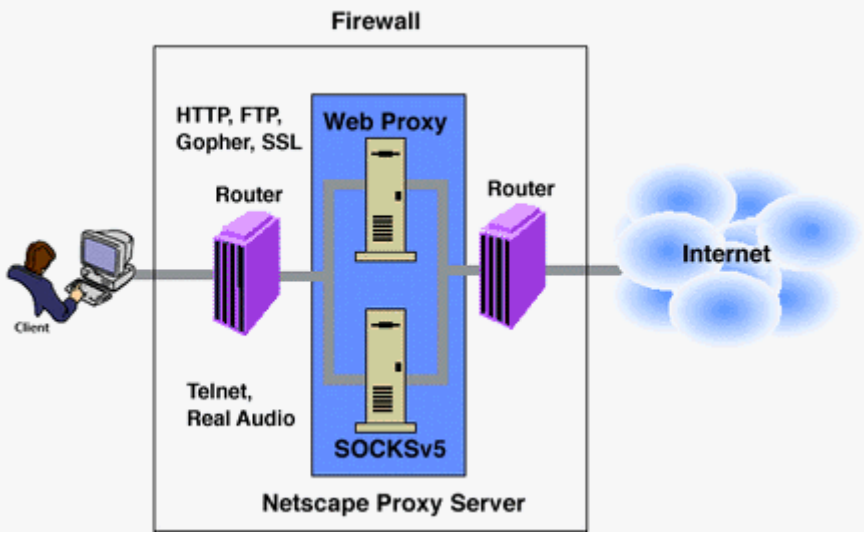
Giả mạo địa chỉ IP (Fake IP)

Thế nào là Fake IP: *Fake IP* là việc truy cập vào Website (hoặc nguồn tài nguyên Web nào đó nào đó) gián tiếp thông qua một Proxy (Máy chủ Proxy). Như vậy điều quan trọng, bạn phải hiểu Proxy là gì

Proxy: Chỉ một hệ thống Computer hoặc một Router tách biệt kết nối, giữa người gửi (Sender) và người nhận (Receiver). Nó đóng vai trò là một hệ thống chuyển tiếp (Relay) giữa 2 đối tượng: ***Client*** (muốn truy cập tài nguyên) và ***Server*** (cung cấp tài nguyên mà Client cần) .

Nhờ chức năng chuyển tiếp (trung chuyển có kiểm soát) này , các hệ thống Proxy (hay Proxy servers) được sử dụng để giúp ngăn chặn attacker xâm nhập vào Mạng nội bộ và các proxy cũng là một trong những công cụ được sử dụng để xây dựng Firewall trong Mạng của các tổ chức có nhu cầu truy cập Internet.



Một proxy server của Netscape

Từ *proxy* còn có nghĩa "hành động nhân danh một người khác" và thực sự Proxy server đã làm điều đó, nó hành động nhân danh cho Client và cả Server . Tất cả các yêu cầu từ Client ra Internet trước hết phải đến Proxy, Proxy kiểm tra xem yêu cầu nếu được cho phép, sẽ chuyển tiếp có kiểm soát yêu cầu ra Internet đến server cung cấp dịch vụ (Internet Hosts). Và cũng tương tự sẽ phản hồi (response) hoặc khởi hoạt các yêu cầu đã được kiểm tra từ Internet và chuyển yêu cầu này đến Client. Cả hai Client và Server nghĩ rằng chúng nói chuyện trực tiếp với nhau nhưng thực sự chỉ "talk" trực tiếp với Proxy.

Như vậy khi bạn dùng một proxy nào đó, xem như bạn bắt đầu đứng từ địa phận (Proxy IP), để tiến hành các giao tiếp mạng.

Fake IP để làm gì ?

- Nhiều Website từ chối giao dịch, mua bán với những vùng địa chỉ IP xác định (IPs blocked) (vd: Những ISP, từ đó phát tán Spam mail, IP của những

ISP/Quốc gia phát tán spam, malware.., những địa chỉ IP mà từ đó bắt nguồn các cuộc tấn công xâm nhập website). Như vậy khi bạn muốn mua hàng trực tuyến và thanh toán sẽ bị chính sách từ chối của website ngăn chặn, cho dù bạn đang thực hiện mua bán hợp pháp, nhưng IP của bạn hiện đang nằm trong Blacklist

- Bị cấm truy cập vào các Website, đã bị các ISP nước sở tại chặn, vì một trong nhiều lý do: Đồi trụy, nguy hiểm, thông tin sai lệch, có yếu tố chính trị…hoặc các lý do khác.

- Bị cấm truy cập vào các Website, bị Quản trị Mạng của cty chặn (LAN firewall block). Khi này User có thể thay đổi các thông số của trình duyệt (vd: IE, Firefox, Maxthon..), không sử dụng Proxy của doanh nghiệp.

