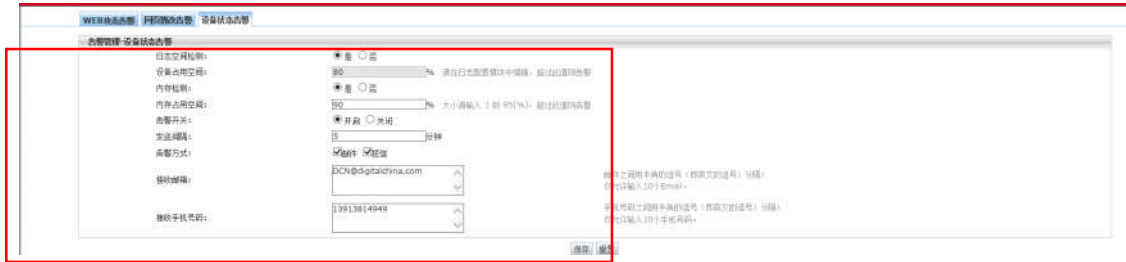


### 配置日志服务器 3 分

- 19、在公司总部的 WAF 上配置，将攻击告警、设备状态告警、服务状态告警信息通过邮件（发送到 DCN@digitalchina.com）及短信方式（发送到 13913814949）发送给管理员。（6 分）

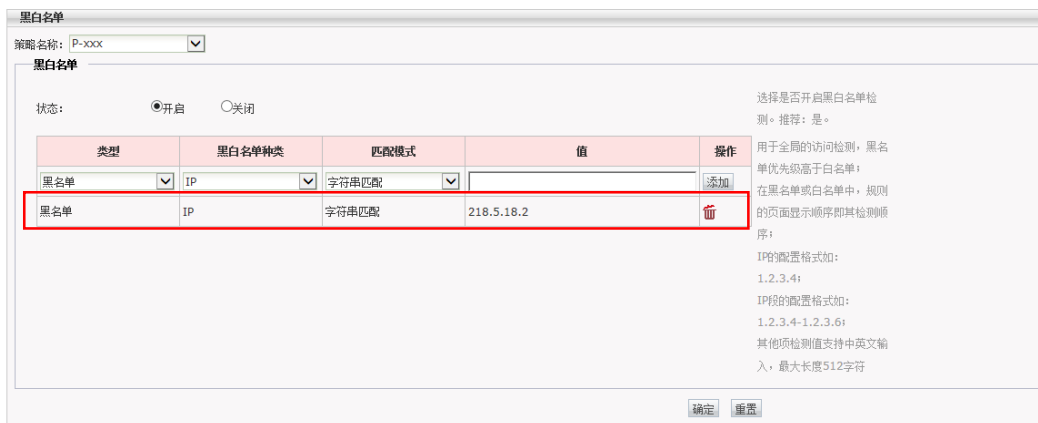


Web 告警攻击 3 分



设备状态告警 3 分

- 20、在公司总部的 WAF 上配置，禁止公网 IP 地址（218.5.18.2）访问网站服务器，网站服务器地址是 172.16.100.30。；（6 分）



- 21、在公司总部的 WAF 上配置，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。大量请求的确认值是：并发访问超过 3000 次请求；（6 分）



暴力浏览防护开启 2 分

最大请求数 2 分

动作阻止 2 分

- 22、在 WAF 上配置，开启基于 session cookie 的 CC 防护，最大请求数为 2000，超过进行阻止；（6 分）



状态开启 2 分

最大请求数 2 分

动作阻止 2 分

23、DCRS 为接入交换机，为终端产生防止 MAC 地址防洪攻击，请配置端口安全，已划分 VLAN 的端口最多学习到 5 个 MAC 地址，发生违规阻止后续违规流量通过，不影响已有流量并产生 LOG 日志；连接 PC1 的接口为专用接口，限定只允许 PC1 的 MAC 地址可以连接；（6 分）

Interface Ethernet1/0/1

switchport mode trunk

switchport port-security

switchport port-security maximum 5 1 分

switchport port-security violation restrict

ip dhcp snooping trust

anti-arpscan trust supertrust-port

!

Interface Ethernet1/0/2

switchport access vlan 1001

switchport port-security

switchport port-security maximum 5 1 分

switchport port-security violation restrict

ip dhcp snooping trust

anti-arpscan trust supertrust-port

Interface Ethernet1/0/6

rate-violation broadcast 2700

switchport access vlan 40

switchport port-security

switchport port-security mac-address 9c-5c-8e-37-31-98 PC1 的 MAC，可以是 6-9

任意接口，得 2 分

ip dhcp snooping binding user-control

Interface Ethernet1/0/7

6-24 口，除连接 PC1 和 WAF 的口外，全部配置得 2

分

rate-violation broadcast 2700

switchport access vlan 40

switchport port-security

switchport port-security maximum 5

switchport port-security violation restrict

ip dhcp snooping binding user-control



!

