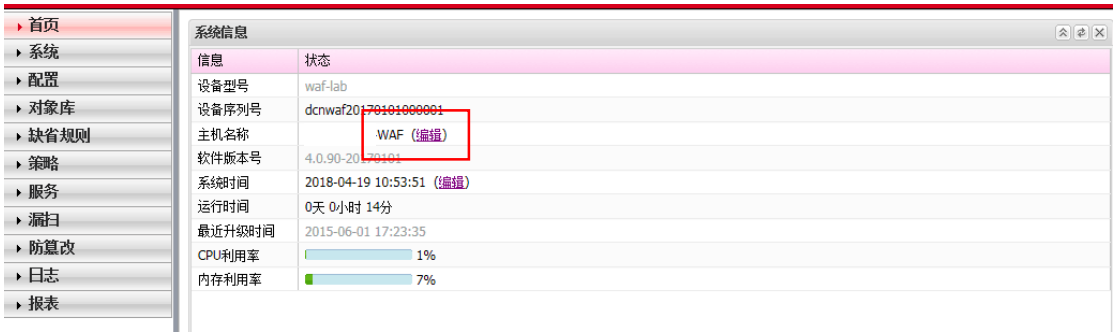
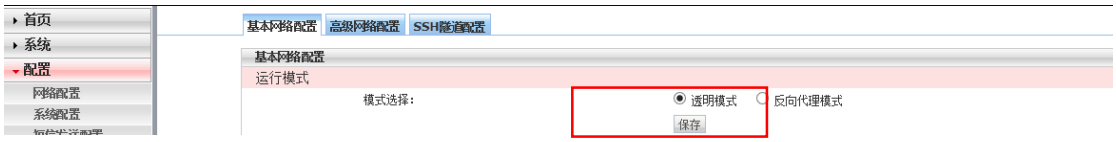
评分标准中参数请以实际题目为准

一、第一阶段任务一

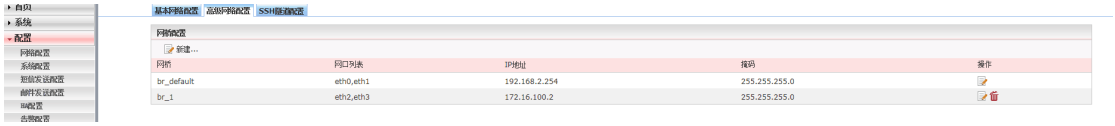
1、根据网络拓扑图所示，按照 IP 地址参数表，对 WAF 的名称、各接口 IP 地址进行配置。（5 分）

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

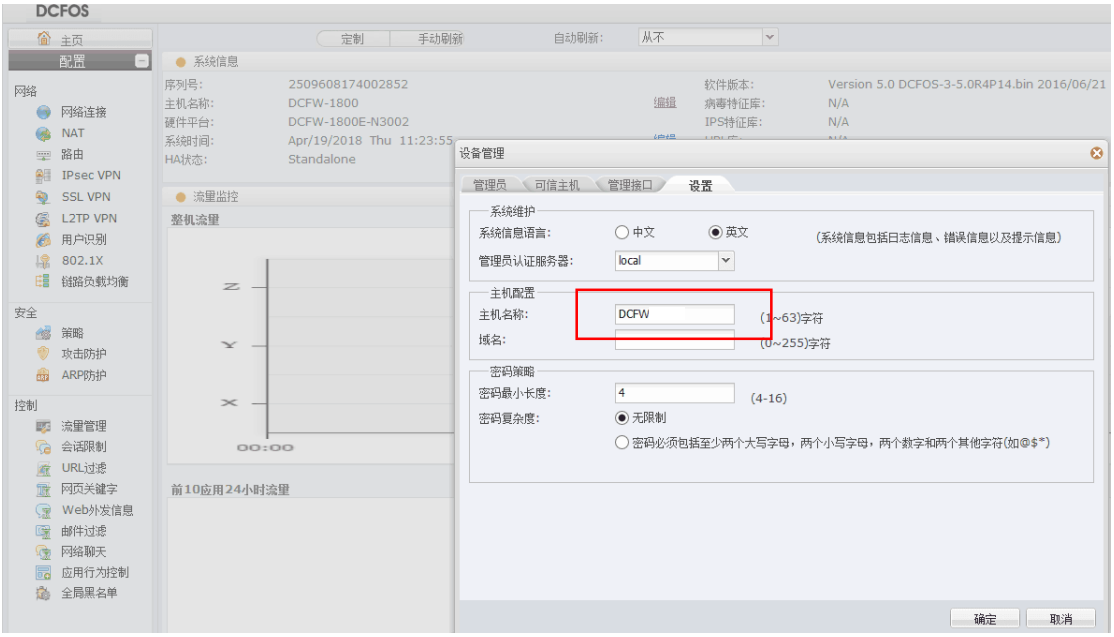
ip address 192.168.100.1 255.255.255.0（匹配参数表）0.5 分

interface Vlan200

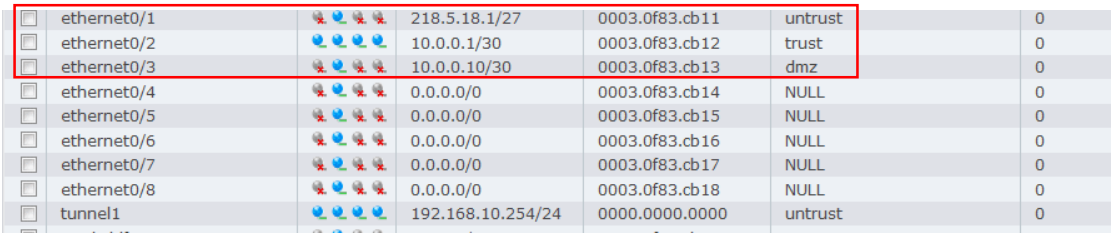
ip address 172.16.200.1 255.255.255.0（匹配参数表）0.5 分

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



ethernet0/1		218.5.18.1/27	0003.0f83.cb11	untrust	0
ethernet0/2		10.0.0.1/30	0003.0f83.cb12	trust	0
ethernet0/3		10.0.0.10/30	0003.0f83.cb13	dmz	0
ethernet0/4		0.0.0.0/0	0003.0f83.cb14	NULL	0
ethernet0/5		0.0.0.0/0	0003.0f83.cb15	NULL	0
ethernet0/6		0.0.0.0/0	0003.0f83.cb16	NULL	0
ethernet0/7		0.0.0.0/0	0003.0f83.cb17	NULL	0
ethernet0/8		0.0.0.0/0	0003.0f83.cb18	NULL	0
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

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:

6 分错一条扣一分扣完为止

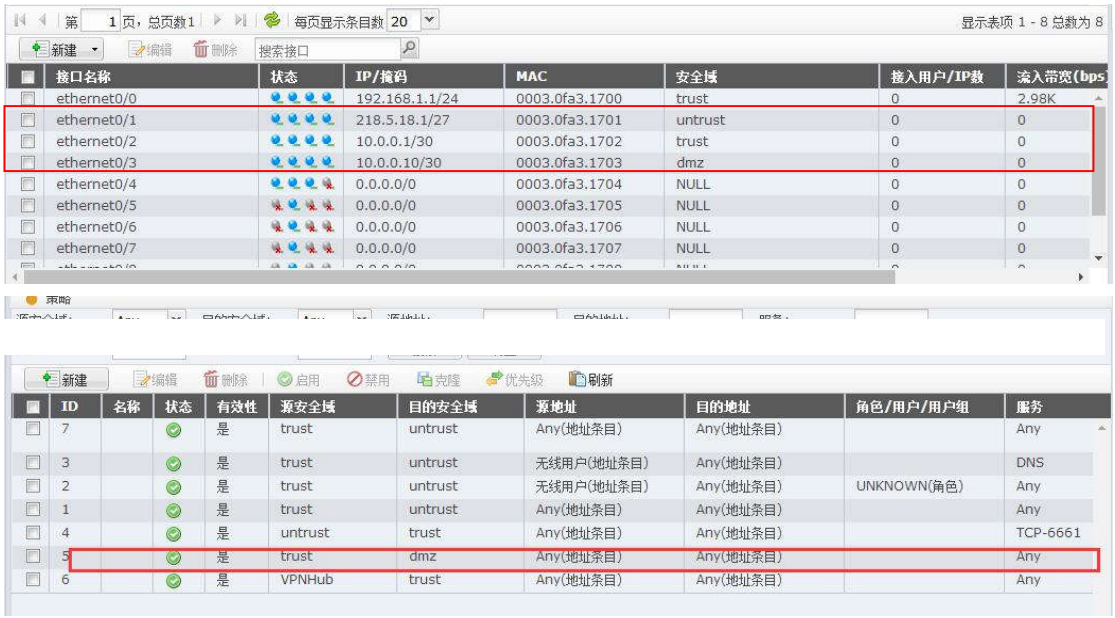
8、防火墙做必要的配置实现内网对外网访问。（20 分）

Nat 配置正确 10 分

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络管理 netlog。（6 分）



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

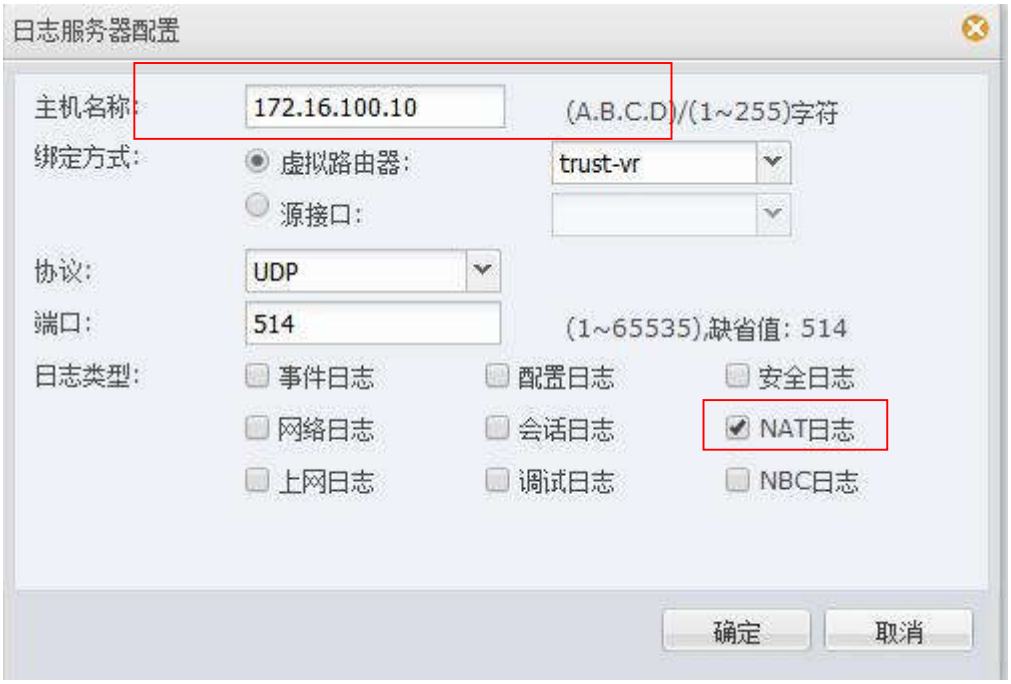
2、接口安全域（连接 PC2：UNTRUST、连接 DCRS：TRUST）1 分

