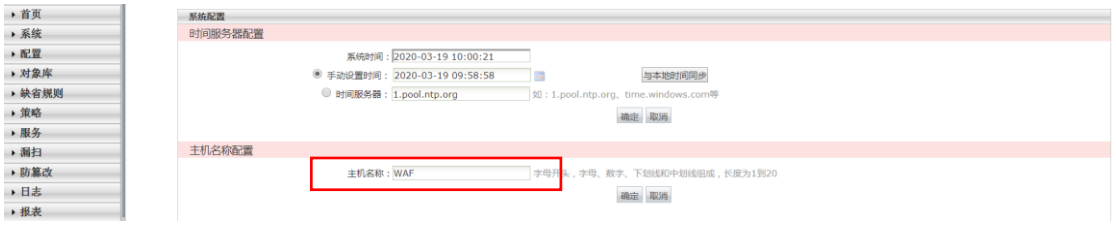
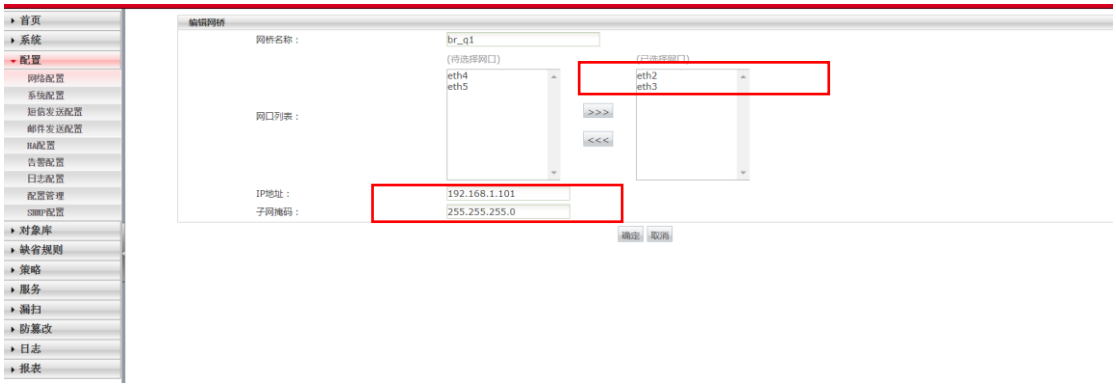
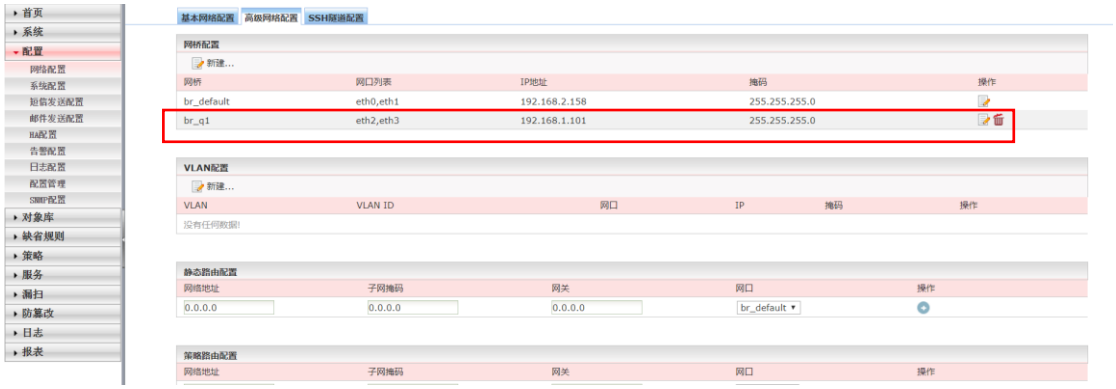
第一阶段，任务一：

一、WAF 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（9 分）说明主机名称正确 3 分，网桥接口配置 3 分，ip 地址配置 3 分







