

## 2019-信息安全管理与评估

author: leadlife

data: 2022/10/13

微信: Tripse

知识星球: LeadlifeSec

QQ: 482949203

QQ群: 775454947

### 赛题基本信息

#### 选取赛题

2019 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-04

#### 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

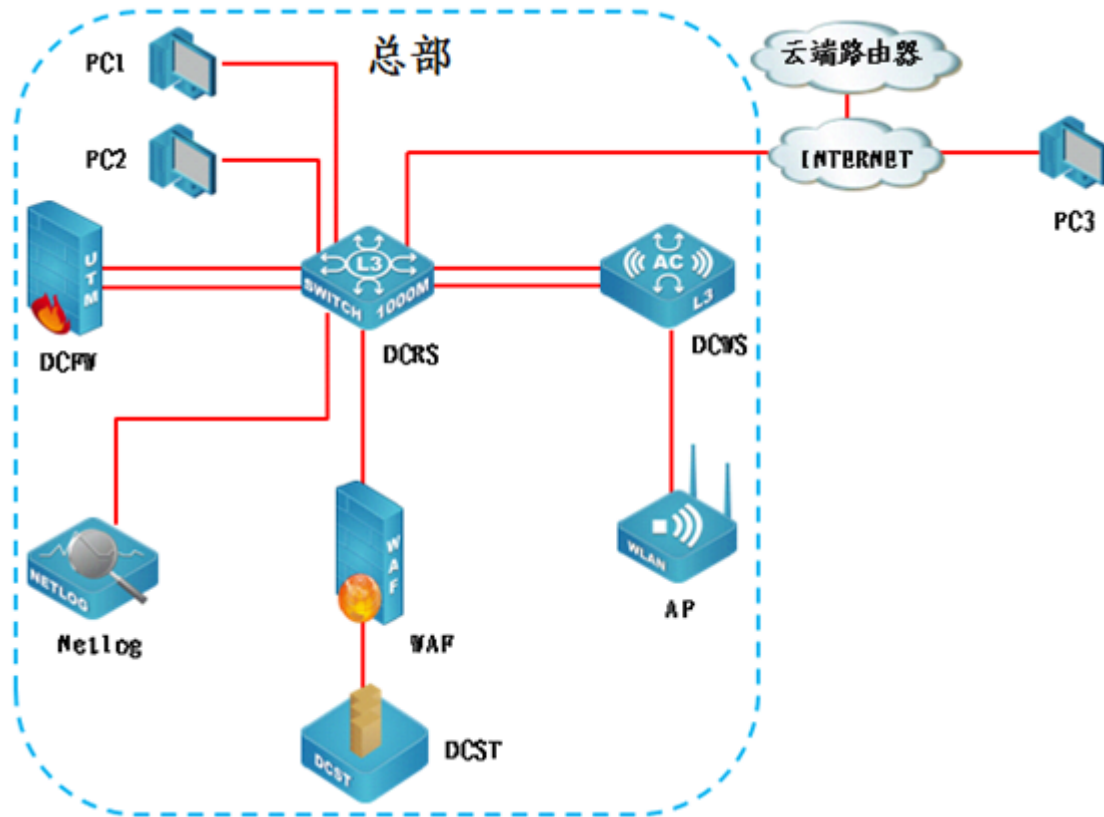
本次大赛，各位选手需要完成三个阶段的任务，其中第一个阶段需要按裁判组专门提供的U盘中的“XXX-答题模板”提交答案。第二、三阶段请根据现场具体题目要求操作。

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 DCFW	ETH0/1-2	10.0.0.1/30 (Trust 安全域)	DCRS
		218.5.18.1/27 (untrust 安全域)	DCRS
		172.16.200.1/24	DCRS
	Tunnel 1	12.12.12.1/24	云端路由器
	SSL Pool	192.168.10.1/24 可用 IP 数量为 20	SSL VPN 地址池
三层交换机 DCRS	ETH1/0/4	—	DCWS ETH1/0/4
	ETH1/0/5	—	DCWS ETH1/0/5
	VLAN49 ETH1/0/1	10.0.0.2/30	DCFW
	VLAN50 ETH1/0/2	218.5.18.2/27	DCFW
	VLAN 51 ETH1/0/3	10.0.0.10/30	DCBI
	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 ETH1/0/7-9	172.16.30.1/26	PC1
	VLAN 40 ETH1/0/10-12	192.168.40.1/24	PC2
	VLAN 100	192.168.100.1/24	DCWS
	VLAN 200	172.16.200.2/24	DCFW
	ETH1/0/24	—	INTERNET
无线控制器 DCWS	VLAN 100	192.168.100.254/24	DCRS
	无线管理 VLAN VLAN 101	192.168.101.1/24	AP

	ETH1/0/3		
日志服务器 DCBI	ETH2	10.0.0.9/30	DCRS
WEB 应用防火墙	ETH2	172.16.100.2/24	DCST
WAF	ETH3		DCRS
堡垒服务器 DCST	—	—	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 DCFW	http://192.168.1.1	ETH0	admin	admin
网络日志系统 DCBI	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 DCRS	—	Console	—	—
无线交换机 DCWS	—	Console	—	—
堡垒服务器 DCST	—	—	—	
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。			

## 第一阶段

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DCFW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DCRS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DCRS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DCWS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DCBI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。

## DCFW 操作

## DCRS 操作

## DCWS 操作

## DCBI (NetLog) 操作

## WAF 操作

## 第二阶段

## RS SSH 远程管理与账户登录

### 涉及题型

- 总部核心交换机 DCRS 上开启 SSH 远程管理功能，本地认证用户名:2019DCN,密码: DCN2014;

## 注意点

- 开启 SSH 服务
- 添加用户和密码
- 操作 vty 本地认证登录

## 命令

code	explanation
ssh-server enable	开启 ssh 服务
authentication line vty login local	操作用户为本地认证方式
若题目要求，只需要密码登录验证可以操作如下	
DCRS(config)#authentication vty login only-password	

## 操作

```
1 DCRS(config)#language chinese
2 DCRS(config)#ssh-server enable
3 DCRS(config)#username 2019DCN password DCN2014
4 DCRS(config)#authentication line vty login local
```

## RS MSTP 多实例生成树冗余线路-负载均衡调式

## 涉及题型

```
1 总部启用 MSTP 协议，NAME 为 DCN2014、 Revision-level 1，实例 1 中包括 VLAN10；
2
3 实例 2 中包括 VLAN20、要求两条链路负载分担，其中 VLAN10 业务数据在 E1/0/4 进行数据转发，要求 VLAN20业务数据在E1/0/5进行数据转发，通过在DCWS两个端口设置COST值 2000000 实现；
4
5 配置 DCRS 连接终端接口立即进入转发模式且在收到 BPDU 时自动关闭端口；防止从 DCWS 方向的根桥抢占攻击；
```

## 注意点

- 开启生成树
- 绑定 vlan 实例
- 操作生成树特性使 vlan 10 与 vlan 20 流量分流
  - 这里需要提一下，在题目中具有提示，我们可以操作生成树不同实例的优先级，和开销使得流量分流
- 开启MSTP BPDU 防抢占 (这里需要注意一个术语：终端，则代表 PC 机，我们观察一下 RS 的连接终端，分别为对应端口为 E1/0/7-9 E1/0/10-12) 所以该特性在这里操作，以防止接入层的网络波动带来业务损失

## 命令

code	exlanation
spanning-tree mode	启用所属生成树特性
spanning-tree	激活生成树
spanning-tree mst configuration	进入生成树配置 Cli
instance num	绑定实例
spanning-tree mst 1 priority 0	操作实例优先级，优先级高则为根桥(数字越小越牛逼)
spanning-tree cost 100	操作端口 cost 值以分流数据，该端口将可能为根端口
spanning-tree portfast bpduguard	开启 portfast 特性中的 bpdu 报文监听，若监听非自身根桥 BPDU 报文则关闭端口，当然这种操作是不可取的，会损坏业务

## 操作

```
1 DCRS#config terminal
2 DCRS(config)#spanning-tree mode mstp
3 DCRS(config)#spanning-tree
4
5 DCRS(config)#spanning-tree mst configuration
```

```
6 DCRS(config-mstp-region)#revision-level 1
7 DCRS(config-mstp-region)#name DCN2014
8 DCRS(config-mstp-region)#instance 1 vlan 10
9 DCRS(config-mstp-region)#instance 2 vlan 20
10 DCRS(config-mstp-region)#exit
11
12 DCRS(config)#spanning-tree mst 1 priority 0
13 DCRS(config)#spanning-tree mst 2 priority 4096
14 DCRS(config)#int e1/0/1
15 DCRS(config-if-ethernet1/0/1)#spanning-tree cost 100
16
17 DCRS(config-if-ethernet1/0/1)#int e1/0/2
18 DCRS(config-if-ethernet1/0/2)#spanning-tree cost 200000
19 DCRS(config-if-ethernet1/0/2)#exit
20
21 DCRS(config)#int e1/0/7-9
22 DCRS(config-if-port-range)#spanning-tree portfast bpduguard
23 DCRS(config-if-port-range)#spanning-tree port-priority 0
24
25 DCRS(config-if-port-range)#int e1/0/10-12
26 DCRS(config-if-port-range)#spanning-tree portfast bpduguard
27 DCRS(config-if-port-range)#spanning-tree port-priority 0
28
29 DCRS(config-if-port-range)#end
```

## Port-Channel 端口聚合--加大宽带

### 涉及题型

- 1 尽可能加大总部核心交换机 DCRS 与防火墙 DCFW 之间的带宽；

### 注意点

- 我们注意是 RS 与 FW 之间的流量
- 端口聚合我们曾经操作过，需要注意 FW 的 LACP 和 on 强制模式
- 对应了 RS 的模式，如果 RS 为 Active 则我们 LACP，如果为 on 强制模式，则为二层区间
- 我们 RS 上创建的 VLAN 与 FW 的 aggregate 子接口相对应，比如 aggregate1.49 vlan 49



RS

```
1 DCRS#config terminal
2 DCRS(config)#port-group 1
3 DCRS(config)#int e1/0/1-2
4 DCRS(config-if-port-range)#switchport mode trunk
5 DCRS(config-if-port-range)#switchport trunk allowed vlan 49;50
6 DCRS(config-if-port-range)#port-group 1 mode active
```

