□□linux防御DDOS攻击方案

□□用
squid是利用端口映射的功能，可以将80端口转换一下，其实一般的DDOS攻击可以修改/proc/sys/net/ipv4
/tcp_max_syn_backlog里的参数就行了，默认参数一般都很小，设为8000以上，一般的DDOS攻击就可以解决了。如果上升到
timeout阶段，可以将/proc/sys/net/ipv4/tcp_fin_timeout设小点。

□□
大家都在讨论DDOS，个人认为目前没有真正解决的方法，只是在缓冲和防御能力上的扩充，跟

□□黑客

□□玩一个心理战术，看谁坚持到最后，网上也有很多做法，例如syncookies等，就是复杂点。

□□sysctl-wnet.ipv4.icmp_echo_ignore_all=1

□□echo1>/proc/sys/net/ipv4/tcp_syncookies

□□sysctl-wnet.ipv4.tcp_max_syn_backlog="2048"

□□sysctl-wnet.ipv4.tcp_synack_retries="3"

□□iptables-AINPUT-ieth0-ptcp--syn-jsyn-flood

□□#Limit12connectionspersecond(burstto24)

□□iptables-Asyn-flood-mlimit--limit12/s--limit-burst24-jRETURN

□□这个地方可以试着该该:

□□iptbales-AFORWARD-ptcp--syn-mlimit--limit1/s-jACCEPT

□□虚拟主机服务商在运营过程中可能会受到

□□黑客

□□攻击，常见的

□□攻击

□□方式有SYN，DDOS等。

□□通过更换IP，查找被

□□攻击

□□的站点可能避开

□□攻击

□□，但是中断服务的时间比较长。比较彻底

□□的解决方法是添置硬件

□□防火墙

□□。不过，硬件

□□防火墙

□□价格比较昂贵。可以考虑利用Linux

□□系统本身提供的

□□防火墙

□□功能来防御。

□□1.抵御SYN

□□SYN攻击是利用TCP/IP协议3次握手的原理，发送大量的建立连接的

□□网络

□□包，但不实际

□□建立连接，最终导致被

□□攻击

□□服务器的

□□网络

□□队列被占满，无法被正常用户访问。

□□Linux内核提供了若干SYN相关的配置，用命令：

□□sysctl-a|grepsyn

□□看到：

□□net.ipv4.tcp_max_syn_backlog=1024

□□net.ipv4.tcp_syncookies=0

□□net.ipv4.tcp_synack_retries=5

□□net.ipv4.tcp_syn_retries=5

□□
tcp_max_syn_backlog是SYN队列的长度，tcp_syncookies是一个开关，是否打开SYNCookie

□□功能，该功能可以防止部分SYN攻击。tcp_synack_retries和tcp_syn_retries定义SYN

□□的重试次数。

□□加大SYN队列长度可以容纳更多等待连接的

□□网络

□□连接数，打开SYNCookie功能可以阻止部分

□□SYN攻击，降低重试次数也有一定效果。

□□调整上述设置的方法是：

□□增加SYN队列长度到2048：

□□sysctl-wnet.ipv4.tcp_max_syn_backlog=2048

□□打开SYNCOOKIE功能：

□□sysctl-wnet.ipv4.tcp_syncookies=1

□□降低重试次数：

□□sysctl-wnet.ipv4.tcp_synack_retries=3

□□sysctl-wnet.ipv4.tcp_syn_retries=3

□□为了系统重启动时保持上述配置，可将上述命令加入到/etc/rc.d/rc.local文件中。

□□2.抵御DDOS

□□DDOS，分布式拒绝访问

□□攻击

□□，是指

□□黑客

□□组织来自不同来源的许多主机，向常见的端口，如80，

