# 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 help encrypt network traffic. [VPNs act as a secure tunnel and encrypt internet traffic, making it difficult for third parties to track activities and steal data](https://bing.com/search?q=Virtual+Private+Networks+pros+and+cons)[1](https://bing.com/search?q=Virtual+Private+Networks+pros+and+cons).

## Pros of implementing VPNs:

* VPNs provide a layer of privacy and security by encrypting internet traffic. This makes it difficult for third parties to track activities and steal data.
* VPNs can help avoid getting hacked while using public Wi-Fi at an airport or library. This is because VPNs act as a secure tunnel and encrypt internet traffic.
* [VPNs can keep your internet service provider from knowing what sites you visited because the traffic coming to and from your computer all travels through the VPN’s servers, or servers VPNs pay to use](https://www.bing.com/aclk?ld=e83gkJ29qbmUu8cYkNgVfaCjVUCUx3vCyorXNIwmWui8A8rISGT4ATMfXuQu_8nGJifMsVNZrD0_vVyNtSvYRynbmDYfM2jUvwoREzv_CIrOKnWn2gIEyYOWegOAxJPNIFOUp5hBSGQU35pxcSs4Qxqzw59vf63cS8Oh_e_94A9QZD8MND&u=aHR0cHMlM2ElMmYlMmZ3d3cudnBubWVudG9yLmNvbSUyZmluLXVzYS1iZXN0LXZwbiUzZmtleXdvcmQlM2R2cG4lMjUyMHJhbmtpbmclMjZnZW8lM2QxMTA3MzUlMjZkZXZpY2UlM2QlMjZ1dG1fc291cmNlJTNkYmluZyUyNmFkaWQlM2Q3NjIxMDA1Nzk0MzY4MCUyNm1zY2xraWQlM2Q3NTEzMDFiNzM2MTQxZTY2ZTBiZDY0MTA0MzJlYjBkYw&rlid=751301b736141e66e0bd6410432eb0dc)[1](https://www.consumerreports.org/electronics-computers/vpn-services/should-you-use-a-vpn-a5562069524/).
* [VPNs can bypass geographical restrictions on content 2](https://privacysavvy.com/vpn/guides/pros-and-cons-of-vpn/) 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 restrictions on content](https://www.bing.com/aclk?ld=e8YiIMdr2QtA2Sk-u0-9k1uDVUCUwZqJo7k-TZ_u3VURZI-3jr14Tl4u2r6BKbbALVRPh16htACtOCb2UysS_OGSA02FnjNda5d_7Dsl3j4em0VxQmLB5dYQ9xV9_8fwf4GatF_vLHO4kWLTXLy2sWMccuzGxta13Ki3OpGEZizfm9Lnk7&u=aHR0cHMlM2ElMmYlMmZ3d3cuZXhwcmVzc3Zwbi5jb20lMmZ3aGF0LWlzLXZwbiUyZnVuYmxvY2std2Vic2l0ZXMlM2ZvZmZlciUzZDNtb250aHNmcmVlJTI2b2ZmZXJfY29kZSUzZDNjNmhqb29yNjklMjZyZWZJRCUzZEJJX2NhbXBhaWduaWQlM2Q0MDU1NDQ1ODUlMjZtc2Nsa2lkJTNkNjU2NzIxOTRkNjRkMWQ1Y2UwNjc0NDMzYTMxNGNjMTE&rlid=65672194d64d1d5ce0674433a314cc11)

## Cons 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 2](https://privacysavvy.com/vpn/guides/pros-and-cons-of-vpn/).
* VPN use is banned in some authoritarian countries. [In some countries, VPNs are banned or heavily regulated](https://www.consumerreports.org/electronics-computers/vpn-services/should-you-use-a-vpn-a5562069524/)[2](https://privacysavvy.com/vpn/guides/pros-and-cons-of-vpn/).
* Using free VPNs risks exposure to ads, malware, and leaks. [Free VPNs may sell user data to third-party advertisers or inject ads into web pages](https://www.consumerreports.org/electronics-computers/vpn-services/should-you-use-a-vpn-a5562069524/)[2](https://privacysavvy.com/vpn/guides/pros-and-cons-of-vpn/).

