OpenVPN

Wstęp

Poradnik jak skonfigurować OpenVPN'a, aby móc się logować za pomocą nazwy użytkownika i hasła oraz zarządzać nim z poziomu prostego panelu dostępnego po http. Panel jest napisany w PHPie i bazuje na bazie danych MySQL.

Instalacja

Instalujemy OpenVPN, Nginx + PHP:

```
aptitude install openvpn nginx php-auth php-auth-http php-auth-sasl php-db
php-doc php-file php-fpdf php-gettext php-html-template-it php-http php-
http-request php-http-upload php-image-text php-log php-mail php-mail-mime
php-mail-mimedecode php-mime-type php-net-checkip php-net-ftp php-net-imap
php-net-ipv4 php-net-ipv6 php-net-smtp php-net-socket php-net-url php-net-
url2 php-pear php-soap php-timer php-xml-parser php5 php5-cgi php5-cli php5-
curl php5-fpm php5-gd php5-geoip php5-gmp php5-imagick php5-imap php5-intl
php5-mcrypt php5-mysql php5-rrd php5-sasl php5-xcache php5-xsl mysql-server
mysql-client
```

Tworzymy katalog i kopiujemy do niego zawartość archiwum panelu:

```
mkdir -p /usr/share/nginx/o/
cd /usr/share/nginx/o/
wget http://kamil.orchia.pl/tmp/simple_openvpn_panel.7z
7z x simple_openvpn_panel.7z
chmod +x ./scripts/*
chmod -R o-rwx /usr/share/nginx/o
chown -R www-data:www-data /usr/share/nginx/o
rm simple_openvpn_panel.7z
```

Konfiguracja

OpenVPN:

```
cd /usr/share/doc/openvpn/examples/easy-rsa/2.0
source ./vars
./clean-all
./build-ca
./build-key-server server
./build-dh
mkdir /etc/openvpn/server
cp ./keys/{ca.crt,dh1024.pem,server.crt,server.key} /etc/openvpn/server/
```

Przykładowy plik /etc/openvpn/server/server.ovpn:

```
local 1.2.2.33
port 12345
proto tcp
dev tap
ca /etc/openvpn/server/ca.crt
cert /etc/openvpn/server/server.crt
key /etc/openvpn/server/server.key
dh /etc/openvpn/server/dh1024.pem
server 1.2.3.0 255.255.255.0
ifconfig-pool-persist /etc/openvpn/server/ipp.txt
push "route 10.20.0.0 255.255.255.0"
client-to-client
keepalive 10 120
persist-key
persist-tun
status /usr/share/nginx/o/openvpn-status.log
log /etc/openvpn/server/openvpn.log
verb 3
auth SHA1
cipher AES-128-CBC
tls-cipher DHE-RSA-AES128-SHA
client-cert-not-required
username-as-common-name
client-connect /usr/share/nginx/o/scripts/client_connect.sh
client-disconnect /usr/share/nginx/o/scripts/client_disconnect.sh
script-security 2
auth-user-pass-verify /usr/share/nginx/o/scripts/checkpass.sh via-file
up /etc/openvpn/server/up.sh
```

Przykładowy plik /etc/openvpn/server/openvpn.sh:

```
#!/bin/bash

pidfile="/etc/openvpn/server/pid"

pid=""

if [ -f $pidfile ];
then
        pid=`cat $pidfile`
fi

start()
{
        if [ "$pid" != "" ];
        then
                if [ "`ps aux | grep $pid | grep -v grep | wc -l`" == "1" ];
```

```
                then
                        echo "OpenVPN is already started!"
                else
                        openvpn --cd /etc/openvpn/server/ --config
server.ovpn --daemon --writepid $pidfile
                fi
        else
                openvpn --cd /etc/openvpn/server/ --config server.ovpn --
daemon --writepid $pidfile
        fi
}

stop()
{
        if [ "$pid" != "" ];
        then
                if [ "`ps aux | grep $pid | grep -v grep | wc -l`" == "1" ];
                then
                        kill $pid
                        echo "" > $pidfile
                fi
         fi
}

restart()
{
        stop
        sleep 5
        start
}

case "$1" in
        'start')
        echo -ne "Starting OpenVPN... "
        start
        echo "OK"
        ;;
        'restart')
        echo -ne "Restarting OpenVPN... "
        stop
        sleep 5
        start
        echo "OK"
        ;;
        'stop')
        echo -ne "Stopping OpenVPN... "
        stop
        echo "OK"
        ;;
        *)
        echo -e "\n Usage: openvpn.sh { start | stop | restart }"
```

```
        ;;
esac
```

