UFW

 **Tento návod je určen pro pokročilé uživatele**

UFW neboli Uncomplicated Firewall je výchozí nástroj k nastavení pravidel pro firewall v Ubuntu. UFW je možné nastavovat pouze přes Terminál, a je proto vhodný hlavně pro servery. Používání UFW vyžaduje více zkušeností s Ubuntu. Méně zkušení uživatelé a uživatelé osobních počítačů jistě uvítají existenci GUFW, což je grafická nadstavba UFW.

Instalace

 Od vydání Ubuntu 8.04 je UFW součástí základní instalace Ubuntu i jeho derivátů.

 Nainstalujte balík ufw.

Spuštění

 UFW se spouští automaticky při startu systému. Ve výchozí instalaci je ovšem tato možnost zakázána. Spusťte tedy v terminálu příkaz

```
sudo ufw enable
```

čímž spouštění UFW při každém startu povolíte.

Spouštění UFW opět zakážete příkazem

```
sudo ufw disable
```

Použití

Nejprve dvě malé poznámky. Každé nastavení je možné předznačit parametrem `–dry-run`, který znamená „běh na sucho“, tedy jen zkusit co by nastavení ovlivnilo, ale neprovádět.

Postojů, který může firewall zaujmout je obecně několik:

- allow - povolit
- deny - zakázat (pro druhou stranu to vypadá, že nikdo nikdo neodpovídá/neexistuje)
- reject - zakázat, ale odpovědět, že aktivní odmítáme
- limit - povolit, ale omezit počet připojeních za nějakou časovou jednotku jako obranu proti brutal-force útokům. Např. více, jak 30 pokusů o spojení za minutu bude zakázáno.

Status

Příkazem

```
sudo ufw status
```

máte možnost zjistit jestli je firewall zapnut a jaká pravidla jsou použita.

Výchozí nastavení

Pokud neurčíte dále jinak, bude použito výchozí globální pravidlo, kterým můžete zakázat (doporučeno), povolit nebo odmítnout všechna příchozí spojení ze sítě. Obecná syntaxe je:

```
ufw [--dry-run] default allow|deny|reject [incoming|outgoing]
```

Pokud nedefinujeme směr (příchozí incoming nebo odchozí outgoing), bude se brát příchozí. Zakázání příchozího je doporučeno, ovšem odchozí způsobí, že se nedostanete nikam.

```
sudo ufw default deny
```

nebo povolit

```
sudo ufw default allow
```

Pokud

Pravidla

Kromě povolení/zakázání všech příchozích spojení, je nejdůležitější vlastností UFW možnost nastavení pravidel pro jednotlivé přenosy podle portu, protokolu nebo IP adresy.

Porty a protokoly

Zakázat/povolit přenosy podle konkrétní portu můžete příkazem

```
sudo ufw allow číslo_portu
```

respektive

```
sudo ufw deny číslo_portu
```

Volitelně můžete přidat i protokol. Tedy příkaz

```
sudo ufw allow číslo_portu/tcp

sudo ufw deny číslo_portu/tcp
```

pro povolení/zákaz přenosu na portu `číslo_portu` pro protokol `tcp`, respektive

```
sudo ufw allow číslo_portu/udp

sudo ufw deny číslo_portu/udp
```

pro protokol `udp`.

Služby

Přímo jednotlivé služby (tak jak jsou vypsány v `/etc/services`) můžete povolovat/blokovat příkazem

```
sudo ufw allow služba
```

respektive

```
sudo ufw deny služba
```

Pokročilá syntaxe

IP adresa

Přenos z konkrétní IP adresy můžete povolit/zakázat příkazem

```
sudo ufw allow from ip_adresa
```

respektive

```
sudo ufw deny from ip_adresa
```

IP adresa a port

Přenos z konkrétní IP adresy přes konkrétní port můžete povolit/zakázat příkazem

```
sudo ufw allow from ip_adresa to any port číslo_portu
```

respektive

```
sudo ufw deny from ip_adresa to any port číslo_portu
```

Smazání pravidla

Pravidlo smažete jednoduše příkazem

```
sudo ufw delete pravidlo
```

kde `pravidlo` je ve stejném formátu jako příkaz, kterým bylo zavedeno (bez `sudo ufw`).

Druhou možností místo složitého znovu vypisování pravidla je `ufw delete 3`, kde 3 je číslo našeho pravidla, které je vidět v `ufw status numbered`.

Omezení počtu spojeních

ufw podporuje parametrem `limit` možnost omezit počet spojeních jako obranu proti opakovaným pokusům např. při brutal-force útoku. ufw odmítne spojení, pokud se IP adresa pokusila navázat více, jak 6 a více spojeních během posledních 30 vteřin.

```
ufw limit ssh/tcp
```

Více informací o této schopnosti najdete na http://www.debian-administration.org/articles/187

Příklady

```
#Porty a protokoly
sudo ufw allow 53                                                    --->
Povolí přenos přes port 53.

sudo ufw deny 23/tcp                                               ---> Zakáže
přenos přes port 23 na protokolu tcp.

#Služby
sudo ufw deny ssh                                                    ---> Zakáže
SSH.

#IP adresa
sudo ufw deny from 207.46.232.182                          ---> Zakáže přenos z IP
adresy 207.46.232.182.

#IP adresa a port
sudo ufw allow from 192.168.0.4 to any port 22  ---> Povolí přenos z IP
adresy 192.168.0.4 přes port 22.
```

```
#Mazání
sudo ufw delete allow 53                                        ---> Smaže
dříve zavedené pravidlo, které umožňovalo
přenos přes port 53.
```

Logování

Ve výchozím nastavení není povolen ufw vůbec, a po `ufw enable` není povoleno logování. Logovacích úrovní rozlišuje ufw několik, ale úplně stačí úroveň on neboli low, kdy se loguje jen zablokované spojení.

```
ufw logging on              --> zapne (úroveň low)
ufw logging off              --> vypne
ufw logging LEVEL         --> zapne na určitou úroveň
```

Popis, co přesně logují jednotlivé úrovně viz manuálová stránka (`man ufw`).

V mém Ubuntu 10.04 Lucid Lynx se ukládají zprávy do `/var/log/ufw.log`.

Odkazy

- http://www.root.cz/clanky/ufw-firewall-jednoduse-a-rychle/ - další český návod
- Domovská stránka programu
- Anglický návod k UFW