# Trey Research Corporation

Virtula Private Network: Tinjauan Teknis untuk Fabrikam, Inc.

**15 Desember 2023**

**Virtual Private Networks (VPN)** adalah solusi keamanan jaringan populer yang dapat membantu mengenkripsi lalu lintas jaringan. [VPN bertindak sebagai terowongan yang aman dan mengenkripsi lalu lintas internet, sehingga sulit bagi pihak ketiga untuk melacak aktivitas dan mencuri data](https://bing.com/search?q=Virtual+Private+Networks+pros+and+cons)[1.](https://bing.com/search?q=Virtual+Private+Networks+pros+and+cons)

## Kelebihan penerapan VPN:

* VPN menyediakan lapisan privasi dan keamanan dengan mengenkripsi lalu lintas internet. Hal ini membuat pihak ketiga sulit untuk melacak aktivitas dan mencuri data.
* VPN dapat membantu menghindari peretasan saat menggunakan Wi-Fi publik di bandara atau perpustakaan. Ini karena VPN bertindak sebagai terowongan yang aman dan mengenkripsi lalu lintas internet.
* [VPN dapat mencegah penyedia layanan internet Anda mengetahui situs apa yang Anda kunjungi karena lalu lintas yang masuk ke dan dari komputer Anda semuanya melakukan perjalanan melalui server VPN, atau server yang dibayar oleh VPN untuk digunakan](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/)
* [VPN dapat melewati pembatasan geografis dalam konten 2](https://privacysavvy.com/vpn/guides/pros-and-cons-of-vpn/)dengan menutupi alamat IP Anda dan mengenkripsi koneksi internet Anda. Saat Anda terhubung ke server VPN, lalu lintas internet Anda diarahkan melalui server VPN, yang memberi alamat IP baru kepada Anda. [Ini membuat seolah-olah Anda mengakses internet dari lokasi berbeda, memungkinkan Anda bisa melewati pembatasan geografis dalam konten](https://www.bing.com/aclk?ld=e8YiIMdr2QtA2Sk-u0-9k1uDVUCUwZqJo7k-TZ_u3VURZI-3jr14Tl4u2r6BKbbALVRPh16htACtOCb2UysS_OGSA02FnjNda5d_7Dsl3j4em0VxQmLB5dYQ9xV9_8fwf4GatF_vLHO4kWLTXLy2sWMccuzGxta13Ki3OpGEZizfm9Lnk7&u=aHR0cHMlM2ElMmYlMmZ3d3cuZXhwcmVzc3Zwbi5jb20lMmZ3aGF0LWlzLXZwbiUyZnVuYmxvY2std2Vic2l0ZXMlM2ZvZmZlciUzZDNtb250aHNmcmVlJTI2b2ZmZXJfY29kZSUzZDNjNmhqb29yNjklMjZyZWZJRCUzZEJJX2NhbXBhaWduaWQlM2Q0MDU1NDQ1ODUlMjZtc2Nsa2lkJTNkNjU2NzIxOTRkNjRkMWQ1Y2UwNjc0NDMzYTMxNGNjMTE&rlid=65672194d64d1d5ce0674433a314cc11)

## Kerugian dalam penerapan VPN:

* Kecepatan koneksi bisa lebih lambat dari ISP Anda. [Hal ini disebabkan oleh VPN menambahkan lapisan enkripsi dan perutean ekstra ke lalu lintas internet2](https://privacysavvy.com/vpn/guides/pros-and-cons-of-vpn/) Anda.
* Penggunaan VPN dilarang di beberapa negara otoriter. [Di beberapa negara, VPN dilarang atau diatur dengan peraturan yang ketat](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/).
* Menggunakan VPN gratis berisiko terpapar iklan, malware, dan kebocoran. [VPN gratis dapat menjual data pengguna kepada pengiklan kepada pihak ketiga atau memasukkan iklan ke halaman web](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/).

