1.关于 AF 的安全防护功能说法错误的是？

A. NGAF 的应用控制策略默认是全部拒绝的，需要手动新建规则进行放通

B. WEB 过滤中的文件类型过滤支持针对 FTP 上传、下载的文件类型进行过滤

C. 配置 IPS 保护客户端和服务器时，源区域为数据连接发起的区域

D. IPS 保护客户端与保护服务器的漏洞规则是不同的

2.网络安全法明确的要求，下列选项中说法错误的是？

A. 企业要求明确网络安全的责任人

B. 必须采取网络防范的相关保护措施

C. 上网行为日志不包括 IT 管理员操作网络设备的操作日志

D. 上网行为日志必须保存至少 6 个月

3.以下关于 L3VPN 资源以下说法正确的是？

A. L3VPN 资源不支持 ICMP 三种协议

B. 配置 L3VPN 资源时必须配置应用程序路径

C. 想要通过 SSL VPN ping 通资源地址必须发布 L3VPN 资源

D. L3VPN 资源不支持单点登录

4.下面____命令可以释放 DHCP 地址？

A. ipconfig／release

B. ipconfig／renew

C. ipconfig／registerdns

D. ipconfig／all

5.SANGFOR VPN 建立的三个过程概括为？

A. 寻址-认证-策略

B. 寻址-认证-授权

C. 认证-寻址-策略

D. 认证-寻址-授权

6.[AC]下面关于全网行为管理的 802.1x 认证功能说法不正确的是？

A. 802.1x 认证的用户只能是本地用户或者域用户

B. 针对哑终端，可以做用户绑定，用户名为 mac 地址，绑定终端的 mac

C. 动态 vlan 支持在用户认证成功的时候，全网行为管理告诉交换机划分端口 vlan

D. radius 报文中默认 1813 是认证端口，1812 是计费端口

7.SSL 同一个客户的不同属性或者不同部门的用户（组）要有自己的个性化登录页面可以通过（）来实现？

A. 策略组

B. 角色授权

C. 登录策略

D. 端点安全

8.下列哪项不是数字签名的主要功能？

A. 防抵赖

B. 完整性检验

C. 身份认证

D. 数据加密

9.[AC]关于密码认证过程，下列选项中说法错误的是？

A. 发起访问网站请求，第一步先进行 DNS 解析

B. 第二步进行 TCP 三次握手

C. 三次握手成功后，客户端发 get 请求

D. 三次握手不成功，可能是因为 AC 设备拦截了 GET 请求

10.【EDR】EDR 与哪个产品线联动可以实现联动下发封锁威胁终端？

A. AF

B. AC

C. SIP

D. X-central

11.[AF]发现一台被具有强烈传播性的病毒感染的终端后，首先应该？

A. 拔掉被感染终端的网线

B. 判断病毒性质、采用的端口

C. 在网上搜寻解决方法

D. 联系网络安全技术人员处理

12.[AC]关于日志查询，选项中说法错误的是？

A. 支持设置拒绝行为过滤条件

B. 支持过滤用户/组

C. 支持选择关注的应用进行分析

D. 高级过滤选项需要授权支持

13.[AC]下列说法错误的是？

A. 如果是单 vlan 环境，可以用 vlan and host x.x.x.x 抓指定 IP 的包

B. 192.168.200.200 转换成十六进制是 c0a8c8c8

C. tcp 头部长度是 20 字节

D. IP 头部长度是 24 字节

14.传输层可以通过（）来标识不同的应用、服务？

A. IP 头部标志字段

B. 端口号

C. IP 地址

