Working in the Cloud

with ClearMedia Academy

Deploying SSL VPN on a WatchGuard FW

**Disclaimer**:

By using the ClearMedia WatchGuard guide, you can greatly reduce the amount of time needed to deploy your setup. These guides have been configured with the best practices in mind, to assure optimal stability and performance. Although use of the guide is not compulsory, it is recommended!

On this first page you can find a small overview of the required steps. It is intended for engineers that already have experience with the WatchGuard configuration and previous ClearMedia WatchGuard deployment guides. The larger, more in-depth explanation with screenshots, can be found further on. It can be used by people without any prior knowledge if the overview is not clear or if it has been a while since your last deployment.

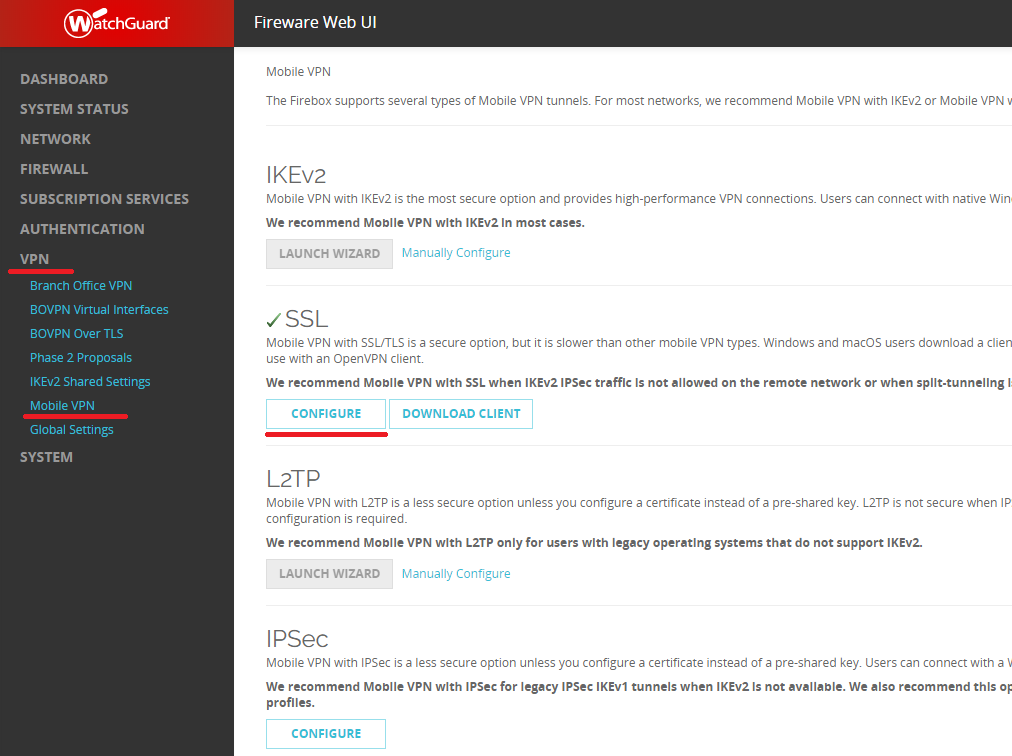
Quick steps

This guide assumes you have a working WatchGuard FireboxV appliance in place, with minimum version Fireware v12. If you do not have that yet, please use the “How-To 3 WatchGuard FireboxV” deployment guide. We will be using the WebUI interface in this guide, to show how to configure mobile SSL VPN.

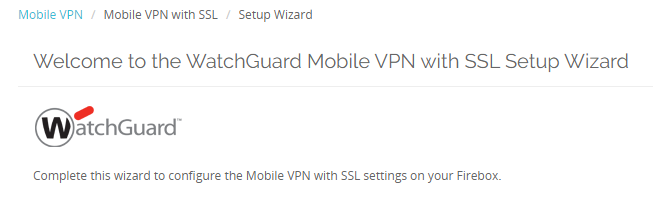
* Do not use the steps below if you do not know how to start. Go to the In-Depth steps instead.
* Note down your public WAN IP or DNS name. You will need it later on.
* Navigate on your WatchGuard device to: **VPN** 🡪 **Mobile VPN 🡪 SSL 🡪 Configure**
* Use the SSL Configuration Wizard to setup the SSL VPN server.
* You can also use an alternate port. For example 8443.
* Finished!

