技能展示

- 了解代理服务的常见类型
- 学会构建传统代理、透明代理服务
- 学会配置Squid的访问控制策略

重点

- squid工作原理
- 搭建传统代理及透明代理
- 管理表中的数据记录
- squid访问控制acl操作

难点

- 透明代理搭建
- squid访问控制acl操作

一、代理服务器简介

1.1.什么是代理服务器

代理服务器(Proxy Server)的功能是代理网络用户去取得网络信息，包括网页、电子邮件、多媒体文件和其它网络应用程序等。形象地说，它是网络信息的中转站，是个人网络和Internet服务商之间的中间代理机构，负责转发合法的网络信息，对转发进行控制和登记。

代理服务器作为连接Internet与Intranet的桥梁，在实际应用中发挥着极其重要的作用，它可用于多个目的，最基本的功能是连接，此外还包括安全性、缓存、内容过滤、访问控制管理等功能。更重要的是，代理服务器是Internet链路级网关所提供的一种重要的安全功能，它的工作主要在开放系统互联（OSI）模型的会话层。

1.2.web代理服务器

web代理服务器(通常所说的代理服务器)是介于浏览器和Web服务器之间的一台服务器,当你通过代理服务器上网浏览时，浏览器不是直接到Web服务器去取回网页而是向代理服务器发出请求，由代理服务器来取回浏览器所需要的信息并传送给你的浏览器。 大部分代理服务器都具有缓存Cache的功能，它有很大的存储空间，它不断将新取得数据储存到它本机的存储器上，如果浏览器所请求的数据在它本机的存储器上已经存在而且是最新的，那么它就不重新从Web服务器取数据，而直接将存储器上的数据传送给用户的浏览器，这样就能显著提高浏览速度和效率。

1.3代理服务器作用优点

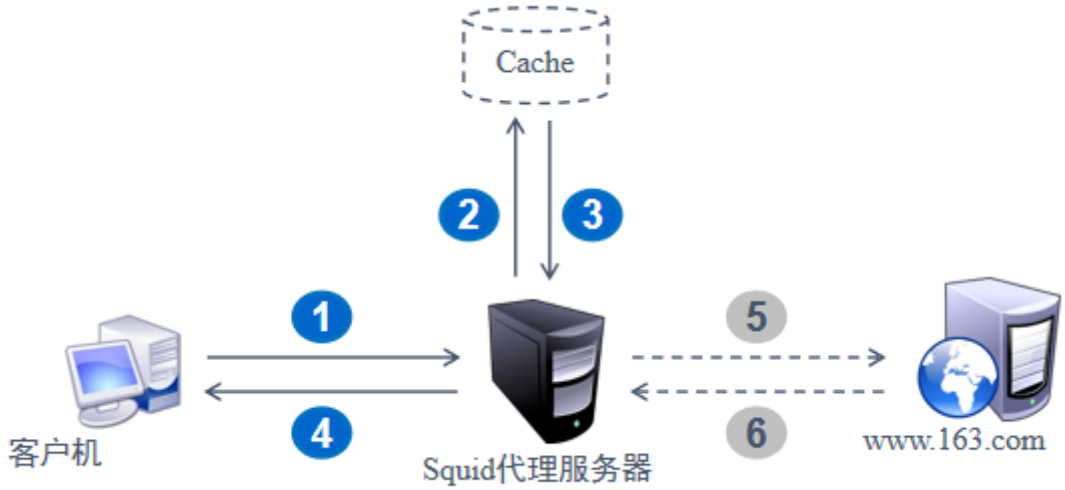
- 通过缓存的方式为用户提供Web访问加速
- 对用户的Web访问进行过滤控制

1.4.squid简介

squid作为应用层代理服务软件，主要提供缓存加速和应用层过滤控制的功能。squid接受来自人们需要下载的目标（object）的请求并适当的处理这些请求。也就是说，如果一个人想下载一web界面，他请求squid为他取得这个页面。squid随之连接到远程服务器并向这个页面发出请求。然后，squid显式地聚集数据到客户端机器，而且同时复制一份。当下一次有人需要同一页面时， squid可以简单的从磁盘中读到它，那样数据会立即传输到客户机上。

