USING A WIRELESS NETWORK WITH VPN

All wireless connections to any network or the internet use radio waves to send and receive instead of wires. Just like any other radio waves, these wireless signals are susceptible to interference and other problems that impact radios. Think about what happens when talking on walkie-talkies or CB radios or AM/FM radio. Only one person can talk at a time – when more than one person talks at the same time the conversation is difficult to understand. If you travel into a tunnel or go next to some electrical machinery the interference may cause you to lose the connection. The same is true with wireless network connections. Household items like microwave ovens and fluorescent lights can interfere with the signal. Even the strongest radio signal can experience interference.

This impacts the VPN connection. Using the VPN technology, both clientless and AnyConnect client, the PC is attempting to establish and maintain a secure private tunnel connection across the radio waves to the wireless receiver and then from there through any number of devices to the state network VPN gateway and back. The security is accomplished using encryption. The PC and the VPN device start “talking” with each other and agree on a secret mathematical code that only they have the passwords for. In addition to the regular network traffic users send over the VPN tunnel, the PC and VPN device add the secret codes and data to tell each other this is the correct traffic and how to decrypt it into something meaningful for the user.

All this encryption and tunnel traffic is time-sensitive. If the wireless connection experiences interference or anything else that blocks or scrambles the signal for even a short duration, it is possible the security of the tunnel could fail, resulting in the VPN tunnel connection being dropped. Users may or may not receive an error message and will always receive a notification they are disconnected and need to log back in. Even if the user never experiences any drops in wireless connectivity when not using the VPN, they still may experience drops using the VPN due to the security overhead and requirements of the VPN tunnel.

This is not a VPN error. This is an issue with the wireless connection at whatever location the VPN user is connected to. The best way to resolve it is to use an Ethernet cable and make a “wired” connection to the user’s home network or whatever network the user is connected to. If a wireless connection is all that is available, users can mitigate the impact by taking steps to reduce the potential of radio signal interference from devices such as wireless mobile home phones, fluorescent lights, microwaves, 2-way radios, thick walls etc.