1.下面的过滤参数表达式正确的是

A. (|(objectClass=organizationalUnit)(objectClass=organization))

B. ((objectClass=organizationalUnit)|(objectClass=organization))

C. ((objectClass=organizationalUnit)(objectClass=organization)|)

D. ((objectClass=organizationalUnit)(objectClass=organization))

2.AF 云脑-云智最新威胁防御规则库订阅服务开通后，不能更新哪个功能的规则

A. SAVE 安全智能文件检测模型库

B. 应用识别库

C. URL 库

D. 热点事件库

3.下面哪个 web 事件不属于 2017 年 OWASP 公布的 TOP 10？

A. 注入

B. CSRF

C. 缓冲区溢出攻击

D. 不安全的直接对象引用

4.用户与 CAS 对接，配置认证接口地址，下列配置正确的是？

A. https://ids6.visedu.com/authserver/login

B. https://ids6.visedu.com/authserver/serviceValidate

C. https://ids6.visedu.com/authserver/logout

D. https://ids6.visedu.com/authserver/portal

5.世界上首例通过网络攻击导致物理核设施瘫痪的是？

A. 以色列核电站冲击波事件

B. 伊朗核电站震荡波事件

C. 巴基斯坦核电站震荡波事件

D. 伊朗核电站震网事件

6.下列选项中属于深信服上网行为管理的规则库的是？

A. 热点事件库

B. 实时漏洞分析识别库

C. 应用识别库

D. 漏洞特征识别库

7.AC 不支持哪个类型的数据库做单点登录？

A. ORACLE

B. MSSQL

C. MYSQL

D. Sybase

8.常见网络设备的高可用部署形式不包括下面哪一项？

A. 主主模式

B. 主备模式

C. 路由模式

D. 集群模式

9.分布式集群下关于虚拟 IP 池说法正确的是？

A. 分布式集群下不支持虚拟 IP 池方式访问

B. 分布式集群下虚拟 IP 池可以共享

C. 各节点采用相同的虚拟 IP 池设置也可以实现共享

D. 分布式集群下也可以独立配置虚拟 ip 池

10.下列关于动态令牌说法正确的是？

A. 动态令牌认证只能使用合作的飞天诚信的令牌

B. 动态令牌只支持物理的动态令牌

C. 动态令牌需要导入种子文件

D. 动态令牌的只支持 PAP 不加密认证

11.配置认证策略时，下面哪些不是单点登录失败的用户备用的认证方式？

A. 不需要认证

B. 用户名密码认证

C. ldap 外部认证

D. QQ 账号认证

12.以下关于 XSS 和跨站请求伪造说法正确的是？

A. XSS 攻击是恶意攻击者通过 web 页面向数据库或 HTML 页面中提交恶意的客户端脚本，当用户浏览此网页时，脚本就会在用户的浏览器上执行，进而达到攻击者的目的

B. XSS 攻击和 CSRF 攻击类似，都可以直接获取到用户的 cookie

C. 反射型和存储型 XSS 攻击，攻击脚本都会经过数据库，并被永久地存放在目标服务器的数据库和文件中

D. 反射型 XSS 只要用户点击过邮件中携带的恶意链接，中招过一次后，下次其他人只要打开这个邮件也会中招

13.关于访客二维码认证的三种场景，下列选项中说法错误的是？

A. “访客填写信息，担保人扫码”方式，在线用户列表中上线用户是其填写的用户名

B. “担保人扫码，访客直接以担保人身份上线”方式，上线用户上线后具备担保人权限

C. “担保人扫码，并备注访客信息”，在线用户列表中上线用户是其填写的用户名

D. 终端做过 NAT 后数据经过 AC/SG 场景不支持访客二维码认证

14.AC 网桥部署，下列选项中，哪个选项必须要使用准入策略？

A. 审计邮件客户端发送邮件内容

B. 审计 webQQ 聊天内容

C. 审计电脑客户端 QQ 聊天内容

D. 审计加密论坛发贴内容

15.关于 AC 主备探测说法正确的是？

A. ARP 探测中如果配置多个地址，只要有一个探测不通，则认为故障

