Published on *Dân Luận* (http://danluan.org)

By *tqvn2004*
Created *02/08/2009 - 14:51*

Cẩm nang vượt tường lửa hay là "How to bypass firewall for dummies" (j/k)

Soạn bởi Tqvn2004

Mục đích của tài liệu này là phổ biến tới độc giả các phương thức vượt tường lửa hiệu quả và phổ biến nhất. Tài liệu gồm hai phần, phần thứ nhất đi thẳng vào giới thiệu cài đặt và sử dụng các chương trình vượt tường lửa, dành cho những người không có nhiều thời gian để tìm hiểu sâu. Phần thứ hai mô tả chi tiết cách thức vận hành của tường lửa, và qua đó giúp độc giả hiểu rõ hơn tại sao các phương pháp vượt tường lửa ở phần thứ nhất lại giúp mình qua được tường lửa. Chúng tôi khuyến nghị độc giả tham khảo kỹ phần thứ hai để hiểu và từ đó có thể "vận dụng sáng tạo" hơn các cách vượt tường lửa được giới thiệu ở phần thứ nhất.

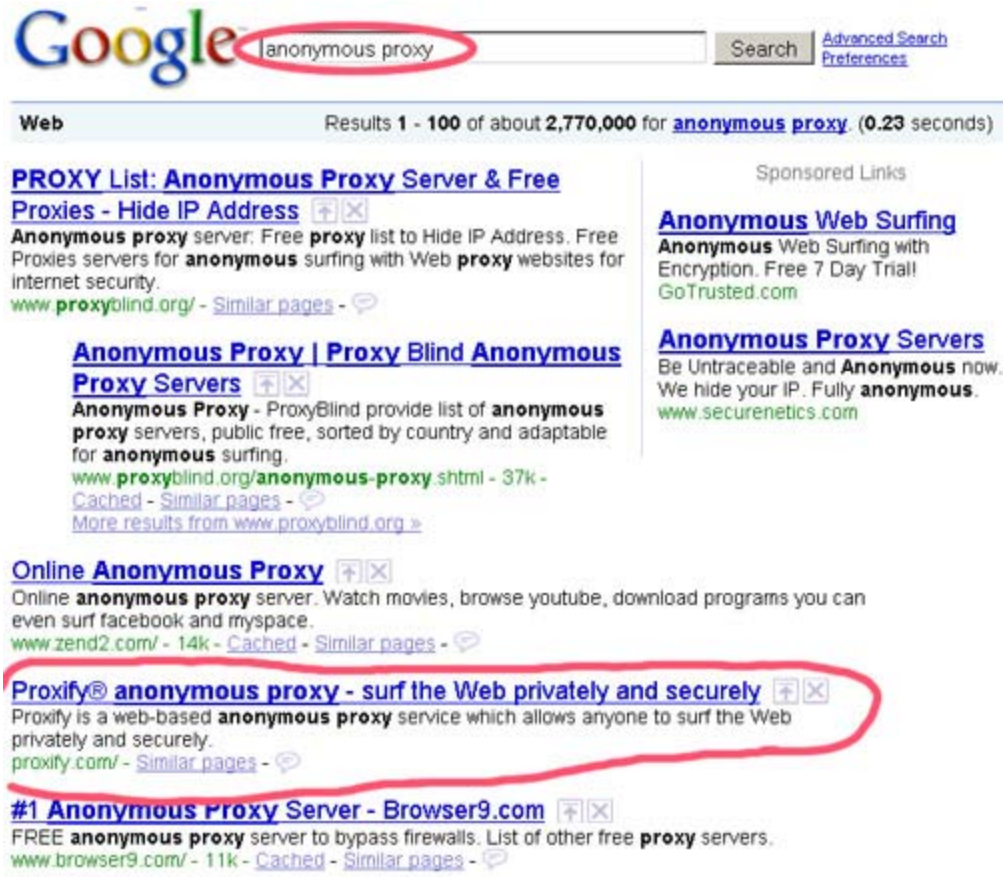
Chúc độc giả sử dụng thành công các phương thức được hướng dẫn tại đây. Xin hãy lưu lại tài liệu này (có sẵn ở dạng PDF lẫn HTML) cùng các chương trình hỗ trợ, để tra cứu và sử dụng lúc cần thiết. Và chúng tôi cũng rất biết ơn nếu độc giả có thể giúp phổ biến tài liệu này một cách rộng rãi khi có điều kiện.

Phần I: Các phương thức vượt tường lửa

Phần II: Tường lửa là gì?

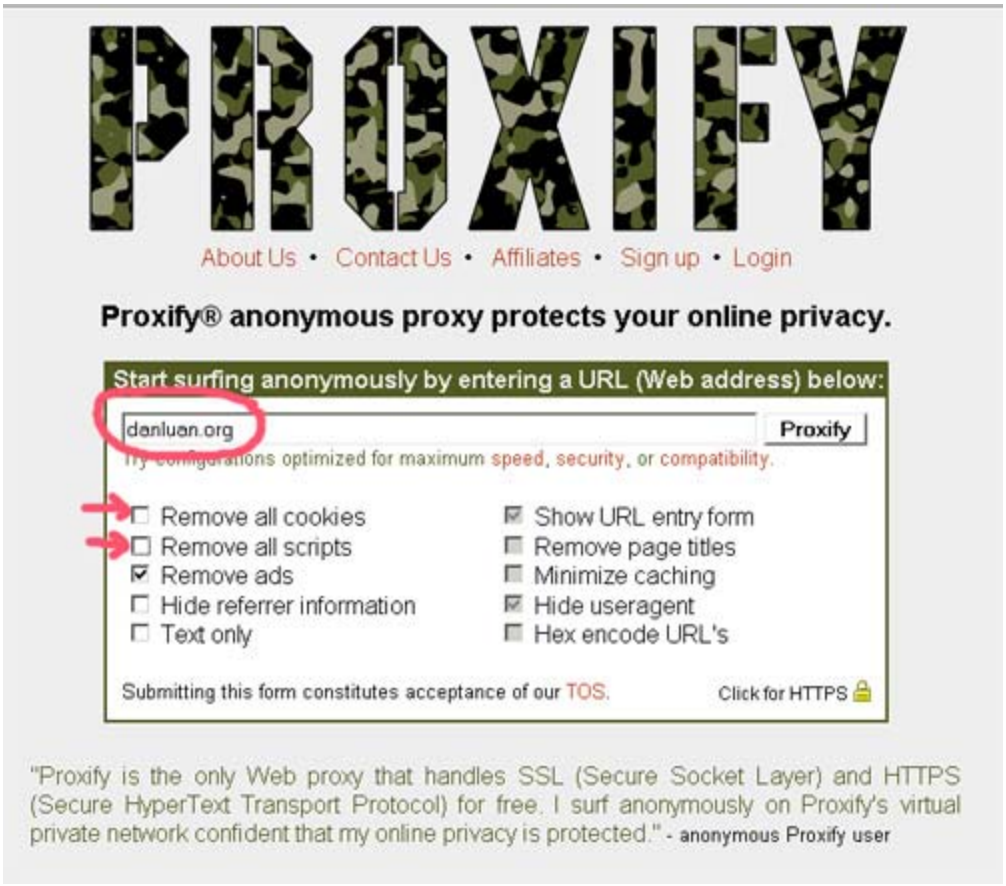
Phần I.A: Dùng web proxy để vượt tường lửa

Nhiều trang web trên Internet cung cấp dịch vụ web proxy miễn phí tới người sử dụng. Những trang như thế thường được biết tới dưới tên "anonymous proxy" or "anonymous surfing". Gõ từ khóa đó vào trang Google [1] để tìm chúng, và giả sử Google [1] trả về kết quả như ở Hình 1:



Hình 1: Kết quả trả về bởi Google với từ khóa "anonymous proxy"

Bạn có thể chọn một trang bất kỳ để thử, giả sử bạn chọn trang Proxify.com [2]. Khi nhấn chuột vào liên kết proxify.com [2], bạn sẽ được đưa tới trang tương tự như ở Hình 2:



Hình 2: Giao diện của Proxify.com, một trang cung cấp dịch vụ web proxy miễn phí trên Internet

Giao diện có thể khác nhau trên mỗi trang web, nhưng các công cụ mà anonymous proxy cung cấp thường giống nhau:

- Một ô để gõ địa chỉ cần truy cập vào, ví dụ ở Hình 2, bạn gõ danluan.org
- “Remove all cookies”: Không cho phép cookies từ trang danluan.org tới được máy của bạn. Thường thì bạn phải cho phép cookies, nếu bạn muốn đăng nhập vào danluan.org. Nếu bạn chỉ định đọc như một khách viếng thăm, thì chọn “remove all cookies” cũng được.
- “Remove all scripts”: Không cho phép Javascript từ trang danluan.org tới máy của bạn. Thường thì bạn phải cho phép Javascript, để xem trang web một cách tốt nhất (nhiều chức năng trên danluan.org cần còn Javascript). Bạn có thể thử tắt bật chức năng này để xem mình được và mất gì :D
- “Show URL entry form”: Proxify sẽ “lồng” vào trang web bạn muốn xem một khung điều khiển, để bạn có thể nhập các liên kết (url) khác mà bạn muốn chuyển tới. Bật khung này có thể gây không tương thích khi xem một số trang, bạn hãy thử nghiệm một vài lần xem mình thích bật hay không.
- v.v... Còn nhiều tùy chọn khác, nhưng có lẽ bạn không cần quan tâm tới chúng.

Bạn có thể phải thử nhiều trang web proxy trước khi tìm được một trang ưng ý. Sẽ có trang đã

bị tường lửa ở Việt Nam chặn, có trang chất lượng kém, tốc độ truy cập rất chậm v.v... Hãy ghi lại địa chỉ trang mà bạn ưng ý, để lần sau tái sử dụng. Hãy nhớ rằng nhiều trang bạn muốn truy cập yêu cầu phải bật Javascript và cookies để có thể sử dụng đầy đủ các tính năng của trang. Do đó, nếu gặp vấn đề với hiển thị hoặc đăng nhập, NHỚ kiểm tra xem mình đã cho phép Javascript và cookies chưa nhé!

