安全：

HCIA(H12-711)

1.（单选题）关于包过滤防火墙功能，以下哪一项的描述是错误的？
A.能够实现禁止内网用户使用 ping 工具访问本地防火墙
B.能够实现禁止外网用户使用 FTP 访问内网
C.能够实现禁止内网用户使用 HTTP 访问外网
D.能够实现禁止内网用户伪造 P 地址访问外网

2.（单选题）受外部用户控制通过窃取本机信息或者控制权来攻击网络安全的方式是以下哪种攻击行为？
A.木马攻击
B.钓鱼攻击
C.拒绝服务攻击
D.缓冲区溢出攻击

3.（多选题）关于路由器和二层交换机的区别，以下哪些项的描述是错误的？
A.交换机对于广播报文的处理方式是泛洪
B.路由器对于广播板文的处理方式是转发
C.默认情况下，路由器能够隔离广播域，但是不能隔离冲突域
D.默认情况下，交换机能够隔离冲突域，但是不能隔离广播域

4.（多选题）在配置 GRE 隧道时需要进行以下哪些操作？
A.指定 Tunnel 接口的源端
B.指定 Tunnel 接口的目的端
C.创建虚拟 Tunnel 接口
D.指定 Tunnel 的封装模式

5.（单选题）二层 ACL 的编号范围是以下哪一项？
A.3000-3999
B.2000-2999
C.4000-4999
D.1000-1999

6.（多选题）以下关于会话表的描述，正确的是哪些项？
A.防火墙可以提供会话快速老化功能
B.会话表老化时间设置越长越好
C.会话表老化时间设置越短越好
D.会话表老化是为了节约系统资源

7.（单选题）防火墙无法防御以下哪一项攻击？
A.畸形报文
B.Dos 攻击

C.扫描窥探
D.病毒木马

8.（多选题）以下关于双机热备中配置的描述，正确的是哪些项？
A.在配置心跳接口时，心跳接口必须是直连的
B.在配置 VRRP 虚拟 IP 地址前，必须先配置接口的 IP 地址
C.VGMP Hello 报文发送间隔设置的越小越好，可以加快防火墙故障的响应速度
D.抢占操作是在主用防火墙故障恢复后启动，完成主备防火墙状态切换

9.（多选题）以下关于 PKI 中验证本地证书的描述，正确的是哪些项？
A.如果 PKI 实体没有可用的 CRL 和 OCSP 服务器，或者不需要检查 PKI 实体的本地证书状态，可以采用 None 方式，即不检查证书是否被撤销
B.通过 CRL 方式验证本地证书时，先查找本地内存的 CRL，如果本地内存没有 CR BL，则需下载 CRL 并安装到本地内存中，如果对端实体的本地证书在 CRL 中，表示此证书已被撤销
C.当验证对端实体的本地证书时，经常需要检查对端实体的本地证书是否有效，例如对端实体的本地证书是否过期、是否被加入 CRL
D.在 IPSec 场景中，PKI 实体间使用证书方式进行 IPSec 协商时，可以通过 OCSP 方式实时检查对端实体的证书状态

10.（单选题）在 IS027001 的风险评估的各个环节中，以下哪一项不属于体系设计与发布环节？
A.召开信息安全管理阶段项目总结会议
B.制度整合及信息安全管理体系文档编写
C.确定风险处置措施并实施整改计划
D.确定风险容忍度和风险偏好

HCIP(H12-721,H12-722,H12-723)

1.IPsec VPN 使用以下哪种加密方式对通信数据流进行加密？
A.公钥加密
B.私钥加密
C.对称密钥加密
D.预共享密钥加密

2.对 web link 的描述，以下哪项是正确的？
A .web Link 功能适用于任问操作系统和浏览器
B.Web Link 不进行加密和适配，只“转发”远程用户的 Web 源请求
C.Web Link 需要加密和适配的环节，因此业务处理效率较慢
D.Web ink 需要加密和适配的环节，因此安全性更高

3.关于防火墙接口绑定 VPN 实例的配置，以下哪个选项是正确的？
A.ip binding vpn-instance vpn-id
B.ip binding vpn-instance vpn-instance-name