24、将连接 DCFW 的双向流量镜像至 Netlog 进行监控和分析；（6分）

```
monitor session 1 source interface Ethernet1/0/2 tx 2分
monitor session 1 source interface Ethernet1/0/2 rx 2分
monitor session 1 destination interface Ethernet1/0/4 2分
```

25、开启防 ARP 扫描功能,单位时间内端口收到 ARP 数量超过 50 便认定是攻击, DOWN 掉此端口；（6分）

```
anti-arpscan enable
anti-arpscan port-based threshold 50 2分
```

```
Interface Ethernet1/0/1
switchport mode trunk
switchport trunk allowed vlan 10;20;30;100;1002
anti-arpscan trust supertrust-port 2分
!
```

```
Interface Ethernet1/0/2
switchport access vlan 1001
ip dhcp snooping trust
anti-arpscan trust supertrust-port 2分
```

26、在公司总部的 DCRS 上配置端口环路检测（Loopback Detection），防止来自 vlan200 接口下的单端口环路,并配置存在环路时的检测时间间隔为 30 秒,不存在环路时的检测时间间隔为 10 秒；（6分）

```
loopback-detection interval-time 30 10 3分
```

```
Interface Ethernet1/0/10
storm-control broadcast 2000
switchport access vlan 200
ip access-group work in
dot1x enable
dot1x port-method portbased
loopback-detection specified-vlan 200 Ethernet1/0/10-24 口全部配对 3分
loopback-detection control shutdown
!
```

27、为了控制接入网络 PC，需要在交换 Eth1/0/10 口开启 DOT1X 认证，配置认证服务器，IP 地址是 172.16.100.40，radius key 是 dcn2018；（6分）

```
radius-server authentication host 172.16.100.40 key 0 dcn2018
aaa enable 3分
!
```

```
dot1x enable
Interface Ethernet1/0/10
 storm-control broadcast 2000
 switchport access vlan 200
 ip access-group work in
 dot1x enable
 dot1x port-method portbased
 loopback-detection specified-vlan 200
 loopback-detection control shutdown
```

3 分

28、交换机开启远程管理，使用 SSH 方式账号为 DCN2018，密码为 123456. (6 分)

```
username DCN2018 privilege 15 password 0 123456
ssh-server enable
```

3 分

3 分

29、VLAN20、vlan30、vlan10 用户采用动态获取 IP 地址方式，DHCP 服务器在 AC 上配置，前十个地址为保留地址，vlan40 用户也动态获取 ip，DHCP server 为 DCFW. (6 分)

DCRS:

```
service dhcp
!
ip forward-protocol udp bootps
interface Vlan10
 ip address 172.16.10.1 255.255.255.0
 !forward protocol udp 67(active)!
 ip helper-address 10.0.0.6
!
interface Vlan20
 ip address 172.16.20.1 255.255.255.128
 !forward protocol udp 67(active)!
 ip helper-address 10.0.0.6
!
interface Vlan30
 ip address 172.16.30.1 255.255.255.192
 ip gratuitous-arp 30
 !forward protocol udp 67(active)!
 ip helper-address 10.0.0.6
!
interface Vlan40
 ip address 192.168.40.1 255.255.255.0
 !forward protocol udp 67(active)!
 ip helper-address 10.0.0.1
```

1 分

1 分

1 分

1 分

1 分

1 分

30、在交换机上配置,在只允 vlan200 用户在上班时间(周一到周五 8:00 到 18:00)内访问 vlan100 段 IP。 (6 分)

```
time-range work
periodic weekdays 08:00:00 to 18:00:00
```

 2 分

```
ip access-list extended work
permit ip 172.16.100.0 0.0.0.255 192.168.100.0 0.0.0.255 time-range work
```

 2 分

```
Interface Ethernet1/0/10
storm-control broadcast 2000
switchport access vlan 200
ip access-group work in
dot1x enable
dot1x port-method portbased
loopback-detection specified-vlan 200
loopback-detection control shutdown
```

 Ethernet1/0/10-24 口全部配对 2 分

31、为拦截、防止非法的 MAC 地址与 IP 地址绑定的 ARP 数据包配置动态 arp 检测功能, VLAN30 用户网络接口的 ARP 阈值为 50。 (6 分)

```
interface Vlan30
ip address 172.16.30.1 255.255.255.192
ip arp dynamic maximum 50
!forward protocol udp 67(active)!
ip helper-address 10.0.0.6
```

