Công ty An ninh mạng Viettel

Báo cáo về Firewall, VPN

Sinh viên: Nguyễn Đan Trường

*MỤC LỤC*

[Chương 1. Firewall Basic 3](#_Toc155616250)

[1. Khái niệm 3](#_Toc155616251)

[2. Các loại Firewall 4](#_Toc155616252)

[3. Thực hành với iptables 7](#_Toc155616253)

[Chương 2. VPN – Virtual Private Network 7](#_Toc155616254)

[1. Khái niệm 7](#_Toc155616255)

[2. Các loại VPN 8](#_Toc155616256)

[a. VPN Site-to-Site 8](#_Toc155616257)

[b. VPN Remote-Access 9](#_Toc155616258)

[c. MPLS VPN 9](#_Toc155616259)

# Firewall Basic

## Khái niệm

Firewall là một hệ thống bảo mật mạng máy tính nhằm hạn chế lưu lượng truy cập internet vào/ra hoặc trong mạng riêng.

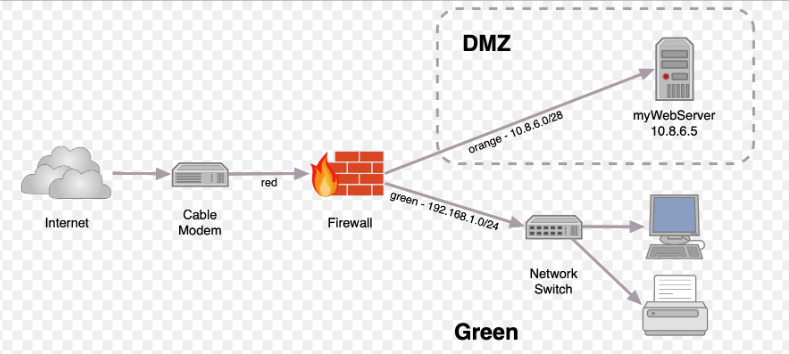
Firewall có thể là phần mềm hoặc phần cứng hoạt động bằng cách chặn hoặc cho phép có chọn lọc các gói dữ liệu. Nó thường nhằm mục đích giúp ngăn chặn hoạt động độc hại và ngăn chặn bất kỳ ai—trong hoặc ngoài mạng riêng—tham gia vào các hoạt động web trái phép.

**Hoạt động của Firewall**

Firewall quyết định lưu lượng mạng nào được phép đi qua và lưu lượng nào được coi là nguy hiểm. Về cơ bản, nó hoạt động bằng cách lọc ra các lưu lượng bất thường và đưa ra hành động đối với chúng.

Các máy tính và thiết bị đầu cuối sử dụng mạng để truy cập Internet hoặc giao tiếp lẫn nhau. Tuy nhiên, trong mạng máy tính sẽ được chia thành các vùng mạng khác nhau để bảo mật và riêng tư. Các phân đoạn mạng cơ bản được chia như sau:

* **External public networks**: thường đề cập đến internet công cộng.
* **Internal private networks**: là mạng nội bộ công ty.
* **Perimeter networks**: là mạng máy tính nằm ở ranh giới giữa mạng nội bộ và mạng bên ngoài (Internet), có thể được sử dụng để chứa các dịch vụ hướng ra ngoài do mạng nội bộ cung cấp (ví dụ: FTP, HTTP, VoIP…)



Các mạng trong phân vùng DMZ thường được sử dụng để bảo vệ mạng nội bộ khỏi các mối đe dọa từ bên ngoài. Các thiết bị thường thấy trong DMZ bao gồm:

* Firewall
* IDS
* IPS
* Proxy Server

**Network Firewalls**: Liên quan đến việc áp dụng một hoặc nhiều firewall giữa các mạng external và mạng internal. Chúng điều chỉnh lưu lượng truy cập vào/ra, tách các mạng external với các mạng internal. Network firewall có thể là phần cứng hoặc phần mềm.

**Host Firewalls:** Liên quan đến việc sử dụng firewall trên các thiết bị người dùng cá nhân và các server. Các thiết bị máy chủ nhận được quy định tùy chỉnh về lưu lượng đến và đi từ các ứng dụng máy tính cụ thể. Host firewall có thể được chạy dưới dạng service của hệ thống, nó cũng có thể đi sâu hơn vào lưu lượng truy cập web, lọc dựa trên HTTP và các giao thức mạng khác, quản lý nội dung nào đến máy của bạn thay vì chỉ quản lý nội dung nó đến từ đâu.

**Filtering traffic via a firewall**: lọc lưu lượng truy cập thông qua tường lửa sử dụng các quy tắc được đặt trước hoặc được học động để permit/deny các kết nối. Tường lửa có thể lọc theo một số trường thông tin sau:

* Soure: gói tin đến từ đâu
* Destination: gói tin đi tới đâu
* Contents: kết nối đang cố gắng gửi gì
* Packet protocol: giao thức mạng được sử dụng để nói chuyện với nhau
* Application protocol: các dịch vụ tầng 7 HTTP, Telnet, FTP, DNS …

## Các loại Firewall

Các loại firewall được phân biệt theo các tiếp cận của chúng đối với:

* Connection tracking
  + Tường lửa theo dõi trạng thái của từng kết nối mạng đang hoạt động
  + Nó ghi nhớ thông tin về source, dest, port và trạng thái kết nối
  + Điều này cho phép tường lửa đưa ra quyết định thông minh hơn về lưu lượng truy cập nào được phép hoặc bị chặn.
* Filtering Rules
  + Tường lửa sử dụng các quy tắc lọc để xác định lưu lương truy cập nào đươc phép
  + Các quy tắc này có thể dựa trên các yếu tối khác nhau.
* Audit logs
  + Tường lửa ghi lại thông tin về tất cả lưu lượng truy cập đi qua nó
  + Các nhật ký này có thể được sử dụng để theo dõi hoạt động mạng, phát hiện các cuộc tấn công vă khắc phục sự cố.
  + Ví dụ: Một quản trị viên mạng có thể sử dụng nhật ký tường lửa để xác định xem một máy tính cụ thể có bị nhiễm phần mềm độc hại hay không.

**Static Packet-Filtering Firewall**

Là tưởng lửa lọc gói tĩnh hoạt động tại layer 3. Cung cấp khả năng lọc cơ bản bằng cách cung cấp khả năng lọc cơ bản bằng cách kiểm tra tất cả các gói dữ liệu riêng lẻ được gửi qua mạng, dựa trên vị trí của chúng và nơi chúng đang cố gắng đi. Việc lọc dựa trên địa chỉ IP, cổng và giao thức gói. Những tường lửa này, ở mức tối thiểu, ngăn hai mạng kết nối trực tiếp mà không được phép.

Rule Filtering được đặt dựa trên ACL tạo thủ công. Chúng sẽ cứng nhắc và khó có thể xử lý lưu lượng không mong muốn cách thích hợp mà không ảnh hưởng đến khả năng sử dụng mang. Lọc tĩnh yêu cầu phải sửa đổi thủ công liên tục để sử dụng hiệu quả. Điểu này chỉ phù hợp với mạng quy mô nhỏ.

**Circuit-Level Gateway Firewall**

Là tường lửa hoặc động ở layer 5 (Session). Các tường lửa này kiểm tra các gói chức năng ttrong một kết nối, nếu hoạt động tốt sẽ cho phép kết nối mở liên tục giữa 2 mạng.

Kết nối không được giám sát đang diễn ra rất nguy hiểm vì các phương tiện hợp pháp có thể mở kết nối và sau đó cho phép tác nhân độc hại truy cập mà không bị gián đoạn.