二、DCRS 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。（24 分）说明每个 vlan 和 IP 地址配置正确 3 分，错一个扣 3 分,设备名称配置正确 3 分，错一个扣 3 分

1、vlan 及 ip 配置

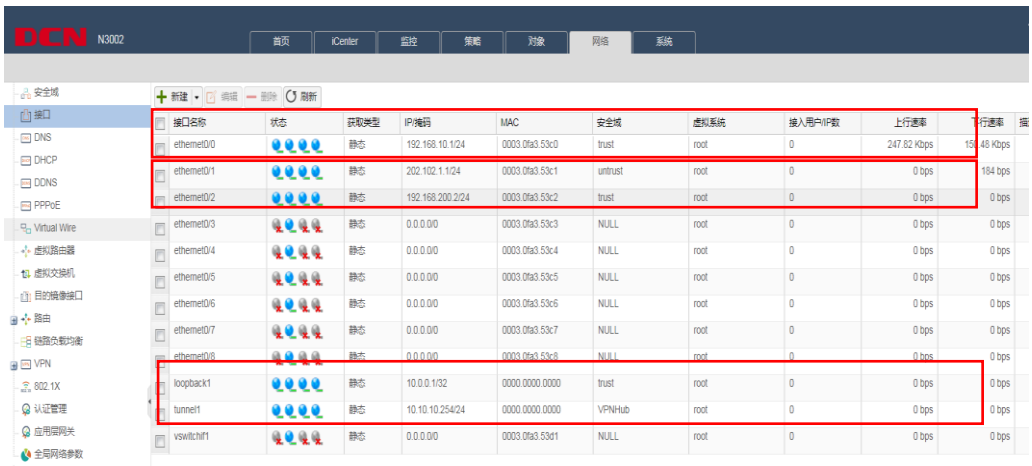
```
DCRS#show running-config | begin interface
interface Vlan1
 ip address 192.168.1.254 255.255.255.0
!
interface Vlan10
 ip address 192.168.10.254 255.255.255.0
!
interface Vlan20
 ip address 192.168.20.254 255.255.255.0
!
interface Vlan30
 ip address 192.168.30.254 255.255.255.0
!
interface Vlan40
 ip address 192.168.40.254 255.255.255.0
!
interface Vlan200
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 0 12345
 ip address 192.168.200.254 255.255.255.0
!
interface Loopback1
 ip address 10.0.0.2 255.255.255.255
!
```

1、 设备命名

```
hostname DCRS
```

三、DCFW 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。（13 分）说明 IP 地址配置 10 分，主机名称 3 分