32、为了防止 vlan40 网段 arp 欺骗,需要在交换机上开启 ip dhcp snooping 并在接口下绑定用户。 (6 分, 扣完为止)

```
ip dhcp snooping enable
ip dhcp snooping binding enable
```

 1 分

```
Interface Ethernet1/0/1
switchport access vlan 1002
ip dhcp snooping trust
anti-arpscan trust supertrust-port
```

 1 分

```
Interface Ethernet1/0/2
switchport access vlan 1001
ip dhcp snooping trust
anti-arpscan trust supertrust-port
```

 1 分

!

```
Interface Ethernet1/0/6
storm-control broadcast 2000
switchport access vlan 40
```

```
switchport port-security
switchport port-security maximum 5
ip dhcp snooping binding user-control
```

1 分

!

```
Interface Ethernet1/0/7
storm-control broadcast 2000
switchport access vlan 40
switchport port-security
switchport port-security maximum 5
ip dhcp snooping binding user-control
```

1 分

!

```
Interface Ethernet1/0/8
storm-control broadcast 2000
switchport access vlan 40
switchport port-security
switchport port-security maximum 5
ip dhcp snooping binding user-control
```

1 分

!

```
Interface Ethernet1/0/9
storm-control broadcast 2000
switchport access vlan 40
switchport port-security
switchport port-security maximum 5
ip dhcp snooping binding user-control
```

1 分

!

33、在 DCRS 上配置，配置设备 enable 密码，密码为 dcn2018，并且在登录设备时必须正确输入 enable 密码才能进入交换机的配置模式。（6 分）

```
enable password level 15 0 dcn2018
```

34、DCRS 上配置，VLAN40 的成员接口开启广播风暴抑制功能，参数设置为 2000pps。（6 分）

!

```
Interface Ethernet1/0/6
storm-control broadcast 2000
```

1.5 分

```
switchport access vlan 40
switchport port-security
switchport port-security maximum 5
ip dhcp snooping binding user-control
```

!

```
Interface Ethernet1/0/7
storm-control broadcast 2000
```

1.5 分

```
switchport access vlan 40
switchport port-security
```

```

switchport port-security maximum 5
ip dhcp snooping binding user-control
!
Interface Ethernet1/0/8
storm-control broadcast 2000 1.5 分
switchport access vlan 40
switchport port-security
switchport port-security maximum 5
ip dhcp snooping binding user-control
!
Interface Ethernet1/0/9
storm-control broadcast 2000 1.5 分
switchport access vlan 40
switchport port-security
switchport port-security maximum 5
ip dhcp snooping binding user-control
!

```

35、AP 通过 option43 方式进行正常注册上线,AC 地址为管理 VLANIP; (6 分)

AC:

```

Interface Ethernet1/0/1
switchport access vlan 1002 1 分

ip access-group acl in
!
Interface Ethernet1/0/2
switchport mode trunk 1 分
switchport trunk native vlan 30
!

ip dhcp pool vlan30
network-address 172.16.30.0 255.255.255.192
lease 0 10 0
default-router 172.16.30.1
dns-server 8.8.8.8
option 43 hex 0104C0A864FE 1 分

wireless
no auto-ip-assign
enable
ap authentication none 1 分

static-ip 192.168.100.254

```

```
ap profile 1
  name Default
  hwtype 59
```

1 分

DCRS:

```
interface Vlan30
  ip address 172.16.30.1 255.255.255.192
  ip arp dynamic maximum 50
  !forward protocol udp 67(active)!
  ip helper-address 10.0.0.6
```

1 分

36、设置 SSID **DCN2018**,vlan10,加密模式为 wpa-personal,其口令为 **GSdcn2018** 的;设置 SSID dcntest ,vlan20 不进行认证加密,做相应配置隐藏该 ssid;  
(6 分)

```
network 1
  hide-ssid
  mac authentication local
  client-qos enable
  client-qos bandwidth-limit down 2048
  client-qos bandwidth-limit up 1024
  arp-suppression
  max-clients 20
  ssid dcntest
  vlan 20
  station-isolation
!
```

1 分

1 分

```
network 2
  mac authentication local
  arp-suppression
  security mode wpa-personal
  ssid DCN2018
  vlan 10
  wpa
  key
  encrypted
30fa7ce6b297a56f68bc50b9fa993039517386929c279637976d7292463c4ae072c64f05d0b388b
b76b9e9614dd792e2a5aefd85727da5e174be0166d29e8744
!
```

2 分

```
ap profile 1
  name Default
  hwtype 59
```

```

ap escape
radio 1
dot11n channel-bandwidth 20
schedule-mode preferred
vap 0
!
vap 1
enable
!
!
radio 2
mode ac
dot11ac channel-bandwidth 40
schedule-mode preferred
vap 0
!
vap 1
enable
!
!

