



The Vietnamese Security Network



TÀI LIỆU HƯỚNG DẪN CẤU HÌNH

ĐẢM BẢO AN TOÀN THÔNG TIN HỆ THỐNG

MỤC LỤC:

LỜI MỞ ĐẦU	2
Cài đặt OpenVPN Server.....	1
Windows:.....	14
MacOS:.....	16
iOS:.....	19
Android:	22
Wazuh.....	26
Các bước cài đặt Wazuh	30
Các bước thêm agent wazuh	33
1. Trên server	33
2. Cài đặt client trên linux.....	33
3. Thêm agent trên window.....	35

LỜI MỞ ĐẦU

Tình hình mất an ninh mạng đang diễn biến phức tạp và ngày càng xuất hiện nhiều nguy cơ đe dọa đến việc phát triển kinh tế xã hội và đảm bảo quốc phòng, an ninh. Theo số liệu mới nhất của Symantec vừa công bố về hiện trạng bảo mật trong 9 tháng đầu năm 2019, Việt Nam đứng thứ 11 trong số các quốc gia bị tấn công mạng nhiều nhất thế giới và đứng số 3 trong khu vực Đông Nam Á (sau Indonesia và Singapore).

Bên cạnh đó, nguy cơ an ninh mạng và bảo mật an toàn thông tin (ATTT) tại các doanh nghiệp ở Việt Nam đang ở mức báo động khi tình trạng bị hacker, virus, malware tấn công gây thất thoát dữ liệu, lộ lọt thông tin bị, bị theo dõi, mất quyền quản trị, lây truyền virus,... liên tục gia tăng không ngừng, gây ra hậu quả và thiệt hại vô cùng lớn về kinh tế và uy tín doanh nghiệp về lâu dài.

Do đó, việc xây dựng hàng rào Bảo mật để ngăn chặn rủi ro thất thoát dữ liệu đang trở thành nhu cầu cấp bách của nhiều doanh nghiệp hiện nay Tuy nhiên, vì một số lý do, nhiều doanh nghiệp chưa đủ khả năng hay thời gian để triển khai các phương pháp bảo mật chuyên sâu cho hệ thống vận hành. Bộ tài liệu dưới đây sẽ giúp cho doanh nghiệp hiểu và tự triển khai cấu hình Open VPN và Wazuh – 2 mã nguồn mở (miễn phí) hỗ trợ tối ưu trong công tác bảo mật, đảm bảo an toàn thông tin kịp thời cho doanh nghiệp.

Cài đặt OpenVPN Server.

(Lưu ý: Tài liệu trên được viết dành cho hệ điều hành Ubuntu 18.06 LTS, dưới quyền user “root”. Người dùng có thể sử dụng user “root” này bằng câu lệnh sau)

```
sudo su -
```

Bước 1: Chạy lệnh

```
apt update
```

Bước 2: Cài đặt OpenVPN

```
apt install openvpn
```

```
root@ip-172-31-36-102:~# apt install openvpn
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libpkcs11-helper1
Suggested packages:
  easy-rsa resolvconf
The following NEW packages will be installed:
  libpkcs11-helper1 openvpn
0 upgraded, 2 newly installed, 0 to remove and 40 not upgraded.
Need to get 514 kB of archives.
After this operation, 1274 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu bionic/main amd64 libpkcs11-helper1 amd64 1.22-4 [43.5 kB]
Get:2 http://ap-southeast-1.ec2.archive.ubuntu.com/ubuntu bionic-updates/main amd64 openvpn amd64 2.4.4-2ubuntu1.3 [470 kB]
Fetched 514 kB in 2s (278 kB/s)
Preconfiguring packages ...
Selecting previously unselected package libpkcs11-helper1:amd64.
(Reading database ... 111653 files and directories currently installed.)
Preparing to unpack .../libpkcs11-helper1_1.22-4_amd64.deb ...
Unpacking libpkcs11-helper1:amd64 (1.22-4) ...
Selecting previously unselected package openvpn.
Preparing to unpack .../openvpn_2.4.4-2ubuntu1.3_amd64.deb ...
Unpacking openvpn (2.4.4-2ubuntu1.3) ...
Setting up libpkcs11-helper1:amd64 (1.22-4) ...
Setting up openvpn (2.4.4-2ubuntu1.3) ...
 * Restarting virtual private network daemon.
Created symlink /etc/systemd/system/multi-user.target.wants/openvpn.service → /lib/systemd/system/openvpn.service.
Processing triggers for systemd (237-3ubuntu10.38) ...
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...
Processing triggers for ureadahead (0.100.0-21) ...
Processing triggers for libc-bin (2.27-3ubuntu1) ...
```

Bước 3: Tải về EasyRSA

```
git clone https://github.com/OpenVPN/easy-rsa-old.git
```

```
root@ip-172-31-36-102:~# git clone https://github.com/OpenVPN/easy-rsa-old.git
Cloning into 'easy-rsa-old'...
remote: Enumerating objects: 1295, done.
remote: Total 1295 (delta 0), reused 0 (delta 0), pack-reused 1295
Receiving objects: 100% (1295/1295), 343.87 KiB | 447.00 KiB/s, done.
Resolving deltas: 100% (442/442), done.
```

Bước 4: Copy thư mục "easy-rsa-old" vừa tải về vào đường dẫn "/etc/openvpn/" - tương tự, copy thư mục đó vào đường dẫn "/usr/share/doc/openvpn/"

```
cp -r easy-rsa-old/ /etc/openvpn  
  
cp -r easy-rsa-old/ /usr/share/doc/openvpn
```

```
root@ip-172-31-36-102:~# cp -r easy-rsa-old/ /etc/openvpn/  
root@ip-172-31-36-102:~# ls -la  
total 28  
drwx----- 5 root root 4096 Apr 25 07:57 .  
drwxr-xr-x 23 root root 4096 Apr 8 06:46 ..  
-rw-r--r-- 1 root root 3106 Apr 9 2018 .bashrc  
-rw-r--r-- 1 root root 148 Aug 17 2015 .profile  
drwx----- 2 root root 4096 Mar 20 02:14 .ssh  
drwxr-xr-x 6 root root 4096 Apr 25 07:57 easy-rsa-old  
drwxr-xr-x 3 root root 4096 Mar 20 02:15 snap  
root@ip-172-31-36-102:~# cd /etc/op  
openvpn/ opt/  
root@ip-172-31-36-102:~# cd /etc/openvpn/  
root@ip-172-31-36-102:/etc/openvpn# ls  
client easy-rsa-old server update-resolv-conf
```

Bước 5: Truy cập vào trong thư mục "easysrsa" để bắt đầu việc chỉnh sửa config cho file "vars"

```
cd /etc/openvpn/easy-rsa-old/easy-rsa/2.0
```

```
root@ip-172-31-36-102:~# cd /etc/openvpn/  
root@ip-172-31-36-102:/etc/openvpn# cd easy-rsa-old/  
.git/ distro/ doc/ easy-rsa/  
root@ip-172-31-36-102:/etc/openvpn# cd easy-rsa-old/easy-rsa/2.0/  
root@ip-172-31-36-102:/etc/openvpn/easy-rsa-old/easy-rsa/2.0# ls  
build-ca build-key-pass build-req-pass openssl-0.9.6.cnf revoke-full  
build-dh build-key-pkcs12 clean-all openssl-0.9.8.cnf sign-req  
build-inter build-key-server inherit-inter openssl-1.0.0.cnf vars  
build-key build-req list-crl pktool whichopensslcnf
```

Trong file "vars", cần sửa thông tin ở các trường "KEY_COUNTRY", "KEY_PROVINCE", "KEY_CITY", "KEY_ORG" và "KEY_EMAIL"

vi vars

```
root@ip-172-31-36-102:/etc/openvpn/easy-rsa-old/easy-rsa/2.0 101x55

# This variable should point to
# the openssl.cnf file included
# with easy-rsa.
export KEY_CONFIG=`$EASY_RSA/whichopensslcnf $EASY_RSA` 

# Edit this variable to point to
# your soon-to-be-created key
# directory.
#
# WARNING: clean-all will do
# a rm -rf on this directory
# so make sure you define
# it correctly!
export KEY_DIR="$EASY_RSA/keys"

# Issue rm -rf warning
echo NOTE: If you run ./clean-all, I will be doing a rm -rf on $KEY_DIR

# PKCS11 fixes
export PKCS11_MODULE_PATH="dummy"
export PKCS11_PIN="dummy"

# Increase this if you
# are paranoid. This will slow
# down TLS negotiation performance
# as well as the one-time DH parms
# generation process.
export DH_KEY_SIZE=2048

# Private key size
export KEY_SIZE=4096

# In how many days should the root CA key expire?
export CA_EXPIRE=3650

# In how many days should certificates expire?
export KEY_EXPIRE=3650

# These are the default values for fields
# which will be placed in the certificate.
# Don't leave any of these fields blank.
export KEY_COUNTRY="VN"
export KEY_PROVINCE="Hanoi"
export KEY_CITY="Hanoi"
export KEY_ORG="VSEC JSC."
export KEY_EMAIL="duongnt@vsec.com.vn"
```

Bước 6: Tạo symbolic link

```
ln -s openssl-1.0.0.cnf openssl.cnf
```

```
root@ip-172-31-36-102:/etc/openvpn/easy-rsa-old/easy-rsa/2.0# ln -s openssl-1.0.0.cnf openssl.cnf
root@ip-172-31-36-102:/etc/openvpn/easy-rsa-old/easy-rsa/2.0#
```

Bước 7: Khởi chạy và làm theo hướng dẫn

```
#Export sẵn các trường thông tin bên trong file "vars" để sử dụng trong các bước tiếp theo
./vars
#Dọn dẹp thư mục "/keys" (nếu có)
./clean-all
#Khởi tạo Certificate Authority
./build-ca
```

```
root@ip-172-31-36-102:/etc/openvpn/easy-rsa-old/easy-rsa/2.0# ./vars
NOTE: If you run ./clean-all, I will be doing a rm -rf on /etc/openvpn/easy-rsa-old/easy-rsa/2.0/keys
root@ip-172-31-36-102:/etc/openvpn/easy-rsa-old/easy-rsa/2.0# ./clean-all
root@ip-172-31-36-102:/etc/openvpn/easy-rsa-old/easy-rsa/2.0# ./build-ca
Can't load /root/.rnd into RNG
140316863148480:error:2406F079:random number generator:RAND_load_file:Cannot open file:../crypto/rand
/randfile.c:88:Filename=/root/.rnd
Generating a RSA private key
.....+++++
.....+
writing new private key to 'ca.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [VN]:
State or Province Name (full name) [Hanoi]:
Locality Name (eg, city) [Hanoi]:
Organization Name (eg, company) [VSEC JSC.]:
Organizational Unit Name (eg, section) [changeme]:Infra Team
Common Name (eg, your name or your server's hostname) [changeme]:Duong Nguyen
Name [changeme]:
Email Address [mail@host.domain]:
root@ip-172-31-36-102:/etc/openvpn/easy-rsa-old/easy-rsa/2.0#
```

