# Instalasi & Konfigurasi Nginx + WAF (ModSecurity)

Langkah pertama adalah menghapus instalasi nginx apt

```
apt purge nginx
```

Pasang libmodsecurity

```
apt install libmodsecurity-dev libmodsecurity3
```

Unduh kode sumber nginx dan modsecurity nginx connector

```
apt install aptitude
aptitude install build-essential libpcre3 libpcre3-dev libssl-dev libtool \
  autoconf apache2-dev libxml2-dev libcurl4-openssl-dev automake \
  pkgconf zlib1g-dev

mkdir -p /usr/src/nginx-modsec
cd /usr/src/nginx-modsec
git clone https://github.com/SpiderLabs/ModSecurity-nginx.git

mkdir -p /usr/src/nginx
cd /usr/src/nginx
git clone -b branches/stable-1.20 https://github.com/nginx/nginx.git
```

Compile bersama nginx connector

```
auto/configure --add-module=/usr/src/nginx-modsec/ModSecurity-nginx \
  --prefix=/usr/local --with-http_ssl_module --with-http_v2_module \
  --http-log-path=/var/log/nginx/access.log \
  --error-log-path=/var/log/nginx/error.log --user=satpas \
  --group=satpas --with-http_geoip_module \
  --with-http_stub_status_module
```

Buat systemd unit service file

```
vim /etc/systemd/system/nginx.service
```

dengan konten sebagai berikut

```
[Unit]
Description=nginx unit
After=network.target

[Service]
Type=forking
```

```
ExecStartPre=/usr/local/nginx/sbin/nginx -t -c
/usr/local/nginx/conf/nginx.conf
ExecStart=/usr/local/nginx/sbin/nginx -c /usr/local/nginx/conf/nginx.conf
ExecReload=/usr/local/nginx/sbin/nginx -s reload
KillStop=/usr/local/nginx/sbin/nginx -s stop
KillMode=process
Restart=on-failure
RestartSec=42s
PrivateTmp=true
LimitNOFILE=200000

[Install]
WantedBy=multi-user.target
```

Buat symlink untuk direktori konfigurasi nginx ke etc:

```
ln -s /usr/local/nginx /etc/nginx
```

Import konfigurasi yang diperlukan:

```
wget
https://raw.githubusercontent.com/SpiderLabs/ModSecurity/v3/master/modsecuri
ty.conf-recommended
wget
https://raw.githubusercontent.com/SpiderLabs/ModSecurity/v3/master/unicode.m
apping
cp modsecurity.conf-recommended /usr/local/nginx/conf/modsecurity.conf
```

Aktifkan SecRuleEngine pada berkas modsecurity.conf dengan mengeksekusi perintah berikut:

```
sed -i "s/SecRuleEngine DetectionOnly/SecRuleEngine On/"
/usr/local/nginx/conf/modsecurity.conf
```

Tambahkan OWASP ModSecurity core rule set dengan eksekusi beberapa perintah berikut:

```
cd /usr/local/nginx/conf
git clone https://github.com/SpiderLabs/owasp-modsecurity-crs.git
cd owasp-modsecurity-crs
mv crs-setup.conf.example crs-setup.conf
cd rules
mv REQUEST-900-EXCLUSION-RULES-BEFORE-CRS.conf.example REQUEST-900-
EXCLUSION-RULES-BEFORE-CRS.conf
mv RESPONSE-999-EXCLUSION-RULES-AFTER-CRS.conf.example RESPONSE-999-
EXCLUSION-RULES-AFTER-CRS.conf
```

Buat sebuah berkas untuk mengaktifkan konfigurasi tadi kendalam sebuah file

```
vim /etc/nginx/modsec_includes.conf
```

Isinya sebagai berikut:

```
include /etc/nginx/modsecurity.conf
include /etc/nginx/owasp-modsecurity-crs/crs-setup.conf
include /etc/nginx/owasp-modsecurity-crs/rules/*.conf
```

Lalu pada berkas-berkas virtualhost, misalnya `/etc/nginx/conf.d/apps.conf`, tambahkan konfigurasi ini:

```
location / {
        modsecurity on;
        modsecurity_rules_file /etc/nginx/modsec_includes.conf;
        proxy_pass http://172.16.10.101:3000;
        include /etc/nginx/proxy.conf;
}
```

Konfigurasi tambahan untuk proxy pada berkas /etc/nginx/proxy.conf sebagai berikut:

```
proxy_http_version                 1.1;
proxy_cache_bypass                 $http_upgrade;

# Proxy headers
proxy_set_header Upgrade           $http_upgrade;
proxy_set_header Connection        $http_connection;
proxy_set_header Host              $host;
proxy_set_header X-Real-IP         $remote_addr;
proxy_set_header X-Forwarded-For   $proxy_add_x_forwarded_for;
proxy_set_header X-Forwarded-Proto $scheme;
proxy_set_header X-Forwarded-Host  $host;
proxy_set_header X-Forwarded-Port  $server_port;
proxy_set_header Origin            $http_origin;

# Proxy timeouts
proxy_connect_timeout              60s;
proxy_send_timeout                 60s;
proxy_read_timeout                 60s;
```

Aktifkan dan jalankan

```
systemctl daemon-reload
systemctl enable nginx
systemctl start nginx
systemctl status nginx
```

Demikian.

Catatan: dokumentasi ini merupakan salinan dari dokumen project dari tahun 2021 dengan penyesuaian sintaks untuk ditempel di dokuwiki ini.