Lợi thế của web proxy là thuận tiện, không phải cài đặt gì, có thể dùng để vượt tường lửa tại các tiệm net. Nhược điểm là phải khá kiên nhẫn mới tìm được một trang ưng ý.

Phần I.B: Sử dụng TOR để vượt tường lửa

Dự án The Onion Router (TOR) [3] cung cấp miễn phí công cụ để vượt tường lửa và giúp trao đổi thông tin một cách bảo mật. Bạn có thể cài đặt các công cụ này trong máy tính cá nhân, hoặc cho chúng vào ổ USB và sử dụng ở nơi công cộng mà không phải cài đặt. Sau đây là hướng dẫn sử dụng cho cả hai loại:

CÀI ĐẶT VÀO MÁY TÍNH CÁ NHÂN

Tải xuống phiên bản mới nhất của TOR ở trang sau:

==>> http://www.torproject.org/easy-download.html.en [4]

Có thể hệ thống firewall ở Việt Nam đã chặn trang này, do đó chúng tôi sẽ cung cấp các phiên bản mới nhất ngay trên Dân Luận. Nếu bạn đã có Firefox trong máy, bạn chỉ cần tải gói có chứa Tor, Vidalia và Privoxy xuống máy để cài:

==>> Bộ cài gồm Tor, Vadilia và Privoxy [5]

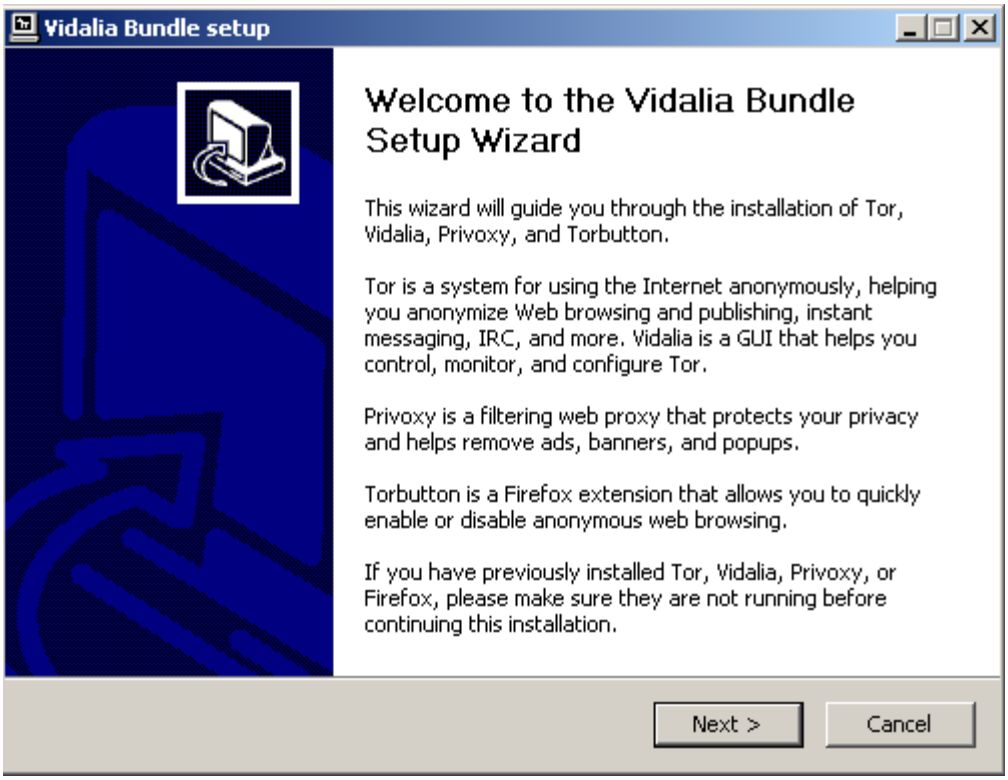
Nếu bạn chưa có Firefox, bạn có thể tải gói có chứa Tor, Vidalia, Privoxy và Firefox:

==>> Bộ cài gồm Tor, Vidalia, Privoxy và Firefox [6]

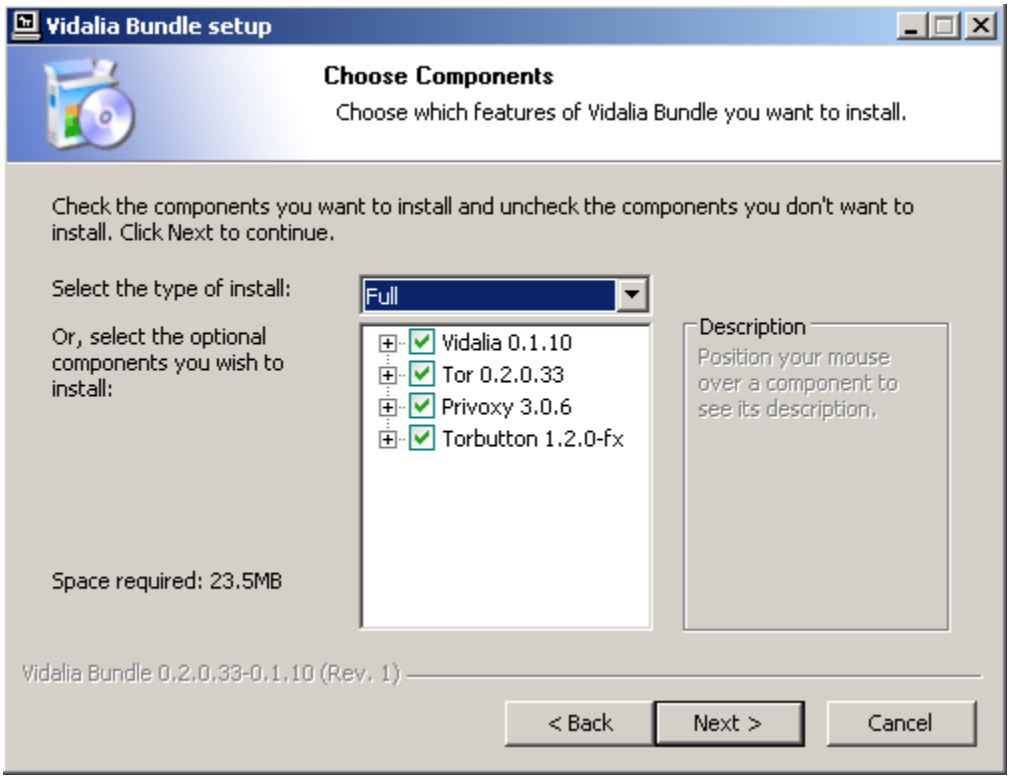
Chú ý: Firefox trong bản này KHÁC MỘT CHÚT với Firefox tải thẳng xuống từ trang chủ của Firefox - tôi không biết khác nhau ở chỗ nào, nhưng nếu bạn nghi ngại thì tự cài Firefox và dùng bản Tor, Vadilia và Privoxy không có Firefox.

Những cái tên Tor, Vadilia và Privoxy có nghĩa là gì? Tor là hạt nhân, là chương trình cơ bản giúp bạn vượt tường lửa và bảo mật thông tin. Nhưng Tor không có giao diện - muốn điều khiển, thay đổi các tùy chọn của nó, bạn cần có Vadilia. Còn Privoxy đưa thêm một số tính năng bảo mật vào Tor, bao gồm khả năng xóa cookies, xóa các banner quảng cáo v.v... ở trang web mà bạn viếng thăm. Bạn có thể cần thêm Torbutton, là một chương trình nhỏ bổ sung cho Firefox, cho phép bạn kiểm soát Tor ngay tại trình duyệt Firefox. Nói tóm lại là bạn cần có 4 chương trình này để duyệt web một cách an toàn và tiện dụng.

Sau khi tải xuống, hãy khởi động quá trình cài đặt bằng cách bấm đúp vào tập tin vừa tải xuống. Bạn sẽ thấy màn hình dưới đây:



Bấm "Next", trang kế tiếp sẽ cho bạn quyền lựa chọn cài đặt những chương trình gì. Khuyến nghị cài tất:



Cài đặt xong thì các chương trình bạn vừa cài sẽ được tự khởi động. Nếu bạn đang có trang web mở bằng Firefox trên màn hình, hãy khởi động lại Firefox để Tor có tác dụng. Nếu bạn cài Torbutton, ở thanh trạng thái nằm ở góc dưới màn hình của Firefox sẽ hiện ra chữ "Tor enabled" khi Tor đã khởi động thành công, và trình duyệt Firefox sử dụng Tor để kết nối internet. Nếu thông điệp là "Tor disabled", thì:

- Hoặc là bạn đã yêu cầu Firefox không dùng Tor: bạn làm điều này (tạm tắt Tor) khi truy cập các trang không bị firewall để đạt tốc độ tối ưu. Để yêu cầu Firefox dùng Tor, hãy bấm chuột (một lần) vào chữ "Tor Disabled" màu đỏ. Nếu chữ này chuyển sang "Tor Enabled" màu xanh, bạn có thể bắt đầu truy cập các trang web đã bị Firewall bằng Tor.
- Nếu bước trên không thành công, hãy kiểm tra xem Tor đã chạy chưa. Hãy mở chương trình Vadalia và bấm vào nút "Start Tor". Khi thấy hình củ hành màu xanh lục với dòng chữ "Connected to Tor Network", khi đó Tor đã chạy và kết nối thành công với các đơn vị Tor khác ở trên mạng.
- Nếu Tor không chạy, hay là quá trình cài đặt của bạn đã có vấn đề. Hãy cài lại gói chương trình TOR từ đầu.

