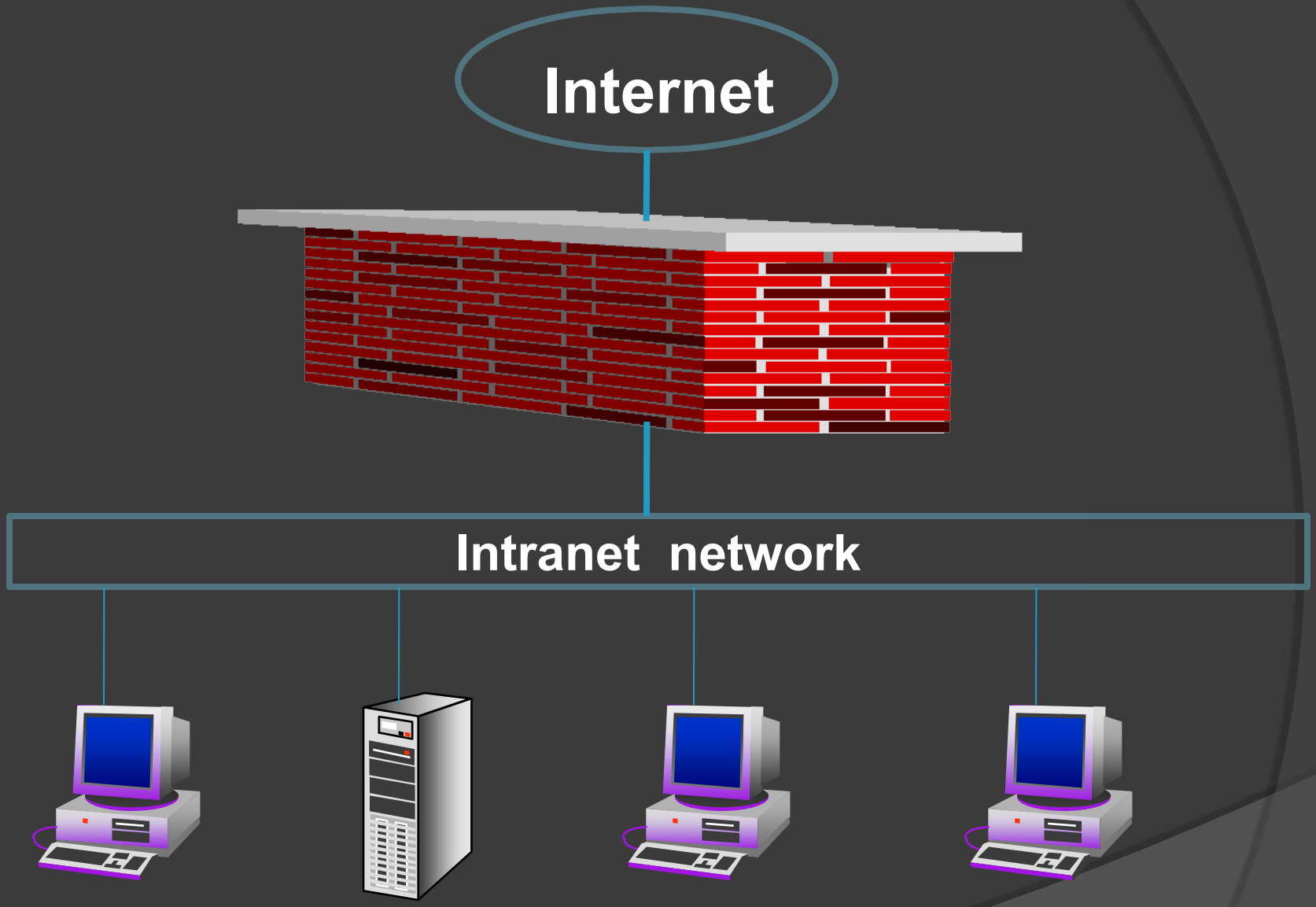
8. 4防火墙技术

学习目的：

- 了解防火墙的概念及原理
- 了解多种防火墙技术
- 掌握防火墙的体系构造
- 了解防火墙的前沿技术


Internet
Intranet network

防火墙的概念及原理

防火墙：是在内部网和外部王之间实施安全防范的系统。用于拟定哪些内部服务对外开放，以及允许哪些外部服务对内部开放。它能够根据网络传播的类型决定IP包是能够进出企业网、预防非侵权访问企业内部网、允许使用授权机器的顾客远程访问企业内部、管理企业内部人员对Internet的访问。

防火墙的构成体现式：防火墙=过滤器+安全策略

防火墙经过逐一审查收到的每个数据包，判断它是否有相匹配的过滤规则，即根据策略表中规则的先后顺序以及每条规则的条件逐项比较，直到满足某一条规则的条件，并作要求的动作（中断或先前转发），从而来保护网络的安全。

