1 Cài đặt squid trên CentOS 7/8

Thực thi lệnh bên dưới để cài Squid trên CentOS 7/8:

[root@localhost ~]# yum -y install squid

Sau khi cài đặt thành công tiến hành chạy các lệnh này

[root@localhost ~]# systemctl status squid (xem trạng thái của squid)

[root@localhost ~]# systemctl start squid (khởi động dịch vụ squid)

[root@localhost ~]# systemctl enable squid

Xem lại trạng thái Squid để chắc chắn Squid chạy.

Tắt tường lửa để Squid hoạt động được:

[root@localhost ~]# systemctl disable firewalld

[root@localhost ~]# systemctl stop firewalld

Một số tệp quan trọng sau khi cài đặt Squid :

* File configuration của squid: /etc/squid/squid.conf
* File Access log của squid: /var/log/squid/access.log
* File Cache log của squid: /var/log/squid/cache.log

# 2 Cấu hình Squid

Check IP của máy Linux bằng lệnh #ip addr

Sau khi biết được IP của máy Linux tiến hành cấu hình, sửa file Squid bằng lệnh

#vi /etc/squid/squid.conf

Chúng ta sẽ định cấu hình Squid làm HTTP proxy chỉ sử dụng địa chỉ IP của client để xác thực.

**Thêm Squid ACLs**

Nếu chúng ta cho phép địa chỉ IP truy cập web thông qua proxy server thì chúng ta cần thêm một dòng ACL mới trong file cấu hình /etc/squid/squid.conf. Dòng chúng ta cần thêm vào có cấu trúc như sau:

acl localnet src X.X.X.X

Trong đó X.X.X.X là địa chỉ IP của client chúng ta cần thêm vào. Dòng này nên được thêm vào đầu file nơi ACL được xác định. Để thay đổi có hiệu lực chúng ta cần khởi động lại Squid:

[root@localhost ~]# systemctl restart squid

**Ví dụ: acl lan src 192.168.1.0/24**

**Sau khi khai báo xong tiếp tục set allow cho dãy vừa khai báo**

**#**

**http\_access deny all**

**http\_access allow lan**

**Mở squid proxy port**

Trong file cấu hình chúng ta thấy một số cổng nhất định được phép kết nối. Chúng ta có thể thêm nhiều hơn bằng cách chỉnh sửa file cấu hình:

Cấu trúc khi cần mở squid port thêm vào file cấu hình:

acl SSL\_ports port X

Trong đó X là số port thực tế chúng ta muốn tải. Để thay đổi có hiệu lực chúng ta cần khởi động lại Squid:

[root@localhost ~]# systemctl restart squid

# 3 Block website với squid proxy

Tại đây chúng ta sẽ tạo môt ACLs cuối cùng để giúp chúng ta chặn các trang web không mong muốn. Đầu tiên cần tạo một file lưu trữ các web trong danh sách đen:

[root@localhost ~]# touch /etc/squid/blacklist\_site.squid

Sau đó chúng ta thêm các domain cần block:

.test1.com

.test2.vn

.test3.net

Trong đó dấu chấm đầu tiên giúp chúng ta loại bỏ www, cũng như các subdomain của domain đó.

Bây giờ chúng ta mở file configuration /etc/squid/squid.conf để thêm 2 dòng sau vào:

#acl block site

acl bad\_urls dstdomain "/etc/squid/blacklist\_site.squid"

http\_access deny bad\_urls

Cuối cùng chúng ta thực hiện lưu file và khởi động lại Squid:

[root@localhost ~]# systemctl restart squid

**Cấm các từ khóa muốn cấm trong tên website**: thêm vào file squid.conf

acl chan\_tukhoa url\_regex -i tukhoa

http\_access deny chan\_tukhoa

Sau đó lưu lại file và khởi động lại Squid

[root@localhost ~]# systemctl restart squid

# 4 Giới hạn truy cập web theo thời gian

#

acl home\_network src 192.168.1.0/24

acl allow\_hours time M T W H F 9:00-17:00

http\_access allow home\_network allow\_hours

http\_access deny all

#

Khai báo mạng 192.168.1.0/24 là home\_network, khai báo thời gian cho phép từ 9h00 đến 17h00 là allow\_hours. Cho phép mạng home\_network truy cập internet trong giờ allow\_hours.

#

acl mornings time 08:00-12:00

#

http\_access allow mornings

Cho phép mọi máy tính truy cập internet vào buổi sáng (8:00 đến 12:00)

Sau đó lưu lại file và khởi động lại Squid

[root@localhost ~]# systemctl restart squid

# 5 Giới hạn bandwidth với squid

Để cấu hình giới hạn băng thông cần một vài tham số sau trong file squid.conf. Ví dụ :

acl whileIP src “/etc/squid/whileip.txt”

delay\_pools 1  
delay\_class 1 3 #pool số 1 có loại class là 3  
delay\_access 1 allow whileIP  
delay\_access 1 deny all  
delay\_parameters 1 200000/200000 50000/50000 20000/20000

Tham số :

delay\_pools : bạn có bao nhiêu pool.

delay\_parameters : giá trị tốc độ được giới hạn cho từng pools

delay\_class : pool đó ứng với class nào.

