# **Triển khai VPN với Openswan**

1. **Danh sách thành viên & Công việc**

|  |  |  |  |
| --- | --- | --- | --- |
| **Họ & tên** | **MSSV** | **Công việc** | **Tiến độ** |
| Nguyễn Hữu Thắng | 175A010514 | - Cài đặt demo Openswan bao gồm triển khai IpSec của 2 máy chủ VPN có 2 mạng A và B  - Hướng dẫn sử dụng | Đang cài đặt OpenSwan.  Đang triển khai các plugin nâng cao. |
| Trần Xuân Lực | 175A071123 | - Tìm hiểu tài tiệu về OpenSwan  - Phân tích Ưu điểm / Nhược điểm của OpenSwan  - So sánh openswan và các mạng riêng ảo khác | Đang tìm hiểu |

1. **Nội dung nghiên cứu**
2. OpenSwan là gì?

OpenSwan là mã nguồn mở dùng để triển khai IpSec trên hệ điều hành Linux. Nó là một nhánh mở của dự án FreeS/WAN bắt đầu bằng vài người phát triển thất bại với việc chính trị bao quanh dự án đó. OpenSwan là một giải pháp để VPN hoạt động trên Linux. OpenSwan là một mã nguồn mở nên bất cứ ai cũng có thể là nhà phát triển, họ có thể sửa đổi, vá lỗi và bổ sung một số chức năng mới. OpenSwan hỗ trợ hấu hết các mở rộng (RFC + bản thảo IETF) có liên quan đến IpSec bao gồm cả kĩ thuật chứng nhận số X.509, NAT Traversel và một số thứ khác.

1. OpenSwan có chức năng cụ thể là gì?

Chức năng của OpenSwan là thiết lập các hệ thống mạng an toàn ( mạng riêng ảo) trên nền tảng công cộng theo công nghệ IpSec.

1. Hoạt động của OpenSwan như thế nào ?

- Hai mạng Lan private ở 2 site có thể nói chuyện được với nhau trên đường truyền Internet một cách bảo mật, thông quan OpenSwan được cấu hình ở 2 server vpn.

- Ngăn chặn hành động "nghe lén" mà hacker bắt các gói tin ở giữa đường truyền.

- OpenSwan có 2 thành phần chính cấu thành là KLIP và PLUTO

1. Hướng dẫn cài đặt OpenSwan trên Ubuntu ?

site A:

+ Địa chỉ ip public: 10.10.40.129/24

+ Địa chỉ ip mạng lan private: 10.10.10.133/24

site B:

+ Địa chỉ ip public: 10.10.40.130/24

+ Địa chỉ ip mạng lan private: 10.10.20.135/24

1. Cài đặt ban đầu: (thực hiện trên cả 2 site A và B)

Các bước sau, thực hiện lần lượt trên cả 2 site A và B.

* Cài đặt OpenSwan trên Ubuntu server:

apt-get install openswan

* Vô hiệu hóa chuyển hướng VPN nếu có, trên các site :

for vpn in /proc/sys/net/ipv4/conf/\*;

do echo 0 > $vpn/accept\_redirects;

echo 0 > $vpn/send\_redirects;

done

* Cho phép chuyển tiếp IP và vô hiệu hóa trang chuyển hướng vĩnh viễn bằng cách:

Sửa file /etc/sysctl.conf , tìm và bỏ comment các dòng sau :

net.ipv4.ip\_forward = 1

net.ipv4.conf.all.accept\_redirects = 0

net.ipv4.conf.all.send\_redirects = 0

* reload /etc/sysctl.conf:

sysctl -p

* Thiết lập rules của Iptables cho phép các gói tin đi qua:

iptables -A INPUT -p udp --dport 500 -j ACCEPT

iptables -A INPUT -p tcp --dport 4500 -j ACCEPT

iptables -A INPUT -p udp --dport 4500 -j ACCEPT

2. Cấu hình ipsec: vi /etc/ipsec.conf

config setup

plutodebug=all

plutostderrlog=/var/log/pluto.log

protostack=netkey

nat\_traversal=yes

virtual\_private=%v4:10.0.0.0/8,%v4:192.168.0.0/16,%v4:172.16.0.0/12

oe=off

## connection definition in Debian ##

conn demo-connection-debian

authby=secret

auto=start

## phase 1 ##

keyexchange=ike

## phase 2 ##

esp=3des-md5

pfs=yes

type=tunnel

left=<siteA-public-IP>

leftsourceip=<siteA-public-IP>

leftsubnet=<siteA-private-subnet>/netmask

## for direct routing ##

leftsubnets=<siteA-public-IP>/netmask

leftnexthop=%defaultroute

right=<siteB-public-IP>

rightsubnet=<siteB-private-subnet>/netmask

| **Lệnh** | **Ý nghĩa** |
| --- | --- |
| protostack=netkey | Trên Linux, có 2 IPSec stacks, đó là NETKEY và KLIPS. NETKEY mặc định có sẵn trong Linux kernel còn KLIPS thì không. Do đó, tôi chọn là NETKEY trong trường hợp này. |
| nat\_traversal=yes | Cho phép các gói tin IPSec đi qua các thiết bị NAT. |
| virtual\_private | Add các dải mảng private không được sử dụng. (The best method is to add all private subnet except those ranges used by the server). |
| oe=off | disable opportunistic encryption in Debian |
| conn | Đặt tên cho connection, dùng để phân biệt các tunnels |
| authby | Cách thức các server thực hiện xác thực. Sử dụng secret với cách shared secret hoặc rsasig với cách RSASIG. Mình có nói phần này ở dưới. |
| type | Kiểu kết nối. Với tunnel thì chấp nhận: host-to-host, host-to-subnet, hoặc subnet-to-subnet. Với transport chấp nhận host-to-host. |
| keyexchange=ike | Tiến hành xác thực khóa bằng giao thức ike |
| esp=3des-md5 | Phương thức mã hóa gói tin |
| left | Địa chỉ ip public của server đang cấu hình |
| leftsourceip | Địa chỉ ip public của server đang cấu hình |
| leftsubnet | Đại chỉ mạng lan private trên đang cấu hình |
| right | Địa chỉ ip public của server cần kết nối (server B) |
| rightsubnet | Địa chỉ ip mạng lan private trên server cần kết nối (server B) |

* Với mô hình như trên thì cấu hình ở ipsec site A như sau:

config setup

plutodebug=all

plutostderrlog=/var/log/pluto.log

protostack=netkey

nat\_traversal=yes

virtual\_private=%v4:10.0.0.0/8,%v4:192.168.0.0/16,%v4:172.16.0.0/12

oe=off

conn vpn

authby=secret

auto=start

## phase 1 ##

keyexchange=ike

## phase 2 ##

esp=3des-md5

pfs=yes

type=tunnel

left=10.10.40.129

leftsourceip=10.10.10.133

leftsubnet=10.10.10.0/24

## for direct routing ##

leftsubnets=10.10.40.0/24

leftnexthop=%defaultroute

right=10.10.40.130

rightsubnet=10.10.20.0/24

* Cấu hình ipsec ở site B:

config setup

plutodebug=all

plutostderrlog=/var/log/pluto.log

protostack=netkey

nat\_traversal=yes

virtual\_private=%v4:10.0.0.0/8,%v4:192.168.0.0/16,%v4:172.16.0.0/12

oe=off

conn vpn

authby=secret

auto=start

## phase 1 ##

keyexchange=ike

## phase 2 ##

esp=3des-md5

pfs=yes

type=tunnel

left=10.10.40.130

leftsourceip=10.10.20.135

leftsubnet=10.10.20.0/24

## for direct routing ##

leftsubnets=10.10.40.0/24

leftnexthop=%defaultroute

right=10.10.40.129

rightsubnet=10.10.10.0/24

3. Cấu hình xác thực OpenSwan ipsec cho phép t sử dụng 2 phương thức để xác thực các gói tin khi đi qua tunnel, đó là: **Shared Secret** hoặc **RSA key**.