**Stateful Inspection Firewall**

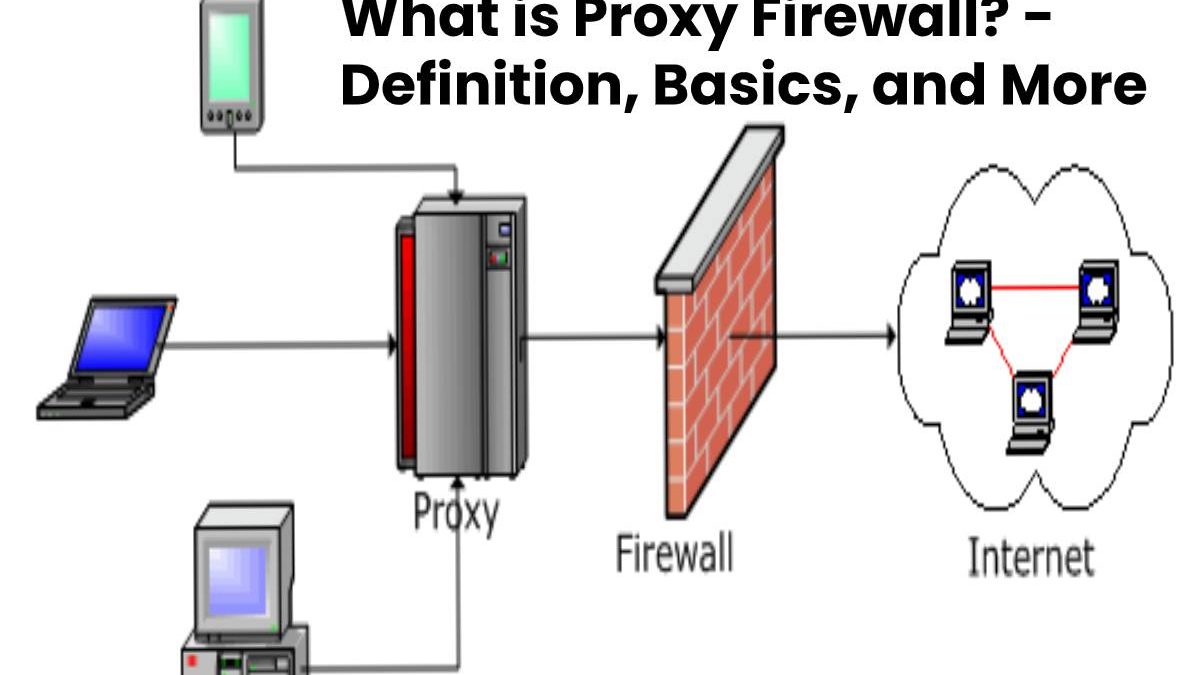
Tường lửa kiểm tra trạng thái, còn được gọi là tường lửa lọc gói động, khác với lọc tĩnh ở khả năng giám sát các kết nối đang diễn ra và ghi nhớ các kết nối trong quá khứ. Chúng bắt đầu bằng cách hoạt động trên lớp vận chuyển (lớp 4) nhưng ngày nay, các tường lửa này có thể giám sát nhiều lớp, bao gồm cả lớp ứng dụng (lớp 7).

Giống như tường lửa lọc tĩnh, tường lửa kiểm tra trạng thái cho phép hoặc chặn lưu lượng truy cập dựa trên các đặc tính kỹ thuật, chẳng hạn như giao thức gói, địa chỉ IP hoặc cổng cụ thể. Tuy nhiên, các tường lửa này cũng theo dõi và lọc riêng dựa trên trạng thái kết nối bằng bảng trạng thái.

Nhìn chung, các quyết định lọc thường dựa trên các quy định của quản trị viên khi thiết lập máy tính và tường lửa. Tuy nhiên, bảng trạng thái cho phép các tường lửa động này đưa ra quyết định của riêng chúng dựa trên các tương tác trước đó mà nó đã 'học được' từ đó. Ví dụ: các loại lưu lượng truy cập gây ra sự gián đoạn trong quá khứ sẽ bị lọc ra trong tương lai. Tính linh hoạt của kiểm tra trạng thái đã củng cố nó như một trong những loại lá chắn phổ biến nhất hiện có.

**Proxy Firewall**

Tường lửa proxy, còn được gọi là tường lửa cấp ứng dụng (lớp 7), có chức năng duy nhất trong việc đọc và lọc các giao thức ứng dụng. Chúng kết hợp kiểm tra cấp ứng dụng hoặc 'deep packet ínpection (DPI)' và kiểm tra trạng thái.



Nó hoạt động như hai máy chủ bổ sung giữa mạng bên ngoài và máy chủ nội bộ, với một máy chủ làm đại diện (hoặc ‘proxy’) cho mỗi mạng.

Việc lọc dựa trên dữ liệu cấp ứng dụng thay vì chỉ địa chỉ IP, cổng và giao thức gói cơ bản (UDP, ICMP) như trong tường lửa dựa trên gói. Việc đọc và hiểu FTP, HTTP, DNS và các giao thức khác cho phép điều tra sâu hơn và lọc chéo đối với nhiều đặc điểm dữ liệu khác nhau.

Nhược điểm của loại bảo mật nghiêm ngặt này là đôi khi nó can thiệp vào dữ liệu đến không phải là mối đe dọa, dẫn đến sự chậm trễ về chức năng.

**Next-Generation Firewall (NGFW)**

được thiết kế để kiểm tra và xác định các mối đe dọa cụ thể, chẳng hạn như phần mềm độc hại nâng cao, ở cấp độ chi tiết hơn. Được sử dụng thường xuyên hơn bởi các doanh nghiệp và mạng phức tạp, chúng cung cấp giải pháp toàn diện để lọc ra các mối đe dọa.

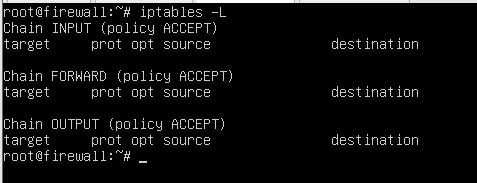
**Hybrid Firewall**

Đây là kiểu sử dụng nhiều loại tường lửa chung với nhau.

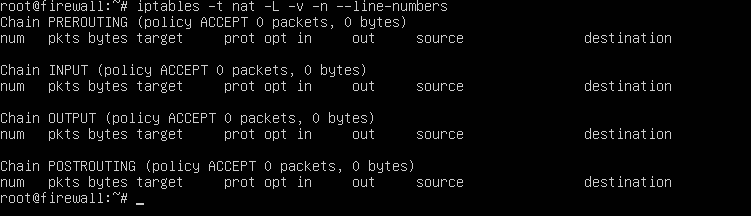
## Thực hành với iptables

Trong iptables có 3 table chính

* **filter table**:
  + INPUT CHAIN: dùng để quản lý traffic đi vào trong máy Linux
  + OUTPUT CHAIN: quản lý traffic từ máy Linux đi ra ngoài
  + FORWARD CHAIN: quản lý traffic đi thông qua máy Linux (router, firewall)
* **NAT table**:
  + OUTPUT CHAIN: sử dụng để quản lý traffic từ máy Linux ra ngoài
  + PREROUTING: sử dụng để NAT IP trước khi định tuyến
  + POSTROUTING: sử dụng để NAT IP sau khi định tuyến
* **Mangle table**: INPUT CHAIN, OUTPUT CHAIN, FORWARD CHAIN, PREROUTING, POSTROUTING - chỉnh sửa thông tin trong header của gói tin phục vụ 1 số bài toán đặc biệt



Mặc định thì iptables được cài đặt sẵn trên các distro và accept tất cả các traffic ra/vào.