DCFW

```
1 DCFW-1800# configure
2 DCFW-1800(config)# hostname DCFW
3 DCFW(config)# int aggregate1
4 DCFW(config-if-aggl)# ip add 0.0.0.0/0
5 DCFW(config-if-aggl)# no shutdown
6 DCFW(config-if-aggl)# exit
7
8 DCFW(config)# int aggregate1.49 ▲
9 DCFW(config-if-aggl.49)# zone trust
10 DCFW(config-if-aggl.49)# ip add 10.0.0.1/30
11 DCFW(config-if-aggl.49)# no shutdown
12 DCFW(config-if-aggl.49)# exit
13
14 DCFW(config)# int aggregate1.50 ▲
15 DCFW(config-if-aggl.50)# zone untrust
16 DCFW(config-if-aggl.50)# ip add 218.5.18.1/27
17 DCFW(config-if-aggl.50)# no shutdown
18 DCFW(config-if-aggl.50)# exit
19
20 DCFW(config)# int e0/1
21 DCFW(config-if-eth0/1)# aggregate aggregate1
22 DCFW(config-if-eth0/1)# int e0/2
23 DCFW(config-if-eth0/2)# aggregate aggregate1
```

最终截图应如此

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	l2-trust	0	0	0	
aggregate1.49		10.0.0.1/30	0003.0f82.e55e	trust	0	0	0	
aggregate1.50		218.5.18.2/27	0003.0f82.e55e	untrust	0	0	0	

然后操作一个 any 策略，RS 即可与 FW 的 10.0.0.1 通信

## 涉及题型

- 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 DCFW 进行最严格的安全防护

## 注意点

- 创建相应地址簿，vlan 业务，INTERNET 地址簿
- 然后操作策略即可，关于这题，如果赛题有强制要求，可以操作相应静态路由，开启基本攻击防护 (我建议开启)

## 操作



地址簿

☒ 名称 ☐ 成员IP

描述:

搜索

清空

配置地址簿

名称: INTERNERT

(1~95)字符

成员:

IP/掩码

IP地址

网络掩码

☐ 类型

成员

添加

删除

☐ IP地址

12.12.12.0/24

描述:

(0~255)字符

确定

取消

详情

地址簿:

地址簿:

描述:

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,

多个...

到

目的地址:

INTERNERT

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: untrust	到	目的安全域: trust
源地址: INTERNET	到	目的地址: 总部 VLAN10, 30,
服务簿: Any		时间表:
应用簿:		源用户:

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

## RS 多接口所属同 VLAN 二层接口流量隔离

### 涉及题型

- 1 总部核心交换机DCRS上实现VLAN40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；

### 注意点

- VLAN 40 所属业务 PC 终端拥有多个接口
- 所以这些接口我们要通过隔离组来操作
- 关于环路检测这里不多赘述---loopback-de...

### 操作

```
1 DCRS>enable
2 DCRS#config terminal
3 DCRS(config)#isolate-port group 10 switchport interface e1/0/10
4 DCRS(config)#isolate-port group 11 switchport interface e1/0/11
5 DCRS(config)#isolate-port group 12 switchport interface e1/0/12
```

### 环路检测

```
1 DCRS(config)#loopback-detection trap enable
2 DCRS(config)#loopback-detection interval-time 10 10
3 DCRS(config)#int e1/0/10-12
4 DCRS(config-if-port-range)#loopback-detection specified-vlan 40
5 DCRS(config-if-port-range)#loopback-detection control shutdown
6 DCRS(config-if-port-range)#exit
7 DCRS(config)#loopback-detection control-recovery timeout 3000
```

## RS 防止 ARP 欺骗-恶意 DHCP 阻断

### 涉及题型

```
1 总部核心交换机 DCRS 检测到 VLAN40 中私设 DHCP 服务器关闭该端口
```

### 注意点

有些题目在 2021 年中有出现，这里就不多赘述

- 该题型考察 DHCP Snooping 操作机制

### 操作

```
1 DCRS(config)#ip dhcp snooping enable
2 DCRS(config)#ip dhcp snooping binding enable
3 DCRS(config)#ip dhcp snooping binding arp
4 DCRS(config)#int e1/0/10-12
5 DCRS(config-if-port-range)#ip dhcp snooping binding user-control
6 DCRS(config-if-port-range)#ip dhcp snooping action shutdown
```

## RS MAC地址访问列表

## 涉及题型

- 1 总部核心交换机 DCRS 上实现访问控制，在 E1/0/14 端口上配置 MAC 地址为 00-03-0f-00-00-04 的主机不能访问 MAC 地址为 00-00-00-00-00-ff 的主机；

## 注意点

- 该题型涉及策略防护操作，就如同 Cisco 的 route-map access-list ... 等等策略一样
- 有关 Cisco 的策略笔记可以参考一下本人的 Cisco-Note 笔记
- 策略基本上若配置则禁止所有，必须有一个 permit 所有
- 记得使能 MAC-ACL ，就如 BGP 路由一样

## 操作

```
1 DCRS(config-macip-ext-nacl-abc)#permit any-source-mac any-destination-mac
  tcp any-source any-destination
2
3 DCRS(config-macip-ext-nacl-abc)#deny host-source-mac 00-03-0f-00-00-04
  host-destination-mac 00-00-00-00-00-ff tcp any-source any-destination
4
5 DCRS(config)#int e1/0/14
6 DCRS(config-if-ethernet1/0/14)#mac-ip access-group abc out
```

## RS 双向防护-访问控制端口-抵御蠕虫攻击

## 注意点

这里多唠叨一下，免得大家有疑惑，我们正常 Windows 在传输外部数据时，会基于 SMB 服务，NetBIOS 服务，而在 2017 年左右基本上流行的 0 Day 攻击，都基于该服务从而造成的，比如 CVE-2020-0796 MS17-010 等不多赘述

所以题目这里的要求，则我们对该所属 SMB 服务类端口 和 NetBISO 服务类端口做安全防护即可

## SMB

- 445

## NetBIOS

- 135
- 137
- 139

## 类似题型

- 1 2017 年勒索蠕虫病毒席卷全球，爆发了堪称史上最大规模的网络 攻击，通过对总部核心交换机 DCRS 所有业务 VLAN 下配置访问控 制策略实现双向安全防护；

## 操作

```
1 DCRS(config-ip-ext-nacl-bd)#permit ip any-source any-destination
2
3 DCRS(config-ip-ext-nacl-bd)#deny tcp any-source any-destination d-port 135
4 DCRS(config-ip-ext-nacl-bd)#deny tcp any-source any-destination d-port 137
5 DCRS(config-ip-ext-nacl-bd)#deny tcp any-source any-destination d-port 139
6 DCRS(config-ip-ext-nacl-bd)#deny tcp any-source any-destination d-port 445
7
8 DCRS(config-ip-ext-nacl-bd)#deny udp any-source any-destination d-port 135
9 DCRS(config-ip-ext-nacl-bd)#deny udp any-source any-destination d-port 137
10 DCRS(config-ip-ext-nacl-bd)#deny udp any-source any-destination d-port 139
11 DCRS(config-ip-ext-nacl-bd)#deny udp any-source any-destination d-port 445
12
13 DCRS(config)#vacl ip access-group BD in vlan 10;20;30;40
```

## RS SNMP-server 网管系统操作

### 涉及题型

- 1 总部部署了一套网管系统实现对核心 DCRS 交换机进行管理，网管 系统 IP 为：172.16.100.21，读团体值为：DCN2014，版本为 V2C， 交换机 DCRS 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
- 开启 snmp-server trap 功能
- 开启 snmp-server trap mac 改变探测功能

```
1 snmp-server enable
2 snmp-server securityip 172.16.100.21
3 snmp-server host 172.16.100.21 v2c DCN2014
4 snmp-server community ro 0 DCN2014
5 snmp-server enable traps
6 snmp-server enable traps mac-notification
7 mac-address-table notification
8 mac-address-table notification interval 35
9 mac-address-table violation-trap-interval 35
```

## RS 出口流量往返-端口镜像

### 涉及题型

1 总部核心交换机 DCRS 出口往返流量发送给 DCBI，由 DCBI 对收到 的数据进行用户所要求的分析；

### 注意点

- monitor 操作
- 我们需要注意 RS 和 DCBI(NETLOG) 的连接端口 (若非直连则操作跨三层网络镜像)
- 注意出口往返流量，代表访问互联网的接口流量，这里对应 E1/0/24

### 操作

```
1 DCRS(config)#monitor session 1 source interface e1/0/24 tx
2 DCRS(config)#monitor session 1 source interface e1/0/24 rx
3 DCRS(config)#monitor session 1 destination interface e1/0/3
```

## FW zone 管理功能操作



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

## 操作

The image shows two screenshots of a firewall configuration interface, likely from a Huawei or H3C device. The first screenshot shows the configuration for interface 'aggregate1.49'. The second screenshot shows the configuration for interface 'aggregate1.50'.

**Interface Configuration: aggregate1.49**

- 名称: aggregate1.49
- 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

**Interface Configuration: aggregate1.50**

- 名称: aggregate1.50
- 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: untrust
- IP配置:
  - 类型: ☒ 静态IP ☐ 自动获取IP ☐ PPPoE
  - IP地址: 218.5.18.2
  - 网络掩码: 255.255.255.224
  - ☐ 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

不同 zone 区域操作如上，其他多余不多赘述

涉及题型

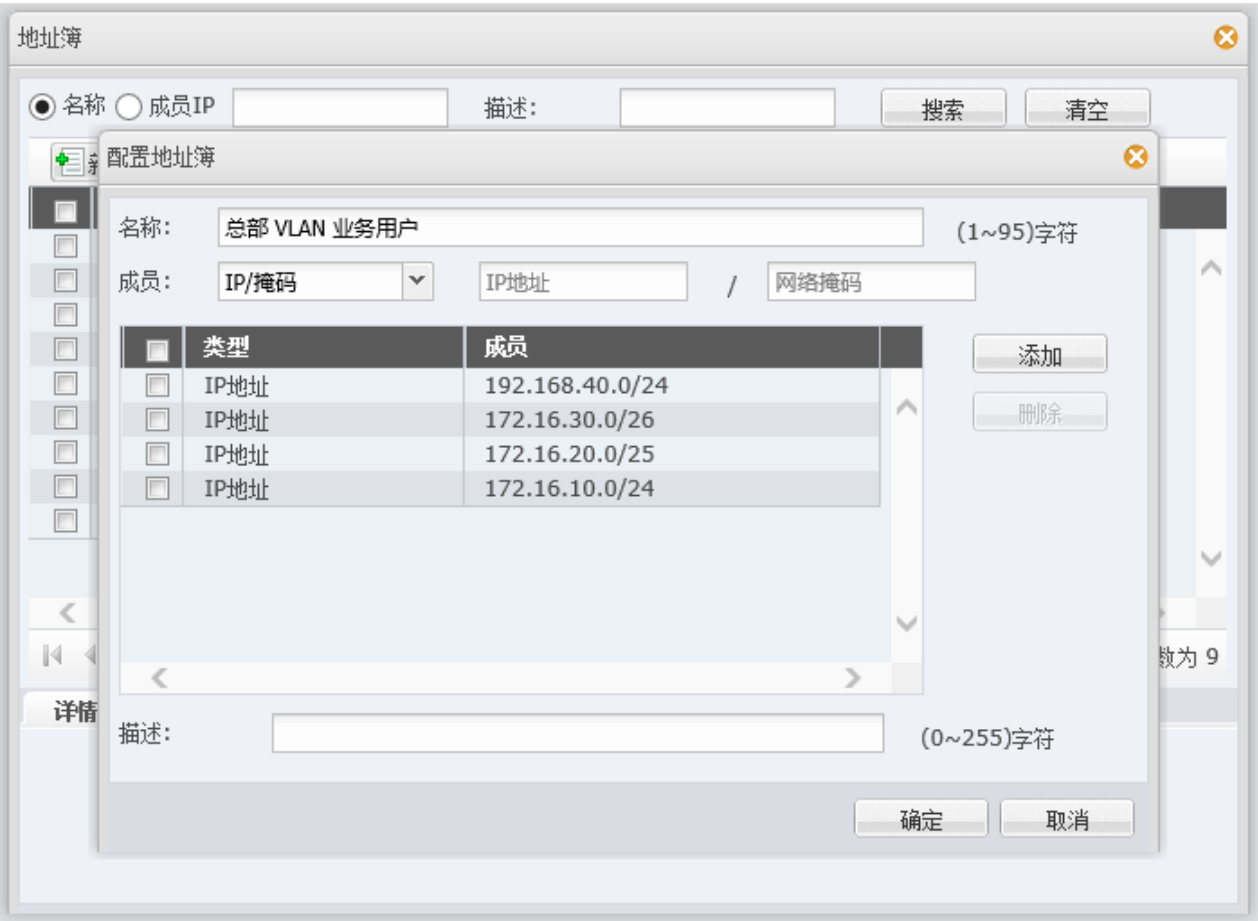
1 总部 VLAN 业务用户通过防火墙访问 Internet 时，复用公网 IP： 218.5.18.9、218.5.18.10；

