Squid服务全攻略

内容简介

代理服务概述

Squid简介

Squid代理服务的安装

Squid代理服务的基本配置

访问控制应用实例

Squid常用命令

案例详解（三种代理的实现）

代理服务器简介

代理服务器是目前网络中常见的服务器之一，它可以提供文件缓存、复制和地址过滤等服务，充分利用有限的出口带宽，加快内部主机的访问速度，也可以解决多用户需要同时访问外网但公有IP地址不足的问题。同时可以作为一个防火墙，隔离内网与外网，并且能提供监控网络和记录传输信息的功能，加强局域网的安全性等。它的主要作用有以下几点。

1．共享网络

2．加快访问速度，节约通信带宽

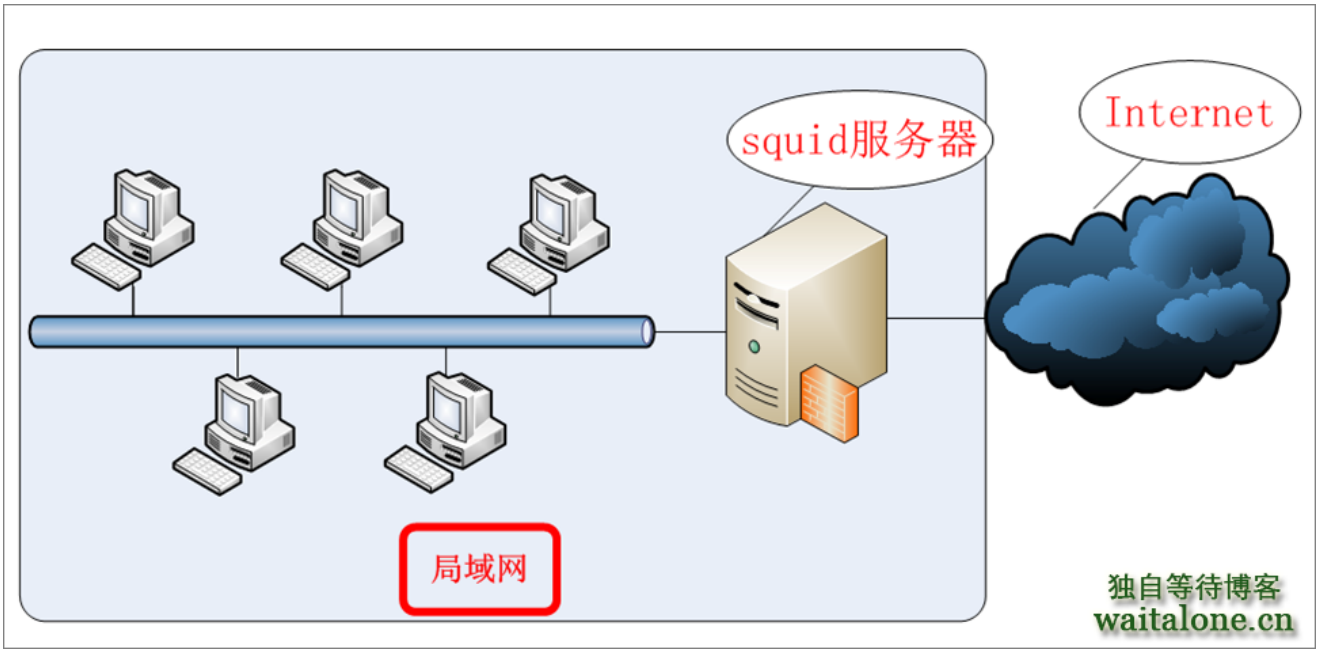
3．防止内部主机受到攻击

4．限制用户访问，完善网络管理

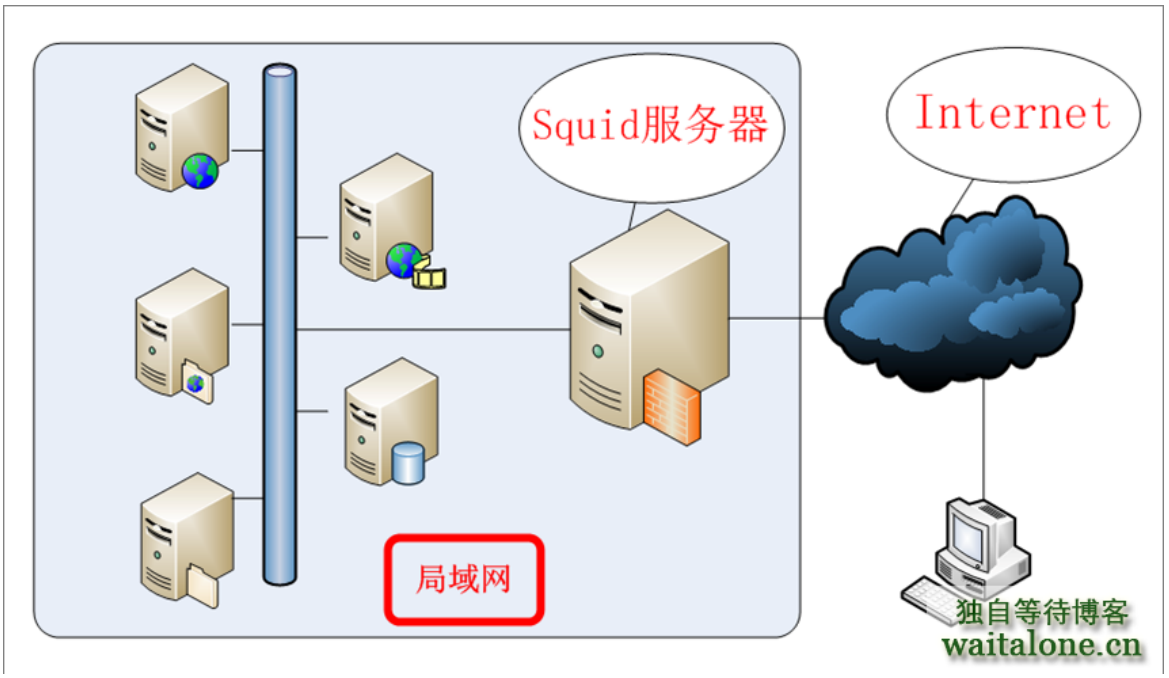
代理服务器的类型

标准代理服务器\透明代理服务器(图1)

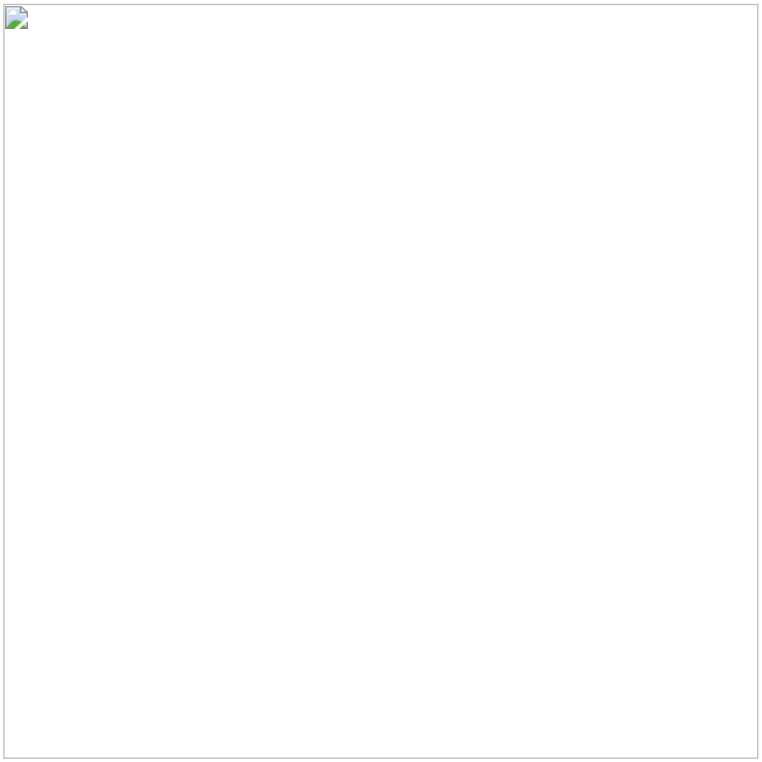
标准代理服务器\透明代理服务器(图1)