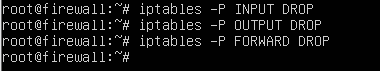
**LAB 1: Hostbase firewall**

Cấu hình các rule cơ bản cho máy Linux

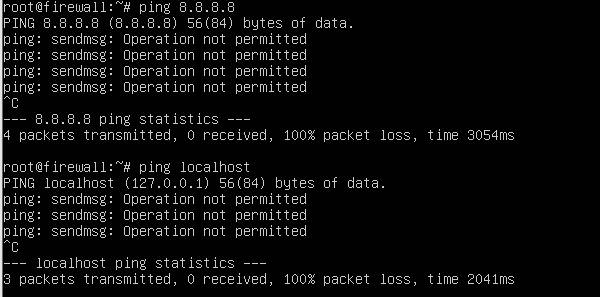
* Xóa hết các rule đang có trong iptables



* Cấu hình các chain INPUT, OUTPUT, FORWARD mặc định DROP tất cả các packet

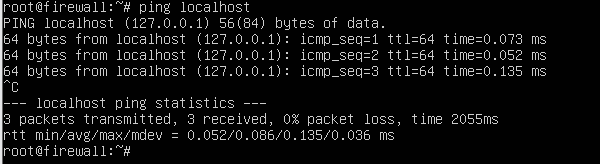


* Như vậy từ chính máy Linux đi đến bất kì vị trí nào đều cần phải thiết lập rule

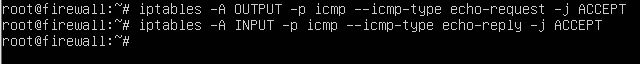


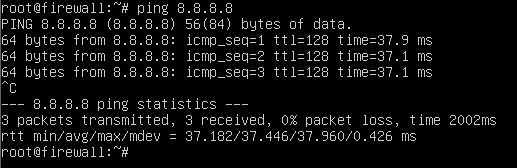
Cho phép traffic đi tới localhost:



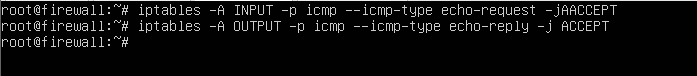


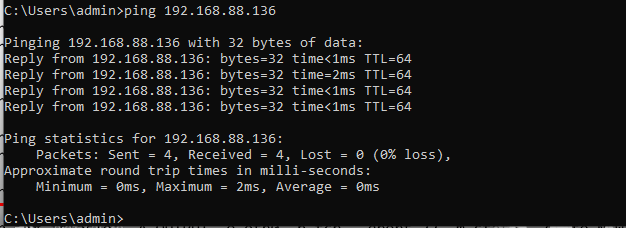
* Cấu hình cho phép ping từ máy Linux ra ngoài



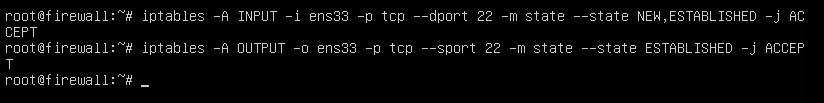


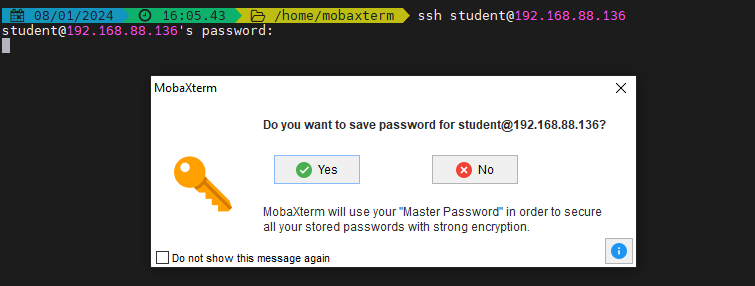
* Cấu hình cho phép máy từ ngoài có thể ping tới máy Linux





* Cấu hình cho phép SSH input vào điều khiển máy Linux trên card mạng ens33

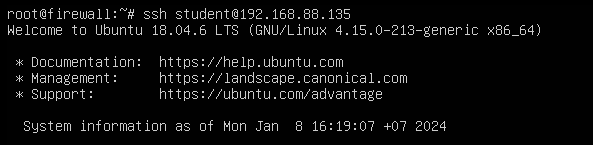




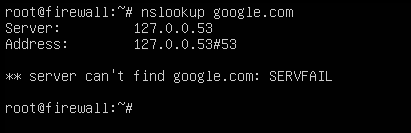
* Cấu hình rule cho phép máy Linux SSH tới một máy khác:



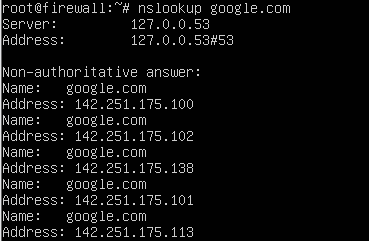




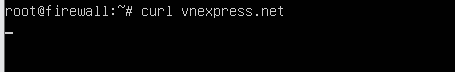
* Cấu hình rule cho phép máy Linux query DNS ở card mạng ens33

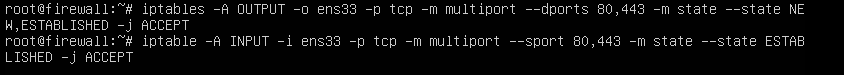


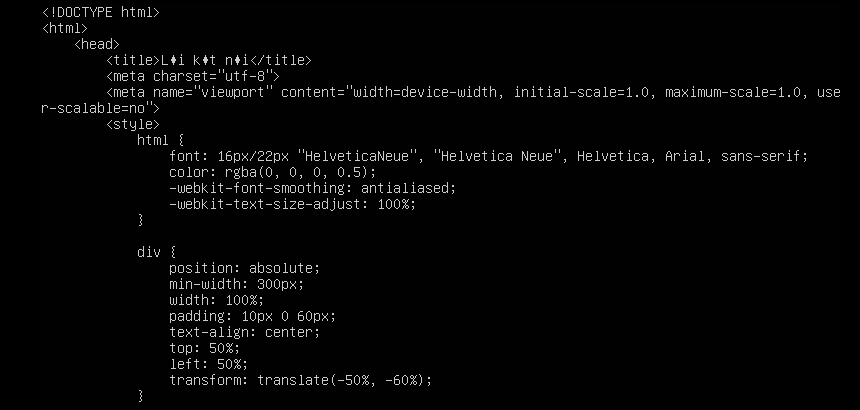




* Cấu hình rule cho phép máy Linux khởi tạo kết nối HTTP, HTTPS ở card mạng ens33

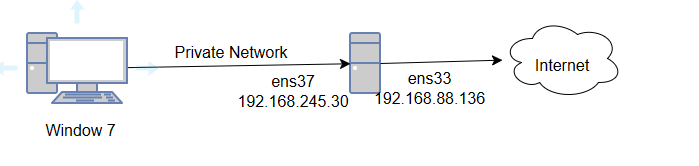




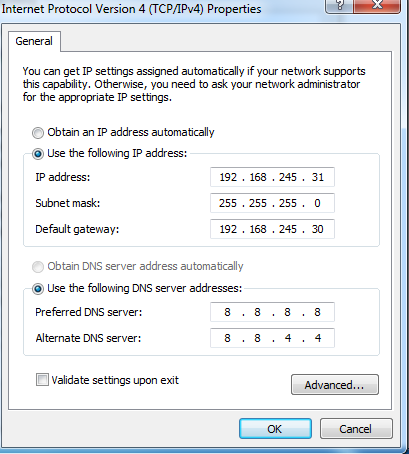


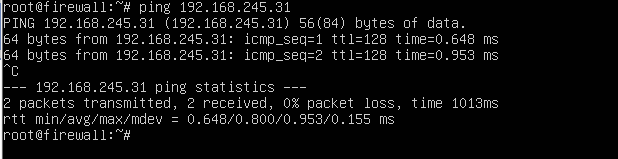
**LAB 2: Network base firewall**

**Mô hình:**

****

Cấu hình IP cho máy window 7:





* Kích hoạt tính năng định tuyến trên firewall



Hoặc bỏ comment dòng sau để khởi động lại hệ thống cấu hình vẫn được lưu:



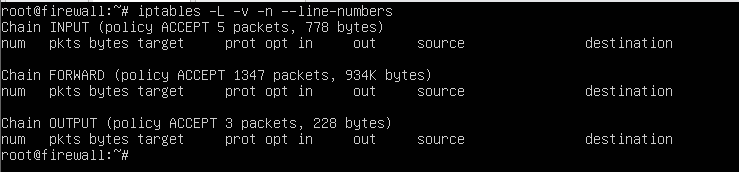


* Thực hiện NAT 192.168.245.0/24 thành IP ở card mạng ens33 (external)

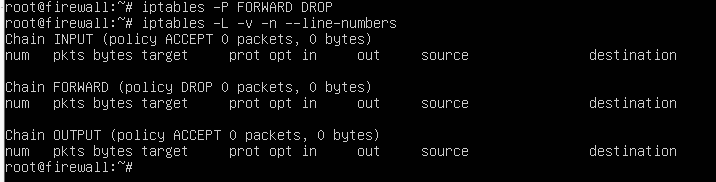


“-j MASQUERADE”: Sử dụng MASQUERADE để thực hiện chức năng masquerade (ẩn địa chỉ nguồn thực tế của gói tin) cho NAT. Điều này thường được sử dụng khi chia sẻ kết nối Internet từ mạng nội bộ.