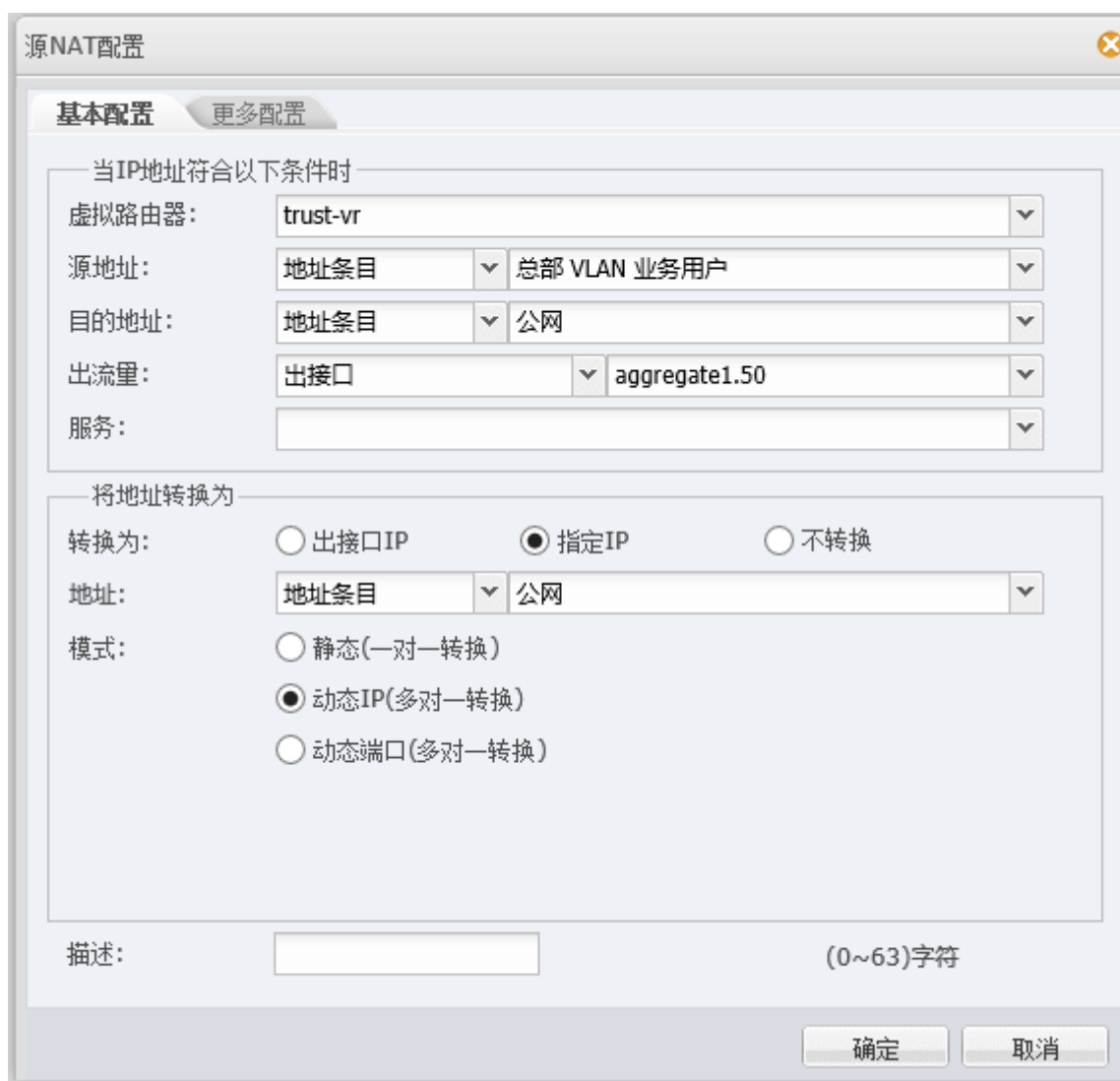
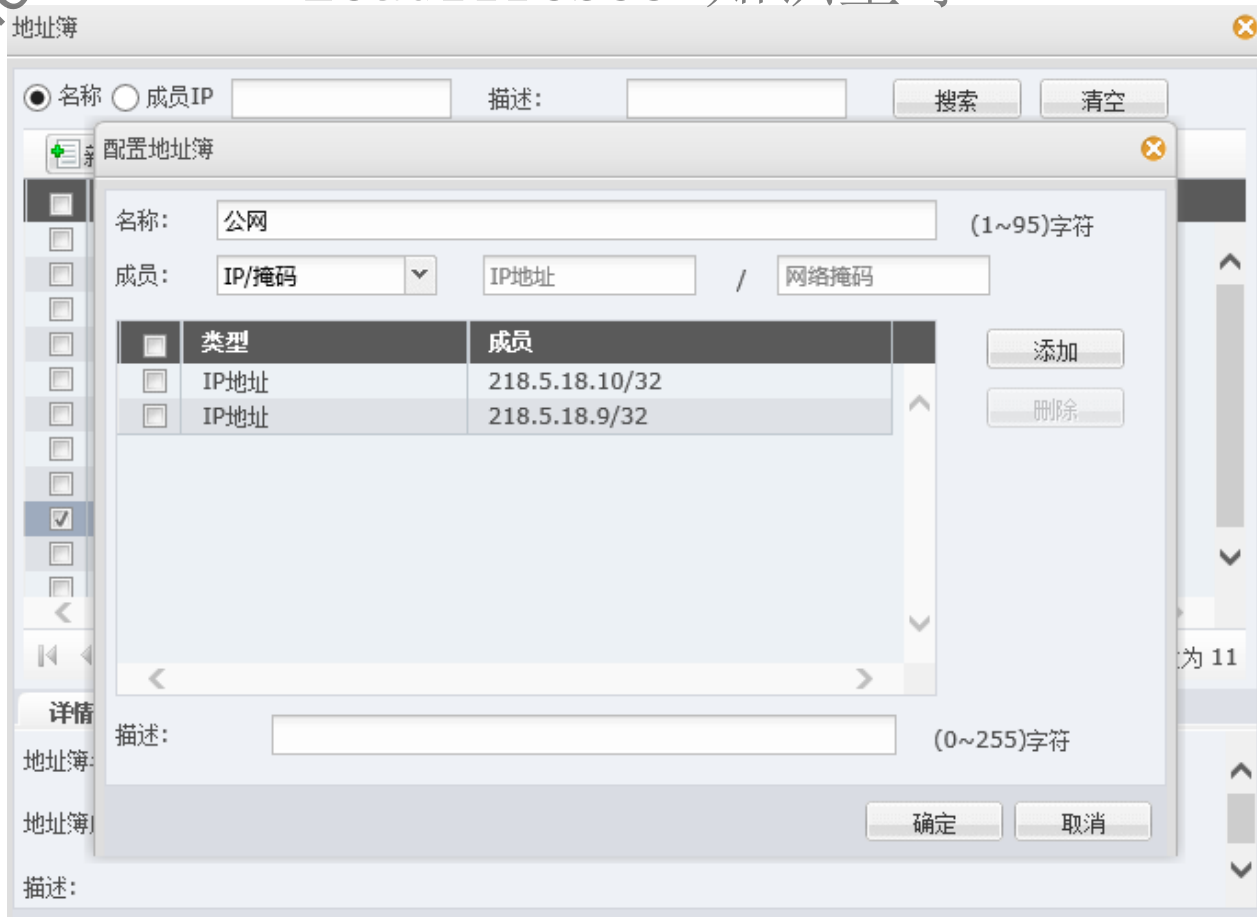
注意点

这道题目我们也在 2021 的题目中做过，简单提一下

- 操作总部 VLAN 业务用户地址簿
- 操作公网地址簿
- NAT 转换，动态一对多
- 注意出接口对应连接 DCFW 的公网 IP 接口 既 E1/0/2 口，我们会发现 E0/2 被绑定为 aggregate1.50 子接口，则我们操作子接口为出接口即可，若评分要求一致，则操作 E1/0/2 即可

操作





## FW 预配置 IPsec Gre VPN tunnel 操作

### 类似题型

- 1 项目二期要启用云端路由器，需要在总部防火墙DCFW上完成以下预配：
- 2
- 3 防火墙DCFW与云端路由器220.5.22.3建立GRE隧道，并使用 IPsec 保护GRE隧道，保证隧道两端2.2.2.2与VLAN20安全通信。
- 4
- 5 第一阶段 采用pre-share认证 加密算法:3DES；
- 6 第二阶段 采用ESP协议， 加密算法:3DES，预设共享密钥

### 注意点

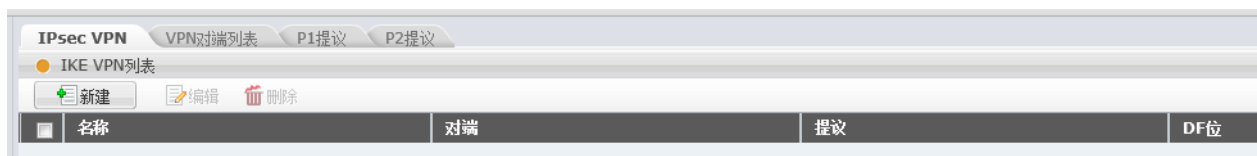
- 注意加密算法
- 注意验证算法
- 注意 GRE 隧道建立
- 注意 VPN 静态路由指定，否则通往该内网流量将被路由器丢弃