反向代理服务器（图2）



代理服务器的原理（图3）



① 客户端A向代理服务器提出访问Internet的请求。

② 代理服务器接受到请求后，首先与访问控制列表中的访问规则相对照，如果满足规则，则在缓存中查找是否存在需要的信息。

③ 如果缓存中存在客户端A需要的信息，则将信息传送给客户端。如果不存在，代理服务器就代替客户端向Internet上的主机请求指定的信息。

④ Internet上的主机将代理服务器的请求信息发送到代理服务器中，同时代理服务会将信息存入缓存中。

⑤ 代理服务器将Internet上主机的回应信息传送给客户端A。

⑥ 客户端B向代理服务器提出相同的请求。

⑦ 代理服务器也首先与访问控制列表中的访问规则相对照。

⑧ 如果满足规则，则将缓存中的信息传送给客户端B。

Squid简介

Squid是Linux和UNIX平台下最为流行的高性能免费应用层代理服务器，它具有权限管理灵活、性能高和效率快等特点。

Squid的另一个优越性在于它使用访问控制列表（ACL）和访问权限列表（ARL）进行权限管理和内容过滤。访问控制清单和访问权限清单通过阻止特定的网络连接来减少潜在的Internet非法连接，可以使用这些清单来确保内部网的主机无法访问有威胁的或不适宜的站点。

Squid代理服务的安装

检查系统是否已经安装了Squid服务

```
rpm -q squid
rpm -ivh /mnt/Server/squid-*.el5.i386.rpm
```

Squid代理服务的基本配置

```
Squid主配置文件是/etc/squid/squid.conf，最基本的设置如下。
http_port 3128 //设置监听的IP与端口号
cache_mem 64 MB //设置内存缓冲的大小
cache_dir ufs /var/spool/squid 2000 16 256 //设置硬盘缓冲大小
cache_effective_user squid //设置缓存的有效用户
cache_effective_group squid //设置缓存的有效用户组
dns_nameservers 192.168.0.254 //设置DNS服务器地址,一般可以不设置，默认使用服务器自己设置的dns
cache_access_log /var/log/squid/access.log //设置访问日志文件
cache_log /var/log/squid/cache.log //设置缓存日志文件
cache_store_log /var/log/squid/store.log //设置存储缓存对象的状态记录文件
visible_hostname 192.168.0.20 //设置squid主机名称
cache_mgr zxf_xxff@163.com //设置管理员邮箱
acl all src 0.0.0.0/0.0.0.0 //设置访问控制列表
http_access allow all //设置访问权限
```

访问控制

acl选项的格式如下。

acl列表名称 列表类型 [-i] 列表值

列表名称：用于区分Squid的各个访问控制列表，任何两个访问控制列表不能用相同的列表名。虽然列表名称可以随便定义，但为了避免以后不知道这条列表是干什么用的，应尽量使用有意义的名称，如badurl、clientip和work time等。

列表类型：是可被Squid识别的类别。Squid支持的控制类别很多，可以通过IP地址、主机名、MAC地址和用户/密码认证等识别用户，也可以通过域名、域后缀、文件类型、IP地址、端口和URL匹配等控制用户的访问，还可以使用时间区间对用户进行管理

-i选项：表示忽略列表值的大小写，否则Squid是区分大小写的。

列表值：针对不同的类型，列表值的内容是不同的。例如，对于类型为src或dst，列表值的内容是某台主机的IP地址或子网地址；对于类型为time，列表值的内容是时间；对于类型为srcdomain和dstdomain，列表值的内容是DNS域名。

访问控制

命令 说明

src 源IP地址（客户机IP地址）

dst 目标IP地址（服务器IP地址）

srcdomain 源名称（客户机所属的域）

dstdomain 目标名称（服务器所属的域）

url_regex URL规则表达式匹配

urlpath_regex: URL-path 略去协议和主机名的URL规则表达式匹配

proxy_auth 通过外部程序进行用户认证

maxconn 单一IP的最大连接数

time 时间段，语法为：[星期] [时间段]。

[星期]：可以使用这些关键字M（Monday星期一）、T（Tuesday星期二）、W（Wednesday星期三）、H（Thursday星期四）、F（Friday星期五）、A（Saturday星期六）和S（Sunday星期天）

