



Setting Up VPN Client on Max Cole High Performance Firewall



Introduction

Thank you for purchasing the Max Cole High Performance Firewall. You are moments away from enjoying seamless communication across your network.

In addition to being a powerful, flexible firewalling and routing platform, it includes a long list of related features and a package system allowing further expandability without adding bloat and potential security vulnerabilities to the base distribution. The Max Cole High Performance Firewall can be used in various environments ranging from ranging from small home networks protecting a PC and an Xbox to large corporations, universities and other organizations protecting thousands of network devices.

1. Setting Up An OpenVPN Client On Windows Vista/XP

This is a guide on how to connect a PC on the internet, to LAN behind a pfSense firewall using OpenVPN. This is also known as a Road-Warrior setup. Windows Vista requires administrative priviledges to run and properly configure OpenVPN.

1. Download and install the most recent software from [OpenVPN Downloads](#). If you plan to connect from a PC with Windows Vista or 7 you should get version 2.1 or newer. Windows XP works well with 2.1 as well. Use the default options when installing.
2. Start a command prompt with administrator-rights!
 1. This is done in Vista by clicking on START and then type CMD -> CMD.EXE should appear, and you RIGHT-Click on it and select 'Run as Administrator'.
 2. If your account has administrative-rights, XP's command prompt automatically runs with them.
3. Change directory to c:\programfiles\openvpn\easy-rsa
4. Run the "init-config.bat" file
5. Edit 'vars.bat' file. 'Worpad' is suggested but Notepad will be fine. For Vista, you need to start Wordpad/Notepad with administrative-rights. (Click on START and then type CMD -> CMD.EXE should appear, and you RIGHT-Click on it and select 'Run as Administrator'.) The following things need to be edited:

```
"set KEY_COUNTRY=US"  
Your 2 Letter country ID Goes Here  
  
"set KEY_PROVINCE=NA"  
2 Letters Province ID - Or use NA as in 'Not Applicable'  
  
"set KEY_CITY=Copenhagen"  
Name of Your City  
  
"set KEY_ORG=pfSense"  
Name of your company  
  
"set KEY_EMAIL=youremail@address.com"  
Put a email-address here. Dont use your private address. since this is the common  
address for the Certificate Authority
```

Save the file
6. Run "vars.bat"
7. Run "clean-all.bat"
8. Run "build-ca.bat". Then you are prompted for some different things; Leave them at default, except

"Common Name" - put something like "pfSense-CA"

9. Run "build-key-server.bat server". Again you are prompted; leave them on default except "Common Name" - use "server"

10. Run build-dh.bat

Now its time to generate keys and certificates for the client(s)

11. Run "build-key.bat ovpn_client1". Again you are prompted; leave them on default except "Common Name" - here you should put in "ovpn_client1" (or whatever you have called it). The ovpn_client1 will be the name of the keys, certificate and the name you identify the connection on later. You can use whatever name you like, and generate as many as you want (with different names).

12. The following files should now be copied from c:\programfiles\openvpn\easy-rsa\keys to c:\programfiles\openvpn\config

1. ca.crt
2. ovpn_client1.key
3. ovpn_client1.crt (if you don't see a .crt file but only a .csr file, chances are that you don't have admin privileges. Worst case generate the keys and certificates on a NON-Vista machine)

13. Make a file in the "C:\programfiles\openvpn\config" called "ovpn_client1.ovpn" and the file should contain (leave out the hashes):

```
client
dev tun
proto udp
remote XXX.XXX.XXX.XXX 1194
ping 10
resolv-retry infinite
nobind
persist-key
persist-tun
ca ca.crt
cert ovpn_client1.crt
key ovpn_client1.key
ns-cert-type server
comp-lzo
pull
verb 3
```

Replace the XXX's in the "remote" line with the public IP address of your pfSense-box. If you don't know what that is, check it [here](#). If you have chosen another name than 'ovpn_client1' then change it in the lines beginning with 'cert' and 'key' If you have more than one VPN client, you make one .ovpn-file per client (with the corresponding .key and .crt name)

Now its time to configure pfSense

14. Log into the web-gui of pfSense

15. Select VPN/OpenVPN and add an entry in the 'server' page. Use the following settings:

Protocol: UDP

Local port: 1194

Address pool: 192.168.200.0/24 (It should be an address range that you ''DONT'' currently use.)

Local Network: 192.168.1.0/24 (Whatever the network is that you want the VPN client to connect to)

Remote Network: blank

Cryptography: BF-CBC (128 bit) - or use what you want

Authentication Method: PKI

16. Now you need to have access to some of the files created in c:\programfiles\openvpn\easy-rsa\keys (mentioned in 12.)

1. Copy the WHOLE content of ca.crt into the "CA certificate" window
2. Copy the WHOLE content of server.crt into the "Server Certificate" window
3. Copy the WHOLE content of server.key into the "Server Key" window
4. Copy the WHOLE content of dh1024.pem into the "DH parameters" window

17. Tick DHCP-Opt: Disable NetBIOS (I dont use it anyway)

18. Tick LZO Compression

Now we need a few simple rules in the firewall

19. On the WAN interface you should make a rule that;

PASS

WAN

Protocol: UDP

source: any

OS type: any

Destination: any

Destination port range from: OpenVPN

Destination port range to: OpenVPN

Tick in the LOG

Leave the rest at default.

Remember to apply the new rules.

20. Add another rule on the LAN interface (or whatever the name of the net defined in 15. 'address pool' is);

PASS

Any protocol

Source: LAN (or whatever the name of the net defined in 15. 'address pool' is)

Any destination

Remember to apply the new rules.

Now you should be able to connect from OpenVPN (right click on the icon in the tray and select Connect). But remember to start OpenVPN with ADMIN RIGHTS!

6. Conclusion

We have come to the end of this manual. The Max Cole team wishes you have an amazing experience with the Max Cole High Performance Firewall and an enjoyable journey with IP Communication. Should you face any difficulties that this manual could not assist you with, you may contact Max Cole Technology Solutions Pte Ltd for additional technical support.

7. Contact Us

Our contact details:

Max Cole Technology Solutions Pte Ltd

3 Raffles Place #07-01

Singapore 048617

Phone : +65 6464 0419 (Press 3 for Technical Support)