### 操作

#### 操作阶段一 与 二 认证与加密算法配置

配置 → IPsec VPN

然后我们注意左上角的操作栏目；



可以看到有 P1,P2 提议，该提议即为密钥认证，和加密算法操作， 分别对应了我们第一阶段、第二阶段的

操作

阶段1提议配置

提议名称: 11 (1~31)字符

认证: ☒ pre-share ☐ RSA-Signature ☐ DSA-Signature

验证算法: ☐ MD5 ☒ SHA ☐ SHA-256 ☐ SHA-384 ☐ SHA-512

加密算法: ☒ 3DES ☐ DES ☐ AES ☐ AES-192 ☐ AES-256

DH组: ☐ Group1 ☒ Group2 ☐ Group5

生存时间: 86400 (300~86400)秒,缺省值:(86400)

确定 取消

阶段2提议配置

提议名称: 22 (1~31)字符

协议: ☒ ESP ☐ AH

验证算法1: ☐ MD5 ☒ SHA ☐ SHA-256 ☐ SHA-384 ☐ SHA-512 ☐ NULL

验证算法2: ☒ 无 ☐ MD5 ☐ SHA ☐ SHA-256 ☐ SHA-384 ☐ SHA-512 ☐ NULL

验证算法3: ☒ 无 ☐ MD5 ☐ SHA ☐ SHA-256 ☐ SHA-384 ☐ SHA-512 ☐ NULL

加密算法1: ☒ 3DES ☐ DES ☐ AES ☐ AES-192 ☐ AES-256 ☐ NULL

加密算法2: ☒ 无 ☐ 3DES ☐ DES ☐ AES ☐ AES-192 ☐ AES-256 ☐ NULL

加密算法3: ☒ 无 ☐ 3DES ☐ DES ☐ AES ☐ AES-192 ☐ AES-256 ☐ NULL

加密算法4: ☒ 无 ☐ 3DES ☐ DES ☐ AES ☐ AES-192 ☐ AES-256 ☐ NULL

压缩: ☒ None ☐ Deflate

PFS组: ☐ Group1 ☐ Group2 ☐ Group5 ☒ No PFS

生存时间: 28800 (180~86400)秒,缺省值:(28800)

启用生存大小: ☐ 启用

确定 取消

操作对端配置-共享双方密钥

VPN 对端配置

基本配置 高级配置

对端名称: 云端路由器 (1~31)字符

接口: aggregate1.50

模式: ☒ 主模式 ☐ 野蛮模式

类型: ☒ 静态IP ☐ 动态IP ☐ 用户组

对端地址: 220.5.22.3

本地ID: ☒ 无 ☐ FQDN ☐ U-FQDN ☐ ASN1-... ☐ KEY-ID

对端ID: ☒ 无 ☐ FQDN ☐ U-FQDN ☐ ASN1-... ☐ KEY-ID

提议1: 11 +

预共享密钥: ..... (5~127)字符

PC N2014

确定 取消

打开VPN列表导入对端 一阶段 二阶段的提议

## 步骤1: 对端

## 基本配置

## 高级配置

对端名称: 云端路由器 新建

接口: aggregate1.50

模式: ☒ 主模式 ☐ 野蛮模式

类型: ☒ 静态IP ☐ 动态IP ☐ 用户组

对端地址: 220.5.22.3

本地ID: ☒ 无 ☐ FQDN ☐ U-FQDN ☐ ASN1-... ☐ KEY-ID

对端ID: ☒ 无 ☐ FQDN ☐ U-FQDN ☐ ASN1-... ☐ KEY-ID

提议1: 11 +

预共享密钥: ..... (5~127)字符

## 步骤2: 隧道

确定

取消

IKE VPN配置

步骤1: 对端  
步骤2: 隧道

基本配置 高级配置

名称: 22 (1~31)字符

模式: ☒ tunnel ☐ transport

p2提议: b2

代理ID: ☒ 自动 ☐ 手工

确定 取消

### 建立gre隧道接口并绑定 VPN

接口配置

常规 属性 高级 RIP

名称: tunnel 2 (1~8)

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: 2.2.2.2

网络掩码: 32

☐ 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

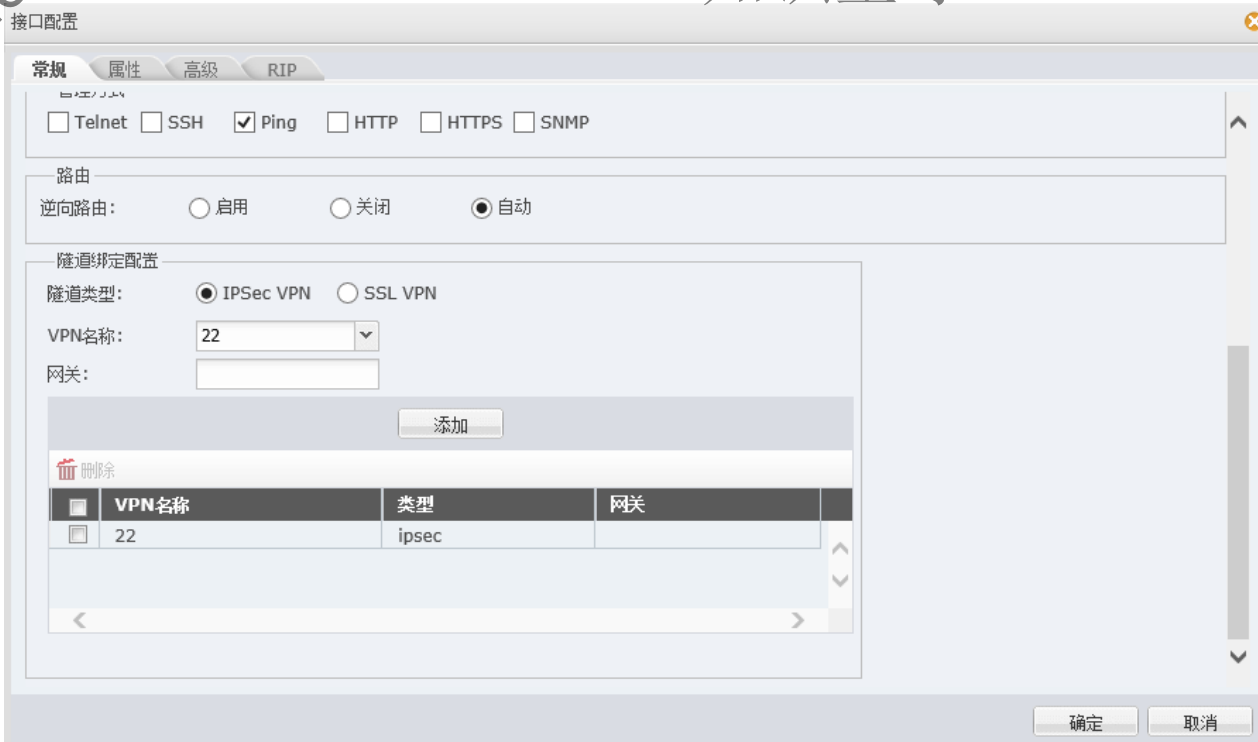
路由

逆向路由: ☐ 启用 ☐ 关闭 ☒ 自动

隧道绑定配置

确定 取消





建立静态路由 目的为将去往云端路由器的流量指向隧道口进行加密



FW 与 DCRS 之间的RIP路由-安全防护配置

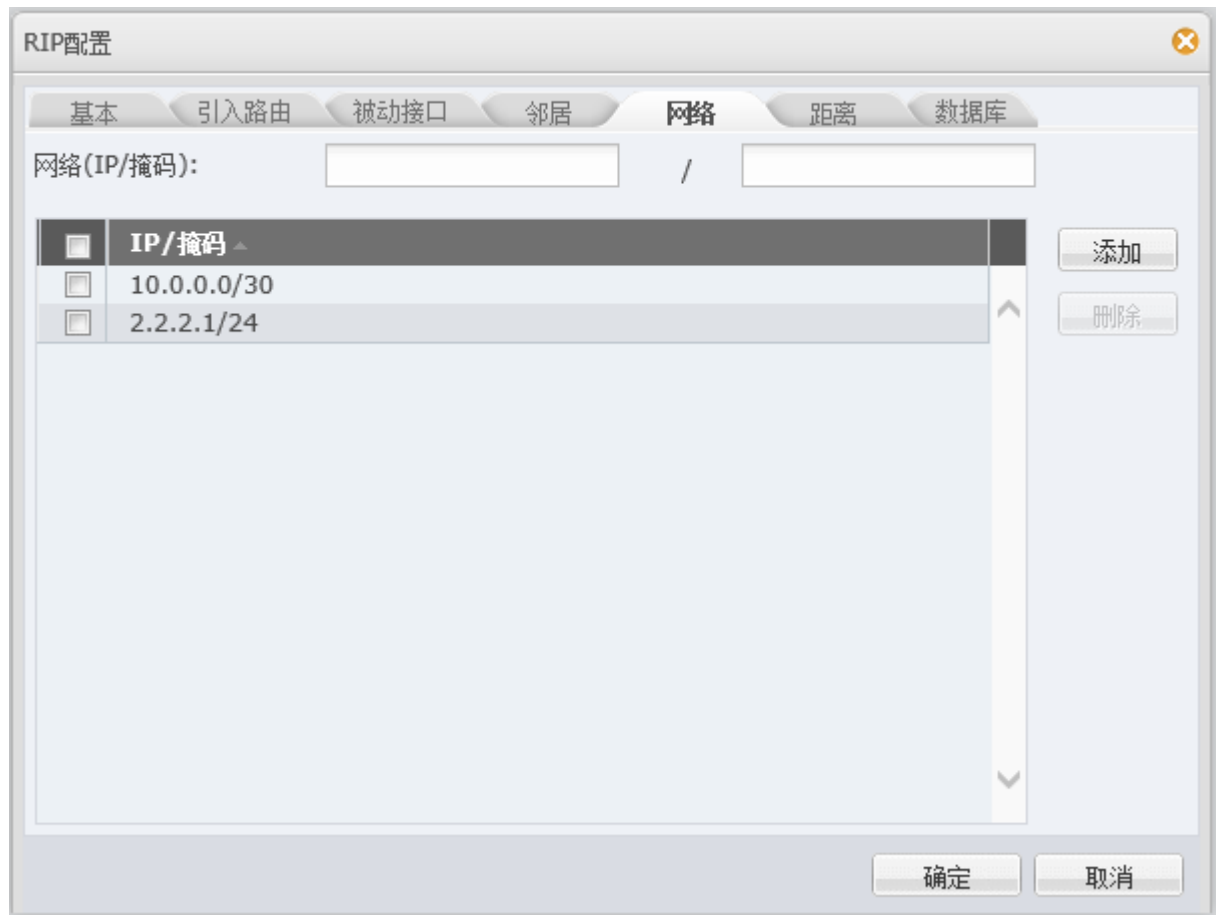
- 1 配置RIP完成云端路由器2.2.2.2、DCFw、总部核心交换机VLAN20 的连通性，使用MD5认证，密钥为DCN2014；