1.5.squid工作机制

代理服务器（Proxy Server）是个人网络和Internet服务商之间的中间代理机构，负责转发合法的网络信息，对转发进行控制和登记。其最基本的功能就是连接，此外还包括安全性、缓存，内容过滤，访问控制管理等功能。当客户机通过代理请求Web页面时，执行的代理服务器会先检查自己的缓存，当缓存中有客户机需要访问的页面，则直接将缓存服务器中的页面内容反馈给客户机；如果缓存中没有客户机需要访问的页面，则由代理服务器想Internet发送访问请求，当获得返回的Web页面以后，将页面数据保存到缓存中并发送给客户机。



1.6.代理的基本类型

根据实现的方式不同，代理服务可以分为传统代理和透明代理两种常见的代理服务。

1、**传统代理：**普通代理服务，必须在浏览器、QQ聊天工具，下载工具等程序中手动设置代理服务器的地址和端口，然后才能使用代理服务来访问网络，对于网页浏览器，访问网站时的域名解析请求也会发送给指定的代理服务器。

2、**透明代理：**提供与传统代理相同的功能和服务，其区别在于客户机不需要指定代理服务器的地址和端口，而是通过默认路由、防火墙策略将Web访问重定向，实际上仍然交给代理服务器来处理。重定向的过程对客户机“透明”的，用户甚至不知道自己在使用代理服务，所以称为“透明代理”。使用透明代理时，网页浏览器访问网站时的域名解析请求将优先发给DNS服务器。

3、反向代理：反向代理是和前两种代理完全不同的一种代理服务。使用它可以降低原始WEB服务器的负载。反向代理服务器承担了对原始WEB服务器的静态页面的请求，防止原始服务器过载。它位于WEB服务器和Internet之间，处理所有对WEB服务器的请求，阻止了WEB服务器和Internet的直接通信。这种方式通过降低了WEB服务器的请求数从而降低了WEB服务器的负载。

小结思考：
使用代理服务器有哪些好处?
传统代理与透明代理的主要区别是什么?
如何限制通过代理访问的Web对象大小?

二、squid服务器安装

2.1.squid安装环境建议

服务器：

> 操作系统：CentOS Linux release 7.6.x (Core)
>
> squid软件版本：squid-4.15.tar.gz
>
> 分区要求：独立磁盘分区足够大，建议>2T
>
> 内存要求：建议至少16G
>
> CPU要求：建议4核
>
> IP地址：192.168.48.128

web服务器

> 安装httpd服务并创建测试页面
>
> IP地址：192.168.48.130

客户测试机

> 安装浏览器
>
> IP地址：192.168.48.129
>
> 关闭防火墙、selinux

参考说明：（以下内容为了解）

> 代理服务器的硬件需求
> 代理服务器对于硬件的要求相当的高！因为我们架设代理服务器的目的就是希望能够加快网络的传输速度因此，虽然代理服务器几乎在任何的 Linux 系统上面都能跑，但是代理服务器最好还是有较高的硬件配置：
>
> CPU 足够好；
>
> RAM 足够大，这也是很重要的一个硬件参数；
>
> Hard Disk 最好能用 SCSI 接口的，因为速度与稳定度都比较好！如果不能的话，那么 IDE 接口的硬盘由于目前速度也越来越快，所以使用 IDE 也没有问题，但是最好是『多块硬盘』的架构，例如我总共需要 30 GB 的硬盘空间，那么最好是 10 GB 的硬盘三块这样的架构较佳。 最好在架设代理服务器时，将整体主机的规划做好，并且让代理服务器主机的服务单纯一点，最好只负责代理服务。
>
> 每颗硬盘的容量不需要太大，此外，最好将硬盘分割一下，一个分区在 2~4 GB 之间即可，因为分太大的话资料的搜寻耗费时间较长，但是分区太小又可能造成空间的浪费
>
> cache 是放置在某个目录下的，而最好一个目录底下就是独立的一个partition 。此外，由于 cache 所在的硬盘常常会有资料的存取，因此可能此一硬盘的损耗率会比较大，所以这个 cache 所在的硬盘最好不要跟重要数据文件，例如 /， /etc， /usr， /home 等等重要的系统文件放在一起！
>
> 也由于 cache 所在的硬盘资料存取太密集了，所以，硬盘的选择上面需要：
>
> (1)转速不能太低；
>
> (2)磁头的机械臂需要可以忍受频繁的动作；
>
> (3)发热量不可太大，或者可以考虑加装硬盘用风扇。
>
> 网络卡与网络周边最好使用 GBytes 的网络卡