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

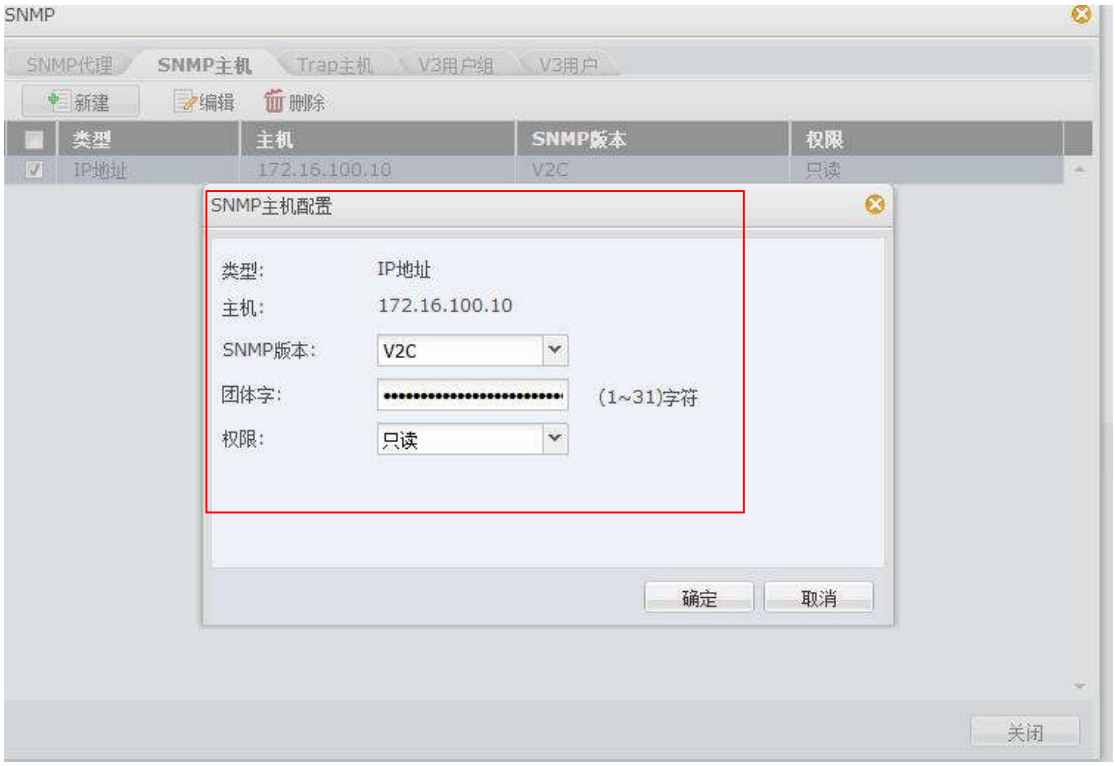
5. 策略配置正确得 1 分

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）



日志服务器配置正确 2 分

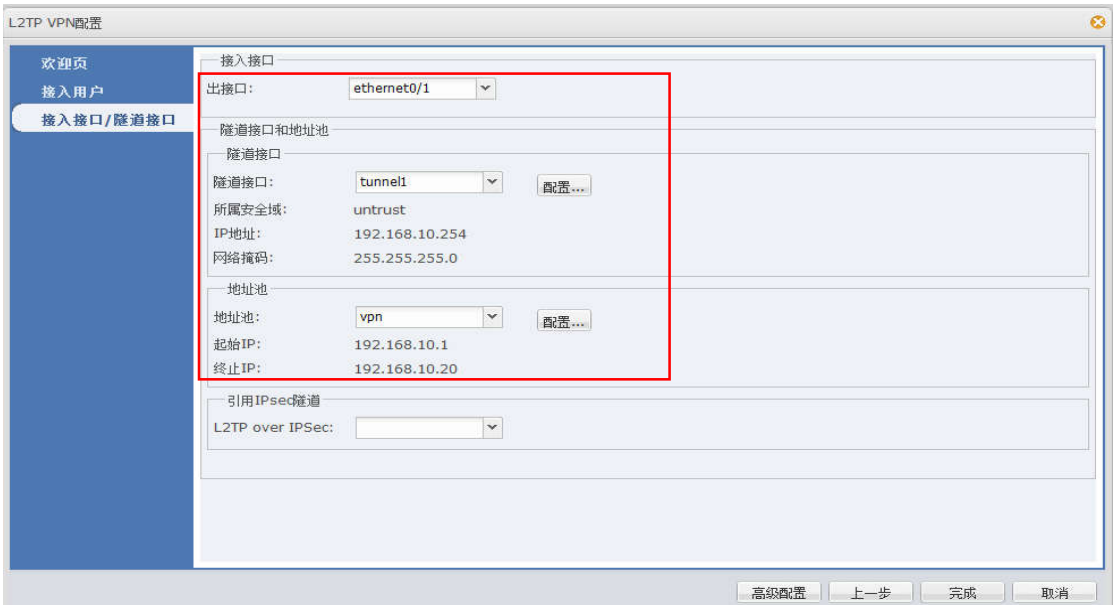
开启 nat 日志记录 2 分

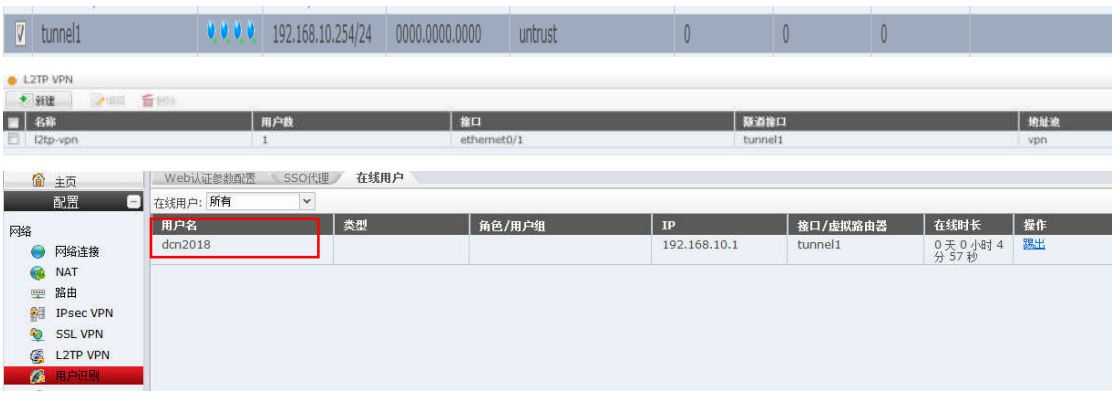


Snmp 服务配置正确 2 分

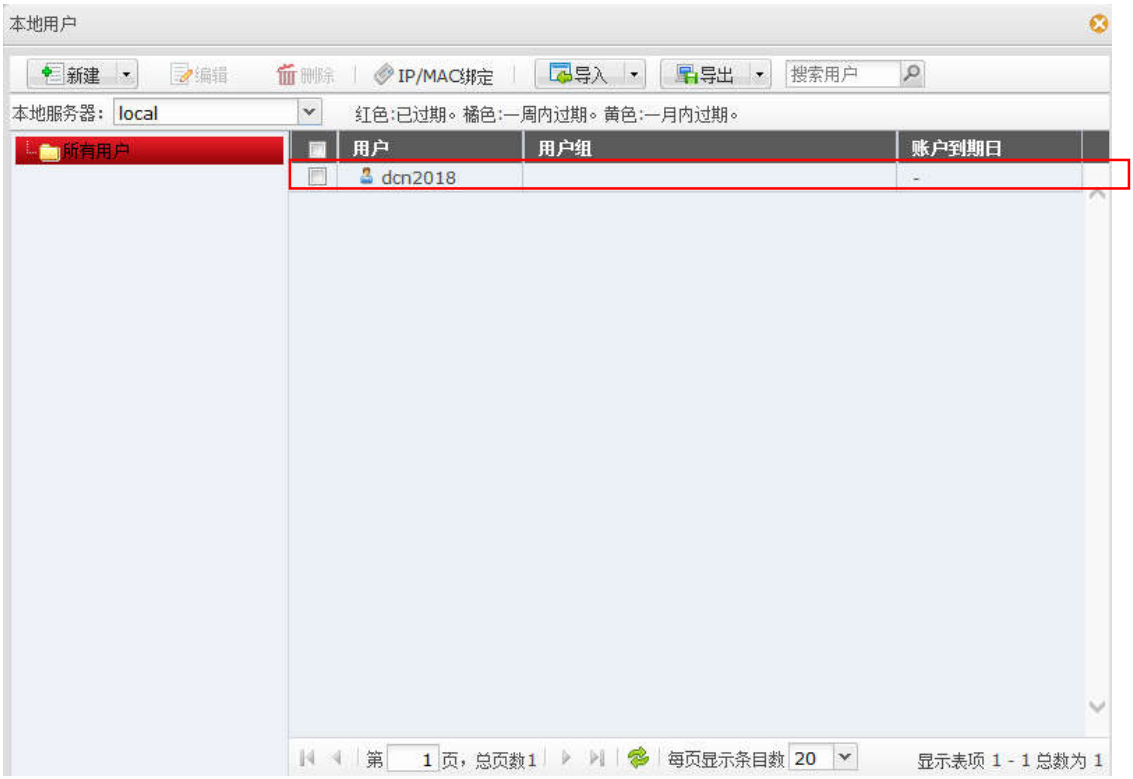
3、DCFW 做相应配置，使用 l2tp 方式让外网移动办公用户能够实现对内网的访问，用户名密码为 dcn2018， VPN 地址池参见地址表；合理配置安全策略。（6 分）

账号、AAA 服务器配置 2 分





隧道接口-地址池配置 2 分　　192.168.10.0



策略配置 2 分

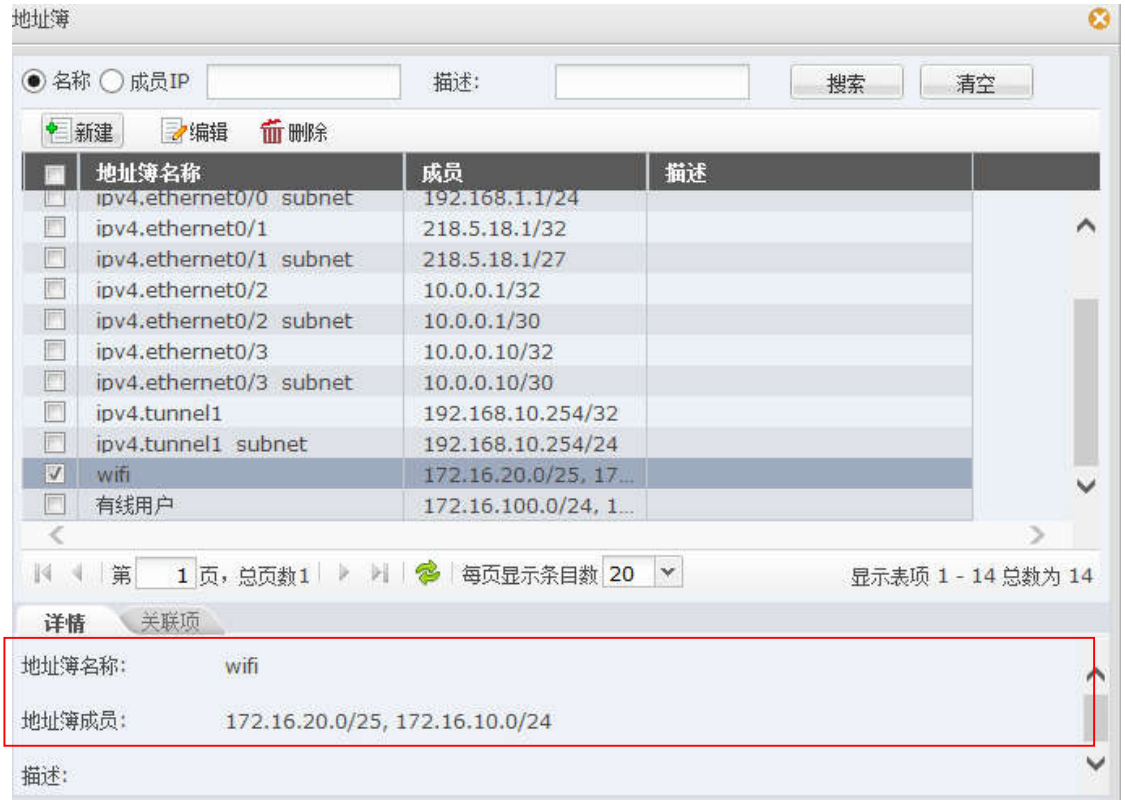
4、出于安全考虑，无线用户移动性较强，无线用户访问 Internet 是需要采用实名认证，在防火墙上开启 web 认证，账号密码为 2018web。（6 分）

