Bài thực hành

Cài đặt và cấu hình Squid Proxy Server

I. Cài đặt và khởi tạo dịch vụ Proxy với Squid

Bước 1. Cấu hình card mạng máy ảo Linux với địa chỉ 192.168.1.1/24, kết nối đến máy ảo Windows có địa chỉ 192.168.1.100/24 qua mạng ảo NAT. Tắt firewall trên máy ảo Linux.

```
[root@CentOS]# ifconfig eth0 192.168.1.1/24 up
[root@CentOS]# service iptables stop
```

Bước 2. Kiểm tra package **squid** đã được cài đặt hay chưa. Nếu chưa cần tiến hành cài đặt package này qua **yum** hoặc **rpm**

```
[root@CentOS]# rpm -qa | grep squid
[root@CentOS]# yum install squid
[root@CentOS]# rpm -qa | grep squid
squid-2.6.STABLE21-6.el5
```

Bước 3. Mở file cấu hình tổng thể của **squid** (**/etc/squid/squid.conf**) và xem các thông tin cấu hình chính

```
[root@CentOS]# less /etc/squid/squid.conf
…
http_port 3128          #Cổng squid lắng nghe cho giao thức HTTP
…
# cache_mem 8 MB        #Dung lượng cache. Mặc định 8MB
…
# cache_dir ufs /var/spool/squid 100 16 256     #Thư mục chứa cache
…
access_log /var/log/squid/access.log squid      #Thư mục chứa log file
…
```

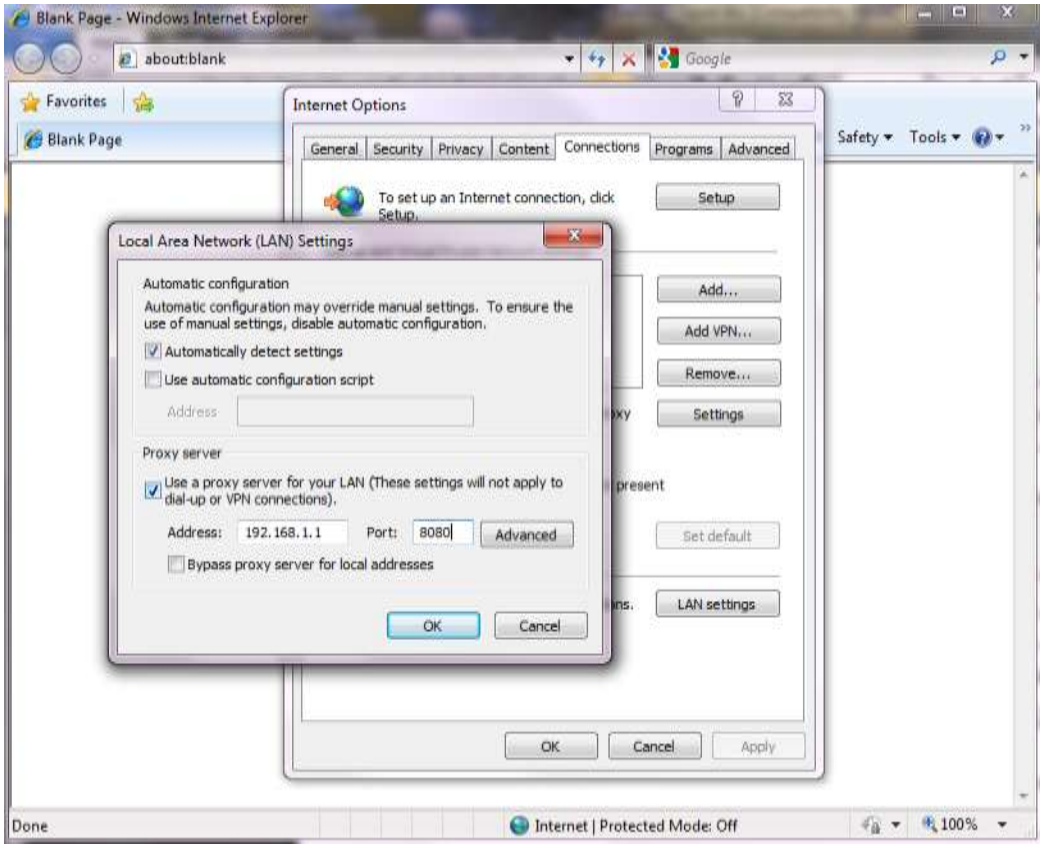
Bước 4. Thay đổi cổng HTTP của Squid thành 8080 và khởi động dịch vụ. Kiểm tra để đảm bảo cổng 8080 đã được mở

```
[root@CentOS]# sed -i -e '/^http_port/s/3128/8080/' /etc/squid/squid.conf
[root@CentOS]# grep ^http_port /etc/squid/squid.conf
[root@CentOS]# service squid start
Starting squid:                                            [  OK  ]
[root@CentOS]# netstat -an | grep 8080
tcp        0      0 0.0.0.0:8080          0.0.0.0:*             LISTEN
```

Bước 5. Mở access log của Squid ở chế độ theo dõi

```
[root@CentOS]# tail -f /var/log/squid/access.log
```

Bước 6. Trên máy thật Windows, mở Internet Explorer và thiết lập tham số Proxy trỏ đến máy ảo Linux (**192.168.1.1**), port **8080**



Bước 7. Trên máy thật Windows, thử truy cập vào website **google.com** để thấy việc truy cập đang bị chặn lại.

