

第一阶段-NETLOG 评分标准

19、在公司总部的 NETLOG 上配置，设备部署方式为旁路模式。增加非 admin 账户 ABC2021，密码 ABC2021，该账户仅用于用户查询设备的日志信息和统计信息。使 NETLOG 能够通过邮件方式发送告警信息，邮件服务器在服务器区，IP 地址是 10.52.0.100，端口号 25，账号 test，密码 test；NETLOG 上配置 SNMPv3，用户名 admin，MD5 秘钥 adminABC，配置 NTP 服务器，服务器地址：10.52.0.100；
共 8 分，共 6 处。

1.1 分

我的导航 × 管理员组 × 权限分配 × 以太网卡 × 部署方式 ×

部署和工作方式配置

设备部署方式 ☐ 串行连接 ☒ 旁路连接

审计引擎模式 ☒ 普通模式

审计服务内存使用比率 % (范围10--50%)

保存

2.1 分

添加系统管理员

管理员配置

名称

ABC2021

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

不激活

有效期

从0000-00-00到0000-00-00

角色

yonghu

确定

3.1 分

我的导航

管理员组

权限分配

选择角色

yonghu

确定

权限列表			全选	全选	全选	全选	全选	全选
系统状态			浏览	添加	修改	删除	使能	执行
系统管理			浏览	添加	修改	删除	使能	执行
网络配置			浏览	添加	修改	删除	使能	执行
安全管理			浏览	添加	修改	删除	使能	执行
策略管理			浏览	添加	修改	删除	使能	执行
应用管理			浏览	添加	修改	删除	使能	执行
内容管理			浏览	添加	修改	删除	使能	执行
统计报表			浏览	添加	修改	删除	使能	执行
其他			浏览	添加	修改	删除	使能	执行

4.1 分

邮箱管理

报警邮箱设置

邮箱名称: 告警

服务器: 10.52.0.100

端口号: 25

帐号: test

密码: *****

消息数限制: 100

抄送:

提示: 如有多个抄送邮箱, 之间以分号(';')相隔

保存

发送测试邮件

5.2 分

我的导航

远程管理

SSH口令修改

当前密码:

新密码:

确认新密码:

修改

集中管理配置

启用: ☒

SNMP协议版本: ☐ SNMP V2 ☒ SNMP V3

SNMP V3配置

用户: amdin

认证密钥(MD5): adminABC

加密密钥(DES): snmpcrypt

保存配置

系统日志输出设置

系统日志输出IP地址: 0.0.0.0

保存

6.2 分

时间自动同步NTP配置

时间自动同步: ☒ 激活 ☐ 不激活

本地时区: +8:00

保存

	添加	删除		
<input type="checkbox"/>	序号	NTP 服务器名称	IP地址	域名
<input type="checkbox"/>	1	北京邮电大学	0.0.0.0	time.buptnet.edu.cn
<input type="checkbox"/>	2	上海复旦大学	0.0.0.0	ntp.fudan.edu.cn
<input type="checkbox"/>	3	美国国家标准与技术局	0.0.0.0	time.nist.gov
<input type="checkbox"/>	4	芬兰	194.137.39.67	
<input type="checkbox"/>	5	比利时	195.13.1.153	
<input type="checkbox"/>	6	清华大学	0.0.0.0	s1b.time.edu.cn
<input type="checkbox"/>	7	NTP	10.52.0.100	

20、在公司总部的 NETLOG 上配置，监控工作日（每周一到周五 9:00-18:00）期间 PC1 网段访问的 URL 中包含 xunlei 的 HTTP 访问记录，并且邮件发送告警。监控 PC2 网段所在网段用户任意时间的即时聊天记录。监控内网所有用户任意时间的邮件收发访问记录。

共 8 分，共 4 处。

1.2 分

策略名称: xunlei

策略描述: description

绝对时间: 从 0000-00-00 到 0000-00-00 恢复默认值 格式为:YYYY-MM-DD

按周为周期: ☐ 按日为周期: ☐

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	删除

2, 3, 4, 每处 2 分

	序号	优先级	用户(组)	规则内容	时间对象	动作	状态
<input type="checkbox"/>	1	500	IP用户:0.0.0.0/0.0.0.0	邮件收发	任意时间	记录	激活
<input type="checkbox"/>	2	500	IP用户:172.16.40.0/255.255.25...	即时聊天	任意时间	记录	激活
<input type="checkbox"/>	3	500	IP用户:172.16.30.0/255.255.25...	网站访问 URL地址 包含 xunlei	xunlei	记录且邮件报警	激活

21、NETLOG 配置应用及应用组“P2P 视频下载”，UDP 协议端口号范围 64521-64621，在周一至周五 8:00-20:00 监控内网中所有用户的“P2P 视频下载”访问记录；

共 8 分，共 3 处。

1.2 分

添加自定义应用

自定义应用配置

自定义名称

P2P视频下载

所属应用组

P2P视频下载

协议类型

UDP

服务器IP

0.0.0.0

服务器端口

从64521到64621

保存

2.2 分

详细信息

修改保存

添加保存

基本设置

策略名称

P2P

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

周期时间

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

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"/>	08:00--20:00	00:00--00:00	00:00--00:00	00:00--00:00	移除

3.4 分

	序号	优先级	用户(组)	策略内容	时间对象	动作	状态
<input type="checkbox"/>	1	500	IP用户:0.0.0.0/0.0.0.0	自定义应用 自定义应用类型 等于 P2P视频下载	P2P	记录	激活

22、NETLOG 配置对内网 ARP 数量进行统计,要求 30 分钟为一个周期;
NETLOG 配置开启用户识别功能,对内网所有 MAC 地址进行身份识别;
共 8 分,共 2 处。

1.4 分

ARP统计配置

ARP统计 ☒ 激活 ☐ 不激活

统计周期 30 分钟

保存

2.4 分

用户识别

识别接口 ☒ 默认 ☐ DCSM ☐ DCBI

说明 默认审计用户识别方式 (支持PPPOE拨号用户自动识别)

详细配置

方法 ☐ 按IP识别 ☒ 按MAC识别

保存

23、NETLOG 配置统计出用户请求站点最多前 20 排名信息，发送到邮箱为 bn2021@chinaskills.com;

共 8 分，共 3 处。

第 1 处 2 分，第 2 处 3 分，第 3 处 3 分。

 详细信息 — □ ×

增加定制报表

名称	站点
创建时间	2021-06-09 09:57:31
报表	用户请求站点最多排名
范围	全部
周期	每天 0时
TopN	20
接收邮箱	bn2021@chinaskills.com
成功发送	0
失败发送	0