Màn hình Vidalia, nơi bạn điều khiển các chức năng của Tor

Hãy chú ý xem Vidalia và Privoxy có chạy không, bằng cách nhìn xuống thanh Taskbar của Windows:

DÙNG TOR TỪ USB MÀ KHÔNG CẦN CÀI ĐẶT

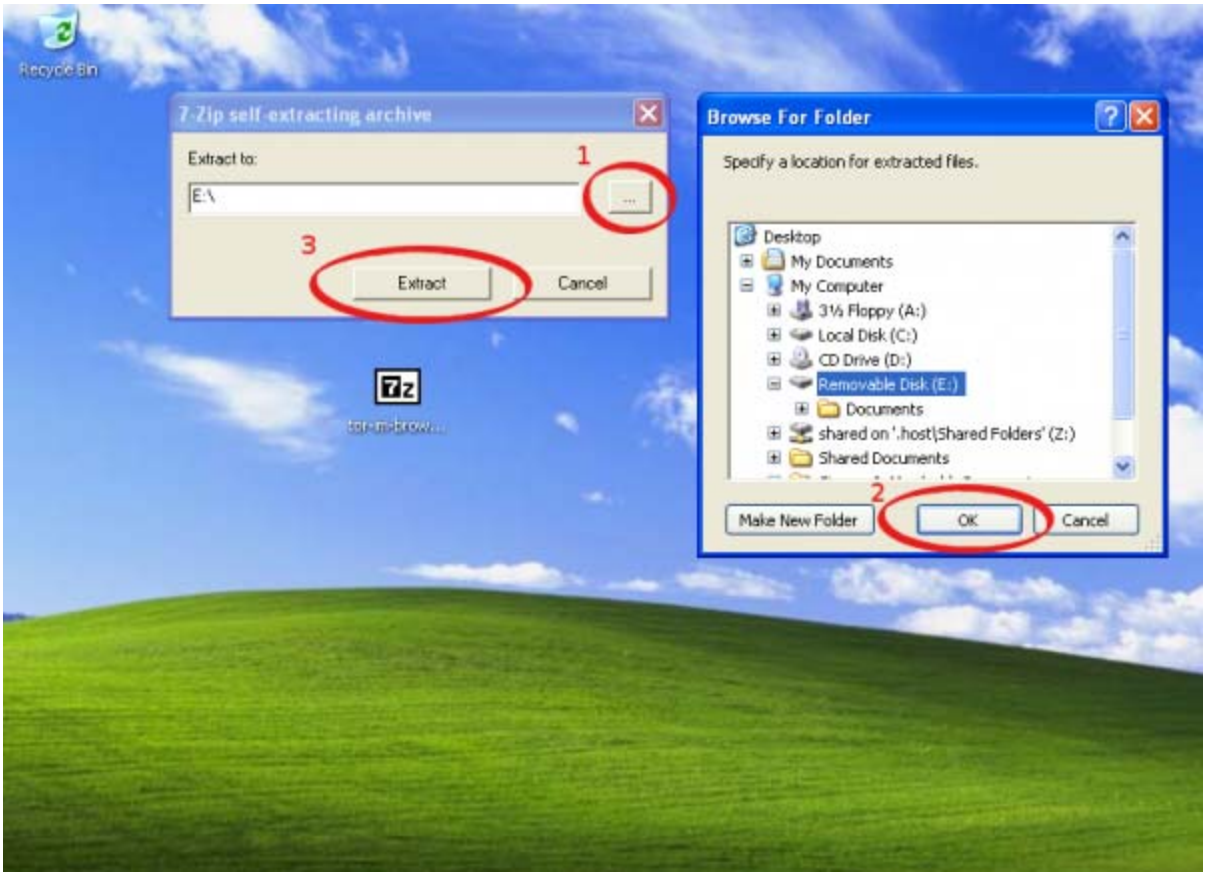
Tải xuống bộ cài Tor có tên là "Zero Install Bundle for Windows" ở trang sau đây:

==>> http://www.torproject.org/easy-download.html.en [4]

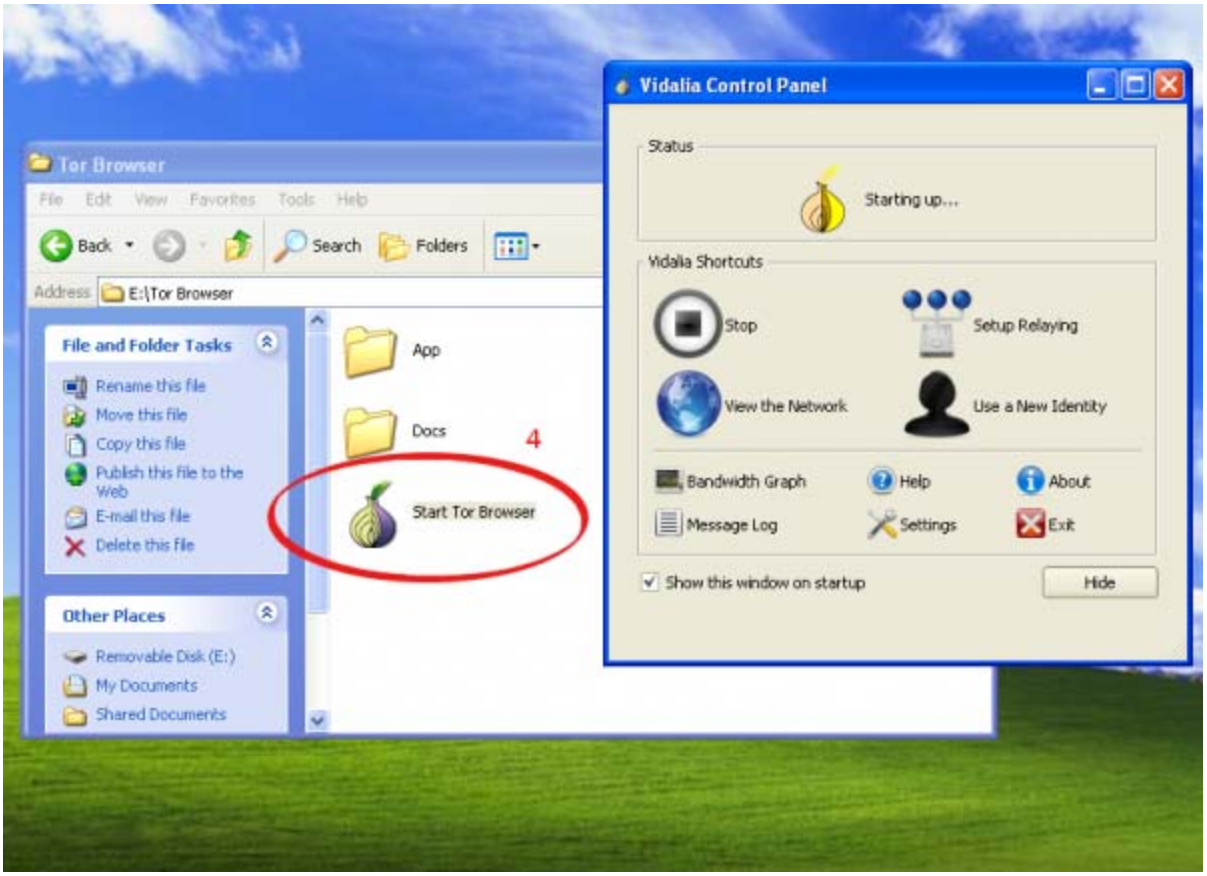
Hoặc tải xuống từ Dân Luận:

==>> Bộ cài Tor không cần cài đặt [7]

Sau khi tải xuống, hãy nháy đúp vào tập tin vừa tải để giải nén (extract) toàn bộ chương trình Tor + Vidalia + Privoxy + Firefox ra một thư mục nào đó:



Giải nén xong, mở thư mục mà bạn vừa giải nén bộ Tor vào, tìm chương trình có tên "Start Tor Browser" và chạy chương trình này:



Vadilia sẽ được khởi động, Tor sẽ được khởi động, và nếu mọi việc đều ổn thỏa, Firefox sẽ tự động khởi động sau đó. Chỉ những trang web bạn duyệt bằng Firefox đi kèm trong bộ Tor nói trên mới được Tor bảo vệ, các trình duyệt khác như Internet Explorer sẽ không bị ảnh hưởng bởi Tor. Hãy kiểm tra để thấy chữ "Tor Enabled" màu xanh lục xuất hiện phía dưới thanh trạng thái của Firefox.

Duyệt trang xong, đóng Firefox. Các thông tin truy cập của bạn trên Firefox sẽ tự động được xóa bỏ, để đảm bảo an ninh.

> **Chú ý:** Bạn có thể dùng một gói Tor không cần cài khác dùng trình duyệt Opera có tên là OperaTor. Tải xuống ở địa chỉ sau:
>
> ==>> http://archetwist.com/opera/operator [8]
>
> ==>> http://operator.pbwiki.com/f/OperaTor-3.3.zip [9]
>
> ==>> http://files.myopera.com/archetwist/operator/OperaTor-3.3.zip [10]
>
> ==>> http://one.xthost.info/archetwist/operator/OperaTor-3.2.zip [11]
>
> hoặc link trên Dân Luận:
>
> ==>> http://danluan.org/files/tor/OperaTor-3.3.zip [12]
>
> Chỉ cần tải ra một thư mục nào đó, và chạy tập tin có tên OperaTor.exe là bạn có thể bắt đầu duyệt web vượt firewall được rồi.

Ưu điểm của Tor là bảo mật cao: Thông tin giữa các trạm trung chuyển của mạng Tor được bảo mật, và do đó nếu ai đó muốn nghe lén thông tin bạn trao đổi qua Tor sẽ gặp khó khăn. Tor cũng giúp bạn che dấu địa chỉ IP thực của mình, bạn có thể truy cập các trang web mà người ta không truy ngược lại được bạn là ai. Nhược điểm là cài đặt vất vả - nhưng nếu bạn đã thử dùng Tor, lợi ích mà nó đem lại là rất lớn.