C.ip binding vpn-id
D.ip binding vp-id spn-instance-name

4.在 USG 的系统视图下，需要删除 hdal:/目录下的 ssiconfig.cfg 文件，以下哪条命令能完成该操作？
A cd:hdal:/remove sslconfig.cfg
B cd：hdal:/delete sslconfig.cfg
C ed:hdal:/rmdir sskconfig.cfg
D cd：ndal:/mkdir sslconfig.cfg

5.如果防火墙工作在二层，与内网之问直连或通过二层交换机相连，以下哪个选项不可以作为策略路由的匹配条件？
A.IP 地址
B.MAC 地址
C.入接口
D.DSCP 优级

6.以下关于华为 USG6000 产品邮件内容过滤配置的描述，错误的是哪一项？
A .只有在安全策略为允许的条件下调用了邮件过滤配置文件，邮件过滤才会生效
B.检测到 IMAP 消息时，如果判定为非法邮件，防火墙的响应动作仅支持发送告警信息，不会阻断邮件
C.检测到 POP3 消息时，如果判定为非法邮件，防火墙的响应动作仅支持发送告警信息，不会阻断邮件
D.附件大小的限制是针对单个附件的限制，而不是对所有附件总体大小的限制

7.以下哪一项不属于基于 IP 地址的邮件过滤技术？
A.邮件地址检查
B.本地黑名单
C.RBL 远程查询
D.本地白名单

8.在 Post 报文中声明一个很大的 content-Length 值,但是每次发送的报文 Body 长度很小，服务器会认为攻击者还有后续的报文发送，攻击者每隔一段时间发送一个 Body 长度很小的报文即可实现让服务器一直保持连接的目的，以上描述是哪种 WEB 攻击的原理？
A .XSS 反射型攻击
B. CC Slow Post
C .CC Slow Header
D .HTTP Flood

9.IPS 及时升级特征库可以使设备更好地防御网络中的威胁，以下关于升级特征库的描述，错误的是哪一项？
A.升级前需要检查恨目录剩余空间
B.支持本地升级
C.如果升级特征率后出现异常情况，可以使用版本回退功能，回遭到升级前的任意版本

D.在线升级模式中可以选择定时升级或者立即升级

10.IPS 处理流程的步骤如下所示：1.重组应用数据 2.匹配签名 3.报文处理 4.协议识别，以下对于该处理流程的排序，正确的是哪一项？
A.1-3-2-4
B.1-4-2-3
C.2-4-1-3
D.4-1-2-3

11.802.1X 认证中，如果认证点在汇聚层交换机，那么除了 RADIUS，AAA，802.1X 等常规配置外，还需要哪些特殊配置？
A.汇聚层和接入层交换机都需要开启 802.1X 功能
B.接入层交换机需要配置 802.1X 报文透传
C.汇聚层交换机需要配置 802.1X 报文透传
D.不需要特殊配置

12.业务管理器下载补丁的方式有两种，当采用分级式部署时，可直接通过微软补丁服务器下载补丁；当采用非分级式部署时，可通过管理中心下载补丁或者直接通过微软的补丁服务器下载补丁。
A 正确
B 错误

13.在 Agile Controller-Campus 上账号分为两类：一类是本地账号，一类是外部账号，下列哪项不属于本地账号？
A.普通账号
B.访春账号
C.匿名账号
D.移动证书账号

14.关于身份认证的方式和认证类型，以下哪个描述是正确的？
A.用户通过 web 方式可以支持本地认证和数字证书认证两种认证类型
B.用户通过 web Agent 方式可以支持数字证书认证和系统认证两种认证类型
C.用户通过 Agent 方式可以支持本地认证、数字证书认证和系统认证三种认证类型
D.用户通过 web Agent 方式可以支持数字证书认证和本地认证两种认证类型

15.某企业采用硬件 SACG 接入方式进行准入控制，配置命令如下，其中 Key：Admin@123
[USG]right-manager server-group
[USG-rightm]local ip 10.1.10.2
[USG-rightm]server ip 10.1.31.78 shared-key Adnln@123
[USG2100-rightm]right-manager server-group enable
假设其他配置均正确，仅根据以上配置，下列选项哪个说法是正确的？
A.完成配置后，SACG 可以和 Agile Controller-Campus 联动成功
B.完成配置后，SACG 不能与 Agile Controller-Campus 联动成功
C.能下发认证前域 ACL

D.联动不能成功但是终端可以访问认证前域服务器