2.2.squid编译安装

安装依赖

> yum install -y gcc gcc-c++ gcc-gnat libgcc libgcc.i686 glibc-devel bison flex texinfo Development Tools
>
> 注：安装系统时选择了开发工具以上软件基本无需安装，如果编译过程中提示缺少依赖则进行安装。

编译安装Squid

```
[root@localhost ~]# tar -xzvf squid-4.15.tar.gz -C /usr/src/
[root@localhost ~]# cd /usr/src/opt/squid-4.15/
#1、配置
[root@localhost squid-4.15]# ./configure \
--prefix=/usr/local/squid \
--sysconfdir=/etc \
--enable-arp-acl \
--enable-linux-netfilter \
--enable-linux-tproxy \
--enable-async-io=100 \
--enable-err-language="Simplify_Chinese" \
--enable-underscore \
--enable-poll \
--enable-gnuregex

选项说明：
--sysconfdir=/etc            #单独将配置文件修改到其他目录
--enable-arp-acl             #可以在规则中设置通过客户端MAC进行管理，防止IP欺骗
--enable-linux-netfilter     #使用内核过滤
--enable-linux-tproxy        #支持透明代理（这个很重要，否则后面透明代理无法实现）
--enable-async-io=100        #异步IO，提升存储性能
--enable-err-language="Simplify_Chinese"     #错误信息的显示语言
--enable-underscore      #允许URL中有下划线
--enable-poll                #使用Poll（）模式，提升性能
--enable-gnuregex            #使用GNU正则表达式

#2、编译并安装
[root@localhost squid-4.15]# make && make install
```

安装后基本设置

```
#1、优化可执行文件路径（任意位置直接使用squid相关的命令）
[root@localhost squid-4.15]# ln -s /usr/local/squid/sbin/* /usr/local/sbin/

#2、创建程序用户和组
[root@localhost squid-4.15]# useradd -M -s /sbin/nologin squid

#3、给安装目录设置权限属性
[root@localhost squid-4.15]# chown -R squid.squid /usr/local/squid/var/

#4、squid服务的配置文件位于/etc/squid.conf
[root@localhost squid-4.15]# vim /etc/squid.conf
cache_effective_user squid       #添加指定程序用户
cache_effective_group squid      #添加指定账号基本组
```

程序初始化及启动

```
#1、检查配置文件语法
[root@localhost ~]# squid -k parse

#2、初始化缓存目录
[root@localhost ~]# squid -z
2021/06/17 22:21:03| Created PID file (/usr/local/squid/var/run/squid.pid)
2021/06/17 22:21:03 kid1| Set Current Directory to
/usr/local/squid/var/cache/squid
2021/06/17 22:21:03 kid1| Creating missing swap directories
2021/06/17 22:21:03 kid1| No cache_dir stores are configured.
2021/06/17 22:21:03| Removing PID file (/usr/local/squid/var/run/squid.pid)
回车返回

#3、启动Squid服务
[root@localhost ~]# squid

#4、查看服务启动
[root@localhost ~]# netstat -ntap | grep squid
tcp6       0      0 :::3128                 :::*                    LISTEN
90280/(squid-1)
```