□□
25等发送大量连接，但这些客户端只建立连接，不是正常访问。由于一般Apache配置的接受连接

□□数有限(通常为256)，这些“假”访问会把Apache占满，正常访问无法进行。

□□Linux提供了叫ipchains的

□□防火墙

□□工具，可以屏蔽来自特定IP或IP地址段的对特定端口的连接。

□□使用ipchains抵御DDOS，就是首先通过netstat命令发现

□□攻击

□□来源地址，然后用ipchains命令阻断

□□攻击

□□。发现一个阻断一个。

□□***打开ipchains功能

□□首先查看ipchains服务是否设为自动启动：

□□chkconfig--listipchains

□□输出一般为：

□□ipchains0ff1ff2n3n4n5n6ff

□□如果345列为on，说明ipchains服务已经设为自动启动

□□如果没有，可以用命令：

□□chkconfig--addipchains

□□将ipchains服务设为自动启动

□□

其次，察看ipchains配置文件/etc/sysconfig/ipchains是否存在。如果这一文件不存在，ipchains

□□即使设为自动启动，也不会生效。缺省的ipchains配置文件内容如下：

□□

#Firewallconfigurationwrittenbylokkit#Manualcustomizationofthisfileisnotrecommended.#Note:if up-postwillpunchthecurrentnameserversthroughthe#firewall;suchentrieswill*not*belistedhere.:inputACCEPT:forwardACCEPTutputACCEPT-Ainput-s0/0-d0/0-ilo-jACCEPT#allowhttp,ftp,smtp,ssh,domainviatcp;domainviaudp-Ainput-ptcp-s0/0-d0/0pop3-y-jACCEPT-Ainput-ptcp-s0/0-d0/0http-y-jACCEPT-Ainput-ptcp-s0/0-d0/0https-y-jACCEPT-Ainput-ptcp-s0/0-d0/0ftp-y-jACCEPT-Ainput-ptcp-s0/0-d0/0smtp-y-jACCEPT-Ainput-ptcp-s0/0-d0/0ssh-y-jACCEPT-Ainput-ptcp-s0/0-d0/0domain-y-jACCEPT-Ainput-pudp-s0/0-d0/0domain-jACCEPT#denyicmppacket#-Ainput-picmp-s0/0-d0/0-jDENY#defaultrules-Ainput-ptcp-s0/0-d0/00:1023-y-jREJECT-Ainput-ptcp-s0/0-d0/02049-y-jREJECT-Ainput-pudp-s0/0-d0/00:1023-jREJECT-Ainput-pudp-s0/0-d0/02049-jREJECT-Ainput-ptcp-s0/0-d0/06000:6009-y-jREJECT-Ainput-ptcp-s0/0-d0/07100-y-jREJECT

□□

如果/etc/sysconfig/ipchains文件不存在，可以用上述内容创建之。创建之后，启动ipchains服务：

□□/etc/init.d/ipchainsstart

□□***用netstat命令发现

□□攻击

□□来源

□□假如说

□□黑客

□□攻击的是Web80端口，察看连接80端口的客户端IP和端口，命令如下：

□□netstat-an-ttcp|grep":80"|grepESTABLISHED|awk'{printf"%s%s\n",$5,$6}'|sort

□□输出：

□□161.2.8.9:123FIN_WAIT2

□□161.2.8.9:124FIN_WAIT2

□□61.233.85.253:23656FIN_WAIT2

□□...

