数字证书不包含下列哪项?
A. 公钥信息
B. 数字信封
C. 数字签名
D. 颁发者
Correct Answer: B

下面关于 Ip sec 中安全联盟 SA 的说法错误的是
A. SA 由一个三元组来唯一标识,这个三元组包括安全参数素引 SP(Security Parameter Index)、源 IP 地址和使用的安全协议号（AH 或 ESP)
B. 使用 display ipsec 命可以查看到与另一个 IPSec 对等体之间所采用的加密算法,感兴趣流量等信息。
C. IPSec 只支持用对称加密算法来对数据进行加密。
D. IPSec 对等体之间必须存在双向的 SA 才能建立 Ipsec VPN 连接
Correct Answer: A
SA 由一个三元组来唯一标识，这个三元组包括安全参数索引 SPI（Security Parameter Index）、目的 IP 地址和使用的安全协议号（AH 或 ESP）。

路由器 HW1 和路由器 HW2 分别连接网络 A 和网络 B。如下图所示，如果你希望在路由器 HW1 和路由器 HW2 之间建立 IPsec VPN。路由器 HW1 需要配置哪个 ACL 以使发送的 LAN 到 LAN 的流量通过加密的 VPN 隧道?
A. rule permit ip source 192.168.1.10 destination 192.168.1.2 0
B. rule permit ip source 10.1.1.0 0.0.0.255 destination 192.168.1.2 0
C. rule permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255

D. rule permit ip source 192.168.1.10 destination 10.1.2.0 0.0.0.255
E. rule permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
Correct Answer: C

以下属于单包攻击的是？
A. 特殊控制报文攻击
B. 扫描探测攻击
C. DDoS 攻击
D. 畸形报文攻击
Correct Answer: ABD

下面关于 IPSec VPN 说法正确的是(多选)
A. 野蛮模式可以支持 NAT 穿越,而主模式不支持 NAT 穿越
B. 两台路由器通过主模式建立 IPSec VPN,从第 5 个报文(包含)开始,载荷的数据常会被加密
C. 两台路由器通过野蛮模式建立 IPSec VPN,那么两台设备之间最少交互 4 个报文才建立隧道
D. 两台路由器之间可以通过 IPSec VPN 隧道建立 OSPF 邻居关系,并交换内网路由
Correct Answer: BC

ike peer peer1 v1 //配置 IKE 对等体
exchange-mode aggressive //使用野蛮模式
exchange-mode main//使用主模式

IKEv1：使用了两个阶段为 IPsec 进行密钥协商，其中第一阶段交换和密钥协商定义了两种模式：主模式（Main Mode）和野蛮模式（Aggressive Mode）。野蛮模式能够更快的创建 IKE SA，但没有

主模式安全；主模式只能采用 IP 地址方式标识对等体，而野蛮模式可以采用 IP 地址方式或者名称方式标识对等体。

主模式和野蛮模式区别
他们都是就 VPN 得第一阶段 IKE 的协商而言。
主模式中双方三层交换信息，总共六个包。简单说下 1、2 个包协商加密和认证算法。3、4 个包 DH 交换。5、6 个包提供身份和密钥的验证。
野蛮模式双方进行两次交换，总共三个包。1.包发起方建议 SA，发起 DH 交换。2.包接收方接受 SA。3.包发起方认证接受方。
这是 IKE 协商方面的一些差别，另外，野蛮模式中数据包是在明文中进行交换的，不提供身份保护，而主模式则不然。
DH：Diffie-Hellman 密钥交换协议
IPSec 主模式和野蛮模式的区别包含如下几点：
1. 交换的消息：主模式为 6 个，野蛮模式为 3 个。
2. NAT 支持：对预共享密钥认证：主模式不支持 NAT 转换，而野蛮模式支持。而对于证书方式认证：两种模式都能支持。
3. 对等体标识：主模式只能采用 IP 地址方式标识对等体；而野蛮模式可以采用 IP 地址方式或者 Name 方式标识对等体。这是由于主模式在交换完 3、4 消息以后，需要使用预共享密钥来计算 SKEYID，当一个设备有多个对等体时，必须查找到该对等体对应的预共享密钥，但是由于其对等体的 ID 信息在消息 5、6 中才会发送，此时主模式的设备只能使用消息 3、4 中的 IP 报文源地址来找到与其对应的预共享密钥；如果主模式采用 Name 方式，Name 信息却包含在消息 5、6 中，而设备必须在消息 5、6 之前找到其对等体的预共享密钥，所以就造成了矛盾，无法完成 Name 方式的标识。
而在野蛮模式中，ID 消息在消息 1、2 中就已经发送了，设备可以根据 ID 信息查找到对应的预共享密钥，从而计算 SKEYID。但是由于野蛮模式交换的 3 个消息没有经过加密，所以 ID 信息也是明文的，也相应造成了安全隐患。

