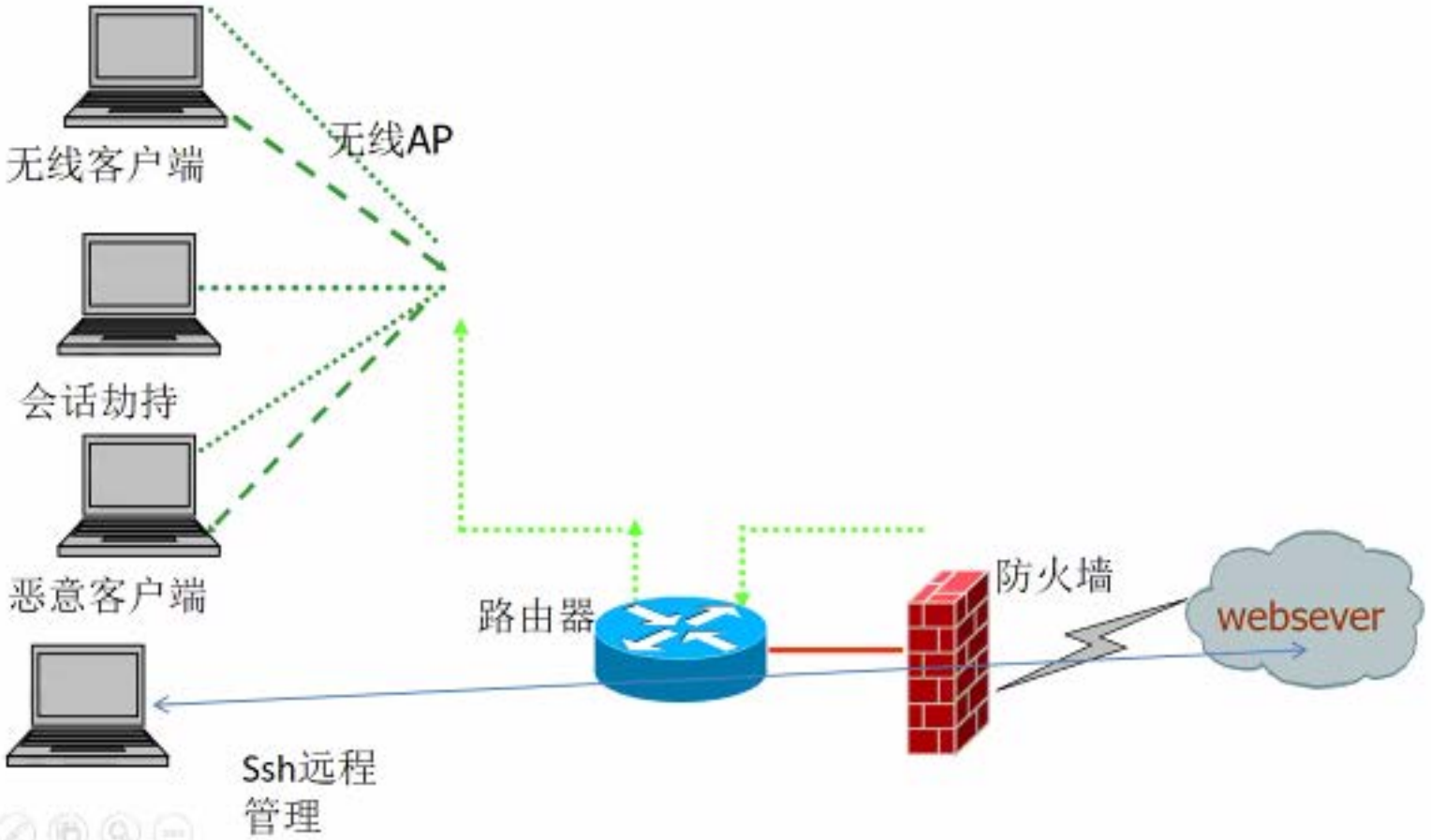
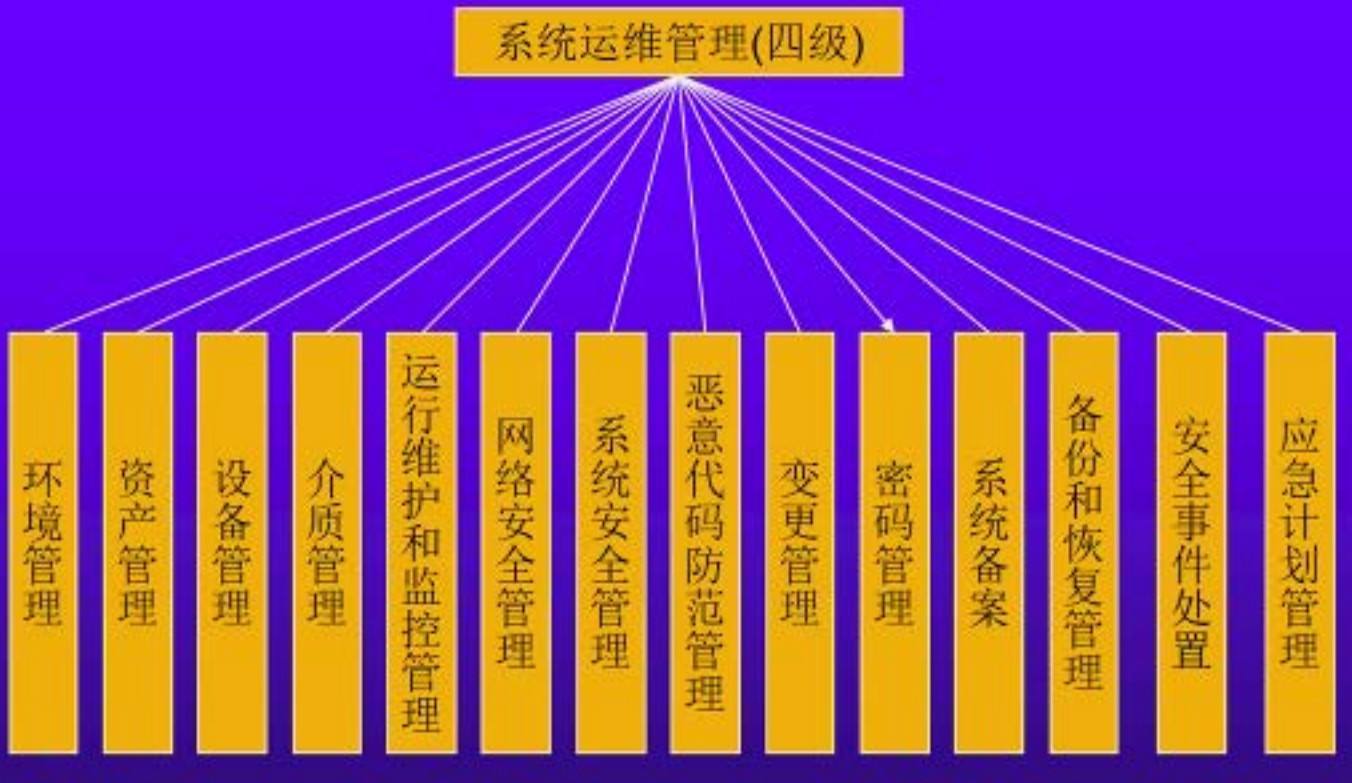
F1 考虑如下应用环境，要求webserver按等级保护3级建立安全机制，如何评估安全体系？