B. ARP 探测中配置的地址都故障后才进入故障状态

C. 当进入故障状态后不会自动恢复

D. ICMP 探测不支持配置域名

16.下列关于账号安全，说法错误的是？

A. 第三方认证中，在认证设置中的防暴力破解，设置封锁 IP 的设置无效

B. 第三方认证中，在认证设置中的防暴力破解，设置封锁用户，设置无效
C. 以安全的角度来说，不建议使用公有账号
D. 定期检查设备中是否存在测试账号，若有，不使用可以禁用或者删除此账号

17.everything 在处理勒索病毒时的作用是？
A. 搜索到病毒样本
B. 搜索到加密文件
C. 分析文件被加密的时间
D. 搜索克隆账号

18.客户反馈内网电脑单接防火墙内网口都 ping 不通防火墙内网口地址，以下说法正确的是？
A. 电脑抓对应网口的所有数据包，发现没发 ARP 的数据包，一定是电脑配置的非同网段地址导致的
B. 防火墙接口抓不到任何电脑发过来的数据包，可能是应用控制策略拦截了
C. 抓包发现 AF 收到数据包之后没有回包，必须做应用控制策略放通
D. 开直通，发现 appcontrol 丢 ping 包，因此必须在接口勾选允许 ping

19.关于 AF 双机心跳口说法正确的是？
A. 管理口不能作为心跳口
B. 聚合口不能作为心跳口
C. 备份心跳口不能同步会话信息
D. 管理口不能作为备份心跳口

20.资源以域名发布，以下哪种情况会导致域名资源无法下发？
A. 设备无法解析该域名
B. 客户端 DNS 解析控件安装出错
C. 内网 DNS 规则没有配置
D. 设备上配置了错误的 HOSTS 规则

21.在组合方案的【方案九(口字型)：AF 路由主备，AC 透明主主的口字型部署】中，下列说法不正确的是？
A. AF 在网口足够的情况下，建议用聚合口做心跳

B. 默认选定的 AF 主机，建议手动设置主控来上线
C. AC 必须配置单独的心跳接口，保证双机的稳定性
D. AC 建议开启多网桥链路同步功能

22.关于 SSL【 匿名认证】安全说法正确的是？
A. 【匿名认证】默认关闭
B. 【匿名认证】默认可访问全网 L3VPN 资源
C. 【匿名认证】用户，只能匹配【默认策略组】
D. 启用【匿名认证】后，全部用户的密码认证将失效

23.关于加密算法的说法中，错误的是？
A. 加密算法分对称加密算法和非对称加密算法
B. 对称加密算法常见有 DES、AES、RC4
C. 非对称加密算法常见有 RSA、ECC、Diffie-Hellman
D. 常用对称加密算法来传递非对称加密算法的公钥

24.在 web 信息中，需要收集的信息不包括以下哪一项？
A. 异常现象发现的时间点
B. 主机异常现象特征
C. 管理员的维护时间
D. 审计日志情况

25.以深信服全景拓扑图为例，哪项不是云 SAAS 服务可以带来的有效安全建设？
A. 深信服云眼可以实时监测用户网站的风险状态，以及风险扫描、快速预警
B. 深信服云盾可以实现网站的实时安全防护，７＊２４小时的专家值守
C. 深信服云守可以实现所有安全设备的日志采集，并对高危事件通过微信快速预警
D. 深信服云图可以实现深信服网络设备的统一管理与可视，同时集中展示风险、处置和批量管理设备

26.关于【防 HTTP 头部攻击设置】根据头部哪个字段判断？
A. Local
B. cookie

C. Referer

D. host

27.深信服上网行为管理，内置的 OA 账号认证，支持下列选项中哪种具体的认证方式？

A. 阿里旺旺

B. 支付宝

C. 陌陌

D. 阿里钉钉

28.使用以下哪个工具可以查看进程的内存空间？

A. everything

B. D 盾

C. process hacker

D. 火绒剑

29.对于恶意程序分析的最常用的第三方工具是？

A. 微步

B. everything

C. EDR

D. 火绒剑

30.关于代理工具列表说法正确的是？

A. 可以显示终端类型

B. 最多可以显示 10000 条数据

C. 可以对某个 IP 标记为信任

D. 刷新时间可以设置为 1S

31.客户需要配置设备防 Host 头部攻击功能，客户外网接入方式 https://vpn.test.com vpn 解析出来的公网 ip 是 3.3.3.3，vpn 单臂部署 lan 口地址 192.168.2.2，下面哪个配置方法可以达到客户要求？