squid服务脚本，

```
#为了使Squid服务启动、停止、重载等操作更加方便，可以编写squid服务脚本，并使用chkconfig和
service工具进行管理。
[root@localhost ~]# vim /etc/init.d/squid
#!/bin/bash
#chkconfig: 2345 90 25

PID="/usr/local/squid/var/run/squid.pid"
CONF="/etc/squid.conf"
CMD="/usr/local/squid/sbin/squid"

case "$1" in
start)
    netstat -natp | grep squid &> /dev/null
    if [ $? -eq 0 ]
    then
        echo "squid is running"
        else
        echo "正在启动 squid..."
        $CMD
    fi
;;
stop)
    kill -9 `expr $(cat $PID) + 2`
;;
status)
    [ -f $PID ] &> /dev/null
    if [ $? -eq 0 ]
    then
        netstat -natp | grep squid
    else
        echo "squid is not running"
    fi
```

```
;;
restart)
    $0 stop &> /dev/null
    echo "正在关闭 squid..."
    $0 start &> /dev/null
    echo "正在启动 squid..."
;;
reload)
    $CMD -k reconfigure
;;
check)
    $CMD -k parse
;;
*)
    echo "用法：$0{start|stop|status|reload|check|restart}"
;;
esac


[root@localhost ~]# chmod +x /etc/init.d/squid      #添加执行权限
[root@localhost ~]# chkconfig --add squid           #使用chkconfig管理
[root@localhost ~]# chkconfig --level 35 squid on   #设置开机启动
```

2.3.构建传统代理服务器

服务器说明

主机	IP地址	主要服务
CentOS7-1	192.168.65.129	http服务
CentOS7-2	192.168.65.128	squid服务
CentOS7-3 或 windows7	192.168.65.130	客户机

配置文件设置

> 修改配置文件，在配置传统代理时，需要添加http_access allow all访问策略，允许任意客户机使用代理。
> 除此以外还要设置reply_body_max_size项，其他参数保持默认。

```
[root@localhost ~]# vim /etc/squid.conf
http_access allow all  #允许任意客户机使用代理
http_port 3128         #使用3128端口
cache_mem 64 MB        #指定缓存功能所使用的内存空间大小，便于保持访问较频繁的WEB对象，容量最好为4的倍数，单位为MB，建议设为物理内存的1/4
reply_body_max_size 10 MB   #允许用户下载的最大文件大小，以字节为单位。默认设置0表示不进行限制
maximum_object_size 4096 KB #允许保存到缓存空间的最大对象大小，以KB为单位，超过大小限制的文件将不被缓存，而是直接转发给用户
```

测试

> centos7-3客户机的代理配置，在IE浏览器中，选择“工具”->“Internet选项”，弹出的“Internet选项”对话框，在“连接”选项中的“局域网（LAN）设置”选项组中单机“局域网设置”按钮，弹出“局域网（LAN）设置”对话框

> centos7-1开启web服务器的httpd服务。
>
> 使用参centos7-3这台虚拟机访问centos7-1，访问成功，查看web服务器的访问日志，查看是那个ip地址访问的，如果是centos7-1代理服务器ip访问的话，说明传统代理部署成功。

2.4.构建透明代理服务器

透明代理提供的服务功能与传统代理一致的，但是其“透明”的实现依赖于默认路由和防火墙重定向策略。因此更适用于为局域网主机服务，而不适合Internet中的客户机提供服务。透明代理的关键在于Linux网关服务器，对于客户机仅需要正确配置网络地址和默认网关，并不需要指定代理服务器。

服务器说明

主机	IP地址	主要服务
CentOS7-1	222.222.222.2	http服务
CentOS7-2	192.168.11.254	squid服务，内网网卡-网关
	222.222.222.254	外网网卡
CentOS7-3 或 windows7	192.168.11.3	客户机
	192.168.11.254	网关设置