防火墙主要提供下列四种服务：

1）服务控制：拟定能够访问的网络服务类型。
2）方向控制：特定服务的方向流控制。
3）顾客控制：内部顾客、外部顾客所需的某种形式的认证机制。
4）行为控制：控制怎样使用某种特定的服务。

防火墙的分类

防火墙一般能够分为下列几种：包过滤型防火墙、应用网关型防火墙、电路级网关防火墙、状态检测型防火墙、自适应代理型防火墙。

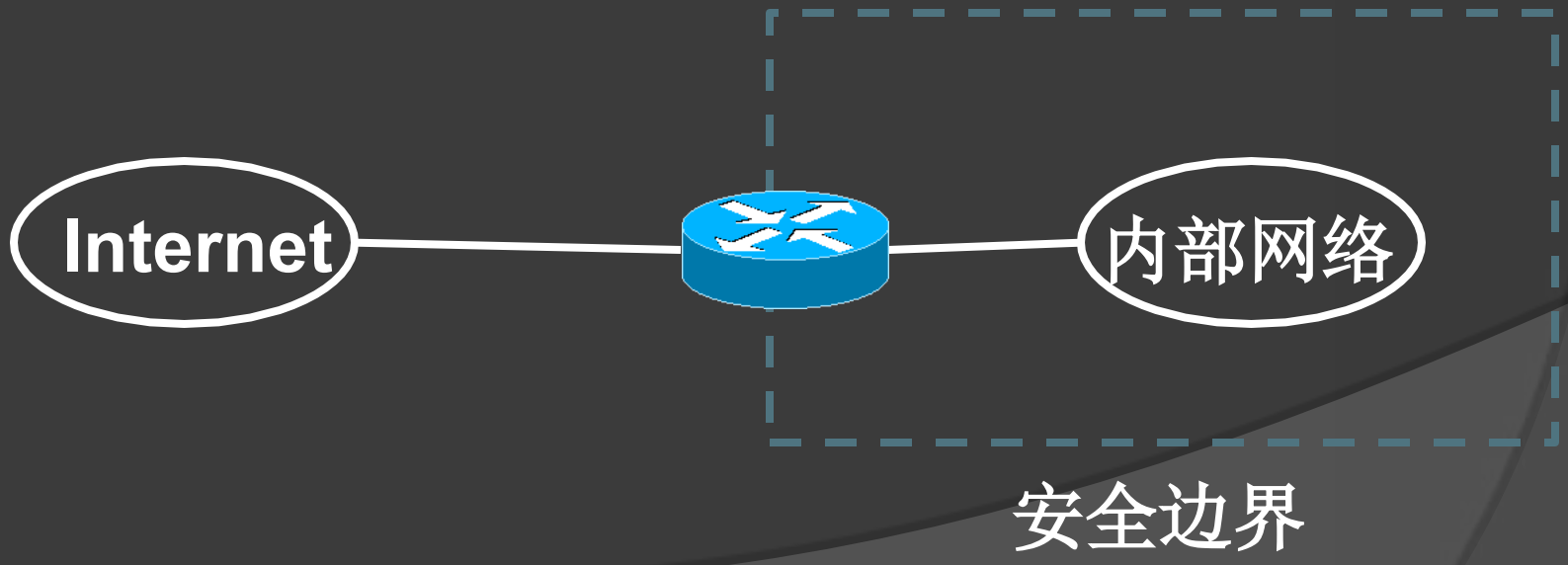
1.包过虑型防火墙

（1）包过滤最早、最简朴的防火墙技术，基于协议的内容进行过滤。

“包过滤”经过将每一输入输出包中发觉的信息同访问控制规则相比较来决定阻塞

或放行包。经过检验数据流中每一种数据包的源地址、目的地址、全部端口、协议状态等原因，或它们的组合来拟定是否允许该数据包经过，假如包在这一测试中失败，将在防火墙处被丢弃。