## 操作

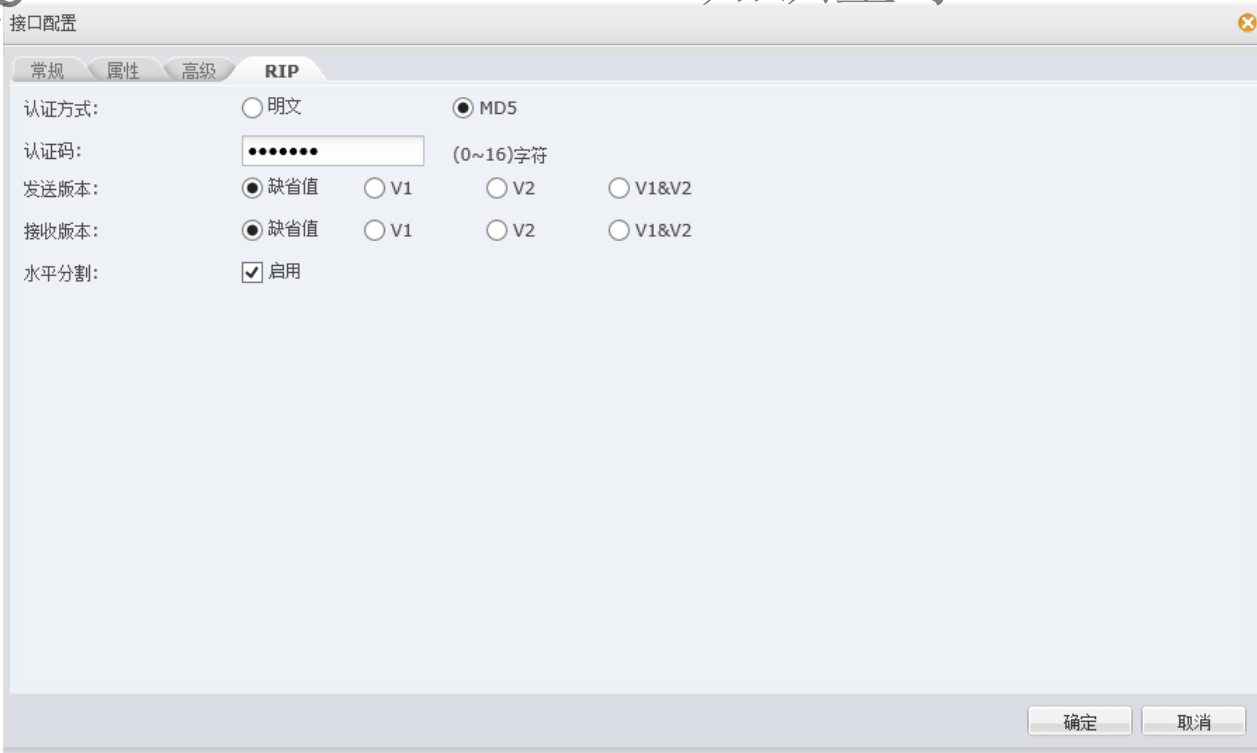
### FW

我们先在防火墙宣告互联端口；

分别对应云端路由器 2.2.2.1/24 以及 FW 与 RS 的路由 10.0.0.0/30



双方建立 RIP 后要进行 MD5 认证安全配置



## RS

```
1 DCRS(config)#router rip
2 DCRS(config-router)#network 10.0.0.0/32
3 DCRS(config-router)#network 172.16.20.0/25
4
5 DCRS#show running-config | include rip
6 ip rip authentication mode md5
7 ip rip authentication string DCN2014
```

## RS VRF VPN 云端路由-访问隔离

### 涉及题目

- 1 总部核心交换机 DCRS 上使用某种技术，将 VLAN20 通过 RIP 连接 云端路由器路由与本地其它用户访问 INTERNET 路由隔离；

### 注意点

- 建立vrf VPN loopback 1
- 配置路由分区符
- 绑定至VLAN20 并且配置IP地址

```
1 DCRS#config terminal
2 DCRS(config)#ip vrf INTERNET
3 DCRS(config-vrf)#rd 1:1
4 DCRS(config-vlan20)#exit
5 DCRS(config)#int vlan 20
6 DCRS(config-if-vlan20)#ip vrf forwarding INTERNET
7 DCRS(config-if-vlan20)#ip address 172.16.20.1 255.255.255.128
8 DCRS(config-if-vlan20)#no shutdown
```

## FW SSL VPN 技术

### 涉及题目

- 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 DCFW 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 DCN2014，地址池参见地址表；