Bước 8: Khởi tạo key cho server và làm theo hướng dẫn

```
./build-key-server server
```

```
root@ip-172-31-36-102:/etc/openvpn/easy-rsa-old/easy-rsa/2.0# ./build-key-server server
Ignoring -days; not generating a certificate
Can't load /root/.rnd into RNG
140468804858304:error:2406F079:random number generator:RAND_load_file:Cannot open file:../crypto/rand
/randfile.c:88:Filename=/root/.rnd
Generating a RSA private key
-----
.....+++++
.....+++++
writing new private key to 'server.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [VN]:
State or Province Name (full name) [Hanoi]:
Locality Name (eg, city) [Hanoi]:
Organization Name (eg, company) [VSEC JSC.]:
Organizational Unit Name (eg, section) [changeme]:
Common Name (eg, your name or your server's hostname) [server]:server
Name [changeme]:
Email Address [mail@host.domain]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from /etc/openvpn/easy-rsa-old/easy-rsa/2.0/openssl.cnf
Can't load /root/.rnd into RNG
140055943799232:error:2406F079:random number generator:RAND_load_file:Cannot open file:../crypto/rand
/randfile.c:88:Filename=/root/.rnd
Can't open /etc/openvpn/easy-rsa-old/easy-rsa/2.0/keys/index.txt.attr for reading, No such file or di
rectory
140055943799232:error:02001002:system library:fopen:No such file or directory:../crypto/bio/bss_file.
c:72:fopen('/etc/openvpn/easy-rsa-old/easy-rsa/2.0/keys/index.txt.attr','r')
140055943799232:error:2006D080:BIO routines:BIO_new_file:no such file:../crypto/bio/bss_file.c:79:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName          :PRINTABLE:'VN'
stateOrProvinceName :PRINTABLE:'Hanoi'
localityName         :PRINTABLE:'Hanoi'
organizationName    :PRINTABLE:'VSEC JSC.'
organizationalUnitName:PRINTABLE:'changeme'
commonName           :PRINTABLE:'server'
name                 :PRINTABLE:'changeme'
emailAddress         :IA5STRING:'mail@host.domain'
Certificate is to be certified until Apr 23 08:57:35 2030 GMT (3650 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]
```

Bước 9: Khởi tạo key cho client và làm theo hướng dẫn

```
./build-key client1
```

```
root@ip-172-31-36-102:/etc/openvpn/easy-rsa-old/easy-rsa/2.0# ./build-key client1
Ignoring -days; not generating a certificate
Can't load /root/.rnd into RNG
140194287243712:error:2406F079:random number generator:RAND_load_file:Cannot open file:../crypto/rand
/randfile.c:88:Filename=/root/.rnd
Generating a RSA private key
.....+++++
.....+++
writing new private key to 'client1.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [VN]:
State or Province Name (full name) [Hanoi]:
Locality Name (eg, city) [Hanoi]:
Organization Name (eg, company) [VSEC JSC.]:
Organizational Unit Name (eg, section) [changeme]:
Common Name (eg, your name or your server's hostname) [client1]:client1
Name [changeme]:
Email Address [mail@host.domain]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from /etc/openvpn/easy-rsa-old/easy-rsa/2.0/openssl.cnf
Can't load /root/.rnd into RNG
140241216152000:error:2406F079:random number generator:RAND_load_file:Cannot open file:../crypto/rand
/randfile.c:88:Filename=/root/.rnd
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName          :PRINTABLE:'VN'
stateOrProvinceName :PRINTABLE:'Hanoi'
localityName         :PRINTABLE:'Hanoi'
organizationName     :PRINTABLE:'VSEC JSC.'
organizationalUnitName:PRINTABLE:'changeme'
commonName           :PRINTABLE:'client1'
name                 :PRINTABLE:'changeme'
emailAddress         :IA5STRING:'mail@host.domain'
Certificate is to be certified until Apr 23 09:05:16 2030 GMT (3650 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]
Write out database with 1 new entries
Data Base Updated
root@ip-172-31-36-102:/etc/openvpn/easy-rsa-old/easy-rsa/2.0#
```

Bước 10: Khởi tạo key Diffie-Hellman

`./build-dh`

```
root@ip-172-31-36-102:/etc/openvpn/easy-rsa-old/easy-rsa/2.0# ./build-dh  
Generating DH parameters, 2048 bit long safe prime, generator 2  
This is going to take a long time
```

A large grid of '+' characters on a black background, forming a pattern that looks like a stylized 'M' or a series of interconnected shapes. The grid is composed of numerous small '+' symbols arranged in a repeating pattern across the entire frame.

Bước 11: Copy các file "server.key", "server.crt", "dh2048.pem" và "ca.crt" về đường dẫn "/etc/openvpn" để tiện sử dụng

```
cp ca.crt /etc/openvpn/  
  
cp server.crt /etc/openvpn/  
  
cp server.key /etc/openvpn/  
  
cp dh2048.pem /etc/openvpn/
```

```
root@ip-172-31-36-102:/etc/openvpn/easy-rsa-old/easy-rsa/2.0/keys# cp ca.crt /etc/openvpn/  
root@ip-172-31-36-102:/etc/openvpn/easy-rsa-old/easy-rsa/2.0/keys# cp dh2048.pem /etc/openvpn/  
root@ip-172-31-36-102:/etc/openvpn/easy-rsa-old/easy-rsa/2.0/keys# cp server.key /etc/openvpn/  
root@ip-172-31-36-102:/etc/openvpn/easy-rsa-old/easy-rsa/2.0/keys# cp server.crt /etc/openvpn/  
root@ip-172-31-36-102:/etc/openvpn/easy-rsa-old/easy-rsa/2.0/keys#
```

Bước 12: Khởi tạo static key

```
openvpn --genkey --secret ta.key
```

```
root@ip-172-31-36-102:/etc/openvpn# openvpn --genkey --secret ta.key  
root@ip-172-31-36-102:/etc/openvpn# ls  
ca.crt dh2048.pem    server        server.crt  ta.key  
client  easy-rsa-old   server.conf  server.key  update-resolv-conf
```

Bước 13: Sử dụng các mẫu có sẵn để tạo ra file config cho server và các client

```
cd /usr/share/doc/openvpn/examples/sample-config-files
```

```
root@ip-172-31-36-102:~# cd /usr/share/doc/openvpn/  
root@ip-172-31-36-102:/usr/share/doc/openvpn# ls  
AUTHORS      NEWS.Debian.gz  README.IPv6      changelog.Debian.gz  management-notes.txt.gz  
COPYING.gz  PORTS          README.auth-pam  copyright  
COPYRIGHT.GPL.gz  README          README.down-root  easy-rsa-old  
Changes.rst.gz  README.Debian.gz  README.mbedtls  examples  
root@ip-172-31-36-102:/usr/share/doc/openvpn# cd examples/sample-  
sample-config-files/ sample-keys/           sample-scripts/  
root@ip-172-31-36-102:/usr/share/doc/openvpn# cd examples/sample-config-files/  
root@ip-172-31-36-102:/usr/share/doc/openvpn/examples/sample-config-files# ls  
README      loopback-client    openvpn-startup.sh  tls-home.conf  
client.conf  loopback-server   server.conf.gz     tls-office.conf  
firewall.sh  office.up          static-home.conf  xinetd-client-config  
home.up      openvpn-shutdown.sh static-office.conf xinetd-server-config
```

Config mẫu của client (client.conf):

```
client
dev tun
proto tcp
remote 13.229.142.9 1443 #server ip public - port to be connected to
resolv-retry 60
nobind
persist-key
persist-tun
remote-cert-tls server
cipher AES-256-CBC
auth SHA512
key-direction 1
verb 3
tun-mtu 6000
mssfix 0
keepalive 5 15

<ca>
#please put your ca.crt content here
</ca>
<cert>
#please put your client.crt content here
</cert>
<key>
#please put your client.key content here
</key>
<tls-auth>
#please put your ta.key content here
</tls-auth>
```

Config mẫu của server (server.conf):

```
port 1443
proto tcp
dev tun
ca ca.crt
cert server.crt
key server.key # This file should be kept secret
dh dh2048.pem

server 10.10.0.0 255.255.0.0 #VPN's LAN IP pool
ifconfig-pool-persist ipp.txt
keepalive 5 15

# performance tuning
```

```
tun-mtu 6000
fragment 0
mssfix
txqueuelen 1000
max-clients 100
tls-auth ta.key 0 # This file is secret
key-direction 0
cipher AES-256-CBC # AES
auth SHA512
engine aesni
# tune
tun-mtu 6000
fragment 0
mssfix 0
txqueuelen 1000

#push all packets from client to server
push "redirect-gateway def1"
push "dhcp-option DNS 10.10.0.1" #default gateway

#push packets for specific website(s)/IP(s) from client to server
#push "route-nopull" #prevents client from creating a standard rule to forces all traffic through
VPN
#push "route 104.27.198.90 255.255.255.255"
#push "route 104.27.199.90 255.255.255.255"
```

Chú ý: Cần mở port tương ứng trong server với port được khai báo bên trong file config.
Sau khi tạo xong các file config, copy các file đó về đường dẫn "/etc/openvpn" để sử dụng
(trên server hay client đều cần được copy tới đường dẫn trên).

Bước 14: Bật IP forward trên server

```
systemctl net.ipv4.ip_forward=1
```

```
root@ip-172-31-36-102:/etc/openvpn# sudo sysctl net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
```

Bước 15: Bật forward packet trong LAN và tunnel mọi packet từ client qua server để ra Internet (sử dụng card mạng được dùng để chạy VPN)

```
iptables -t nat -A POSTROUTING -s 10.10.0.0/16 -o eth5 -j MASQUERADE
```

```
iptables -A FORWARD -i ens5 -j ACCEPT
```

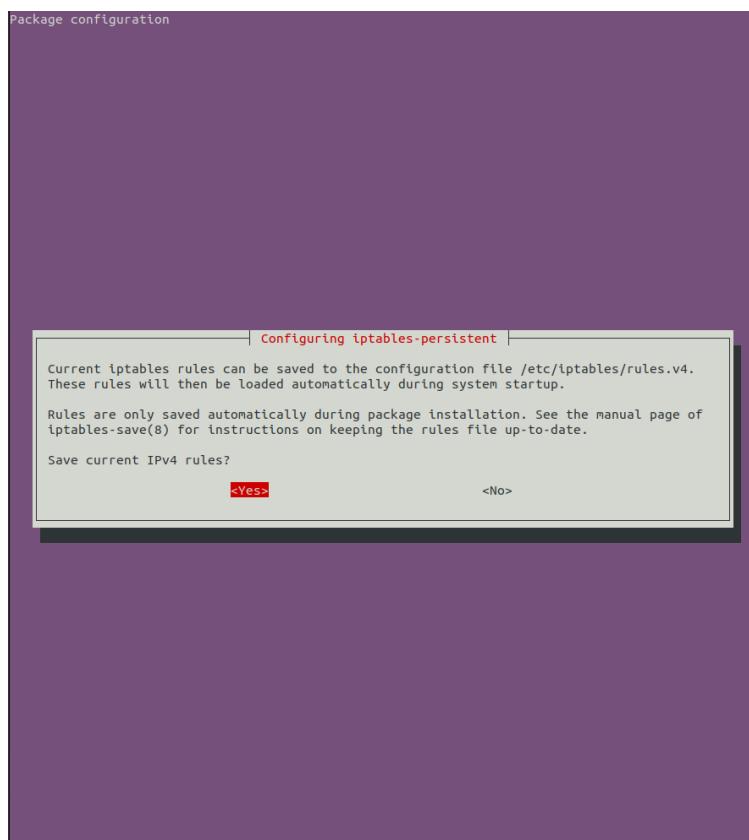
```
iptables -A FORWARD -o ens5 -j ACCEPT
```

```
iptables -t nat -A POSTROUTING -o eth5 -j MASQUERADE
```

```
iptables -A FORWARD -i ens5 -j ACCEPT  
iptables -A FORWARD -o ens5 -j ACCEPT
```

Cài đặt iptables-persistent (tránh trường hợp server reboot mất cấu hình iptables)

```
apt install iptables-persistent -y
```



Chọn “Yes” để lưu cấu hình IPv4 hiện tại (đã setup để sử dụng VPN).

Làm tương tự để lưu cấu hình IPv6 hiện tại (nếu có).

