# 配置普通代理

## 安装squid

查是否安装了squid

rpm –qa squid

安装

yum –y intall squid\*

是否启动

natstat –tunpl |grep:3128

psTree | grep squid

目录下的文件个数统计

tree 00

## 普通代理实现

### 局域网内部用户设置

ip 192.168.10.2 子网掩码 255.255.255.0

网关 192.168.10.1 网卡类型eth0

在浏览器中设置代理

### squid服务器设置

ip 192.168.10.1 子网掩码 255.255.255.0

网关 192.168.10.1 网卡类型eth0

ip 200.168.10.1 子网掩码 255.255.255.0

网卡类型eth1

1)修改squid配置文件

cd /etc/squid/

vi squid.config

http\_port 192.168.10.0/24

visible\_hostname 192.168.10.1

acl innet src 192.168.10.0/24

acl all src 0.0.0.0/0.0.0.0

http\_access allow innet

http\_access deny all

2)启动squid 服务 service squid start

## 常用的acl列表类型

|  |  |
| --- | --- |
| src | 源ip |
| dst | 目的ip |
| port | 端口 |
| srcdomain | 源域名 |
| dstdomain | 目的域名 |
| time | 时间 |
| maxconn | 最大连接 |
| url\_regex | url正则过滤 |
| urlpath\_regex | urlpath正则过滤 |

## ACl列表定义示例

### 定义acl

acl LAN1 src 192.168.1.0/24

acl PC1 stc 192.168.1.66/32

acl BLK\_Domain dstdomain .qq.com .kaixin001.com

acl Work\_Hours time MTWHF 08:30-17:30

acl Max20\_Conn maxconn 20

acl Blk\_URL url\_regex –I ^rtsp://^mms://

acl Blk\_Words urlpath\_regex –i sex adult

acl RealFile urlpath\_regex –I \.rmvb$ \.rm$

### 根据已经定义的acl列表进行访问控制

http\_access deny LAN1 Blk\_URL

http\_access deny L AN1 B lk\_Words

http\_access deny PC1 RealFile

htttp\_access deny PC1 Max20\_Conn

http\_access allow LAN1 Work\_Hours

# 配置squid透明代理

## 实现透明代理

前提：

1. 客户机的Web访问数据要能经过防火墙
2. 代理服务器构建在网关主机中

配置要求：

1. 代理服务程序能够支持透明代理
2. 配置iptables将客户机的Web请求转发到squid代理窗口

### 局域网内部用户设置

ip 192.168.10.2 子网掩码 255.255.255.0

网关 192.168.10.1 网卡类型eth0

### squid服务器设置

ip 192.168.10.1 子网掩码 255.255.255.0

网关 192.168.10.1 网卡类型eth0

ip 200.168.10.1 子网掩码 255.255.255.0

网卡类型eth1

1)修改squid配置文件

cd /etc/squid/

vi squid.config

http\_port 192.168.10.0/24 transparent

visible\_hostname 192.168.10.1

acl innet src 192.168.10.0/24

acl all src 0.0.0.0/0.0.0.0

http\_access allow innet

http\_access deny all

2)重新加载配置文件: squid –k reconfig

3)添加iptable规则，将内部请求转发到3128端口上

iptables -t nat -A PREROUTING -i etho -s 192.168.10.0/24 -p -tcp --port 80 –j REDIRECT --to 3128

# 配置squid反向代理

## 实现反向代理

### internet中的客户机

ip ip 200.168.10.2 子网掩码 255.255.255.0

网卡类型eth0

### squid服务器设置

ip 192.168.10.1 子网掩码 255.255.255.0

网卡类型eth1

ip 200.168.10.1 子网掩码 255.255.255.0

网卡类型eth0

1)修改squid配置文件

cd /etc/squid/

vi squid.config

http\_port 200.168.10.1:80 vhost

visible\_hostname 200.168.10.1

acl all src 0.0.0.0/0.0.0.0

http\_access allow all

cache\_peer 192.168.10.2 parent 80 0 origubserber weight=1 max-conn=30

cache\_peer 192.168.10.3 parent 80 0 origubserber weight=1 max-conn=30

cache\_peer 192.168.10.4 parent 80 0 origubserber weight=1 max-conn=30

cache\_peer 192.168.10.5 parent 80 0 origubserber weight=1 max-conn=8

2)重新加载配置文件: squid –k reconfig

## 加速

移动文件

rsnc -a –e ssh myweb/ 192.168.10.2:/var/www/html/

看一下squid缓存池

cd /var/spool/squid

tree 00

cd 00

stirngs 000007 !head

## 虚拟主机实现

修改webserver的配置文件

vi /etc/httpd/conf/httpd.config

1)修改squid配置文件

cd /etc/squid/

vi squid.config

http\_port 200.168.10.1:80 vhost

visible\_hostname 200.168.10.1

acl all src 0.0.0.0/0.0.0.0

http\_access allow all

cache\_peer 192.168.10.2 parent 80 0 originserver name=a

cache\_peer 192.168.10.2 parent 80 0 originserver name=b

cache\_peer\_domain a [www.lamp.com](http://www.lamp.com)

cache\_peer\_domain b [www.web.com](http://www.web.com)

cache\_peer\_access a allow all

cache\_peer\_access b allow all

# Mysql 主从复制与分区技术

## Mysql用户授权

## Mysql bin-log日志

## Mysql主从复制

## Mysql分区技术