pfSense – как да направим защитна стена за вкъщи или за нашия офис

„Линукс за българи“,
София, март 2011

pfSense - въведение

- FreeBSD-базирана безплатна дистрибуция с отворен код за защитни стени (firewalls) и маршрутизатори (routers)
- Проектът стартира през 2004 на базата на m0n0wall
- Гъвкава дистрибуция със широко приложение
  - Защитна стена
  - Малък/домашен рутер
  - Рутер за средни/големи мрежи
  - Wireless Access Point
  - Устройство със специално предназначение – VPN, VoIP, DNS сървър, подслушване на мрежовия трафик, ...
- Версии
  - Последната стабилна 1.2.3
  - Експериментална 2.0-RC1

pfSense – възможности в 1.2.3 (FreeBSD 7.3)

- Защитна стена – pf от OpenBSD
  - Филтриране на IP, TCP и UDP по различни параметри
  - Ограничение на едновременните конекции за всяко правило
  - Избирателни логове за трафика за всяко правило
  - Филтриране по критерий OS
  - Policy Routing
  - Псевдоними (aliases) – групиране на IP-та, портове и мрежи
  - Прозрачно филтриране на етернет ниво
  - Нормализиране на трафика
  - Таблица със състояние на конекциите – ограничения и оптимизации
- Network Adress Translation (NAT)
- Redundancy – CARP, pfsync
- Load Balancing
- VPN – IPSec, OpenVPN, PPTP
- PPPoE
- Следене и състояние на системата
- Динамичен DNS
- Captive Portal
- DHCP Server и Relay

pfSense – нови възможности в 2.0 (FreeBSD 8.1)

- GRE и GIF тунели
- Поддръжка на 3G, LAGG, Dial up модеми, QinQ VLANs
- Виртуални IP адреси
- HTTPS Web GUI по подразбиране
- Филтриране на ниво 7
- Подобрени опции за NAT
- Драйвери за безжични мрежови адаптери
- Виртуални Access Points
- Нов тип VPN - L2TP
- Управление на сертификати
- Управление на портребители
  - Ограничение на достъпа за администатори
  - LDAP аутентикация
- Хронология на промените в конфигурацията

pfSense – налични пакети

- Advanced Routing – OpenBGP, OpenOSPF
- Телефония – FreeSWITCH, SIP proxy
- Управление на мрежата – zabbix, nagios
- Диагностика на мрежата – bandwithd, rated, iperf, nmap, pfflowd
- Уеб прокси – squid, squidGuard, Lightsquid, HAVP Antivirus
- Network Intrusion Detection - snort

Системни изисквания

- 100Mhz Pentium CPU, 128MB RAM, 1GB Hard driver/512MB CF card (embedded)
- В зависимост от необходимата производителност (throughput)
  - 10-20Mbps – 266Mhz CPU
  - 21-50Mbps – 500Mhz CPU
  - 51-200Mbps – 1GHz CPU
  - 201-500Mbps – 2.0Ghz CPU, PCI-e network adapters
  - 501Mbps+ - server-class hardware, 3.0Ghz CPU, PCI-X/PCI-e network adapters
- В зависимост от използваните възможности
  - VPN – CPU ресурс и/или HW entcyption, 500Mhz CPU за 10Mbps IPSec
  - Captive Portal - CPU ресурс
  - Големи таблици със състоянията на установените конекции – 1Кб RAM за всяка конекция
  - Използвани пакети – допълнително RAM за диагностика (snort, ntop,)

Инсталиране

- Изтегляне на версия - www.pfsense.org
- Подготвяне на инсталационната медиа
  - http://people.freebsd.org/~syrinx/fbsd-install-iso2img.sh
- Стартиране от инсталационната медиа
- Инсталиране в/у диска – опция 99
- Начална конфигурация на мрежовите интерфейси
- General Configuration Wizzard

Уеб конфигуратор

- Системно меню
  - Настройки на SSH сървър
  - Настройки на HTTP/HTTPS достъпа
  - Firmware Update
  - Инсталиране на пакети
  - Статични маршрути (static routes)
- Меню с интефрейси
- Меню за настройка на VPN

Уеб конфигуратор (2)

- Меню за настройка на защитната стена
  - Псевдоними
  - Правила
  - NAT
  - Виртуални IP адреси/CARP
  - Traffic Shaper
  - Планиране на правила

Уеб конфигуратор (3)

- Меню за настройка на услугите
- Статус меню
  - Системни логове
  - Графики
  - Презареждане на филтъра
  - ...
- Меню за диагностика
  - Запазване/възстановяване на конфигурация
  - Рестартиране на системата
  - ....

Пакети за диагностика

- States summary
- arping
- bandwithd
- iperf
- nmap
- rate / pfflowd
- Zabbix Agent (?)

