1.

(1) 服务控制

决定Internet服务可以被访问，无论这些服务是从内而外还是从外而内

(2) 方向控制

决定在哪些特定的方向上服务请求可以被发起并通过防火墙

(3) 用户控制

根据用户正在试图访问的服务器，来控制其访问。

(4) 行为控制

控制一个具体的服务器怎样被实现。

2. 基本原理：

包过滤技术是最早的防火墙技术，工作在网络层。

这种防火墙的原理是将IP数据报的各种包头信息与防火墙内的规则进行比较，然后根据过滤规则有选择的阻止或允许数据包通过防火墙。

包过滤防火墙要遵循的一条基本准则就是"最小特权原则"，即明确地管理员希望通过的那些数据包，禁止其他的数据包。包过滤的核心技术是安全策略制及过滤规则的设计。

包过滤防火墙一般由路由器充当，要求路由器在完成路由选择和数据转发外，同时具有包过滤功能。

3.

(1)

(2)

(3)

(4)

(5)

3.

(1) 事件生成器：它是采集和过滤事件程序的程序或模块
负责收集原始数据，对数据流、日志文件等进行追踪，然后将搜集到的原始数据转化为事件，并向系统其它部份提供此事件。

(2) 事件分析器：事件分析器是分析事件数据和任何 CIDF 组件传送给它的各种数据。

(3) 事件数据库：负责存放各种原始数据或已加工数据。
它从事件生成器或事件分析器接收数据并进行保存，它可以是复杂的数据库，也可以是简单的文本。

(4) 响应单元：是针对分析组件所产生的分析结果，根据响应策略采取相应的行为，发出命令响应攻击。

(5) 目录服务器：目录服务器用于各组件定位其他组件，以及控制其他组件传递的数据并认证其他组件的使用，以防止检测入侵系统本身受到攻击。

4. 异常检测与误用检测不同：
异常检测是基于行为偏离正常或所期望的系统和用户规律而被检测出来；而误用检测是检测行为符合某一种已知的入侵行为相匹配而被检测出来。

5、蜜罐的功能：

①布置具有诱导欺骗性的主机，诱使攻击方对其进行网络攻击，从而可以对攻击进行捕获与分析，了解攻击方所使用的工具与方法，推测攻击意图和动机，让防御方清晰的认识威胁，并通过技术与管理手段来增强实际的安全防护能力。