Bước 16: Chạy OpenVPN Server và Client

- Trên server:

```
systemctl enable openvpn@server

systemctl start openvpn@server

systemctl status openvpn@server
```

```
root@ip-172-31-36-102:/etc/iptables# sudo systemctl status openvpn@server
● openvpn@server.service - OpenVPN connection to server
   Loaded: loaded (/lib/systemd/system/openvpn@.service; indirect; vendor preset: enabled)
   Active: active (running) since Wed 2020-04-29 03:46:02 UTC; 28min ago
     Docs: man:openvpn(8)
           https://community.openvpn.net/openvpn/wiki/Openvpn24ManPage
           https://community.openvpn.net/openvpn/wiki/HOWTO
   Main PID: 8565 (openvpn)
      Status: "Initialization Sequence Completed"
        Tasks: 1 (limit: 4647)
       CGroup: /system.slice/system-openvpn.slice/openvpn@server.service
                 └─8565 /usr/sbin/openvpn --daemon ovpn-server --status /run/openvpn/server.status 10

Apr 29 03:46:02 ip-172-31-36-102 systemd[1]: Starting OpenVPN connection to server...
Apr 29 03:46:02 ip-172-31-36-102 systemd[1]: Started OpenVPN connection to server.
```

- Trên client:

+ Ubuntu/Linux:

```
systemctl start openvpn@client

systemctl status openvpn@client
```

```
⚡ ~ systemctl status openvpn@client
● openvpn@client.service - OpenVPN connection to client
   Loaded: loaded (/lib/systemd/system/openvpn@.service; disabled; vendor preset: enabled)
   Active: active (running) since Wed 2020-04-29 11:09:17 +07; 1min 0s ago
     Docs: man:openvpn(8)
           https://community.openvpn.net/openvpn/wiki/Openvpn24ManPage
           https://community.openvpn.net/openvpn/wiki/HOWTO
   Main PID: 9941 (openvpn)
      Status: "Initialization Sequence Completed"
        Tasks: 1 (limit: 9404)
       CGroup: /system.slice/system-openvpn.slice/openvpn@client.service
                 └─9941 /usr/sbin/openvpn --daemon ovpn-client --status /run/openvpn/client.status 10 --cd /etc/openvpn --script-security 2 --config /etc/openvpn/client.conf --writepid /run/openvpn/client.pid

Apr 29 11:09:19 duong-desk-ubun ovpn-client[9941]: TUN/TAP device tun0 opened
Apr 29 11:09:19 duong-desk-ubun ovpn-client[9941]: TUN/TAP TX queue length set to 100
Apr 29 11:09:19 duong-desk-ubun ovpn-client[9941]: do_ifconfig, tt->id_ifconfig_tovc_setup=0
Apr 29 11:09:19 duong-desk-ubun ovpn-client[9941]: /sbin/ip link set dev tun0 up mtu 6000
Apr 29 11:09:19 duong-desk-ubun ovpn-client[9941]: /sbin/ip addr add dev tun0 local 10.10.0.6 peer 10.10.0.5
Apr 29 11:09:19 duong-desk-ubun ovpn-client[9941]: /sbin/ip route add 104.27.198.90/32 via 10.10.0.5
Apr 29 11:09:19 duong-desk-ubun ovpn-client[9941]: /sbin/ip route add 104.27.199.90/32 via 10.10.0.5
Apr 29 11:09:19 duong-desk-ubun ovpn-client[9941]: /sbin/ip route add 10.10.0.1/32 via 10.10.0.5
Apr 29 11:09:19 duong-desk-ubun ovpn-client[9941]: WARNING: this configuration may cache passwords in memory -- use the auth-nocache option to prevent this
Apr 29 11:09:19 duong-desk-ubun ovpn-client[9941]: Initialization Sequence Completed
```

Kết quả: Máy tính Client có thể truy cập mạng Internet thành công thông qua VPN và sở hữu một địa chỉ IP hợp lệ trong mạng LAN của VPN

My Public IPv4 is: 13.229.142.9

My Public IPv6 is: Not Detected

Location: Singapore, - SG ?

ISP: Amazon Data Services Singapore

```
duongnguyen@duong-desk-ubun:~$ dig +short myip.opendns.com @resolver1.opendns.com
13.229.142.9
duongnguyen@duong-desk-ubun:~$ dig +short myip.opendns.com @resolver1.opendns.com
113.20.106.102
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 6000
    inet 10.10.0.6 netmask 255.255.255.255 destination 10.10.0.5
    inet6 fe80::c79e:2181:2158:57fb prefixlen 64 scopeid 0x20<link>
      unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 100 (UNSPEC)
        RX packets 0 bytes 0 (0.0 B)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 3 bytes 168 (168.0 B)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
⚡ ~ systemctl status openvpn@client
● openvpn@client.service - OpenVPN connection to client
  Loaded: loaded (/lib/systemd/system/openvpn@.service; disabled; vendor preset: enabled)
  Active: active (running) since Wed 2020-04-29 11:09:17 +07; 8min ago
    Docs: man:openvpn(8)
          https://community.openvpn.net/openvpn/wiki/Openvpn24ManPage
          https://community.openvpn.net/openvpn/wiki/HOWTO
  Main PID: 9941 (openvpn)
  Status: "Initialization Sequence Completed"
    Tasks: 1 (limit: 9464)
   CGroup: /system.slice/system-openvpn.slice/openvpn@client.service
           └─9941 /usr/sbin/openvpn --daemon ovpn-client --status /run/openvpn/client.status 10 --cd /etc/ope

Apr 29 11:09:19 duong-desk-ubun ovpn-client[9941]: TUN/TAP device tun0 opened
Apr 29 11:09:19 duong-desk-ubun ovpn-client[9941]: TUN/TAP TX queue length set to 100
Apr 29 11:09:19 duong-desk-ubun ovpn-client[9941]: do_ifconfig, tt->did_ifconfig_ipv6_setup=0
Apr 29 11:09:19 duong-desk-ubun ovpn-client[9941]: /sbin/ip link set dev tun0 up mtu 6000
Apr 29 11:09:19 duong-desk-ubun ovpn-client[9941]: /sbin/ip addr add dev tun0 local 10.10.0.6 peer 10.10.0.5
Apr 29 11:09:19 duong-desk-ubun ovpn-client[9941]: /sbin/ip route add 104.27.198.90/32 via 10.10.0.5
Apr 29 11:09:19 duong-desk-ubun ovpn-client[9941]: /sbin/ip route add 104.27.199.90/32 via 10.10.0.5
Apr 29 11:09:19 duong-desk-ubun ovpn-client[9941]: /sbin/ip route add 10.10.0.1/32 via 10.10.0.5
Apr 29 11:09:19 duong-desk-ubun ovpn-client[9941]: WARNING: this configuration may cache passwords in memory
Apr 29 11:09:19 duong-desk-ubun ovpn-client[9941]: Initialization Sequence Completed
⚡ ~ curl google.com
<HTML><HEAD><meta http-equiv="content-type" content="text/html; charset=utf-8">
<TITLE>301 Moved</TITLE></HEAD><BODY>
<H1>301 Moved</H1>
The document has moved
<A href="http://www.google.com/">here</A>.
</BODY></HTML>
⚡ ~ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=128 time=28.7 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=128 time=27.1 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=128 time=32.0 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=128 time=25.7 ms
^C
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 25.792/28.422/32.020/2.327 ms
⚡ ~
```

Windows:

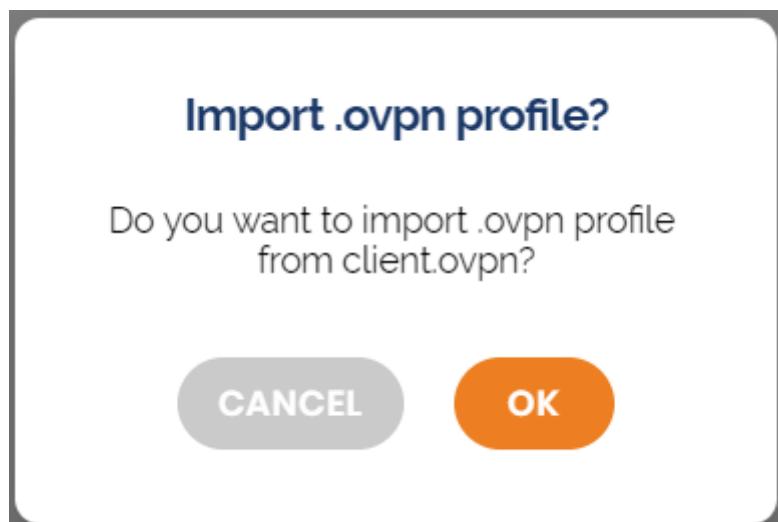
Bước 1: Truy cập <https://openvpn.net/client-connect-vpn-for-windows/> và tải về, cài đặt OpenVPN Connect V3 (Beta).



The screenshot shows the official OpenVPN Connect Client Program page. The title is "OpenVPN Connect for Windows". A paragraph describes it as the official client for Windows. It mentions that if you have an OpenVPN Access Server, you can download the client directly from it, which will be pre-configured for VPN for Windows. An orange button says "DOWNLOAD OPENVPN CONNECT V3 (BETA)". Below it, release notes for version 3.1.3 (713) beta are provided, along with download links for Windows 7, 8, 8.1, and 10, both 32-bit and 64-bit versions.

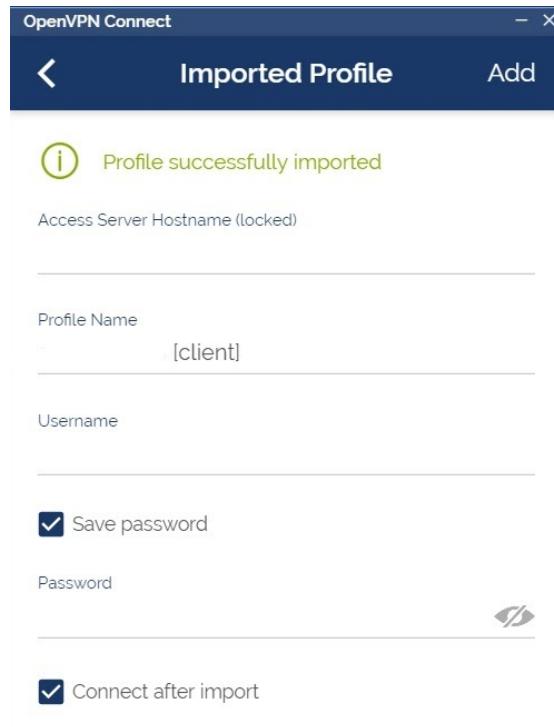
Bước 2: Lưu về máy file cấu hình cho client, rename đuôi extension từ “*client.conf*” thành “*client.ovpn*”

Bước 3: Sử dụng file cấu hình VPN bằng cách click đúp chuột vào file, sau đó cửa sổ OpenVPN Connect sẽ được mở ra kèm thông báo xác nhận import file cấu hình VPN.

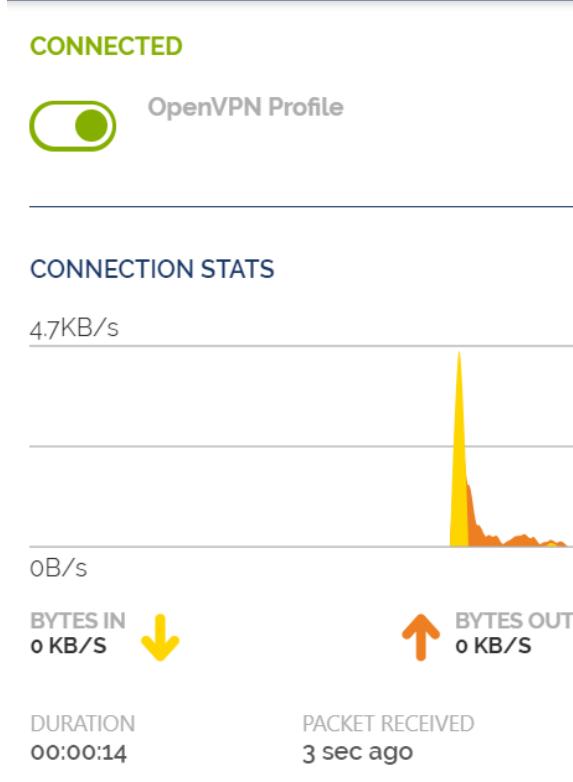


Bấm OK để xác nhận.

Bước 4: Tích vào Connect after import để kết nối.