D. TCP 序号

15.[SSL]下列关于 SANGFOR VPN 中的用户、角色、资源之间关系的描述错误的是？

A. 一个用户可以对应多个角色

B. 一个角色可以对应多个用户

C. 一个角色可以对应多个资源

D. 一个用户可以对应多个用户组

16.【SIP】AF 与 EDR 进行联动，对检测到的主机存在访问恶意域名，可以通过与 EDR 的什么联动功能进行问题确认？

A. 联动封锁

B. 访问控制

C. 进程取证

D. 一键查杀

17.【EDR】下列有关 EDR 基线检查功能说法正确的是？

A. 可以检查 windows 系统是否符合基线要求，不符合项可以进行自动修复

B. 可以检查 Linux 系统是否符合基线要求，不符合项可以进行自动修复

C. 可以检查 windows 系统是否符合基线要求，对根据修复指导文档对不符合项进行修复加固

D. 可以检查客户业务系统软件是否符合基线要求

18.[AF]下列哪项不是深信服下一代防火墙的核心价值点？

A. 可以提供全面的风险可视化，简化运维，快速定位风险

B. 提供企业业务全生命周期链的防护，包括从事前、事中、事后的整体防护

C. 提供企业内网全面的防护能力，网、端、东西向流量全方位防护

D. 提供应对未知威胁的防护能力，应对不断变化的外部威胁

19.[SSL]以下关于“公共用户”，描述正确的是？

A. “公共用户”支持本地用户认证和证书认证

B. “公共用户”支持短信认证，令牌认证等辅助认证

C. “公共用户”不支持硬件特征码认证

D. “公共用户”不允许用户在线修改登录密码

20.对勒索病毒的紧急预防措施做法不正确的是？

A. 避免弱口令

B. 做好应用服务控制

C. 及时打补丁，修复漏洞

D. 使用解密软件就能对中毒主机进行解密

21.[AC]惩罚通道不可以在哪里引用？

A. 流量配额

B. 应用控制

C. 时长配额

D. 流速控制

22.【SSL】关于本地密码认证以下说法不正确的是？

A. 公有用户可以自行修改密码
B. 私有用户可以自行修改密码
C. 密码可以设置过期策略，过期时强制修改密码
D. 用户设置密码时可以指定密码强度，不符合密码策略则强制修改密码

23.关于 SQL 注入攻击中 Get 和 Post 请求方法的特点，说法正确的是？
A. Get 的特点，提交的内容经过 URI 编码直接在 url 栏中显示
B. Post 的特点，提交的内容经过 URI 编码直接在 url 栏中显示
C. Post 的特点，提交的内容会直接显示在 url 部分，会在 post 包的 data 字段中
D. Post 的特点，提交的内容不会直接显示在 url 部分，会在 post 包的 http 头部信息中

24.【SIP】安全感知平台的产品定位说法不正确的是？
A. 精准检测
B. 全局可视
C. 快速检测
D. 协同响应

25.数据包如果经过二层交换机转发后，那这个数据包的源 MAC 会变化吗？如果经过三层交换机理由转发，源 MAC 会变化吗?
A. 会 会
B. 会 不会
C. 不会 会
D. 不会 不会

26.[AC]客户和管理员申请休息时间放通应用'王者荣耀'权限，管理员放通了'游戏'分类下面的所有应用，其他默认拒绝（基本的协议默认放通，不在此题考虑）但是客户反馈依然无法访问，下面的排查思路，错误的是？
A. 这个问题现象和规则库无关，应检查管理员配置的生效时间是否正确关联给这条策略
B. 查看'王者荣耀'是否属于'游戏'分类
C. 在在线用户列表里搜索问题用户，查看其策略结果集，关联是否正确