Plik /etc/openvpn/server/up.sh:

```
#!/bin/sh

chmod o+r /usr/share/nginx/o/openvpn-status.log
```

Nadajemy uprawnienia:

```
chmod 700 /etc/openvpn/server/*.sh
/etc/openvpn/server/openvpn.sh start
```

Przykładowy plik client.ovpn, który dołączamy z plikiem ca.crt:

```
client
dev tap
proto tcp
remote 1.2.2.33 12345
resolv-retry infinite
nobind
persist-key
persist-tun
ca ca.crt
ns-cert-type server
verb 3
auth-user-pass
auth SHA1
cipher AES-128-CBC
tls-cipher DHE-RSA-AES128-SHA
```

MySQL:

```
cd /usr/share/nginx/o/
mysql -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 43
Server version: 5.5.44-0+deb7u1 (Debian)

Copyright (c) 2000, 2015, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input
statement.
```

```
mysql> CREATE USER 'openvpn'@'localhost' IDENTIFIED BY 'tajnepass';
Query OK, 0 rows affected (0.00 sec)

mysql> CREATE DATABASE openvpn;
Query OK, 1 row affected (0.00 sec)

mysql> GRANT ALL PRIVILEGES ON openvpn.* TO openvpn@'localhost';
Query OK, 0 rows affected (0.00 sec)

mysql> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.00 sec)

mysql> use openvpn;
Database changed
mysql> source ./initdb.sql;
Query OK, 0 rows affected (0.00 sec)

Query OK, 0 rows affected (0.00 sec)

Query OK, 0 rows affected (0.11 sec)

Query OK, 0 rows affected (0.08 sec)

Query OK, 0 rows affected (0.07 sec)

Query OK, 0 rows affected (0.08 sec)

Query OK, 0 rows affected (0.32 sec)
Records: 0  Duplicates: 0  Warnings: 0

Query OK, 0 rows affected (0.22 sec)
Records: 0  Duplicates: 0  Warnings: 0

Query OK, 0 rows affected, 1 warning (0.09 sec)

mysql> \q
Bye
```

Nginx:

```
        location /o/ {
                alias /usr/share/nginx/o/public/;
                allow 1.2.3.0/24;
                deny all;
                auth_basic "Restricted!";
                auth_basic_user_file /etc/nginx/htpasswd;
                index index.php;
                #try_files $uri /o/index.php;
                location ~ \.php$ {
                        fastcgi_split_path_info ^(.+\.php)(/.+)$;
                        fastcgi_pass unix:/var/run/php5-fpm.sock;
```

```
                        fastcgi_index index.php;
                        include fastcgi_params;
                }
        }
```

Przy generowaniu htpasswd pomoże nam link: http://kamil.orchia.pl/php/nginx.php

Sekcję allow i deny ustawiamy dopiero po dodaniu pierwszego użytkownika.

Kopiujemy plik /usr/share/nginx/o/config/config.ini.example:

```
cp /usr/share/nginx/o/config/config.ini.example
/usr/share/nginx/o/config/config.ini
```

Konfiguracja panelu jest odczytywana z pliku: /usr/share/nginx/o/config/config.ini

Uwaga! Pliki /usr/share/nginx/o/scripts/genfw.php oraz /usr/share/nginx/o/scripts/reload.php należy dostosować pod swoją konfigurację.

Crontab:

```
*/5 * * * * root cd /usr/share/nginx/o/scripts && ./reload.php
```