F2 研究以下问题if该web服务基于lamp实现:

- SEC 1 如果该LAMP定级为等级保护第三级，其数据安全、应用安全技术要求分别有哪些类、多少检查点？描述其具体细则。
- SEC 2 比较分析可对数据安全进行评估的主流扫描工具或系统，用表格对比其适用、用法、优点、局限性
- Sec3 比较分析可对web服务可用性进行评估的主流扫描工具或系统，用表格对比其适用、用法、优点、局限性
- Sec 4 用sec2、sec3优选出的工具对sec1典型的lamp网站进行数据安全和服务安全等级保护3级评估，具体描述实施方法、流程、数据采集、分析及验证实例。

基本要求-组织方式


系统运维管理(四级)
环境管理
资产管理
设备管理
介质管理
运行维护和监控管理
网络安全管理
系统安全管理
恶意代码防范管理
变更管理
密码管理
系统备案
备份和恢复管理
安全事件处置
应急计划管理

基本要求标注方式

- 基本要求
  - 技术要求
  - 管理要求

- 要求标注
  - 业务信息安全类要求（标记为S类）
  - 系统服务保证类要求（标记为A类）
  - 通用安全保护类要求（标记为G类）

三类要求之间的关系

安全要求

安全保护和系统定级的关系

- 定级指南要求按照“业务信息”和“系统服务”的需求确定整个系统的安全保护等级
- 定级过程反映了信息系统的保护要求

安全等级	信息系统保护要求的组合
第一级	S1A1G1
第二级	S1A2G2，S2A2G2，S2A1G2
第三级	S1A3G3，S2A3G3，S3A3G3，S3A2G3，S3A1G3
第四级	S1A4G4，S2A4G4，S3A4G4，S4A4G4，S4A3G4，S4A2G4，S4A1G4

不同级别系统控制点的差异

安全要求类	层面	一级	二级	三级	四级
技术要求	物理安全	7	10	10	10
	网络安全	3	6	7	7
	主机安全	4	6	7	9
	应用安全	4	7	9	11
	数据安全及备份恢复	2	3	3	3
管理要求	安全管理制度	2	3	3	3
	安全管理机构	4	5	5	5
	人员安全管理	4	5	5	5
	系统建设管理	9	9	11	11
	系统运维管理	9	12	13	13
合计	/	48	66	73	77
级差	/	/	18	7	4

应用安全	7	19	31	36
数据安全及备份恢复	2	4	8	11

各级系统安全保护要求-网络安全

控制点	一级	二级	三级	四级
结构安全	*	*	*	*
访问控制	*	*	*	*
安全审计		*	*	*
边界完整性检查		*	*	*
入侵防范		*	*	*
恶意代码防范			*	*
网络设备防护	*	*	*	*
合计	3	6	7	7

各级系统安全保护要求-网络安全

- 一级网络安全要求：主要提供网络安全运行的基本保障，包括网络结构能够基本满足业务运行需要，网络边界处对进出的数据包头进行基本过滤等访问控制措施。
- 二级网络安全要求：不仅要满足网络安全运行的基本保障，同时还要考虑网络处理能力要满足业务极限时的需要。对网络边界的访问控制粒度进一步增强。同时，加强了网络边界的防护，增加了安全审计、边界完整性检查、入侵防范等控制点。对网络设备的防护不仅局限于简单的身份鉴别，同时对标识和鉴别信息都有了相应的要求。
- 三级网络安全要求：对网络处理能力增加了“优先级”考虑，保证重要主机能够在网络拥堵时仍能够正常运行；网络边界的访问控制扩展到应用层，网络边界的其他防护措施进一步增强，不仅能够被动的“防”，还应能够主动发出一些动作，如报警、阻断等。网络设备的防护手段要求两种身份鉴别技术综合使用。
- 四级网络安全要求：对网络边界的访问控制做出了更为严格的要求，禁止远程拨号访问，不允许数据带通用协议通过；边界的其他防护措施也加强了要求。网络安全审计着眼于全局，做到集中审计分析，以便得到更多的综合信息。网络设备的防护，在身份鉴别手段上除要求两种技术外，其中一种鉴别技术必须是不可伪造的，进一步加强了对网络设备的防护。