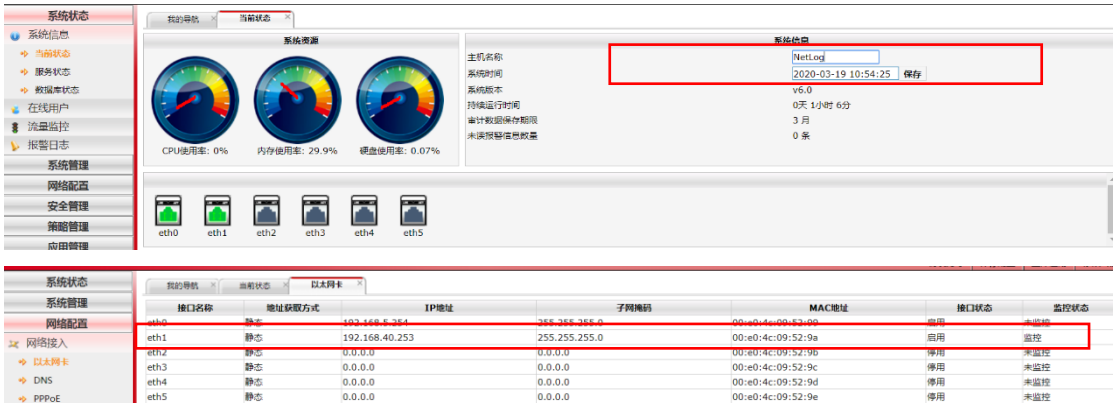
2、 防火墙接口配置



四、DCWS 根据网络拓扑图所示，按照 IP 地址参数表，在 DCWS 上创建相应的 VLAN，并将相应接口划入 VLAN，对 DCWS 的管理 IP 地址进行配置。（12 分）说明设备命名 3 分，vlan 及 ip 地址配置正确 9 分

```
AC#show run
!
no service password-encryption
!
hostname AC
sysLocation China
sysContact 400-810-9119
!
username admin privilege 15 password 0 admin
!
authentication line console login local
!
!
!
AC# show running-config | begin interface
interface Vlan50
 ip address 192.168.50.254 255.255.255.0
!
interface Vlan60
 ip address 192.168.60.254 255.255.255.0
!
interface Vlan200
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 0 12345
 ip address 192.168.200.253 255.255.255.0
!
```

五、DCBI-Netlog 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。（8 分）说明名称设置 3 分，接口及 ip 地址设置 5 分



六、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。（11 分）每个 vlan 及 接口配置正确 1 分

```
CS6200-28X-EI#show vlan
VLAN  Name            Type        Media      Ports
----  --------------  ----------  ---------  ------------------------------------
1     default         Static      ENET       Ethernet1/0/1         Ethernet1/0/3
                                             Ethernet1/0/9         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
                                             Ethernet1/0/25        Ethernet1/0/26
                                             Ethernet1/0/27        Ethernet1/0/28
10    VLAN0010        Static      ENET
20    VLAN0020        Static      ENET       Ethernet1/0/4
30    VLAN0030        Static      ENET       Ethernet1/0/5
40    VLAN0040        Static      ENET       Ethernet1/0/7         Ethernet1/0/8
200   VLAN0200        Static      ENET       Ethernet1/0/2         Ethernet1/0/6
```

七、外网出口采用静态路由的方式，无线 AC,核心交换机和防火墙之间 ospf 动态路由实现全网络互连（23 分）说明：防火墙路由配置 7 分，交换机和 AC 路由配置每个 8 分

1、 防火墙路由

```
router ospf 1
  router-id 10.0.0.1
  default-information originate
  network 192.168.200.0/24 area 0.0.0.0
  network 10.0.0.1/32 area 0.0.0.0
  redistribute connected
  area 0.0.0.0 authentication message-digest
 exit
exit
```

2、 交换机路由

```
!
router ospf
 area 0 authentication message-digest
 network 10.0.0.2/32 area 0
 network 192.168.1.0 0.0.0.255 area 0
 network 192.168.10.0/24 area 0
 network 192.168.20.0/24 area 0
 network 192.168.30.0/24 area 0
 network 192.168.40.0/24 area 0
 network 192.168.200.0/24 area 0
!
!
```

3、AC 路由配置

```
!
router ospf
 area 0 authentication message-digest
 network 192.168.50.0 0.0.0.255 area 0
 network 192.168.60.0 0.0.0.255 area 0
 network 192.168.200.0 0.0.0.255 area 0
!
!
```

第一阶段，任务二：

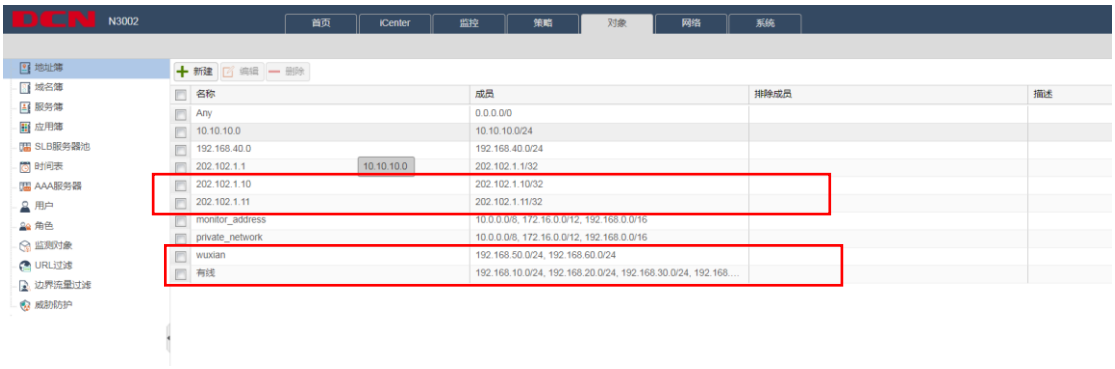
DCFW:

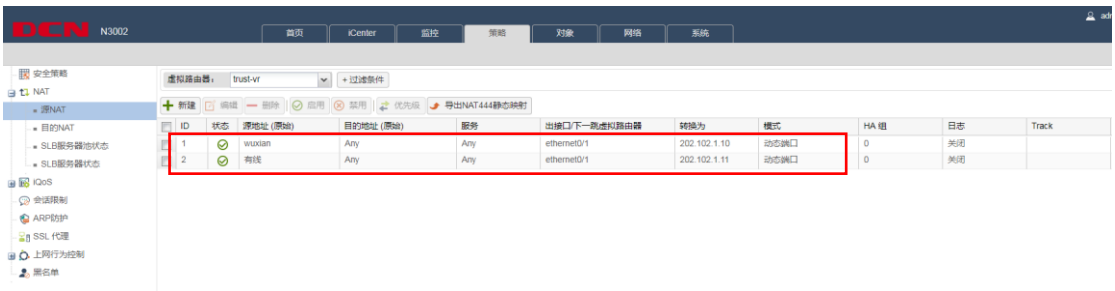
1. 在总公司的 DCFW 根据题意配置 Trust,Untruct,VPNhub 区域，并配置区域之间的放行策略，策略采用严格控制；15 分

   说明：接口区域配置正确 6 分，错一个 2 分，策略配置正确 9 分，错一个 3 分

2. 防火墙做基本配置，实现内网对外网因特网的访问；无线用户上网转换为 202.102.1.10，有线用户转换为 202.102.1.11；10 分

说明：地址配置正确 5 分，NAT 配置正确 5 分





3. DCFW 连接 Internet 的区域上配置以下攻击防护：10 分

开启以下 Flood 防护：

ICMP 洪水攻击防护，警戒值 2000，动作丢弃；

UDP 供水攻击防护，警戒值 1500，动作丢弃；

SYN 洪水攻击防护，源警戒值 5000，目的警戒值基于 IP 2000，动作丢弃；

开启以下 DOS 防护：

Ping of Death 攻击防护；

Teardrop 攻击防护；

IP 选项，动作丢弃；

ICMP 大包攻击防护，警戒值 2048，动作丢弃；

4. 配置回环接口 ip 为 10.0.0.1/32，作为 OSPF 协议 router-id； 4 分

5. 防火墙和三层交换机之间运行 OSPF 路由协议，为了路由协议安全两个设备之间 ospf 之间要进行加密认证,key 为 12345，采用 MD5 认证。10 分

说明：ospf 配置正确 3 分；认证 3 分；结果 4 分；

```
interface ethernet0/2
  zone  "trust"
  ip address 192.168.200.2 255.255.255.0
  manage ping
  manage telnet
  manage ssh
  manage http
  manage https
  ip ospf authentication message-digest
  ip ospf message-digest-key 1 md5 GtIX7KCpy8aI20lpWYBxumuLRWcM
exit
```