A. 配置 https://vpn.test.com

B. 配置 https://vpn.test.com 和 https://3.3.3.3

C. 配置 vpn.test.com 和 3.3.3.3

D. 配置 vpn.test.com

32.关于 TCP 说法正确的是？

A. TCP 是面向连接的

B. 传输可靠

C. 应用场合为传输大量数据

D. 传输速度快

33.深信服安全产品对标等保 2.0 技术要求工具表涵盖了以下产品，不包括？

A. AF

B. AC

C. FGAP

D. DAS

34.深信服上网行为管理支持 OAuth 认证，下列选项中说法错误的是？

A. 深信服上网行为管理 OAuth 认证支持获取到企业 OA，例如企业微信的组织结构

B. AC 会定时（1h）对开启自动获取用户所属组功能的 OA 服务器进行组织结构同步

C. 不在企业微信组织结构的用户，认证时，点击申请加入组织结构，管理员审批后，可以完成认证

D. 获取 OA 组织结构需要在深信服 AC 本地配置一个起始组

35.以下关于系统命令注入说法错误的是？

A. 操作系统命令攻击是攻击者提交特殊的字符或者操作系统命令，web 程序没有进行检测或者绕过 web 应用程序过滤，把用户提交的请求作为指令进行解析，导致操作系统命令执行

B. 系统命令注入主要用于 asp/php/jsp 等网页中嵌入 webshell 后，执行各种命令提权或收集系统信息

C. 系统命令注入中，多命令按成功顺序执行（linux 与 windows 使用“&&”），多命令按失败顺序执行（linux 与 windows 使用“||”）

D. 系统命令注入的直接危害包括：获取服务器信息、构造一句话木马、更改网

站主页、盗取当前用户 cookie 等

36.丢包标记 evasion 是 AF 的什么模块丢包？

A. 应用控制

B. 异常包检测

C. IPS

D. 僵尸网络

37.在传统安全建设思路下，不属于“内部风险无法可视”的现象是？

A. 缺少南北向流量的风险防护

B. 缺少东西向流量的风险防护

C. 缺少全面的流量监测攻击链、攻击举证展示

D. 缺少基于业务和用户视角的安全展示

38.企业需要用户先认证才允许访问业务系统，选项中说法错误的是？

A. 防止非法终端接入内网，传播病毒等风险

B. 防止非法用户进入内网，盗取内部资料

C. 实现每个接入内网的用户都可以进行溯源，出现安全事件可以找到对应责任人

D. 防止内部员工与访客使用的网络混淆的情况

39.SIP 可以检测到业务在公网上的开放端口，很可能被通报的端口有？

A. 443、80

B. 8080

C. 3306

D. 110

40.以下关于获取 Windows 客户端日志的说法错误的是？

A. 通过 SSLVPN 诊断修复工具的工具箱里面的日志记录在出现问题时点击开始记录，问题复现完成后点击停止可以获取这个过程的日志

B. 通过 SSLVPN 诊断修复工具的工具箱里面的 debugview，在登录 vpn 前打开 debugview，点击开始，登录 vpn 完成后，再结束记录，将日志保存，可以获取 VPN 登录过程的日志

C. 在问题已经恢复正常之后，通过 SSLVPN 诊断修复工具的工具箱里面的日志记录功能可以获取到之前问题发生时的日志

D. debugview 工具相较于日志记录功能更加灵活，可以设置选项记录更详细的客户端调试日志

41.下面说法错误的是？

A. 链路高可用：可以接入多家运营商

B. 接口高可用：可以使用端口聚合技术

C. 设备高可用：主备模式部署

D. 接口高可用：可以使用异地容灾技术实现

42.关于深信服网端云联动解决方案，以 EDR 为视角，不属于可以结合 AF 联动的功能是？

A. 联动实现推广部署 edr 的 agent

B. 联动实现查杀

C. 联动实现僵尸网络举证

D. 联动实现处理威胁文件

43.以行业标准为前提，对于下列对于端口及对应的服务说法错误的是？

A. 21 是 FTP 协议端口

B. 22 是 ssh 协议端口

C. 113 是 stmp 协议端口

D. 1521 是数据库端口

44.客户是多分支型公司，总部部署了深信服认证中心、BBC，总部有一台外置 AD 域场景，分支各有一台 AC，下列选项中描述错误的是？

A. 分支都有 AC 的情况下，可以将分支 AC 认证托管到认证中心，实现统一认证

B. BBC 主要作用是集中管控各个分支 AC 设备，同时集中下发策略到各个分支 AC

C. 想实现认证托管统一下发，需 BBC-AC 模板配置认证托管，下发配置到分支 AC，完成 AC 认证托管到认证中心

D. BBC 加入认证中心认证托管，分支 AC 加入 BBC 集中管控后，分支 AC 可

以获取到外置 AD 域组织结构，进行上网策略关联

45.动态令牌使用什么协议与 SSL 进行交互认证？

A. LDAP

B. Radius

C. 802.1X

D. HTTP

46.针对安全区域边界合规要求，方案设计可以从如下几点进行考虑，除了？

A. 链路负载均衡：实现互联网多出口链路的负载均衡

B. 下一代防火墙：实现网络访问控制和逻辑隔离，防止非授权访问

C. 上网行为管理：针对内部网络用户私自访问互联网的用户行为进行行为审计和数据分析

D. 安全感知平台内建的算法能够对病毒行为、异常外联行为、黑客常用攻击行为等特征进行分析

47.在常见网络安全行业分类中，哪个不属于“安全网关”的分类？

A. 防火墙

B. 上网行为管理

C. 入侵检测设备

D. 堡垒机

48.关于多产品双机组合涉及的产品版本要求，不在建议的产品版本范围内的是？

A. AF8.0.5

B. AD7.0.5

C. AF6.8

D. AC12.0.14

49.下列常见的数据库中，哪项属于非关系型数据库？

A. Redis

B. SQL Server

C. DB2

D. Oracle

50.深信服哪些产品使用了 UEBA 技术？

A. AD

B. SIP

C. SSLVPN

D. 以上所有

51.AC 设备路由模式部署，一条外网线路，2 条内网线路，使用期间发现 lan1 口 PC 可以 ping 通 lan2 口 PC，lan2 口 PC 不能 ping 通 lan1 口 PC，开启直通后网络正常了，什么原因导致？