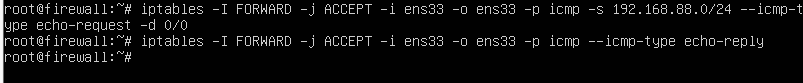
Với những cấu hình này thì Firewall mới chỉ đóng vai trò là router, forward gói tin

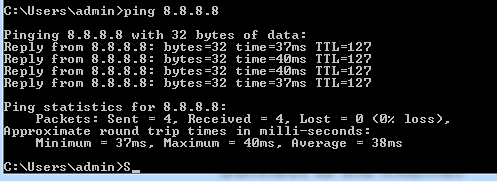


Thiết lập CHAIN FORWARD mặc định sẽ DROP tất cả các gói tin

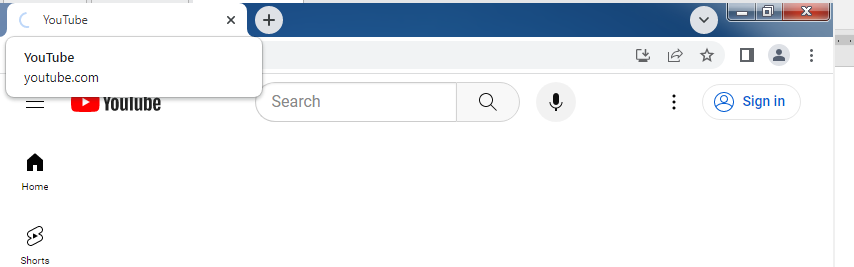


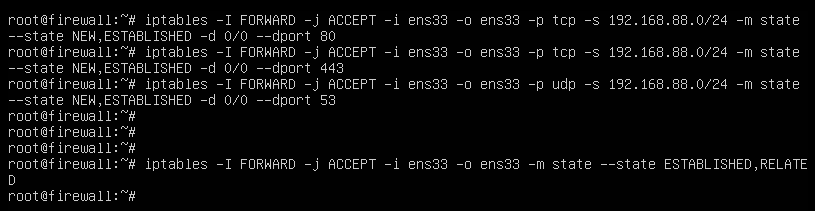
* Thiết lập rule cho phép Ping (trong ví dụ chỉ sử dụng cổng ens33)

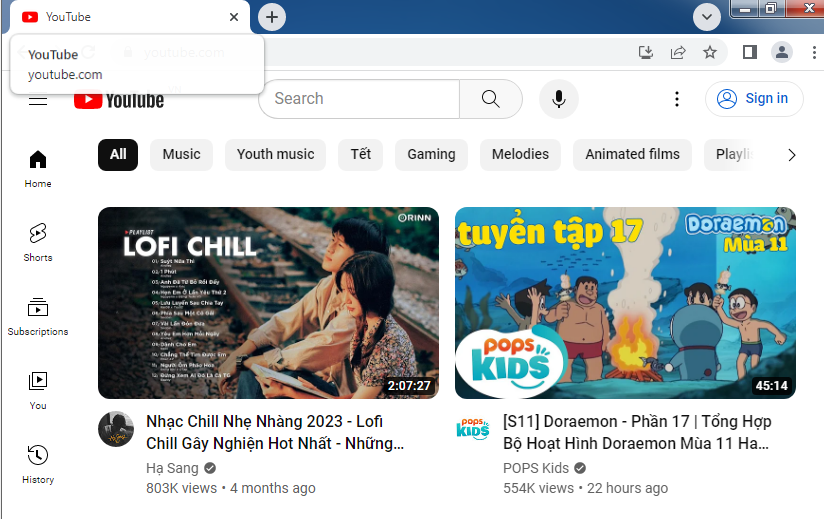




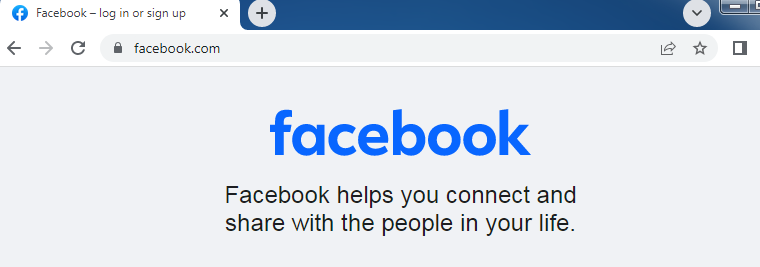
* Cho phép window 7 truy cập các trang web:

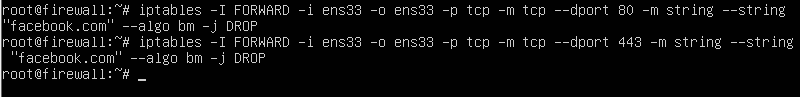






* Cấu hình rule không cho phép truy cập facebook.com





**-I FORWARD**: Thêm một quy tắc vào đầu của chuỗi FORWARD.

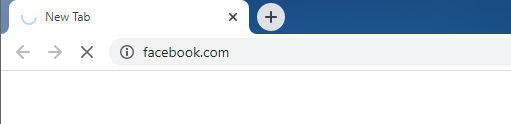
**-i ens37 -o ens33**: Áp dụng quy tắc cho các gói tin đi qua giao diện mạng **ens37** vào giao diện mạng **ens33**.

**-p tcp**: Áp dụng quy tắc cho gói tin sử dụng giao thức TCP.

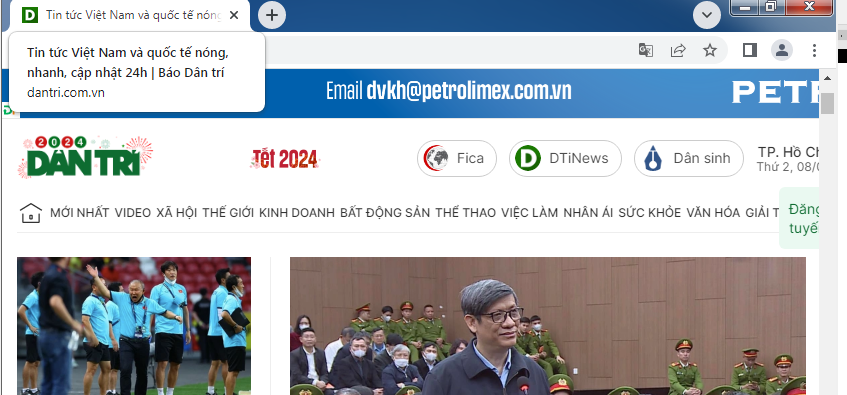
**-m tcp --dport 80**: Áp dụng quy tắc cho gói tin có cổng đích là cổng 80 (HTTP).

**-m string --string "facebook.com" --algo bm**: Sử dụng mô-đun **string** để kiểm tra nếu chuỗi "facebook.com" xuất hiện trong dữ liệu gói tin. Option **--algo bm** sử dụng thuật toán Boyer-Moore để tối ưu hóa việc tìm kiếm chuỗi.

**-j DROP**: Nếu điều kiện trước đó được đáp ứng (chuỗi "facebook.com" xuất hiện trong gói tin), thì gói tin sẽ bị loại bỏ (DROP).