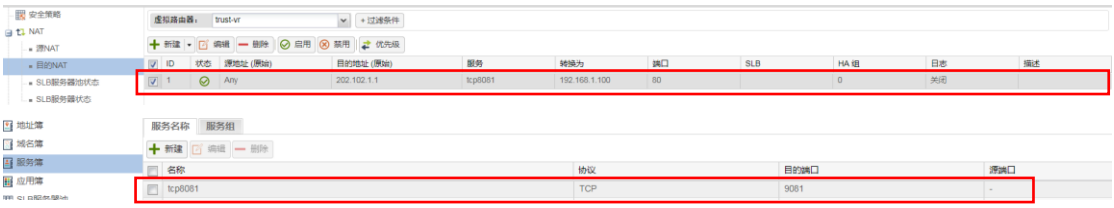
```
  router ospf 1
    router-id 10.0.0.1
    default-information originate
    network 192.168.200.0/24 area 0.0.0.0
    network 10.0.0.1/32 area 0.0.0.0
    redistribute connected
    area 0.0.0.0 authentication message-digest
  exit
exit
```

```
login: admin
password:
DCFW-1800# show ip route
Codes: K - kernel route, C - connected, S - static, Z - ISP, R - RIP, O - OSPF,
       B - BGP, D - DHCP, P - PPPoE, W - wireless, H - HOST, G - SCVPN, U - VPN, M - IMPORT,
       I - ISIS, Y - SYNC, L - llb outbound, > - selected first nexthop, * - FIB route, b - BFD enab
le

Routing Table for Virtual Router <trust-vr>
------------------------------------------------------------------------------
S>* 0.0.0.0/0 [1/0/1] via 202.102.1.2, ethernet0/1
H>* 10.0.0.1/32 [0/0/1] is local address, loopback1
O>* 10.0.0.2/32 [110/2/1] via 192.168.200.254, ethernet0/2, 00:50:38
C>* 10.10.10.0/24 is directly connected, tunnel1
H>* 10.10.10.254/32 [0/0/1] is local address, tunnel1
O>* 192.168.1.0/24 [110/2/1] via 192.168.200.254, ethernet0/2, 00:50:38
C>* 192.168.10.0/24 is directly connected, ethernet0/0
H>* 192.168.10.1/32 [0/0/1] is local address, ethernet0/0
O>* 192.168.50.0/24 [110/2/1] via 192.168.200.253, ethernet0/2, 00:17:56
O>* 192.168.60.0/24 [110/2/1] via 192.168.200.253, ethernet0/2, 00:20:08
C>* 192.168.200.0/24 is directly connected, ethernet0/2
H>* 192.168.200.2/32 [0/0/1] is local address, ethernet0/2
C>* 202.102.1.0/24 is directly connected, ethernet0/1
H>* 202.102.1.1/32 [0/0/1] is local address, ethernet0/1
------------------------------------------------------------------------------
DCFW-1800#
```

6. 根据 IP 地址表，把 DCST 的 IP 地址映射到外网，使 PC 能够通过防火墙外网地址访问 DCST，外网访问端口号为 9081. 15 分

说明：服务簿配置正确 4 分，目的 nat 配置正确 6 分，策略配置正确 5 分



7. 出于安全考虑，只允许 192.168.1.0/24 和 192.168.200.0/24 网段地址能通过带内方式管理防火墙。6 分

DCRS：

1. 将连接 DCFW 的双向流量镜像至 8 口由 Netlog 进行监控和分析； 10 分

```
monitor session 1 source interface Ethernet1/0/2 tx
monitor session 1 source interface Ethernet1/0/2 rx
monitor session 1 destination interface Ethernet1/0/8
```

2. 接入 DCRS Eth4，仅允许 IP 地址 192.168.20.1-10 为源的数据包为合法包，以其它 IP 地址为源地址，交换机直接丢弃； 10 分

```
!
am enable
!
Interface Ethernet1/0/4
 switchport access vlan 30
 am port
 am ip-pool 192.168.20.1 10
```

3. 配置认证服务器，IP 地址是 192.168.2.100，radius key 是 dcn2020;在公司总部的 DCRS 上配置，需要在交换机 E1/0/21 接口上开启基于 MAC 地址模式的认证，认证通过后才能访问网络；18 分

```
radius-server key 0 dcn2020
radius-server authentication host 192.168.2.100
aaa enable
!
dot1x enable
Interface Ethernet1/0/21
 dot1x enable
 dot1x port-method macbased
```

