http://www.jdzj.com/diangong/article/2009-8-27/12145-1.htm

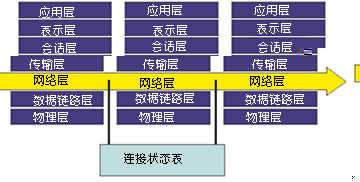
防火墙能增强机构内部网络的安全性。防火墙系统决定了哪些内部服务可以被外界访问；外界的哪些人可以访问内部的服务以及哪些外部服务可以被内部人员访问。防火墙必须只允许授权的数据通过，而且防火墙本身也必须能够免于渗透。  
  
　　防火墙的五大功能   
  
　　一般来说，防火墙具有以下几种功能：   
  
　　1．允许网络管理员定义一个中心点来防止非法用户进入内部网络。   
  
　　2．可以很方便地监视网络的安全性，并报警。   
  
　　3．可以作为部署NAT（Network Address Translation，网络地址变换）的地点，利用NAT技术，将有限的IP地址动态或静态地与内部的IP地址对应起来，用来缓解地址空间短缺的问题。   
  
　　4．是审计和记录Internet使用费用的一个最佳地点。网络管理员可以在此向管理部门提供Internet连接的费用情况，查出潜在的带宽瓶颈位置，并能够依据本机构的核算模式提供部门级的计费。   
  
　　两种防火墙技术的对比  
  
　　包过滤防火墙   
  
　　优点   
  
　　价格较低   
  
　　性能开销小，处理速度较快

缺点   
  
　　定义复杂，容易出现因配置不当带来问题   
  
　　允许数据包直接通过，容易造成数据驱动式攻击的潜在危险

　　代理防火墙   
  
　　内置了专门为了提高安全性而编制的Proxy应用程序，能够透彻地理解相关服务的命令，对来往的数据包进行安全化处理   
  
　　速度较慢，不太适用于高速网（ATM或千兆位以太网等）之间的应用   
  
　　5．可以连接到一个单独的网段上，从物理上和内部网段隔开，并在此部署WWW服务器和FTP服务器，将其作为向外部发布内部信息的地点。从技术角度来讲，就是所谓的停火区（DMZ）。   
  
　　防火墙的两大分类   
  
　 　尽管防火墙的发展经过了上述的几代，但是按照防火墙对内外来往数据的处理方法，大致可以将防火墙分为两大体系：包过滤防火墙和代理防火墙（应用层网关防 火墙）。前者以以色列的Checkpoint防火墙和Cisco公司的PIX防火墙为代表，后者以美国NAI公司的Gauntlet防火墙为代表。   
  
　　1．包过滤防?   
  
　　第一代：静态包过滤   
  
　 　这种类型的防火墙根据定义好的过滤规则审查每个数据包，以便确定其是否与某一条包过滤规则匹配。过滤规则基于数据包的报头信息进行制订。报头信息中包括 IP源地址、IP目标地址、传输协议(TCP、UDP、ICMP等等)、TCP/UDP目标端口、ICMP消息类型等。包过滤类型的防火墙要遵循的一条基 本原则是“最小特权原则”，即明确允许那些管理员希望通过的数据包，禁止其他的数据包。

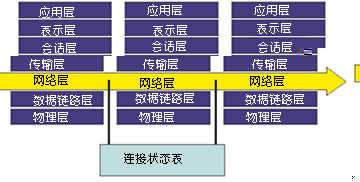
  
  
　　图1 简单包过滤防火墙

第二代：动态包过滤   
  
　　这种类型的防火墙采用动态设置包过滤规则的方法，避免了静态包过滤所具有的问题。这种技术后来发展成为所 谓包状态监测（Stateful Inspection）技术。采用这种技术的防火墙对通过其建立的每一个连接都进行跟踪，并且根据需要可动态地在过滤规则中增加或更绿跄俊?

  
  
　　图2 动态包过滤防火墙

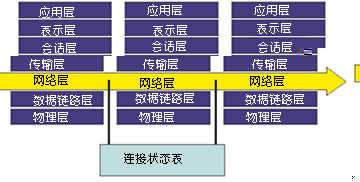
　　2． 代理防火墙   
  
　　第一代：代理防火墙   
  
　　代理防火墙也叫应用层网关（Application Gateway）防火墙。这种防火墙通过一种代理（Proxy）技术参与到一个TCP连接的全过程。从内部发出的数据包经过这样的防火墙处理后，就好像是 源于防火墙外部网卡一样，从而可以达到隐藏内部网结构的作用。这种类型的防火墙被网络安全专家和媒体公认为是最安全的防火墙。它的核心技术就是代理服务器 技术。   
  
　　所谓代理服务器，是指代表客户处理在服务器连接请求的程序。当代理服务器得到一个客户的连接意图时，它们将核实客户请求，并 经过特定的安全化的Proxy应用程序处理连接请求，将处理后的请求传递到真实的服务器上，然后接受服务器应答，并做进一步处理后，将答复交给发出请求的 最终客户。代理服务器在外部网络向内部网络申请服务时发挥了中间转接的作用。

第二代：动态包过滤   
  
　　这种类型的防火墙采用动态设置包过滤规则的方法，避免了静态包过滤所具有的问题。这种技术后来发展成为所 谓包状态监测（Stateful Inspection）技术。采用这种技术的防火墙对通过其建立的每一个连接都进行跟踪，并且根据需要可动态地在过滤规则中增加或更绿跄俊?