Trên các web khác vẫn sử dụng được

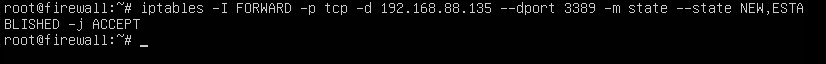


* Cấu hình rule cho phép Remote Desktop vào máy window 7

Đầu tiên cần NAT port 3389 ra ngoài



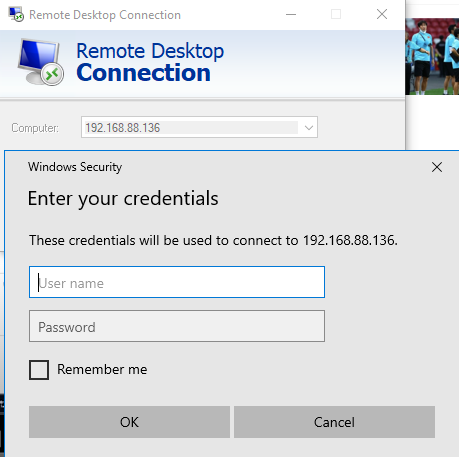
Thực hiện thêm rule ở CHAIN FORWARD

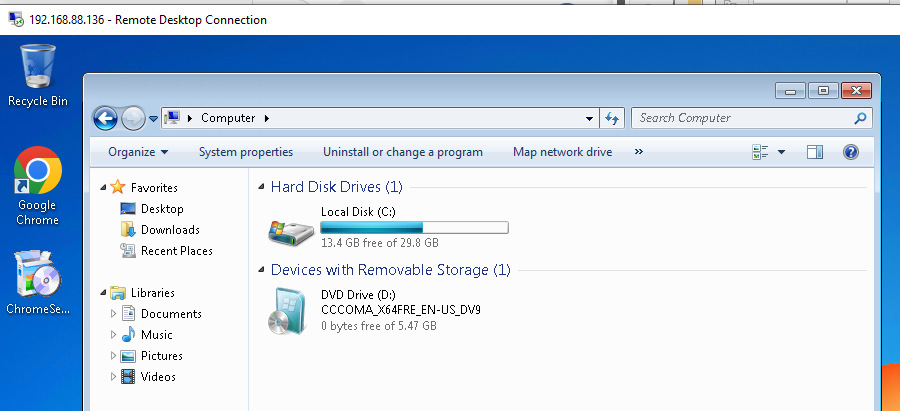


Thêm rule accept dữ liệu phản hồi:



Test kết nối:





# VPN – Virtual Private Network

## Khái niệm

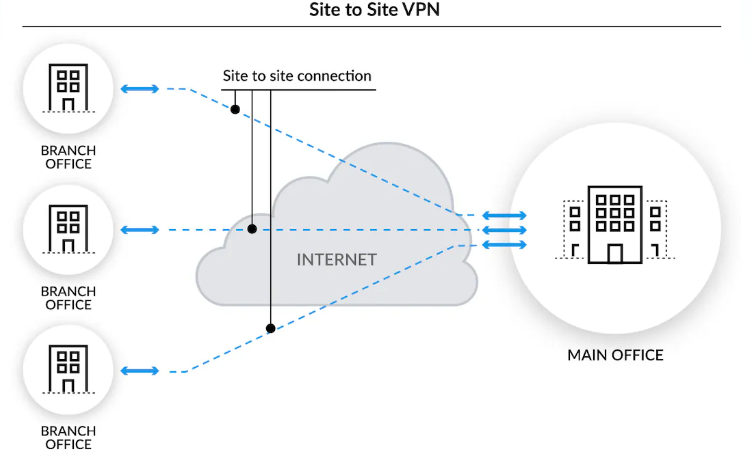
VPN hay Mạng riêng ảo tạo ra kết nối mạng riêng tư giữa các thiết bị thông qua Internet. VPN được sử dụng để truyền dữ liệu một cách an toàn và ẩn danh qua các mạng công cộng. VPN hoạt động bằng cách ẩn địa chỉ IP của người dùng và mã hóa dữ liệu để chỉ người được cấp quyền nhận dữ liệu mới có thể đọc được.

**Công dụng của VPN**

* Quyền riêng tư: Nếu không có mạng riêng ảo, dữ liệu cá nhân của bạn như mật khẩu, thông tin thẻ tín dụng và lịch sử duyệt web có thể bị ghi lại và rao bán bởi các bên thứ ba. VPN sử dụng mã hóa để giữ bí mật những thông tin này, đặc biệt là khi bạn kết nối qua mạng Wi-Fi công cộng.
* Tính ẩn danh: Địa chỉ IP chứa thông tin về vị trí và hoạt động duyệt web của bạn. Tất cả các trang web trên Internet theo dõi dữ liệu này bằng cookie và công nghệ tương tự. Họ có thể nhận dạng bạn bất cứ khi nào bạn ghé thăm trang web của họ. Kết nối VPN sẽ ẩn địa chỉ IP của bạn, để bạn được ẩn danh trên Internet.
* Bảo mật: Dịch vụ VPN sử dụng mật mã để bảo vệ kết nối Internet của bạn khỏi những truy cập trái phép. VPN cũng có thể hoạt động như một cơ chế tắt, hủy bỏ các chương trình được chọn trước đó phòng khi có hoạt động đáng ngờ trên Internet. Việc này làm giảm khả năng dữ liệu bị xâm phạm. Những tính năng trên cho phép các công ty cấp quyền truy cập từ xa cho người dùng được ủy quyền thuộc mạng lưới kinh doanh của họ.

## Các loại VPN

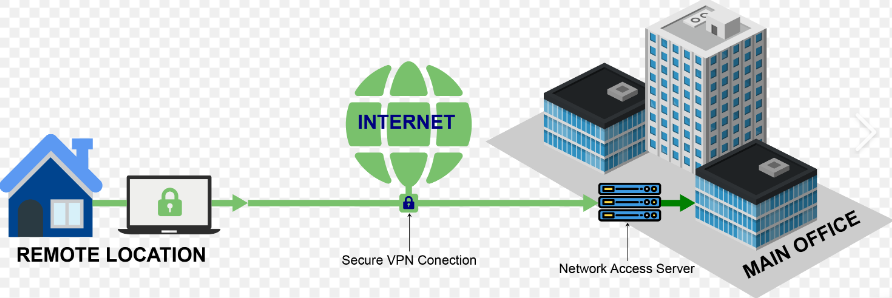
### VPN Site-to-Site



VPN site-to-site là kết nối giữa 2 hoặc nhiều mạng, chẳng hạn như mạng công ty và mạng văn phòng chi nhánh. Mục tiêu của VPN Site-to-site là tạo ra một kênh truyền thông an toàn và bảo mật giữa các địa điểm để cho phép truyền dữ liệu qua mạng internet một cách an toàn.

### VPN Remote-Access

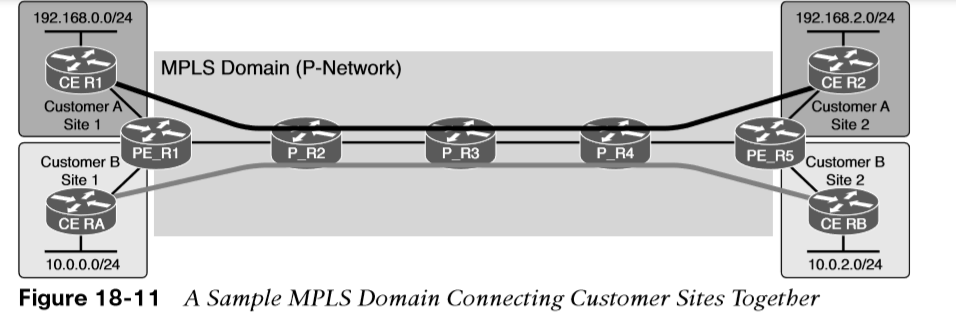
VPN Remote-Access cho phép người dùng từ xa kết nối với mấy chủ thuộc công ty. Hệ thống cho phép nhân viên duy trì kết nối tới mạng văn phòng của họ khi làm việc bên ngoài văn phòng đảm bảo kết nối được an toàn và bảo mật.



### MPLS VPN

MPLS là một phương thức chuyển tiếp gói tin dựa trên nhãn thay vì IP dest trên layer 3.

MPLS VPN (Multi-Protocol Label Switching Virtual Private Network) là một loại dịch vụ VPN sử dụng công nghệ MPLS để cung cấp mạng riêng ảo an toàn và có hiệu suất cao.



## Cơ chế và quá trình hoạt động

**Mã hóa**

Mã hóa là quá trình biến đổi dữ lệu thành dạng không thể đọc được đối với những người không được phép truy cập. Trong VPN, mã hóa được sử dụng để bảo vệ dữ liệu được truyền qua mạng công cộng khỏi những kẻ nghe trộm.