4. 配置公司总部的 DCRS，通过 DCP（Dynamic CPU Protection）策略，防止 DCRS 受到来自于全部物理接口的 DOS（Denial Of Service）攻击，每秒最多 30 个包；10 分

```
dcp enable
dcp limit-rate 30
!
```

5. 交换机上启用回环接口 IP 地址为 10.0.0.2/32,并配置 dhcp server 服务为 AP 分配 IP 地址，地址池范围为：192.168.200.100-192.168.200.150，AP 通过 Option43 方式获取 AC 地址。16 分 说明错一个本题不得分

```
!
service dhcp
!
ip dhcp pool vlan200
 network-address 192.168.200.0 255.255.255.0
 default-router 192.168.200.254
 option 43 hex 0104C0A8C8FD
!
interface Loopback1
```

ip address 10.0.0.2 255.255.255.255

!

6. 在交换机上实现禁止 VLAN20 网段的任何计算机通过 BT 下载和做 BT 种子，BT 常用端口范围 6881~6890。 6 分

```
ip access-list extended bt
  deny tcp 192.168.20.0 0.0.0.255 any-destination d-port range 6881 6890
  deny udp 192.168.20.0 0.0.0.255 any-destination d-port range 6881 6890
  permit ip any-source any-destination
  exit
```

DCWS：

1. 开启无线功能，指定 AC 管理地址为 192。168.200.253；10 分 说明配置需要全部正确错一个本题不得分。

```
wireless
 no auto-ip-assign
 enable
 static-ip  192.168.200.253
ap profile 1
  name Default
  hwtype 59
Interface Ethernet1/0/23
 switchport mode trunk
 switchport trunk native vlan 200
```

2. AP 注册到 AC 采用序列号认证；14 分

```
ap authentication serial-num
ap database 00-03-0f-93-93-00
  serial-num WL0204201525002287
```

3. 开启 dhcp 服务，为无线用户分配 IP 地址，前 10 个 ip 为保留地址，地址租约时间为 10 小时，DNS-SERVER 为 61.147.37.1；10 分 说明服务开启 2 分，每个地址池 3 分，排除 2 分；

```
service dhcp
!
ip dhcp excluded-address 192.168.50.1 192.168.50.10
ip dhcp excluded-address 192.168.60.1 192.168.60.10
ip dhcp pool vlan50
 network-address 192.168.50.0 255.255.255.0
 lease 0 10 0
 default-router 192.168.50.254
 dns-server 61.147.37.1
!
ip dhcp pool vlan60
 network-address 192.168.60.0 255.255.255.0
 lease 0 10 0
 default-router 192.168.60.254
 dns-server 61.147.37.1
!
```

4. 设置 SSID DCN2020，VLAN50，加密模式为 wpa-personal，其口令为 GSdcn2020 的；设置 SSID dcntest ，VLAN60 不进行认证加密，做相应配置隐藏该 ssid；14 分 说明 network1 配置正确 7 分，network2 配置正确 7 分。

```
network 1
  security mode wpa-personal
  ssid DCN2020
  vlan 50
  wpa key encrypted 7d5a1f46ec0c4b544b5fc
!
```

```
 network 2
  hide-ssid
  client-qos bandwidth-limit down 2048
  client-qos bandwidth-limit up 1024
  max-clients 20
  ssid dcntest
  vlan 60
  station-isolation
!
radio 1
   dot11n channel-bandwidth 20
   vap 0
!
   vap 1
    enable
!
!
  radio 2
   dot11n channel-bandwidth 40
   vap 0
!
   vap 1
    enable
```

5. 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；10 分

```
network 2
hide-ssid
  client-qos bandwidth-limit down 2048
  client-qos bandwidth-limit up 1024
```

```
max-clients 20
```

6. 禁止 MAC 地址为 C417.C417.C417 的无线终端连接。12 分

```
mac-authentication-mode black-list
static-ip  172.17.254.1
known-client c4-17-c4-17-c4-17 action global-action
```