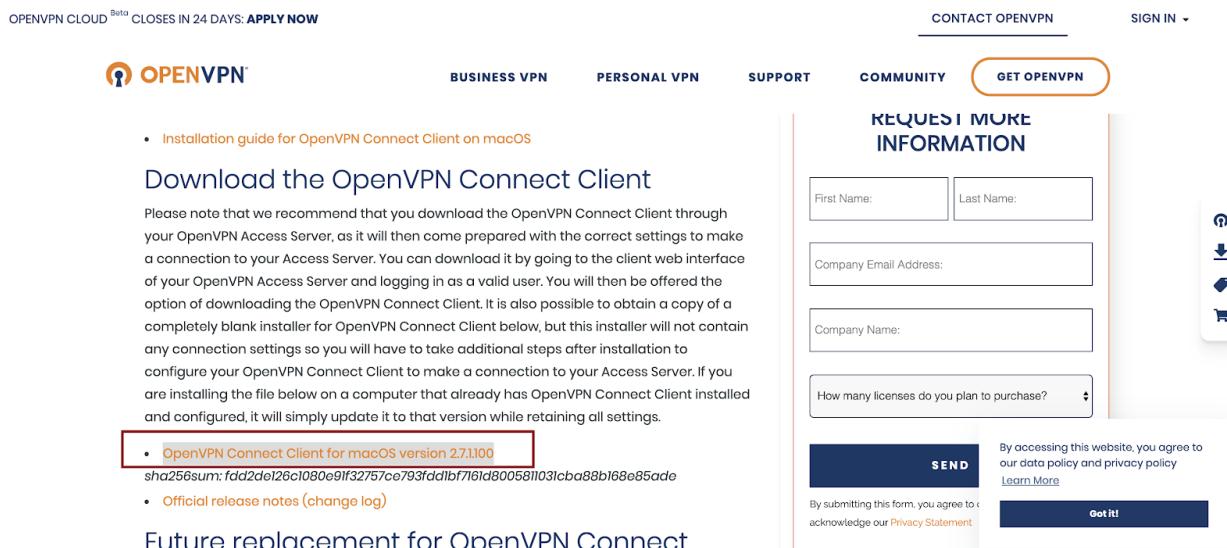


Giao diện sẽ hiện ra là Connected. Người dùng có thể tắt cửa sổ đó và sử dụng VPN.



MacOS:

Bước 1: Vào đường link <https://openvpn.net/vpn-server-resources/connecting-to-access-server-with-macos/> và ấn vào phần trong khung để download openvpn về.



The screenshot shows the OpenVPN website's download section for the macOS client. At the top, there are links for OPENVPN CLOUD (Beta closes in 24 days: APPLY NOW), CONTACT OPENVPN, and SIGN IN. Below these are navigation tabs for BUSINESS VPN, PERSONAL VPN, SUPPORT, COMMUNITY, and a highlighted GET OPENVPN button. To the right is a 'REQUEST MORE INFORMATION' form with fields for First Name, Last Name, Company Email Address, Company Name, and How many licenses do you plan to purchase? A 'SEND' button is at the bottom of the form, along with a note about agreeing to data policy and privacy policy, and a 'Learn More' link. On the far right, there are icons for a user profile, download, update, and cart. The main content area displays the download link for the OpenVPN Connect Client for macOS version 2.7.1.100, including its SHA256 sum and a link to official release notes.

OPENVPN CLOUD Beta closes in 24 days: APPLY NOW

BUSINESS VPN PERSONAL VPN SUPPORT COMMUNITY GET OPENVPN

REQUEST MORE INFORMATION

First Name: Last Name:

Company Email Address:

Company Name:

How many licenses do you plan to purchase?

SEND

By accessing this website, you agree to our data policy and privacy policy
[Learn More](#)

By submitting this form, you agree to acknowledge our [Privacy Statement](#)

Got it!

- Installation guide for OpenVPN Connect Client on macOS

Download the OpenVPN Connect Client

Please note that we recommend that you download the OpenVPN Connect Client through your OpenVPN Access Server, as it will then come prepared with the correct settings to make a connection to your Access Server. You can download it by going to the client web interface of your OpenVPN Access Server and logging in as a valid user. You will then be offered the option of downloading the OpenVPN Connect Client. It is also possible to obtain a copy of a completely blank installer for OpenVPN Connect Client below, but this installer will not contain any connection settings so you will have to take additional steps after installation to configure your OpenVPN Connect Client to make a connection to your Access Server. If you are installing the file below on a computer that already has OpenVPN Connect Client installed and configured, it will simply update it to that version while retaining all settings.

[OpenVPN Connect Client for macOS version 2.7.1.100](#)
sha256sum: fdd2de126c1080e9f32757ce793fdd1bf710d80058103cba88b168e85ade

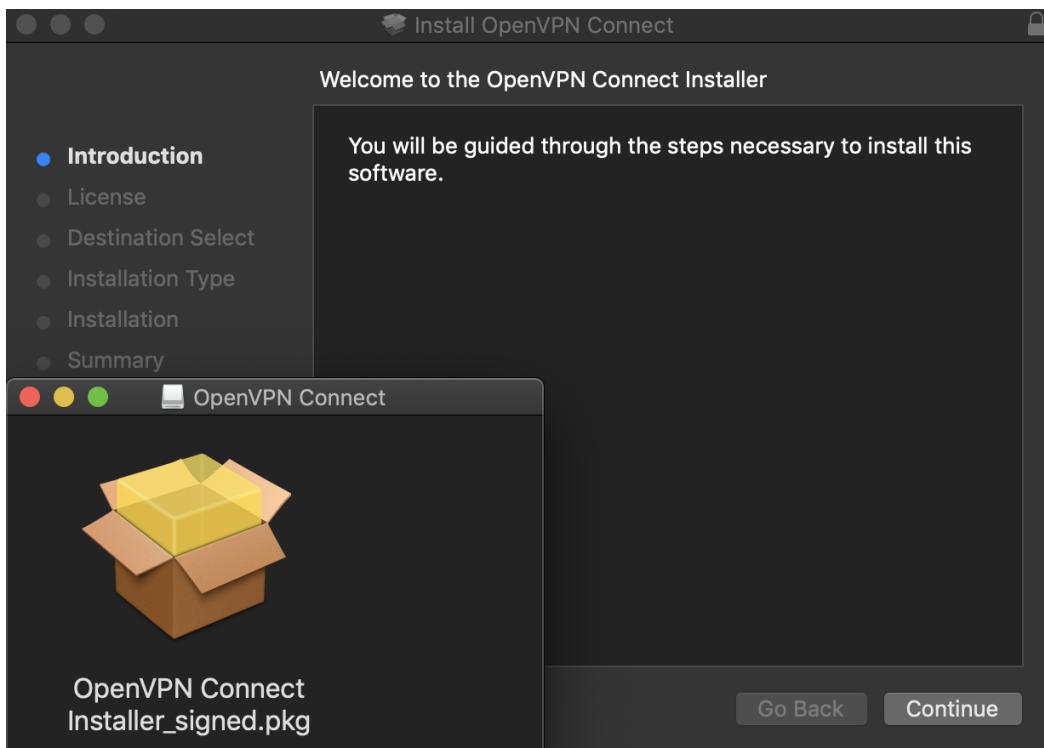
[Official release notes](#) ([change log](#))

Future replacement for OpenVPN Connect

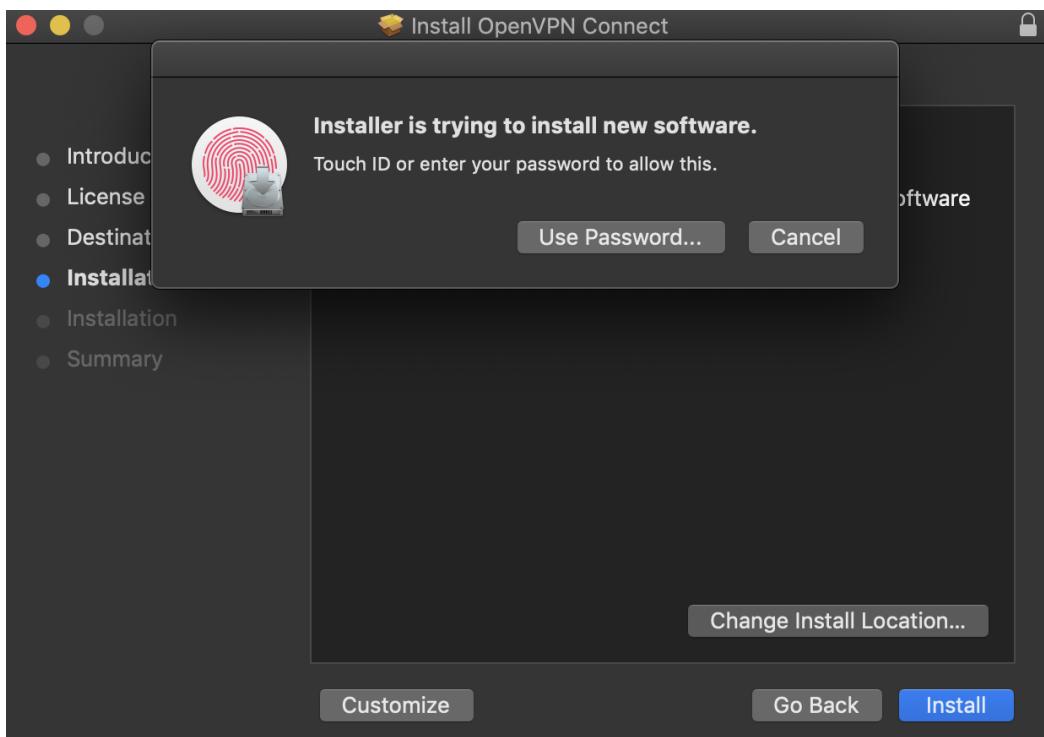
Bước 2: Ấn vào 'OpenVPN Connect installer' để tiếp tục cài đặt.