  
  
　　图2 动态包过滤防火墙

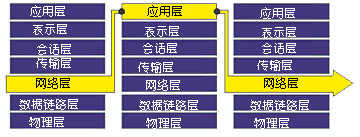
　　2． 代理防火墙   
  
　　第一代：代理防火墙   
  
　　代理防火墙也叫应用层网关（Application Gateway）防火墙。这种防火墙通过一种代理（Proxy）技术参与到一个TCP连接的全过程。从内部发出的数据包经过这样的防火墙处理后，就好像是 源于防火墙外部网卡一样，从而可以达到隐藏内部网结构的作用。这种类型的防火墙被网络安全专家和媒体公认为是最安全的防火墙。它的核心技术就是代理服务器 技术。   
  
　　所谓代理服务器，是指代表客户处理在服务器连接请求的程序。当代理服务器得到一个客户的连接意图时，它们将核实客户请求，并 经过特定的安全化的Proxy应用程序处理连接请求，将处理后的请求传递到真实的服务器上，然后接受服务器应答，并做进一步处理后，将答复交给发出请求的 最终客户。代理服务器在外部网络向内部网络申请服务时发挥了中间转接的作用。

第二代：动态包过滤   
  
　　这种类型的防火墙采用动态设置包过滤规则的方法，避免了静态包过滤所具有的问题。这种技术后来发展成为所 谓包状态监测（Stateful Inspection）技术。采用这种技术的防火墙对通过其建立的每一个连接都进行跟踪，并且根据需要可动态地在过滤规则中增加或更绿跄俊?

  
  
　　图2 动态包过滤防火墙

　　2． 代理防火墙   
  
　　第一代：代理防火墙   
  
　　代理防火墙也叫应用层网关（Application Gateway）防火墙。这种防火墙通过一种代理（Proxy）技术参与到一个TCP连接的全过程。从内部发出的数据包经过这样的防火墙处理后，就好像是 源于防火墙外部网卡一样，从而可以达到隐藏内部网结构的作用。这种类型的防火墙被网络安全专家和媒体公认为是最安全的防火墙。它的核心技术就是代理服务器 技术。   
  
　　所谓代理服务器，是指代表客户处理在服务器连接请求的程序。当代理服务器得到一个客户的连接意图时，它们将核实客户请求，并 经过特定的安全化的Proxy应用程序处理连接请求，将处理后的请求传递到真实的服务器上，然后接受服务器应答，并做进一步处理后，将答复交给发出请求的 最终客户。代理服务器在外部网络向内部网络申请服务时发挥了中间转接的作用。

代理类型防火墙的最突出的优点就是安全。由于每一个内外网络之间的连接都要通过Proxy的介入和转换，通过专门为特定的服务如Http编写的安全 化的应用程序进行处理，然后由防火墙本身提交请求和应答，没有给内外网络的计算机以任何直接会话的机会，从而避免了入侵者使用数据驱动类型的攻击方式入侵 内部网。包过滤类型的防火墙是很难彻底避免这一漏洞的。就像你要向一个陌生的重要人物递交一份声明一样，如果你先将这份声明交给你的律师，然后律师就会审 查你的声明，确认没有什么负面的影响后才由他交给那个陌生人。在此期间，陌生人对你的存在一无所知，如果要对你进行侵犯，他面对的将是你的律师，而你的律 师当然比你更加清楚该如何对付这种人。

  
  
　图3 传统代理型防火墙

　　代理防火墙的最大缺点就是速度相对比较慢，当用户对内外网络网关的吞吐量要求比较高时，（比如要求达到75-100Mbps时）代理防火墙就会 成为内外网络之间的瓶颈。所幸的是，目前用户接入Internet的速度一般都远低于这个数字。在现实环境中，要考虑使用包过滤类型防火墙来满足速度要求 的情况，大部分是高速网（ATM或千兆位以太网等）之间的防火墙。   
  
　　第二代：自适应代理防火墙   
  
　　自适应代理技术 （Adaptive proxy）是最近在商业应用防火墙中实现的一种革命性的技术。它可以结合代理类型防火墙的安全性和包过滤防火墙的高速度等优点，在毫不损失安全性的基础 之上将代理型防火墙的性能提高10倍以上。组成这种类型防火墙的基本要素有两个：自适应代理服务器（Adaptive Proxy Server）与动态包过滤器（Dynamic Packet filter）。

  
  
　　图4 自适应代理防火墙

在自适应代理与动态包过滤器之间存在一个控制通道。在对防火墙进行配置时，用户仅仅将所需要的服务类型、安全级别等信息通过相应Proxy的管理界 面进行设置就可以了。然后，自适应代理就可以根据用户的配置信息，决定是使用代理服务从应用层代理请求还是从网络层转发包。如果是后者，它将动态地通知包 过滤器增减过滤规则，满足用户对速度和安全性的双重要求。   
  
小资料   
  
　　防火墙的发展史   
  
　　第一代防火墙   
  
　　第一代防火墙技术几乎与路由器同时出现，采用了包过滤（Packet filter）技术。下图表示了防火墙技术的简单发展历史。



　　第二、三代防火墙   
  
　　1989年，贝尔实验室的Dave Presotto和Howard Trickey推出了第二代防火墙，即电路层防火墙，同时提出了第三代防火墙——应用层防火墙（代理防火墙）的初步结构。   
  
　　第四代防火墙   
  
　 　1992年，USC信息科学院的BobBraden开发出了基于动态包过滤（Dynamic packet filter）技术的第四代防火墙，后来演变为目前所说的状态监视（Stateful inspection）技术。1994年，以色列的CheckPoint公司开发出了第一个采用这种技术的商业化的产品。  
  
　　第五代防火墙   
  
　　1998年，NAI公司推出了一种自适应代理（Adaptive proxy）技术，并在其产品Gauntlet Firewall for NT中得以实现，给代理类型的防火墙赋予了全新的意义，可以称之为第五代防火墙。