Web 认证参数配置 2 分

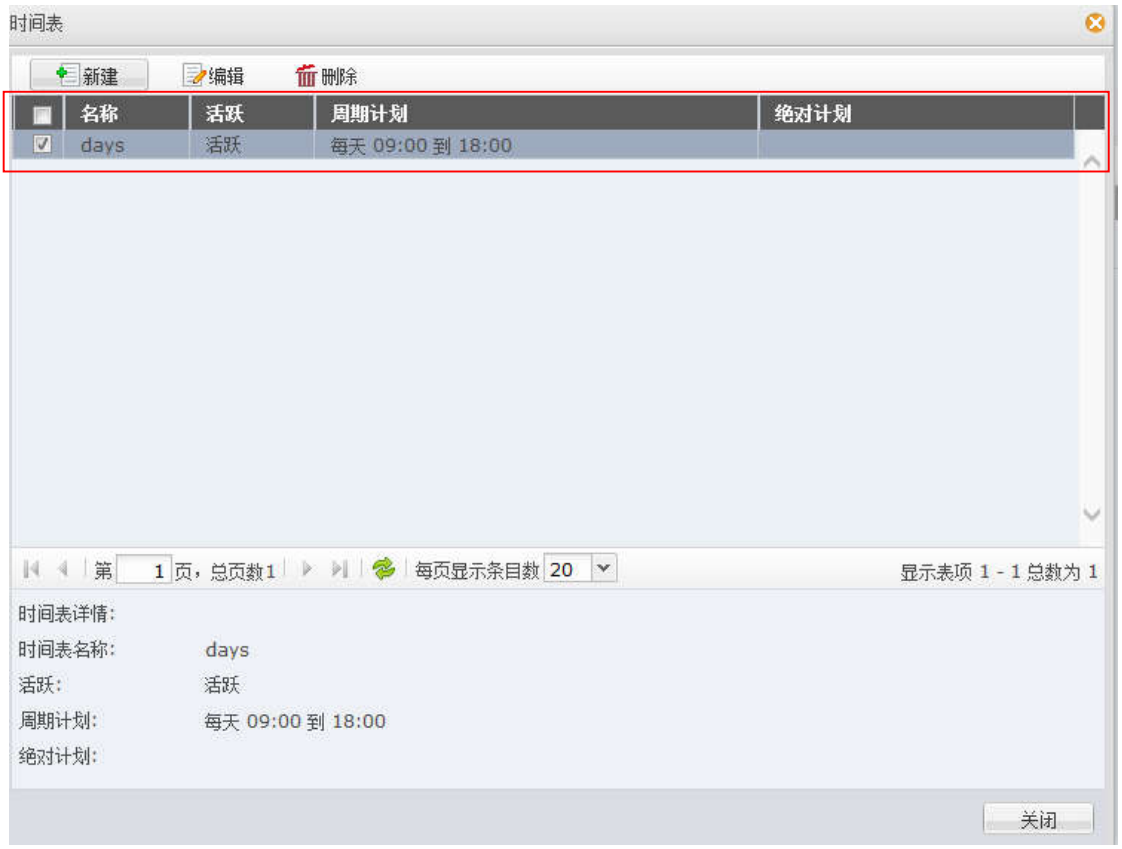
策略配置 2 分

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）



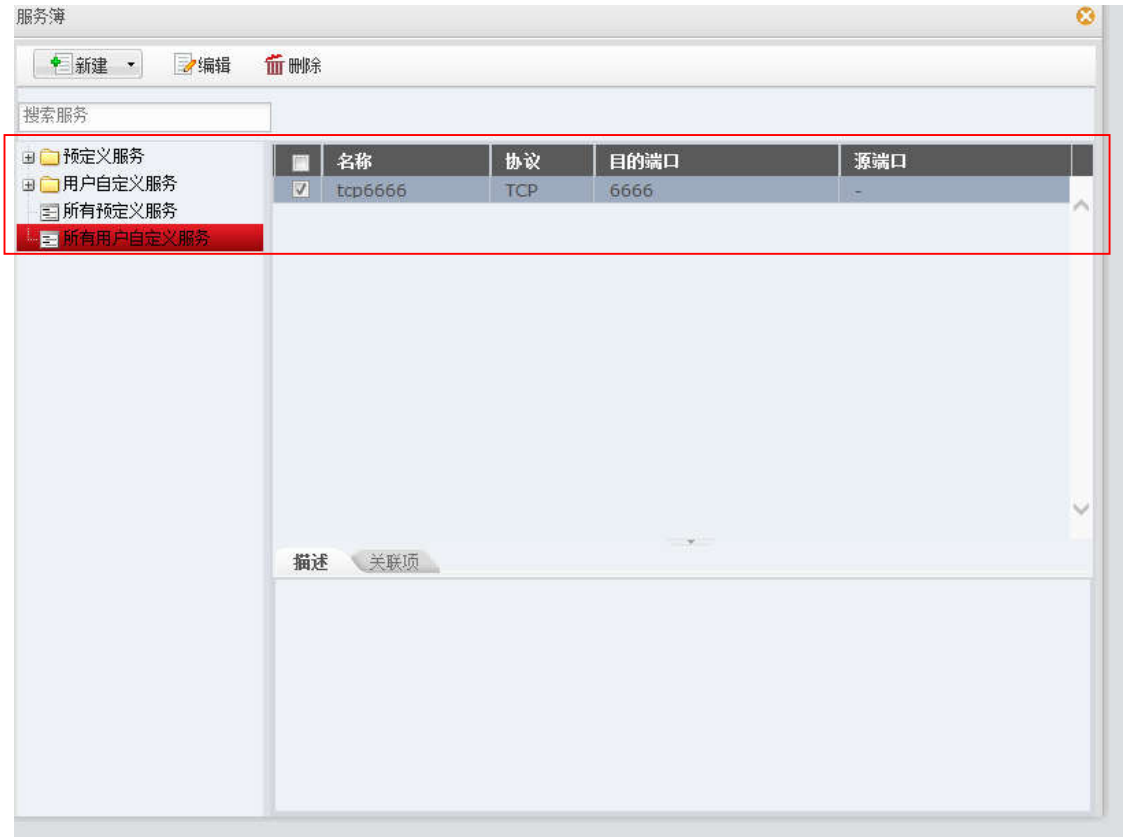
地址设置 2 分



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）

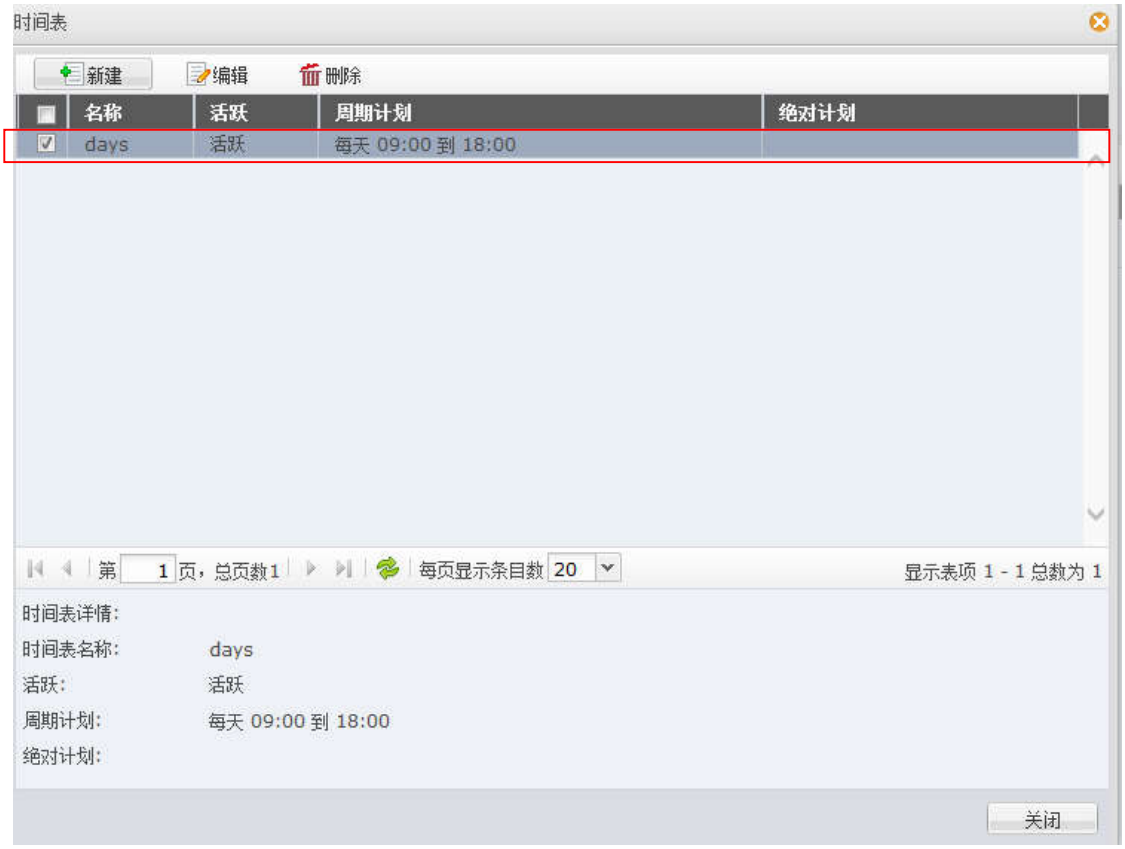


服务簿设置 2 分

目的 nat 2 分

策略 2 分

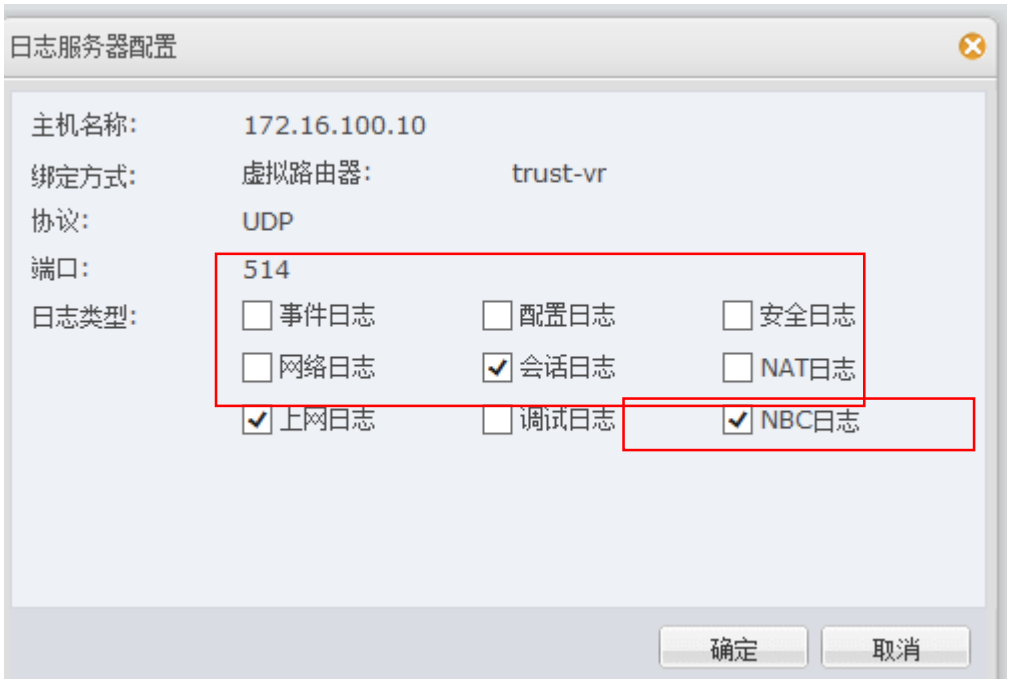
7、在 DCFW 做相关配置要求防火墙能够记录每天 9:00-18:00 内网用户访问外网的 URL，保存在日志服务器；（6 分）



时间表 2 分


应用行为控制规则配置
名称:
url日志
(1~31)字符
当满足以下条件时
目的安全域:
untrust
用户:
Any
配置
时间表:
days
配置
做如下控制
FTP控制
HTTP控制
GET
请输入域名
允许
记录日志
添加
类型
域名
动作
日志
编辑
GET
-
允许
记录日志
删除
HTTP阻止下载
确定
取消

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
确定
取消

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 外发规则配置无线 1 分


关键字类别
新建
编辑
删除
关键字类别
内容
病毒
病毒
攻击
攻击
关键字详情
关键字
类型
信任值
病毒
完全匹配
1
关闭

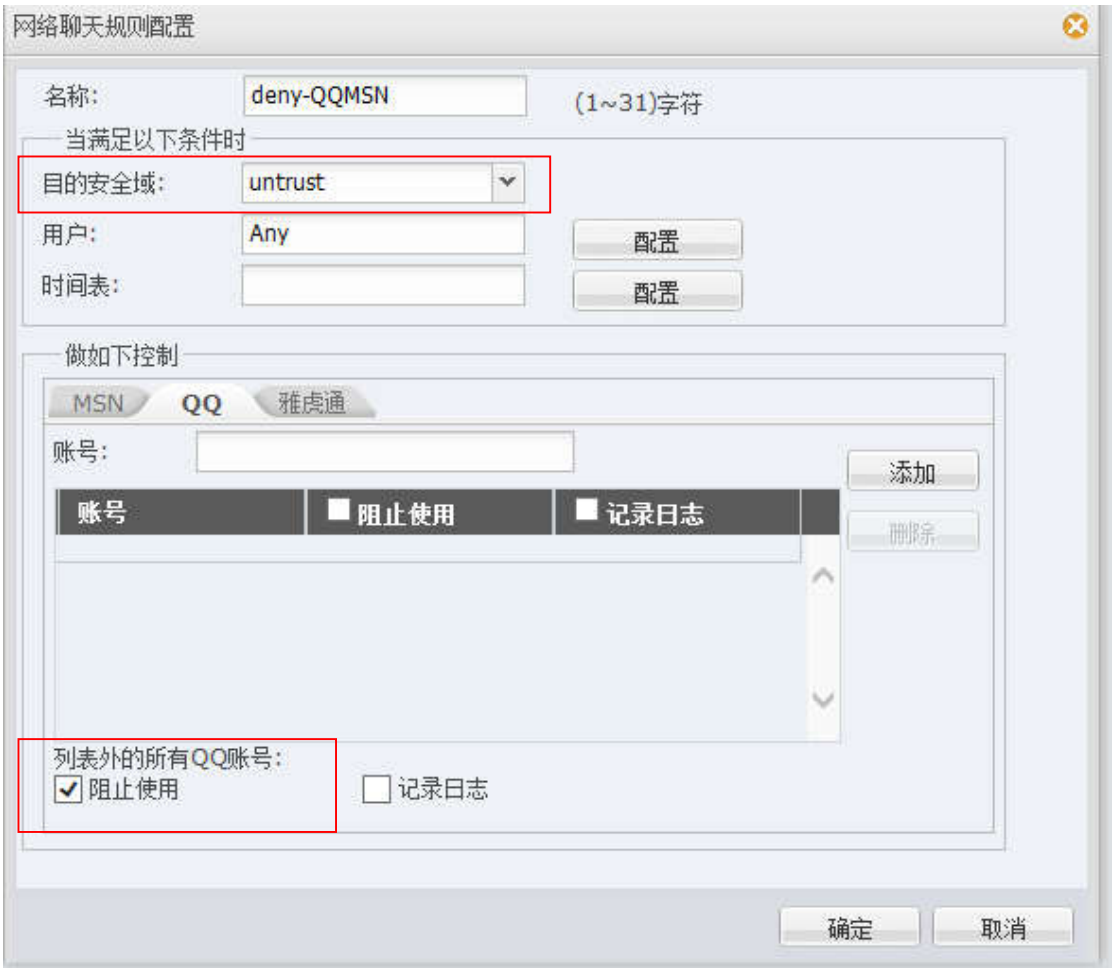
关键字配置 2 分


Web外发信息规则配置
名称:
有线用户web外发
(1~31)字符
当满足以下条件时
目的安全域:
untrust
用户:
有线用户
配置
时间表:
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
阻止外发
记录日志
病毒
攻击
确定
取消

