Reverse SSH Tunneling

Contributed by kcharoen
Saturday, 20 September 2008

Have you ever wanted to ssh to your Linux box that sits behind NAT? Now you can with reverse SSH tunneling. This document will show you step by step how to set up reverse SSH tunneling. The reverse SSH tunneling should work fine with Unix like systems.

Let's assume that Destination's IP is 192.168.20.55 (Linux box that you want to access).

You want to access from Linux client with IP 138.47.99.99.

Destination (192.168.20.55) <- |NAT| <- Source (138.47.99.99)

1. SSH from the destination to the source (with public ip) using command below:

ssh -R 19999:localhost:22 sourceuser@138.47.99.99

* port 19999 can be any unused port.

2. Now you can SSH from source to destination through SSH tuneling:

ssh localhost -p 19999

3. 3rd party servers can also access 192.168.20.55 through Destination (138.47.99.99).

Destination (192.168.20.55) <- |NAT| <- Source (138.47.99.99) <- Bob's server

3.1 From Bob's server:

ssh sourceuser@138.47.99.99

3.2 After the sucessful login to Source:

ssh localhost -p 19999

* the connection between destination and source must be alive at all time.

Tip: you may run a command (e.g. watch, top) on Destination to keep the connection active.

{mosgoogle}