## Penginstalan spesifik:

* [VPN membuat terowongan terenkripsi antara sistem yang menjalankan klien VPN dan server VPN yang kemudian menjadi penghubung lalu lintas melalui terowongan ke seluruh jaringan perusahaan](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/). Langkah-langkahnya meliputi:
  1. Klien VPN diinstal pada perangkat pengguna yang mengenkripsi semua lalu lintas antara perangkat dan server VPN.
  2. Server VPN mendekripsi lalu lintas dan meneruskannya ke server yang dituju.
  3. Server tujuan merespons permintaan dengan mengirim lalu lintas kembali ke server VPN.
  4. Server VPN mengenkripsi lalu lintas dan mengirimkannya kembali ke klien VPN.
  5. [Klien VPN mendekripsi lalu lintas dan mengirimkannya ke perangkat pengguna](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).
* Untuk menginstal dan mengonfigurasi server VPN, ikuti langkah-langkah berikut:
  1. Buat profil VPN di komputer Anda.
  2. Klik mulai lalu klik Pengaturan untuk membuka menu pengaturan.
  3. Pada menu pengaturan, klik Jaringan dan Internet klik VPN.
  4. Pilih Tambahkan koneksi VPN.
  5. Pada tambahkan window koneksi VPN ada beberapa tugas yang harus dilakukan.
  6. [Simpan perubahan yang telah Anda lakukan](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).

## Mitigasi dan risiko

* Penyerang telah menyadari pekerjaan jarak jauh sebagai vektor ancaman selama waktu yang cukup lama. Lingkungan kerja jarak jauh sangat menarik bagi penyerang karena beberapa alasan. Pertama, lingkungan jaringan rumah tidak dikelola secara profesional. Satu hal yang paling kritis, ini berarti masih banyak sistem di jaringan rumah tidak diperbarui secara teratur, dan sejumlah sistem tersebut sudah ketinggalan zaman dalam hal mitigasi kerentanan. Agar dapat bertahan di jaringan perusahaan, penyerang yang telah mengeksploitasi sistem harus menghindari deteksi dan menolak perbaikan dalam kerentanan Di sini juga, jaringan rumah lebih ramah bagi penyerang; biasanya deteksi ancaman hampir tidak ada, dan perbaikan bersifat insidental, seperti ketika PC diinstal ulang atau dihentikan karena berjalan lambat. Untuk mengamankan lingkungan kerja jarak jauh, penting untuk memperluas asumsi zero-trust lebih lanjut. [Ini bukan hanya jaringan yang harus dianggap bermusuhan, tetapi segala sesuatu yang tidak berada di bawah kendali perusahaan](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/).
* [Perbarui VPN, perangkat infrastruktur jaringan, dan perangkat yang digunakan untuk masuk lingkungan kerja jarak jauh dengan modifikasi perangkat lunak dan konfigurasi keamanan terbaru](https://bing.com/search?q=Virtual+Private+Networks+pros+and+cons)[6](https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-073a).

## Praktik terbaik penerapan

Praktik terbaik untuk menerapkan VPN dalam jaringan perusahaan meliputi:

* [Pilih VPN berbasis standar yang menggunakan standar yang diterima, seperti Internet Key Exchange/Internet Protocol Security (IKE/IPSec), yang pada umumnya risikonya lebih rendah dan lebih aman daripada VPN Secure Sockets Layer/Transport Layer Security (SSL/TLS) yang menggunakan kode khusus untuk mengirim lalu lintas melalui 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/).
* Gunakan VPN dengan kriptografi yang kuat. Validasi bahwa algoritma enkripsi, algoritma autentikasi, dan protokol yang digunakan oleh VPN kuat dan divalidasi FIP. [Konfigurasikan semua VPN untuk menggunakan autentikasi multifaktor (MFA) dan ganti autentikasi berbasis kata sandi dengan autentikasi klien melalui sertifikat digital (disimpan di smartcard) jika memungkinkan](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/).
* Mengelola kerentanan perangkat lunak. Eksploitasi kerentanan VPN adalah vektor serangan yang biasa dilakukan penjahat siber. Pilih vendor VPN dengan rekam jejak yang kuat dalam menambal kerentanan, dan meminta daftar software bill of materials (SBOM) untuk memvalidasi bahwa kode pihak ketiga sudah mutakhir dan aman. Selain itu, cari produk yang dapat melakukan validasi kodenya saat dijalankan untuk mendeteksi potensi gangguan. [Setelah menyebarkan VPN, periksa secara berkala dan segera terapkan pembaruan perangkat lunak](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/).
* Bersiap menghadapi lonjakan penggunaan. [Personel keamanan IT harus menguji batasan VPN sebagai persiapan untuk penggunaan massal](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/).
* Hindari VPN gratis. [Menggunakan VPN gratis berisiko terpapar iklan, malware, dan kebocoran 3](https://forti1.com/en/ssl-vpn-best-practices-7-security-tips/).