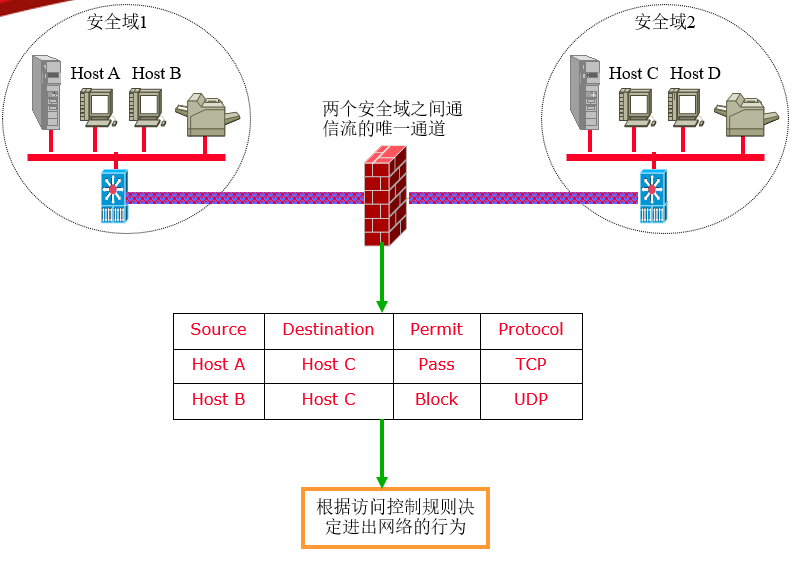
防火墙技术原理

# 一、防火墙的概念

防火墙（Firewall），也称防护墙，是由Check Point 创立者Gil Shwed于1993 年发明并引入国际互联网（US5606668（A）1993-12-15）。

它是一种位于内部网络与外部网络之间的网络安全系统。是一项信息安全的防护系统，依照特定的规则，允许或是限制传输的数据通过。

（图片来源于网络）



在网络的世界里，要由防火墙过滤的就是承载通信数据的通信包。

在网络中，所谓“防火墙”，是指一种将内部网和公众访问网（如Internet）分开的方法，它实际上是一种隔离技术。防火墙是在两个网络通讯时执行的一种访问控制尺度，它能允许你“同意”的人和数据进入你的网络，同时将你“不同意”的人和数据拒之门外，最大限度地阻止网络中的黑客来访问你的网络。换句话说，如果不通过防火墙，公司内部的人就无法访问Internet，Internet上的人也无法和公司内部的人进行通信。

# 二、防火墙的发展历程

防火墙从诞生开始，已经历了四个发展阶段：

* 基于路由器的防火墙
* 用户化的防火墙工具套
* 建立在通用操作系统上的防火墙
* 具有安全操作系统的防火墙

现阶段常见的防火墙属于具有安全操作系统的防火墙，例如NETEYE、NETSCREEN、TALENTIT等。

# 三、防火墙的基本类型

网络层防火墙

网络层防火墙可视为一种 IP 封包过滤器，运作在底层的TCP/IP协议堆栈上。可以以枚举的方式只允许符合特定规则的封包通过，其余的一概禁止穿越防火墙（病毒除外，防火墙不能防止病毒侵入）。这些规则通常可以经由管理员定义或修改，不过某些防火墙设备可能只能套用内置的规则。

应用层防火墙

应用层防火墙是在 TCP/IP 堆栈的“应用层”上运作，您使用浏览器时所产生的数据流或是使用 FTP 时的数据流都是属于这一层。应用层防火墙可以拦截进出某应用程序的所有封包，并且封锁其他的封包（通常是直接将封包丢弃）。理论上，这一类的防火墙可以完全阻绝外部的数据流进到受保护的机器里。

数据库防火墙是一款基于数据库协议分析与控制技术的数据库安全防护系统。基于主动防御机制，实现数据库的访问行为控制、危险操作阻断、可疑行为审计。

数据库防火墙通过SQL协议分析，根据预定义的禁止和许可策略让合法的SQL操作通过，阻断非法违规操作，形成数据库的外围防御圈，实现SQL危险操作的主动预防、实时审计。

