1.[AC]关于 AC 旁路模式，下面描述哪一项不正确？

A. 旁路模式主要用于实现审计功能，完全不需要改变用户的网络环境

B. 不支持 NAT、VPN、 DHCP 等功能

C. 不支持流量控制功能

D. 对基于 TCP 协议的应用无法控制

2.[SSL]以下关于 SSL 设备说法正确的是？

A. SSL 默认使用 443 端口登录控制台

B. SSL 默认所有网口都可以作为 WAN 口使用

C. SSL 的 DMZ 口默认地址 10.254.253.254/24

D. SSL 的 LAN 口子接口地址是 10.111.222.33/24

3.[AF]下列哪项不属于热点事件预警与处置功能带来的价值点？

A. 推送当前的热点事件到设备，让用户感知当前的外部威胁

B. 主动扫描用户关注的业务段，是否存在相应的风险

C. 一键生成安全防护策略，帮忙用户实现快速防护

D. 被动分析相关流量，确认内网是否已被入侵

4.[AC]下面关于外置数据中心的说法，错误的是？

A. 当客户需要长期保存日志时，推荐安装外置数据中心

B. 外置数据中心才有附件内容搜索功能

C. 外置数据中心支持安装在 Linux 系统上

D. 外置数据中心推荐安装在 windows 服务器系统上

5.目前网络设备的 MAC 地址由（）位二进制数字构成，IP 地址由（）位二进制数字构成？

A. 48，16

B. 64，32

C. 48，32

D. 64，48

6.【EDR】如何才能释放 EDR 授权？

A. 从管理平台卸载客户端 Agent 软件

B. 从管理平台停止客户端 Agent 软件
C. 从管理平台卸载客户端 Agent 软件后，再移除此客户端
D. 从管理平台停止客户端 Agent 软件后，再卸载此客户端

7.计算机病毒工作步骤是以下哪种？
A. 潜伏阶段-传染阶段-触发阶段-发作阶段
B. 传染阶段-潜伏阶段-触发阶段-发作阶段
C. 传染阶段-触发阶段-潜伏阶段-发作阶段
D. 潜伏阶段-触发阶段-传染阶段-发作阶段

8.针对 SSL VPN 启用数字证书认证的说法，错误的是？
A. 证书认证不可以单独使用
B. 只有私有用户才能使用数字证书认证
C. 证书认证和 LDAP 认证可以同时使用
D. 使用客户端和浏览器登录时都支持证书认证

9.下面哪个说法是正确的？
A. AH 在传输模式中验证整个 IP 数据包，在隧道模式中验证整个 IP 数据包
B. AH 在传输模式中验证整个 IP 数据包，在隧道模式中验证新 IP 头外数据包
C. AH 在传输模式中验证 IP 头后的数据包，在隧道模式中验证整个 IP 数据包
D. AH 在传输模式中验证 IP 头后的数据包，在隧道模式中验证新 IP 头外数据包

10.[AF]当前 AF 的策略路由功能中，下列需求暂时不能实现的是？
A. 出口有电信和联通两个出口，希望内网用户访问电信的数据走电信出口，访问联通的数据走联通出口
B. 出口两条互联网线路，希望两条线路正常时分别承载数据，故障时能实现互为备份
C. 出口两条互联网线路，内网两个部门，每个部门不同 IP 段，希望实现不同部门上网时，走不出的互联网出口
D. 出口两条互联网线路，对外发布了门户网站，希望实现访问网站域名时，电信用户自动跳转电信线路，联通用户自动跳转联通线路

11.VLAN 用来分割？

A. 广播域

B. 组播域

C. 单播域

D. 交换域

12.[AC]移动端和移动端之间识别检查机制没有的是？

A. cookie 识别

B. 应用规则识别

C. URL 识别

D. UA 识别

13.【EDR】EDR 终端发现功能中的发起扫描设备可以是下列哪项？

A. EDR 管理平台

B. Windows Server

C. Windows PC

D. Android 平板

14.对于漏洞攻击防护拦截业务，使用下列哪种方法放通业务（不能影响到策略正常运行）是正确的？

A. 直接绕开设备

B. 删除漏洞攻击防护策略

C. 将源目的 ip 加入全局排除

D. 将拦截业务的规则 id 动作改成允许

15.[AC]关于上网权限策略的适用对象说法正确的是？

A. 本地用户和域用户是“与”的关系

B. 域安全组和源 IP 是“与”的关系

C. 本地用户和终端类型是“或”的关系

D. 目标区域”和“源 IP”是“与”的关系

16.【SIP】以下事件，不可以转为通报事件的是？

A. 安全事件

B. 辖区内攻击
C. 辖区外攻击
D. 漏洞隐患

17. [AC]帮客户配置了密码认证，但是测试时发现密码认证页面重定向失败，下列选项中说法正确的是？
A. 打开的是 HTTP 网站，设备不支持访问 https 网站重定向
B. 可能是 AC 下联设备有拦截限制
C. 测试 PC 做了代理配置不会影响重定向页面正常弹出
D. 重定向是已经发起 get 请求，和 DNS 解析没有关系可以排除