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）

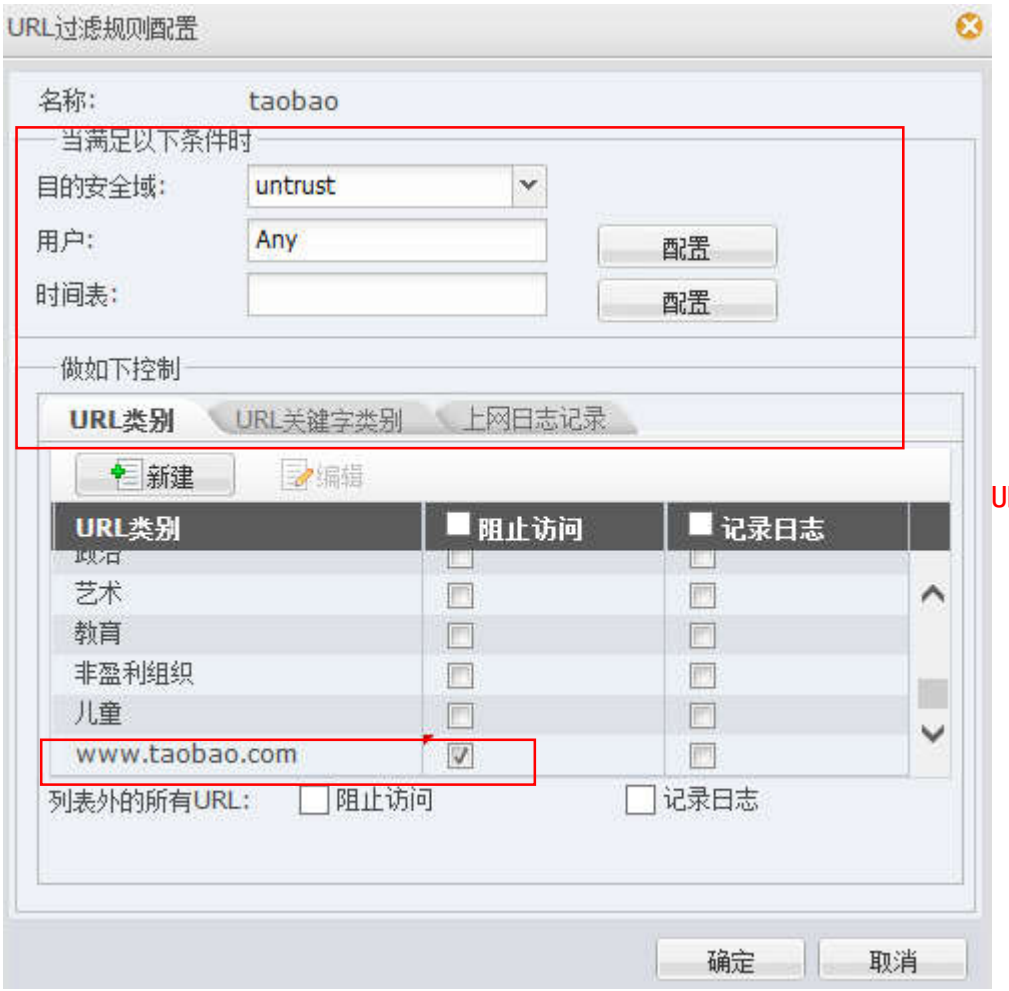
网络聊天规则 MSN 配置 1.5 分



网络聊天规则 QQ 配置 1.5 分

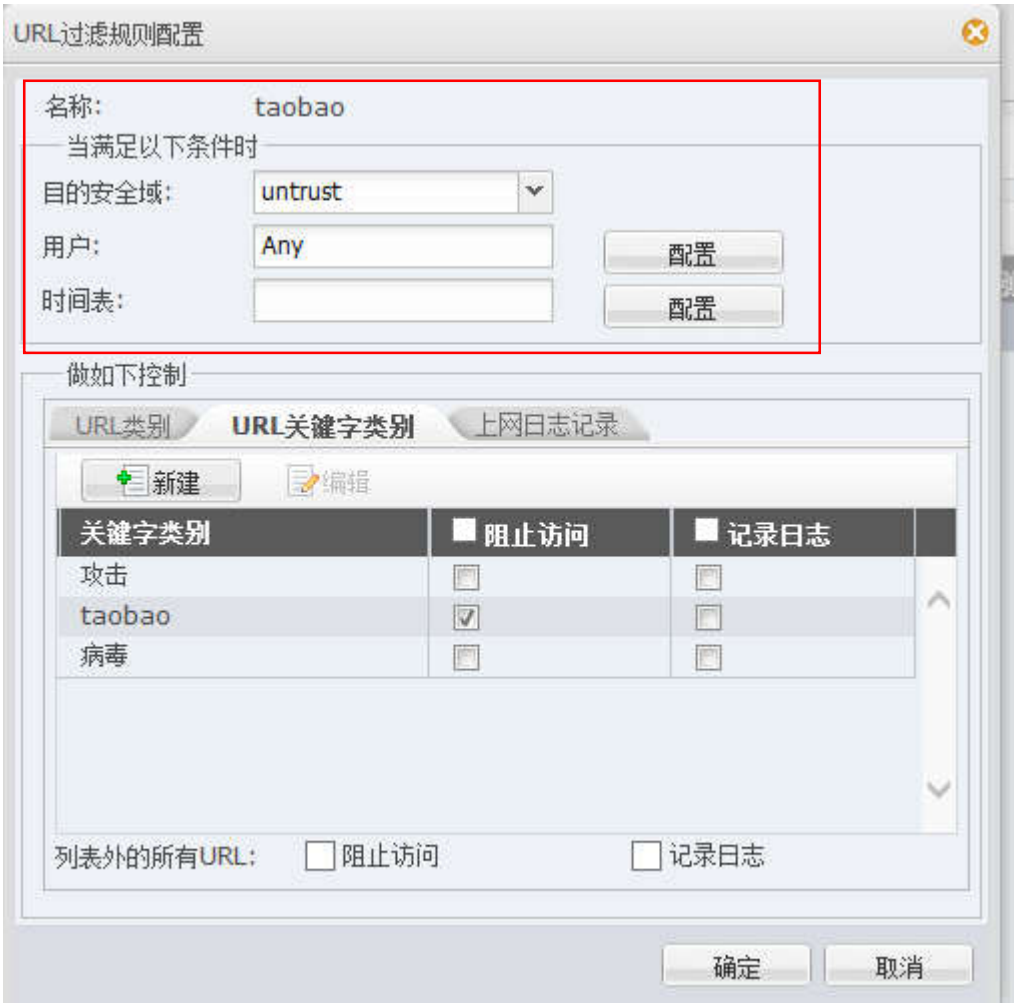
Untrust 区域启用应用识别 3 分

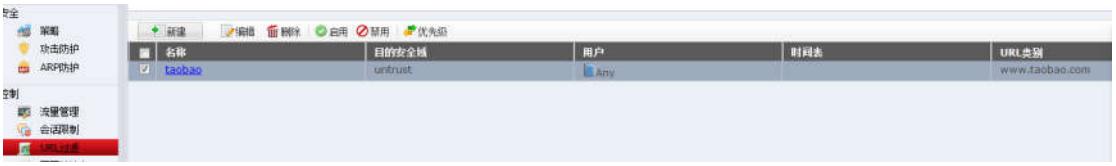
10、DCFW 上配置限制内网用户访问 www.taobao.com ，限制内网用户访问 URL 中带有 taobao 关键字的所有网站。（6 分）