In-Depth explanation and step-by-step procedures

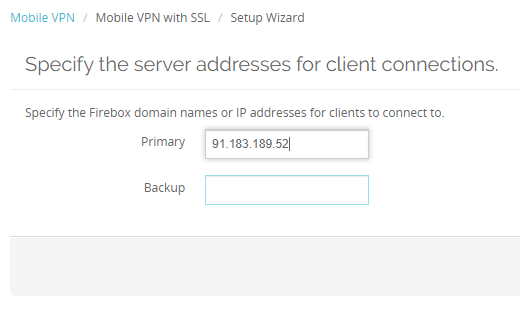
* Note down your public WAN IP or DNS name. You will need it later on.
* Login to the WatchGuard WebUI interface with the admin user, either from remote (if that is allowed by the firewall rules), using the public IP, or, from inside.
* Using the format https://<WG\_IP>:8080
* Navigate to **VPN** 🡪 **Mobile VPN 🡪 SSL 🡪 Configure**



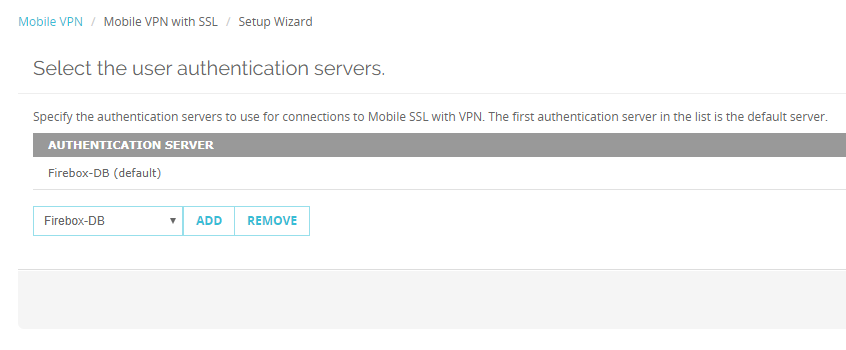
* The first time you configure SSL VPN, the WatchGuard appliance will suggest using the setup guide. Please choose to do so.
* Follow the steps in the screenshots below:



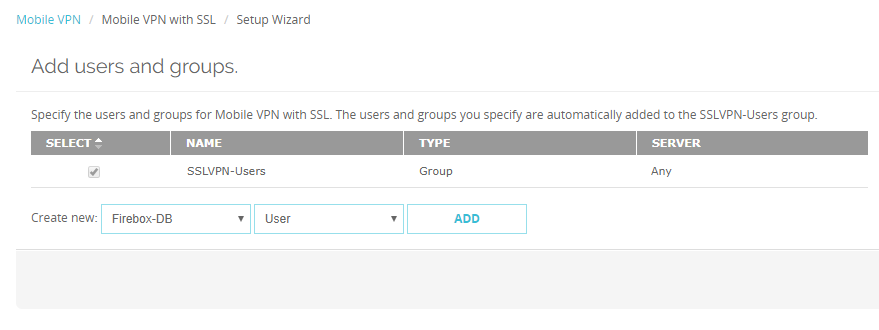
* On the General tab make sure you configure the Public IP or DNS name in the “Primary” Field. Do not use the local or NAT IP! This will not work. Here you configure the IP or DNS the client is actually is going to use to connect to. In this example: 91.183.189.52.



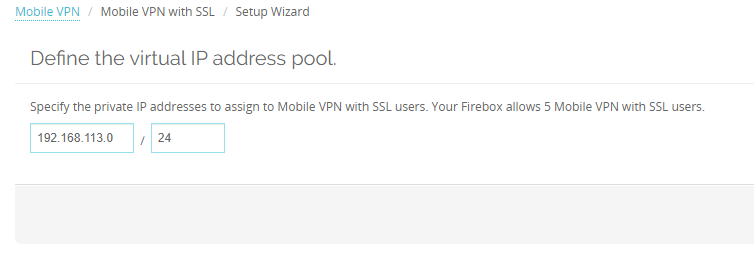
* On the Authentication step, keep the default settings.



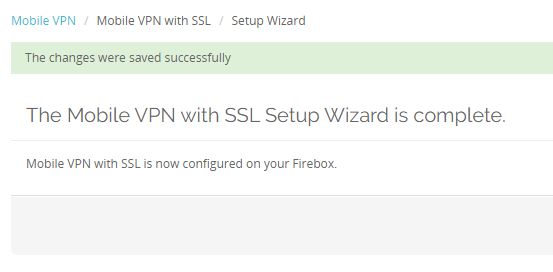
* Next, the Authentication tab. Here you configure how the customer logs on with the SSL VPN.
* Keep the default settings on “Firebox-DB”. This will use the build-in users database on the WG.
* However, if you would like to use Active Directory accounts, please use the next guide “How-To 9 AD integration on Watchguard” deployment guide.