18.【SSL】如果要分配资源的访问权限给用户，是通过以下哪项配置实现的？
A. 通过用户管理把用户帐号绑定指定的虚拟 IP
B. 通过角色管理把用户和资源关联起来
C. 通过准入策略设置用户允许访问资源
D. 只要硬件特征码认证通过了，就能访问资源

19.【SIP】客户相检查内网中有多少台主机中了勒索病毒，可能通过哪个模块查看？
A. 风险业务视角
B. 风险终端视角
C. 安全事件视角-聚合模式
D. 风险安全域视角

20.【EDR】EDR 可以根据什么实现终端上线自动分组？
A. 终端 IP
B. 终端 MAC
C. 终端计算机名
D. 终端 IP 和 MAC

21.[AC]数据经过 AC 设备的处理过程选项中说法错误的是？
A. 用户认证-->应用识别
B. 用户认证-->流量控制

C. 应用识别-->行为动作识别

D. 应用审计-->防火墙规则

22.[AC]某客户反馈，AC 设备网桥部署，做了 URL 过滤，结果发现不生效，下列排查错误的是？

A. 检查策略是否关联了用户

B. 检查用户地址段是否加入全局排除地址

C. 检查是否匹配了自定义的应用，将自定义应用放通

D. 重启设备，检查是否能够恢复

23.某领导想要实现自己的账号登录 SSL VPN 后就直接跳转到门户登录界面，对其他人的账号不做要求，该如何配置？

A. 新建该领导账号，将门户资源与账号直接关联即可

B. 新建该领导账号，同时新建策略组；将新建策略组关联给该用户

C. 新建该领导账号，同时新建策略组，在策略组中修改账号控制的用户登录后跳转到门户资源；最后将用户和新建策略组关联

D. 新建该领导账号，同时修改默认策略组中修改账号控制的用户登录后跳转到门户资源；最后将用户和默认策略组策略组关联'

24.【SSL】关于外置数据中心，下列说法正确的是？

A. 外置数据中心可以使用 Redhat 系统安装

B. 外置数据中心登录端口默认是 443

C. 外置数据中心使用 UDP514 端口通信

D. 外置数据中心日志默认保存 180 天

25.SSL 协议不提供哪种安全特性？

A. 机密性

B. 可靠性

C. 完整性

D. 可用性

26.下列关于 SSL 专线功能的应用场景，说法正确的是？

A. 启用 SSL 专线功能后，用户可以访问所有内网资源

B. 通过 SSL 专线功能，移动用户只能访问 TCP 资源
C. 通过 SSL 专线功能，移动用户和总部建立一条专有的线路，加快访问速度
D. 启用 SSL 专线功能后，移动用户接入 SSL VPN 后将无法访问 Internet

27.[AC]某公司用户的电脑通过 DHCP 获取地址，且每个用户都是使用固定分配的电脑办公，现在管理员通过 AC 进行管控，希望能识别到每个用户的上网行为，且下面的用户无感知认证，请问应该采用以下哪种认证方式？
A. 密码认证
B. 不需要认证，以 IP 地址作为用户名
C. 不需要认证，以 MAC 地址作为用户名
D. 不需要认证，以 VLAN ID 作为用户名

28.[AF]在个别场景中，会要求 AF 旁路部署，在旁路部署下，下列说法错误的是？
A. 旁路部署的优势是无论是上线还是设备故障，均不会影响到用户现有网络
B. 旁路部署可以实现当前设备所有安全功能的防护
C. 旁路部署不支持对 UDP 协议的拦截操作
D. 旁路部署一般需要有一个单独管理口来进行设备的管理

29.[AC]请问以下关于旁路模式的说法错误的是？
A. 旁路模式需要客户交换机配置镜像接口，将需要监控的流量镜像过来
B. 管理口和镜像口可以使用同一个物理接口
C. 旁路模式可以对用户的上网行为进行审计
D. 旁路模式下对用户的应用进行拦截，如果该应用使用 TCP 协议可以通过发送 RST 包进行拦截，如果使用 UDP 协议，则无法进行拦截，原因是 UDP 协议是无连接的