## Installation specifics:

* [A VPN establishes an encrypted tunnel between the system running the VPN client and a VPN server that then proxies traffic through the tunnel to the rest of the enterprise network](https://bing.com/search?q=Virtual+Private+Networks+pros+and+cons) [4](https://insights.sei.cmu.edu/blog/remote-work-vulnerabilities-and-threats-to-the-enterprise/). Steps include
  1. A VPN client is installed on the user’s device, which encrypts all traffic between the device and the VPN server.
  2. The VPN server decrypts the traffic and forwards it to the intended destination.
  3. The destination server responds to the request by sending traffic back to the VPN server.
  4. The VPN server encrypts the traffic and sends it back to the VPN client.
  5. [The VPN client decrypts the traffic and sends it to the user’s device](https://www.bing.com/aclk?ld=e8OcZUYHFbvxJgBgmEWpxgCzVUCUz-UOb13n9w7mOCOGgLkPnDhd3Uh-ipDjPE6Hpo4QBuX2o2EUlY6g5-dRpoq53O3haHMQ8RcFRpVU95xD1yO9RVjEOu3gsgBNFb6xmA-Gvbq-gT8RFWo2P6R0BeJBd5LyAIvbSKlU_DPbqAqdr2ubUB&u=aHR0cHMlM2ElMmYlMmZ3d3cub3BlcmEuY29tJTJmZmVhdHVyZXMlMmZmcmVlLXZwbiUzZnV0bV9zb3VyY2UlM2RiaW5nJTI2dXRtX21lZGl1bSUzZHBhJTI2dXRtX2NhbXBhaWduJTNkVVMlMjUyMC0lMjUyMFBlcmZvcm1hbmNlJTI1MjBNYXglMjUyMC0lMjUyMEVOJTI2dXRtX2NvbnRlbnQlM2QlN2Jhc3NldEdyb3VwSWQlN2QlMjZtc2Nsa2lkJTNkZDVhYzJiMDEzNDM2MWVkNDRmNGE0ZWE2NDA1MDk5MjIlMjZ1dG1fdGVybSUzZHd3dy5vcGVyYS5jb20&rlid=d5ac2b0134361ed44f4a4ea640509922)[1](https://www.cisco.com/c/en/us/solutions/small-business/resource-center/security/how-to-setup-a-vpn.html).
* To install and configure a VPN server, follow these steps:
  1. Create a VPN profile on your computer.
  2. Click start and then click on Settings to open settings menu.
  3. On settings menu, click on Network and Internet click on VPN.
  4. Select Add a VPN connection.
  5. On add a VPN connection window there are a few tasks to carry out.
  6. [Save the changes you have made](https://bing.com/search?q=Virtual+Private+Networks+pros+and+cons) [5](https://www.techzone360.com/topics/techzone/articles/2020/09/16/446567-how-install-configure-virtual-private-network-server.htm).

## Risks and mitigations:

* Attackers have been aware of remote work as a threat vector for some time. The remote work environment is particularly appealing for attackers for several reasons. First, the home-network environment is not professionally managed. Most critically, this means that many more systems on home networks are not patched regularly, and a number of them are out of date with respect to vulnerability mitigation. To persist on an enterprise network, an attacker who has exploited a system must avoid detection and resist remediation. Here too, the home network is friendlier to the attacker; threat detection is typically nearly absent, and remediation incidental, such as when a PC is reinstalled or retired because it is running slowly. To secure the remote work environment, it is essential to extend zero-trust assumptions further. [It isn’t just the network that should be assumed hostile, but everything that is not under the enterprise’s control](https://bing.com/search?q=Virtual+Private+Networks+pros+and+cons) [4](https://insights.sei.cmu.edu/blog/remote-work-vulnerabilities-and-threats-to-the-enterprise/).
* [Update VPNs, network infrastructure devices, and devices being used to remote into work environments with the latest software patches and security configurations](https://bing.com/search?q=Virtual+Private+Networks+pros+and+cons) [6](https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-073a).