- Làm thêm các công việc kiếm tiền Online: Click vào các banner quảng cáo, đọc email hàng ngày (*lưu ý*: Thường đa số email quảng cáo chỉ dành cho các thị trường của các nước phát triển như Âu-Mỹ và một số nước Châu Á,vì lẽ đó những trang trả tiền đọc email chỉ gửi cho các thành viên ở những nước này. Như vậy nếu ở Việt Nam, bạn có thể không tham gia vào việc này được. Như vậy phải làm thế nảo ? Có thể làm cho website "ngộ nhận" bạn đang ở Mỹ hay Châu Âu, bằng cách sử dụng 1 Proxy Server ở US hay EU).

- Giả mạo IP để thực hiện các hành vi như xâm nhập các hệ thống / website trên Internet, xâm nhập vào mạng của các tổ chức, mục đích sau này tránh bị lần ra dấu vết thật.

- Giả mạo IP để tránh attacker có thể xâm nhập vào computer của bạn. Hoặc tránh việc bị các website cài spy/bot thu thập các thông tin cá nhân của bạn.

- Và rất nhiều lý do khác, chỉ vì người sử dụng muốn ..fake IP

Ưu điểm của việc Fake IP thông qua việc sử dụng các Proxy server:

- Vì một trong số các lý do đã đề cập, User có thể che dấu địa chỉ IP thực của mình thông qua Proxy, để có thể tiến hành giao tiếp qua Internet.

- Tìm thấy nhanh những nội dung web cần tìm, nếu nội dung ấy đã được proxy server lưu trữ vào cache, không phải load lại tại website chính.

Nhược điểm của việc Fake IP thông qua việc sử dụng các Proxy server:

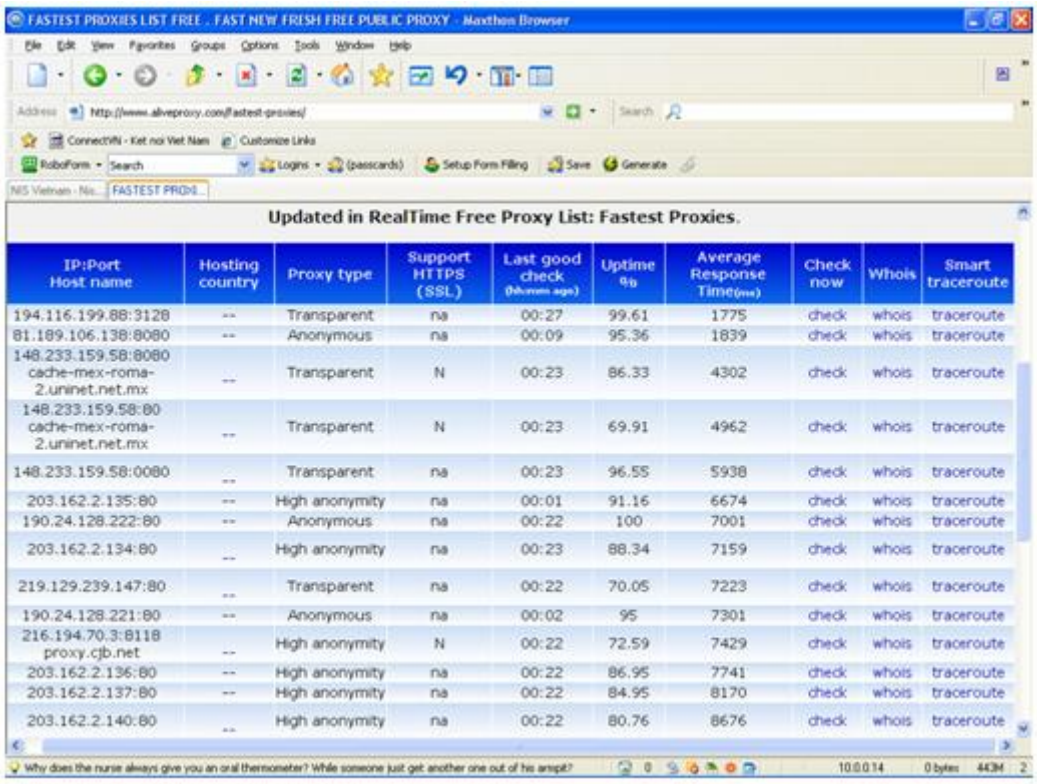
- Giả mạo IP thông qua dùng Proxy, có nghĩa là bạn không đi trực tiếp được, mà phải đi đường vòng, đến Proxy server trước, rồi mới đến website cần truy cập, việc này mất thời gian, nên bạn thường thấy..chậm.

- Phải tìm được các Proxy server trên Internet (có thể vào google.com, gõ *Free proxy*) việc này gây tốn kém thời gian cho bạn, tìm được một Proxy vừa free vừa fast không phải dễ và có thể phải trả phí nếu Proxy đó yêu cầu, "sử dụng – trả tiền "

- Network hoặc Website Admin, có thể phát hiện ra bạn đang dùng Proxy, và stop truy cập hiện tại, hoặc lần ra dấu vết của bạn nếu bạn tiến hành xâm nhập. Như vậy, hầu hết các Anonymous Proxies không phải là chiếc áo "tàng hình" siêu việt, có thể giúp bạn "ẩn tích" 100%

Tìm proxy ở đâu ?