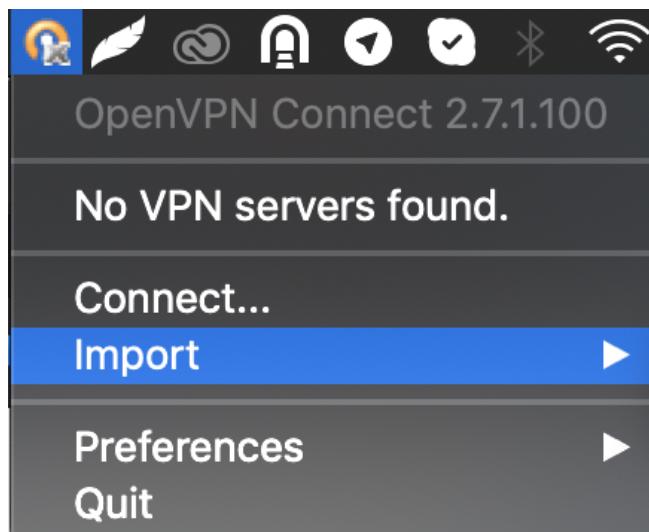
Bước 3: Click continue



Bước 4: Continue and Install

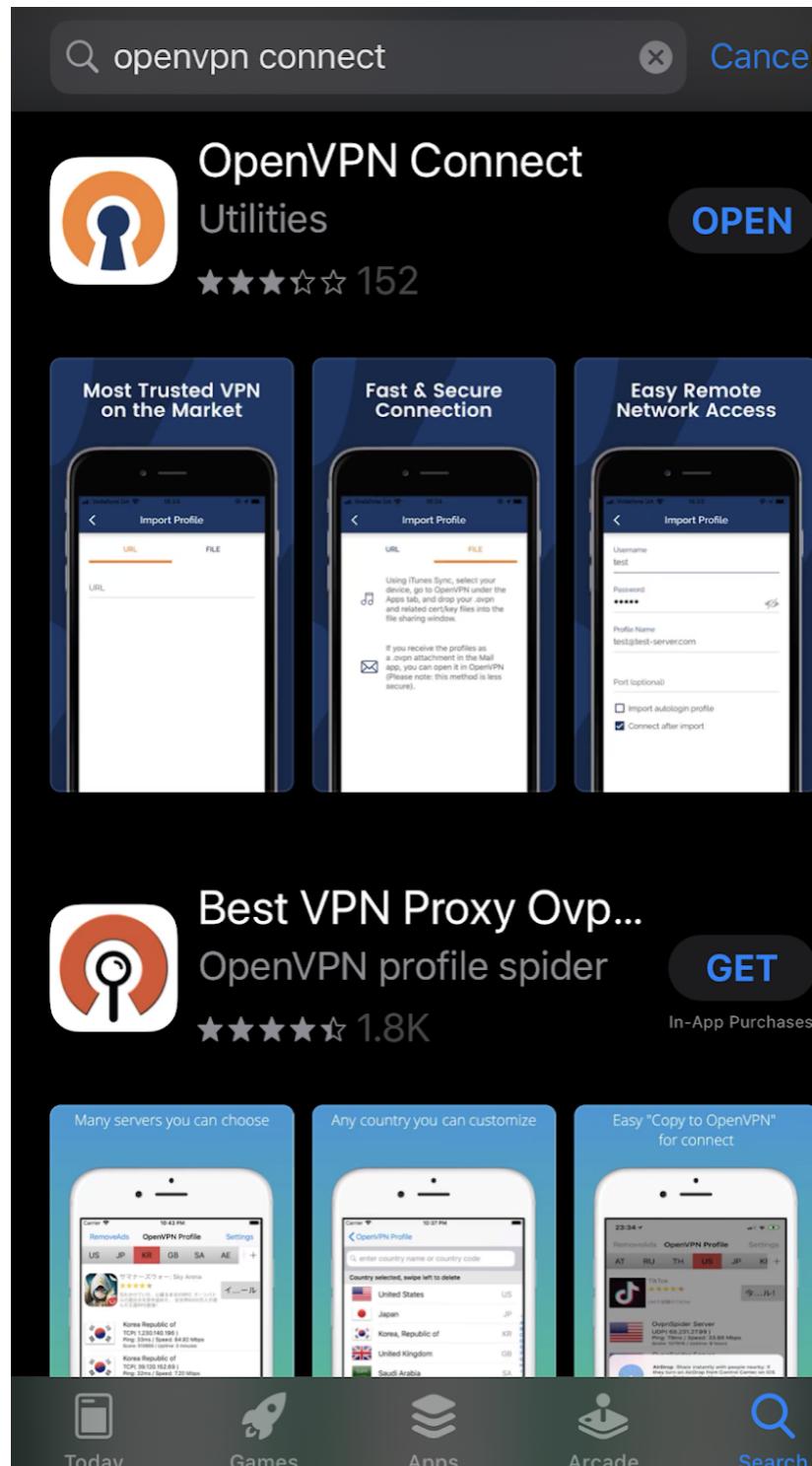


Bước 5: Nhấn vào biểu tượng góc phải màn hình và chọn From local file (import file) mà người dùng đã lưu về máy file cấu hình cho client, rename đuôi extension từ “client.conf” thành “client.ovpn”.



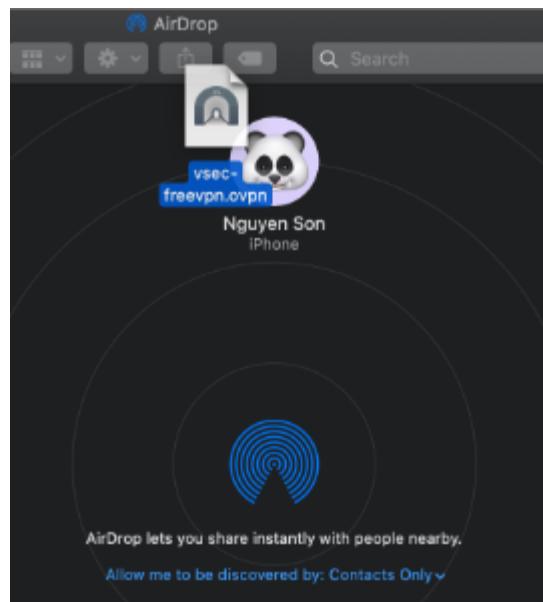
iOS:

Bước 1: Cài đặt ứng dụng :OpenVPN Connect từ App Store

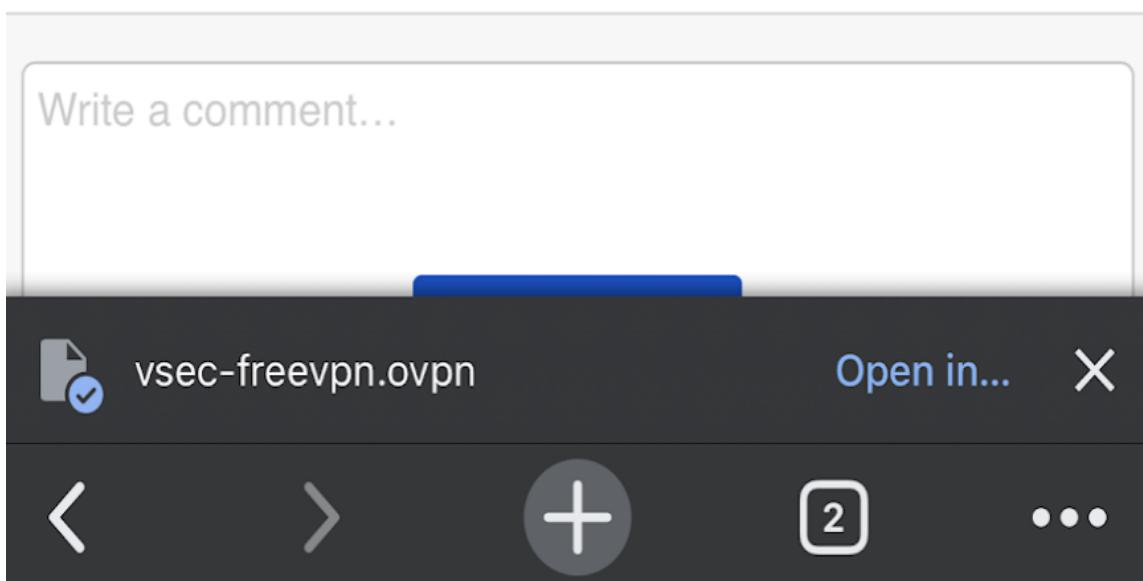


Bước 2: Copy file cấu hình vào máy

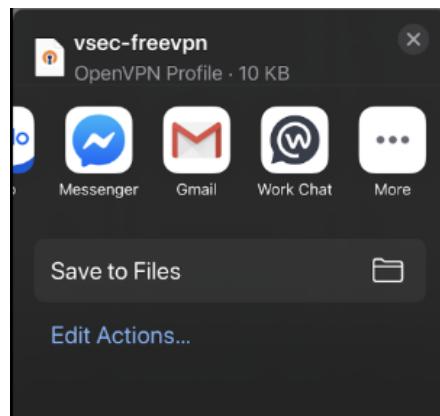
- Nếu bạn có máy Mac, bạn có thể sử dụng tính năng airdrop để gửi file từ máy tính của bạn sang thiết bị iOS



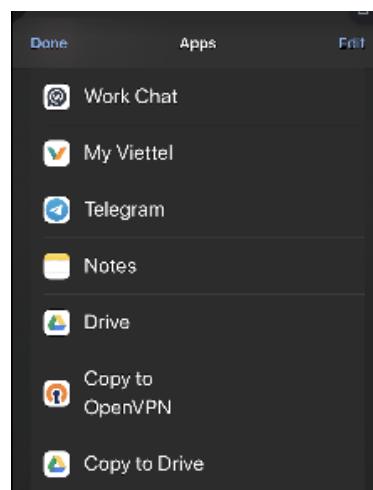
- Nếu bạn sử dụng Windows có thể copy file vào thiết bị qua Itunes.



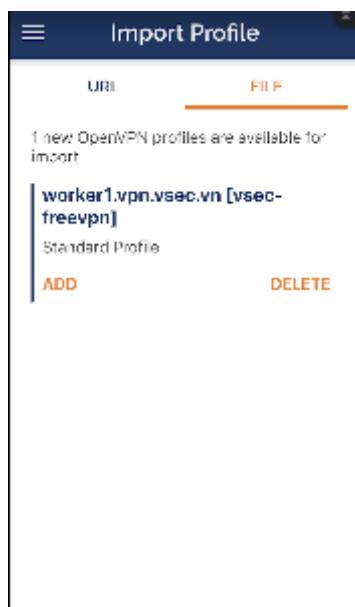
Bước 3: Sau khi lưu file cấu hình về , chọn Open in



Click vào More, tìm ứng dụng OpenVPN Connect

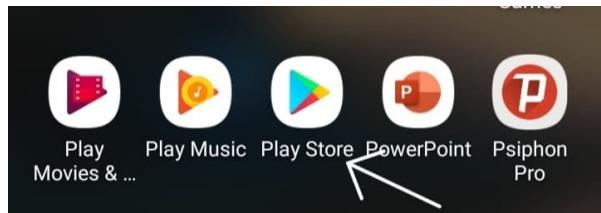


Chọn Add để import profile

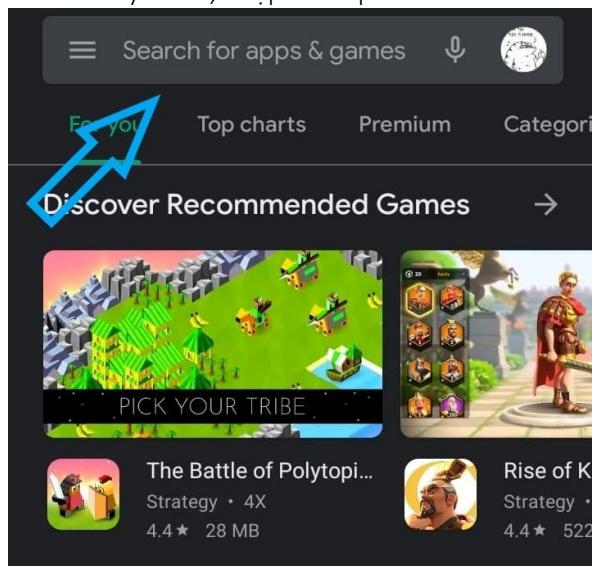


Android:

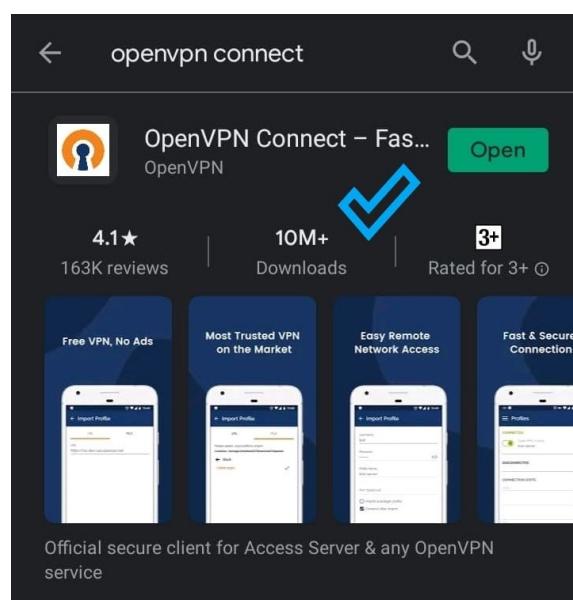
Bước 1: Tìm ứng dụng Play Store (CH Play) trên thiết bị:



Bước 2: Trên thanh tìm kiếm của Play Store, nhập vào OpenVPN Connect rồi bấm nút để tìm kiếm:



Bước 3: Chọn tải về đúng ứng dụng OpenVPN connect của nhà phát triển OpenVPN:



Bước 4: Lưu về máy file cấu hình cho client, rename đuôi extension từ “*client.conf*” thành “*client.ovpn*”.

Bước 5: Bật ứng dụng OpenVPN Connect.

Trong giao diện ứng dụng, bấm nút (+) để thêm file cấu hình cho thiết bị.



Bước 6: Chọn đúng hướng dẫn tới thư mục chứa tập tin cấu hình được lưu:



Bước 7: Tích vào Connect after import để kết nối vào VPN.

[← Imported Profile](#)[ADD](#)

 Profile successfully imported

Profile Name

worker1.vpn.vsec.vn [vsec-freevpn]

Username

Save password

Password



Connect after import

Đăng nhập thành công, giao diện thông báo Connected và VPN đã sẵn sàng để sử dụng.