URLU

URL 类别规则 3 分



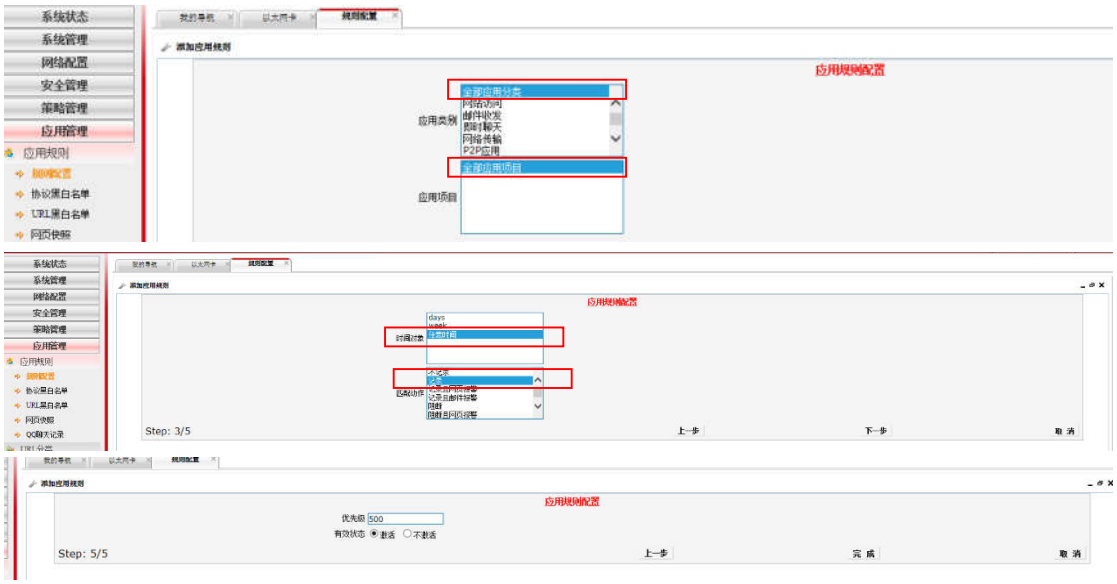


URL 关键字规则 3 分

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）

设置旁路模式 2 分

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）

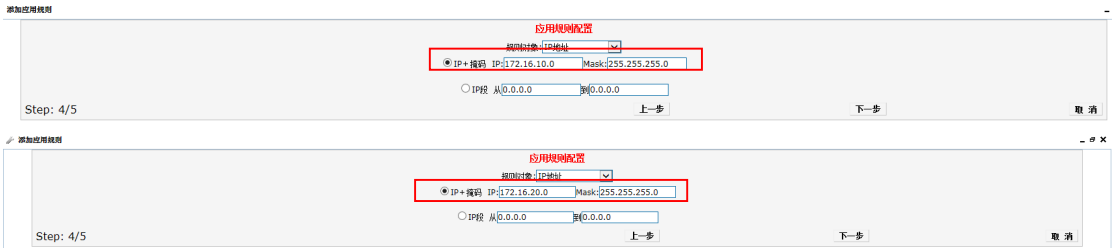
创建时间对象 1 分

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

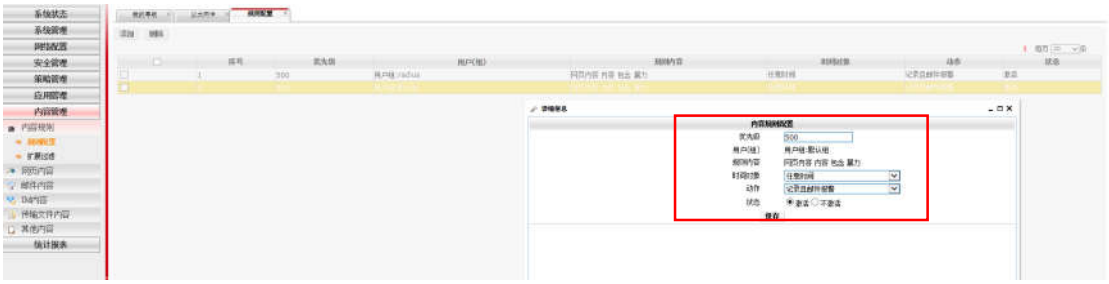
时间对象：上面自定时间范围 匹配动作 ：记录且邮件报警 1 分



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

报警阀值 3 分

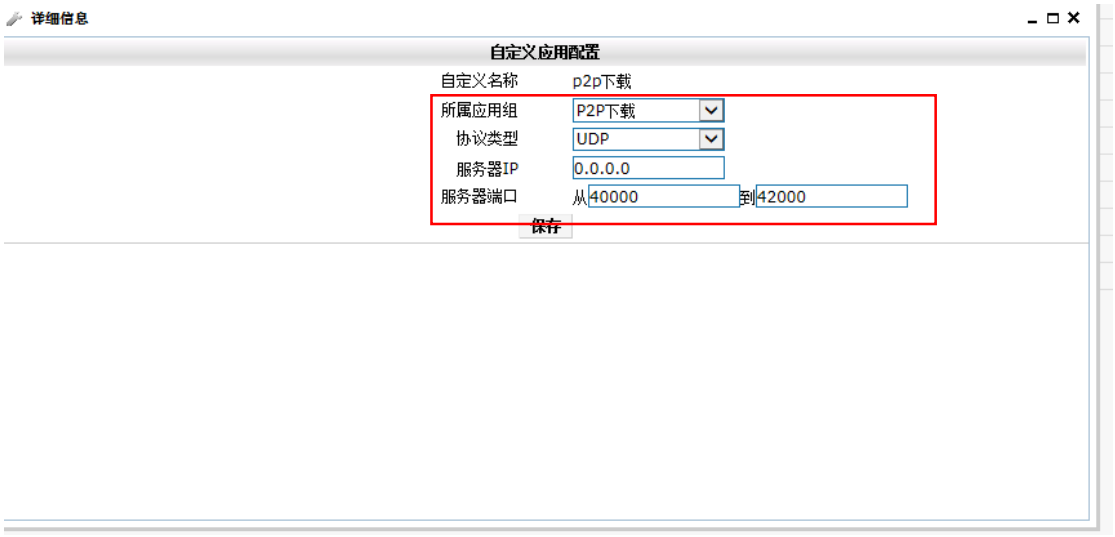
15、在 DCBI 上配置，将 DCBI 的日志信息发送到日志服务器，日志服务器 ip 172.16.100.10，community 名字 public。（6 分）

