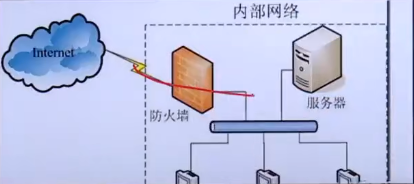
防火墙与入侵检测系统

1. 防火墙基本概念

防火墙：能够隔离组织内部网络与公共互联网，允许某些分组通过，而阻止其它分组进入或离开内部网络的软件、硬件或者软件硬件结合的一种设施

前提：从外部到内部和从内部到外部的所有流量都经过防火墙



1. 防火墙分类
2. 无状态分组过滤器：基于特定的规则对分组是通过还是丢弃进行抉择。使用访问控制列表（ACL）（通过地址以及端口）实现防火墙规则
3. 有状态分组过滤器：跟踪每个TCP连接建立、拆除，根据状态确定是否允许分组通过
4. 应用网关：鉴别用户身份或针对授权用户开放特定服务
5. 入侵检测系统

入侵检测系统（IDS）是当观察到潜在的恶意流量时，能够产生警告的设备或系统