Добавяне на OpenVPN

- Необходими пакети – OpenVPN Status
- Генериране на сертификати

```
> mkdir pfsense-keys
> cd /usr/local/share/doc/openvpn/easy-rsa/2.0/
> cp /etc/ssl/openssl.cnf ~/
> sudo chmod +x ./*
> /bin/bash
$ export KEY_CONFIG=$PWD/openssl.cnf
$ export KEY_DIR="/compat/linux/home/shteryana/pfsense-keys"
$ export KEY_COUNTRY="BG"
$ export KEY_PROVINCE="Sofia"
$ export KEY_CITY="Sofia"
$ export KEY_ORG="Shteryana"
$ export KEY_EMAIL="admin@shteryana.org"
$ export KEY_SIZE=1024
$ ./vars
NOTE: If you run ./clean-all, I will be doing a rm -rf on /usr/local/share/doc/openvpn/easy-rsa/2.0/keys
$ ./clean-all
$ ./build-ca
Generating a 1024 bit RSA private key
.........
$ ./build-key-server pfSenseVPN
.....................
$ ./build-key ShteryanaShopova
.............
$ which openssl
/usr/bin/openssl
$ export OPENSSL=/usr/bin/openssl
$ ./build-dh
....
```

- Конфигурация на OpenVPN сървър

Конфигурация на OpenVPN сървър

- Настройка на OpenVPN услугата
  - Address pool → адреси за VPN клиентите (напр. 172.16.1.0/24)
  - Authentication method → PKI
  - CA certificate → $KEY_DIR/ca.crt
  - Server certificate → $KEY_DIR/pfSenseVPN.crt
  - Server key → $KEY_DIR/pfSenseVPN.key
  - DH parameters → $KEY_DIR/dh1024.pem
  - Custom options → management 127.0.0.1 1194;
  - Description → (optional)
  - Local network → LAN мрежата (192.168.1.0/24)

Конфигурация на OpenVPN сървър (2)

- Правила на защитната стена
  - Псевдоними
    - OpenVPNPort (1194)
    - OpenVPNSubnet (172.16.1.0/24)
  - Правила
    - pass on WAN UDP from any to any port = 1194
    - pass on LAN UDP from LAN net to LAN net
  - NAT
    - NAT OutBound → Manual Outbound NAT rule generation
    - NAT on LAN from 172.16.1.0/24 to 192.168.1.0/24

Конфигурация на OpenVPN клиента

- Необходими файлове
  - $KEY_DIR/ca.crt
  - $KEY_DIR/ca.key
  - $KEY_DIR/ShteryanaShopova.crt
  - $KEY_DIR/ShteryanaShopova.csr
  - $KEY_DIR/ShteryanaShopova.key
  - $KEY_DIR/ShteryanaShopova.ovpn

Конфигурация на OpenVPN клиента (2)

- Конфигурационен файл

```
client
dev tun
proto udp
remote <server-ip> <port>
ping 10
resolv-retry infinite
nobind
user nobody
group nobody
persist-key
persist-tun
mute-replay-warnings
ca ca.crt
cert ShteryanaShopova.crt
key ShteryanaShopova.key
pull dhcp-options
mute 20
verb 3
```

Добавяне на Web Caching Proxy

- Необходими пакети
  - squid, squidGuard, Lightsquid
  - HAVP antivirus
- Конфигуриране на Proxy Server
  - Proxy interface → LAN
  - Allow users on interface → √
  - Transparent proxy → √
  - Bypass proxy for Private Address Space → √
  - Bypass proxy for these source IPs → (admin IP напр.)
  - Proxy port → 3128
  - Language → Bulgarian

Конфигуриране на Web Proxy Filter

- Основни настройки
  - Enable → √
  - Enable GUI log → √
  - Blacklist → √
  - Blacklist URL → (http://www.shallalist.de/Downloads/shallalist.tar.gz напр.)
- Създаване на ACLs
  - Proxy filter SquidGuard: Target categories
    - Name, Domains list, URLs list
  - Proxy filter SquidGuard: Common Access Control List (ACL)
    - Target Rules List → BlockedAll → deny
- Статистики за посетени сайтове
  - Services: Proxy server Report(LightSquid) → Lightsquid Report

Обновяване на системата

- http://doc.pfsense.org/index.php/UpgradeGuide
- Методи
  - Автоматично през SSH – опция 13
  - Ръчно през Web Configurator
- Обновяване през Web Configurator
  - Пълен Backup на системата (!)
  - Изтегляне на файл с обновленията
  - System: Firmware: Manual Update → Enable firmware upload
  - Firmware image file → (пътя до свалените файл)
  - Upgrade Firmware

Управление на потребители в pfSense 2.0

- Методи
  - Локални потребители
  - LDAP
  - Raduis
- Създаване на групи и права за достъп
  - System: Group manager
  - Assigned Privileges
  - System: User Manager

Въпроси?