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

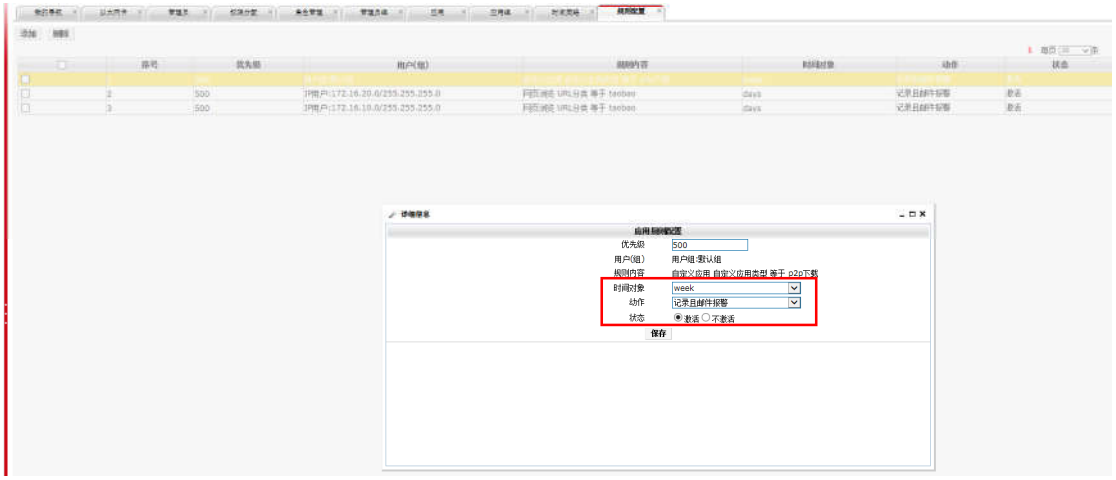
账号配置 3 分

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）



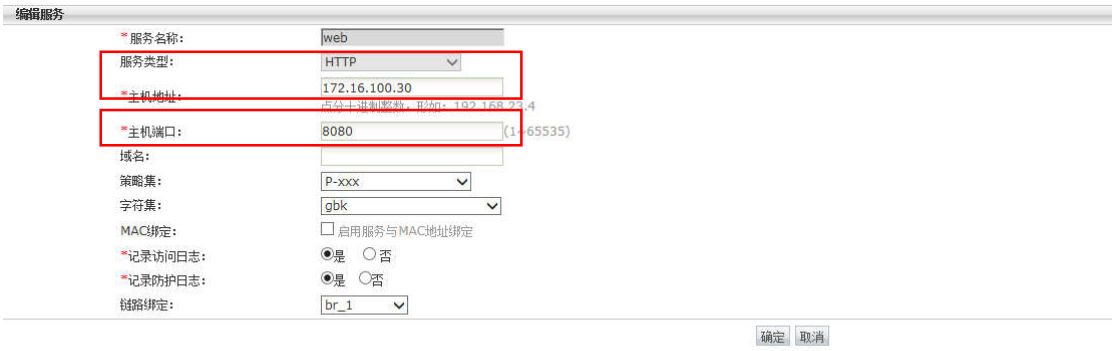
P2p 下载端口号定义 2 分

时间对象 2 分

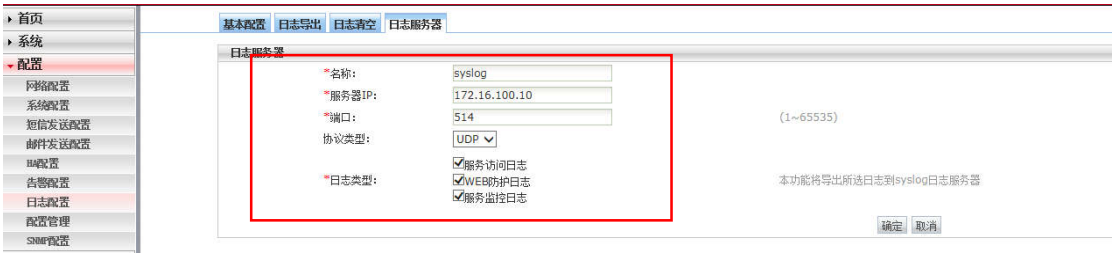


应用规则设置 2 分

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）



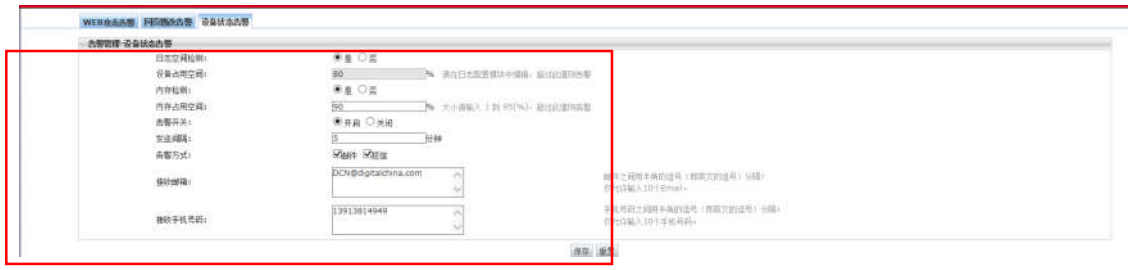
创建服务 3 分



配置日志服务器 3 分

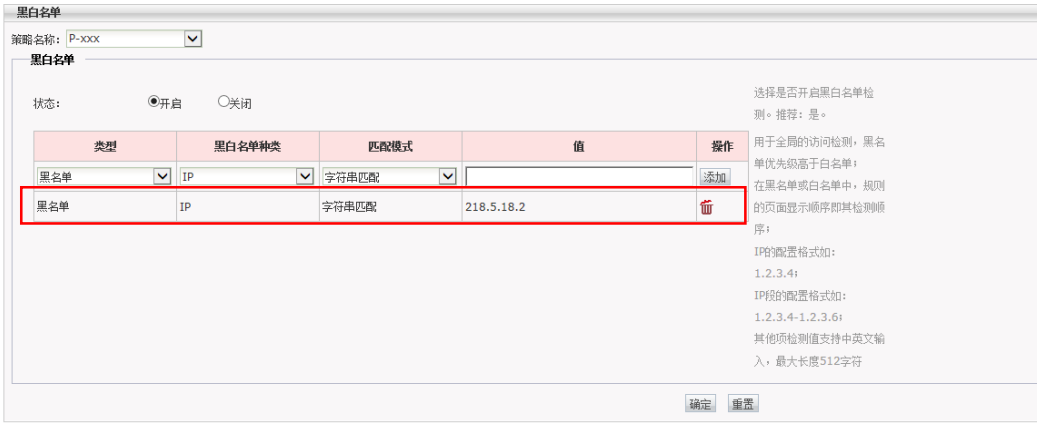
19、在公司总部的 WAF 上配置，将攻击告警、设备状态告警、服务状态告警信息通过邮件(发送到 DCN@digitalchina.com)及短信方式(发送到 13913814949)发送给管理员。（6 分）

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

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

2 分

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
 loopback-detection control shutdown
!
```

Ethernet1/0/10-24 口全部配对 3 分

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

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 阀值为 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
Interface Ethernet1/0/2
 switchport access vlan 1001
 ip dhcp snooping trust
 anti-arpscan trust supertrust-port
!
Interface Ethernet1/0/6
 storm-control broadcast 2000
 switchport access vlan 40
```

1 分

1 分

```
 switchport port-security
 switchport port-security maximum 5
 ip dhcp snooping binding user-control
!
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
!
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
!
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　1 分　1 分　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
 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
 switchport access vlan 40
 switchport port-security
```

1.5 分　1.5 分

```
 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
!
network 2
  mac authentication local
  arp-suppression
  security mode wpa-personal
  ssid DCN2018
  vlan 10
  wpa                                   key                                   encrypted
80fa7ce6b297a56f68bc50b9fa993039517386929c279637976d7292463c4ae072c64f05d0b388b
b76b9e9614dd792e2a5aefd85727da5e174be0166d29e8744
!
ap profile 1
  name Default
  hwtype 59
```

1 分

1 分

2 分

```
  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、dcntest 最多接入 20 个用户，用户间相互隔离，并对 dcntest 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 dcntest
  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	4c5bde74a8f110656874902f07378009	10
第二阶段	密码学与 IPSec 应用 2.2.4	182	4c5bde74a8f110656874902f07378009	10
第二阶段	密码学与 IPSec 应用 2.2.5	94	f4b9ec30ad9f68f89b29639786cb62ef	10
第二阶段	密码学与 IPSec 应用 2.2.6	126	069059b7ef840f0c74a814ec9237b6ec	10
第二阶段	Web 应用渗透测试与安全开发 2.3.1	Ismae_SC-2018	7ac300f71f8406a818f3d29f68010376	8
第二阶段	Web 应用渗透测试与安全开发 2.3.2	%|_|.|-|''|strstr($keyword,$str3)	c244e4a9361ae28d0e2db6a164d77f25	8
第二阶段	Web 应用渗透测试与安全开发 2.3.3	strstr($keyword,$str5)	89b53faa25aa01b615b4ada07cd2ba78	8
第二阶段	Web 应用渗透测试与安全开发 2.3.4	strstr($keyword,$str1)	95185a526beb869daf2861853674652d	9
第二阶段	Web 应用渗透测试与安全开发 2.3.5	strstr($keyword,$str2)	c4e7be02c8ab5fb244e1ae75f4e6f57f	9
第二阶段	Web 应用渗透测试与安全开发 2.3.6	strstr($keyword,$str4)	2a523f2ce9c3ab2d983a9348393ac9e3	9
第二阶段	Web 应用渗透测试与安全开发 2.3.7	MayBe Web Attack!	9aae798c312c02c8611f5604bc8a5fcb	9
第二阶段	ICMP 扫描渗透测试 2.4.1	time.Ether().IP().UDP()	c0bf3d4b1ae0e9423d0d72512bf7eac7	10
第二阶段	ICMP 扫描渗透测试 2.4.2	ethernet/ip/udp.tos.id	07720032a91e0d3679ecc7dfe987a87d	10
第二阶段	ICMP 扫描渗透测试 2.4.3	ttl.proto.src.dst	06493ad8a94a67a59a034d9022eb7ce7	10
第二阶段	ICMP 扫描渗透测试 2.4.4	sport.dport.len	641cb45abdf2f5722edc2ff62bf2c18c	10
第二阶段	ICMP 扫描渗透测试 2.4.5	srp1.sleep.ICMP	fc5fd0be302afb87ed7b32e10a84a053	10
第二阶段	ICMP 扫描渗透测试 2.4.6	H:!	cc1c6443a914c25bc93a4fdc674b4602	10
第二阶段	逆向分析和缓冲区溢出渗透测试 2.5.1	P@ssWOrd_FLAG01	873fa5f8f187209e96f4ac83ea90bb9e	8
第二阶段	逆向分析和缓冲区溢出渗透测试 2.5.2	P@ssWOrd_FLAG02	c241d98c7547093b88829952ad6f3ade	8
第二阶段	逆向分析和缓冲区溢出渗透测试 2.5.3	P@ssWOrd_FLAG03	66f99900e09e636ea17bce461ef2b7c0	8
第二阶段	逆向分析和缓冲区溢出渗透测试 2.5.4	P@ssWOrd_FLAG04	c622ddedf96ae83bba1bf1b5f9945841	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	cee3b41114e32be4d35c6ce96ef877e1	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	663337aae0b0f155d01af87188affd02	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	1db3e4f1e87944c183ce9abb72222237	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	e75dc7bb22c50084efbf965336433cbf	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	0590b112cd2c4e2ae4f4021bee0512db	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	93df62c5ff4421aaa8de680f3034a712	8
第二阶段	云服务安全渗透测试 2.6.1	230	6da9003b743b65f4c0ccd295cc484e57	7
第二阶段	云服务安全渗透测试 2.6.2	9	45c48cce2e2d7fbdea1afc51c7c6ad26	7
第二阶段	云服务安全渗透测试 2.6.3	buf + ret + pad + shellcode	9d2ea64dc9ba850991741eb93499cc2d	7
第二阶段	云服务安全渗透测试 2.6.4	conn.connect((host,port))	c0657468eb445839acba679770cc5143	7
第二阶段	云服务安全渗透测试 2.6.5	conn.recv	a63bba5d241515337f3daa652a20a82d	7
第二阶段	云服务安全渗透测试 2.6.6	USER	2e40ad879e955201df4dedbf8d479a12	7
第二阶段	云服务安全渗透测试 2.6.7	inp	2c6f00854b4702a9da9a18e5fcfdf279	7
第二阶段	云服务安全渗透测试 2.6.8	\r\n	81051bcc2cf1bedf378224b0a93e2877	7
第二阶段	云服务安全渗透测试 2.6.9	os.system	666c6cd1eeaf67cba5b5425295fcb75c	8
第二阶段	云服务安全渗透测试 2.6.10	8888	cf79ae6addba60ad018347359bd144d2	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.	0f815e1d54fbdda2e3fd0f925cae7e6e	8
第三阶段	基本 FLAG	123456		