 Profiles



CONNECTED



OpenVPN Profile

CONNECTION STATS

47KB/s

0B/s

BYTES IN
4.82 KB/S 

BYTES OUT
3.69 KB/S 

DURATION
00:00:13

PACKET RECEIVED
0 sec ago

YOU

YOUR PRIVATE IP

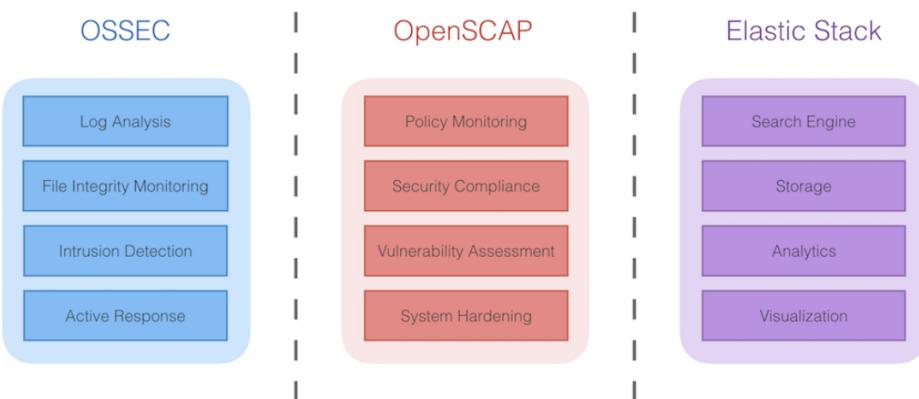
SERVER





Wazuh

Wazuh là 1 project mã nguồn dùng cho việc bảo vệ an ninh. Được xây dựng từ các thành phần : OSSEC HIDS, OpenSCAP và Elastic Stack.



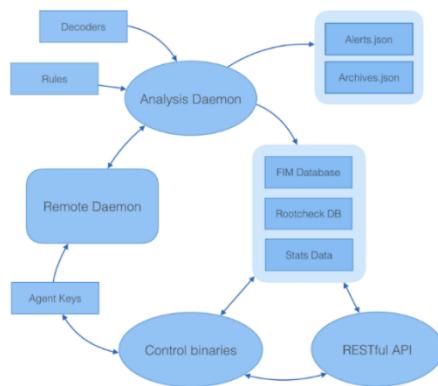
Hình 1.1: Thành phần Wazuh

- **OSSEC HIDS** : host-based Intrusion Detection System (HIDS) được dùng cho việc phát hiện xâm nhập, hiển thị và giám sát. Nó dựa vào 1 multi-platform agent cho việc đẩy dữ liệu hệ thống (log message, file hash và phát hiện bất thường) tới 1 máy quản lý trung tâm, nơi sẽ phân tích và xử lý, dựa trên các cảnh báo an ninh. Các agent truyền event data event data tới máy quản lý trung tâm thông qua kênh được bảo mật và xác thực. OSSEC HIDS cung cấp syslog server trung tâm và hệ thống giám sát không cần agent, cung cấp việc giám sát tới các event và thay đổi trên các thiết bị không cài được agent như firewall, switch, router, access point, thiết bị.
- **ELK Stack**: Sử dụng cho việc thu thập, phân tích, index, store, search và hiển thị dữ liệu log.

Thành phần chính bao gồm Wazuh server và Wazuh agent:

I. Wazuh server:

Thành phần server phụ trách việc phân tích dữ liệu nhận từ agent, tạo các ngưỡng cảnh báo khi 1 event ánh xạ với rule (phát hiện xâm nhập, thay đổi file, cấu hình không tương thích với policy, rootfit...)



Hình 1.2: Process trong Wazuh server

Server thông thường chạy các thành phần agent với mục tiêu giám sát chính nó. Một số thành phần chính của server là :

- *Registration service*: Được dùng để register agent mới được việc cung cấp và phân phối các key xác thực pre-shared, các key này là độc nhất với mỗi agent. Process này chạy như 1 network service và hỗ trợ việc xác thực qua TLS/SSL với 1 fixed password.
 - *Remote daemon service*: Service này nhận dữ liệu từ agent. Nó sử dụng pre-shared key để xác thực định danh của mỗi agent và mã hóa giao tiếp với chúng.
 - *Analysis daemon*: Process này thực hiện việc phân tích dữ liệu. Nó sử dụng các bộ giải mã để nhận dạng thông tin được xử lý (các Windows event, SSHD logs...) và sau đó giải nén các yếu tố dữ liệu thích hợp từ log message (source ip, event id, user...) Sau đó, bằng cách sử dụng các rule được định nghĩa bằng cách pattern đặc biệt trên bộ giải mã, nó sẽ tạo các ngưỡng cảnh báo thậm chí ra lệnh để thực hiện các biện pháp đối phó như chặn IP trên firewall.
 - *RESTful API*: Cung cấp interface để quản lý và giám sát cấu hình và trạng thái triển khai của các agent. Nó cũng được dùng bởi Wazuh web interface (Kibana)

Một Elasticsearch index là một tập hợp các document có một chút đặc trưng tương tự nhau (như các trường chung hoặc các yêu cầu về data retention được chia sẻ). Wazuh sử dụng 3 index khác nhau, được tạo hàng ngày và lưu trữ các event khác nhau :

- *Wazuh-alert*: Index cho các cảnh báo được sinh ra bởi Wazuh server mỗi khi một event ứng với rule tạo ra.

- *Wazuh-events*: Index cho tất cả các event (archive data) được nhận từ các agent, bất kể có ứng với rule hay không.
- *Wazuh-monitoring*: Index cho dữ liệu liên quan đến trạng thái agent. Nó được dùng bởi web interface cho việc hiển thị agent đã hoặc đang "Active", "Disconnect" hoặc "Never connected"

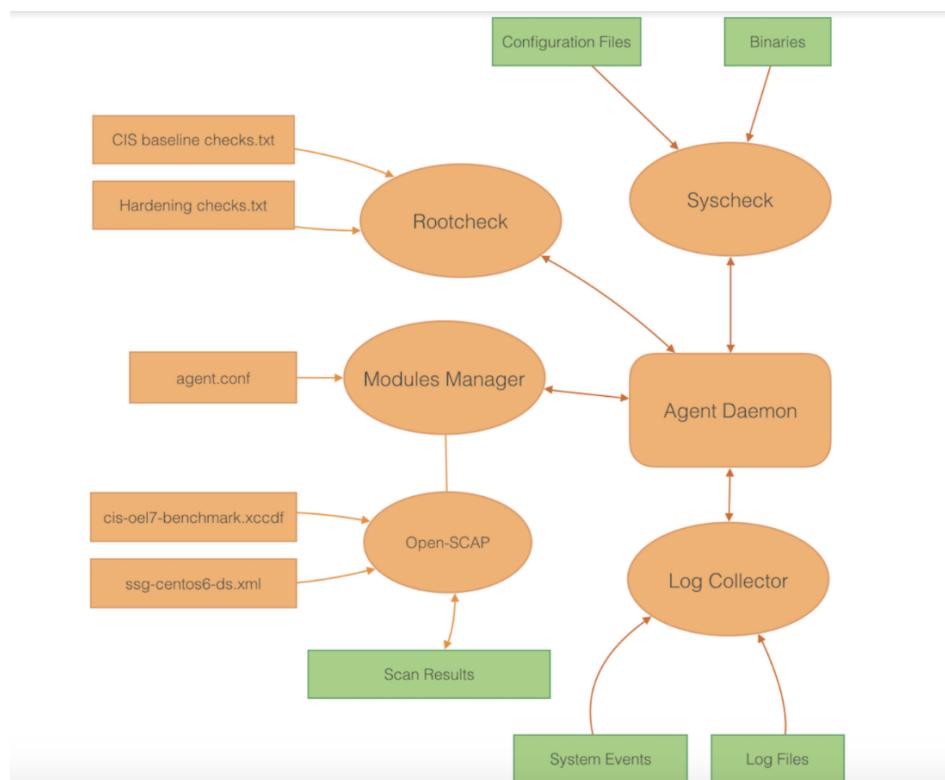
Với các index trên, document là các cảnh báo, archived event hoặc status event riêng lẻ.

II. Wazuh agent

Chạy trên : Windows, Linux, Solaris, BSD hoặc MAC OS. Dùng thu thập các dạng khác nhau của dữ liệu hệ thống và ứng dụng. Dữ liệu được chuyển tới Wazuh server thông qua 1 kênh được mã hóa và xác thực. Để thiết lập kênh này, 1 quá trình đăng ký bao gồm pre-shared key duy nhất được thiết lập.

Các agent task hoặc process khác nhau được dùng để giám sát hệ thống theo các cách khác nhau (giám sát sự thay đổi về file, đọc log, quét các thay đổi hệ thống).

Sơ đồ sau thể hiện các internal task và process diễn ra trên các agent level.



Hình 3.8: Process trong wazuh agent

Tất cả các process agent có mục tiêu và thiết lập khác nhau.

- *Rootcheck*: Thực hiện các task liên quan đến phát hiện về Rootkits, malware và các bất thường của hệ thống. Nó chạy 1 số công cụ kiểm tra an ninh cơ bản dựa vào các file cấu hình hệ thống.
- *Log Collector*: Dùng để đọc và thu thập các log message, bao gồm các file flat log như Windows event log và thậm chí là Windows Event Channel. Nó cũng được cấu hình để chạy định kỳ và bắt 1 số output của các câu lệnh cụ thể.
- *Syscheck*: Process này thực hiện file integrity monitoring (FIM) (Giám sát tính toàn vẹn của file). Nó cũng có thể giám sát registry key trên Windows. Nó sẽ bắt các thay đổi về nội dung file, quyền và các thuộc tính khác, cũng như phát hiện việc tạo và xóa file.
- *OpenSCAP*: Được dùng để publish OVAL và XCCDF dựa vào các hồ sơ bảo mật cơ bản, định kỳ quét hệ thống, nó sẽ phát hiện được các ứng dụng và cấu hình sẽ bị tấn công, không tuân theo các chuẩn được xác định theo CIS (Center of Internet Security)
- *Agent Daemon*: Process nhận dữ liệu được tạo hoặc được thu thập bởi tất cả các thành phần agent khác. Nó nén, mã hóa và phân phối dữ liệu tới server thông qua kênh được xác thực. Process này chạy trên "chroot" environment được cô lập, có nghĩa rằng nó sẽ hạn chế truy cập tới các hệ thống được giám sát. Điều này cải thiện được an toàn cho agent vì process đó là process duy nhất kết nối tới mạng.

Chú giải :

- *Rootkits*: Phần mềm hoặc công cụ phần mềm che giấu sự tồn tại của 1 phần mềm khác, thường là virus xâm nhập vào hệ thống.
- Malware: Mọi loại mã gây hại trên máy tính người dùng : spyware, trojan, virus...