Lưu ý là chúng ta chỉ chọn 1 trong 2 phương thức để xác thực.

3.1 Pre-Share-Key

* Tạo Pre-Share-Key (PSK). PSK trên 2 server phải giống nhau.
* Đường dẫn file chứa PSK /etc/ipsec.secrets.

root@adk:~# vi /etc/ipsec.secrets

ip-public-site1 ip-publici-site2 : PSK "123456a@"

* Hoặc chúng ta có thể tạo PSK cho mọi tunnel với nội dung sau:

%any %any : PSK "123456a@"

* Ở đây, cấu hình với site A:

10.10.40.129 10.10.40.130 : PSK "123456a@"

* Tương tự, với site B.

10.10.40.130 10.10.40.129 : PSK "123456a@"

* Restart lại dịch vụ

service ipsec restart

3.2 RSA key

* Phương thức xác thực thứ 2, sử dụng RSAIG.
* Chúng ta cần tạo rsa keys trên cả 2 server vpn.
* Để tạo rsa key cho vpn server, ta chạy lệnh sau:

root@adk:~# ipsec newhostkey --output /etc/ipsec.secrets --bits 2048 --verbose --hostname <your VPN server hostname>

Trong đó, tạo thay đổi bằng hostname của server bạn.

Lệnh trên sẽ tạo key có độ dài là 2048 bit

Chạy lệnh tạo key ở trên với server vpn còn lại.

* Chỉnh sửa file ipsec.conf, sửa và thêm các thông số sau.

authby=rsasig

leftrsasigkey=keypublic của chính server.

rightrsasigkey=keypublic của server bên kia.

* Trong đó:
  + **leftrsasigkey:** là key rsa public trên chính vpn server này.
  + **rightrsasigkey:** là key rsa trên vpn server bên kia.
* Các cấu hình còn lại giữ nguyên giống như ở trên.
* Ví dụ ở trên site A, có cấu hình như sau:

conn vpn

authby=rsasig

leftrsasigkey=0sAQOXleUvusHJRkzJOlNw6B1xbMBOTEZXeGkeRj48MOC/F4VtXgLD7DNlPmrPDHaA4TQ0B2agMIgR/uY+tXiaknwzRVR0L/3OVLlZklnOkToo27ofMB+COPbcPpNMXZgwPkmCeMdf8CuPJcZdqw20/fI7LJC83PPXwFJf7O7SH1hjBznFdFNh8EnKDDoCic4qEu9ECXGmBELHiHBS+yKGeOfAb9wPjagJD7N+qcjijyBfEms2yVqodbfq3yGrGzfvw1xOLTgLWSVKqLOuEj0HF4njMGBh6/GtLCVwNoTOpkLj+J9WyEvELjS/Z2hrUslERwJBK8186IYGmq8gqUjxGfRh

rightrsasigkey=0sAQNXuoHPULTMOwzXX+CwiQSFq6OnxIkvUEa+6tkk9dtCONZnS7fYDtt+DxVgFShsUC2nOE4crRqrIyDBXCAWHutbTisdSROKS3pBhBRYC1jlxN6gg6Vz+2HvxgsXlatO4NdS9+e2DWH65mvuF9O+Ty6IAGaUZfHsmqvdbqeCn/0RApoYvJmSW6XQZymwq5X5gELG1/2l2NkEzbzdHBhUH/XcjaeVKSY1U8PVDAPHfdpIuT6L46CFvzBeMUyE/7J9/psy+ugIC72LY5HvgAxVtQiMe/h864UuB6cu2iPzZPDYPdgc8+69nGPDnvOnDk17Y5/tBfw4tyfKzoFxQal2dxbp