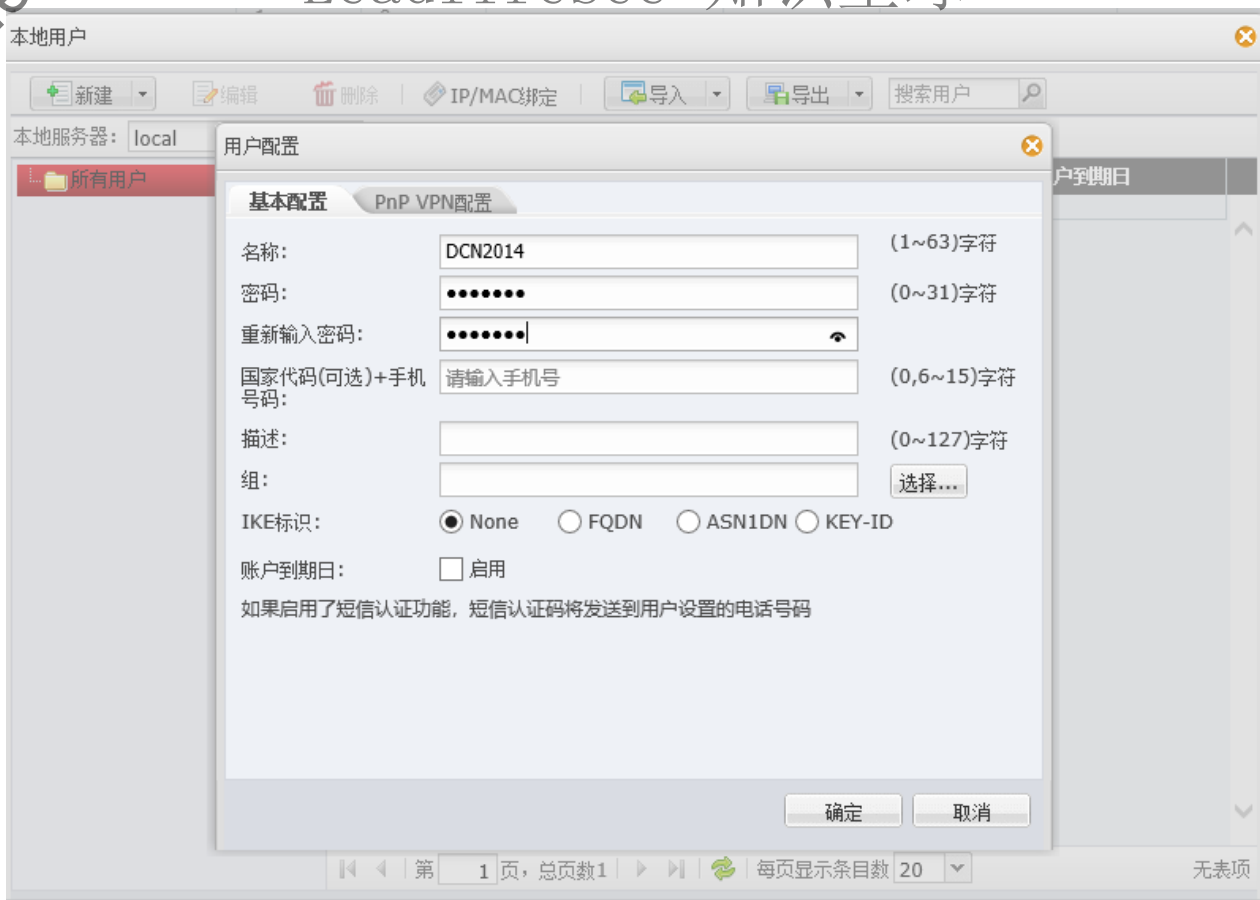
这提我们也做过，这里不多赘述，直接操作

需要注意一个点：在创建了 SSL VPN 后需要指定 VPNHUB 策略通过 Trust 区域

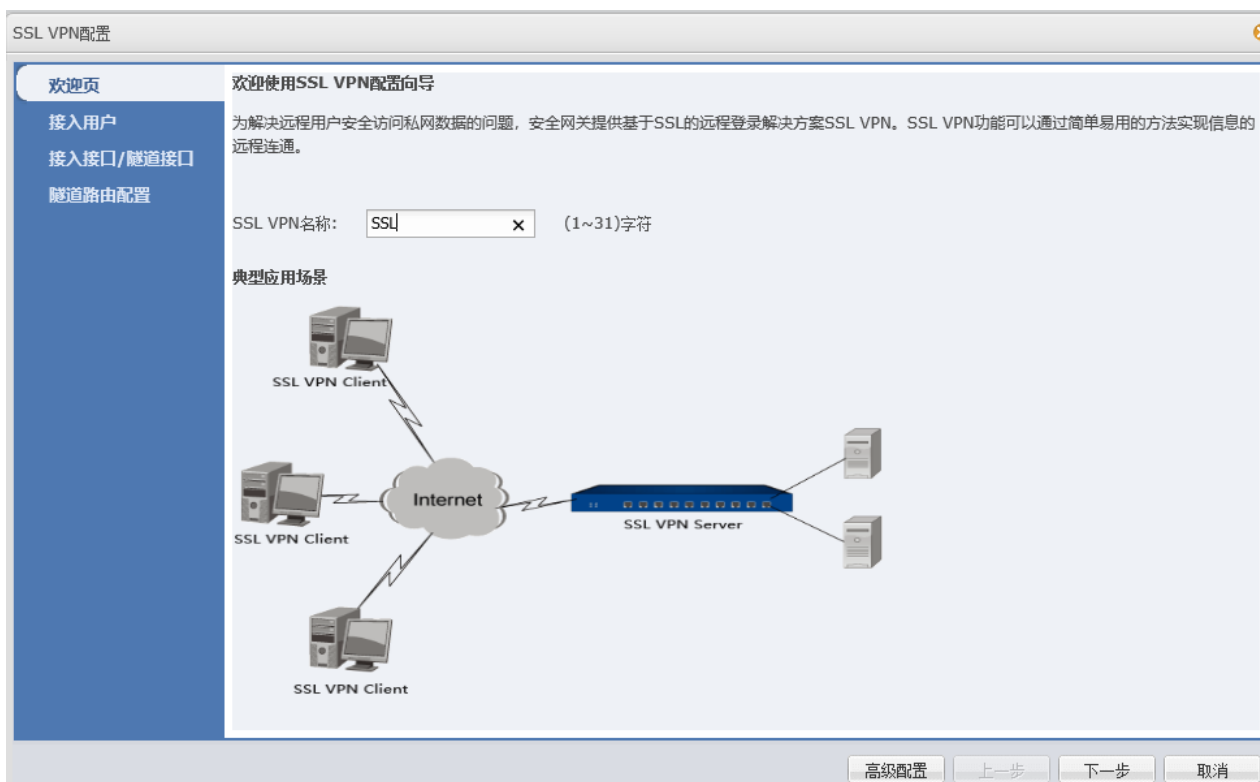
测试方法，目前无法完成，SSLVPN 无法测试

### 操作

先建立本地用户




再新建 SSL

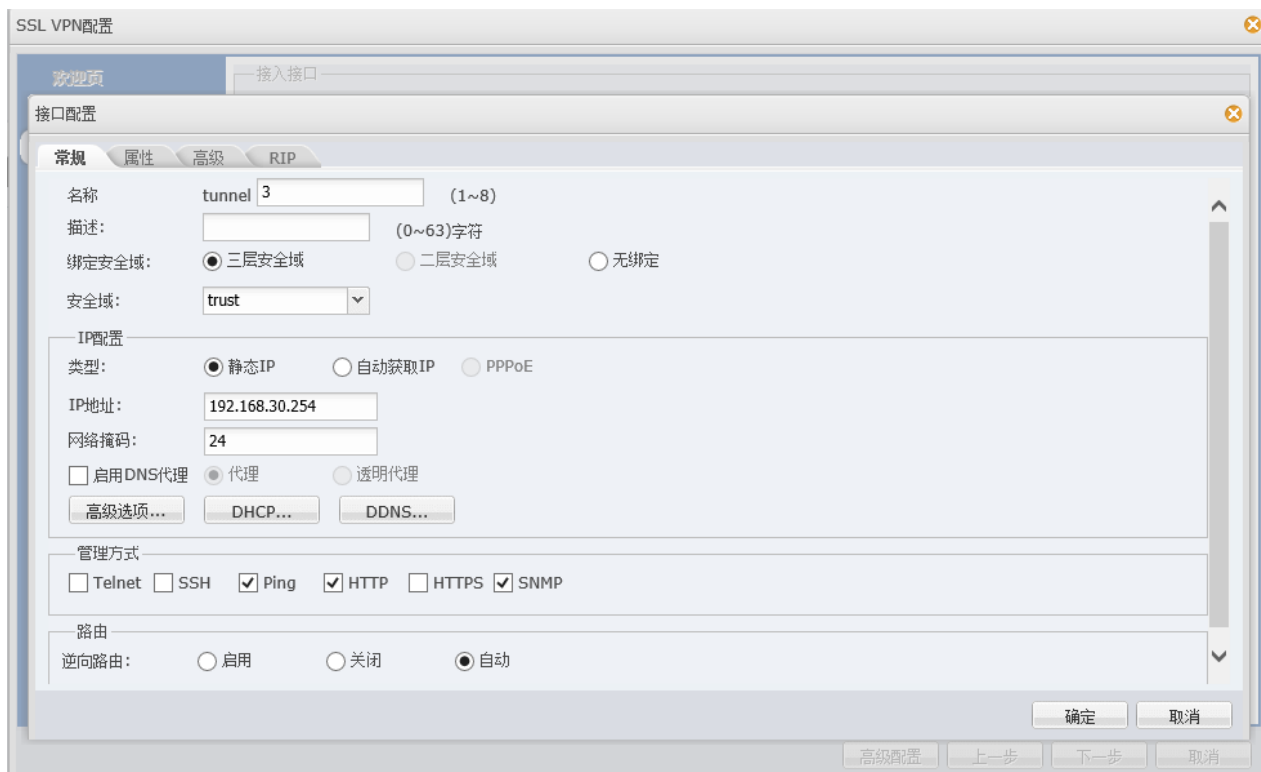




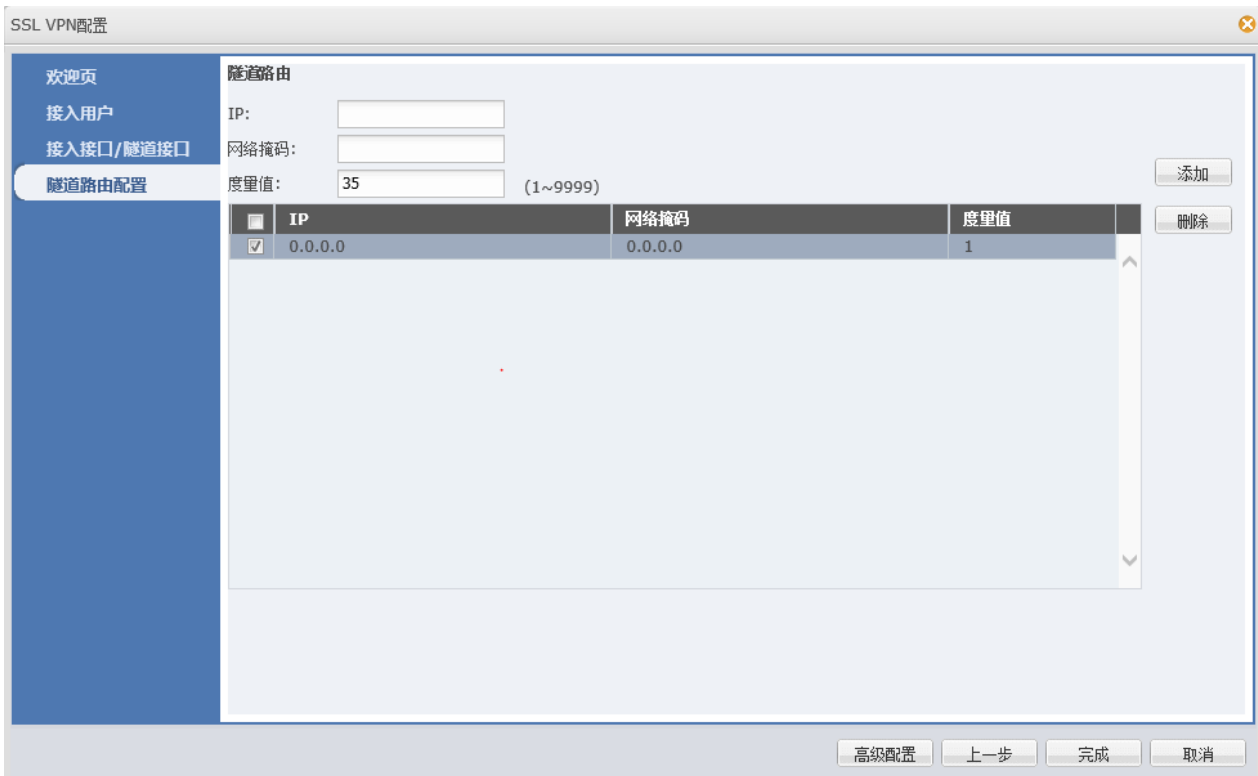
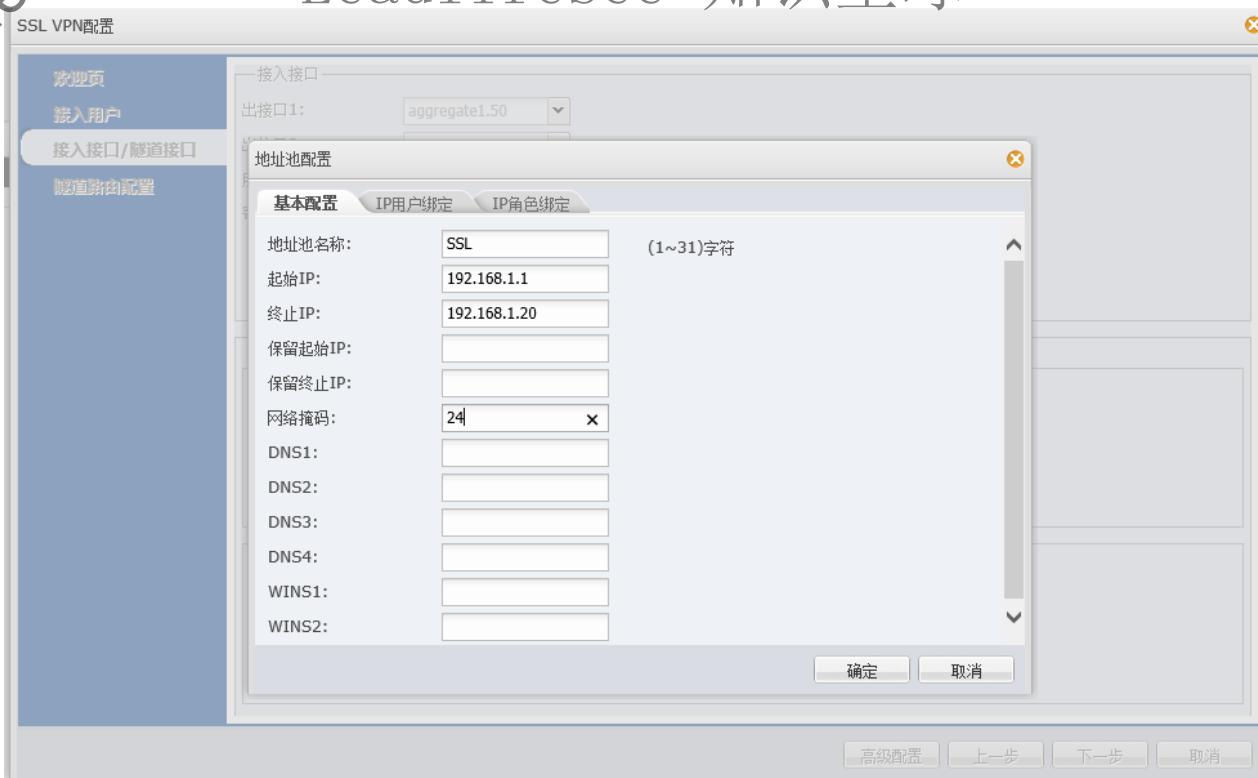
这里有一个配置错误，出接口 2 不用配置，出接口一为 E0/2 对应逻辑接口 aggregate 1.50