数据库防火墙面对来自于外部的入侵行为，提供SQL注入禁止和数据库虚拟补丁包功能。

# 四、Linux 防火墙

Linux 防火墙在企业应用中非常有用，举例如下：

中小企业与网吧里有iptables 作为企业的NAT路由器，可以用来代替传统路由器，而节约成本。

IDC机房一般没有硬件防火墙，IDC机房的服务器可以用Linux 防火墙代替硬件防火墙。

iptables 可以结合squid 作为企业内部上网的透明代理。传统代理需要在浏览器里配置代理服务器信息，而iptables+squid 的透明代理则可以把客户端的请求重定向到代理服务器的端口。客户端不要作任何设置，而感觉不到代理的存在。

将iptables 作为企业NAT 路由器时，可以使用iptables 的扩展模块屏蔽P2P 流量，还可以禁止非法网页。

iptables 可以用于外网IP 向内网IP 映射。

iptables 可以轻松防止轻量级DOS 攻击，比如ping 攻击及SYN 洪水攻击。

综述，Iptables 有两种应用模式：主机防火墙，NAT路由器。

# 五、防火墙的基本原理

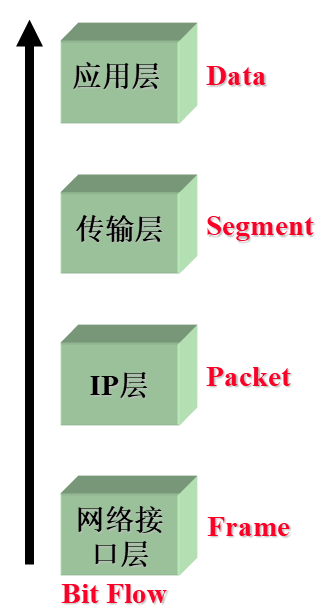
对应下图的字节传输流程，可以分为以下几层：

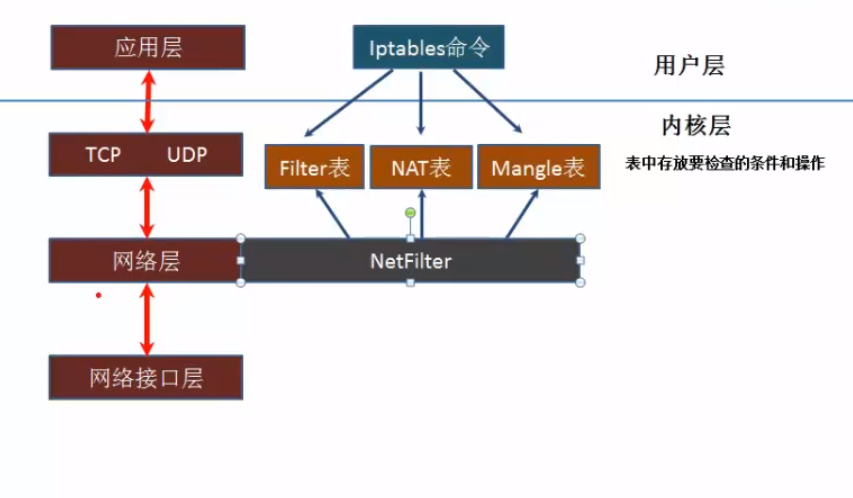
包过滤（Packet filtering）：工作在网络层，仅根据数据包头中的IP地址、端口号、协议类型等标志确定是否允许数据包通过。

应用代理（Application Proxy）：工作在应用层，通过编写不同的应用代理程序，实现对应用层数据的检测和分析。

状态检测（Stateful Inspection）：工作在2~4层，访问控制方式与1同，但处理的对象不是单个数据包，而是整个连接，通过规则表和连接状态表，综合判断是否允许数据包通过。

完全内容检测（Compelete Content Inspection）：工作在2~7层，不仅分析数据包头信息、状态信息，而且对应用层协议进行还原和内容分析，有效防范混合型安全威胁。





