1. 防火墙基本信息

\*定义：I T 领域使用的防火墙是一种高级访问控制设备，置于不同网络安全域之间的一系列部件的组合，它是不同网络安全域间通信流的唯一通道，能根据企业有关的安全政策控制进出网络的访问行为。

\*作用：通过部署防火墙，可以实现比交换机、路由器更为强大、有效的访问控制功能；大大提高抗攻击的能力。

\*具体功能：（1）过滤进出网络的数据。（2）管理进出网络的访问行为。（3）封堵某些禁止的业务。（4）记录进出网络的信息和活动。（5）对网络攻击进行检测和告警。

\*分类：（1）软件防火墙；（2）硬件防火墙。

\*须满足的要求：（1）所有进出网络的数据流都必须经过防火墙。（2）只允许经过授权的数据流通过防火墙。（3）只允许经过授权的数据流通过防火墙。

\*局限性：（1）不能防御内部攻击。（2）不能防御绕过防火墙的攻击。（3）不能防御不断更新的攻击。（4）不能防御数据驱动的攻击。

\*性能指标：（1）吞吐量（2）时延（3）丢包率（4）背靠背（5）并发连接数

#防火墙是网络开放性和安全控制性矛盾对立的产物。

1. 包过滤防火墙（分组过滤）

\*基本概念：分组过滤器，顾名思义，就是从一个网络进入另一个网络的全部IP分组中筛选出符合用户指定特征的一部分IP分组，并对这一部分IP分组的网络间传输过程实施控制。

\*工作原理：防火墙在网络层中根据数据包中包头信息有选择地实施允许通过或阻断。

\*特点：包过滤方式是一种通用、廉价和有效的安全手段。

\*分类：（1）静态（2）动态

3.包过滤防火墙（分组过滤）—-静态包过滤防火墙

\*工作原理：防火墙在网络层中根据数据包中包头信息有选择地实施允许通过或阻断。

\*访问控制列表的配置有两种方式：

严策略（白名单）。列出所有允许传输的IP分组类型，，拒绝其他所有IP包；

宽策略（黑名单）。列出所有禁止传输的IP分组类型，接受其他所有IP包。

\*优缺点：

优点：（1）逻辑简单，价格便宜。（2）对网络性能的影响较小，有较强的透明性。

（3）它的工作与应用层无关，易于安装和使用。

缺点：（1）配置需要对IP、TCP、UDP、ICMP等各种协议有深入的了解；（2）由于过滤判别的只有网络层和传输层的有限信息，因而各种安全要求不能得到充分满足；（3）由于数据包的地址及端口号都在数据包的头部，不能彻底防止地址欺骗；（4）允许外部客户和内部主机的直接连接；（5）不提供用户的鉴别机制。

\*常用：商业版防火墙产品、个人防火墙、路由器。

#访问控制规则常称为数据包过滤访问控制列表（ACL）。

#开始从上至下扫描过滤规则，如果匹配成功则按照规则设定的操作执行，不再匹配后续规则。所以，在访问控制列表中规则的出现顺序至关重要。



4.包过滤防火墙（分组过滤）—动态包过滤防火墙（有状态分组过滤）

\*工作原理：状态包过滤（Stateful Packet Filter）是一种基于连接的状态检测机制，将属于同一连接的所有包作为一个整体的数据流看待，对接收到的数据包进行分析，判断其是否属于当前合法连接，从而进行动态地过滤。

\*与静态包过滤防火墙区别：（1）访问策略不同，不是定义了允许或不允许传输的IP分组，而是定义了整个服务过程。（2）跟传统包过滤只有一张过滤规则表不同，状态包过滤同时维护过滤规则表（静态不变）和状态表（动态变化）。



\*局限性：

1. 基于网络层和传输层实现的包过滤防火墙难以实现对应用层服务的过滤。
2. 访问控制列表的配置和维护困难。
3. 对安全管理人员的要求高。
4. 包过滤防火墙难以详细了解主机之间的会话关系。
5. 很容易遭受欺骗型攻击。

#首先需要鉴别出属于同一会话的IP分组，然后根据会话的属性与状态对属于该会话的IP分组的网络间传输过程进行控制。

5.应用代理型防火墙

\*概述：采用应用代理技术的防火墙工作在应用层。其特点是完全“阻隔”了网络通信流，通过对每种应用服务编制专门的代理程序，实现监视和控制应用层通信流的作用。

\*分类：（1）电路级网关防火墙（2）应用级网关防火墙

1. 应用代理型防火墙—电路级网关防火墙

\*概述：电路级网关防火墙（Circuit Level Gateway）是一个通用代理服务器。它工作在TCP/IP协议的传输层（TCP），可以对各种不同的应用协议提供服务，但这种代理需要改进客户程序。