□□第一栏是客户机IP和端口，第二栏是连接状态

□□如果来自同一IP的连接很多(超过50个)，而且都是连续端口，就很可能是

□□攻击

□□。

□□http://bbs.92bbs.net/read-tid-31313.html

□□如果只希望察看建立的连接，用命令：

□□netstat-an-ttcp|grep":80"|grepESTABLISHED|awk'{printf"%s%s\n",$5,$6}'|sort

□□***用ipchains阻断

□□攻击

□□来源

□□用ipchains阻断

□□攻击

□□来源，有两种方法。一种是加入到/etc/sysconfig/ipchains里，然后重启动

□□ipchains服务。另一种是直接用ipchains命令加。屏蔽之后，可能还需要重新启动被

□□攻击

□□的服务，

□□是已经建立的

□□攻击

□□连接失效

□□*加入/etc/sysconfig/ipchains

□□
假定要阻止的是218.202.8.151到80的连接，编辑/etc/sysconfig/ipchains文件，在utputACCEPT

□□行下面加入：

□□-Ainput-s218.202.8.151-d0/0http-y-jREJECT

□□保存修改，重新启动ipchains：

□□/etc/init.d/ipchainsrestart

□□如果要阻止的是218.202.8的整个网段，加入：

□□-Ainput-s218.202.8.0/255.255.255.0-d0/0http-y-jREJECT

□□*直接用命令行

□□
加入/etc/sysconfig/ipchains文件并重起ipchains的方法，比较慢，而且在ipchains重起的瞬间，

□□可能会有部分连接钻进来。最方便的方法是直接用ipchains命令。

□□假定要阻止的是218.202.8.151到80的连接，命令：

□□ipchains-Iinput1-ptcp-s218.202.8.151-d0/0http-y-jREJECT

□□如果要阻止的是218.202.8的整个网段，命令：

□□ipchains-Iinput1-ptcp-s218.202.8.0/255.255.255.0-d0/0http-y-jREJECT

□□其中，-I的意思是插入，input是规则连，1是指加入到第一个。

□□您可以编辑一个shell脚本，更方便地做这件事，命令：

□□viblockit

□□内容：

□□#!/bin/sh

□□if[!-z"$1"];then

□□echo"Blocking:$1"

□□ipchains-Iinput1-ptcp-s"$1"-d0/0http-y-jREJECT

□□else

□□echo"whichiptoblock?"

□□fi

□□保存，然后：

□□chmod700blockit

□□使用方法：

□□./blockit218.202.8.151

□□./blockit218.202.8.0/255.255.255.0

□□上述命令行方法所建立的规则，在重起之后会失效，您可以用ipchains-save命令打印规则：

□□ipchains-save

□□输出：

□□:inputACCEPT:forwardACCEPTutputACCEPTSaving`input'.-Ainput-s0.0.0.0/0.0.0.0-d0.0.0.0/0.0.0.0-ilo-jACCEPT-Ainput-s0.0.0.0/0.0.0.0-d0.0.0.0/0.0.0.0110:110-p6-jACCEPT-y-Ainput-s0.0.0.0/0.0.0.0-d0.0.0.0/0.0.0.080:80-p6-jACCEPT-y-Ainput-s0.0.0.0/0.0.0.0-d0.0.0.0/0.0.0.022:22-p6-jACCEPT-y-Ainput-s0.0.0.0/0.0.0.0-d0.0.0.0/0.0.0.088:88-p6-jACCEPT-y-Ainput-s0.0.0.0/0.0.0.0-d0.0.0.0/0.0.0.089:89-p6-jACCEPT-y-Ainput-s0.0.0.0/0.0.0.0-d0.0.0.0/0.0.0.090:90-p6-jACCEPT-y-Ainput-s0.0.0.0/0.0.0.0-d0.0.0.0/0.0.0.091:91-p6-jACCEPT-y-Ainput-s0.0.0.0/0.0.0.0-d0.0.0.0/0.0.0.08180:8180-p6-jACCEPT-y-Ainput-s0.0.0.0/0.0.0.0-d0.0.0.0/0.0.0.0443:443-p6-jACCEPT-y-Ainput-s0.0.0.0/0.0.0.0-d0.0.0.0/0.0.0.021:21-p6-jACCEPT-y-Ainput-s0.0.0.0/0.0.0.0-d0.0.0.0/0.0.0.025:25-p6-jACCEPT-y-Ainput-s0.0.0.0/0.0.0.0-d0.0.0.0/0.0.0.022:22-p6-jACCEPT-y-Ainput-s0.0.0.0/0.0.0.0-d0.0.0.0/0.0.0.053:53-p6-jACCEPT-y-Ainput-s0.0.0.0/0.0.0.0-d0.0.0.0/0.0.0.09095:9095-p6-jACCEPT-y-Ainput-s0.0.0.0/0.0.0.0-d0.0.0.0/0.0.0.08007:8007-p6-jACCEPT-y-Ainput-s0.0.0.0/0.0.0.0-d0.0.0.0/0.0.0.053:53-p17-jACCEPT-Ainput-s0.0.0.0/0.0.0.0-d0.0.0.0/0.0.0.00:1023-p6-jREJECT-y-Ainput-s0.0.0.0/0.0.0.0-d0.0.0.0/0.0.0.02049:2049-p6-jREJECT-y-Ainput-s0.0.0.0/0.0.0.0-d0.0.0.0/0.0.0.00:1023-p17-jREJECT-Ainput-s0.0.0.0/0.0.0.0-d0.0.0.0/0.0.0.02049:2049-p17-jREJECT-Ainput-s0.0.0.0/0.0.0.0-d0.0.0.0/0.0.0.06000:6009-p6-jREJECT-y-Ainput-s0.0.0.0/0.0.0.0-d0.0.0.0/0.0.0.07100:7100-p6-jREJECT-yhttp://bbs.92bbs.net/read-tid-31313.html