```

1 分

1 分

37、dctest 最多接入 20 个用户，用户间相互隔离，并对 dctest 网络进行流控，上行速率 1Mbps，下行速率 2Mbps；（6 分）

```

network 1
hide-ssid
mac authentication local
client-qos enable
client-qos bandwidth-limit down 2048
client-qos bandwidth-limit up 1024
arp-suppression
max-clients 20
ssid dctest
vlan 20
station-isolation

```

3 分

1.5 分

1.5 分

38、通过配置避免接入终端较多且有大量弱终端时，高速客户端被低速客户端“拖累”，低速客户端不至于长时间得不到传输；（6 分）

```

ap profile 1
name Default
hwtype 59
ap escape
radio 1
dot11n channel-bandwidth 20
schedule-mode preferred

```

3 分



```

vap 0
!
vap 1
enable
!
!
radio 2
mode ac
dot11ac channel-bandwidth 40
schedule-mode preferred 3分
vap 0
!
vap 1
enable
!

```

39、通过配置防止多 AP 和 AC 相连时过多的安全认证连接而消耗 CPU 资源,检测到 AP 与 AC 在 10 分钟内建立连接 5 次就不再允许继续连接,两小时后恢复正常。(6分)

```

wireless ap anti-flood interval 10 2分
wireless ap anti-flood max-conn-count 5 2分
wireless ap anti-flood agetime 120 2分

```

40、AC 开启 web 管理,账号密码为 DCN2018; (6分)

```
username DCN2018 privilege 15 password 0 DCN2018
```

### 三、第二阶段与第三阶段

阶段	任务	答案 (明文)	答案 (散列值)	分数
第二阶段	XSS 渗透测试与安全开发 2.1.1	str_replace	7c3b75986a18638d635a5d5d67e5364d	10
第二阶段	XSS 渗透测试与安全开发 2.1.2	\$info	355ef3fa24dcc8bbcfec5305fe99574b	10
第二阶段	XSS 渗透测试与安全开发 2.1.3	SERVER	3d27c95bfdbea691b250894d96852844	10
第二阶段	XSS 渗透测试与安全开发 2.1.4	REMOTE_ADDR	d9caaec77df8c1005802859e069c6264	10
第二阶段	XSS 渗透测试与安全开发 2.1.5	!\$conn	605945d15c289b5702638bf4ca534ec6	10
第二阶段	XSS 渗透测试与安全开发 2.1.6	\$res	4002603e450f0db8d5a7ff540344175c	10
第二阶段	密码学与 IPSec 应用 2.2.1	338	819f46e52c25763a55cc642422644317	10
第二阶段	密码学与 IPSec 应用 2.2.2	210	6f3ef77ac0e3619e9815	10