Phần I.C: Sử dụng UltraSurf hay FreeGate để vượt tường lửa

Chương trình UltraSurf

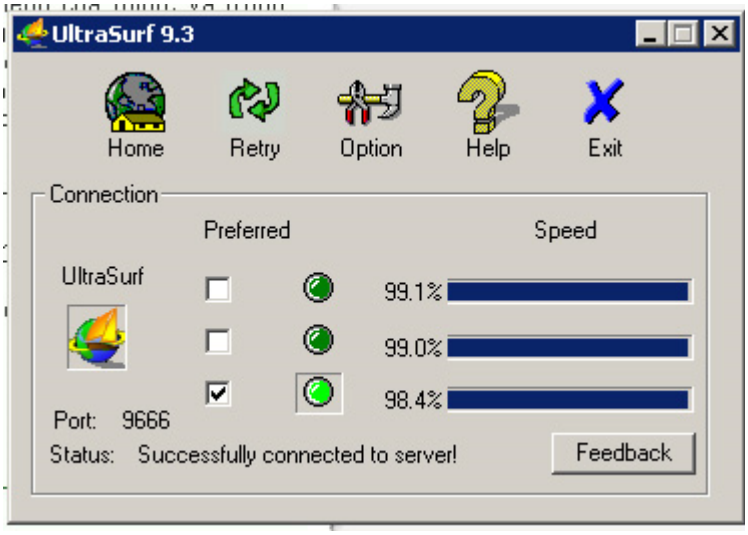
UltraSurf là phần mềm miễn phí nổi tiếng chuyên cho vượt tường lửa. Bạn có thể tải xuống phần mềm này ở trang sau:

==>> http://www.ultrareach.com/download_en.htm [13]

Hoặc tải xuống từ Dân Luận (phiên bản 9.3):

==>> http://danluan.org/files/tor/u93.zip [14]

Chỉ cần gỡ nén, chạy tập tin có tên u.exe, UltraSurf sẽ khởi động (xem hình vẽ). Có thể chọn 1 server khác trong 3 server, nếu bạn thấy kết nối hiện tại chậm chạp hoặc tỏ ra có vấn đề. Nhấn vào một trong 3 ô vuông (checkbox) ở cửa sổ UltraSurf để chuyển server. UltraSurf sử dụng Internet Explorer như trình duyệt mặc định của mình, khi nó khởi động, nó sẽ mở một cửa sổ Internet Explorer để bạn duyệt web.



Cửa sổ chính của UltraSurf

Nếu bạn muốn dùng Firefox, bạn phải tải xuống và cài một chương trình bổ sung nhỏ cho Firefox:

==>> http://www.ultrareach.com/downloads/ultrasurf/wjbutton_en.zip [15]

Hoặc dùng tải xuống từ Dân Luận:

==>> http://danluan.org/files/tor/wjbutton_en.zip [16]

Gỡ nén, mở cửa sổ Firefox và kéo tập tin có tên wjbutton_en.xpi vào trong cửa sổ Firefox để cài

chương trình bổ xung này. Sau đó đóng tất cả các cửa sổ Firefox và mở lại (restart).

Biểu tượng UltraSurf màu xám có nghĩa là UltraSurf đang bị tắt, ngược lại biểu tượng màu vàng sáng là UltraSurf đang bật vào bảo vệ bạn. Bấm vào biểu tượng để bật tắt chức năng vượt tường lửa và che dấu IP bằng UltraSurf.

Chương trình FreeGate

Chương trình này cũng tương tự như UltraSurf, chỉ cần tải về và chạy là nó sẽ tự động mở Internet Explorer để giúp bạn truy cập tới các trang bình thường bị tường lửa.

Tải xuống ở đây (trực tiếp hoặc qua link của Dân Luận):

==>> http://us.dongtaiwang.com/loc/download_en.php [17]

==>> http://danluan.org/files/tor/fg679p3df.exe [18]

Màn hình sau khi chạy FreeGate

Ngoài UltraSurf và FreeGate, nếu cần, bạn có thể tự tìm hiểu và cài đặt các chương trình vượt firewall sau đây:

- JAP: http://anon.inf.tu-dresden.de/index_en.html [19]

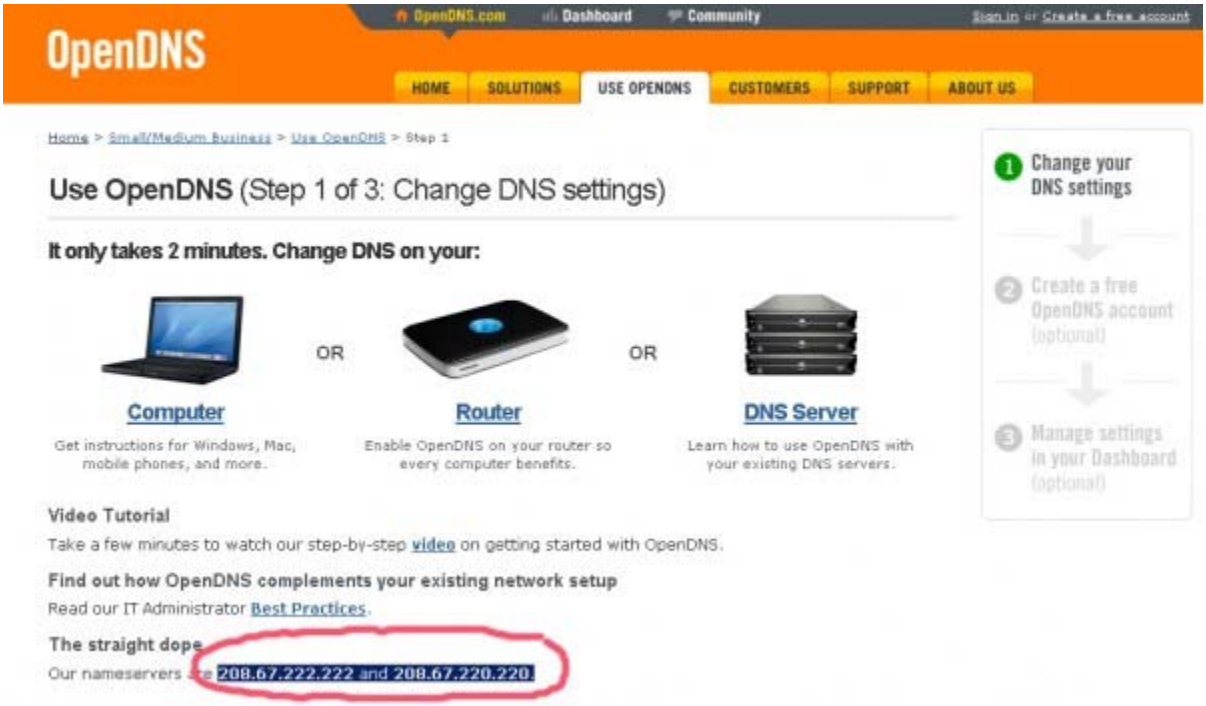
- Hopster: http://www.hopster.com/ [20]

- Your Freedom: http://www.your-freedom.net/ [21]

Phần I.D: Vượt tường lửa bằng OpenDNS

Theo thông tin của độc giả từ trong nước, dịch vụ Internet của FPT không dùng tường lửa chặn IP, mà chỉ thiết lập để DNS server của họ từ chối trả về địa chỉ IP của trang web bị chặn (xem phần 2: Tường lửa là gì? để tìm hiểu cụ thể hơn về sự khác biệt giữa hai loại tường lửa này). Như thế, chỉ cần dùng DNS server khác, thay vì dùng DNS server cung cấp bởi FPT, là người sử dụng dịch vụ Internet của FPT đã có thể truy cập vào những trang bị cấm rồi.

Để tìm DNS server thay thế, bạn hãy gõ vào Google từ khóa "public DNS server". Google sẽ trả về danh sách các trang web có địa chỉ IP của các DNS server miễn phí mà bạn có thể dùng. Tuy nhiên, một trang hay được độc giả trong nước sử dụng là OpenDNS (tại địa chỉ: https://www.opendns.com/smb/start [22]).



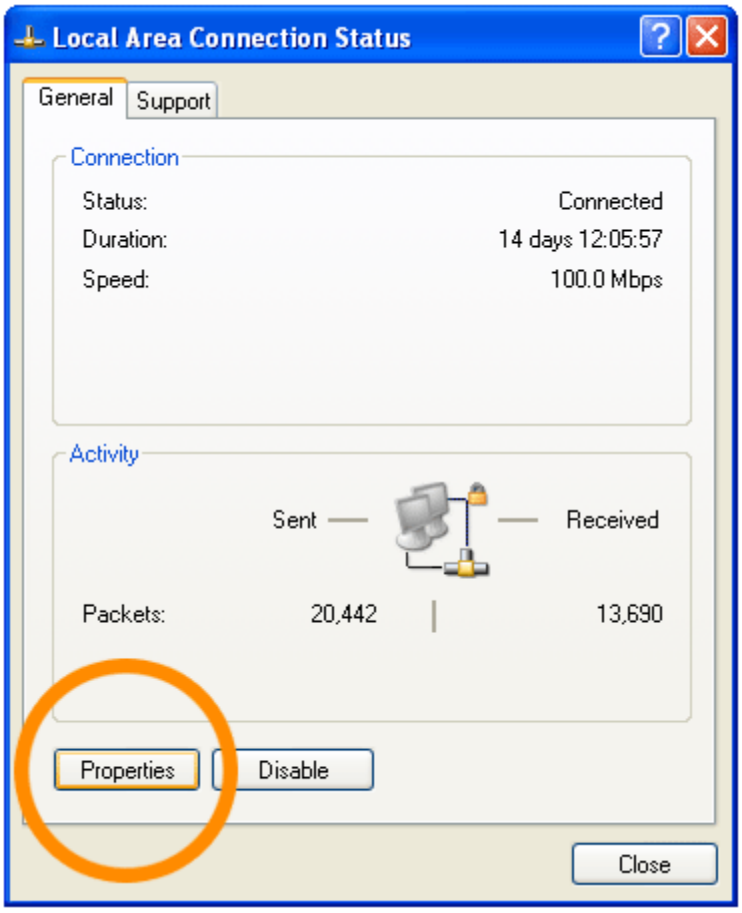
Trang OpenDNS.com, phần đánh dấu chính là địa chỉ DNS server mà bạn cần dùng