Bước 8. Trên máy ảo Linux, kiểm tra để thấy việc truy cập vào **google.com** đang bị Squid ngăn chặn

```
[root@CentOS]# tail –f /var/log/squid/access.log
1298913828.335  1 192.168.1.100 TCP_DENIED/403 1441 GET http://google.com/ -
NONE/- text/html
…
```

Bước 9. Mở file **squid.conf** để thấy mặc định khi mới cài đặt, Squid không cho phép bất kỳ truy cập nào từ client ngoại trừ localhost

```
[root@CentOS]# less /etc/squid/squid.conf
…
http_access  allow  localhost    #Cho phép truy cập từ localhost
http_access  deny   all          #Chặn tất cả các truy cập còn lại
…
```

II. Cấu hình quản lý truy cập với Squid

Cho phép các client ở subnet 192.168.1.0/24 được phép truy cập

Bước 10. Chỉnh sửa **squid.conf** để cho phép các client ở subnet 192.168.1.0/24 được phép truy cập

```
[root@CentOS]# vi /etc/squid/squid.conf
```

Chỉnh sửa dòng:

```
#acl our_networks src 192.168.1.0/24 192.168.2.0/24
#http_access allow our_networks
```

thành:

```
acl our_networks src 192.168.1.0/24
http_access allow our_networks
```

Bước 11. Reload lại cấu hình của Squid

```
[root@CentOS]# service squid reload
```

Bước 12. Mở access log của Squid ở chế độ theo dõi

```
[root@CentOS]# tail –f /var/log/squid/access.log
```

Bước 13. Trên máy thật Windows, mở Web Browser và truy cập lại vào website **google.com** để thấy việc truy cập đã có thể thực hiện được.

Bước 14. Kiểm tra trạng thái truy cập trên accesslog của Squid

```
[root@CentOS]# tail –f /var/log/squid/access.log
…
1298914701.472  378 192.168.1.100 TCP_MISS/301 806 GET http://google.com/ -
DIRECT/74.125.71.99 text/html
…
```

Giới hạn truy cập đến một số website

Bước 15. Tạo file **/etc/squid/deny_sites** và liệt kê danh sách các website không được phép truy cập

```
[root@CentOS]# vi /etc/squid/deny_sites
docbao.vn
vnexpress.net
```

Bước 16. Chỉnh sửa **squid.conf** để chặn các website có trong danh sách **deny_sites** (chèn thêm các nội dung như trong phần không in nghiêng). Reload lại squid sau khi hoàn tất thay đổi.

```
[root@CentOS]# vi /etc/squid/squid.conf
…
acl our_networks src 192.168.1.0/24
acl bad_sites  dstdom_regex -i "/etc/squid/deny_sites"
…
http_access deny    bad_sites
http_access allow our_networks
…
[root@CentOS]# service squid reload
```

Bước 17. Mở access log của Squid ở chế độ theo dõi

```
[root@CentOS]# tail –f /var/log/squid/access.log
```

Bước 18. Trên máy thật Windows, mở Web Browser và thử truy cập vào website **docbao.vn** và **vnexpress.net** để thấy việc truy cập đã bị chặn lại.

Bước 19. Kiểm tra trạng thái truy cập trên accesslog của Squid

```
[root@CentOS]# tail –f /var/log/squid/access.log
…
1298914701.335  1 192.168.1.100 TCP_DENIED/403 1441 GET http://docbao.vn/ -
NONE/- text/html
…
```

Cấu hình yêu cầu xác thực người dùng khi truy cập qua Squid

Bước 20. Tạo cơ sở dữ liệu người dùng để xác thực truy cập, trong cơ sở dữ liệu này sẽ chứa thông tin về người dùng có tên là **ipmac**. Nhập thông tin về password cho người dùng này.

```
[root@CentOS]# htpasswd –c /etc/squid/squid.htpasswd ipmac
New password:
Re-type new password:
Adding password for user ipmac
```

Bước 21. Chỉnh sửa file **squid.conf** và chèn thêm nội dung như bên dưới (phần không in nghiêng) để yêu cầu người dùng phải xác thực khi truy cập. Sau khi chỉnh sửa xong, reload dịch vụ **squid**.

```
[root@CentOS]# vi /etc/squid/squid.conf
…
#auth_param basic credentialsttl 2 hours
#auth_param basic casesensitive off
auth_param basic program /usr/lib/squid/ncsa_auth /etc/squid/squid.htpasswd
…
…
acl our_networks src 192.168.1.0/24
acl bad_sites  dstdom_regex –i "/etc/squid/deny_sites"
acl allow_users  proxy_auth  REQUIRED
…
http_access deny    bad_sites
http_access allow our_networks allow_users
…
[root@CentOS]# service squid reload
```

Bước 22. Trên máy thật Windows, thử truy cập vào website www.yahoo.com để thấy việc truy cập đã yêu cầu xác thực người dùng.