30.关于“计算机病毒”说法正确的是？
A. 计算机病毒是指被损坏的程序
B. 计算机病毒是指特制的具有破坏性的程序
C. 染过计算机病毒的计算机具有对该病毒的免疫性
D. 任何的计算机病毒都会感染其他的设备

31.【AF】保护客户端软件不包含哪些类型？

A. 后门
B. 木马
C. 恶意代码
D. 对应用软件的攻击

32.【SIP】在 SIP 处置中心中有中危、低危都是不能 100%确认存在安全问题，这时还需要通过哪个功能进行分析确认？
A. 分析中心
B. 监控中心
C. 大屏可视
D. 通报预警

33.【AF】下列哪些功能是对外部攻击只检测不拦截的？
A. 入侵检测系统
B. web 应用防护
C. DOS 防护
D. 应用控制

34.[AC]测试防共享，选项中测试方法正确的是？
A. 两台 win7 电脑接入同一个共享热点 wifi，可以在两个 PC 分别登录不同的 QQ 账号
B. 一台 win7 电脑，一部安卓手机，接入同一个共享热点 wifi，可以在电脑和手机登录同一个 QQ 号
C. 一台 win7 电脑，一部 iPhone 手机，接入同一个共享热点 wifi，可以在电脑和手机登录同一个 QQ 号
D. 一台 win7 电脑，两部 iPhone 手机，接入同一个共享热点 wifi，可以在电脑和手机登录同一个 QQ 号，并且两部手机登录不同的微信号

35.【EDR】下列关于暴力破解检测说法错误的是？
A. 暴力破解检测支持 SSH、RDP、SMB 协议
B. RDP、SSH、SMB 暴力破解策略无法独立配置，只能统一配置
C. 暴力破解检测支持界面配置快速爆破阈值
D. 支持配置暴力破解白名单配置，可以将误判的攻击源加入白名单

36.[SSL]关于 SANGFOR SSL VPN 中 TCP 应用类型资源说法错误的是？

A. 需要依赖客户端控件

B. 支持 DNS 解析

C. 支持用户新开浏览器输入地址访问

D. 支持点资源页面访问

37．[AF]测试 AF 的 DoS/DDoS 防护的功能时候，下列哪一项不建议开启？

A. 未知协议防护类型

B. IP 数据分块传输防护

C. SMURF 攻击防护

D. LAND 攻击防护

38.【SIP】在 SIP 组集群时需要注意的事项中说法错误的是？

A. 两台 SIP 组集群，需要使用 3 个同网段 IP

B. 集群开启维护模式时，可以对 SIP 进行升级

C. 解散集群会丢失数据，需要谨慎

D. 可以直接访问登录到集群中的子节点

39.[AC]选项中不属于默认负载策略的特征是？

A. 不支持基于用户选路

B. 支持 VPN 做专线备份选路

C. 支持优先使用优先级最高的线路

D. 能看到线路状态

40.[AC]下列选项中，关于关于 B/s 和 b/s 的关系（B/s 表示 Byte/s，b/s 表示 bit/s），正确的是？

A. 1MB/s=10Mb/s

B. 1MB/s=8Mb/s

C. 1Mb/s=1000KB/s

D. 1Mb/s=10MB/s

41.[AF]下列关于 SYN Cookie 说法错误的是？

A. SYN Cookie 经常用来防御 DOS 攻击中的 SYN Flooding 攻击
B. SYN Cookie 经常结合代理服务器一起工作
C. SYN Cookie 可以防御 DOS 中的重放攻击
D. SYN cookie 建立连接的过程是无状态的三次握手

42.以下（）不是保证网络安全的要素？
A. 信息的保密性
B. 发送信息的不可否认性
C. 数据交换的完整性
D. 数据存储的唯一性

43．[AC]深信服上网审计技术选项中说法错误的是？
A. 审计的前提是内网用户先完成用户认证
B. 审计的前置条件是数据经过 AC 设备或者镜像数据给 AC 设备
C. 应用审计动作会对客户端有感知
D. 全局排除功能添加 www.baidu.com 并启用后，审计会审计不到访问百度网页行为

44.【SSL】下列关于 vpn 设备网络配置说法正确的是？
A. 单臂模式部署，DMZ 口无法做内网口使用
B. 单臂模式部署，设备 lan 口上一定是配置私网 IP
C. 网关模式部署，设备 wan 口上一定是配置公网 IP
D. 网关模式部署，设备 wan 口支持配置静态 IP 或动态获取 IP 两种模式

45.【SIP】安全感知平安体从脆弱性、外部攻击、内部异常进行三大维度的安全实时监测能力构建，来达成全面的检测体系，以下说法正确的是?
A. 脆弱性是事中事件
B. 内部异常是事中事件
C. 外部攻击是事中事件
D. 外部攻击是事前事件