A. 防火墙策略限制导致

B. 上网策略限制导致

C. 流控策略限制导致

D. 审计策略导致

52.深信服防火墙不支持以下哪种认证方式？

A. 本地密码认证

B. 微信认证

C. 结合 AD 域做单点登录

D. 结合 AD 域做密码认证

53.等级保护 2.0 技术要求中安全管理中心不包括？

A. 系统管理

B. 审计管理

C. 边界管理

D. 集中管控

54.关于地域访问控制与应用控制功能说法正确的是？

A. 先匹配地域访问控制，再匹配应用控制

B. 先匹配应用控制，再匹配地域访问控制

C. 地域访问控制与应用控制策略是同时匹配

D. 先匹配的地址访问控制的拒绝之后，还是会匹配应用控制策略

55.AF 如需接入云脑，版本要求说法正确的是？

A. AF 至少需要 7.3 及以上版本

B. AF 至少需要 7.5.1 及以上版本

C. AF 至少需要 8.0.2 及以上版本

D. AF 至少需要 8.0.5 及以上版本

56.关于【密码认证选项】说法错误的是？

A. 可以配置连续 16 次输入错误后启用验证码

B. 可以配置连续 24 次输入错误后启用验证码

C. 可以配置连续 32 次输入错误后启用验证码

D. 可以配置连续 48 次输入错误后启用验证码

57.SSL 设备在 SIP（安全感知平台）中被检测到开放了 UDP 67 端口，下面说法正确的是？

A. 下架 SSL 设备

B. 检查是否有开启 DHCP 功能，若开启了与客户沟通是否有使用该功能，若无则关闭此功能

C. 检查是否有开启 SNMP 功能，若开启了与客户沟通是否有使用该功能，若无则关闭此功能

D. 升级到最新版本

58.关于 SRadius 软件，下列说法错误的是？

A. SRadius 支持安装在 Linux 系统上

B. SRadius 支持安装在 32 位的 Windows Server 系统中

C. SRadius 不支持 Unix 系统

D. SRadius 软件可以从深信服社区下载

59.AF 的业务安全有报某个关键业务系统“曾被收集信息”，如果需要你做加固，下列加固措施不适用的是？

A. 判断日志记录攻击源 IP 的攻击持续时间和频率等，确认该 IP 是否具备风险，如有，可将该源 IP 加入黑名单

B. 部署深信服僵尸网络查杀软件或者 EDR 产品，对该业务系统进行病毒清查

C. 了解该业务系统提供服务的地域范围，如有，可通过地域访问控制只允许指

定地域对该业务发起访问

D. 确认访问该业务系统的来源是否有经过 SNAT 或者 CDN 等环境，如无，可建议用户开启漏洞防扫描功能

60.下面关于 RADIUS 认证说法不正确的是？

A. AC 网桥模式不支持外部 RADIUS 认证

B. AC 路由模式支持外部 RADIUS 认证

C. SSLVPN 路由模式支持外部 RADIUS 认证

D. SSLVPN 单臂模式支持外部 RADIUS 认证

61.关于资源访问模式以下说法正确的是？

A. 访问某一个资源时想要以虚拟 IP 为源，直接在【SSLVPN 选项】-【系统选项】-【资源服务选项】-【WEB 应用】进行设置即可

B. WEB 应用不支持以虚拟 IP 去访问资源

C. L3VPN 若要以虚拟 IP 为源去访问资源则需要在【SSLVPN 选项】-【系统选项】-【资源服务选项】-【L3VPN 应用】进行设置

D. L3VPN 应用资源访问模式默认是以虚拟 IP 为源

62.内网是 DNS 代理环境下开启蜜罐功能还是无法定位到真实的异常主机，可能的原因是？

A. PC 访问蜜罐 IP 地址的数据没有经过防火墙

B. PC 解析恶意域名的数据经过防火墙

C. DNS 服务器解析恶意域名的数据经过防火墙

D. PC 解析恶意域名的数据没有经过防火墙

63.以下关于 WEB VPN 方案 CAS 认证流程说法正确的是？