网卡配置

```
关闭vmware软件dhcp服务

方法一：
squid服务器
[root@localhost ~]# vim /etc/sysconfig/network-scripts/ifcfg-ens32
TYPE="Ethernet"
BOOTPROTO="static"
DEFROUTE="yes"
NAME="ens32"
DEVICE="ens32"
ONBOOT="yes"
IPADDR="192.168.11.254"
NETMASK="255.255.255.0"

[root@localhost ~]# vim /etc/sysconfig/network-scripts/ifcfg-ens34
TYPE="Ethernet"
BOOTPROTO="static"
DEFROUTE="yes"
NAME="ens34"
DEVICE="ens34"
ONBOOT="yes"
IPADDR="222.222.222.254"
NETMASK="255.255.255.0"

web服务器
[root@localhost ~]# vim /etc/sysconfig/network-scripts/ifcfg-ens32
TYPE="Ethernet"
BOOTPROTO="static"
DEFROUTE="yes"
NAME="ens32"
DEVICE="ens32"
```

```
ONBOOT="yes"
IPADDR="222.222.222.2"
NETMASK="255.255.255.0"

客户机
[root@localhost ~]# vim /etc/sysconfig/network-scripts/ifcfg-ens32
TYPE="Ethernet"
BOOTPROTO="static"
DEFROUTE="yes"
NAME="ens32"
DEVICE="ens32"
ONBOOT="yes"
IPADDR="192.168.11.3"
NETMASK="255.255.255.0"
GATEWEY="192.168.11.254"

方法二：(临时设置)
所有服务器设置网卡为静态ip地址
[root@localhost ~]# systemctl stop NetworkManager

squid服务器
[root@localhost ~]# ip addr add 192.168.11.254/24 dev ens32
[root@localhost ~]# ip link set dev ens32 up

[root@localhost ~]# ip addr add 222.222.222.254/24 dev ens34
[root@localhost ~]# ip link set dev ens34 up

web服务器
[root@localhost ~]# ip addr add 222.222.222.2/24 dev ens32
[root@localhost ~]# ip link set dev ens32 up
[root@localhost ~]# ping 222.222.222.254

客户机
[root@localhost ~]# ip addr add 192.168.11.3/24 dev ens32
[root@localhost ~]# ip link set dev ens32 up

设置网关
[root@localhost ~]# route add default gw 192.168.11.254
```

squid代理服务器

```
#1、开启路由转发
[root@localhost ~]# vim /usr/lib/sysctl.d/50-default.conf
net.ipv4.ip_forward = 1 #添加开启路由转发

[root@localhost ~]# sysctl -p

#2、开启路由转发方法二
echo "1" > /proc/sys/net/ipv4/ip_forward      #开启路由转发
```

squid配置文件设置

> 修改squid.conf配置文件，主要修改http_port，这里和4.1之前的版本修改方法不同，如果像以前一样设置http_port 192.168.11.254:3129 transparent，服务会无法启动，而且查看/usr/local/squid/var/logs/cache.log日志，会发现报错信息。

> 可能4.1版本传统代理默认使用3128端口，无法再做透明代理，新方法是是重新使用一个端口，专门用来做透明代理，配置方法如下。

```
[root@localhost ~]# vim /etc/squid.conf
http_port 3128
http_port 192.168.11.254:3129 transparent #添加透明代理内容

#重启服务
[root@localhost ~]# service restart squid

#查看服务是否启动
[root@localhost ~]# netstat -anpt
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
tcp        0      0 192.168.11.254:3129     0.0.0.0:*               LISTEN
65422/(squid-1)
tcp6       0      0 :::3128                 :::*                    LISTEN
65422/(squid-1)
```

设置iptables重定向策略

```
#清空防火墙规则
[root@localhost ~]# iptables -F
[root@localhost ~]# iptables -t nat -F

#将80端口（http）的请求重新定向到3129端口
[root@localhost ~]# iptables -t nat -I PREROUTING -i ens33 -s 192.168.11.0/24 -p
tcp --dport 80 -j REDIRECT --to 3129
```

测试

```
取消浏览器代理设置
配置客户端网卡信息。（主要设置网关为192.168.11.254）
验证效果，访问http://222.222.222.2,我们再查看web服务器的access.log日志，检查到底是哪个ip对
web服务器访问的。可以看到是222.222.222.254这个IP对即代理服务器的访问记录。
```

三、ACL访问控制

3.1.ACL简介

> 所谓ACL（Access Control List）就是在服务器端设定特定的上网策略，哪些用户能上网，能访问什么网站，能下载什么文件等等对用户的上网行为进行约束和管理，企业一般都会进行ACL上网控制，对员工的上网行为进行控制，从而提高工作效率。
>
> Squid 服务程序的 ACL 是由多个策略规则组成的，它可以根据指定的策略规则来允许或限制访问请求，而且策略规则的匹配顺序与防火墙策略规则一样都是由上至下；在一旦形成匹配之后，则立即执行相应操作并结束匹配过程。

