6950 SW Hampton St., Ste 308
Tigard, OR 97223

VPN Access Guide

VPN Access Overview

This guide is an introduction to VPN access and the various different applications that can be used on top of a VPN access for Remote Access and Secure data transfers.

An Introduction to TightVNC

Using a service like TightVNC allows for users to remotely access a computer's for anywhere around the world. Using this in combination with a remote access VPN service makes this process easy and secure for users, their companies, and the people managing their services. This means being able to access files, printers, or any other device located on a machine from anywhere in the world.
The first step in this process is to remotely connect to the desired network via remote VPN access. This can be done by following the "Remote Access Instruction" presentations from Uplevel Systems located in Dropbox and Sharefile. Once a secure connection has been established remotely accessing a device can be done using a remote access service like TightVNC. This software must be downloaded on both the systems accessing as well as being accessed. The downloadable software can be found at http://www.tightvnc.com/download.php. Once the software is fully installed onto both systems and a VPN connection has been established the only remaining item is to identify the IP address of the machine you are wishing to access on the local network. This can be found on the Uplevel Systems interface under "Devices". Using Remote Access VPN to control a device is much safer than the standard RDP protocol and allows for control from anywhere. Once an IP address has been identified it can be input into the TightVNC Viewer and connected to. Ensure that when you VPN into the desired network that the computer you are also attempting to remote access is on the same network. i.e. If the computer is connected to Wifi that the Wifi service is a part of the security group where the VPN access is terminated. The purpose of the security groups is to keep groups and groups of people separate so VPNing into the Employee Group will not grant you access to a computer on the Boss Group. It will however allow you access to the All Employees group.

Windows RDP

Windows RDP operates in a very similar fashion to that of Tight VNC. Older versions of Windows will come fully equipped with Windows RDP however the new versions require a professional license to unlock the functionality. Once the software is installed and a VPN connection is established a simple IP address on the network will allow for users to remotely control the device and access all of its capabilities as well as resources. Similar to TightVNC discovery protocols will not work under certain conditions so in order to find other devices or establish connectivity the server name and device name must be known or an local IP address.

RealVNC

RealVNC can be downloaded onto all major operating system platforms from https://www.realvnc.com/en/download/viewer/. This allows you to remotely control a device of any operating system kind from an operating system of any kind. This is done by downloading the viewer onto both the controlling as well as controlled device after which a secure VPN connection must be made to access the enterprise network from there the desired server address should be entered in the top command line. This will allow access into the desired computer provided that the requesting computer also has RealVNC downloaded and available.

TeamViewer

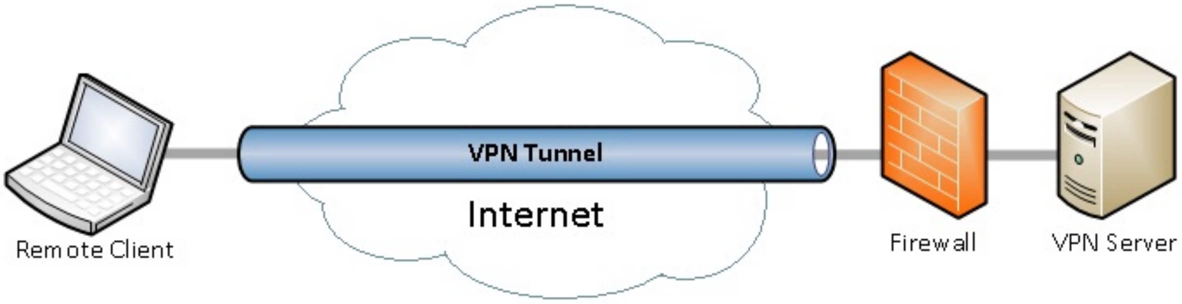
TeamViewer similarly allows you to remote access a device however unlike TightVNC as well as Windows RDP, TeamViewer is compatible with Mac's. Team Viewer can be found at https://www.teamviewer.com/en/?pid=google.tv_teamviewer_exact.s.us&gclid=CODx2-yB2NQCFQIOaQodCqICJw. This allows for Mac's to be remotely accessed and controlled from anywhere. Once the software is downloaded onto both systems in question the local IP address of the desired device can be input into the dialog box and the connection will be made. This will allow remote access to the device from anywhere providing full access to the resources on the system and its drives. Teamviewer is however a costly product and allows for some cross over in capabilities that are already including the Unbox.

Connecting to a Printer

However, like when you are physically located in the office, locating devices requires either the path or IP address since autodetection protocols will not be able to locate devices across separate subnets. These devices can be found by going to the device and printer information located within the control panel. By clicking the "Add Device" or "Add Printer" button the computer will automatically attempt to locate the device. Connecting from a different security group than where the device is located will prohibit this automatic detection including attempting to access the printer via VPN. In which case, a button will appear saying "Don't see your device?" Clicking this will allow you to input a local IP address and connect to the device over different security groups, granted that you have access across these various groups. This process also must be used to find devices and printers when VPNing into the network and attempting to print or identify an additional device than the one you are VPNed into. Once this process is complete the functionality of one device to the other is identical to being physically located on the network.

Possible WiFi Issues

Connecting to the VPN ensures an encrypted tunnel from your personal computer outside of the network to the company's server. This, however, means that the WiFi on the originated computer will no longer be active. From there all internet connections should be made from the terminated or tunneled computer. This will ensure that all internet traffic is passing through the Firewall of the company rather than being exposed to the internet on the device outside of the network that the user might be physically located at. This also allows for you to remotely access the computers on that local network and print remotely any files just like you are in the office. It also allows for a secure connection be established with the protection of the firewall at the office.



Because the VPN tunnel is a secured connection the internet connection on the remote client computer is terminated to force all internet traffic to go through the VPN tunnel.

Discovering a Device

Establishing a VPN connection automatically puts the network into “Public” mode. This means that the connection will not be identifiable for the purpose of finding or sharing files. In order to make it “Private” you must go to VPN connection under settings while the VPN connection is on and click Advance options. This will allow you to turn “Make this PC discoverable” On.

Connecting a Drive

Once a VPN connection is established, like when crossing different subnetworks, a drive can then be mapped to the local device. In order to do this the device must be VPNed to the network and discoverable. You can then go to the folder, press “This PC” and selecting “Map a Device”.

This will then prompt you to locate the device using the network server and device requesting. In many cases the “Browse” function will not work because the connection is across subnets. Once the server and device have been located you will be able to choose a letter to assign to the drive and add the folders accordingly. This will allow you to use the drives and folders located on the drive when on the VPN as well as internally located within the office but across security groups.