Mikrotik RouterOS:

Základní zabezpečení RouterOS

Obsah

Platné verze

Mikrotik RouterOS verze 2.8.x

Úvod

Zabezpečení směrovače proti neautorizovaným pokusům o administraci je častou otázkou současných i budoucích uživatelů Mikrotik RouterOS. V následujícím dokumentu naleznete základní pokyny pro zajištění optimální míry bezpečnosti.

Elementární zásady bezpečnosti

Nejčastějším prostředkem pro administraci je grafická konzole WinBox. Samotná komunikace mezi WinBox a RouterOS je kryptována, pokud máte nainstalován balíček Security. Připojení k serveru proběhne na portu, kde běží služba www (standardně 80), další komunikace již běží na portu 3987, který je kryptován.

Další formy administrace jsou telnet a SSH. Telnet v žádném případě nepoužívejte, neboť se jedná o nekryptovaný přenos. SSH již ze svého názvu Secure Shell značí jeho poslání, tedy bezpečnou (šifrovanou) administraci.

Pro přenos souborů z/na RouterOS je možné využít službu FTP a SCP. Službu FTP nedoporučujeme ze stejných důvodu jako telnet. Přenos pomocí SCP je kryptován. Jako klienta SCP můžete použít pro Windows například WinSCP (winscp.sourceforge.net/cze/). SCP klienta v Unixu obsahuje jakýkoliv balíček SSH client.

Dalšími předpoklady jsou samozřejmě dostatečně silná hesla a jejich pravidelná obměna. Pokud zálohujete směrovač, je nutno brát v potaz, že ve výsledném BACKUP souboru je uloženo heslo v plain textu. Je tedy nutno zajistit bezpečný přenos (SCP) a uložení těchto souborů.

Zabezpeční služeb běžící na RouterOS

Na směrovači běží standardně tyto služby (naleznete je v `/ip service`):

Služba	Port
ftp	21
hotspot	80
hotspot-ssl	443
ssh	22
telnet	23
www	80

Služby hotspot a hotspot-ssl jsou aktivní pouze v případě, že je nainstalován balíček hotspot.

Zabezpečení služeb

Z hlediska bezpečnosti je krajně nevhodné, aby na směrovači běžely nezabezpečené služby (ftp, telnet) a služby, které se event. nepoužívají (hotspot, balíček můžete úplně odinstalovat, pokud ho nepoužíváte). Ostatní služby je vhodné přesunout na jiné (nestandardní) porty. Volbu portů provedete v menu `/ip service`, kde můžete také zadat, a to doporučuji, z jakých IP adres (jedna IP adresa nebo subnet) budou tyto služby přístupné. Pokud chcete zadat více adres nebo subnetů, můžete k tomu použít pravidla ve firewallu:

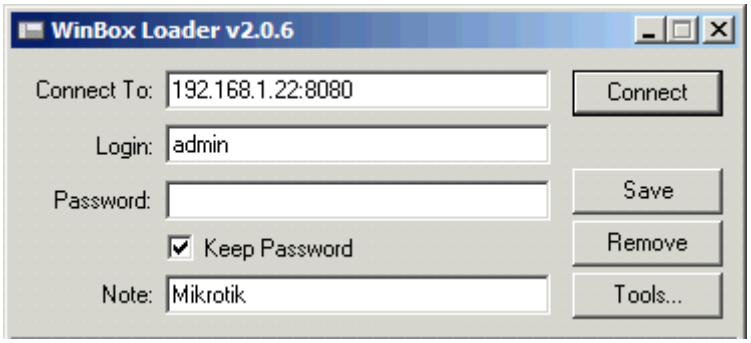
```
ip firewall rule input

add src-address=10.10.10.0/24 dst-address=:2222 protocol=tcp action=accept \
    comment="" disabled=no
add dst-address=:2222 protocol=tcp action=drop comment="" disabled=no

add src-address=10.10.10.0/24 dst-address=:8080 protocol=tcp action=accept \
    comment="" disabled=no
add dst-address=:8080 protocol=tcp action=drop comment="" disabled=no
```

S tímto nastavením budou služby www a ssh přístupné pouze z adres v rozsahu 10.10.10.1 – 10.10.10.254

Pokud změníte port, na kterém běží služba www, musíte tento port zadat do přihlašovacího dialogu winboxu jako ip_adresa:port



Další možnosti zabezpečení

Další možností, jak zabezpečit administraci směrovače, je použití některého mechanismu VPN, které RouterOS podporuje. Princip spočívá v tom, že vytvoříte zabezpečený tunel, kterým probíhá veškerá komunikace se směrovačem. V povolených IP adresách lze pak definovat pouze vnitřní adresy použité VPN tunelem.