## Implementation best practices:

Best practices for implementing VPNs in a corporate network include:

* [Select a standards-based VPN that uses accepted 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](https://www.bing.com/aclk?ld=e8IaDdghmbnebPF9t8NDtSPTVUCUzEN_M1950bORweSvjTxQ_j5Hx8cAExcEXM0D9tIxdCoCR_Jw7t7hWJ87VsGu1b1NcLpgYJAJvLbk73VuMpBtE5y4UGUvcr2PV-wLevlqXTg4Ng7Q5s3eKLWASODIm5vCFYV3bH2LqA92NtuM3IAecU&u=&rlid=488aa28de39614beea91c72a9258abad) [1](https://resources.infosecinstitute.com/topic/how-to-choose-and-harden-your-vpn-best-practices-from-nsa-cisa/)[2](https://www.sdxcentral.com/security/definitions/what-is-encryption-definition/what-is-virtual-private-network-vpn/what-are-vpn-best-practices/).
* Use a VPN with strong cryptography. Validate 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 authentication through digital certificates (stored on smartcards) when possible](https://www.bing.com/aclk?ld=e8IaDdghmbnebPF9t8NDtSPTVUCUzEN_M1950bORweSvjTxQ_j5Hx8cAExcEXM0D9tIxdCoCR_Jw7t7hWJ87VsGu1b1NcLpgYJAJvLbk73VuMpBtE5y4UGUvcr2PV-wLevlqXTg4Ng7Q5s3eKLWASODIm5vCFYV3bH2LqA92NtuM3IAecU&u=&rlid=488aa28de39614beea91c72a9258abad) [1](https://resources.infosecinstitute.com/topic/how-to-choose-and-harden-your-vpn-best-practices-from-nsa-cisa/)[2](https://www.sdxcentral.com/security/definitions/what-is-encryption-definition/what-is-virtual-private-network-vpn/what-are-vpn-best-practices/).
* Manage software vulnerabilities. The exploitation of VPN vulnerabilities is a common attack vector for cybercriminals. Select a VPN vendor with a strong track record of vulnerability patching, and request a software bill of materials (SBOM) to validate that third-party code is up-to-date and secure. Also, look for a product that can perform validation of its code when running to detect potential intrusions. [After deploying a VPN, regularly check for and promptly apply software updates](https://www.bing.com/aclk?ld=e8IaDdghmbnebPF9t8NDtSPTVUCUzEN_M1950bORweSvjTxQ_j5Hx8cAExcEXM0D9tIxdCoCR_Jw7t7hWJ87VsGu1b1NcLpgYJAJvLbk73VuMpBtE5y4UGUvcr2PV-wLevlqXTg4Ng7Q5s3eKLWASODIm5vCFYV3bH2LqA92NtuM3IAecU&u=&rlid=488aa28de39614beea91c72a9258abad) [1](https://resources.infosecinstitute.com/topic/how-to-choose-and-harden-your-vpn-best-practices-from-nsa-cisa/)[2](https://www.sdxcentral.com/security/definitions/what-is-encryption-definition/what-is-virtual-private-network-vpn/what-are-vpn-best-practices/).
* Prepare for surges in use. [IT security personnel should test VPN limitations in preparation for mass usage](https://resources.infosecinstitute.com/topic/how-to-choose-and-harden-your-vpn-best-practices-from-nsa-cisa/) [2](https://www.sdxcentral.com/security/definitions/what-is-encryption-definition/what-is-virtual-private-network-vpn/what-are-vpn-best-practices/).
* Avoid free VPNs. [Using free VPNs risks exposure to ads, malware, and leaks 3](https://forti1.com/en/ssl-vpn-best-practices-7-security-tips/).