# Trey Research Corporation

Virtual Private Networks: A Technical Overview for Fabrikam, Inc.

December 15, 2023

Virtual Private Networks (VPNs) are a popular network security solution that can encrypt network traffic. VPNs act as a secure tunnel, encrypting internet traffic, making it difficult for third parties to track activities and steal data

Benefits of Implementing VPNs:

* VPNs provide an additional layer of privacy and security by encrypting internet traffic. This makes it difficult for third parties to track activities and steal data.
* VPNs can prevent you from being hacked when using public Wi-Fi at airports or libraries. This is because VPNs function like a secure tunnel, encrypting internet traffic.
* VPNs can prevent your internet service provider from knowing which websites you have visited, as all traffic to and from your computer runs through the VPN servers or servers that the VPNs pay to use.
* VPNs can bypass geographical content restrictions by masking your IP address and encrypting your internet connection. When you connect to a VPN server, your internet traffic is routed through the VPN server, which assigns you a new IP address. This makes it appear as if you are accessing the internet from a different location, allowing you to bypass geographical content restrictions.
* Disadvantages of Implementing VPNs:
* Connection speeds can be slower than your ISP. This is because VPNs add an extra layer of encryption and routing to your internet traffic.
* The use of VPNs is banned in some authoritarian countries. In some countries, VPNs are banned or heavily regulated.
* Using free VPNs carries the risk of ads, malware, and data leaks. Free VPNs may sell user data to third-party advertisers or insert ads into web pages.

## Installation Specifics:

A VPN sets up an encrypted tunnel between the system running the VPN client and a VPN server, which then acts as a proxy, routing traffic through the tunnel to the rest of the corporate network. The steps include:

* A VPN client is installed on the user's device, encrypting all traffic between the device and the VPN server.
* The VPN server decrypts the traffic and forwards it to the desired destination.
* The destination server responds to the request by sending the traffic back to the VPN server.
* The VPN server encrypts the traffic and sends it back to the VPN client.
* The VPN client decrypts the traffic and sends it to the user's device.

To install and configure a VPN server, follow these steps:

* Create a VPN profile on your computer.
* Click "Start" and then "Settings" to open the settings menu.
* In the settings menu, click "Network & Internet" and then "VPN."
* Select "Add a VPN connection."
* Complete the tasks in the "Add a VPN connection" window.
* Save the changes you have made.

## Risks and Mitigation:

Attackers have been aware of remote work as a threat vector for some time. The remote work environment is particularly attractive to attackers for several reasons. First, the home network environment is not professionally managed. Most critically, this means that many more systems in home networks are not regularly patched, and a number of them are outdated in terms of risk mitigation. To persist in a corporate network, an attacker who has exploited a system must be resistant to detection and remediation. Here, too, the home network is more comfortable for the attacker; threat detection is typically minimal, and remediation measures are taken more casually, such as when a PC is reinstalled or taken out of service because it is running too slowly. To secure the remote work environment, it is important to extend Zero Trust assumptions. Not only should the network be considered hostile, but everything not under the company's control should be considered hostile.

Update VPNs, network infrastructure devices, and devices used for remote access to work environments with the latest software patches and security configurations.

## Best Practices for Implementation:

Best practices for implementing VPNs in a corporate network include:

* Choose a standards-based VPN that uses recognized standards, such as Internet Key Exchange/Internet Protocol Security (IKE/IPSec), which are generally less risky and more secure than Secure Sockets Layer/Transport Layer Security (SSL/TLS) VPNs that use custom code to send traffic over TLS.
* Use a VPN with strong cryptography. Verify that the encryption algorithms, authentication algorithms, and protocols used by a VPN are strong and FIP-validated. Configure all VPNs to use multi-factor authentication (MFA) and replace password-based authentication with client-based authentication using digital certificates (stored on smart cards) whenever possible.
* Manage software risks. Exploiting VPN security risks is a common attack vector for cybercriminals. Choose a VPN provider with a good track record of patching security vulnerabilities and request a Software Bill of Materials (SBOM) to verify that third-party code is up-to-date and secure. Also, look for a product that can inspect its code during execution to detect potential attacks. After deploying a VPN, regularly check for software updates and apply them promptly.
* Prepare for increased usage. IT security personnel should test VPN limitations in preparation for mass usage.
* Avoid free VPNs. Using free VPNs carries the risk of ads, malware, and leaks.