Có nhiều loại mã hóa khác nhau được sử dụng trong VPN, bao gồm:

* AES (Advanced Encryption Standard): Đây là loại mã hóa phổ biến nhất được sử dụng trong VPN. AES sử dụng một khóa 256 bit để mã hóa dữ liệu, mang lại mức độ bảo mật cao.
* RSA (Rivest–Shamir–Adleman): Đây là loại mã hóa khóa công khai được sử dụng để xác thực các thiết bị và người dùng. RSA sử dụng một cặp khóa công khai và khóa bí mật để mã hóa và giải mã dữ liệu.
* SHA (Secure Hash Algorithm): Đây là một loại hàm băm được sử dụng để xác minh tính toàn vẹn của dữ liệu. SHA tạo ra một giá trị băm duy nhất cho dữ liệu đầu vào. Nếu dữ liệu bị thay đổi, giá trị băm cũng sẽ thay đổi.

**Xác thực**

Xác thực là quá trình xác minh danh tính của một thiết bị hoặc người dùng. Trong VPN, xác thực được sử dụng để ngăn chặn những kẻ giả mạo truy cập vào mạng.

Có nhiều phương pháp xác thực khác nhau được sử dụng trong VPN, bao gồm:

* Xác thực qua tên người dùng và mật khẩu: Đây là phương pháp xác thực phổ biến nhất. Người dùng nhập tên người dùng và mật khẩu của họ để xác thực.
* Xác thực qua chứng chỉ: Chứng chỉ là một tệp kỹ thuật số chứa thông tin về danh tính của một thiết bị hoặc người dùng. Chứng chỉ được sử dụng để xác thực thiết bị hoặc người dùng mà không cần phải nhập tên người dùng và mật khẩu.
* Xác thực qua 2 yếu tố (2FA): 2FA yêu cầu người dùng nhập cả tên người dùng, mật khẩu và một mã xác minh được gửi đến thiết bị của họ. 2FA cung cấp mức độ bảo mật cao hơn so với xác thực qua tên người dùng và mật khẩu.

**Quá trình thiết lập phiên kết nối**

Quá trình thiết lập phiên kết nối VPN bao gồm các bước sau:

Thiết bị khách kết nối với máy chủ VPN.

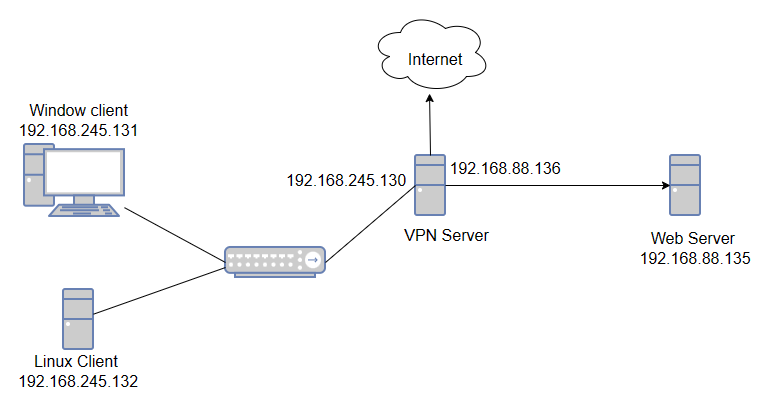
Máy chủ VPN xác thực thiết bị khách.

Thiết bị khách và máy chủ VPN thiết lập một đường hầm được mã hóa, đồng thuận về cách mã hóa dữ liệu.

Thiết bị khách và máy chủ VPN bắt đầu trao đổi dữ liệu qua đường hầm.

## Thực hành với openvpn

**Mô hình**

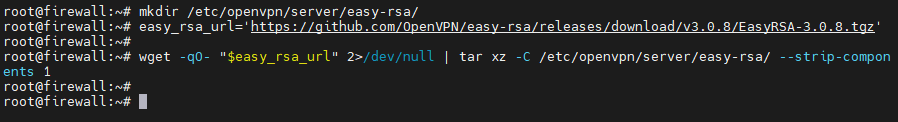


**Cấu hình VPN Server**

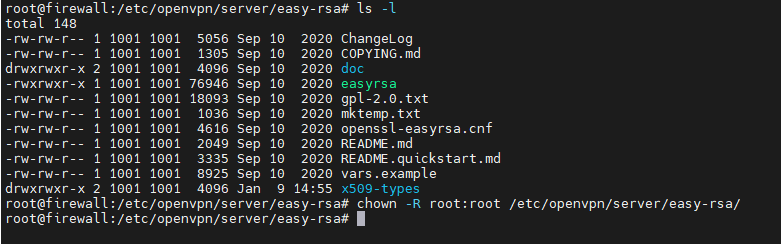
Install openvpn



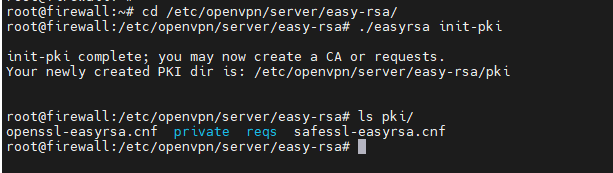
Create easy-rsa



Change the owner of the files



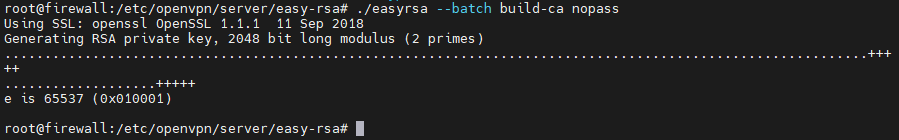
Init PKI



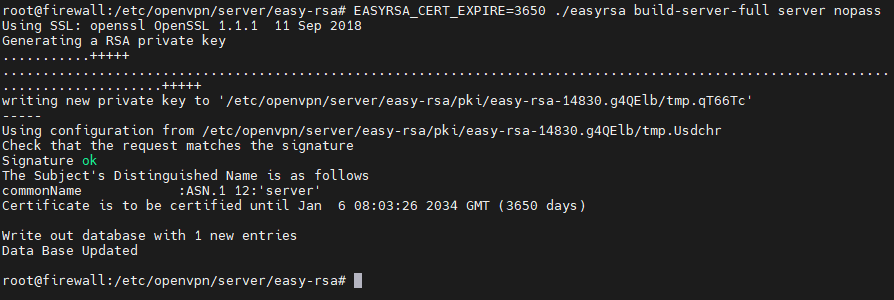
Create Dir



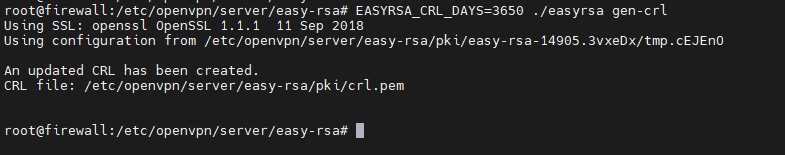
Build CA



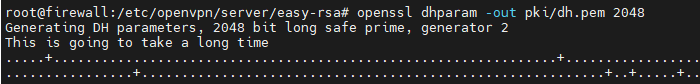
Build Server Cert and Key



Create crl



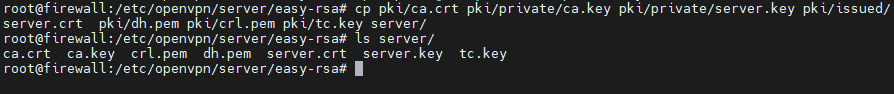
Create DH paramter



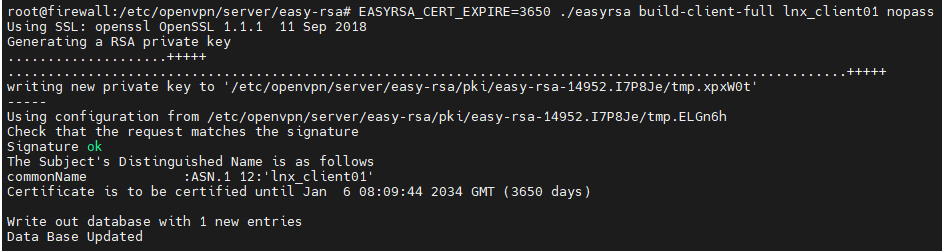
Create TLS Crypt key



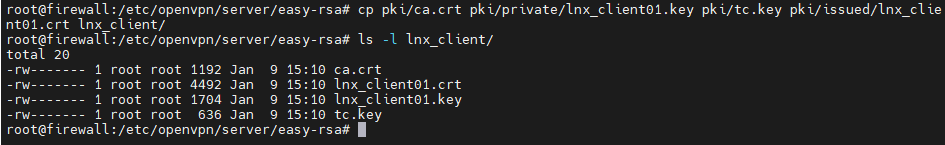
Copy all the needed files to folder server



