链滴

防火墙的结构和原理

作者：Gakkiyomi2019

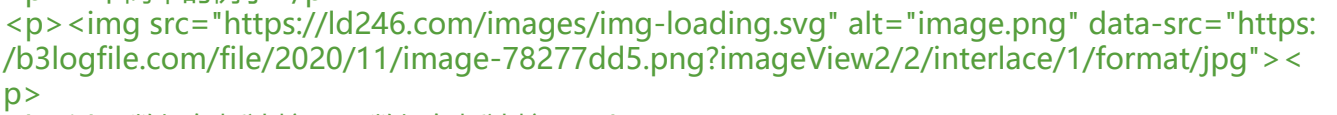
原文链接：https://ld246.com/article/1606550909030

来源网站：链滴

<img src="https://ld246.com/images/img-loading.svg" alt="" data-src="https://b3logfile
com/bing/20191010.jpg?imageView2/1/w/960/h/540/interlace/1/q/100">
<h2 id="防火墙的结构和原理">防火墙的结构和原理</h2>
<blockquote>
防火墙技术是计算机网络中的一个概念,我们使用防火墙来保护我们的计算机的安全,帮助计算机
络在内网和外网中构建一道相对隔绝的保护屏障,是一种信息安全技术。
防火墙可由硬件或者软件实现。
</blockquote>
<h2 id="软件防火墙">软件防火墙</h2>
软件防火墙也称为个人防火墙，它是最常用的防火墙，通常作为计算机系
上的程序运行。
它是可定制的，允许用户控制其功能。
软件防火墙单独使用软件系统来完成防火墙功能，将软件部署在系统主机上，其安全性较硬
件防火墙差，同时占用系统资源，在一定程度上影响系统性能。与基于硬件的防火墙不同，软件
火墙只能保护安装它的系统。
我们的 pc 就会自带防火墙，我们可以选择打开或者关闭或者启动防火墙策略来保护我们的计算
的安全。
<h2 id="硬件防火墙">硬件防火墙</h2>
基于硬件的防火墙专门保护你的本地网络。它是一种可以购买的独立产品
通常用于宽带路由器。它通常比软件防火墙提供给用户更好的安全性，但是它的价格更高。
至于价格高，原因在于，软件防火墙只有包过滤的功能，硬件防火墙中可能还有除软
防火墙以外的其他功能，例如 CF（内容过滤）IDS（入侵侦测）IPS（入侵防护）以及 VPN
等等的功能。
硬件防火墙由各个不同的防火墙厂商开发生产，其中比较著名的防火墙厂商有：cisco,juniper,ch
ckpoint 等，现在国内也涌现大量的优秀防火墙厂商如：huawei，h3c, hillstone 等。
<h3 id="如何达到防火墙的过滤作用-">如何达到防火墙的过滤作用？</h3>
防火墙的目的就是允许或者阻止特定的网络包到达目的地。而为了实现这
目的，人们也设计了许多的方法:例如包过滤，应用层网关，电路层网关等，现
最为普及的就是包过滤方式。
<h3 id="如何设置包过滤的规则-">如何设置包过滤的规则？</h3>
一个网络包分为头部和数据包。防火墙会基于网络包的头部来对通信进行控制。如果是懂网络的
学会很容易理解这句话,我们看看网络包中的头部携带者哪些信息。
<img src="https://ld246.com/images/img-loading.svg" alt="image.png" data-src="https:
/b3logfile.com/file/2020/11/image-478ea046.png?imageView2/2/interlace/1/format/jpg"></
>
<img src="https://ld246.com/images/img-loading.svg" alt="image.png" data-src="https:
/b3logfile.com/file/2020/11/image-387e932a.png?imageView2/2/interlace/1/format/jpg"></
>
<img src="https://ld246.com/images/img-loading.svg" alt="image.png" data-src="https:
/b3logfile.com/file/2020/11/image-1cc06a48.png?imageView2/2/interlace/1/format/jpg"></
>
根据上面的图，大概可以知道防火墙可以根据 源地址，目的地址，端口，以及协议来
行允许或者阻止的操作
下图是防火墙工作的一个例子
<img src="https://ld246.com/images/img-loading.svg" alt="image.png" data-src="https:
/b3logfile.com/file/2020/11/image-3a10bd6f.png?imageView2/2/interlace/1/format/jpg"></
>
第一条 只写了接收方 IP 地址和端口以及动作是允许，代表着这条防火墙策略允许互联网的任意 i
和端口来访问 192.0.2.0/24
第二条 阻止 192.0.2.0/24 的 80 端口向任意 ip 发送请求 TCP 控制位的 SYN=1 和 ACK=0 代
着主动发起 TCP 连接，因为如果互联网的 ip 来访问 192.0.2.0/24 的 80 端口是需要建立 tcp 连接，
92.0.2.0/24 是需要进行回包的
第三条就是允许 192.0.2.0/24 的 80 端口向任意 ip 返回请求
第四条 防火墙策略是最后匹配到的，如果上面 3 条防火墙策略都没有匹配到，那么就拒绝请求<