D. 开直通测试是否能访问，如果可以，看拒绝列表显示是什么

27.[AF]关于 AF 物理接口配置路由模式情况下，相关功能配置，说法错误的是？

A. 不能在界面直接调整接口的 MTU

B. 配置的下一跳网关不会生成 8 个 0 的缺省路由

C. 勾选的 WAN 属性，会影响到流控、流审功能的使用

D. 设置的线路带宽，与流控功能没有关系

28.AC 不支持以下哪种部署模式？

A. 路由模式

B. 旁路模式

C. 网桥模式

D. 单臂模式

29.【SIP】客户使用 DHCP 分配地址时，无法定位风险终端，该环境中应该可以使用什么产品进行对接解决？

A. AF

B. VSS

C. AC

D. DAS

30.[AC]关于准入策略不生效的原因，以下说法不正确的是？

A. 检查是否开启直通

B. 准入策略关联的用户是否在线，适用终端和区域是否正确

C. 检查是否添加了相关全局地址排除

D. 所有的操作系统都支持安装准入插件

31.【SIP】在客户网络梳理中，客户想知道 IP1 有没有访问 IP2 可以通过以下哪个功能快速监控到？

A. 威胁分析

B. 外连分析

C. 横向访问

D. 访问控制核查

32.[SSL]关于硬件特征码的描述中，错误的是？

A. 一个终端设备只有一个硬件特征码

B. 多个用户可以对应一个硬件特征码

C. 一个用户可以对应多个硬件特征码

D. 硬件特征码根据时间变化会自动改变

33.【SIP】以下不是 SAVE 的优势的是？

A. 能够查杀病毒变种

B. 要求实时升级规则库

C. 使用机器学习识别恶意文件特征

D. 占用内存小

34.【EDR】以下哪个安全策略对 Linux 系统服务器生效？

A. 文件实时监控

B. webshell 检测

C. 勒索病毒防护

D. 系统漏洞修补

35.【SSL】针对于外置数据中心，以下说法正确的是？

A. 忘记密码需要重装系统

B. 使用的 syslog 协议

C. 对接集群，在传输限制中只用添加集群 IP

D. 安装系统时，磁盘文件类型需要选择 ext4

36.[AC]下列需求描述与功能实现匹配正确的是？

A. 客户和你反馈了一个需求，希望实现色情网站 DNS 请求直接丢弃，不要被网监监控到，AC 路由模式部署，配置 DNS 代理策略，动作丢弃所有用户访问色情网站的 DNS 请求

B. 客户所在地区的 DNS 发生了变化，可以在【流量管理】-【线路配置】修改 dns，不会重启网络服务

C. 客户环境是多线路，想让访问某些域名解析走线路二，DNS 代理策略指定这些域名，策略选择“重定向至指定线路”，选择线路二

D. 客户反馈 DNS 代理到内网 DNS 服务器失败，可能是防火墙 WAN->LAN 的流量没有放通

37.不属于 OWASP TOP10 的攻击有？

A. 跨站脚本

B. 敏感信息泄漏

C. 使用未知漏洞的组件

D. SYN 洪水攻击

38.下列关于 AF8017 版本联动封锁说法不正确的是？

A. 策略触发的联动封锁是针对数据包的源 ip 进行封锁

B. 联动封锁的添加封锁攻击者 ip 或者添加到永久封堵是针对源 ip 进行阻断，与之前老版本的机制一样

C. "在联动封锁列表中的主机可访问 AF 控制台，无法访问数据中心"

D. 联动封锁防火墙容量为 20000 条

39.[AC]给客户演示“共享接入管理”识别封堵效果，请问下列的测试环境不合理的是？

A. AC 路由模式部署，使用 iPhone 和小米两部手机通过 360wifi 共享上网

B. AC 网桥模式部署，使用一部 iPhone 手机和一台 Windows PC 通过 360wifi 共享上网

C. AC 网桥模式部署，使用两台 Windows PC 过无线路由器共享上网，无线路由器默认启用 nat

D. AC 旁路模式部署，使用两台 windows PC 通过代理服务器代理上网

40.[AC]关于上网行为可视可控的行为审计，下列选项中说法正确的是？

A. 应用控制行为不需要审计，只需要阻断

B. QQ 聊天记录不能审计

C. 行为审计能审计具体访问网页内容，但是不知道对应的用户

D. 行为审计是记录用户上网轨迹

41.[AF]在防火墙的高可用性技术中，下列哪些是非常少见的？

A. 集群

B. 主备
C. 多机
D. 冷备

42.[SSL]关于 SANGFOR SSL VPN 中角色的作用说法正确的是？
A. 将资源与用户关联起来
B. 将用户与用户组关联起来
C. 将资源与资源组关联起来
D. 将资源与访问权限关联起来

43.[AF]客户开启了 AF 的实时漏洞分析功能，但是过了很长一段时间都没有任何记录生成，对此现象下列分析不正确的是？
A. 实时漏洞分析策略关联的目标服务器流量没有经过设备
B. 实时漏洞分析只支持 TCP 80 端口的 HTTP 数据包识别和分析，非 80 端口识别不到
C. 实时漏洞分析规则库没有更新，识别不了服务器的最新漏洞
D. 客户将所监控的服务器地址添加到实时漏洞分析的排除列表

44.【EDR】下列哪项不属于 EDR 授权的组成？
A. 智防
B. 智检测
C. 智控
D. 智响应

45.计算机网络安全是指？
A. 网络中设备部署环境的安全
B. 网络使用者的安全
C. 网络中的信息安全
D. 网络的财产安全

46.[AC]关于不需要认证，下列选项中说法错误的是？
A. 单位不允许呼叫中心的办公电脑私自修改 IP 地址，可以固定 IP，做不需要认证，绑定 IP 和 MAC 地址