[时间段]：可以表示为10:00-20:00

Squid会针对客户HTTP请求检查http_access规则，定义访问控制列表后，就使用http_access选项根据访问控制列表允许或禁止访问了。

该选项的基本格式为：

http_access [allow | deny] 访问控制列表名称

[allow | deny]：定义允许（allow）或禁止（deny）访问控制列表定义的内容。

访问控制列表名称：需要http_access控制的ACL名称。

访问控制应用实例

【例1】禁止IP地址为192.168.16.200的客户机上网。

```
acl badclientip1 src 192.168.16.200
http_access deny badclientip1
```

【例2】禁止192.168.1.0这个子网里所有的客户机上网。

```
acl badclientnet1 src 192.168.1.0/255.255.255.0
http_access deny badclientnet1
```

【例3】禁止用户访问IP地址为210.21.118.68的网站。

```
acl badsrvip1 dst 210.21.118.68
http_access deny badsrvip1
```

【例4】禁止用户访问域名为www.163.com的网站。

```
acl baddomain1 dstdomain -i www.163.com
http_access deny baddomain1
```

【例5】禁止用户访问域名包含有163.com的网站。

```
acl badurl1 url_regex -i 163.com
http_access deny badurl1
```

【例6】禁止用户访问域名包含有sex关键字的URL。

```
acl badurl2 url_regex -i sex
http_access deny badurl2
```

【例7】限制IP地址为192.168.16.200的客户机并发最大连接数为5。

```
acl clientip1 src 192.168.16.200
acl conn5 maxconn 5
http_access deny client1 conn1
```

【例8】禁止192.168.2.0这个子网里所有的客户机在周一到周五的9:00到18:00上网。

```
acl clientnet1 src 192.168.2.0/255.255.255.0
acl worktime time MTWHF 9:00-18:00
http_access deny clientnet1 worktime
```

【例9】禁止客户机下载*.mp3、*.exe、*.zip和*.rar类型的文件。

```
acl badfile1 urlpath_regex -i \.mp3$ \.exe$ \.zip$ \.rar$
http_access deny badfile1
```

【例10】禁止QQ通过Squid代理上网。

```
acl qq url_regex -i tencent.com
http_access deny qq
```

Squid代理服务常用命令

```
1、初始化squid 缓存目录
/usr/sbin/squid -zX
/usr/sbin/squid -NCd1
2、启动代理服务
```

```
/etc/init.d/squid start
3、停止代理服务
/etc/init.d/squid stop
/usr/sbin/squid -k shutdown
4、重新启动代理服务
/etc/init.d/squid restart
5、重新载入配置文件
/etc/rc.d/init.d/squid reload
/usr/sbin/squid -k reconfig
6、自动启动代理服务
执行”ntsysv”命令启动服务配置程序
7、通过crontab每小时截断/轮循日志 59 * * * * /usr/sbin/squid -k rotate
service squid start/stop/restart
```

一般代理的实现

配置Squid

开启内核路由功能（一般代理好像不用开启）

echo 1> /proc/sys/net/ipv4/ip_forward

vim /etc/sysctl.conf >>>>>>> net.ipv4.ip_forward = 1

修改配置文件

创建缓存目录

启动服务测试

透明代理的实现

配置Squid

配置iptables

关键点：

1、设置transparert(不在像以前那么麻烦)

2、IPTABLES防火墙设置

iptables在这里所起的作用是端口重定向，执行以下命令，将所有由eth0接口进入的Web服务80端口的请求直接转发到3128端口，由Squid处理。

iptables -t nat -A PREROUTING -i eth0 -p tcp –dport 80 -j REDIRECT –to-ports 3128

iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE

反向代理的实现

配置Squid

http_port 80 transparent

cache_peer 192.168.182.130 parent 80 0 no-query name=a

cache_peer_domain a www.lamp.cn

cache_peer_access a allow all

cache_peer选项

格式

```
cache_peer hostname type proxy-port icp-port options
type: parent sibling multicast
proxy-port: 代理服务的监听端口
icp-port： ICP服务的监听端口（关闭的时候用0）
options：
weight=n优先级，数字越大，优先级越高
no-query 禁止ICP协议（原始主机用）
Originserver 该服务器是WEB服务的原始主机
Name=XXX用来识别同一台主机上，多个不同的端口(主要在
cache_peer_access用)
Max-conn=n 反向代理服务器到WEB服务器的最大连接数
Connect-timeout=n 超时设置
```