Vào công cụ tìm kiếm Google, gõ cụm từ *Free Proxy* , kết quả hàng trăm ngàn Proxy sẽ xuất hiện. Điều bạn quan tâm là, không phải 100% các Proxy server này đều *Live –sống, như vậy cần tìm ra proxy sống và tốc độ nhanh.* Cũng chẳng mất nhiều thời gian, chỉ cần thêm từ *fastest proxy* vào google.



Hình 01:Dịch vụ cung cấp fatest proxies của aliveproxy.com

Aliveproxy.com là một website điển hình cung cấp cho các bạn, một danh sách hàng loạt các fast proxy server.

Các proxy này ghi rõ các thông tin cung cấp cho người dùng, không chỉ có thông tin về Proxy Server như:

Proxy Hostname: Tên máy chủ proxy, Địa chỉ IP, Port (cổng Proxy hiện đang open, để cung cấp dịch vụ)

Hosting Country: Proxy đang đặt ở quốc gia nào

Proxy type: Loại Proxy (phổ biến là: Anonymous – Proxy nặc danh, Transparent – Proxy "xuyên suốt", High Anonymity…*xem thêm phần phụ lục giải thích sự khác nhau của các proxy type, cuối bài viết*).

Support HTTPS (SSL): Có đảm bảo an toàn cho thông tin giao tiếp web, qua giao thức SSL hay không. *Cũng lưu ý các bạn không may khi gặp phải một Free Hostile Proxy (proxy có ý đồ xấu). Proxy này có thể tóm tất cả các thông tin giao dịch của bạn, là mối nguy lớn khi ID/password của bạn bị tóm khi dùng thẻ thanh toán Online.*

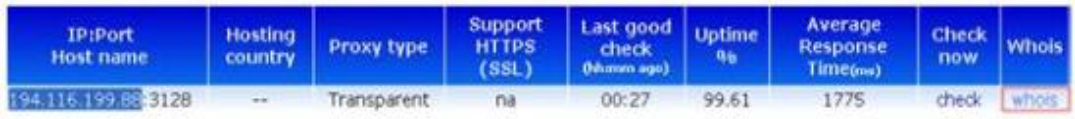
Last good check: Thời gian gần nhất, đã tiến hành kiểm tra proxy này, đảm bảo Proxy đang hoạt động

Uptime: Độ tin cậy về sự ổn định của proxy (tỉ lệ thời gian "sống"), tính bằng phần trăm, càng cao càng tốt

Average Response time: thời gian phản hồi khi yêu cầu truy cập web của bạn được gửi đến proxy (tính bằng ms, 1s = 1000 ms, thông thường bạn phải chờ từ 2-10s hoặc lâu hơn)

Check now: cho phép bạn kiểm tra proxy này ngay, trước khi dùng.

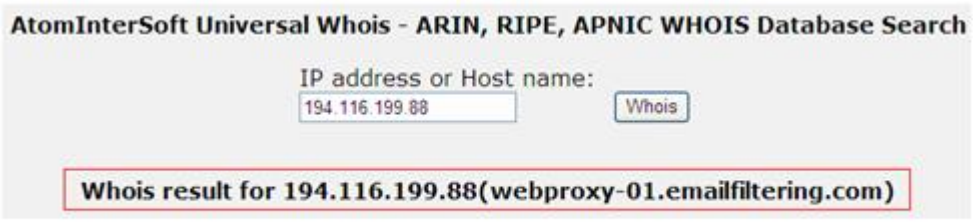
Whois/Trace Route: Lần theo dấu vết, thông tin về proxy server này, tên domain và thuộc quản lý của tổ chức nào, thông tin cụ thể về tổ chức đó, các bài viết chi tiết nhận định đánh giá về nó (những info này, cần phải biết trước hi dùng proxy)



IP:Port Host name	Hosting country	Proxy type	Support HTTPS (SSL)	Last good check (hh:mm ago)	Uptime %	Average Response Time(ms)	Check now	Whois
194.116.199.88:3128	--	Transparent	na	00:27	99.61	1775	check	whois

Hình 02: Dùng Whois của aliveproxy.com, check thông tin cụ thể về proxysrv có IP 194.116.199.88

Các thông tin bạn có được, cho biết 194.116.199.88, có Server name là: webproxy-01.emailfiltering.com



Hình 03: Kết quả Dùng Whois của aliveproxy.com

Nếu chưa tin cậy về Whois của aliveproxy,bạn có thể dùng *Whois.net* để tìm hiểu rõ hơn về tổ chức nào chứa Server này.

