# **Installing/Connecting to the Sonicwall NetExtender VPN**

This document provides a quick overview of what a Virtual Private Network (VPN) is, what you should know about VPNs, how to initially install the VPN software, and how to begin using the VPN.

**What is a VPN and What is it used for?**
A VPN is software used to create a secure/encrypted connection from your PC to the corporate office. This essentially bridges your PC from wherever it is physically located, to being as if it were in the office. When connected to the VPN, you can browse/access files that are located on the servers that you would normally be able to access if you were in the office.

A VPN is very helpful to allow for employees to continue to access files or applications while working remote, however, there are a few caveats that must be acknowledged when using a VPN:

1. VPN might not connect everywhere you can get internet. Depending on the VPN setup, your internet provider you are accessing the VPN from may not allow for you to connect. When possible, we like to configure VPN’s so that the traffic looks like normal web-browsing traffic to the internet provider, however, there are instances when we can not make this configuration, in which case, you may be at the mercy of the Internet provider if they decide to block that type of traffic. This is common on public wireless (such as hotels, coffee shops, airports, etc.), as well as on some home internet connections.

Ways to work around this would be, if it is your home internet, contacting your Internet provider and ensuring they are not blocking any ports on your modem/router if they manage that equipment, or whomever configured your network. If you do not control the network (eg. Public wireless), your option is to use your phone as a wireless hotspot if possible, however, keep in mind that a VPN may use a lot of data depending on the workload you have, so be aware if you use this method of any cost you may be incurring with your phone provider.
2. Performance will not be the same as if you were in the office. Unfortunately, because your traffic is now going over this secure connection, performance is not going to be nearly as good as when you are in office. This can be limited by the internet connection at your home, to the internet connection at the office, to the delay between your computer and the office (known as latency).

Normally, when in office, the connection between your computer and the server is instantaneous and fast (1000x1000mbps bandwidth with <1ms of latency). See below for a common scenario with a VPN:

|  |  |  |
| --- | --- | --- |
| **Home Internet:**200mbps Download**15**mbps Upload**50ms** Latency | **Office Internet:****30**mbps Upload30mbps Download30ms Latency | **Effective Connection over VPN to your Computer:****30**mbps Download**15**mbps Upload>~**50ms** Latency |

As you can see, since we must take the weakest link of both the connections, you end up with an effective 30x15mbps with somewhere over 50ms of latency. This would result in about 33 times slower file downloads from the server compared to when you are in office, however, luckily, if you are dealing with small files such as normal Word/Excel documents, this should be fairly usable (only adding a few seconds of time to open).

Applications that talk to a database, however, will be much slower, since the latency is 50 times slower **PER REQUEST**. For example, this means that if you had an application that isn’t optimized for use over a VPN referencing a database at the office that needs to pull the information for a client with 50 fields (name, street name, city name, state, etc), you take the latency, multiply it by 4 (since it needs to make the travel back and forth once to initiate the transfer, then once more to actually transfer the data), then multiply that by the amount of fields. This means that 50 field request quickly goes from being instantaneous on-site, to a request that would take 10 seconds over a VPN. If you had to run a larger report (think one that normally takes 15-30 seconds on-site, you can imagine that this would be exponentially slower. If it is found that the delay is too much to run these applications reasonably, we can evaluate other options that we can use that, although it would be different than what you may be used to, would perform better than a VPN. The primary benefit of a VPN is that once you are connected, you don’t have to change much of how you work (if your workflow can accept the slower performance).

1. A VPN does not mean that you can safely browse online without fear of getting viruses or compromised. This is a common misconception about VPNs due to a bit of misleading marketing.

Depending on the way the VPN is configured, the most you can expect is that you can browse to a website without them knowing where you are coming from, and potentially stave off **SOME** less common attacks used on public networks. If you were connected to a VPN and opened an email link from a malicious sender (most common form of compromise), or clicked a malicious pop-up when browsing a website, you are just as vulnerable as if you were not connected to the VPN. Please continue to be mindful of any suspicious emails/websites that you might come across and as always, report any to Keystone if you want for us to confirm a valid email or website.

## **Installing the VPN Software**

The first time that you connect to the NetExtender VPN, you must install the client. On subsequent connections, this is not necessary. If you already have the NetExtender client installed, please skip this section and follow the instructions in the following section titled “Connecting to the VPN”

Before you begin, you will need the following items from Keystone, if you are missing any, please contact us for assistance:

* VPN Website:
* Server Name:
* Domain Name:
1. Go to the VPN Website provided by Keystone. If prompted, you may have to click proceed to get to the portal login:

|  |  |
| --- | --- |
| **Internet Explorer:** | **Chrome:** |
|  |  |

1. Log into the portal with your domain username and password (this should be the same as your login to your PC) :

2. Once signed in, click the link to download the Windows NetExtender Client.

3. Run the file that was downloaded (NXSetupU.exe).

4. Click Next to the first prompt

5. Ensure “I Agree” is selected and click Next:

6. Click Next:

7. Type the server name and domain name provided to you by Keystone into the appropriate fields. Keep in mind, the “Default Domain” field is cAsE sEnSiTiVe, so enter it as it was provided by the technician. Click Next:

8. Click Next, then Finish once the Install is completed:


## **Connecting to the VPN**

1. To open the VPN Client, click the NetExtender Icon that should be on your desktop or in your start menu:

2. Fill out your domain username/password (same as what you use to log into your PC) and click Connect to connect to the VPN

3. If prompted, click Always Trust to the security alert:

4. You are now connected to the VPN. When you are finished with working on the VPN, please click “Disconnect” from the popup. This both terminates your connection and frees up a license for one of your co-workers to connect to the VPN. Please remember to disconnect when finished, as if you shut down before disconnecting, the license will not be released until the session times out (normally 8-24 hours)