Thiết lập DNS server mới cho máy tính của bạn

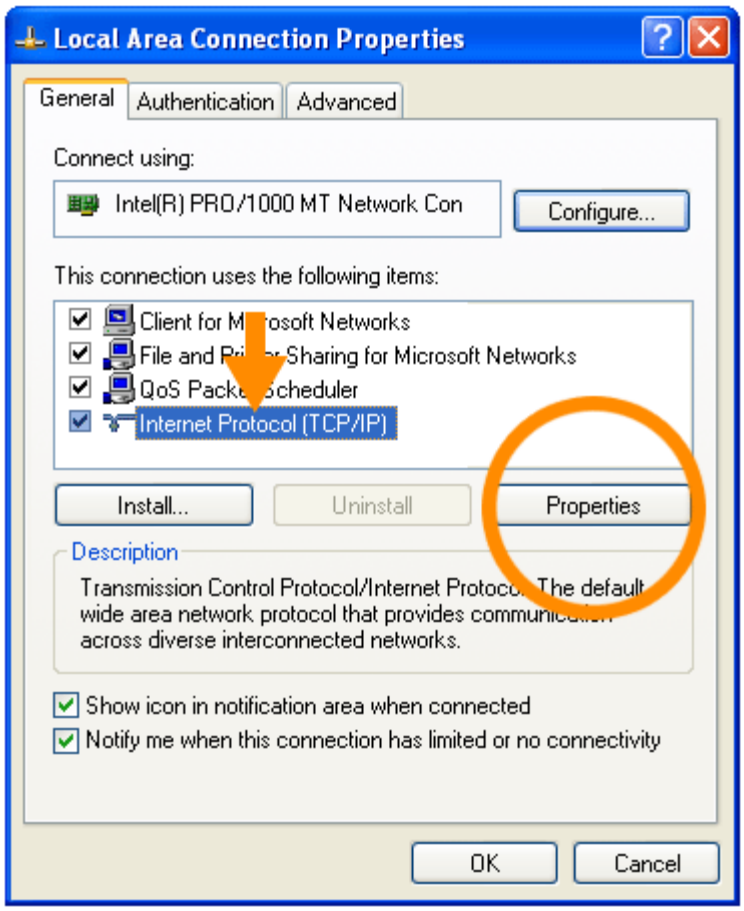
Giả sử địa chỉ IP của DNS server mà bạn muốn dùng là **208.67.222.222** và **208.67.220.220** (tìm qua Google như hướng dẫn nói trên, hoặc vào trang OpenDNS để đọc).

Đối với Windows XP

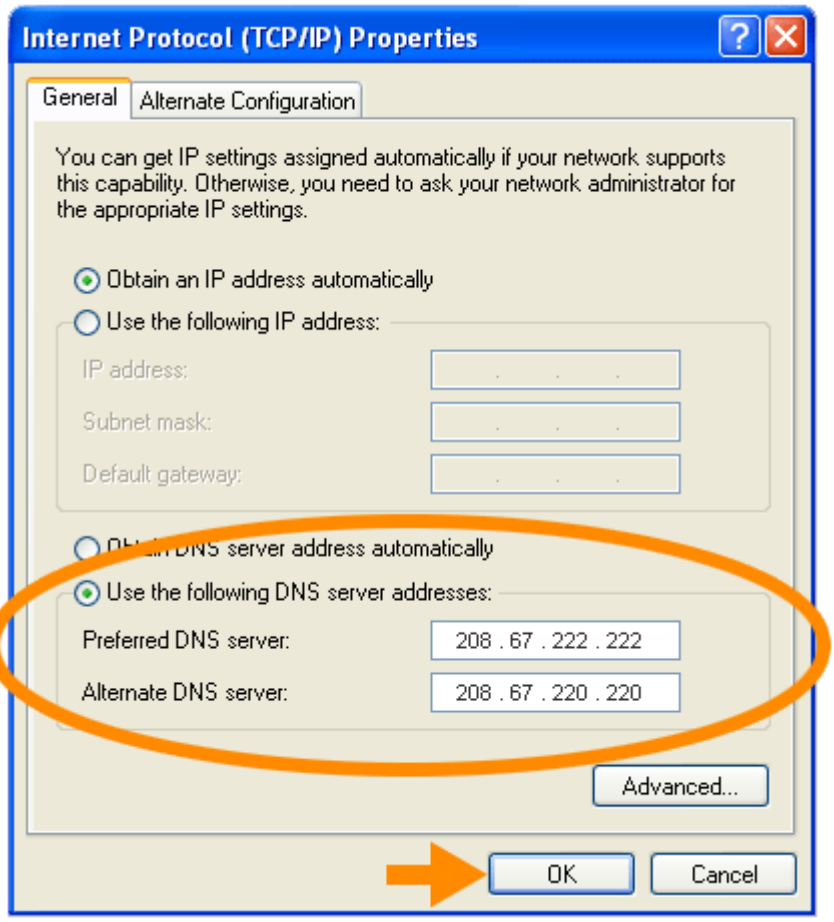
Mở Control Panel, chọn Network Connections, chọn tiếp Local Area Connection. Cửa sổ dưới đây sẽ mở ra để bạn chọn tiếp Properties:



Chọn tiếp mục "Internet Protocol (TCP/IP)" rồi Properties:



Trong cửa sổ mới mở ra, điền hai địa chỉ IP nói trên (cũng có thể là địa chỉ khác, nếu bạn chọn DNS server từ một trang khác) vào và ấn Ok:

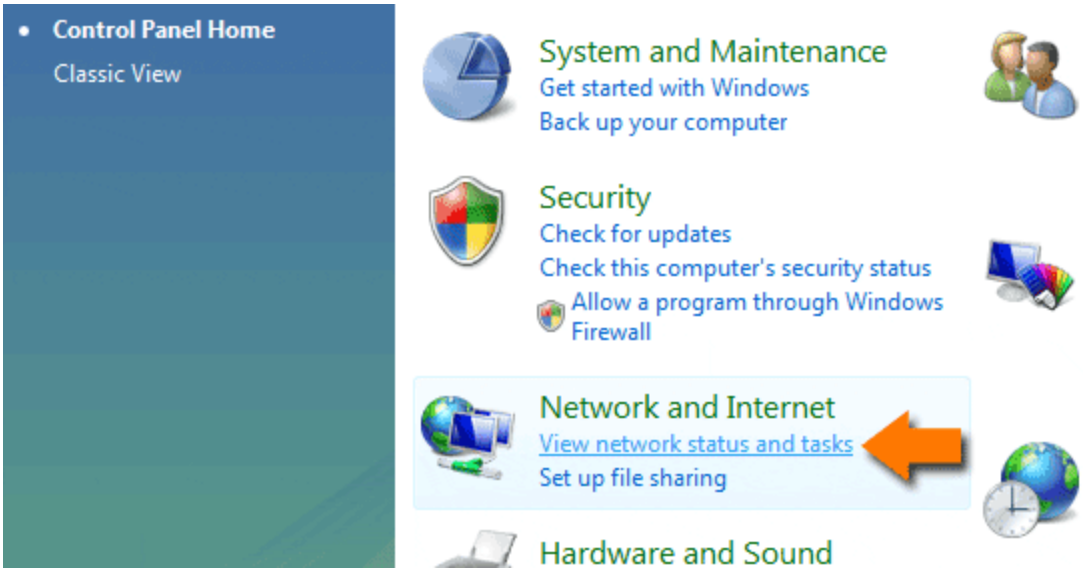


Nếu bạn cẩn thận, hãy ghi lại địa chỉ DNS server cũ (của FPT cung cấp) và cất đi, để nếu cần lặp lại các bước nói trên để khôi phục lại chúng.

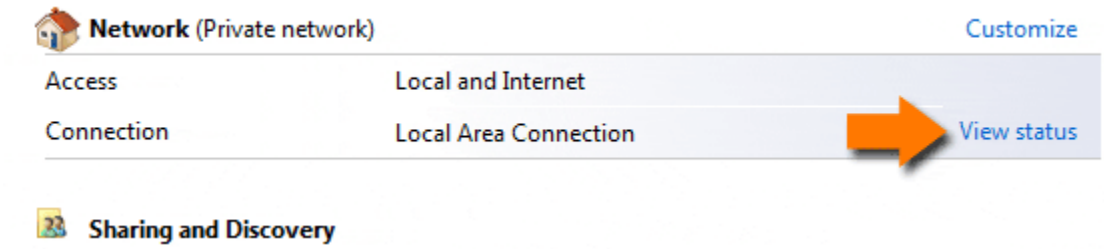
Đối với Vista

Tìm và mở "Control Panel":

Chọn "Network and Internet":

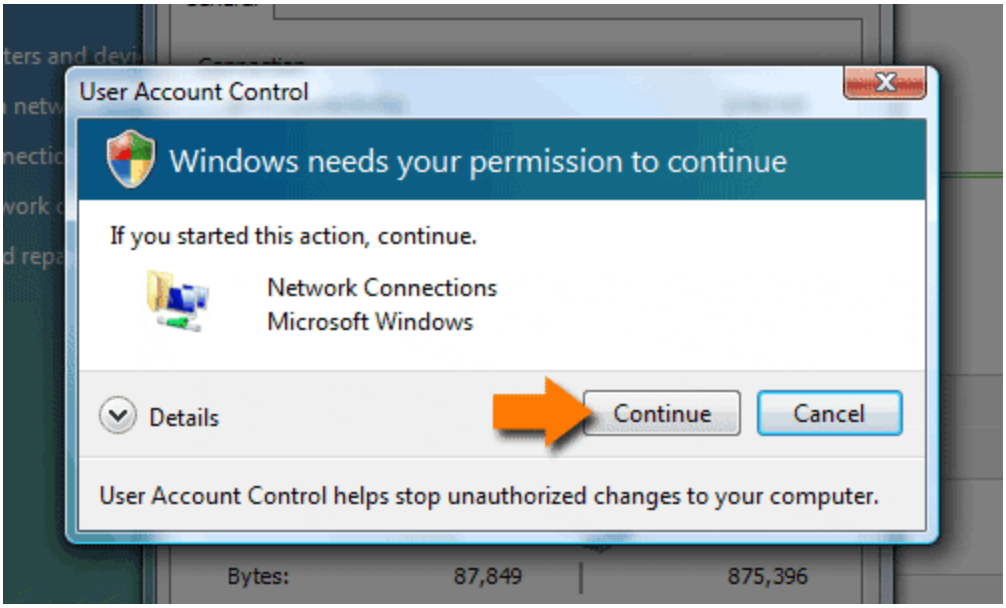


Chọn "View Status":