\*工作原理：不允许进行端-端的TCP连接。而是建立两个TCP连接：一个在网关和内部主机上的TCP用户程序之间；另一个在网关和外部主机的TCP用户程序之间。一旦建立两个连接，电路级网关防火墙只是把TCP数据包从一个连接转送到另一个连接中去而不检验其中的内容。**其安全功能就是确定哪些连接是允许的。**

\*优缺点：

优点：它能对各种不同的协议提供服务。

缺点：它对因代理而发生的情况几乎不加控制。

\*一些实现：Socks、Winsock、Dante

1. 应用代理型防火墙—应用级网关防火墙

\*工作原理：当外部网络向内部网络请求服务时，首先对用户的身份进行验证，若为合法用户，则将请求转发给真正的某个内部网络的主机，同时监控用户的操作，拒绝不合法的访问；当内部网络向外部网络申请服务时，应用代理服务器工作过程相反。

\*检测层次：分组过滤器一般只检测IP首部和传输层首部中的源和目的端口号，不会检测传输层报文中净荷的内容。电路层代理通常只检测传输层首部，同样不会检测传输层报文中净荷的内容。应用层网关要求检测应用层消息首部，应用层消息中的消息体，如HTTP首部和HTTP消息体等。

\*安全功能：应用层网关的安全功能是对对应的应用服务器提供保护，有效防御对该应用服务器实施的攻击。

\*优缺点：

优点：（1）易于配置，界面友好；（2）不允许内外网主机的直接连接；（3）可以提供比包过滤更详细的日志记录，例如在一个HTTP连接中，包过滤只能记录单个的数据包，无法记录文件名、URL等信息；（4）可以隐藏内部IP地址；（5）可以给单个用户授权；（6）可以为用户提供透明的加密机制；（7）可以与认证、授权等安全手段方便的集成。

缺点：（1）代理速度比包过滤慢；（2）代理对用户不透明，给用户的使用带来不便，灵活性不够；（3）需要针对每种协议设置一个不同的代理服务器。

\*一些应用：商业版防火墙产品、商业版代理(cache)服务器

#应用层代理只能为一种特定的服务（如FTP和Telnet等）提供代理服务。

1. 防火墙的体系结构—双宿主主机模式

\*工作原理：堡垒主机充当应用层网关。在主机中需要插入两块网卡，用于将主机分别连接到被保护的内网和外网上。在主机上运行防火墙软件，被保护内网与外网间的通信必须通过主机，因而可以将内网很好地屏蔽起来。内网可以通过堡垒主机获得外网提供的服务。

\*特点：堡垒主机的路由功能是被禁止的，两个网络之间不能直接互相通信，它们之间的通信通过应用层代理服务来完成。

\*优缺点：

优点：这种应用层网关能有效地保护和屏蔽内网，且要求的硬件较少，因而是应用较多的一种防火墙；

缺点：但堡垒主机本身缺乏保护，容易受到攻击。

#“堡垒主机” 起着防火墙的作用，即隔离内外网的作用。

1. 防火墙的体系结构—屏蔽主机模式

\*特点：屏蔽主机（Screened Host）防火墙由包过滤路由器和堡垒主机组成， 实现了网络层安全（包过滤）和应用层安全（代理服务）的结合。

\*优缺点：

优点：屏蔽主机网关是一种更为灵活的防火墙软件，它可以利用屏蔽路由器来做更进一步的安全保护。

缺点：（1）堡垒主机与其他主机在同一个子网，一旦堡垒主机被攻破或被越过，整个内网和堡垒主机之间就再也没有任何阻挡。（2）此时的路由器又处于易受攻击的地位。（3）此外，网络管理员应该管理在路由器和堡垒主机中的访问控制表，使两者协调一致，避免出现矛盾。

10.防火墙的体系结构—屏蔽子网模式

\*基本原理：采用了两个包过滤路由器和一个堡垒主机，在内外网络之间建立了一个被隔离的子网，定义为“非军事区” ，有时也称作周边网，用于放置堡垒主机，WEB服务器、Mail服务器等公用服务器。内部网络和外部网络均可访问屏蔽子网，但禁止它们穿过屏蔽子网通信。在这一配置中，即使堡垒主机被入侵者控制，内部网仍受到内部包过滤路由器的保护。

\*特点：建立了一个被隔离的子网——DMZ。

\*分为3个不同的安全区域：（1）外部网络。（2）DMZ网络。（3）内部网络。

\*优点：安全性高（...）。

11.对于以上典型的网络体系结构，可以部署3种类型的防火墙

\*外部防火墙。

\*内部防火墙。

\*主机型防火墙，又称个人防火墙。