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 pakitu 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
ssh-keygen -t rsa
cd .ssh/
scp id_rsa.pub tunnel@dev.bnet.pl:
ssh tunnel@dev.bnet.pl

# Na zdalnym serwerze
cat id_rsa.pub >> .ssh/authorized_keys2
exit

# Jeszcze raz się logujemy i voila!
$ssh tunnel@dev.bnet.pl

# Teraz wiemy że tak samo zadziała
$autossh -L 2219:localhost:22 tunnel@dev.bnet.pl
```

Od tej pory możemy poprzez hosta dev.bnet.pl łączyć się na lokalnym porcie ze zdalnym serwerem. Aby usługa działała niezależnie od rebootów to można polecenie autossh zapisać do skryptu i dodać go 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.