B. 跨三层场景，做不需要认证想获取到真实 MAC 地址只能通过跨三层识别功能实现

C. 动态获取 IP 地址场景，不能使用不需要认证

D. 不需要认证方式适用于对管理要求不高的上网场景

47.以下哪个不是计算机病毒的特征？

A. 隐藏性

B. 破坏性

C. 繁殖性

D. 可预见性

48. 【EDR】下列有关 EDR “试用版授权” 说法正确的是？

A. 该授权已经过期

B. 核心功能无法使用

C. 有试用时间限制

D. EDR 无法和授权服务器通信

49. 关于登录策略说法正确的是？

A. 登录策略功能不支持 EC 登录，只支持浏览器方式登录

B. 登录策略功能可以和 SSL VPN 多线路选路功能一起用

C. 启用登录策略不会导致 VPN 在线用户断开

D. 以上说法都都不对

50.[AC]网络中，下列选项中属于会给公司带来负面影响的共享接入终端场景是？

A. 办公网出口前使用有路由转发功能的交换机

B. 办公笔记本做热点

C. 用个人手机 4G 信号共享热点

D. 入网要求一人一账号，电脑登录账号后，手机也用相同账号登录入网

51.[AF]关于镜像接口的说明，说法错误的是？

A. 不能配置 IP 地址

B. 只能划分到二层区域

C. 允许同时多个镜像口存在

D. 可以划分到对应 VLAN

52.【SIP】探针需要通过 SIP 进行升级，更新规则库和上传日志，会使用到对应的端口，以下哪项是更新规则库使用到的端口？

A. TCP443

B. TCP4430

C. TCP4488

D. TCP22345

53.[AF]SQL 注入是一种常见且危害很大的攻击方式，以下的攻击属于 SQL 注入的是？

A. http://www.example.com/news.php?id=1' or '1'='1

B. http://www.example.com/news.php?id=1&net user admin admin /add

C. http://www.example.com/news.php?id=1%3cscript%3econfirm(%27hello%2cworld!%27)%3c%2fscript%3e

D. http://www.example.com/news.php?id=1=1

54.如下关于 SSL VPN 的控件，说法正确的是？

A. 所有用户登录 SSL VPN，必须安装控件，否则访问不了任何资源

B. SSL VPN 的控件可以自动安装，也可以手动下载安装

C. 如果 IE 安全级别较高导致控件不能自动安装，换个浏览器就可以正常登录

D. 控件如果损坏，可以使用升级客户端 Updater6.0 手动卸载，重新安装

55.SSLVPN 单臂部署的说法正确的是？

A. 单臂部署不支持配置静态路由

B. 单臂部署不支持防火墙过滤规则

C. 单臂部署不支持防 DOS 攻击功能

D. 单臂部署不支持配置 WAN 口地址

56.[AF]vlan 接口是一种逻辑接口，下列关于 vlan 接口的说法，错误的是？

A. vlan 接口属于路由属性接口，可配置 IP 地址

B. vlan 接口可以支持链路探测功能

C. vlan 接口只能划分到三层区域

D. vlan 接口支持 adsl 拨号

57.[SSL]关于 SANGFOR SSL VPN 中 TCP 资源，说法正确的是？

A. 只支持 windows 系统 32 位/64 应用程序

B. 用户端系统会自动添加指向资源的路由

C. 用户登录后可以 ping 通服务器地址

D. 支持 BS、CS 架构的 32 位基于 TCP 协议的应用

58.在 NAT 环境下建立 IPSEC VPN 需要使用以下哪种模式？

A. AH 传输模式

B. AH 隧道模式

C. ESP 传输模式

D. ESP 隧道模式

59.[AF]AF 通过区域，定义并归类接口，在各类安全策略中引用区分不同区域的安全等级以及安全方向，下列关于区域的说法，错误的是？

A. 一个物理接口可以划分到多个同安全级别的区域内

B. 区域根据接口转发类型分为二层、三层、虚拟网线三类

C. 可以把三个路由属性的接口划入到同一个三层区域中

D. 可以通过区域关闭该区域内接口对外提供的控制台登录权限

60.【EDR】以下哪个选项不是 EDR 的组成部分？

A. 云查服务中心

B. EDR 管理平台

C. Agent 客户端

D. SSL VPN 设备

1-5 BCCAA 6-10 DCDDC 11-15 ADDBD 16-20CCCDD 21-25 BAACC 26-30 AADCD 31-35 DDBBB 36-40ADADD 41-45 AABBC 46-50 CDCAB 51-55 DCABD 56-60 DDDAD