□□您需要把其中的"Saving`input'."去掉，然后把其他内容保存到/etc/sysconfig/ipchains文件，

□□这样，下次重起之后，建立的规则能够重新生效。

□□3.如果使用iptables

□□RH8.0以上开始启用iptables替代ipchains，两者非常类似，也有差别的地方。

□□*启用iptables

□□如果/etc/sysconfig/下没有iptables文件，可以创建：

□□
#Firewallconfigurationwrittenbylokkit#Manualcustomizationofthisfileisnotrecommended.#Note:ifup-postwillpunchthecurrentnameserversthroughthe#firewall;suchentrieswill*not*belistedhere.*filter:INPUTACCEPT[0:0]:FORWARDACCEPT[0:0]:OUTPUTACCEPT[0:0]:RH-Lokkit-0-50-INPUT-[0:0]-AINPUT-jRH-Lokkit-0-50-INPUT-ARH-Lokkit-0-50-INPUT-ilo-jACCEPT-ARH-Lokkit-0-50-INPUT-ptcp-mtcp--dportftp-jACCEPT-ARH-Lokkit-0-50-INPUT-ptcp-mtcp--dportssh-jACCEPT-ARH-Lokkit-0-50-INPUT-ptcp-mtcp--dporthttp-jACCEPT-ARH-Lokkit-0-50-INPUT-ptcp-mtcp--dportsmtp-jACCEPT-ARH-Lokkit-0-50-INPUT-ptcp-mtcp--dportpop3-jACCEPT-ARH-Lokkit-0-50-INPUT-ptcp-mtcp--dportmysql-jACCEPT-ARH-Lokkit-0-50-INPUT-ptcp-mtcp--dport2001-jACCEPT-ARH-Lokkit-0-50-INPUT-ptcp-mtcp--dportdomain-jACCEPT-ARH-Lokkit-0-50-INPUT-pudp-mudp--dportdomain-jACCEPT-ARH-Lokkit-0-50-INPUT-ptcp-mtcp--dport0:1023--syn-jREJECT-ARH-Lokkit-0-50-INPUT-ptcp-mtcp--dport2049--syn-jREJECT-ARH-Lokkit-0-50-INPUT-pudp-mudp--dport0:1023-jREJECT-ARH-Lokkit-0-50-INPUT-pudp-mudp--dport2049-jREJECT-ARH-Lokkit-0-50-INPUT-ptcp-mtcp--dport6000:6009--syn-jREJECT-ARH-Lokkit-0-50-INPUT-ptcp-mtcp--dport7100--syn-jREJECTCOMMIT

□□以上配置允许了ftp,ssh,http,smtp,pop3,mysql,2001(Prim@HostingACA端口)，domain端口。

□□*启动iptables

□□/etc/init.d/iptablesstart

□□*设置iptables为自动启动

□□chkconfig--level2345iptableson

□□*用iptables屏蔽IP

□□iptables-IRH-Lokkit-0-50-INPUT1-ptcp-mtcp-s213.8.166.227--dport80--syn-jREJECT

□□注意到，和ipchains的区别是：

□□-I后面跟的规则名称的参数和ipchains不同，不是统一的input，而是在/etc/sysconfig/iptables里定义的那个

□□多了-mtcp

□□指定端口的参数是--dport80

□□多了--syn参数，可以自动检测sync攻击

□□使用iptables禁止ping：

□□-AINPUT-picmp-micmp--icmp-type8-mlimit--limit6/min--limit-burst2-jACCEPT-AINPUT-picmp-micmp--icmp-type8-jREJECT--reject-withicmp-port-unreachable

□□允许某ip连接

□□-IRH-Firewall-1-INPUT1-ptcp-mtcp-s192.168.0.51--syn-jACCEPT

□□注:具体的端口需要根据自己的

□□网络

□□来进行相应的修改。