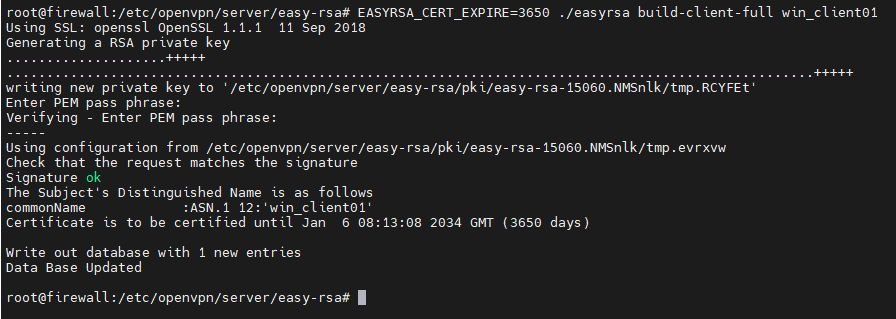
Build Linux Client Cert and Key



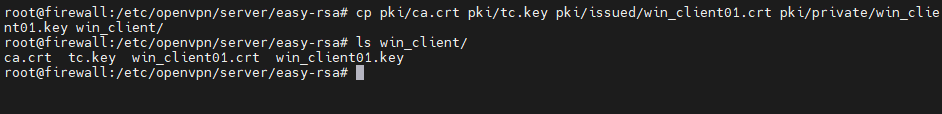
Copy Linux client files



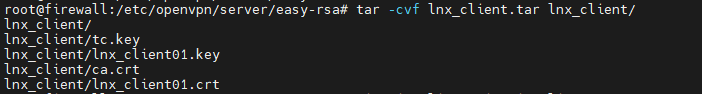
Build Window Client Cert and Key

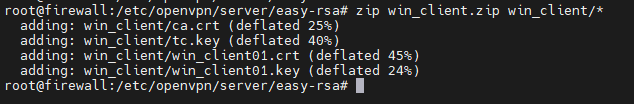


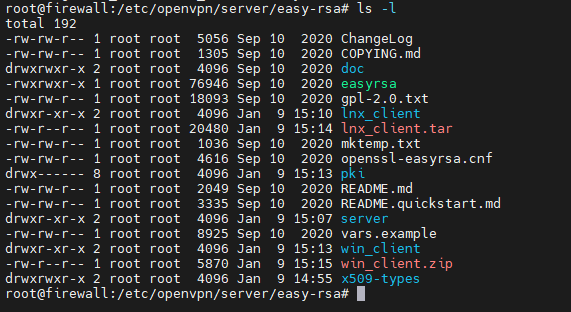
Copy Window Client Cert and Key



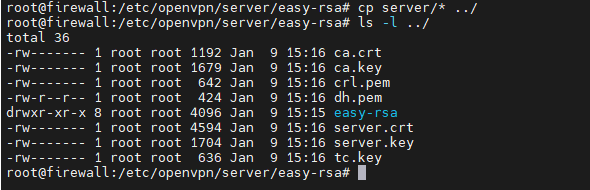
Tar the client folder







Copy Server files to server folder



Grant the server ability to forward the IP (IP Forwarding)



Apply change: *sysctl --system*



Create config file

#vim server.conf

|  |
| --- |
| local 192.168.245.130  port 443  proto tcp  dev tun  ca ca.crt  cert server.crt  key server.key  dh dh.pem  tls-crypt tc.key  crl-verify crl.pem  auth SHA512  topology subnet  server 10.8.0.0 255.255.255.0  ifconfig-pool-persist ipp.txt  route 192.168.88.0 255.255.255.0  push "route 192.168.88.0 255.255.255.0"  push "redirect-gateway def1"  keepalive 10 120  cipher AES-256-GCM  user nobody  group nogroup  persist-key  persist-tun  verb 3  status /var/log/openvpn/openvpn-status.log  log-append /var/log/openvpn/openvpn.log |

**local 192.168.245.130**: Xác định địa chỉ IP hoặc tên máy chủ mà máy chủ OpenVPN sẽ lắng nghe kết nối từ các máy khách.

**port 443**: Xác định cổng mạng mà máy chủ OpenVPN sẽ sử dụng để lắng nghe các kết nối VPN. Trong trường hợp này, sử dụng cổng 443, thường được sử dụng cho HTTPS.

**proto tcp**: Xác định giao thức sử dụng cho kết nối. Ở đây sử dụng giao thức TCP.

**dev tun**: Xác định loại giao diện mạng ảo sẽ được sử dụng. Ở đây, sử dụng TUN, loại giao diện ảo cấp mạng 3.

**ca ca.crt**: Xác định đường dẫn đến tệp chứng chỉ CA (Certificate Authority).

**cert server.crt**: Xác định đường dẫn đến tệp chứng chỉ máy chủ.

**key server.key**: Xác định đường dẫn đến tệp khóa riêng của máy chủ.

**dh dh.pem**: Xác định đường dẫn đến tệp Diffie-Hellman, được sử dụng trong quá trình thiết lập khóa.

**tls-crypt tc.key**: Xác định đường dẫn đến tệp chứa thông tin khóa bảo vệ TLS.

**crl-verify crl.pem**: Xác định đường dẫn đến tệp danh sách đen đã thu hồi (CRL - Certificate Revocation List).

**auth SHA512**: Sử dụng phương pháp xác thực SHA-512.

**topology subnet**: Thiết lập mô hình mạng là subnet.

**server 10.8.0.0 255.255.255.0**: Xác định mạng và masquerade (mask) cho máy chủ VPN.

**ifconfig-pool-persist ipp.txt**: Lưu trạng thái địa chỉ IP của mỗi máy khách và thời gian cấp phát vào tệp ipp.txt.

**route 192.168.88.0 255.255.255.0**: Thêm một tuyến đường trong bảng định tuyến của máy chủ.

**push "route 192.168.88.0 255.255.255.0"**: Gửi thông báo đến các máy khách với tuyến đường được định nghĩa trước.

**push "redirect-gateway def1"**: Thực hiện chuyển hướng tất cả lưu lượng mạng của máy khách qua kết nối VPN.

**keepalive 10 120**: Gửi gói tin keepalive mỗi 10 giây và đợi 120 giây trước khi coi máy khách là đã ngắt kết nối.

**cipher AES-256-GCM**: Sử dụng thuật toán mã hóa AES-256-GCM.

**user nobody**: Chuyển đổi quyền người dùng của quá trình OpenVPN thành "nobody".

**group nogroup**: Chuyển đổi quyền nhóm của quá trình OpenVPN thành "nogroup".

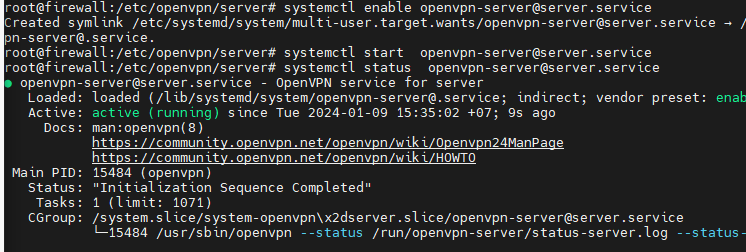
**persist-key** và **persist-tun**: Đảm bảo rằng khóa và giao diện mạng ảo sẽ không bị đổi sau khi quá trình OpenVPN khởi động.

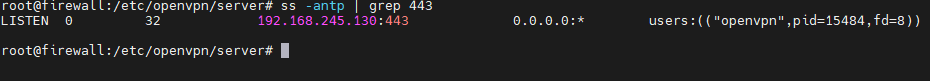
**verb 3**: Xác định mức độ chi tiết của việc ghi log (3 là mức chi tiết cao).