 2019-FW-24

然后配置隧道接口地址池



再配置 SSL 地址池



FW Web 认证技术

- 1 出于安全考虑，无线用户移动性较强，无线用户访问 INTERNET 时需要采用认证，在防火墙上开启 WEB 认证，账号密码为 DCN2014；

### 注意点

- 配置无线用户地址簿
- 开启 Web 认证

### 操作

用户识别 → Web 认证参数配置 → 新建 Web 认证

Web认证配置向导

参数配置  
认证用户  
策略配置

认证模式：  
☒ HTTP ☐ HTTPS

HTTP端口：

8181

(1~65535),缺省值:8181

上一步

下一步

取消



Web认证配置向导

参数配置

认证用户

策略配置

请选择需要用户认证所属AAA服务器，此AAA服务器下的所有用户都要进行用户认证

AAA服务器: local

上一步 下一步 取消

Web认证配置向导

参数配置

认证用户

策略配置

策略

源安全域: Any

目的安全域: Any

DNS安全域: Any

源安全域	目的安全域	源地址	目的地址
Any	Any	Any	Any
Any	Any	Any	Any
Any	Any	Any	Any

Web 认证只能工作在trust-vr。

上一步 完成 取消

涉及题型

- 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；

这题咋们也做过，不多赘述

操作

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

aggregate1.49

所属安全域为trust

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:2,048Kbps

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

FW 邮件关键字过滤-时间段操作

涉及题型

- 1

为净化上网环境，要求在防火墙DCFW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；

- 新建地址簿--无线用户
- 新建时间表
- 操作关键字

这里省略地址簿与添加操作

邮件过滤规则配置

名称: DB BD (1~31)字符

当满足以下条件时

目的安全域: trust

用户: 无线用户 配置

时间表: 1-5 配置

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

例外

确定 取消

## NetLog 监控 “流媒体”

### 涉及题型

- 1 DCBI 配置应用及应用组“流媒体”，UDP 协议端口号范围 10847-10848，在周一至周五 8:00-20:00 监控内网中所有用户的“流媒体”访问记录；

有关 Netlog 的题目没啥好说的，送分来的

这里直接操作，没啥注意点能讲

添加自定义应用

自定义应用配置

自定义名称

流媒体

所属应用组

流媒体

协议类型

UDP

服务器IP

0.0.0.0

服务器端口

从10847到10848

保存

我的导航

应用组

应用

时间策略

添加时间策略

添加保存

基本设置

策略名称

流媒体监控

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)08:00--20:00(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

1

08:00--20:00

00:00--00:00

我的导航

应用组

应用

时间策略

规则配置

添加应用规则

应用规则配置

应用类别

网络电视  
股票软件  
音视频流媒体  
应用代理  
自定义应用  
其他应用

应用项目

全部应用项目  
SIP  
H323

Step: 1/5

我的导航

应用组

应用

时间策略

规则配置

添加应用规则

应用规则配置

时间对象

流媒体监控  
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

Step: 3/5

上一步

涉及题型

- 1 DCBI 配置对内网 ARP 数量进行统计，要求 30 分钟为一个周期

我的导航 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

Netlog 监控内网会话安全

涉及题型

- 1 DCBI 配置内网用户并发会话超过 1000，60 秒报警一次；

注意点

- 分析一下，通常内网用户并发会话不会很高，一般是存在一个暴力破解情况
- 记录这种日志，当内网被入侵，能够有效的警报，和溯源

操作

策略管理 → 报警策略 → 会话数报警

我的导航 ARP统计 基本配置 会话数报警

并发会话策略配置

并发会话检查 ☐ 激活 ☒ 不激活

会话阈值 10000 并发会话

报警间隔 60 秒(0表示不报警)

会话阻断 ☐ 阻断 ☒ 不阻断

保存

## 涉及题型

1 DCBI 配置监测到内网使用 RDP、Telnet 协议时，进行网页报警

## 注意点

- 记住是黑名单，其他协议仍然放行
- 注意应用于内网 ALL
- 注意应用于网页报警

## 操作

应用管理 → 应用规则 → 协议黑白名单



## Netlog 定制表单统计 send email

### 涉及题型

- 1 DCBI 配置统计出用户请求站点最多前 100 排名信息，发送到邮箱 为 DCN2014@chinaskills.com

### 操作

增加定制报表

名称: 请求站点最多前100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: 90

生成报表周期: 每天 0时

接收邮箱: 4@chinaskills.com

保存

## Netlog 定制年间时间段邮箱检查任务

### 类似题型

- 1 DCBI 配置创建一个检查 2019-05-01 至 2019-05-05 这个时间段邮箱内容包含“密码”的关键字的任务；

### 注意点

- 创建时间策略
- 添加应用规则 -- 内容规则检查
- 最后操作规则配置生效

添加时间策略

添加保存

基本设置

策略名称  
策略描述

详细设置

绝对时间  
从 2019-05-01 到 2019-05-05 恢复默认值 格式为:YYYY-MM-DD  
按月为周期 从 1 到 31 日  
月周期时段 (1) 00:00--11:59 (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--00:00 (2) 00:00--00:00 (3) 00:00--00:00 (4) 00:00--00:00 设定 重置  
月周期设置的详细时间列表  
日期 时间段一 时间段二  
1--31 00:00--11:59 00:00--00:00

添加内容规则

内容规则配置

内容选项 内容 包含  
匹配内容 密码 导入匹配内容

应用选项 匹配关系 密码

Step: 2/5 上一步

我的导航 搜索内容 SMTP POP3 IMAP 规则配置 扩展过滤

添加内容规则

内容规则配置

时间对象 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

Step: 3/5 上一步

添加 删除

	序号	优先级	用户(组)	规则内容	时间对象	动作
<input type="checkbox"/>	1	500	IP用户:0.0.0.0/0.0.0.0	邮件内容 正文 包含 密码	年間时间段	记录

WAF 爬虫防护-阻拦特定爬虫

涉及题目

- 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



## 注意点

- 创建特定爬虫标识组
- 开启特定爬虫防护
- 操作扫描器标识组，当识别为 360Spider 时自动阻止

## 操作

爬虫标识组 爬虫标识

爬虫标识特征: 360\_Spider 添加

爬虫标识特征: 匹配 360 查询

序号	选择	爬虫标识特征	类型	操作
1	<input type="checkbox"/>	360_Spider	自定义	删除

全选 ☐ 删除所选

爬虫标识组 爬虫标识

爬虫标识组名称: 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	操作
1	<input type="checkbox"/>	DefaultRobots	删除
2	<input type="checkbox"/>	pe_360spider	删除

全选 ☐ 删除所选

爬虫标识组 爬虫标识

编辑爬虫标识组【pe\_360spider】

请选择搜索条件: 等于 查询

序号	选择	爬虫标识特征	类型
148	<input type="checkbox"/>	libwww	默认
149	<input type="checkbox"/>	download demon	默认
150	<input type="checkbox"/>	lynx	默认
151	<input type="checkbox"/>	curl	默认
152	<input type="checkbox"/>	w3mirror	默认
153	<input type="checkbox"/>	microsoft url control	默认
154	<input type="checkbox"/>	autohttp	默认
155	<input type="checkbox"/>	eCatch	默认
156	<input type="checkbox"/>	netants	默认
157	<input type="checkbox"/>	snoopy	默认
158	<input type="checkbox"/>	perl	默认
159	<input type="checkbox"/>	wget	默认
160	<input type="checkbox"/>	pavuk	默认
161	<input type="checkbox"/>	mozilla/2.0 (compatible; newt activex; win32)	默认
162	<input checked="" type="checkbox"/>	360_Spider	自定义

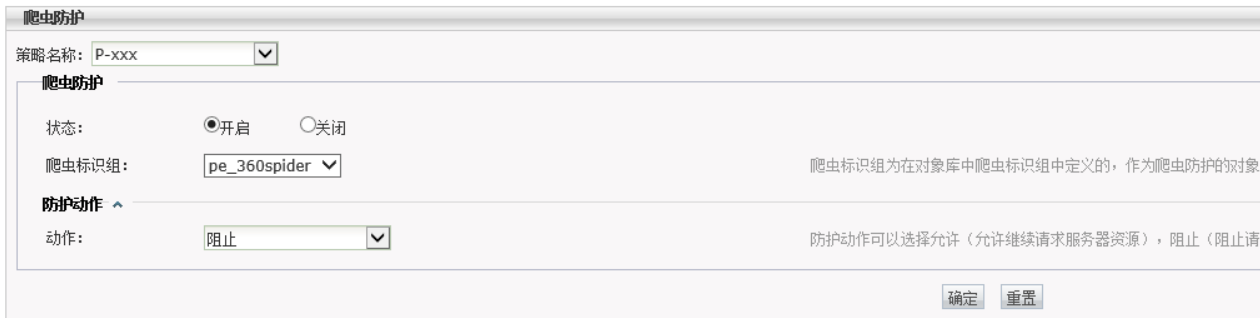
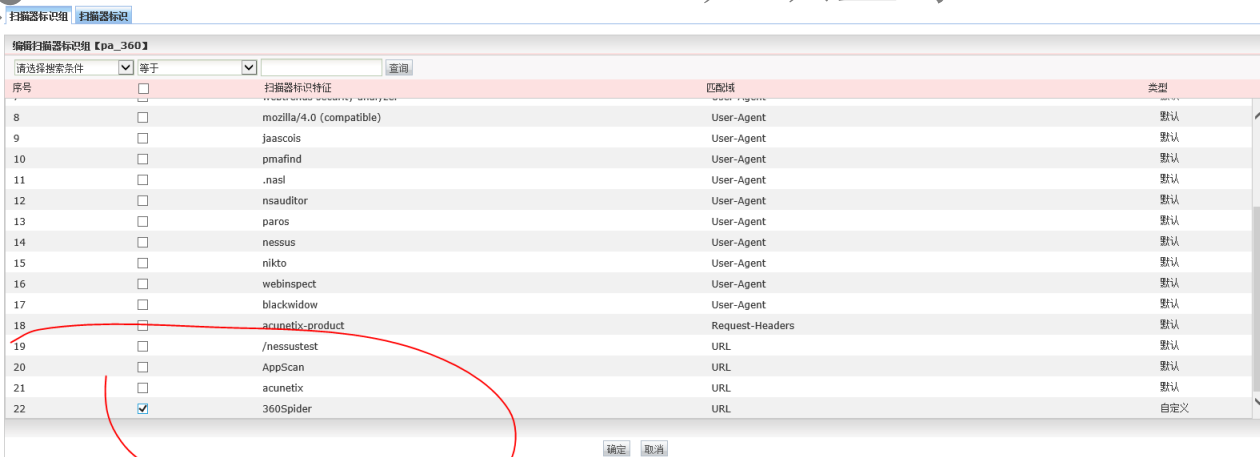
确定 取消