Các bước cài đặt Wazuh

1. Cài đặt wazuh

```
apt-get install curl apt-transport-https lsb-release gnupg2
curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | apt-key add -
echo "deb https://packages.wazuh.com/3.x/apt/ stable main" | tee -a
/etc/apt/sources.list.d/wazuh.list
apt-get update
apt-get install wazuh-manager=3.11.4-1
systemctl status wazuh-manager
```

2. Cài đặt wazuh-api

```
# wazuh-api sử dụng nodejs, do đó phải cài đặt nodejs trước
curl -sL https://deb.nodesource.com/setup_8.x | bash -
apt-get install nodejs
apt-get install wazuh-api
# block auto-update
echo "wazuh-manager hold" | sudo dpkg --set-selections
echo "wazuh-api hold" | sudo dpkg --set-selections
```

3. Cài đặt elk

```
apt install default-jdk
apt-get install elasticsearch=7.6.1
# disable swap
swapoff -a
# remove all swap partition in fstab
# cấu hình tăng limit, sửa file, /etc/security/limit.conf, thêm các dòng sau.
```

```
* soft nofile 65536
* hard nofile 131072
* soft nproc 9012
* hard nproc 10000
# cấu hình để elasticsearch lưu trữ toàn bộ memory trên RAM.
systemctl edit elasticsearch
# thêm các dòng sau
[Service]
LimitMEMLOCK=infinity
# sau khi cấu hình xong chạy,
systemctl daemon-reload
# trong file cấu hình của elasticsearch, /etc/elasticsearch/elasticsearch.yml, thêm dòng sau
bootstrap.memory_lock: true
# sửa file /etc/elasticsearch/jvm.options
-Xms6g
-Xmx6g
# cấu hình cluster, điền IP server cài elasticsearch
discovery.seed_hosts: ["a.b.c.d"]
cluster.initial_master_nodes: ["a.b.c.d"]
```

4. Cài đặt filebeat

```
curl -s https://artifacts.elastic.co/GPG-KEY-elasticsearch | apt-key add -
echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | tee
/etc/apt/sources.list.d/elastic-7.x.list
apt-get update
apt-get install filebeat=7.6.1
# download file cấu hình
```

```
curl -so /etc/filebeat/filebeat.yml  
https://raw.githubusercontent.com/wazuh/wazuh/v3.11.4/extensions/filebeat/7.x/filebeat.yml  
curl -so /etc/filebeat/wazuh-template.json  
https://raw.githubusercontent.com/wazuh/wazuh/v3.11.4/extensions/elasticsearch/7.x/wazuh-template.json  
curl -s https://packages.wazuh.com/3.x/filebeat/wazuh-filebeat-0.1.tar.gz | sudo tar -xvz -C /usr/share/filebeat/module  
filebeat setup --index-management -E setup.template.json.enabled=false  
# sau khi download file cấu hình cần sửa địa chỉ Elasticsearch = địa chỉ tương ứng của khách hàng
```

5. kibana

```
apt-get install kibana=7.6.1  
https://packages.wazuh.com/key/GPG-KEY-WAZUH  
https://packages.wazuh.com
```

6. Cài đặt wazuh app

```
cd /use/share/kibana  
sudo -u kibana bin/kibana-plugin install https://packages.wazuh.com/wazuhapp/wazuhapp-3.11.4\_7.6.1.zip  
# secure wazuh-api, run and set user/pass  
/var/ossec/api/scripts/configure\_api.sh  
# setup wazuh app, fill the user/pass above to the conf file  
vi /usr/share/kibana/plugins/wazuh/wazuh.yml
```

Các bước thêm agent wazuh

1. Trên server

```
#Thêm agent. Tên agent là ubuntu-ag, Địa chỉ ip address hoặc IP là any  
/var/ossec/bin/manage_agents -a any -n ubuntu-ag

#Xem list agent  
/var/ossec/bin/manage_agents -l

#Xem key với ID tương ứng  
/var/ossec/bin/manage_agents -e ID
```

2. Cài đặt client trên linux

```
#Cài đặt wazuh agent  
apt-get install curl apt-transport-https lsb-release gnupg2

curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | apt-key add -  
  
echo "deb https://packages.wazuh.com/3.x/apt/stable main" | tee  
/etc/apt/sources.list.d/wazuh.list  
  
apt-get update  
  
apt install wazuh-agent  
  
#Xác minh agent  
/var/ossec/bin/manage_agents -i key
```

```
root@hung-artifact:~# /var/ossec/bin/manage_agents -i MDY5IHRlc  
lMDJjZWY1MDA00TFjMDUyOGM2MjA2MmM3MjJiYzE4MDE2MTZjNTZLYmM3N2NlND
```

Agent information:

ID:069

Name:test-ubuntu

IP Address:any

Confirm adding it?(y/n): y
Added.

#Sửa file config wazuh agent

Sửa địa chỉ address

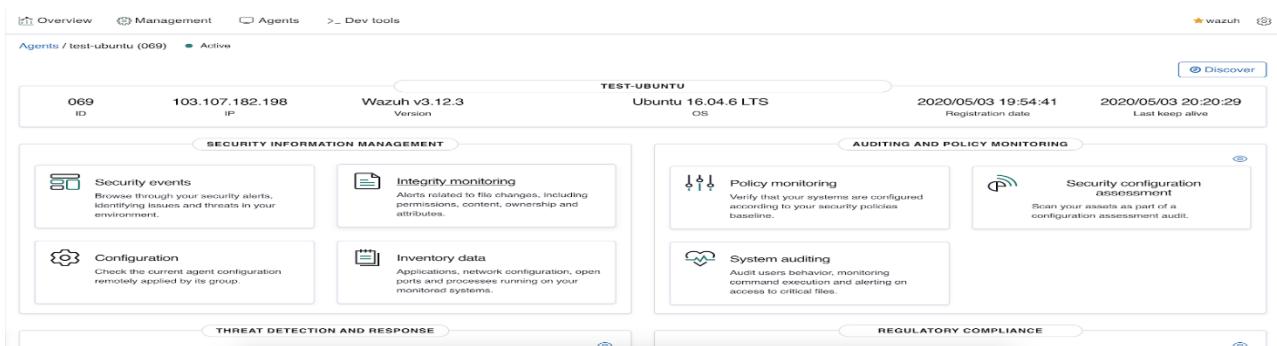
Sửa port

#Restart server wazuh agent

systemctl restart wazuh-agent.service

```
<ossec_config>
  <client>
    <server>
      <address>m[REDACTED]</address>
      <port>5555</port>
      <protocol>tcp</protocol>
```

Kết quả

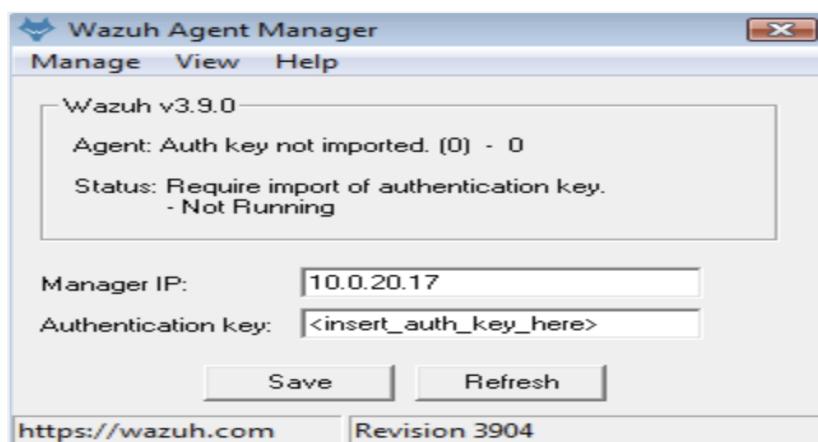


The screenshot shows the Wazuh Agent Overview page for agent ID 069, which is active and connected to the IP 103.107.182.198. The agent is running Wazuh v3.12.3 on Ubuntu 16.04.6 LTS. It was registered on 2020/05/03 at 19:54:41 and last kept alive on 2020/05/03 at 20:29:29. The page is divided into several sections: SECURITY INFORMATION MANAGEMENT, AUDITING AND POLICY MONITORING, THREAT DETECTION AND RESPONSE, and REGULATORY COMPLIANCE. Each section contains cards for Security events, Configuration, Integrity monitoring, Inventory data, Policy monitoring, System auditing, and Security configuration assessment.

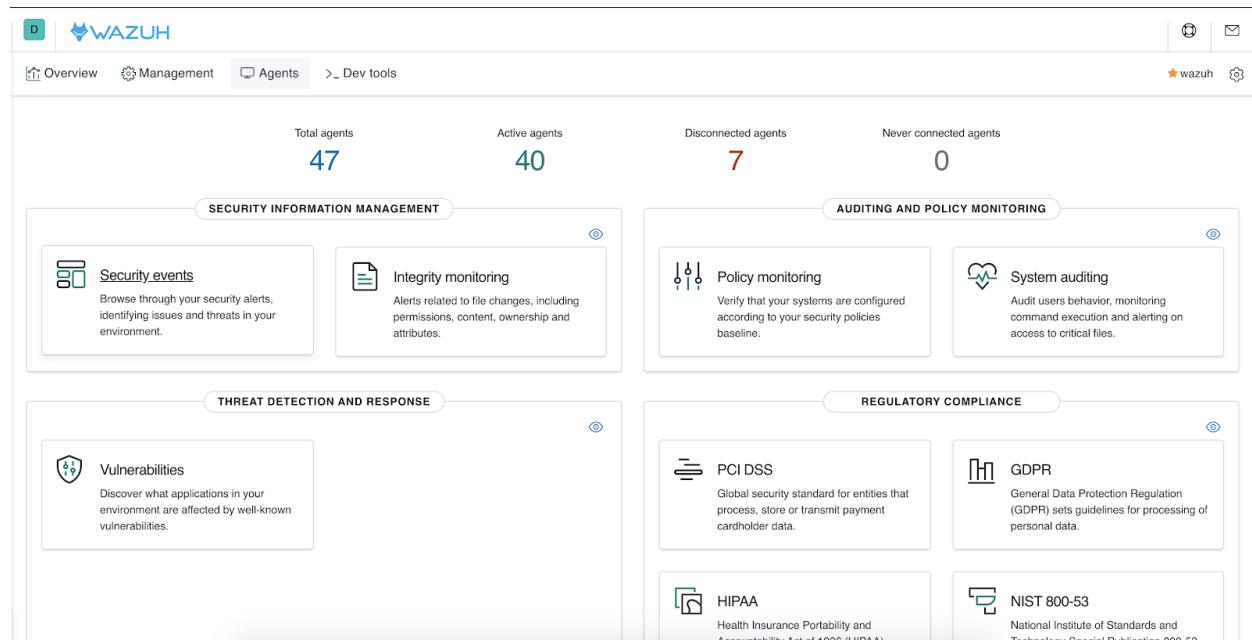
3. Thêm agent trên window

```
#Cài đặt wazuh agent dùng CMD
wazuh-agent-3.11.4-1.msi /q

#Sửa file config trên window như hình dưới
Thay manage IP: IP server hoặc domain server
Add key đã gen trên server
```



Hình ảnh khi cài đặt xong wazuh



The screenshot shows the Wazuh web interface with several sections:

- OVERVIEW:** Shows Total agents (47), Active agents (40), Disconnected agents (7), and Never connected agents (0).
- SECURITY INFORMATION MANAGEMENT:**
 - Security events:** Browse through your security alerts, identifying issues and threats in your environment.
 - Integrity monitoring:** Alerts related to file changes, including permissions, content, ownership and attributes.
- AUDITING AND POLICY MONITORING:**
 - Policy monitoring:** Verify that your systems are configured according to your security policies baseline.
 - System auditing:** Audit users behavior, monitoring command execution and alerting on access to critical files.
- THREAT DETECTION AND RESPONSE:**
 - Vulnerabilities:** Discover what applications in your environment are affected by well-known vulnerabilities.
- REGULATORY COMPLIANCE:**
 - PCI DSS:** Global security standard for entities that process, store or transmit payment cardholder data.
 - GDPR:** General Data Protection Regulation (GDPR) sets guidelines for processing of personal data.
 - HIPAA:** Health Insurance Portability and Accountability Act of 1996 (HIPAA)
 - NIST 800-53:** National Institute of Standards and Technology Special Publication 800-53

Hình ảnh wazuh gửi cảnh báo qua SMS khi có sự kiện level cao, có thể gây nguy hiểm cho hệ thống

Wazuh Notification.

2019 Dec 02 10:06:29

Received From: ip-20-0-**[REDACTED]**-3>/var/log/nginx/access.log

Rule: 31533 fired (level 10) -> "High amount of POST requests in a small period of time (likely bot)."