p>
<h3 id="数据包在防火墙中的传递过程">数据包在防火墙中的传递过程</h3>
上面简单的介绍了包过滤的规则，下面来来了解下数据包的传递过程。整个数据包在防火墙的传会经过这么几个阶段

数据包抵达接口
匹配 connection 表项
ACL 检查
匹配地址转换
深度包检查
IP 头转换
抵达外部出口
三层路由表查找
二层 mac 表查找
发送数据包

一个简单的例子


<h4 id="数据包抵达接口">数据包抵达接口</h4>

数据包进入防火墙的物理接口
增加 input counters 的数值
检查是否异常流量，如流量过大

<h4 id="匹配connection项">匹配 connection 项</h4>

首先查找存在的 connection 项
如果数据包匹配存在的 connection，则跳过 ACL check 和 Match Xlate
如果数据包没有匹配 connection

TCP non-SYN 数据包将被抛弃并被系统日志记录
TCP SYN 或者 UDP 数据包则传给 ACL check

<h4 id="ACL检查">ACL 检查</h4>
这里就是防火墙的核心功能，匹配 ACL 也就是防火墙策略

数据包首先匹配 ACL 条目
匹配到，hitcount +1（hitcount 是防火墙策略的命中数）
Denied（拒绝）的策略将被丢弃和记录日志

<h4 id="匹配地址转换">匹配地址转换</h4>

首先数据包必须匹配转换规则
检查数据包的目的端口进行快速路由查找
转换规则可以是 NAT control 或者是 no NAT control
NAT 配置定义何时执行转换规则
当转换规则匹配成功，则建立 connection

<h4 id="深度包检查">深度包检查</h4>

Inspections 用于检查协议的一致性
(可选)自定义 AIC 检查
NAT 保障报文里的地址和 ip 头地址一致 对应用层数据包的补充检查
(可选)数据包传给内容安全和控制(CSC)模块

<h4 id="IP头转换">IP 头转换</h4>

对 IP 报头的 IP 地址转换
如果 PAT 执行则转换端口
更新校验结果
(可选)执行完上面的步骤，数据包传递给 IPS(AIP)模块

<h4 id="抵达外部出口">抵达外部出口</h4>

数据包转发到出接口位置(尚未从设备转发出去)
出接口是由转换规则确定的
如果转换规则没有规定出接口(例如:原始输出数据包)则通过全 局路由查找来决定数据包的出接口

<h4 id="三层路由表查找">三层路由表查找</h4>

一旦数据包到达出接口，接着就执行接口路由查找
路由表只提供合适的出接口
注意:转换规则可以将数据包转发到出接口,即使路由表中指向的不 同的出接口

<h4 id="二层mac表查找">二层 mac 表查找</h4>

一旦匹配三层路由表和下一跳则执行二层解析
重写二层的 MAC 报头
如果二层解析失败将不被日志记录
Show arp 无法显示三层下一跳
当没有收到 arp 响应使用 Debug arp 可以显示出来

<h4 id="发送数据包">发送数据包</h4>

数据包传递结束
端口上的 interface counters 将会增加

<h3 id="如何使用防火墙-">如何使用防火墙？</h3>
防火墙的品牌是非常多的，而各个防火墙厂商开发的防火墙，cli 命令差异极大，所以需要获取方文档进行学习。
我也会继续在博客和 github 上发布各类防火墙的使用方法和命令参考。