4. 提议转换对数量：在野蛮模式中，由于第一个消息就需要交换 DH 消息，而 DH 消息本身就决定了采用哪个 DH 组，这样在提议转换对中就确定了使用哪个 DH 组，如果第一个消息中包含多个提议转换对，那么这多个转换对的 DH 组必须相同(和 DH 消息确定的 DH 组一致)，否则消息 1 中只能携带和确定 DH 组相同的提议转换对。
5. 协商能力：由于野蛮模式交换次数的限制，因此野蛮模式协商能力低于主模式。

分别在什么环境下采用
IKE 野蛮模式和主模式的理论上的区别在与进行 IKE 协商的时候，所采用的协商方式不同，具体在于，IKE 主模式在 IKE 协商的时候要经过三个阶段：SA 交换、密钥交换、ID 交换和验证。IKE 的野蛮模式只有两个阶段：SA 交换和密钥生成、ID 交换和验证。
在实际应用中，一般情况下，IKE 的主模式适用于两设备的公网 IP 固定、且要实现设备之间点对点的环境。对于例如 ADSL 拨号用户，其获得的公网 IP 不是固定的，且可能存在 NAT 设备的情况下，采用野蛮模式作 NAT 穿越，同时，由于 IP 不是固定的，用 name 作为 id-type，总部采用模板的方式接收分支的 IPSEC 接入。

以下哪项关于 HTTPS 说法错误?
A. HTTPS 协议默认使用 TCP 端口 443
B. HTTPS 通过使用 SSL VPN 保障访问数据的安全。
C. 当使用 HTTPS 访问某网站时,如果用户浏览器不能识别网站的数字证书,则不能访问该网站。
D. 如果 HTTPS 流量中包含病毒,路由器无法使用 IPS 技术直接检测出病毒。
Correct Answer: B

书店提供有线网络供客户在线学习。但是，有些用户突然无法访问

网络。排除故障后，发现 DHCP 地址池中的所有 IP 地址都已用完。以下哪一项是最好的解决问题的方法？
A. 配置静态 ARP 绑定表项
B. 配置 IPSG
C. 配置 DAI
D. 限制可以在接口上学习的 DHCP Snooping 绑定表项的最大数量
Correct Answer: D

NAC 是一个端到端的安全解决方案。它将终端安全状况和网络准入控制结合在一起以保护整个网络的安全性。
A. 正确
B. 错误
Correct Answer: A
NAC（Network Admission Control，网络许可控制）是一套从用户终端角度考虑内部网络安全的“端到端”安全解决方案总称，也就是针对用户终端的接入进行严格控制的解决方案。在华为 S 系列交换机中 NAC 包括 802.1x 认证、MAC 认证与 Portal 认证。它包括用户（User）、网络接入设备（NAD）和接入控制服务器（ACS）三大部分。

NAC 的关键组成部分有哪些?（多选）
A. 通信代理
B. NAC 设备
C. 访问终端
D. 策略服务器
Correct Answer: ABD

在华为 VRP 上配置 AAA 认证的时候，可以将用户按照域（Domain）进行区分，接入用户可以在用户名中携带域名来指定认证域。
A. 正确

B. 错误
Correct Answer: A

CPU 被恶意流量攻击。以下哪些方式可以防止攻击：（多选）
A. 对上送 CPU 的报文进行限速。
B. 用 ACL 在受到攻击的路由器端口过滤数据包。
C. 对上送 CPU 的报文进行分析统计，找出攻击源用户或者攻击源接口。
D. 利用 CPCAR 对上送 CPU 的报文按照协议类型进行速率限制。
E. 关闭路由器的远程登陆功能。
Correct Answer: ACD

路由器工作在三层，可以用 uRPF 这样的技术对数据包的源地址进行校验，二层交换机虽然工作在二层，但是只要启用相应的功能，也可以对数据包的源 IP 地址进行校验。
A. 正确
B. 错误
Correct Answer: A

下面哪个是 NAC 提供的访问控制方法?（多选）
A. 802.1x 认证
B. AAA 认证
C. MAC 地址认证
D. Web 认证
Correct Answer: ACD