案例详解

【案例1】使用Squid建立一个基本的代理服务，并根据以下要求配置。

（1）设置Squid监听的端口号为8888。

（2）设置内存缓冲的大小128MB。

（3）设置硬盘缓冲的大小最大为4096MB，硬盘缓冲存放的目录下的第一级子目录的数目是16，第二级子目录的数目是254。

（4）设置管理员的E-mail地址为root@example.com。

（5）设置访问控制列表为允许所有客户机访问。

（6）禁止客户机下载*.mp3、*.exe、*.zip和*.rar类型的文件。

配置文件设置如下：

http_port 8888

cache_mem 128 MB

cache_dir ufs /var/spool/squid 4096 16 256

cache_mgr root@example.com

http_access allow all

acl badfiles urlpath_regex -i \.mp3$ \.exe$ \.zip$ \.rar$

http_access deny badfiles

visible_hostname squid server

access_log /var/log/squid/access.log squid

cache_log /var/log/squid/cache.log

cache_store_log /var/log/squid/store.log

其它的为默认选项

#squid -zX

#du -sh /var/spool/squid/ (查看缓存文件夹的大小，以便后面比较)

#service squid start

配置客户端

(只要是与服务器的IP在一个网段就行，可以不用设置网关)

测试结果

tail /var/log/squid/access.log

cache_log /var/log/squid/cache.log

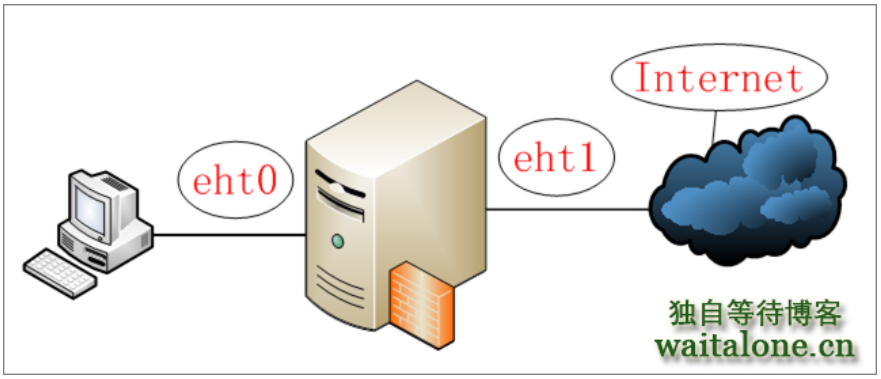
tail /var/log/squid/store.log

如果测试下载文件的权限，可以自己建立个网站进行测试!

注：本人没有开启内核的路由功能，同样的能实现。

/etc/sysctl.conf net.ipv4.ip_forward = 0

【案例2】配置一个简单的透明代理（图4）



配置文件设置如下：

http_port 8888 transparent

cache_mem 128 MB

cache_dir ufs /var/spool/squid 4096 16 256

cache_mgr root@example.com

http_access allow all

关于文件类型的限制我们这里取消了

visible_hostname squid server

access_log /var/log/squid/access.log squid

cache_log /var/log/squid/cache.log

cache_store_log /var/log/squid/store.log

#service squid stop

#rm -fr /var/spool/squid/*

#squid -zX

#service squid start

配置防火墙(如果防火墙已经设置过其它的规则的话，最好全部清空，然后用下面的两个)

#iptables -F

#iptables -t nat - F

上面两个命令是清空规则

#iptables -t nat -A PREROUTING -i eth0 -p tcp –dport 80 -j REDIRECT –to-ports 8888

#iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE

第一个命令是开启端口的转发功能

第二个命令是开启NAT功能

#service iptables save

#service iptables start

编辑/etc/sysctl.conf

把net.ipv4.ip_forward = 0改成1

配置客户配置

设置IP并指定网关（LINUX与XP连接的网卡的IP）

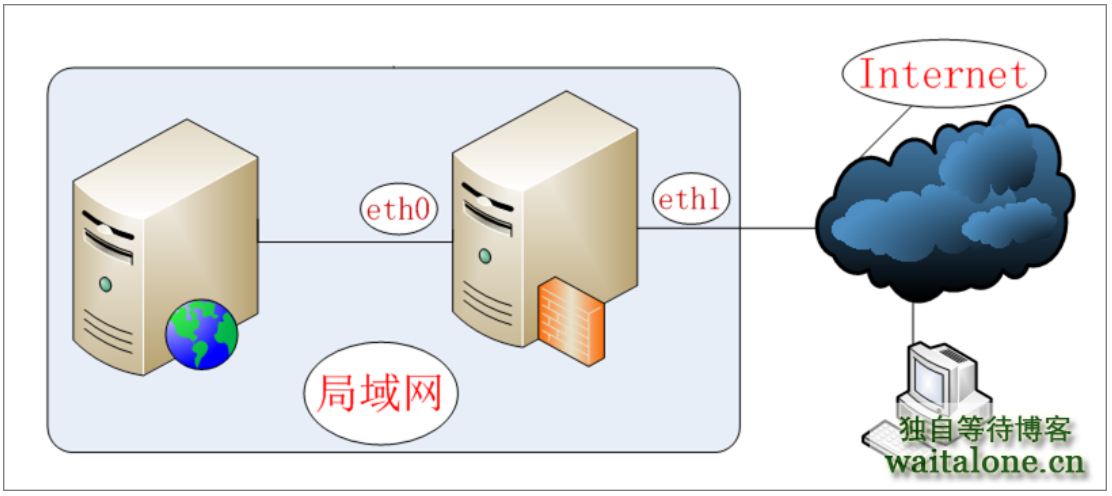
相应的DSN地址，必需是能用在互联网上能用的

浏览网页，然后进行测试!

也可以用下面的网页直接进行测试！！！

http://ipid.shat.net/

【案例3】配置一个简单的反向代理（图5）



反向代理(在透明代理的配置文件基础上做实验，这里要清空所有的防火墙规则)

编辑配置文件

http_port 80 transparent （把SQUID监听的端口设置成80，为了不让访问者在访问网站的时候输入端口）

cache_peer 10.0.0.4 parent 80 0 no-query originserver name=web1

cache_peer_domain web1 www.squidtest.com

注：上面二行的主要意图是

从客户端过来的请求，如果是 www.squidtest.com，则 Squid 向 web1 10.0.0.4的端口 80发送请求；

cache_peer_access web1 allow all

这一行的意思是设置访问权限，允许所有外部客户端访问web1

其它的配置都不变（在透明代理的基础上）

#service squid stop

#rm -fr /var/spool/squid/*

#squid -zX

#service squid start

在服务器上（/etc/hosts）配置一下域名对应的IP

10.0.0.4 www.justtest.com （10.0.0.4这个是我局域网中提供服务的主机）

这一步，在很多教程上都没有，不知道是不是一定需要，我在实际操作中，必须要设置，否则在客户端浏览网站的时候会很慢，而且网站显示的也不正常！

这一步仅供大家参考！

在客户端设置

在微软的系统中设置下面的文件

C:\WINDOWS\system32\drivers\etc\hosts

在LINUX或UNIX系统中，设置/etc/hosts

192.168.1.4 www.justtest.com（192.168.1.4这个是Squid服务器的连接外网的IP）

增加相应的域名和IP地址（如果在实际应用中，会由DNS服务提供商提供）

然后进行测试！

如果说，内部的网络有相应的DNS服务器的话，大家在squid的服务器中可以设置/etc/reslov.conf

★★★★★★★★★★★★★★★★★★视频观看地址★★★★★★★★★★★★★★★★★★

http://www.boobooke.com/v/bbk3736

http://www.boobooke.com/v/bbk3737

http://www.boobooke.com/v/bbk3738

http://www.boobooke.com/v/bbk3739

原文地址：http://www.opsers.org/server/chapter-viii-squid-service-raiders.html