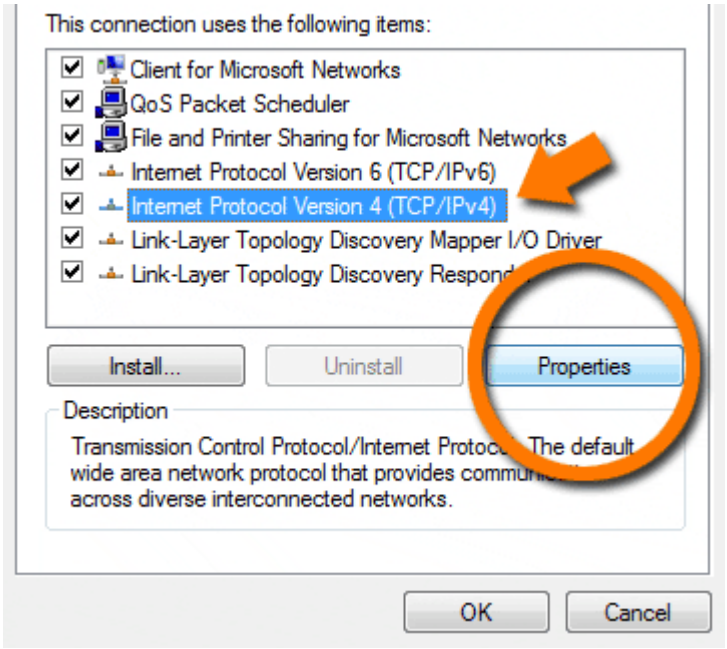


Nhấn vào nút Properties:

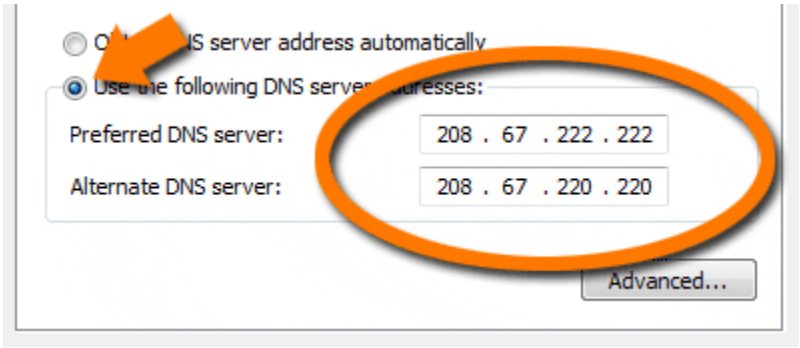
Windows Vista có thể yêu cầu bạn chấp nhận việc thay đổi thông số:



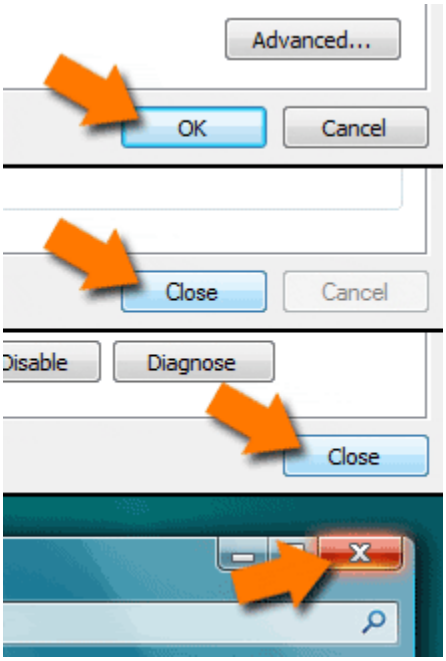
Chọn "Internet Protocol Version 4 (TCP/IPv4)", rồi nhấn vào nút Properties:



Nhấn vào "Use the following DNS server addresses:", và gõ vào địa chỉ DNS server bạn chọn trong mục "Preferred DNS server" và "Alternate DNS server":



Nhấn một đống OK để đóng các cửa sổ và ghi lại thay đổi:



Lưu ý rằng cách sử dụng DNS server mới thay vì cái mà nhà cung cấp dịch vụ Internet đưa cho bạn chỉ giúp bạn vượt firewall khi nhà cung cấp dịch vụ chặn các trang bằng DNS. Nếu họ chặn bằng IP thì cách làm này của bạn không có tác dụng. Bạn sẽ phải dùng các phương pháp nêu ở phần A, B, C để vượt tường lửa.

Thay đổi DNS Server cũng không giúp bạn bảo vệ IP của mình. Máy bạn sẽ truy cập thẳng tới những trang web bị cấm, và người ta có thể dò được IP của bạn. Do vậy, hãy dùng thêm chương trình khác để bảo mật đường truyền và giấu IP, nếu bạn lo lắng cho sự an toàn của mình.

Nếu bạn chỉ cần vào một vài trang web bị cấm, và bạn biết địa chỉ IP của các trang web đó, bạn có thể làm theo hướng dẫn sau đây để máy tính của bạn tự động đổi tên của các trang web đó thành IP.

Ví dụ, www.danluan.org [23] nằm tại địa chỉ 74.55.40.99. Hãy đăng nhập vào máy tính của bạn với account có quyền Administrator. Dùng Notepade mở tập tin có tên là "hosts" nằm tại "C:\WINDOWS\system32\drivers\etc". Thêm hai dòng sau đây vào phần cuối của tập tin này:

74.55.40.99 http://www.danluan.org [23]
74.55.40.99 danluan.org

Lưu tập tin lại và từ nay khi bạn mở trang www.danluan.org [23], máy sẽ tự động liên lạc tới địa chỉ IP 74.55.40.99.

Điểm dở của phương pháp này là nếu địa chỉ IP của Dân Luận thay đổi thì bạn sẽ không còn kết nối được với Dân Luận nữa. Khi đó, bạn sẽ phải mở tập tin nói trên, cập nhật địa chỉ IP mới hoặc xóa hai dòng cuối đi để trả lại tình trạng ban đầu.

Phần II: Tường lửa là gì

Mục đích của bài viết này là giúp bạn trả lời ba câu hỏi: "Tường lửa là gì?", "Nó hoạt động ra sao?", "Làm sao có thể vượt qua được tường lửa?".

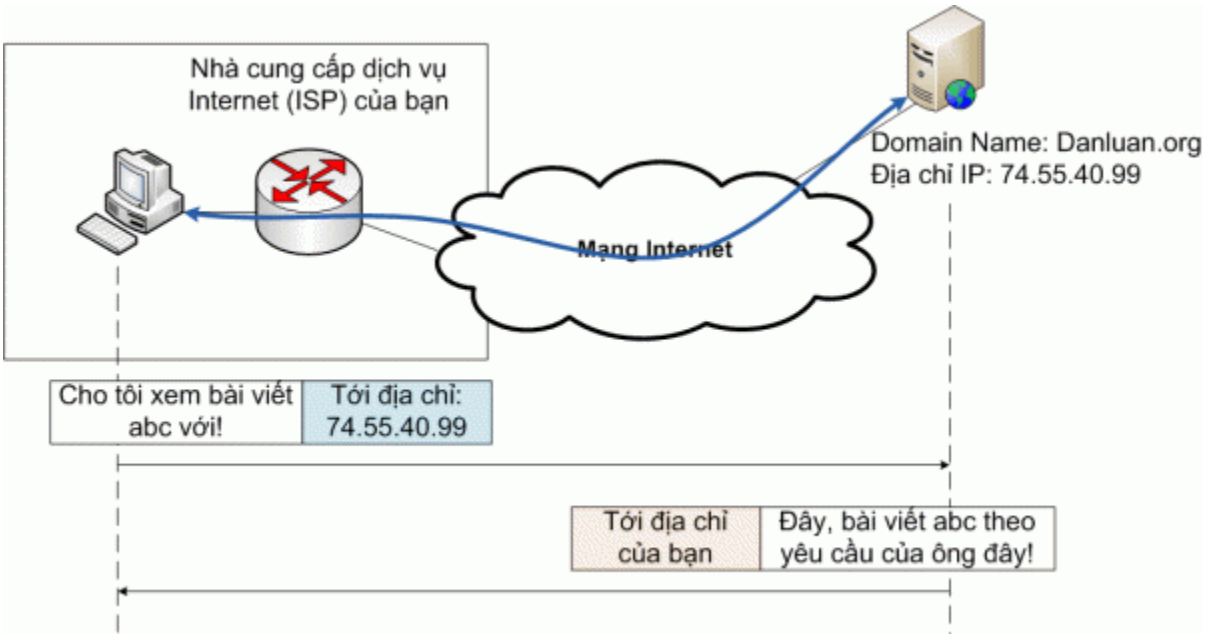
Chúng tôi đoán rằng, khi bạn quyết định đọc bài viết này, tức là bạn không phải là người có hiểu biết cơ bản về hệ thống mạng Internet nói chung, và tường lửa nói riêng. Do đó, chúng tôi sẽ cố gắng giải thích bằng hình tượng và đơn giản hóa vấn đề để bạn dễ nắm bắt hơn. Thành thật xin lỗi nếu các bạn cảm thấy bài viết quá sơ đẳng...