# 六、Netfilter 与 iptables

Netfilter是由Rusty Russell提出的Linux 2.4内核防火墙框架，该框架既简洁又灵活，可实现安全策略应用中的许多功能，如数据包过滤、数据包处理、地址伪装、透明代理、动态网络地址转换(Network Address Translation，NAT)，以及基于用户及媒体访问控制(Media Access Control，MAC)地址的过滤和基于状态的过滤、包速率限制等。Iptables/Netfilter的这些规则可以通过灵活组合，形成非常多的功能、涵盖各个方面，这一切都得益于它的优秀设计思想。Netfilter/Iptables 数据包过滤系统可以当成一个整体，netfilter是内核的模块实现，iptables是对上层操作工具。

如果不严格的区分则在Linux中 netfilter 和 iptables 都可以认为是指Linux防火墙。

实际 Iptables 是一个管理内核包过滤的工具，可以用来配置核心包过滤表格中的规则。运行于用户空间。

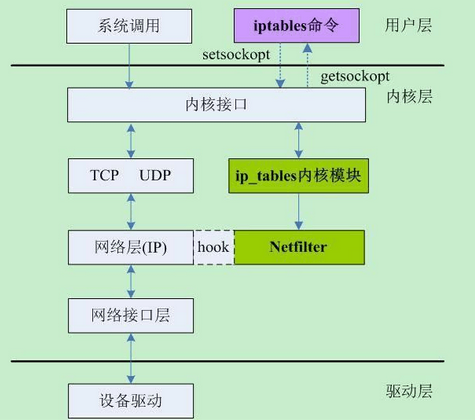
区别在于：netfilter 是 Linux的2.4版内核引入了一种全新的包过滤引擎，称为Netfilter。指的是Linux内核中实现包过滤防火墙的内部结构，不以程序或文件的形式存在，属于“内核态”的防火墙功能体系。iptables指的是用来管理Linux防火墙的命令程序，通常位于/sbin/iptables，属于“用户态”的防火墙管理体系。iptables是控制Netfilter的工具，是Linux 2.2版内核中比较老的命令ipchains的兄弟。

Netfilter 所设置的规则是存放在内核内存中的，而 iptables 是一个应用层的应用程序，它通过 Netfilter 放出的接口来对存放在内核内存中的 XXtables（Netfilter的配置表）进行修改。这个XXtables由表tables、链chains、规则rules组成，iptables在应用层负责修改这个规则文件。类似的应用程序还有 firewalld 。

iptables 和 netfilter 的联系？

很多人一提到防火墙立马就想到了是iptables，其实iptables并不是防火墙，他只是一个软件或者说是一个工具，这个软件可以编写某些规则，将写好的规则保存到netfilter的规则数据库中。因此，真正起到"防火"的功能是netfilter，并不是iptables。netfilter是内核中的一个框架，这个框架里面包含了4个表和5个链，这些链又包含了很多的规则。而数据包要比对的规则就是这个链中所定义的规则。

在下述的内容中我们就以iptables来称呼Linux防火墙了。



# 七、防火墙的性能

**吞吐量**：该指标直接影响网络的性能，吞吐量

**时延**：入口处输入帧最后1个比特到达至出口处输出帧的第1个比特输出所用的时间间隔

**丢包率**：在稳态负载下，应由网络设备传输，但由于资源缺乏而被丢弃的帧的百分比

**背靠背**：从空闲状态开始，以达到传输介质最小合法间隔极限的传输速率发送相当数量的固定长度的帧，当出现第一个帧丢失时，发送的帧数

**并发连结数**：并发连接数是指穿越防火墙的主机之间或主机与防火墙之间能同时建立的最大连接数

# 八、防火墙的局限性

防火墙虽然是保护网络安全的基础性设施，但是它还存在着一些不易防范的安全威胁：

首先防火墙不能防范未经过防火墙或绕过防火墙的攻击。例如，如果允许从受保护的网络内部向外拨号，一些用户就可能形成与Internet 的直接连接。

防火墙基于数据包包头信息的检测阻断方式，主要对主机提供或请求的服务进行访问控制，无法阻断通过开放端口流入的有害流量，并不是对蠕虫或者黑客攻击的解决方案。

另外，防火墙很难防范来自于网络内部的攻击或滥用。

————————————————

版权声明：本文为CSDN博主「石硕页」的原创文章，遵循CC 4.0 BY-SA版权协议，转载请附上原文出处链接及本声明。

原文链接：https://blog.csdn.net/u014209205/article/details/83070305