扫描器标识组 扫描器标识

扫描器标识特征: 360Spider 匹配域: URL 添加

请选择搜索条件: 等于 查询

序号	选择	扫描器标识特征	匹配域	类型	操作
1	<input type="checkbox"/>	metis	User-Agent	默认	
2	<input type="checkbox"/>	bilbo	User-Agent	默认	
3	<input type="checkbox"/>	n-stealth	User-Agent	默认	
4	<input type="checkbox"/>	black widow	User-Agent	默认	
5	<input type="checkbox"/>	brutus	User-Agent	默认	
6	<input type="checkbox"/>	cgichk	User-Agent	默认	
7	<input type="checkbox"/>	webtrends security analyzer	User-Agent	默认	
8	<input type="checkbox"/>	mozilla/4.0 (compatible)	User-Agent	默认	
9	<input type="checkbox"/>	jaascols	User-Agent	默认	
10	<input type="checkbox"/>	pmafind	User-Agent	默认	
11	<input type="checkbox"/>	.nasil	User-Agent	默认	
12	<input type="checkbox"/>	nsauditor	User-Agent	默认	
13	<input type="checkbox"/>	paros	User-Agent	默认	
14	<input type="checkbox"/>	nessus	User-Agent	默认	
15	<input type="checkbox"/>	nikto	User-Agent	默认	
16	<input type="checkbox"/>	websinspect	User-Agent	默认	
17	<input type="checkbox"/>	blackwidow	User-Agent	默认	
18	<input type="checkbox"/>	acunetix-product	Request-Headers	默认	
19	<input type="checkbox"/>	/nessustest	URL	默认	
20	<input type="checkbox"/>	AppScan	URL	默认	



## WAF 重写 DATA 为 DATE

### 涉及题目

- 1 WAF 上配置开启防护策略，将请求报头 DATA 自动重写为 DATE；

### 操作

#### 策略 → 站点转换



## WAF 防盗链功能-约束放行特定 User-Agent

### 涉及题目

- 1 WAF 上配置开启盗链防护功能，User-Agent 参数为 PPC Mac OS X 访问 `www.DCN2014.com/index.php` 时不进行检查；

### 注意点

这里说一下我的理解，防止特定 User-Agent 并不能够起到防御的效果，该参数课任意修改

- 操作策略和盗链防护

### 操作

#### 策略 → 盗链防护

盗链防护

策略名称：

P-xxx

盗链防护

状态：

开启

关闭

防护算法：

Referer防护

允许入站页面：

www.DCN2014.com/index.php

填写相对url，例如：页面http://www.test.com/index.html应填写/i

Referer URL：

www.DCN2014.com/index.php

例如：www.example.com URL之间用回车符（换行）分隔；最大长度

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，

例外

例外检测域	匹配方式	例外检测值	操作
User-Agent	正则匹配	PPC Mac OS X	添加
User-Agent	正则匹配	PPC Mac OS X	删除

配置例外数据，不进行盗链防护检测

确定

重置

## WAF 错误屏蔽操作

### 类似题型

- 1 WAF 上配置开启错误代码屏蔽功能，屏蔽 404 错误代码；

## 策略 → 错误码过滤

## WAF 阻止特定文件格式上传

## 1 WAF 上配置阻止用户上传 ZIP、DOC、JPG、RAR 格式文件

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 ☐ XLS ☐ XLSX ☒ ZIP

检测上传文件的格式特征，文件格式不正确，不允许其上传。  
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。

未检测文件动作：

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>删除</div>
表单参数值	字符串匹配	admin	<div>删除</div>
表单参数值	正则匹配	admin	<div>删除</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

## 涉及题型

- 1 WAF 上配置开启基本防护功能，阻止 SQL 注入、跨站脚本攻击；

## 操作

**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

**创建自定义规则**

规则名称: 规则名称用于识别自定义规则,最大长度为32  
URI匹配: /\* 对URI进行字符串匹配，大小写不敏感。如配置'/\*',表示不对URI进行检测，最大长度为512。  
高级匹配: /\* 用于配置HTTP请求头域的检测规则，大小写不敏感

**自定义规则列表**

规则名称	启用	URL匹配	高级匹配	操作
------	----	-------	------	----

确定 重置

## WAF 操作外网访问内网策略防护

## 涉及题型

- 1 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；

## 注意点

- 这里我们需要尤其注意，在一般的中大型企业都会架设堡垒机来约束和管理公司集群服务器，进而增强安全与防护
- 所以有关题目中如果有出现堡垒机标识的 IP 地址，那么一些外访内的服务器时，如果需要指定 IP 地址，则指定堡垒机器的 IP 地址
- 堡垒服务器的默认管理 IP 为 192.168.1.100 ▲

访问控制

策略名称: P-xxx

初始页面过滤

状态: ☐ 开启 ☒ 关闭

默认初始页面: 192.168.1.100

选择是否开启访问控制。推荐: 是。

填写相对url, 例如: 页面http://www.test.com/index.html应填写/index.html, 填写应完整、准确, 大小写敏感。

用户访问允许的入站页面时, 允许其访问; 用户访问禁止目录或禁止页面时, 跳转到默认初始页面。该列表配置内容大小写敏感, 最大长度为512

访问资源类型	值	操作
禁止访问目录	*.bat	添加
禁止访问目录	*.bat	删除

确定 重置

## WS 二层发现 AP 与基本配置 ▲

### 涉及题目

- 1 配置VLAN101 并且管理地址 IP为第二个地址 (192.168.101.2) 无线控制器 DCWS 上配置管理 VLAN 为 VLAN101, 第二个地址作为 AP 的管理地址, 配置 AP 二层手工注册并启用序列号认证, 要求连接 AP 的接口禁止使用 TRUNK;

### 注意点

关于这题, 也是搞了我一镇子, 这里说一下操作步骤, 是我自己摸索加参考学长的笔记搞出来的, 实在是坑呀这题

- 在 AC 上起 DHCP 使用 option 43 字段绑定 vlan 100 的 IP 地址
- 然后进入无线模式配置为序列号认证
- 绑定 AP MAC 地址和序列号 num (这些在 AP 的物理面板上, 就是屁股上写着)

这里顺便提一个小知识

- 1: AP 放绿光一闪一闪的, 代表 AP 未被 AC 发现
- 2: AP 放蓝光一闪一闪的, 代表 AP 已经被 AC 发现

### 操作

```
1 DCWS-6028#show running-config
2 !
3 service dhcp
4 !
5 ip dhcp pool AP
6 network-address 192.168.101.0 255.255.255.0
7 default-router 192.168.101.1
8 option 43 hex 0104C0A86401
```

```
9  !
10 Interface Ethernet1/0/3
11  switchport mode hybrid
12  switchport hybrid allowed vlan 101 untag
13  switchport hybrid native vlan 101
14  !
15  interface Vlan101
16  ip address 192.168.101.1 255.255.255.0
17  !
18  no login
19  wireless
20  no auto-ip-assign
21  enable
22  ap authentication serial-num
23  discovery vlan-list 101
24  static-ip 192.168.101.2
25  !
26  ap database 00-03-0f-82-2d-b0
27  serial-num WL020420H815002349
28  !
29  end
```

## WS DHCP 服务架设分配 vlan 10-20-30-40 IP

### 类似题型

- 1 无线控制器 DCWS 上配置 DHCP 服务，前十个地址为保留地址，无线用户 VLAN10,20，有线用户 VLAN 30,40 从 DCWS 上动态获取 IP 地址；

### 注意点

- 这个题目我们以前做过，但是这里任然多说一下
- 我们需要配置不同地址池的网关 IP
- 需要配置 udp 转发特性
- 由于 WS 做 DHCP 服务器，需要跨三层转发，RS 做 DHCP 中继

```
1 DCWS-6028#config terminal
2 DCWS-6028(config)#ip dhcp pool 10
3 DCWS-6028(dhcp-10-config)#network-address 172.16.10.0 24
4 DCWS-6028(dhcp-10-config)#default-router 172.16.10.1
5 DCWS-6028(dhcp-10-config)#exit
6
7 DCWS-6028(config)#ip dhcp pool 20
8 DCWS-6028(dhcp-20-config)#network-address 172.16.20.0 25
9 DCWS-6028(dhcp-20-config)#default-router 172.16.20.1
10 DCWS-6028(dhcp-20-config)#exit
11
12 DCWS-6028(config)#ip dhcp pool 30
13 DCWS-6028(dhcp-30-config)#network-address 172.16.30.0 26
14 DCWS-6028(dhcp-30-config)#default-router 172.16.30.1
15 DCWS-6028(dhcp-30-config)#exit
16
17 DCWS-6028(config)#ip dhcp pool 40
18 DCWS-6028(dhcp-40-config)#network-address 172.16.40.0 26
19 DCWS-6028(dhcp-40-config)#default-router 172.16.40.1
20 DCWS-6028(dhcp-40-config)#exit
21
22 DCWS-6028(config)#ip forward-protocol udp bootps
```

## RS

```
1 DCRS(config)#service dhcp
2 DCRS(config)#ip forward-protocol udp bootps
3
4 DCRS(config)#int vlan 10
5 DCRS(config-if-vlan10)#ip helper-address 192.168.100.254
6
7 DCRS(config)#int vlan 20
8 DCRS(config-if-vlan20)#ip helper-address 192.168.100.254
9
10 DCRS(config)#int vlan 30
11 DCRS(config-if-vlan30)#ip helper-address 192.168.100.254
12
13 DCRS(config)#int vlan 40
14 DCRS(config-if-vlan40)#ip helper-address 192.168.100.254
```



## AC 操作 igmp 限制组播数量

### 类似题型

- 1 在 SSID DCN2019 下启动组播转单播功能，当某一组播组的成员个数超过 8 个时组播 M2U 功能就会关闭；

### 注意点

- 注意操作 dist-tunnel 使用分布式隧道

### 操作

```
1 WS(config-network)#igmp snooping m2u
2 WS(config-network)#m2u threshold 8
3 WS(config-network)#dist-tunnel
```

## AC ARP 抑制功能 强制漫游功能-动态黑名单功能

### 类似题型

- 1 开启 ARP 抑制功能，开启自动强制漫游功能、动态黑名单功能

### 注意点

- 题目要求开启功能则所有 network 开启
- 全局功能为漫游-黑名单

### 操作

```
1 WS(config-wireless)#network 1
2 WS(config-network)#arp-suppression
3 WS(config-network)#network 2
4 WS(config-network)#arp-suppression
5
6 WS(config-network)#exit
7 WS(config-wireless)#dynamic-blacklist
8 WS(config-wireless)#force-roaming mode auto
9 WS(config-wireless)#exit
```