A. Kiến thức cơ bản

Mạng Internet được xây dựng dựa trên một bộ luật, hay tập hợp của các quy tắc chung, có tên là Giao thức Internet (viết tắt là IP). Giao thức chung này đảm bảo rằng các thiết bị Internet có thể "nói chuyện" được với nhau, và hệ thống mạng Internet ở Mỹ có thể giao tiếp được với hệ thống mạng Internet ở Việt Nam, ở Lào, ở Campuchia v.v... mà không gặp trở ngại gì.

Để giao tiếp được với nhau, mỗi thiết bị trên mạng được đánh một số riêng biệt, gọi là địa chỉ IP. Địa chỉ IP có tác dụng giống như số nhà: khi bạn muốn gửi thông tin tới anh A hoặc chị B, bạn phải viết địa chỉ của anh A hoặc chị B ngoài phong bì. Nhìn vào địa chỉ đó, bưu tá sẽ biết được phải chuyển thư của bạn như thế nào.

Quá trình chuyển yêu cầu đọc một trang web và trả lời của server diễn ra giống như ở Hình 1. Máy tính của bạn gửi yêu cầu tới nhà cung cấp dịch vụ ISP của bạn (giống bỏ thư vào thùng thư), nhà cung cấp sẽ đọc địa chỉ trên phong bì, và chuyển lá thư tới đúng người nhận là server Danluan.org.

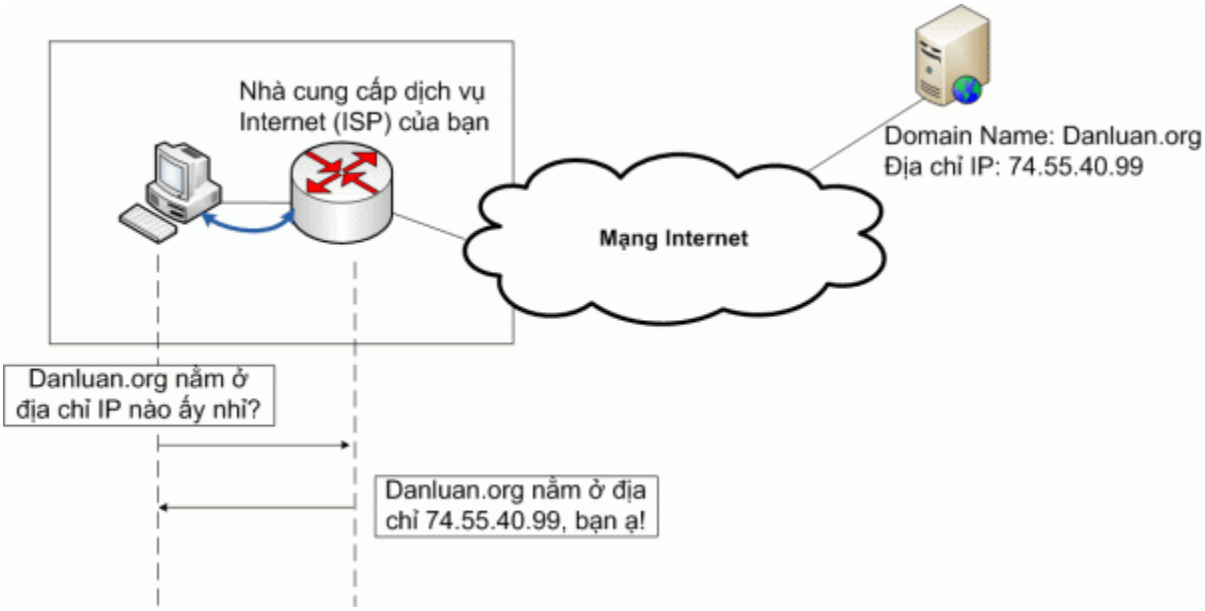


Hình 1: Máy tính của bạn muốn xem một trang web từ Danluan.org

Một điểm cần chú ý là địa chỉ IP dưới dạng số rất thích hợp với máy tính, nhưng rất khó nhớ đối với con người. Hãy thử tương tượng bạn muốn đọc tin tức từ CNN hoặc BBC, mà lại phải nhớ CCN là 157.166.224.25, BBC là 212.58.253.68 thì quả là điên cái đầu. Do đó, người ta đã đưa ra cái gọi là Domain Name System (DNS), để đặt tên cho các địa chỉ IP. Từ tên miền, dễ

nhớ và gần gũi với con người, bạn có thể tìm ra địa chỉ IP của một trang web.

Như vậy, trước khi gửi bất cứ thứ gì tới Danluan.org, máy tính của bạn sẽ phải đi hỏi, trong đa số trường hợp là hỏi chính ISP của bạn, xem danluan.org tương ứng với địa chỉ IP nào, như trong Hình 2.



Hình 2: Tra địa chỉ IP của tên miền Danluan.org

Ở trên là trường hợp ISP của bạn không lắp đặt tường lửa. Chuyện gì xảy ra nếu ISP của bạn lắp tường lửa, và nó quyết định chặn trang Danluan.org?

B. Tường lửa là gì?

Tường lửa (firewall) là hệ thống gồm cả phần cứng và phần mềm làm nhiệm vụ ngăn chặn các truy nhập "không mong muốn" từ trong ra bên ngoài hoặc từ bên ngoài vào trong. Tường lửa thường được đặt ở cổng giao tiếp giữa hai hệ thống mạng, ví dụ giữa mạng trong nước và mạng quốc tế, giữa mạng nội bộ của doanh nghiệp và mạng Internet công cộng v.v... để lọc thông tin theo các nguyên tắc được định trước.

Các công ty lớn, các trung tâm nghiên cứu quan trọng cần tường lửa để loại bỏ các cuộc tấn công của tin tặc từ bên ngoài vào, hoặc để ngăn nhân viên của mình không gửi thông tin mật ra ngoài, hoặc đơn giản hơn là không cho nhân viên sử dụng dịch vụ chat hay xem Youtube trong giờ làm việc. Ở Việt Nam và Trung Quốc, hệ thống tường lửa còn được dùng để ngăn cản người dân đọc các thông tin liên quan đến tự do, dân chủ, đa đảng hay về các bê bối của chính quyền, những thông tin mà theo chính quyền, là có hại tới họ.

Có nhiều phương pháp lọc thông tin để ngăn cản người sử dụng Internet truy cập dịch vụ mà mình mong muốn, ví dụ:

1) Lọc theo tên miền:

Theo độc giả trong nước cho biết, thì FPT sử dụng cách lọc này. Khi máy của bạn hỏi FPT rằng danluan.org nằm ở địa chỉ IP nào, thì FPT sẽ từ chối trả lời, nếu trang danluan.org nằm trong danh sách "bị cấm". Nói một cách khác, danluan.org không nằm trong cuốn "danh bạ điện thoại" của FPT.

Phương pháp này có ưu điểm là... gọn và rẻ. Số lần người sử dụng hỏi DNS server mỗi ngày ít hơn nhiều so với số yêu cầu đọc trang web, do đó số lần phải đọc, kiểm tra xem trang này có bị cấm hay không, sẽ ít hơn.

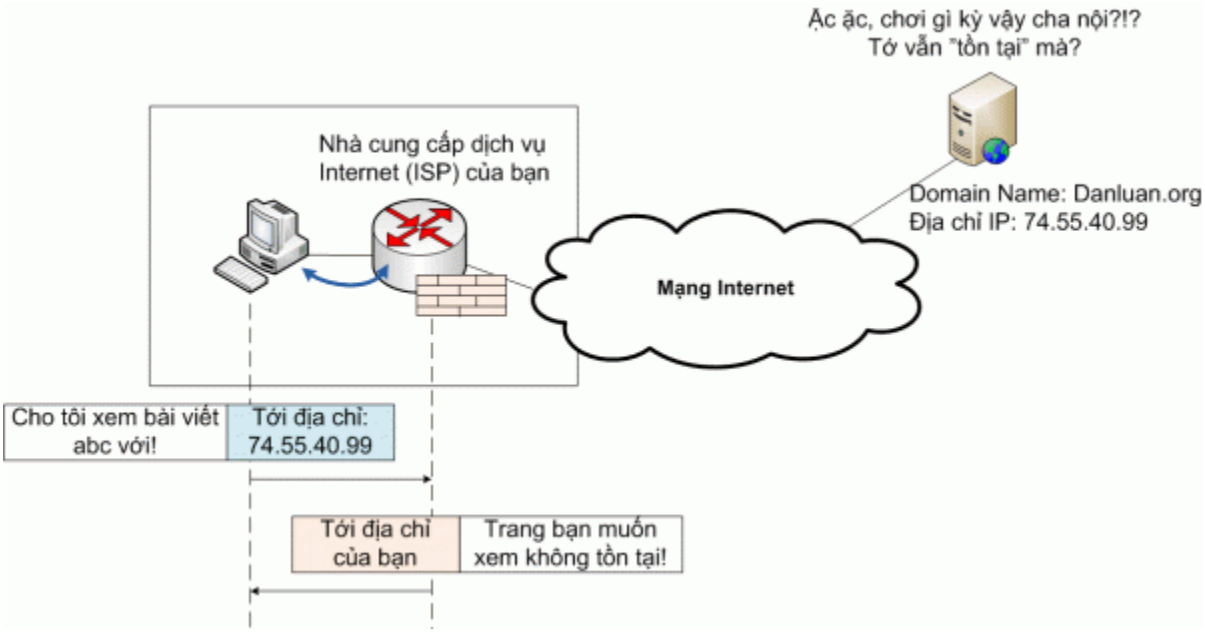
Ngược lại, đây là loại tường lửa dễ bị phá nhất. Vì nó chỉ ngăn cản truy cập dựa theo tên miền, nếu người sử dụng biết địa chỉ IP, họ có thể dùng trực tiếp địa chỉ IP để truy cập tới trang muốn xem mà không gặp trở ngại nào. Ví dụ, thay vì - http://danluan.org/node/285 [24] -, bạn có thể đọc bài viết này bằng - http://74.55.40.99/node/285 [25] - với FPT.