3.2.ACL访问控制方式

ACL访问控制通过以下两个步骤来实现：

1、使用acl配置项定义需要控制的条件

> 定义acl配置项，每一行acl配置可以定义一条访问控制列表，格式如下：
>
> **acl 列表名称 列表类型 列表内容 ...**
>
> 说明：
> 列表名称：由管理员自行指定，用来识别控制条件
>
> 列表类型：必须使用Squid预定义的值，对应不同类别的控制条件
>
> 列表内容：具体控制的对象，不同的类型对应的内容也不一样，可以有多个值，用空格分隔

2、针对已定义的acl列表进行限制

> 通过http_access配置项对已定义的条件做限制，如“允许”或“拒绝”
>
> 定义好acl后，需要设置访问权限，并必须放置在对应的acl配置项之后，格式如下：
>
> **http_access allow或deny 列表名称 ...**

3.3.常用的ACL列表类型

> 列表类型 列表内容示例 含义/用途
>
> src 192.168.1.1
192.168.1.0/24
192.168.1.0-192.168.3.0/24 源IP地址、网段、IP地址范围
>
> dst 192.168.1.1
192.168.1.0/24
www.baidu.com 目标IP地址、网段、主机名
>
> port 80 443 8080 20 21 目标端口
>
> dstdomain .163.com 目标域名
>
> time MTWHF 8:30-17:30 M-Monday 周一
T-Tuesday 周二
W-Wednesday 周三
H-Thursday 周四
F-Friday 周五
A-Saturday 周六
S-Sunday 周日
>
> maxconn 20 每个客户机的并发连接数
>
> url_regex url_regex –i ^rtsp:// 目标资源的URL地址，-i 表示忽略大小写
>
> urlpath_regex urlpath_regex -i .mp3$ 目标资源的整个URL地址，-i 表示忽略大小写，$表示结尾

3.4.ACL列表的应用示例

1、禁止任何客户机使用此代理服务：

```
定义一条名为all的列表，匹配来自任意源地址的代理访问；然后拒绝此列表，注意ACL列表要写在前面
[root@localhost ~]# vi  /etc/squid.conf
acl  all src 0.0.0.0/0.0.0.0
http_access  deny  all

[root@localhost ~]# service squid  reload
```

2、允许多个局域网段在工作时间上网

```
[root@localhost ~]# vim /etc/squid.conf
acl all src 0.0.0.0/0.0.0.0  （有些版本要这么写acl all src all）
acl MYLAN src  192.168.1.0/24   192.168.4.0/24
acl  WORKTIME  time  MTWHF  08:30-17:30   （其中MTWHF是周一到周五的英文首字母）
http_access allow  MYLAN  WORKTIME
http_access  deny  all

[root@localhost ~]# service squid  reload
#注意要先写http_access allow  MYLAN  WORKTIME再写http_access  deny  all，因为先执行前面的，后面的就不执行了
```

3、通过黑名单限制目标网站

（1）首先创建地址列表文件（直接在配置文件里写也行，但是这种用列表文件的方式适合拒绝或允许的网站域名比较多的情况，而且方便增删管理）

```
[root@localhost ~]# vim  /etc/squid/ipblock.list
61.135.167.36
60.28.14.0/24
[root@localhost ~]# vim /etc/squid/dmblock.list
.qq.com
```

（2）配置acl

```
[root@localhost ~]# vim /etc/squid.conf
acl IPBLOCK dst "/etc/squid/ipblock.list"
acl DMBLOCK dstdomain "/etc/squid/dmblock.list"
http_access  deny  IPBLOCK
http_access  deny  DMBLOCK

[root@localhost ~]# service squid  reload
```

3、其它常用控制解析

```
acl localhost src 127.0.0.1                          //定义变量localhost的值为
127.0.0.1
acl mylan src 192.168.11.0/24                        //定义变量mylan的值为
192.168.11.0网段
acl to_localhost dst 127.0.0.0/8                     //定义变量to_localhost的值为
127.0.0.0网段
acl mc20 maxconn 20                                  //定义变量mc20的值为20
```

```
acl blackurl url_regex -i ^rtsp://                      //定义变量blackurl  的值是url路径 为^rtsp://
acl mediafile urlpath_regex -i \.mp3$ \.avi$            //定义变量mediafile 的值是url路径资源为 \.mp3
acl worktime time MTWHF 08:30-17:30                     //定义变量worktime 的值为周一到周五8点半到下午5点半
acl ipblock dst "/etc/squid/ipblock.list"               //定义变量ipblock 的值为/etc/squid/ipblock.list文件的内容
acl dmblock dstdomain "/etc/squid/dmblock.list"         //定义变量dmblock 的值为/etc/squid/dmblock.list文件的内容

http_access deny mylan mediafile                        //禁止mylan客户机下载mp3和avi文件
http_access deny mylan ipblock                          //禁止mylan客户机访问黑名单中的IP地址
http_access deny mylan dmblock                          //禁止mylan客户机访问黑名单中的域名
http_access deny mylan mc20                             //禁止mylan客户机并发连接超过20时被阻止
http_access allow mylan worktime                        //允许mylan客户机在指定时间上网
http_access deny all                                    //把之前的http_access  allow all  进行修改
```

