

Konfiguracja tunelu SSH

Jeżeli chcemy zachować bezpieczny dostęp do serwera, który jest umieszczony za NAT lub Firewall to możemy wykorzystać do tego tunelowanie połączeń ssh. Aby ułatwić nawiązywanie połączenia można użyć dodatkowo pakietu autossh w połączeniu z wymianą kluczy ssh.

Do tego celu musimy dysponować oczywiście kontem shellowym na publicznie dostępnym serwerze (tutaj dev.bnet.pl). Serwer edokumenty musi z kolei przynajmniej mieć wyjście w świat na porcie 22.

```
apt-get install autossh
[jwhite@edokumenty ~]ssh-keygen -t rsa
[jwhite@edokumenty ~]cd .ssh/
[jwhite@edokumenty ~]scp id_rsa.pub tunnel@dev.bnet.pl:

# Teraz na zdalnym serwerze dopisujemy klucz publiczny
[jwhite@edokumenty ~]ssh tunnel@dev.bnet.pl
tunnel@dev:~$cat id_rsa.pub >> .ssh/authorized_keys2
exit

# Jeszcze raz się logujemy i voila nie potrzebujemy hasła!
[jwhite@edokumenty ~]$ssh tunnel@dev.bnet.pl

# Teraz na serwerze edokumenty wpisujemy polecenie tunelujące
[jwhite@edokumenty ~]$ssh -L 2219:localhost:22 tunnel@dev.bnet.pl

# Dzięki czemu będąc zalogowanym na serwerze dev.bnet.pl możemy
# połączyć się z serwerem edokumenty pod adresem localhost na porcie 2219
tunnel@dev:~$ssh localhost -p 2219
Password:
```

Od tej pory możemy poprzez hosta dev.bnet.pl łączyć się na lokalnym porcie ze zdalnym serwerem. Aby usługa działała niezależnie od rebootów można polecenie ssh zastąpić poleceniem autossh i zapisać do skryptu który dodamy do skryptów startowych rc.d.

W podobny sposób możemy zforwardować port 443 lub 80, dzięki czemu możemy uzyskać również dostęp do interfejsu webowego programu edokumenty.

Na przykład na serwerze edokumenty forwardujemy port 80 na zdalny serwer na port 5080:

```
[jwhite@edokumenty ~]$ssh -f -N -R 5080:localhost:80 tunnel@dev.bnet.pl

# na zdalnym serwerze forward na kolejny port:
tunnel@dev:~$ssh -f -N -L 6080:localhost:5080 tunnel@dev.bnet.pl

# i lokalnie forward umożliwi oglądanie strony edokumenty
[me@pldmachine ~]$ ssh -f -N -L 7080:localhost:6080 tunnel@dev.bnet.pl
```

Teraz wpisując do przeglądarki <http://localhost:6080> otrzymamy stronę z serwera edokumenty z portu 80.

Jeżeli używamy Windows, to ostatecznie polecenie możemy zastąpić odpowiednią konfiguracją PuTTY.