46.某公司网管希望 SSL VPN 连接进来之后能 ping 通内网服务器进行测试，需要给他建哪种资源？

A. L3VPN 资源
B. TCP 资源
C. 远程应用资源
D. WEB 资源

47.[AC]下面关于全网行为管理，下列说法正确的是？
A. 不支持认证托管功能
B. 包含原上网行为管理所有功能
C. 不支持 U 盘离线审计功能
D. 不支持 802.1x 认证

48.[AF]AF 的多线路负载不支持以下哪种方式？
A. 轮询
B. 优先使用前面线路
C. 加权最小流量
D. 随机 HASH

49.以下关于 SSL VPN 公有用户和私有用户的说法，错误的是？
A. '公有用户'允许多人使用，在同一时间内同时登陆 SSL VPN
B. '私有用户'同一时间只允许一台 PC 使用
C. '公有用户'可以在线修改 DKEY 的 PIN 码
D. '私有用户'可以在线修改登陆密码、DKEY 的 PIN 码、手机号码等

50.【SIP】SIP 部署在多分支级联场景时，需要满足一些要求，如下场景可以部署的是？
A. 分支 IP 网段无冲突，分支使用 IP 范围模式，级联部署
B. 分支 IP 网段冲突，分支使用设备模式，级联部署
C. 会存在资产识别冲突，无法部署
D. 可以部署，与分支 IP 网段是否冲突无关

51.【EDR】EDR 和 SIP 联动，不能实现下列哪个功能？
A. EDR 安全日志上报到 SIP，在 SIP 集中分析
B. SIP 发现威胁流量，联动 EDR 一键分析处置威胁文件

C. SIP 发现威胁终端，联动 EDR 一键隔离封锁威胁终端

D. SIP 联动 EDR，为内网终端推广部署 Agent 客户端

52.[AC]关于应用选路能力，选项中说法错误的是？

A. 应用选路的前提是应用识别能力和多条线路

B. 应用选路是精准的识别出应用，进而对应用进行引流

C. 可以配合负载均衡设备实现应用选路

D. DNS 代理使用场景是 AC 设备做内网 DNS

53.【AF】AF 杀毒功能不支持哪个协议？

A. HTTP

B. FTP

C. POP3

D. ALG

54.【EDR】EDR 管理端部署在下列哪个操作系统上？

A. CentOS

B. Redhat

C. Windows Server

D. Debian

55.【SSL】某公司想要实现数字证书认证，该如何操作？

A. 创建公有用户组，勾选数字证书认证；在认证设置的数字证书认证中启用证书认证（内置 CA 或者外置 CA）；下载驱动及导入控件；在用户组中创建用户，生成数字证书

B. 创建私有用户组，勾选数字证书认证；在认证设置的数字证书认证中启用证书认证（内置 CA 或者外置 CA）；下载驱动及导入控件；在用户组中创建用户，生成数字证书

C. 创建公有用户组，勾选数字证书认证；在用户组中创建用户；在认证设置的证书设置中下载安装驱动即可

D. 创建私有用户组，勾选数字证书认证；在用户组中创建用户；在认证设置的证书设置中下载安装驱动即可'

56.[AF]关于 AF 旁路部署的说法错误的是？

A. 不需要单独配置管理接口

B. 需要开启旁路 reset 功能，才能实现阻断

C. 防护策略对 FTP 服务器有效

D. 设备宕机也不会对现有业务造成影响

57.在 NAT 环境下通过什么技术可以解决多 VPN 连接的问题？

A. NAPT

B. NAT-T

C. GRE

D. TRUNK

58.[AF]关于深信服下一代防火墙的核心价值说法，不包含？

A. 提供健康的上网管理

B. 提供安全全面可视的能力

C. 提供业务安全全面防护的能力

D. 提供未知威胁抵御的能力

59.[AF]对新建的应用连接，预先设置安全规则，允许符合规则的连接通过，并在内存中记录下该连接的相关信息，生成规则表。对该连接的后续数据包，只要符合规则表就可以通过。这种防火墙技术称为？

A. 包过滤技术

B. 状态检测技术

C. 代理服务技术

D. 入侵检测技术

60.可以认为数据的加密和解密是对数据进行的某种变换，加密和解密的过程都是在（）的控制下进行的？

A. 明文

B. 密文

C. 信息

D. 密钥

1-5 DCDCC 6-10 CAAAD 11-15 AAADD 16-20 CBBCA 21-25 DDCDD 26-30 DCBBB 31-35 DAAAB 36-40 BBDBB 41-45 CDCDC 46-50 ABDCA 51-55 DDDAB 56-60 ABABD