**TỔNG HỢP MÃ LỆNH TRIỂN KHAI ĐỒ ÁN**

*FIREWALL PFSENSE + SNORT + ZABBIX + TELEGRAM*

**1. TRIỂN KHAI FIREWALL PFSENSE**

Không cần lệnh CLI vì cấu hình qua WebGUI, mô tả logic cấu hình như sau:

*BƯỚC 1: Tạo Alias cho địa chỉ IP cần chặn*

IP TikTok: 23.32.74.112, 23.32.74.122

IP VnExpress: 111.65.250.2

*BƯỚC 2: Alias theo FQDN (Domain)*

- tiktok.com

- vnexpress.net

*BƯỚC 3: Alias cho máy Windows 10*

- IP: 192.168.1.100

*BƯỚC 4: Firewall > Rules > LAN*

Tạo rule BLOCK từ máy Win10 đến alias IP/FQDN

*BƯỚC 5: NAT Port Forward DNS*

Chuyển tất cả traffic DNS về pfSense:

Redirect DNS (53) về 192.168.1.1

**2. CÀI ĐẶT SNORT**

sudo apt update

sudo apt install -y build-essential libpcap-dev libpcre3-dev libdumbnet-dev \

bison flex zlib1g-dev liblzma-dev openssl libssl-dev libntirpc-dev

**Cài DAQ**

mkdir ~/snort\_src && cd ~/snort\_src

wget https://www.snort.org/downloads/snort/daq-2.0.7.tar.gz

sudo tar -xvzf daq-2.0.7.tar.gz

cd daq-2.0.7

./configure && make && sudo make install

**Cài Snort**

cd ~/snort\_src

wget https://www.snort.org/downloads/snort/snort-2.9.20.tar.gz

sudo tar -xvzf snort-2.9.20.tar.gz

cd snort-2.9.20

./configure --enable-sourcefire --disable-open-appid

make CFLAGS=-I/usr/include/ntirpc && sudo make install

sudo ldconfig

sudo ln /usr/local/bin/snort /usr/sbin/snort

**Tạo cấu trúc thư mục Snort**

sudo mkdir -p /etc/snort/rules/iplists

sudo mkdir -p /etc/snort/preproc\_rules

sudo mkdir -p /usr/local/lib/snort\_dynamicrules

sudo mkdir -p /etc/snort/so\_rules

sudo mkdir -p /var/log/snort/archived\_logs

sudo touch /etc/snort/rules/iplists/black\_list.rules

sudo touch /etc/snort/rules/iplists/white\_list.rules

sudo touch /etc/snort/rules/local.rules

sudo touch /etc/snort/sid-msg.map

cd ~/snort\_src/snort-2.9.20/etc

sudo cp \*.conf\* \*.map \*.dtd /etc/snort

cd ~/snort\_src/snort-2.9.20/src/dynamic-preprocessors/build/usr/local/lib/snort\_dynamicpreprocessor/

sudo cp \* /usr/local/lib/snort\_dynamicpreprocessor/

**CẤU HÌNH LUẬT TÙY CHỈNH SNORT**

**1. ICMP Ping**

sudo nano /etc/snort/rules/icmp.rules

alert icmp any any -> any any (msg:"Co hoat dong ping dang ngo"; sid:1000001; rev:1;)

**2. Port Scan**

sudo nano /etc/snort/rules/scan.rules

alert tcp any any -> any 1:1024 (msg:"Phat hien do quet cong TCP"; flags:S; sid:1000002; rev:1;)

**3. ICMP DoS**

sudo nano /etc/snort/rules/dos.rules

alert icmp any any -> any any (msg:"Phat hien tan cong DoS bang ICMP"; sid:1000003; rev:1;)

**Bật rules trong snort.conf:**

include $RULE\_PATH/icmp.rules

include $RULE\_PATH/scan.rules

include $RULE\_PATH/dos.rules

**Test config**

sudo snort -i ens33 -c /etc/snort/snort.conf -T

**Chạy snort**

sudo snort -i ens33 -c /etc/snort/snort.conf

**Kiểm tra log cảnh báo**

sudo tail -f /var/log/snort/alert

**3. CÀI ZABBIX SERVER + TELEGRAM ALERT**

**Cài Zabbix Server + Agent + MySQL**

sudo apt install mysql-server

sudo systemctl enable --now mysql

wget https://repo.zabbix.com/zabbix/7.0/ubuntu/pool/main/z/zabbix-release/zabbix-release\_latest\_7.0+ubuntu22.04\_all.deb

sudo dpkg -i zabbix-release\_latest\_7.0+ubuntu22.04\_all.deb

sudo apt update

sudo apt install -y zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-sql-scripts zabbix-agent

**Tạo database**

mysql -uroot -p <<EOF

create database zabbix character set utf8mb4 collate utf8mb4\_bin;

create user truc@localhost identified by '123456';

grant all privileges on zabbix.\* to truc@localhost;

set global log\_bin\_trust\_function\_creators = 1;

quit;

EOF

**Import dữ liệu**

zcat /usr/share/zabbix-sql-scripts/mysql/server.sql.gz | mysql -utruc -p zabbix

**Tắt log\_bin\_trust**

mysql -uroot -p -e "set global log\_bin\_trust\_function\_creators = 0;"

**Cấu hình DBPassword trong /etc/zabbix/zabbix\_server.conf**

sudo sed -i 's/ DBPassword=.\*/DBPassword=123456/' /etc/zabbix/zabbix\_server.conf

**Khởi động dịch vụ**

sudo systemctl enable --now zabbix-server zabbix-agent apache2

**Telegram Integration**

/usr/lib/zabbix/alertscripts/telegram.sh

Gán quyền thực thi: chmod +x telegram.sh

**Trong giao diện Zabbix:**

1. Administration > Media types > Script: telegram.sh

2. Users > Admin > Add media: Send to = <chat\_id>, type = Telegram

3. Configuration > Actions: Trigger alert → Telegram