Hình 04: Kết quả Dùng Whois.net cho biết tên cty/tổ chức là Verio Inc.

Click tiếp vào *click here* , để dùng SiteTiki.com, để nhận được thông tin chi tiết và minh bạch hơn về Verio Inc.

Hình 05: Kết quả cho thấy emailfiltering.com, là công ty phần mềm bảo mật email

Và bên dưới kết quả chi tiết của SiteTiki.com, có hàng trăm bài viết phổ biến về emailfiltering.com. Từ đó bạn có thể quyết định dùng proxy server của họ hay không.

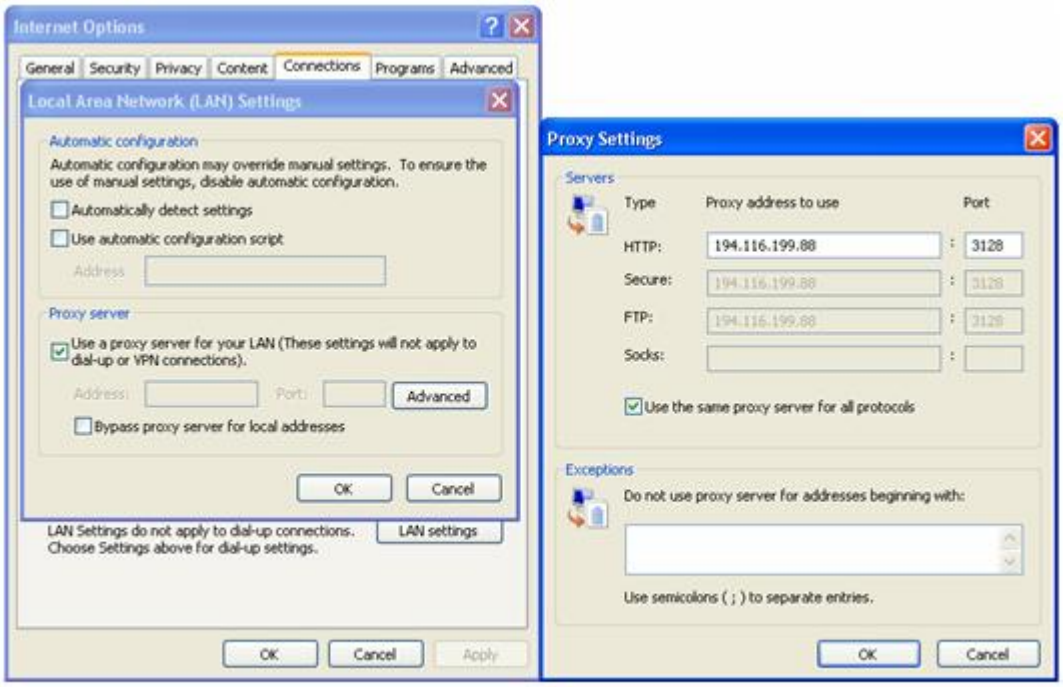
Danh sách một số proxy server của Việt nam được update tại Aliveproxy.com

http://www.aliveproxy.com/proxy-list/proxies.aspx/Vietnam-vn

Bước tiếp theo, sau khi kiểm tra toàn bộ các thông số của 1 proxy và chọn proxy này, bạn có thể cấu hình trình duyệt web của mình (như IE, Firefox, Netscape, Maxthon, Opera..) *hoặc bất cứ ứng dụng Internet nào*, hiện đang bị LAN proxy của công ty ngăn chặn như Yahoo, AIM, ICQ, game online, Phone IP, chia sẽ mạng ngang hàng Bittorrent, eMule, KaZaa, eDonkey..

Xác lập các thông số proxy cho trình duyệt Internet Explorer :

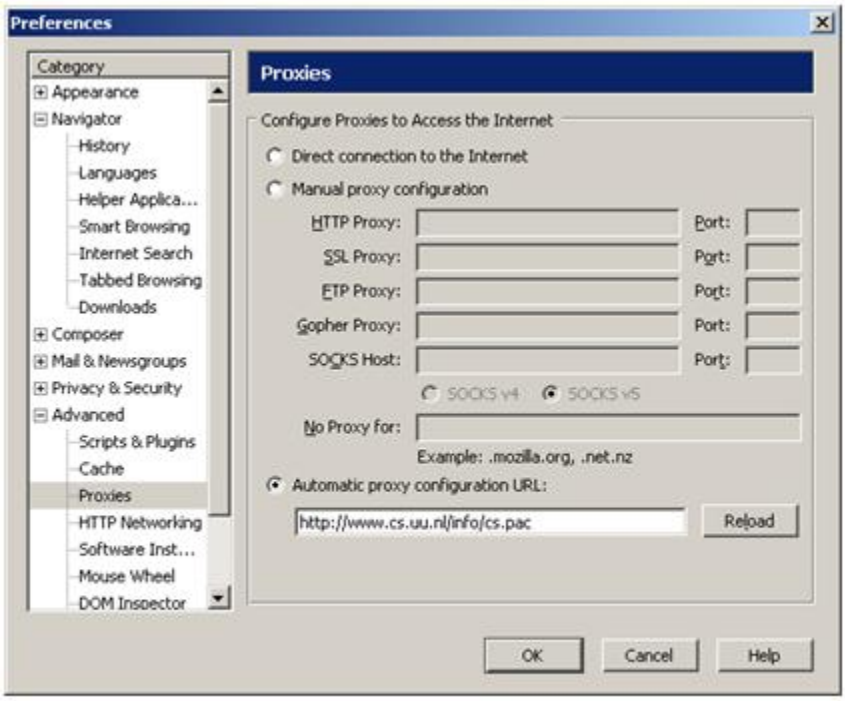
Mở IE, chọn **Tools/ Internet Options/ Connections/ LAN Settings**