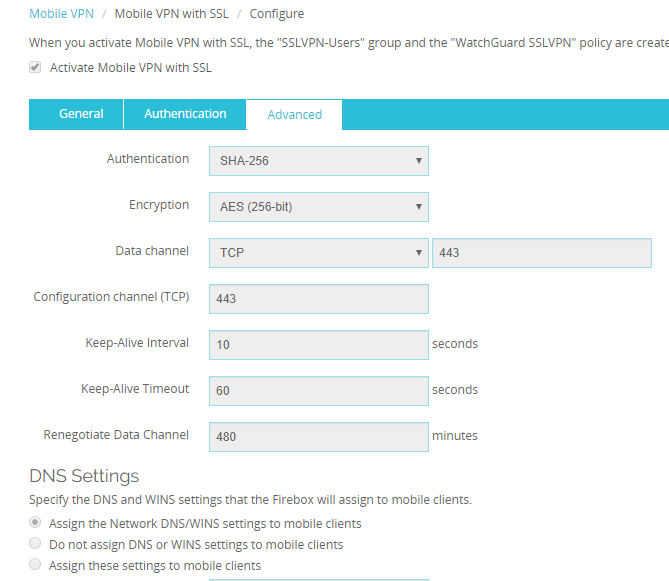
* Do not change the “virtual IP address pool”. Or at the very least, make sure it is not the same as the Cloud LAN subnet or any On-Premise LAN subnet. Otherwise users will not be able to connect.



* The setup wizard is now finished.



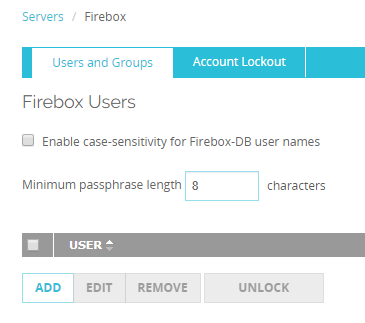
* Now open up the config, via the “Configure” button.
* On the last tab, “Advanced”, you can configure the encryption settings, used port and DNS.
* If you are already using the https 443 port on you vApp, you cannot use the default SSL VPN 443 port for Mobile SSL VPN on the WatchGuard. In this case, you must use an alternative port. We strongly recommend using **port 8443**. This incoming port is also opened up on the ClearMedia backbone firewall. If you want to **use a different port** then (8)443, you must **contact ClearMedia** support to open up that port.
* If the normal HTTPS port 443 is free, you can keep the default port.
* Keep all other settings to their default value.



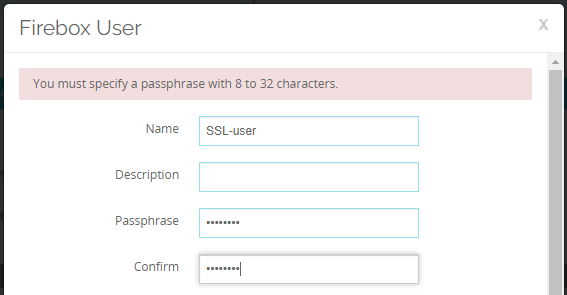
* Do not forget to click on the **Save** button at the bottom of the page. Finished!

**Creating SSL VPN Users on the Firebox User Database**

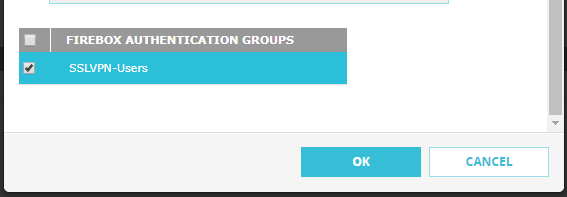
* Now you must create SSLVPN users to be able to use the SSL VPN.
* Go to Authentication 🡪 Servers 🡪 FireboxDB.
* Under “Firebox Users” click on ADD



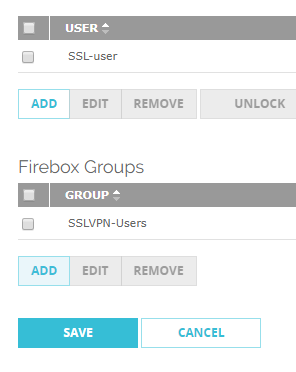
* Create a user. Type the password 2 times.



* Add this user to the “SSLVPN-Users” group.

