

Forum: [Hack Forums](#)

Thread: [\(Tutorial\) make your own SSH proxy on Windows \(SSH Tunneling\)](#)

?Ñåg?I - May 3, 2016, 7:42 pm

Having your own SSH proxy at home is a great way to keep your connection encrypted if your are on a network you don't trust
this is basically a simplified VPN server for your own network

you need two computers (server must be microsoft windows for this guide) I was going to do linux but there are already plenty of tutorials out there for linux
port forwarding will be required as this is not a reverse proxy
and some software that you will need to install (so you might need admin rights on your PC)

software required for home computer (or server): Bitvise SSH Server

<https://www.bitvise.com/download-area>

software required for work computer (client)

either Putty (portable software) <http://www.chiark.greenend.org.uk/~sgtatham/putty/>

or the bitvise client (requires install) <https://www.bitvise.com/download-area>

for linux there are probably other alternatives so google it if you want something better

Bitvise SSH Home Server Tutorial

[\(Click to View\)](#)

so start by installing bitvise SSH server

once you have the control panel running open up easy settings

this will get your server set up as fast as possible you can always modify the more advanced settings later

use the settings that I have

you can chose any listening port you want I would recommend you don't use a popular port (don't use 22) as it makes you more vulnerable to script kiddies and their l33t bruteforcing tools
make sure that your listening port is forwarded on your router check here to see

<http://www.canyouseeme.org/>

dont make a windows account make a virtual account it will add more security

make sure your virtual account name is a private name like your own don't use popular keywords such as root or admin as it will make it easier for script kiddies to bruteforce it

for the virtual account password use a password which is at least 25 characters long and use a password generator to make the password.

dont allow file transfer or terminal only port forwarding, (file transfer and terminal are not require for

SSH tunnels

second step is to generate a host key
try generating both RSA and DSA keys
make sure the size is at least 2048 bits (but the stronger the better)
the reason why you need multiple keys is to increase compatibility with clients some use DSA while others use RSA

If you have a dynamic IP address you should get a DNS address (but it's up to you)
www.no-ip.com or <https://freedns.afraid.org/>

after configuring the tutorial above you can start on step 2 configuring your work computer
you can use whatever you want I made a guide for the putty client, and the bitvise client
you should use putty if you don't have admin rights

if you are using Putty follow this tutorial

[\(Click to View\)](#)

open up putty and head to: Connection--->SSH--->Auth----> Tunnels

use the settings I put but you can change the port if you wish, NO it does not need to be forwarded

then head to Category-->Session in putty

put in the IP address or DNS address of your Bitvise Server IP

use the port that your bitvise server is using

then just open your session and a login terminal should show up fill in your name and password

once logged in you need to configure firefox to connect to the SSH tunnel

open firefox options head to Advanced--->Network---> settings

use the same settings that I'm using (the port number must be the same port used for Tunnels in putty)

If you disabled terminal in your Bitvise server settings then go in PuTTY client, enable Connection > SSH > Don't start a shell or command at all.

your connection should now be encrypted use wireshark on your work computer to check if the connection is encrypted

If you are using Bitvise client follow this tutorial (in development)

[\(Click to View\)](#) on Bitvise client go to service and enable socks use listen interface of 127.0.0.1 and a port of your choice the port will be used for the tunnel
on options disable terminal remote desktop and SFTP

then on login fill out details (you will notice that authentication has additional features such as public key for more security)

Security settings for Bitwise Server

[\(Click to View\)](#)

In order to avoid frustration, do not start locking down your SSH server settings prematurely. Make sure that you can establish a connection first. Make sure that you have tested Putty or Bitwise client to see if it works

here are a list of ways to secure your SSH server even further I will explain each with pictures later make public key authentication a requirement to log in (this will stop bruteforce attacks as the hacker will need the public key)

make a username blacklist (if the hacker enters the wrong username while bruteforcing then his IP address is banned)

use a port other then port 22 (a lot of computers from around the world scan random IP addresses for port 22 by using a different port it makes it harder to know that you are using a SSH server)

do not allow file transfer and do not allow terminal (you don't need it for SSH tunneling and hackers will now have less to use if they do compromise the server)

ok now let's configure our server for more security

this is the way that I set up my security you can change your's to whatever you think is suitable

and here is the username blacklist

what the username blacklist does is it blacklists your IP address if you login with a certain username I added root and admin to the list

add some more names like Code test, guest, postgres, mysql, user

Q&A

[\(Click to View\)](#)

your client disconnects unless you also allow terminal shell access. on server

Most clients can be configured to not require a terminal shell when using port forwarding:

If using OpenSSH, use the -T parameter ("Disable pseudo-tty allocation").

If using plink (part of PuTTY), use the -N parameter ("don't start a shell/command").

If using the graphical PuTTY client, enable Connection > SSH > Don't start a shell or command at all.

If using Bitwise SSH Client, the session won't be disconnected if a terminal window can't be opened, in the first place. However, if terminal shell and/or SFTP access are not available, you may want to disable the automatic opening of a terminal shell and/or SFTP window. This is configured under Options > On Login.

total0wnage - *May 3, 2016, 7:48 pm*

thanks for the info might try it and set it up for my friend

Mariano Gregorio - *September 6, 2019, 10:17 am*

Anyone here who can help me on CONFIGURE SSH TUNNEL/RROT TO ANY MASS-SENDER or ANY OFFICE365 INBOX?

Please DM on skype @ jane.jane118