Hình 06: Xác lập IE dùng Proxy có IP:Port 194.116.199.88:3128

Xác lập các thông số proxy cho trình duyệt Netscape:

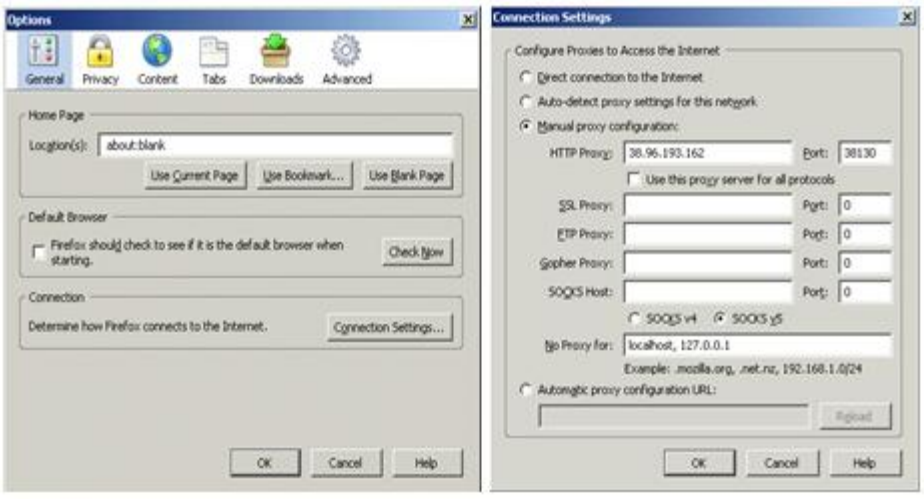
Mở Netscape, chọn **Edit menu, click Preferences/ Advanced tab, click Proxies**, điền vào địa chỉ URL, nơi cung cấp thông số proxy tự động cho Browser



Hình 07: Xác lập netscape dùng Proxy tự động thông qua URL

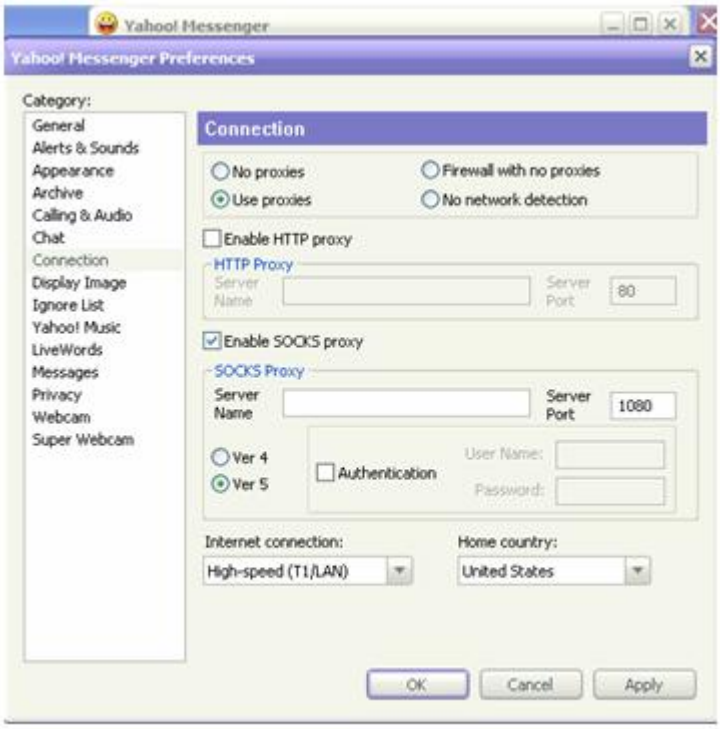
Xác lập các thông số proxy cho trình duyệt Firefox:

Click chọn **Tools/ Options/ Connection Settings/ Manual Proxy Configuration** và điền thông số proxy vào