Có nhiều loại class khác nhau :

* **Class 1** : mọi thứ đều bị giới hạn bởi tổng băng thông cho phép. Ví dụ :

acl whileIP src “/etc/squid/whileip.txt”

delay\_pools 1  
delay\_class 1 1 #pool số 1 có loại class là 1  
delay\_access 1 allow whileIP  
delay\_access 1 deny all  
delay\_parameters 1 200000/200000 #200000Byte = 200KByte/s

Diễn giải : Với cách cấu hình như trên, tổng băng thông cho phép là 200KByte/s , tất cả các máy tính đều được download với tốc độ tối đa là 200KByte/s. Và tốc độ này là **share** ! Tức là nếu có 1 máy, nó sẽ download ở tốc độ 200KByte/s, nhưng nếu có 4 máy thì tốc độ này được chia làm 4. Vậy mỗi máy download với tốc độ là 200KByte / 4 máy = 50KByte/s. Ngoài ra, ta không thể chia nhỏ đường truyền để sử dụng cho mục đích khác nữa. ( VD: ta muốn chia 50% băng thông cho client truy cập internet, còn 50% còn lại dùng cho Update Server… đại loại vậy )

* **Class 2** : mọi thứ đều bị giới hạn bởi tổng băng thông, nhưng mỗi host thì bị giới hạn bởi băng thông của “individual” đó.

acl whileIP src “/etc/squid/whileip.txt”

delay\_pools 1  
delay\_class 1 2 #pool số 1 có loại class là 2  
delay\_access 1 allow whileIP  
delay\_access 1 deny all  
delay\_parameters 1 200000/200000 150000/150000

Diễn giải : Tổng băng thông là 200KByte/s như phía trên đã giải thích. Số 150000 = 150KByte là tốc độ download tối đa của một host ( một PC ). Nhưng tổng băng thông là 200KByte/s. Vậy nếu có 1 máy tính thì nó sẽ download với tốc độ là 150KByte/s, nhưng khi có 2 máy tính thì nó sẽ bị giới hạn bởi tổng băng thông. Nên mỗi máy sẽ download với tốc độ là 100KByte/s. Vì vậy nên không tối ưu.

Nên thông thường, ở đây người ta sẽ cấu hình như sau :

acl whileIP src “/etc/squid/whileip.txt”

delay\_pools 1  
delay\_class 1 2 #pool số 1 có loại class là 2  
delay\_access 1 allow whileIP  
delay\_access 1 deny all  
delay\_parameters 1 200000/200000 -1/-1

Diễn giải : Tổng băng thông là 200KByte/s như phía trên đã giải thích. Số -1/-1 là tốc độ download tối đa của 1 host ( một PC ) là không giới hạn ( Unlimited ). Như vậy nếu có 1 máy tính thì nó sẽ download với tốc độ tối đa ( 200KByte/s ). Nhưng khi có 2 máy tính thì nó sẽ chia đều tổng băng thông. Vậy mỗi máy tính sẽ download : 200KBytes / 2 máy = 100KBytes. Cách cấu hình này tối ưu khi có ít máy, nhưng khuyết điểm là dễ bị máy khác “cướp” băng thông.

* **Class 3** : mọi thứ đều bị giới hạn bởi tổng băng thông, nhưng mỗi “network” có giới hạn băng thông của nó, và mỗi “individual” có giới hạn băng thông riêng. ( chia ra 3 cấp độ )

Lưu ý : Địa chỉ IPv4 có dạng : a.b.c.d

Squid quy ước ứng với mỗi c ( 0 – 255 ) sẽ là một network. Đây là Squid quy ước.

acl whileIP src “/etc/squid/whileip.txt”

delay\_pools 1  
delay\_class 1 3 #pool số 1 có loại class là 3  
delay\_access 1 allow whileIP  
delay\_access 1 deny all  
delay\_parameters 1 200000/200000 50000/50000 10000/10000

Diễn giải : mỗi “individual” cho phép tối đa 10KByte/s, và mỗi “network” là 50KByte/s. Tổng băng thông là 200KByte/s. Class 3 này sử dụng cho một lượng client khá lớn.

Nếu client không nằm trong whileIP thì nó sẽ không chịu ảnh hưởng của việc giới hạn băng thông. Nó sẽ chạy max speed mà không bị kiểm soát gì cả.

Sau đó lưu lại file và khởi động lại Squid

[root@localhost ~]# systemctl restart squid

# 6 Test

# Vào 1 trình duyệt web xong vào Internet options để setting Proxy Server

# 

# Sau đó vào bảng Connections chọn LAN settings

# 

# Sau đó thiết lập như trong hình với Address là IP của Squid và Port là port trong file squid.conf

# 

# Sau đó test thử một vài trang web và một vài từ khóa đã block

# 

# 

# 

# Test tốc độ download

# Lúc giới hạn tối đa chỉ 200kB/s

# 

# Lúc download bình thường

# 