1. 误用检测是事先定义出已知的入侵行为的入侵特征，将实际环境中的数据与之匹配，根据匹配程度来判断是否发生了入侵攻击行为。

异常检测是根据使用者的行为或资源使用状况的程度与正常状态下的标准特征（活动轮廓）之间的偏差来判断是否遭到入侵。如果偏差高于阈值，则发生异常。

因而误用检测依赖于已知的具体行为，要不断更新已知入侵特征，而异常检测不依赖，通用性较强，但确定偏差是否达到阈值有难度。

2.CIDF是对IDS进行标准化和研究的一个开放组织。CIDF通用模型包括：事件产生器，事件分析器，事件数据库，响应单元。

3.我认为不行，防火墙只是静态检测，对已经通过防火墙的数据包就不再检查，而入侵检测系统是动态的，对数据实时进行检测，可以进一步检测防火墙没有发现的入侵行为，从而提高安全性。