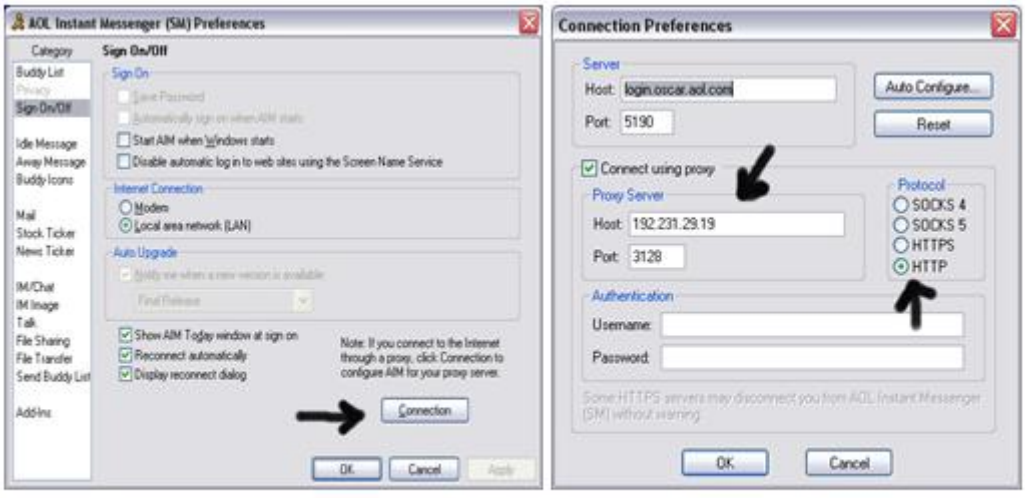


Hình 08: Xác lập Firefox dùng Proxy

Xác lập các thông số proxy cho Yahoo IM:



Hình 09: Xác lập proxy cho Yahoo IM



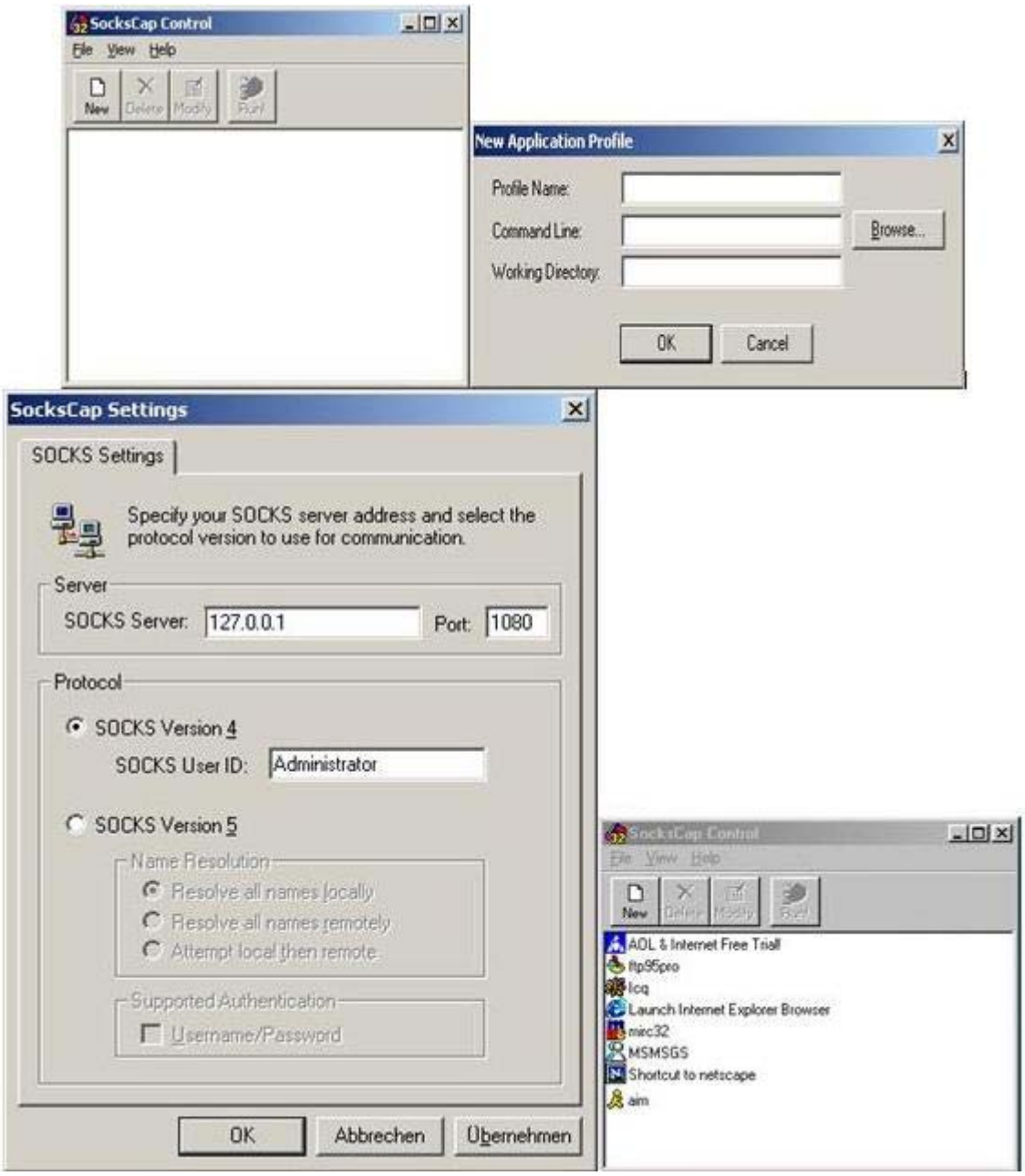
Hình 10: Xác lập proxy cho **AOL IM**

Hình 11: Xác lập Socks5 proxy cho **ICQ**, nếu dùng HTTP hoặc HTTPS proxy, ICQ có thể bị ngắt kết nối mạng
(Xem thêm sự khác nhau giữa Proxy và Socks proxy tại phụ lục cuối bài)

Những Tools giúp bạn Fake IP:

Tất nhiên, để thuận tiện hơn cho việc fake IP, thường User sẽ sử dụng các fake IP software. Các soft này đều dễ cấu hình, cập nhật danh sách các Proxy Server tốt nhất và an toàn nhất cho bạn.

Sockscap: Cung cấp proxy cho các chương trình dùng Internet như (Instant Messaging, Email, Peer to Peer Share – *E-Donkey, eMule, KaZaa*..). Sau khi cài đặt, chương trình sẽ hỏi bạn muốn cài đặt cấu hình cho Sockscap, chọn Yes, điền thông số Sock Proxy, với địa chỉ của Socks Server là chính máy bạn, nơi vừa cái đặt sockscap (**127.0.0.1** còn gọi là loopback address, địa chỉ này không dùng truy cập mạng, mục đích chính để kiểm tra cấu hình TCP/IP của chính máy tính bạn có chính xác hay chưa), sử dụng socks port 1080, Socks version 4 (xem thêm phần phụ lục để hiểu rõ sự khác nhau giữa: HTTP/HTTPS proxy và Socks 4 – 5 Proxy.



Hình 12: Sockscap rất dễ dùng, cấu hình với một số thao tác đơn giản, đưa vào list những ứng dụng cần dùng proxy

Sau khi điền các thông số, có thể chọn các chương trình ứng dụng cần dùng proxy. Ví dụ: Chọn **File/ New/**

Click chọn **C:Program Files AOL AIM.exe** , AIM sẽ xuất hiện trong danh sách, tương tự làm cho các ứng dụng khác…

Ngoài *sockscap* còn nhiều proxy tool mạnh khác như:

Fake IP tools: Hide the I, GhostSurf Proxy Platinum, Anonymizer Anonymous Surfing; Proxy Finder Pro ... (click download link & dùng demo..)

Tất nhiên, đối với người dùng thông thường, chủ yếu truy cập các website, việc hiểu các khái niệm proxy, sau đó cấu hình hoặc cái đặt các tools này là hết sức..phức tạp.

Do đó, một trong các phương thức dễ dàng nhất, để truy cập các trang web bị cấm, là sử dụng một browser web proxy như: http://browsesecurely.net/ , chỉ cần vào website này, điền tên website bạn muốn truy cập.

***Phụ lục*:**

1. Các loại Proxy Server và chức năng

Phân biệt Proxy theo chức năng, thì có rất nhiều kiểu chức năng (caching proxy server, web proxy, Content Filtering Web Proxy, Anonymizing proxy server, Intercepting proxy server..) . Ở ví dụ trong phần đầu, sau khi tìm kiếm được danh sách một loạt các Proxy server, tại mục Proxy type, có những loại sau: Anonymous, Transparent, High Anonymity, phân biệt các kiểu Proxy này như thế nào

Anonymous:

Đôi khi còn được gọi là web proxy, giúp người dùng ẩn danh (giấu IP), khi lướt Web. HTTP Proxy server không gửi thông số cụ thể của biến HTTP_X_FORWARDED_FOR tới Host đang truy cập, do vậy có thể che dấu IP của bạn. tuy nhiên, điều đó không có nghĩa giúp bạn ẩn dấu hoàn toàn, vì các website có thể sử dụng các site script để thu thập thông tin về việc bạn đang truy cập Host của họ thông qua một Proxy nào đó đang..phục vụ cho bạn