Src IP: 118.70.**[REDACTED]**

Portion of the log(s):

Thông tin inventory máy chủ - Network

Network interfaces

Name	MAC	State	MTU	Type
eth2	00:50:56:03:31:a9	up	1500	etherent
eth3	00:50:56:03:37:69	up	1500	etherent

Network ports

Local IP	Local port	State	Protocol
0.0.0.0	6379	listening	tcp
0.0.0.0	10050	listening	tcp
0.0.0.0	80	listening	tcp
0.0.0.0	20022	listening	tcp
0.0.0.0	443	listening	tcp
::	3306	listening	tcp6
::	6379	listening	tcp6
::	81	listening	tcp6
::	10050	listening	tcp6
::	20022	listening	tcp6

Thông tin inventory máy chủ - Packages

Packages

Packages				
Name	Architecture	Version	Vendor	Description
ConsoleKit	x86_64	0.4.1-3.el6	CentOS	System daemon for tracking users, sessions and seats
ConsoleKit-libs	x86_64	0.4.1-3.el6	CentOS	ConsoleKit libraries
GConf2	x86_64	2.28.0-6.el6	CentOS	A process-transparent configuration system
GConf2-devel	x86_64	2.28.0-6.el6	CentOS	Headers and libraries for GConf development
GeoIP	x86_64	1.6.5-1.el6	Fedor Project	Library for country/city/organization to IP address or hostname mapping
GeoIP-GeoLite-data	noarch	2015.12-1.el6	Fedor Project	Free GeoLite IP geolocation country database
GeoIP-GeoLite-data-extra	noarch	2015.12-1.el6	Fedor Project	Free GeoLite IP geolocation databases
GeoIP-devel	x86_64	1.6.5-1.el6	Fedor Project	Development headers and libraries for GeoIP
MAKEDEV	x86_64	3.24-6.el6	CentOS	A program used for creating device files in /dev
ORBit2	x86_64	2.14.17-5.el6	CentOS	A high-performance CORBA Object Request Broker

Rows per page: 10

< 1 2 3 4 5 ... 112 >

Formatted

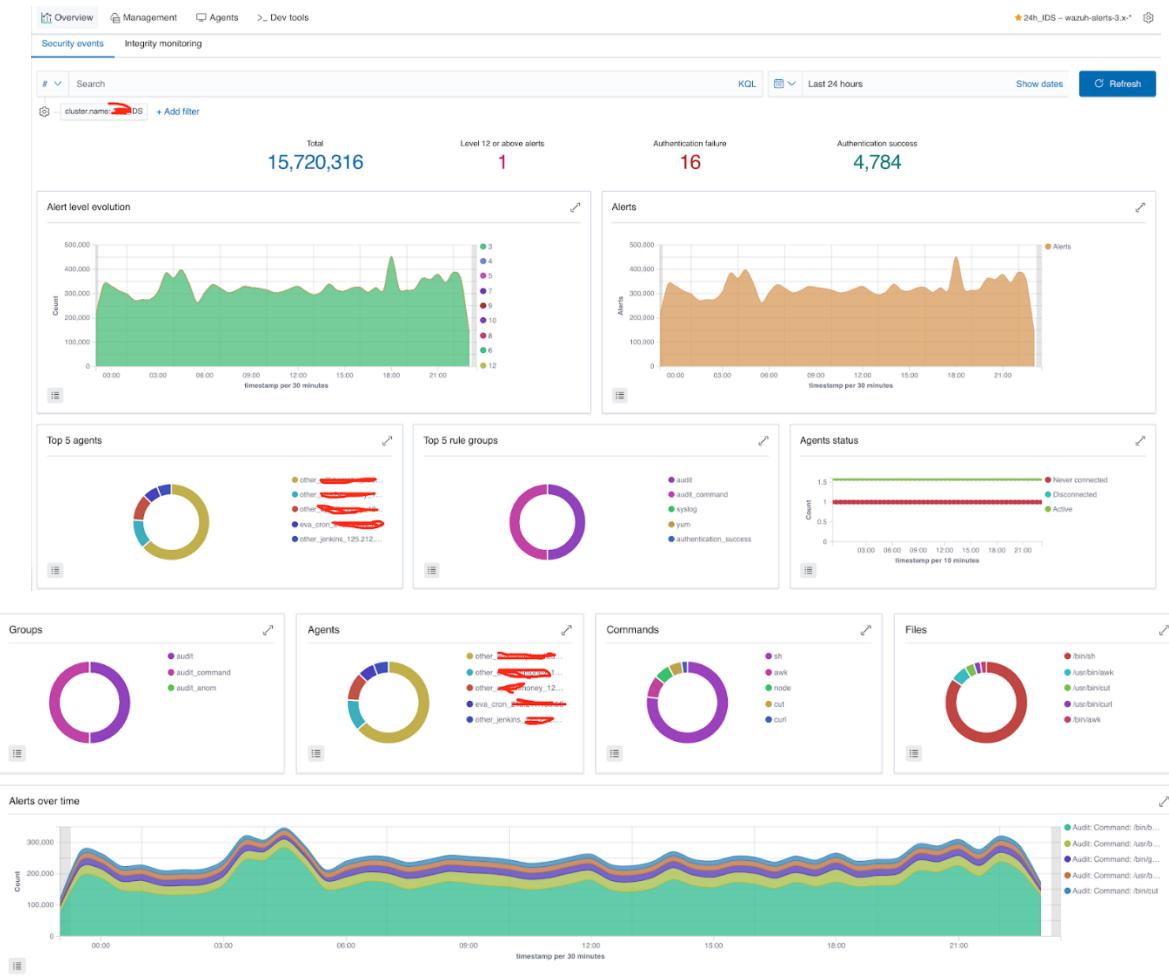
Thông tin inventory máy chủ - Processes

>_ Processes

Name	Effective user	Effective group	PID	Parent PID	Command	Args	VM size	Size	Session	Priority	State
init	root	root	1	0	/sbin/init	-	19360	4840	1	0	Interruptible sleep (waiting for an event to complete)
khreadd	root	root	2	0	-	-	0	0	0	0	Interruptible sleep (waiting for an event to complete)
migration/0	root	root	3	2	-	-	0	0	0	0	Interruptible sleep (waiting for an event to complete)
ksftfingd0	root	root	4	2	-	-	0	0	0	0	Interruptible sleep (waiting for an event to complete)
stopper/0	root	root	5	2	-	-	0	0	0	0	Interruptible sleep (waiting for an event to complete)
watchdog/0	root	root	6	2	-	-	0	0	0	0	Interruptible sleep (waiting for an event to complete)
migration/1	root	root	7	2	-	-	0	0	0	0	Interruptible sleep (waiting for an event to complete)
stopper/1	root	root	8	2	-	-	0	0	0	0	Interruptible sleep (waiting for an event to complete)
ksftfingd1	root	root	9	2	-	-	0	0	0	0	Interruptible sleep (waiting for an event to complete)
watchdog/1	root	root	10	2	-	-	0	0	0	0	Interruptible sleep (waiting for an event to complete)

Rows per page: 10 < 1 2 3 4 5 ... 32 > [Formatted](#)

Tổng quan về các sự kiện



Audit command

Alerts summary

Rule ID	Description	Level	Count
80792	Audit: Command: /bin/bash	3	8,404,226
80792	Audit: Command: /usr/bin/bash	3	1,535,151
80792	Audit: Command: /bin/gawk	3	947,497
80792	Audit: Command: /usr/bin/node	3	823,230
80792	Audit: Command: /bin/cut	3	617,260
80792	Audit: Command: /usr/bin/curl	3	300,234
80792	Audit: Command: /usr/bin/mysql	3	255,944
80792	Audit: Command: /usr/bin/wget	3	254,661
80792	Audit: Command: /usr/bin/php	3	175,775
80792	Audit: Command: /usr/local/bin/redis	3	169,697

Export: Raw ▲ Formatted ▲

1 2 3 4 5 ... 11 »

> Apr 23, 2020 @ 23:30:31.728	Audit: Command: /bin/rm	rm	-rf	/var/lock/lck_check.sh	0
> Apr 23, 2020 @ 23:30:27.894	Audit: Command: /bin/rm	rm	-rf	/var/lock/mysql.sh	0
> Apr 23, 2020 @ 23:30:26.004	Audit: Command: /bin/rm	rm	-rf	/var/lock/rsync_upload.sh	500
> Apr 23, 2020 @ 23:30:11.245	Audit: Command: /bin/rm	rm	-rf	/home/mdv/cache/quickcache/all/f8/qcc-f88e41b24c7ce842ac246f4df106747	501
> Apr 23, 2020 @ 23:30:10.785	Audit: Command: /bin/rm	rm	-rf	/home/mdv/cache/quickcache/all/8e/qcc-8e157f68889e9e18f51859fb2d70ef32	501
> Apr 23, 2020 @ 23:30:10.781	Audit: Command: /bin/rm	rm	-rf	/home/mdv/cache/quickcache/all/9d/qcc-9d79070c519c3f7d25c75a0e0489cd86	501
> Apr 23, 2020 @ 23:30:09.997	Audit: Command: /bin/rm	rm	-rf	/home/mdv/cache/quickcache/all/78/qcc-78af2f6986168b67846b1f4d8491322e	501
> Apr 23, 2020 @ 23:30:09.978	Audit: Command: /bin/rm	rm	-rf	/home/mdv/cache/quickcache/all/83/qcc-8382f4d2605d1b046c59c521eeb5af01	501

Giám sát sự thay đổi của files

```

File '/home/[REDACTED]/public_html/modules/blocks/header/header.php' checksum changed.
Size changed from '26414' to '26133'.
Old md5sum was: 'b49a778220a493ccc5ff22b7027e4c19'.
New md5sum is : 'a5a2162ed93faee66f223039c7c8ce8'.
Old sha1sum was: 'c0db5e201e4ebf172ece9542745db2c5a209d97b'.
New sha1sum is : 'e7ec86deb45b073e0f4d57096a4dabb8e7ee0b2e'.
Old sha256sum was: '5a6951f51cd1278f31c0472cf8822d1275c4e189ce607682dc415e55c46cc829'.
New sha256sum is : '1df773e510477a09892f27ec4c5f7ead8d4eac45d97df6e8f351fa05de88fe0b'.
Old modification time was: 'Fri Sep 27 05:13:24 2019', now it is 'Fri Apr 10 04:00:45 2020'.
(Audit) User: 'web[REDACTED] (500)'.
(Audit) Login user: 'web[REDACTED] (500)'.
(Audit) Effective user: 'web[REDACTED] (500)'.
(Audit) Group: 'web[REDACTED] (501)'.
(Audit) Process id: '28322'.
(Audit) Process name: '/usr/bin/scp'.
108,109d107
<           //$/v_code_script_criteo = xu_ly_gan_code_cript_criteo($v_row_slot_dfp,$v_region_id);
<           //$/this->setParam('v_code_script_criteo', $v_code_script_criteo);
269c267
<           $v_code_script_criteo = xu_ly_gan_code_cript_criteo($v_row_slot_dfp,$v_region_id);
---
>           $v_code_script_criteo = '';
395c393
<           $v_code_script_criteo = xu_ly_gan_code_cript_criteo($v_row_slot_dfp,$v_region_id);
---
>           $v_code_script_criteo = '';

```

Giám sát policy cấu hình

Alerts summary

Rule description	Control	Count
Host-based anomaly detection event (rootcheck).	File is owned by root and has written permissions to anyone.	408
System Audit event.	SSH Hardening - 8: Wrong Grace Time	19
System Audit event.	SSH Hardening - 4: No Public Key authentication	19
System Audit event.	SSH Hardening - 1: Port 22	19
System Audit event.	PHP - Allow URL fopen is enabled.	17
System Audit event.	CIS - RHEL6 - 4.1.2 - Network parameters - IP send redirects enabled	13
System Audit event.	CIS - RHEL6 - 1.4.3 - SELinux policy not set to targeted	13
System Audit event.	CIS - RHEL6 - 1.4.1 - SELinux Disabled in /etc/grub.conf	13
System Audit event.	CIS - RHEL6 - 1.1.16 - /dev/shm without 'noexec' set	13
System Audit event.	CIS - RHEL6 - 1.1.15 - /dev/shm without 'nosuid' set	13



Công ty Cổ phần An Ninh Mạng Việt Nam

Điện thoại: 024.7308 2299

Hỗ trợ: support(at)vsec.com.vn

Trụ sở: Tòa nhà N01A – Tầng M - Golden Land Building

275 Nguyễn Trãi, Hà Nội, Việt Nam