			9e9b6febf557	
第二阶段	密码学与 IPsec 应用 2.2.3	182	4c5bde74a8f110656874 902f07378009	10
第二阶段	密码学与 IPsec 应用 2.2.4	182	4c5bde74a8f110656874 902f07378009	10
第二阶段	密码学与 IPsec 应用 2.2.5	94	f4b9ec30ad9f68f89b29 639786cb62ef	10
第二阶段	密码学与 IPsec 应用 2.2.6	126	069059b7ef840f0c74a8 14ec9237b6ec	10
第二阶段	Web 应用渗透测试与安全开发 2.3.1	Ismae_SC-2018	7ac300f71f8406a818f3 d29f68010376	8
第二阶段	Web 应用渗透测试与安全开发 2.3.2	% _ .  - ' strstr(\$keyword , \$str3)	c244e4a9361ae28d0e2d b6a164d77f25	8
第二阶段	Web 应用渗透测试与安全开发 2.3.3	strstr(\$keyword, \$str5)	89b53faa25aa01b615b4 ada07cd2ba78	8
第二阶段	Web 应用渗透测试与安全开发 2.3.4	strstr(\$keyword, \$str1)	95185a526beb869daf28 61853674652d	9
第二阶段	Web 应用渗透测试与安全开发 2.3.5	strstr(\$keyword, \$str2)	c4e7be02c8ab5fb244e1 ae75f4e6f57f	9
第二阶段	Web 应用渗透测试与安全开发 2.3.6	strstr(\$keyword, \$str4)	2a523f2ce9c3ab2d983a 9348393ac9e3	9
第二阶段	Web 应用渗透测试与安全开发 2.3.7	MayBe Web Attack!	9aae798c312c02c8611f 5604bc8a5fcb	9
第二阶段	ICMP 扫描渗透测试 2.4.1	time. Ether(). IP(). UDP()	c0bf3d4b1ae0e9423d0d 72512bf7eac7	10
第二阶段	ICMP 扫描渗透测试 2.4.2	ethernet/ip/udp. tos. id	07720032a91e0d3679ec c7dfe987a87d	10
第二阶段	ICMP 扫描渗透测试 2.4.3	ttl. proto. src. dst	06493ad8a94a67a59a03 4d9022eb7ce7	10
第二阶段	ICMP 扫描渗透测试 2.4.4	sport. dport. len	641cb45abdf2f5722edc 2ff62bf2c18c	10
第二阶段	ICMP 扫描渗透测试 2.4.5	srp1. sleep. ICMP	fc5fd0be302afb87ed7b 32e10a84a053	10
第二阶段	ICMP 扫描渗透测试 2.4.6	H:!	cc1c6443a914c25bc93a 4fdc674b4602	10
第二阶段	逆向分析和缓冲区溢出渗透测试 2.5.1	P@ssW0rd_FLAG01	873fa5f8f187209e96f4 ac83ea90bb9e	8
第二阶段	逆向分析和缓冲区溢出渗透测试 2.5.2	P@ssW0rd_FLAG02	c241d98c7547093b8882 9952ad6f3ade	8
第二阶段	逆向分析和缓冲区溢出渗透测试 2.5.3	P@ssW0rd_FLAG03	66f99900e09e636ea17b ce461ef2b7c0	8
第二阶段	逆向分析和缓冲区溢出渗透测试 2.5.4	P@ssW0rd_FLAG04	c622ddedf96ae83bba1b f1b5f9945841	8

第二阶段	逆向分析和缓冲区溢出渗透测试 2.5.5	P@ssW0rd_FLAG05	cee3b41114e32be4d35c 6ce96ef877e1	8
第二阶段	逆向分析和缓冲区溢出渗透测试 2.5.6	P@ssW0rd_FLAG06	663337aee0b0f155d01a f87188affd02	8
第二阶段	逆向分析和缓冲区溢出渗透测试 2.5.7	P@ssW0rd_FLAG07	1db3e4f1e87944c183ce 9abb7222237	8
第二阶段	逆向分析和缓冲区溢出渗透测试 2.5.8	P@ssW0rd_FLAG08	e75dc7bb22c50084efbf 965336433cbf	8
第二阶段	逆向分析和缓冲区溢出渗透测试 2.5.9	P@ssW0rd_FLAG09	0590b112cd2c4e2ae4f4 021bee0512db	8
第二阶段	逆向分析和缓冲区溢出渗透测试 2.5.10	P@ssW0rd_FLAG10	93df62c5ff4421aaa8de 680f3034a712	8
第二阶段	云服务安全渗透测试 2.6.1	230	6da9003b743b65f4c0cc d295cc484e57	7
第二阶段	云服务安全渗透测试 2.6.2	9	45c48cce2e2d7fbdea1a fc51c7c6ad26	7
第二阶段	云服务安全渗透测试 2.6.3	buf + ret + pad + shellcode	9d2ea64dc9ba85099174 1eb93499cc2d	7
第二阶段	云服务安全渗透测试 2.6.4	conn. connect ((host, port))	c0657468eb445839acba 679770cc5143	7
第二阶段	云服务安全渗透测试 2.6.5	conn. recv	a63bba5d241515337f3d aa652a20a82d	7
第二阶段	云服务安全渗透测试 2.6.6	USER	2e40ad879e955201df4d edbf8d479a12	7
第二阶段	云服务安全渗透测试 2.6.7	inp	2c6f00854b4702a9da9a 18e5fcfd279	7
第二阶段	云服务安全渗透测试 2.6.8	\r\n	81051bcc2cf1bedf3782 24b0a93e2877	7
第二阶段	云服务安全渗透测试 2.6.9	os. system	666c6cd1eeaf67cba5b5 425295fcb75c	8
第二阶段	云服务安全渗透测试 2.6.10	8888	cf79ae6addba60ad0183 47359bd144d2	8
第二阶段	云服务安全渗透测试 2.6.11	Congratulations To You To Get The Highest Privilege Of The Cloud Server.	0f815e1d54fbdda2e3fd 0f925cae7e6e	8
第三阶段	基本 FLAG	123456		