包过滤防火墙如图：



包过滤器操作的基本过程：包过滤规则必须被包过滤设备端口存储起来。当包到达端口时，对包报头进行语法分析。（大多数包过滤设备只检验IP、TCP或UDP报头中的字段）

在包过滤器中根据包过滤规则来决定是否让数据包经过：

若一条规则阻止包传播或接受，则此包便不被允许。

若一条规则允许包传播或接受，此包便能够被继续处理。

若包不满足任何一条规则，则此包便被继续处理。

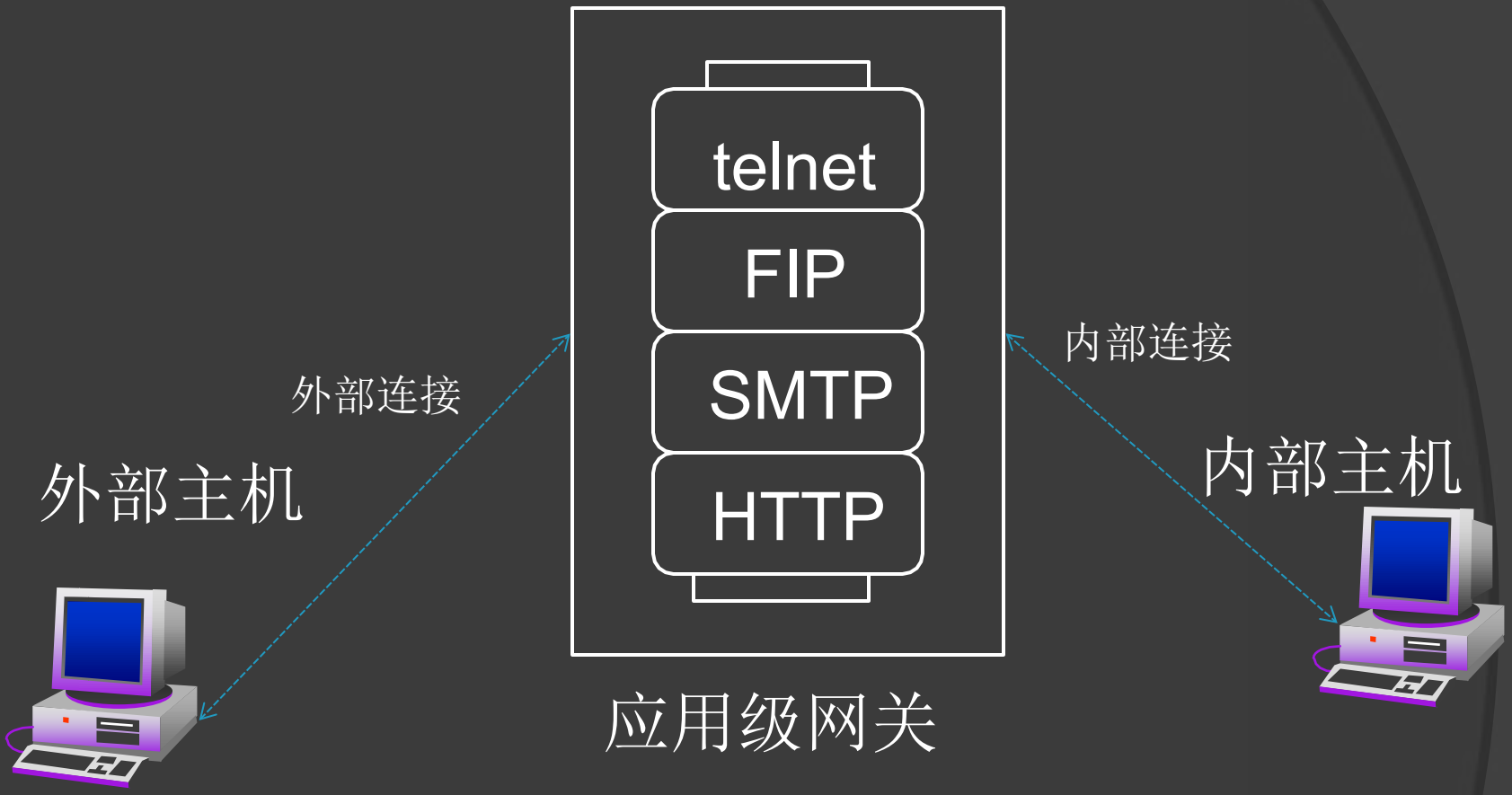
包过滤技术优点:对于一种小型的、不太复杂的站点，包过滤比较轻易实现；而且处理包的速度比代理服务器快；过滤路由器在价格上一般比代理服务器便宜。

缺陷：某些包过滤网关不支持有效的顾客认证；包过滤防火墙只能阻止一种类型的IP欺骗，即外部主机伪装内部主机的IP，对于外部主机伪装外部主机的IP欺骗却不可能阻止，而且它也不能预防DNS欺骗。

2.应用代理级防火墙

应用代理级防火墙模式提供了十分先进的安全控制机制。它经过在协议栈的最高层（应用层）检验每一种包从而提供足够的应用级连接信息。目前大多采用一种网关来管理应用服务，在其上安装相应于每种服务的特殊代码，在此网关上控制和管理各类应用层的网络连接。

应用级代理防火墙能很轻易看见前面提及的每一种连接的细节从而实现多种安全策略。


telnet
FIP
SMTP
HTTP
外部连接
内部连接
外部主机
内部主机
应用级网关

3.电路级网关型防火墙

电路级网关防火墙起一定的代理服务作用，它监视两个主机建立连接的握手信息，从而判断该会话祈求是否正当，一旦会话连接有效，该网关仅复制、传递数据。它在IP层代理多种高层会话，具有隐藏内部网络信息的能力，且透明性高，但安全性稍低。

其中，电路型网关不允许进行端点到端点的TCP连接，而是建立两个TCP连接。网关一般就是将TCP数据包从一种连接转送到另一种连接中去，而不检验里面的内容。目的是拟定哪些连接是允许的。