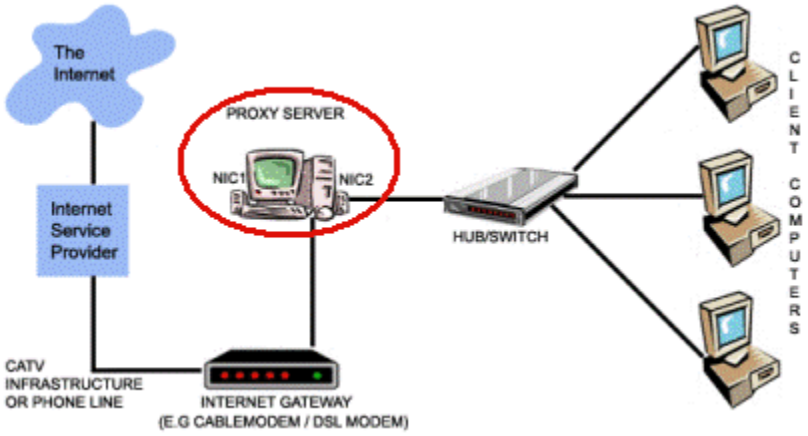
High Anonymity:

Mức độ che dấu tung tích cao hơn anonymous. Http Proxy hoàn toàn không gửi đi bất kì thông số nào của các biến HTTP_X_FORWARDED_FOR, HTTP_VIA và HTTP_PROXY_CONNECTION. Do vậy Internet Host không thể biết bạn đang dùng Proxy server, cũng như không detect được real IP của bạn

Transparent:

Proxy xuyên suốt, Đôi khi còn được gọi là Intercepting proxy, khác với 2 loại trên, transparent là sự kết hợp 1 proxy server và 1 gateway.

Đây là phương thức thường được các Network Admin "ép" User trong mạng Lan, User không nhận thức được mình đang truy cập internet qua một "cổng giám sát"



Admin Mạng có đang theo dõi bạn khi bạn "đi qua" Proxy ?

Yêu cầu truy cập của Client đước chuyển đến gateway sau đó gateway chuyển sang Proxy server xử lý. Khi user dùng loại proxy này, thì họ không biết được rằng họ đang dùng 1 proxy và bị..kiểm soát. User chỉ cần thiết lập địa chỉ IP của gateway do Admin cung cấp, mà không phải xác lập các thông số Proxy trong trình duyệt cũng như Internet applications khác..

Thường được các Admin trong công ty triển khai, họ muốn các chính sách của Policy được áp đặt lên user, nhưng user hầu như không biết mình đang qua 1..proxy

2. HTTP proxy và Socks proxy là gì, khác nhau như thế nào ?

HTTP/HTTPS Proxy(proxy thông thường):

Các proxy servers sẵn sàng cho các dịch vụ thông thường trên internet, ví dụ như: một HTTP proxy được dùng cho truy cập Web, một FTP proxy được dùng cho truyền File.

Những Proxies trên, được gọi là application-level proxies hay "application-level gateways", bởi vì chúng được chỉ định để làm việc với những application và protocol và nhận ra được nội dung các Packet được gửi đến nó.
Một hệ thống proxy khác được gọi là circuit-level proxy, hỗ trợ nhiều applications cùng lúc. ví dụ, SOCKS là một IP-based proxy server (circuit-level proxy), hổ trợ hầu hết các applications trên nền TCP và UDP

SOCKS hay Sockets:

Chính là một circuit-level proxy server cho các IP networks theo định nghĩa từ (IETF (Internet Engineering Task Force)- một cộng đồng các chuyên gia về network designers, operators, vendors, and researchers tham gia vào cuộc xây dựng kiến trúc Internet và ngày càng hoàn thiện Internet hơn.) SOCKS được viết bởi David và Michelle Koblas vào những năm đầu của thập niên 90.

SOCKS đã nhanh chóng trở thành một de facto standard (hardware hay software được dùng rộng rãi nhưng không được chứng nhận từ những tổ chức chuyên cung cấp các định chuẩn), ngược lại là de jure standard. Mặc dù SOCKS ra đời sớm và được dùng phổ biến, nhưng SOCKS được IETF thông qua lần đầu tiên là SOCKS5. SOCKS ban đầu là hệ thống Proxy được sủ dụng cho các traffic như FTP, Telnet, v.vv, nhưng không dành cho HTTP. SOCKS4 kiểm soát các TCP connections (là phần lớn các Application trên Internet),

SOCKS5 còn hỗ trợ thêm UDP, ICMP, xác thực User (user authentication) và giải quyết hostname (DNS service).

SOCKS bắt buộc Client phải được cấu hình để chuyển trực tiếp các yêu cầu đến SOCKS server, hoặc ngược lại SOCKS driver sẽ ngăn chặn các Clients chuyển các yêu cầu non-SOCKS application. Nhiều Web browsers và các Internet applications khác hiện nay hỗ trợ SOCKS, cho nên khá dễ dàng khi làm việc với các SOCKS server. ìm hiểu chi tiết về SOCKS và các Applications tuân theo SOCKS Cũng cần xem thêm mô hình giao tiếp TCP/IP stack **tại đây** (Permeo Technologies' SOCKS Web site).

 ***Video dùng HideIP để fake IP***

Network Security 2008 - ***www.Nis.com.vn***