A. 输入 VPN 地址打开 SSL 的认证页面

B. 认证页面输入账号后 CAS 会给客户端分配给一个 ticket

C. 用户提交用户名密码后 vpn 设备会向 cas 平台提交用户名密码去认证

D. 资源列表点击注销后会注销掉 CAS，显示的是 CAS 的注销页面

64.对于异常流量 SIP 的检测较 AF 好的原因是？

A. SIP 对外网攻击的检测比 AF 好

B. AF 可以做拦截
C. SIP 的探针可以部署在内网多个位置，进行东西向和南北向的检测
D. AF 需要串接在客户网络中

65.计算机病毒按传染方式划分，不包括下列哪项？
A. 良性病毒
B. 文件型病毒
C. 复合型病毒
D. 引导型病毒

66.关于“全局排除地址”功能影响范围说法错误的是？
A. 被排除的 IP 的认证功能失效
B. 被排除的 IP 防火墙过滤规则失效
C. 被排除的 IP 权限控制策略失效
D. 被排除的 IP 审计策略失效

67.AD 域单点登录优缺点描述错误的是？
A. 脚本方式成功率高，客户普遍使用方式，可以同时实现登录和注销
B. 监控方式的缺点是，需要在域服务器上修改组策略，部分客户不愿意修改
C. IWA 的缺点是，用户登录域后，打开网页才能触发认证，无法实现用户从域中注销同时从设备下线
D. IWA 的优点是不需要改变域的组策略

68.等级保护 2.0 中安全物理环境不包括？
A. 物理位置选择
B. 电力供应
C. 电磁防护
D. 身份防伪

69.关于打不开 SSL 登录页面的问题，进行现象确认，以下说法错误的是？
A. 确认是单台电脑有问题还是所有电脑都有问题
B. 确认打不开具体是如何体现的，是卡住，还是直接提示无法连接
C. 重启电脑看是否恢复正常

D. 确认之前使用是否正常

70.关于 EDR 和 AF 的联动条件和配置，说法错误的是？

A. AF 需要保障 EDR 和 tcp:443 端口进行通信

B. AF 要求版本是 8.0.6 及以上

C. EDR 需要提前配置好 AF 的接入账号

D. AF 与 EDR 联动只需要 AF 上配置即可，无需 EDR 配置

71.深信服认证中心做认证控制器与深信服设备对接，下列选项中说法正确的是

A. 深信服认证中心支持认证托管功能可直接对接深信服 AC/SG

B. 深信服认证中心支持认证托管功能可直接对接深信服 AF

C. 深信服认证中心支持认证托管功能可直接对接深信服 SSLVPN

D. 深信服认证中心支持认证托管功能可直接对接深信服 SIP

72.下面关于集群部署模式说法错误的是？

A. 集群模式可以多台设备同时在工作

B. 集群模式可扩展性强，可以后期增加设备

C. 集群模式部署可以充分利用设备资源

D. 集群模式数据交互非常简单，易于实现

73.SSLVPN 使用外部 RADIUS 认证时，下面说法正确的是？

A. SSLVPN 作为 RADIUS 客户端

B. SSLVPN 作为 RADIUS 服务端

C. 用户需要导入到 SSLVPN 本地

D. 不需要新建角色关联用户和资源

74.关于准入下列说法错误的是？

A. 准入是支持 nat 环境的

B. AC 12.0.22 版本，旁路支持准入

C. 所有版本，多机模式均不支持准入

D. 4.3 版本开始，双机支持准入

75.SYN Flooding 一般是发生在 OSI 模型的哪一层？

A. 网络层
B. 传输层
C. 会话层
D. 应用层

1-5 AACBD 6-10 CDCDC 11-15 DACCA 16-20 ACDCA 21-25 CADCC 26-30 DDCAA 31-35 CDCCD 36-40 BADCC 41-45 DACDB 46-50 DDCAB 51-55 ABCAD 56-60 DBABA 61-65 CABCA 66-70 BBDCC 71-75 ADAAB