CNS Review-Text 重要考点（高频版）

2026 年 2 月 17 日

1 对比题（必背）

1. Bell-LaPadula (BLP) vs Biba

   - BLP 目标是保密性（Confidentiality）：No Read Up，No Write Down。
   - Biba 目标是完整性（Integrity）：No Read Down，No Write Up，并且执行也遵循不向上污染（可理解为 No Execute Up）。
   - 结论：两者方向相反，一个防泄密，一个防低可信数据污染高可信数据。

2. PAP vs CHAP

   - PAP：口令（或口令哈希）直接发给服务器，容易被嗅探与重放，安全性弱。
   - CHAP：挑战-应答，不传输明文口令，每次挑战不同，抗重放更好。

3. AH vs ESP（IPSec）

   - AH：有完整性、认证、防重放；不提供加密；可保护 IP 头完整性。
   - ESP：提供加密（机密性）并可提供完整性/认证与防重放；不保护外层 IP 头完整性。
   - 结论：ESP 更常用；也可 AH+ESP 组合。

4. HIDS vs NIDS

   - HIDS：部署在主机上，能看日志/系统调用/文件完整性，适合重点服务器深度检测。
   - NIDS：部署在网络链路，按流量检测，覆盖面大；但对加密流量可见性差，交换网络下需特殊配置。

5. SSL/TLS vs IPSec VPN

   - SSL/TLS：主要保护传输层之上的应用数据（常见于 HTTPS），更偏应用接入。
   - IPSec VPN：网络层隧道封装，可保护整个原始 IP 包（ESP 隧道模式），适合站点到站点/全流量保护。

6. Signature-based IDS vs Anomaly-based IDS

   - 特征型：已知攻击检测好、上线快；但对未知攻击弱、需持续维护签名库。
   - 异常型：能发现新型攻击；但误报率通常更高，正常基线难定义。

2 流程题（必背顺序）

1. CHAP 流程

   - 客户端发 userID。
   - 服务器发随机 challenge。
   - 客户端用 challenge + password 计算响应并回传。
   - 服务器用本地口令做同样计算，比对一致则通过。

2. SSL/TLS 握手（服务器认证场景）

   - 客户端发起连接并请求页面。
   - 服务器发送证书。
   - 客户端用本地 CA 公钥链验证证书。
   - 验证通过后生成会话对称密钥，用服务器公钥加密发给服务器。
   - 服务器用私钥解密得到会话密钥，后续双方用对称密钥加密通信。

3. Kerberos 流程（AS/TGS/Service）

   - C -> AS：请求票据，拿到 TGT 和 C-TGS 短期密钥材料。
   - C -> TGS：带 TGT 申请目标服务票据，拿到 service ticket 和 C-S 会话密钥材料。
   - C -> S：提交服务票据和认证器，服务端验证后建立会话（可双向确认）。
   - 核心思想：长期密钥尽量短时使用，后续靠票据与短期会话密钥。

4. IKE 两阶段（IPSec）

   - Phase 1：建立受保护的 IKE 信道，完成对等体认证、算法协商、共享密钥交换（主模式/野蛮模式）。
   - Phase 2：在 Phase 1 保护下协商具体 IPSec SA（AH/ESP 参数、流量选择器、生命周期），用于真实业务流量。

5. 认证协议新鲜性（Freshness）机制

   - 不能只靠加密解决重放问题，必须加 Time-stamp、Sequence Number、Nonce 之一。
   - 时间戳方案消息轮次少，但依赖时钟同步；Nonce 更通用但需保证随机且不可预测。

3 设计题（高分模板）

1. 防火墙规则设计模板

   - 原则：默认拒绝（deny all）+ 最小权限 + 显式放行。
   - 先写具体规则再写兜底 drop any any（规则匹配通常是自上而下第一条命中）。
   - 同时考虑源地址、目的地址、端口/服务、状态（stateful）、日志审计。

2. DMZ 与双防火墙架构

   - 外防火墙：只允许公网访问 DMZ 必要服务（如 Web/邮件），其余拒绝。
   - 内防火墙：严格限制 DMZ 到内网，仅放行明确业务流（如 DNS/邮件中继等）。
   - 目标：公网可访问服务与内网核心资产物理/逻辑隔离。

3. 网络加固清单（可直接作答）

   - 设备补丁及时更新（交换机/路由器/防火墙）。
   - 交换机启用端口安全（MAC 绑定、限制非法接入）。
   - 路由器 ACL 前置过滤恶意或无关流量，减轻边界防火墙压力。
   - 使用 SNMPv3（认证 + 加密 + 访问控制），避免弱管理协议暴露。
   - 关键链路和安全设备做冗余，避免单点故障。
   - 主机加固：关闭不必要服务、最小化开放端口、强化认证与审计。
   - 出站过滤（egress filtering），防止内网被利用对外攻击。
   - 远程接入走 VPN 并强化端点安全，防止“被感染终端穿透内网”。

4. IDS/IPS 部署与响应

   - 典型放置点：防火墙前后、敏感子网前、关键主机本地。
   - 响应策略：被动（日志 + 告警）与主动（断连/重配置/阻断）结合。
   - NIDS 若要“防御化”（IPS 能力）需串联在线，但要评估性能与单点风险。

4 常见易错点（考试容易丢分）

1. 把 BLP 和 Biba 读写方向记反。

2. 误以为 CHAP 会传口令本身。

3. 误以为 AH 提供加密，或误以为 ESP 保护外层 IP 头完整性。

4. 把 IKE Phase 1 与 Phase 2 职责混淆（先建安全信道，再建业务 SA）。

5. 只写“上防火墙”不写规则顺序、默认拒绝、日志与 DMZ 隔离边界。

6. 忽略加密流量下 NIDS 可见性问题与交换网络镜像/旁路部署条件。