* Trên site B:

conn vpn

authby=rsasig

leftrsasigkey=0sAQNXuoHPULTMOwzXX+CwiQSFq6OnxIkvUEa+6tkk9dtCONZnS7fYDtt+DxVgFShsUC2nOE4crRqrIyDBXCAWHutbTisdSROKS3pBhBRYC1jlxN6gg6Vz+2HvxgsXlatO4NdS9+e2DWH65mvuF9O+Ty6IAGaUZfHsmqvdbqeCn/0RApoYvJmSW6XQZymwq5X5gELG1/2l2NkEzbzdHBhUH/XcjaeVKSY1U8PVDAPHfdpIuT6L46CFvzBeMUyE/7J9/psy+ugIC72LY5HvgAxVtQiMe/h864UuB6cu2iPzZPDYPdgc8+69nGPDnvOnDk17Y5/tBfw4tyfKzoFxQal2dxbp

rightrsasigkey=0sAQOXleUvusHJRkzJOlNw6B1xbMBOTEZXeGkeRj48MOC/F4VtXgLD7DNlPmrPDHaA4TQ0B2agMIgR/uY+tXiaknwzRVR0L/3OVLlZklnOkToo27ofMB+COPbcPpNMXZgwPkmCeMdf8CuPJcZdqw20/fI7LJC83PPXwFJf7O7SH1hjBznFdFNh8EnKDDoCic4qEu9ECXGmBELHiHBS+yKGeOfAb9wPjagJD7N+qcjijyBfEms2yVqodbfq3yGrGzfvw1xOLTgLWSVKqLOuEj0HF4njMGBh6/GtLCVwNoTOpkLj+J9WyEvELjS/Z2hrUslERwJBK8186IYGmq8gqUjxGfRh

4. Kết quả.

* Trạng thái hoạt động

root@adk:~# service ipsec status

IPsec running - pluto pid: 6227

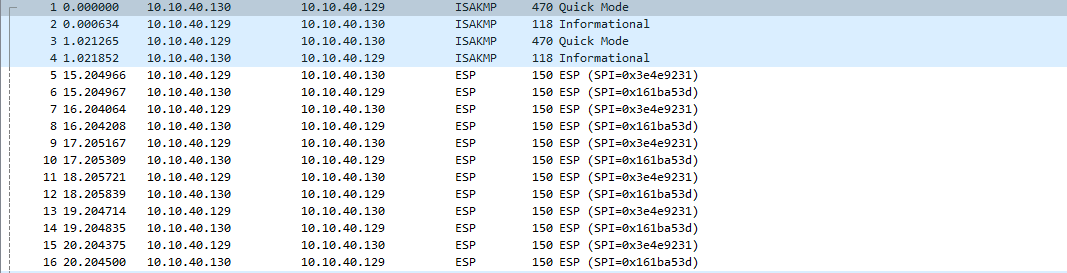
pluto pid 6227

2 tunnels up

some eroutes exist

Nếu kiểm tra mà không có tunnels hoạt động, thì hãy kiểm tra lại bảng định tuyến. Bảng định tuyến mà không có default gateway thì sẽ không thể tạo được tunnel.

* Tiến hành bắt gói tin trên máy trung gian khi 2 máy server "ping" nhau.

[](https://camo.githubusercontent.com/29e9ce6dd29a4ba567a38ede3e72356c1a1da901/687474703a2f2f696d6167652e70726e747363722e636f6d2f696d6167652f61653964616436323836323534623561616138616235393632303531636138392e706e67)

Các gói tin ISAKMP là các gói tin trao đổi khóa giữa 2 server.

Các gói tin ESP là các gói tin icmp đã được mã hóa khi đi trên đường truyền.

5. Chú ý:

* Nếu là Direct routing thì không cần phải nat, ngược lại, phải nat trước khi đi ra internet.
* Câu lệnh dưới đây sẽ dùng iptables để thay đổi địa chỉ nguồn của gói tin trong mạng private trước khi được gửi ra internet.

root@adk:~# iptables -t nat -A POSTROUTING -s 10.10.10.0/24 -j MASQUERADE

1. Hướng dẫn Sử dụng/Quản trị ?