Đôi khi một trang web có nhiều tên miền khác nhau, chẳng hạn danluan.org hoặc www.danluan.org [23] hoặc danluan.info (hehe, cái này không tồn tại), mà FPT quên không chặn hết các tên miền, bạn có thể vào được các trang web cấm bằng sử dụng tên miền chưa bị chặn. Đã có người cho biết, chỉ cần bỏ www đi là có thể truy cập một số trang bị cấm ngon lành ==> FPT quên không đưa các cái tên đó vào danh sách "đen" :)

Hoặc chỉ cần người sử dụng kiếm cho mình một cuốn danh bạ điện thoại "ngon lành" để thay thế cho cuốn danh bạ "bị kiểm duyệt" kia (xem ở đây "Phần I.D: Vượt tường lửa bằng OpenDNS [26]"), để có thể tự tra được danluan.org nằm ở địa chỉ IP nào, mà không cần thông qua ISP, là họ đã vượt được tường lửa kiểu đơn giản này.

2) Lọc theo địa chỉ IP

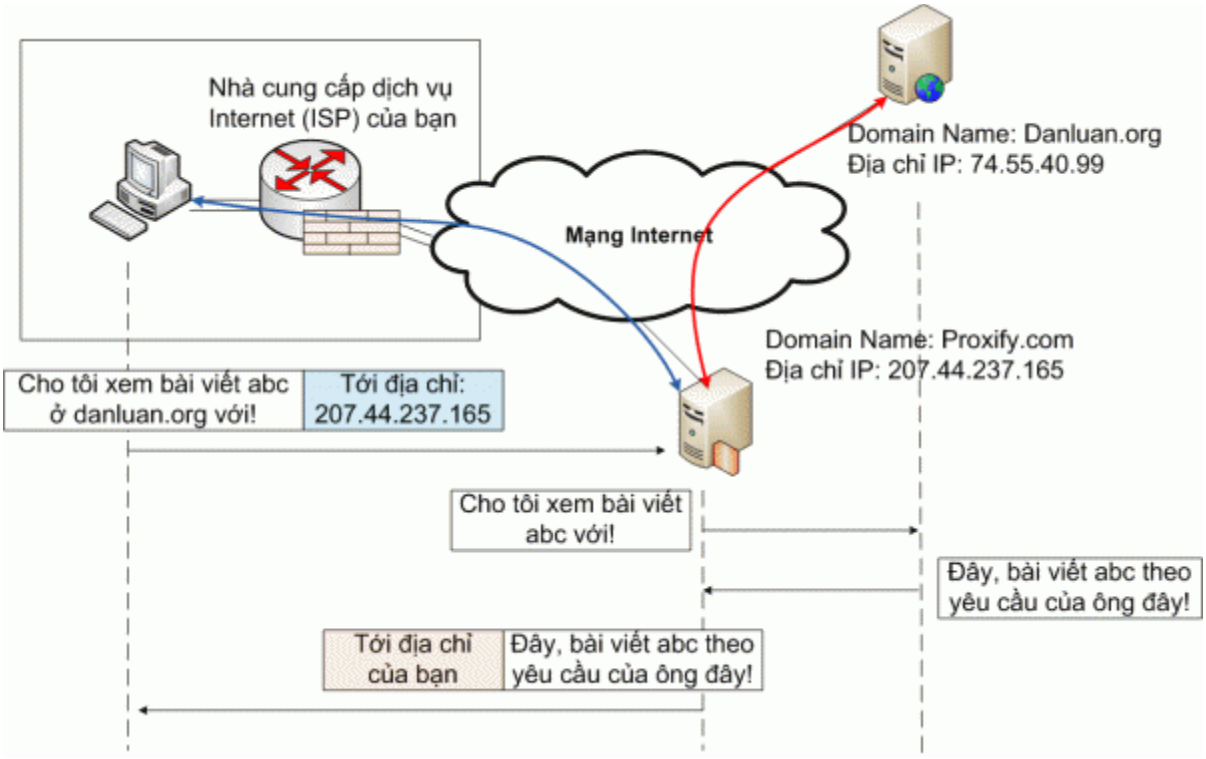
Loại tường lửa này chặt hơn tường lửa nói ở phần trên. Giả sử bạn đã tra được danluan.org nằm ở địa chỉ IP là 74.55.40.99, và bạn gửi yêu cầu đọc trang abc tới địa chỉ vừa tra. Tường lửa sẽ đọc gói tin, kiểm tra địa chỉ IP, nếu thấy nằm trong danh sách bị cấm, nó sẽ trả về thông báo: "Trang web không tồn tại" (xem Hình 3). Tường lửa kiểu này giống như người đưa thư, sau khi đọc địa chỉ thư của bạn, thấy có trong danh sách bị cấm, sẽ vứt thư của bạn đi mà không chuyển tới đúng địa chỉ.



Hình 3: Tường lửa lọc IP chặn yêu cầu của người sử dụng dựa trên địa chỉ IP.

Biện pháp vượt tường lửa lọc IP là sử dụng proxy server (xem Hình 4). Proxy server được định nghĩa là máy chủ cung cấp dịch vụ "đi gom hàng" hộ cho các khách của mình. Thay vì gửi thẳng yêu cầu xem bài viết abc tới danluan.org (bị tường lửa lọc ngay lập tức), bạn hãy gửi yêu

cầu đó tới proxy server, và proxy server sẽ đi tới danluan.org lấy tin, và gửi ngược lại cho bạn. Vì tên và địa chỉ IP của proxy server "chưa" nằm trong danh sách đen, do đó tường lửa sẽ chấp nhận cho bạn kết nối tới proxy server nằm bên ngoài tầm kiểm soát của tường lửa.



Hình 4: Vai trò của proxy server trong việc vượt tường lửa lọc IP.

Ưu điểm của phương pháp lọc IP này là chặt chẽ hơn, dù bạn có địa chỉ IP của trang cần truy cập thì vẫn không qua được tường lửa như trường hợp tường lửa lọc tên miền. Tuy nhiên, nhược điểm của nó là tốn kém vì phải đầu tư hệ thống xử lý tốc độ cao, đủ để lọc tất cả các gói tin gửi ra Internet.

Lọc IP cũng không phải khó phá. Các phương pháp tìm và cài đặt, sử dụng proxy server để vượt tường lửa lọc IP đã được hướng dẫn ở đây, mời các bạn tham khảo:

- Phần I.A: Dùng web proxy để vượt tường lửa [27]
- Phần I.B: Sử dụng TOR để vượt tường lửa [28]
- Phần I.C: Sử dụng UltraSurf hay FreeGate để vượt tường lửa [29]

C. Một số công cụ mà bạn có thể cần dùng

Dưới đây giới thiệu một số công cụ tra cứu tên miền, địa chỉ IP trên Internet mà có thể hữu ích cho bạn trong tương lai. Chúng tôi không cấp địa chỉ cụ thể, vì các trang web được giới thiệu có thể không còn tồn tại trong tương lai. Nhưng nếu các bạn dùng Google để kiếm theo tên tiếng Anh của công cụ, các bạn sẽ tìm thấy nhiều trang web cung cấp dịch vụ kiểu đó.

- Nếu bạn có tên miền của một trang web, muốn kiểm tra xem địa chỉ IP của trang đó là gì, dùng DNS lookup (gõ vào Google từ khóa "DNS lookup tool" để tìm), ví dụ tại trang:

  http://www.bankes.com/nslookup.htm [30]

- Nếu bạn có tên miền, muốn biết ai là chủ sở hữu của tên miền này, dùng công cụ WHOIS (gõ vào Google từ khóa "Whois").
- Nếu bạn muốn biết một địa chỉ IP nằm ở khu vực nào trên thế giới (Mỹ, Anh, hay Việt Nam), hãy dùng công cụ IP location (gõ vào Google từ khóa "IP location").
- Nếu bạn muốn biết địa chỉ IP CỦA CHÍNH MÌNH là gì, hãy dùng công cụ My IP address (gõ vào Google từ khóa "My IP address").

Bài giảng đến đây là hết, thân ái chào các bạn. Chúc các bạn ứng dụng nó thành công!

firewall tường lửa

Source URL: http://danluan.org/node/244

Links:
[1] http://www.google.com
[2] http://www.proxify.com
[3] http://www.torproject.org
[4] http://www.torproject.org/easy-download.html.en
[5] http://danluan.org/files/tor/vidalia-bundle-0.2.0.33-0.1.10.exe
[6] http://danluan.org/files/tor/tor-browser-1.1.8_en-US.exe
[7] http://danluan.org/files/tor/tor-im-browser-1.1.8_en-US.exe
[8] http://archetwist.com/opera/operator
[9] http://operator.pbwiki.com/f/OperaTor-3.3.zip
[10] http://files.myopera.com/archetwist/operator/OperaTor-3.3.zip
[11] http://one.xthost.info/archetwist/operator/OperaTor-3.2.zip
[12] http://danluan.org/files/tor/OperaTor-3.3.zip
[13] http://www.ultrareach.com/download_en.htm
[14] http://danluan.org/files/tor/u93.zip
[15] http://www.ultrareach.com/downloads/ultrasurf/wjbutton_en.zip
[16] http://danluan.org/files/tor/wjbutton_en.zip
[17] http://us.dongtaiwang.com/loc/download_en.php
[18] http://danluan.org/files/tor/fg679p3df.exe
[19] http://anon.inf.tu-dresden.de/index_en.html
[20] http://www.hopster.com/
[21] http://www.your-freedom.net/
[22] https://www.opendns.com/smb/start
[23] http://www.danluan.org
[24] http://danluan.org/node/285
[25] http://74.55.40.99/node/285
[26] http://danluan.org/node/249
[27] http://danluan.org/node/247
[28] http://danluan.org/node/246
[29] http://danluan.org/node/248
[30] http://www.bankes.com/nslookup.htm