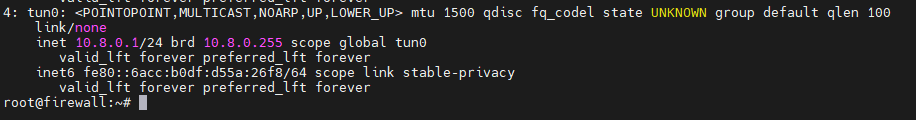
**status /var/log/openvpn/openvpn-status.log**: Xác định đường dẫn đến tệp log chứa thông tin về trạng thái của máy chủ OpenVPN.

**log-append /var/log/openvpn/openvpn.log**: Xác định đường dẫn đến tệp log chứa các thông báo của quá trình OpenVPN.

Enable OpenVPN Server Service





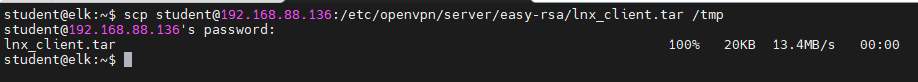


NAT network

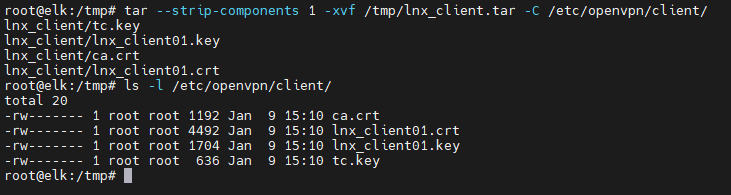


**Linux Client**

Download openvpn linux client file from server



Untar on linux client



Create client.conf

vim /etc/openvpn/client/client.conf

|  |
| --- |
| client  dev tun  proto tcp  remote 192.168.245.130 443  ca /etc/openvpn/client/ca.crt  cert /etc/openvpn/client/lnx\_client01.crt  key /etc/openvpn/client/lnx\_client01.key  tls-crypt /etc/openvpn/client/tc.key  askpass  resolv-retry infinite  nobind  persist-key  persist-tun  remote-cert-tls server  auth SHA512  cipher AES-256-GCM  ignore-unknown-option block-outside-dns  block-outside-dns  verb 3 |

**client**: Xác định rằng đây là cấu hình cho một máy khách OpenVPN.

**dev tun**: Sử dụng giao diện mạng ảo TUN (Layer 3).

**proto tcp**: Xác định sử dụng giao thức TCP cho kết nối.

**remote 192.168.245.130 443**: Xác định địa chỉ IP hoặc tên máy chủ và cổng mà máy khách sẽ kết nối đến.

**ca /etc/openvpn/client/ca.crt**: Đường dẫn đến tệp chứng chỉ CA (Certificate Authority) để xác thực máy chủ.

**cert /etc/openvpn/client/lnx\_client01.crt**: Đường dẫn đến tệp chứng chỉ của máy khách.

**key /etc/openvpn/client/lnx\_client01.key**: Đường dẫn đến tệp khóa riêng của máy khách.

**tls-crypt /etc/openvpn/client/tc.key**: Đường dẫn đến tệp chứa thông tin khóa bảo vệ TLS.

**askpass**: Sử dụng một hộp thoại để yêu cầu mật khẩu từ người dùng khi máy khách khởi động và cần khóa riêng.

**resolv-retry infinite**: Tiếp tục thử lại cố gắng giải quyết tên miền DNS nếu kết nối ban đầu không thành công.

**nobind**: Không ràng buộc (bind) địa chỉ và cổng cục bộ cho kết nối.

**persist-key** và **persist-tun**: Đảm bảo rằng khóa và giao diện mạng ảo của máy khách sẽ không bị đổi sau khi máy khách OpenVPN khởi động.

**remote-cert-tls server**: Máy khách chỉ chấp nhận chứng chỉ từ máy chủ, giúp tránh được các cuộc tấn công giả mạo.

**auth SHA512**: Sử dụng phương thức xác thực SHA-512.

**cipher AES-256-GCM**: Sử dụng thuật toán mã hóa AES-256-GCM.

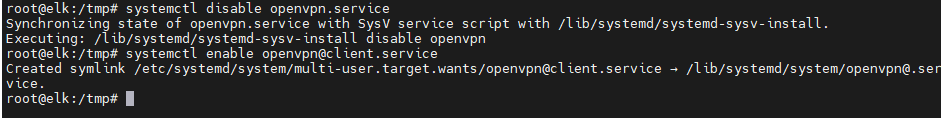
**ignore-unknown-option block-outside-dns**: Bỏ qua các tùy chọn không được hiểu, đặc biệt là **block-outside-dns**.

**block-outside-dns**: Ngăn chặn máy khách từ việc sử dụng các máy chủ DNS ngoại vi khác ngoài máy chủ OpenVPN, giúp đảm bảo tất cả lưu lượng DNS được định hình qua máy chủ VPN.

**verb 3**: Xác định mức độ chi tiết của việc ghi log (3 là mức chi tiết cao).



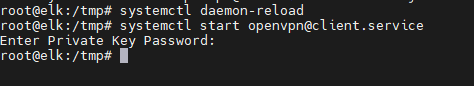
Disable currunt openvpn service

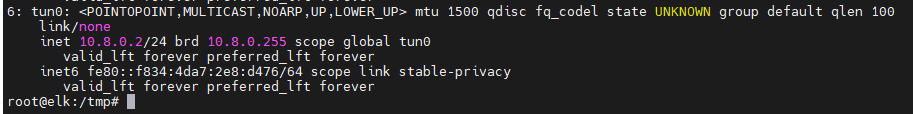


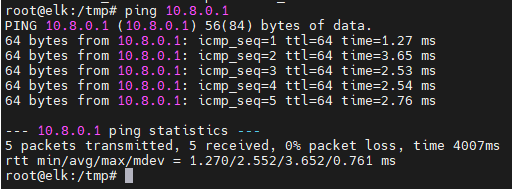


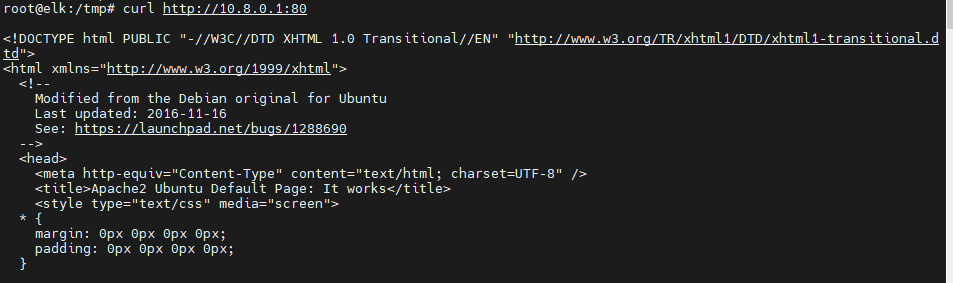


Start Service



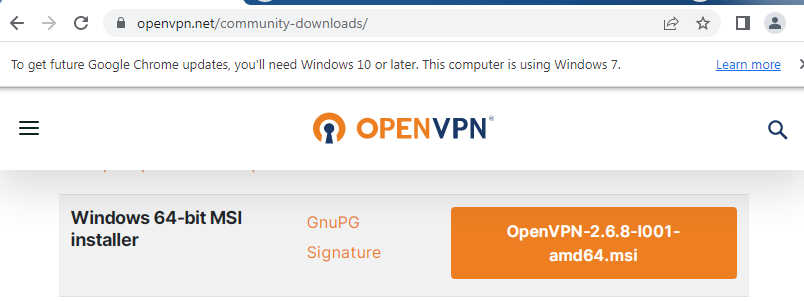






**Window Client**

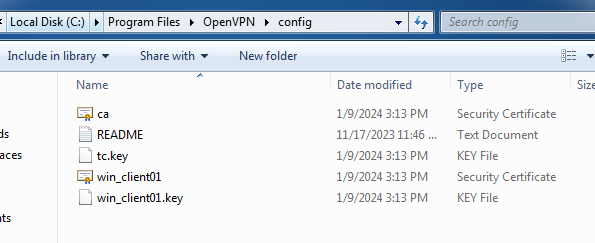
Tải và install openvpn



Download file win\_client.zip



Copy all file to C:/Program Files/OpenVPN/config



Create file client.conf