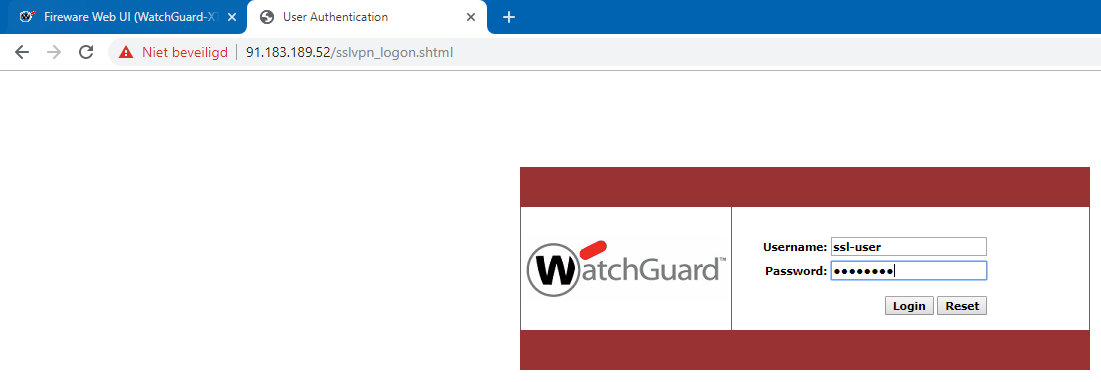


* Click on “OK”. You should now see the user in the “Users and groups” screen.
* Press “SAVE” at the bottom!
* Finished.

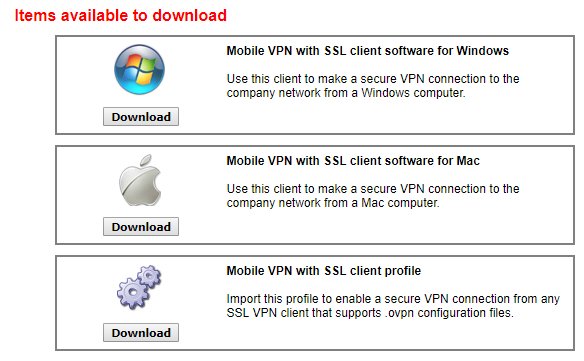


**Downloading and installing the SSL VPN Client (For OpenVPN clients on Mac, Linux, Android, iPhone)**

* Open up a browser.
* Navigate to the WatchGuard using a special url: **https://<WG\_IP>/sslvpn\_logon.shtml**



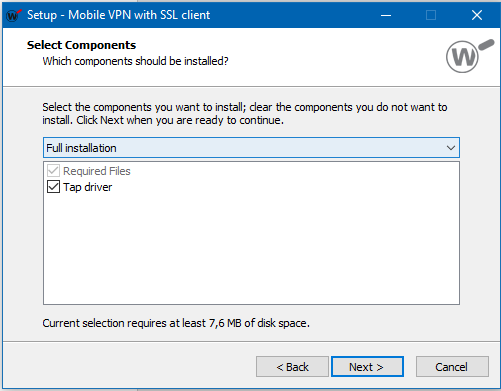
* This will open up the WatchGuard authentication portal. Users can login with the credentials you provided, to download the Windows or Mac SSL VPN software.
* Download and install the WatchGuard SSL VPN software. Downloading the version from the WatchGuard appliance directly will ensure you are using a compatible version with the WatchGuard firewall.



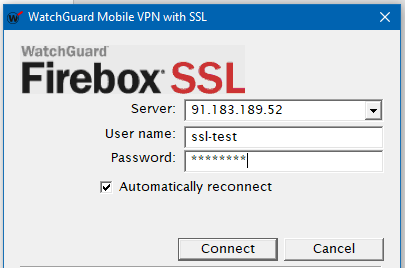
* Install the client on all users intending to use the SSL VPN.



* Allow the install of the TAP Driver on Windows PC’s.



* Now start the “WatchGuard Mobile VPN with SSL” software.
* You will see a box for the server, a User Name and a password.
* Provide the Public IP or DNS name of the WatchGuard firewall. Do not use http or https in the server field. In our example: 91.183.189.2 or firewall.inthecloud.net
* Also note, that if you changed the port in the SSL VPN config, you must provide the alternate port. In our example: 91.183.189.2:8443
* Again, use the provided credentials, to log on.



* The software should now connect to the WatchGuard firewall and a connection should have been established.
* You will see a green Watchguard SSL VPN logo in the system tray, indicating you are connected.



**You’re new WatchGuard SSL VPN setup is now ready!**