四、squid日志分析：

> 为了使我们查看日志更为直观一些，可以使用SARG，它是一款squid日志分析工具，采用HTML格式， 详细列出每位用户访问Internet的站点信息，时间占用信息、排名、连接次数、访问量等。

SARG的部署过程如下：

4.1.安装GD库

```
[root@localhost yum.repos.d]# yum -y install gd gd-devel
```

4.2.安装SARG

```
[root@localhost src]# tar zxf sarg-2.3.7.tar.gz
[root@localhost src]# cd sarg-2.3.7/
[root@localhost sarg-2.3.7]# ./configure --prefix=/usr/local/sarg --sysconfdir=/etc/sarg --enable-extraprotection
[root@localhost src]# make && make install

配置项含义如下：
-prefix=/usr/local/sarg：指定安装目录；
-sysconfdir=/etc/sarg：配置文件目录，若不指定，默认是/usr/local/etc；
-enable-extraprotection：添加额外的安全保护
```

4.3.配置

```
[root@localhost sarg-2.3.7]# cd /etc/sarg/
[root@localhost sarg]# vim sarg.conf
.....................
#若只实现基本的功能，则配置以下三项即可：
access_log /usr/local/squid/var/logs/access.log      #指定squid的访问日志文件
```

```
output_dir /var/www/html/sarg                          #sarg报告的输出目录，指向网站的根目录下
www_document_root /var/www/html                        #网页根目录

#其余一些优化的配置项如下，根据需求来改即可：
title "Squid User Access Reports"                      #网页标题
user_ip no                                             #使用用户名显示
exclude_hosts /usr/local/sarg/noreport                 #指定不计入排序的站点列表文件
topuser_sort_field connect BYTES reverse               #在top排名中，指定连接次数、访问字节数，采用降序排列，升序将reverse换成normal即可。
user_sort_field connect reverse                        #对于用户访问记录，连接次数按降序排列
overwrite_report no                                    #当那个日期报告已经存在，是否覆盖报告
mail_utility mailq.postfix                             #发送邮件报告的命令
charset utf-8                                          #使用字符集
weekdays 0-6                                           #指定top排序时的星期周期，0为周日。
hours 7-12,14,16,18-20                                 #指定top排序时的时间周期。
```

4、运行：

```
#上面的配置项中添加了不计入排序的站点，需要存在这个文件中。这个文件中添加的域名将不被显示在排序中。
[root@localhost sarg]# touch /usr/local/sarg/noreport

#设置软链接
[root@localhost sarg]# ln -s /usr/local/sarg/bin/sarg /usr/local/bin

#执行sarg启动一次记录
[root@localhost sarg]# sarg
SARG: 纪录在文件: 546, reading: 100.00%
SARG: 成功的生成报告在 /var/www/html/sarg/2019Jun07-2019Jun07

#启动httpd服务，若没有该服务，须自行安装。
[root@localhost sarg]# systemctl start httpd
```

小结考题

- 如何配置透明代理服务器?
- 如何定义ACL访问控制列表?
- 定义好访问控制列表后如何进行访问控制?

实验案例：

- 构建透明代理网关

实验环境

- 通过透明代理提高上网速度

需求描述

- 通过缓存代理服务来提高上网速度
- 免除客户机的代理设置工作

实现思路

- 编写iptables规则，实现REDIRECT应用，实现80、443端口的重定向

- 构建squid服务器，支持透明代理
- 合理使用ACL列表，针对代理访问进行控制