# Trey Research Corporation

Redes Privadas Virtuais: uma visão geral técnica da Fabrikam, Inc.

**15 de dezembro de 2023**

As **VPNs (redes privadas virtuais)** são uma solução popular de segurança de rede que pode ajudar a criptografar o tráfego de rede. [As VPNs atuam como um túnel seguro e criptografam o tráfego da Internet, dificultando o rastreamento de atividades e o roubo de dados por parte de terceiros](https://bing.com/search?q=Virtual+Private+Networks+pros+and+cons)[1](https://bing.com/search?q=Virtual+Private+Networks+pros+and+cons).

## Prós da implementação de VPNs:

* As VPNs fornecem uma camada de privacidade e segurança ao criptografarem o tráfego da Internet, dificultando que terceiros rastreiem atividades e roubem dados.
* As VPNs são especialmente úteis para proteger contra ataques ao usar Wi-Fi público em locais como aeroportos ou bibliotecas, pois atuam como um túnel seguro e criptografam o tráfego da Internet.
* [As VPNs podem impedir que seu provedor de serviços de Internet saiba quais sites você visitou porque o tráfego que entra e sai do seu computador passa pelos servidores da VPN ou servidores que as VPNs pagam para usar](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/).
* [As VPNs podem ignorar as restrições geográficas do conteúdo 2](https://privacysavvy.com/vpn/guides/pros-and-cons-of-vpn/)mascarando o seu endereço IP e criptografando a sua conexão com a Internet. Quando você se conecta a um servidor VPN, seu tráfego de internet é roteado através do servidor VPN, que atribui a você um novo endereço IP. [Isso faz parecer que você está acessando a Internet de um local diferente, permitindo que você ignore as restrições geográficas do conteúdo](https://www.bing.com/aclk?ld=e8YiIMdr2QtA2Sk-u0-9k1uDVUCUwZqJo7k-TZ_u3VURZI-3jr14Tl4u2r6BKbbALVRPh16htACtOCb2UysS_OGSA02FnjNda5d_7Dsl3j4em0VxQmLB5dYQ9xV9_8fwf4GatF_vLHO4kWLTXLy2sWMccuzGxta13Ki3OpGEZizfm9Lnk7&u=aHR0cHMlM2ElMmYlMmZ3d3cuZXhwcmVzc3Zwbi5jb20lMmZ3aGF0LWlzLXZwbiUyZnVuYmxvY2std2Vic2l0ZXMlM2ZvZmZlciUzZDNtb250aHNmcmVlJTI2b2ZmZXJfY29kZSUzZDNjNmhqb29yNjklMjZyZWZJRCUzZEJJX2NhbXBhaWduaWQlM2Q0MDU1NDQ1ODUlMjZtc2Nsa2lkJTNkNjU2NzIxOTRkNjRkMWQ1Y2UwNjc0NDMzYTMxNGNjMTE&rlid=65672194d64d1d5ce0674433a314cc11)

## Contras da implementação de VPNs:

* As velocidades de conexão podem ser mais lentas do que o seu ISP. [Isso ocorre porque as VPNs adicionam uma camada extra de criptografia e roteamento ao tráfego da Internet 2](https://privacysavvy.com/vpn/guides/pros-and-cons-of-vpn/).
* O uso de VPN é proibido em alguns países autoritários. [Em alguns países, as VPNs são proibidas ou fortemente regulamentadas](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/).
* O uso de VPNs gratuitas corre o risco de exposição a anúncios, malware e vazamentos. [As VPNs gratuitas podem vender dados do usuário a anunciantes terceirizados ou injetar anúncios em páginas da 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/).

## Especificações de instalação:

* [Uma VPN estabelece um túnel criptografado entre o sistema que executa o cliente VPN e um servidor VPN que, em seguida, faz proxy do tráfego através do túnel para o restante da rede corporativa](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/). As etapas incluem
  1. Um cliente VPN é instalado no dispositivo do usuário, que criptografa todo o tráfego entre o dispositivo e o servidor VPN.
  2. O servidor VPN descriptografa o tráfego e o encaminha para o destino pretendido.
  3. O servidor de destino responde à solicitação enviando o tráfego de volta para o servidor VPN.
  4. O servidor VPN criptografa o tráfego e o envia de volta para o cliente VPN.
  5. [O cliente VPN descriptografa o tráfego e o envia para o dispositivo do usuário](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).
* Para instalar e configurar um servidor VPN, siga estas etapas:
  1. Crie um perfil VPN no seu computador.
  2. Clique em "Iniciar" e, em seguida, clique em "Configurações" para abrir o menu de configurações.
  3. No menu de configurações, clique em "Rede e Internet" e, em seguida, em "VPN".
  4. Selecione Adicionar uma conexão VPN.
  5. Na janela "Adicionar uma conexão VPN", há algumas tarefas a serem realizadas.
  6. [Salve as alterações feitas](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).

## Riscos e mitigações:

* Os invasores estão cientes do trabalho remoto como um vetor de ameaça há um tempo. O ambiente de trabalho remoto é particularmente interessante para os invasores por vários motivos. Primeiro, o ambiente de rede doméstica não é gerenciado profissionalmente. Mais criticamente, isso significa que muitos outros sistemas em redes domésticas não são corrigidos regularmente e vários deles estão desatualizados em relação à mitigação de vulnerabilidades. Para persistir em uma rede corporativa, um invasor que explorou um sistema deve evitar a detecção e resistir à correção. Neste caso a rede doméstica também é mais fácil para o invasor; a detecção de ameaças geralmente é quase inexistente e a correção é incidental, como quando um computador é reinstalado ou desativado porque está lento. Para proteger o ambiente de trabalho remoto, é essencial estender ainda mais as suposições de confiança zero. [Não é apenas a rede que deve ser considerada hostil, mas tudo o que não está sob o controle da empresa](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/).
* [Atualize as VPNs, os dispositivos de infraestrutura de rede e os dispositivos que estão sendo usados para ambientes de trabalho remotos com os patches de software e configurações de segurança mais recentes](https://bing.com/search?q=Virtual+Private+Networks+pros+and+cons) [6](https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-073a).

## Melhores práticas de implementação:

Estas são algumas das melhores práticas para implementar VPNs em uma rede corporativa:

* [Selecione uma VPN baseada em padrões que use padrões aceitos, como os protocolos IKE/IPSec, que geralmente são menos arriscados e mais seguros do que as VPNs de protocolos SSL/TLS que usam código personalizado para enviar tráfego por 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 uma VPN com criptografia forte. Valide se os algoritmos de criptografia, algoritmos de autenticação e protocolos usados por uma VPN são fortes e validados por FIP. [Configure todas as VPNs para usar a MFA (autenticação multifator ) e substitua a autenticação com senha pela autenticação do cliente com certificados digitais (armazenados em cartões inteligentes) quando possível](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/).
* Gerencie vulnerabilidades de software. A exploração de vulnerabilidades de VPN é um vetor de ataque comum para quem comete crimes cibernéticos. Escolha um fornecedor de VPN com um forte histórico de aplicação de patches de vulnerabilidade e solicite uma SBOM (lista de materiais de software) para validar se o código de terceiros está atualizado e é seguro. Além disso, procure um produto que possa realizar a validação de seu código durante a execução para detectar possíveis invasões. [Depois de implantar uma VPN, verifique regularmente e aplique rapidamente as atualizações de software.](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-se para surtos de uso. [A equipe de segurança de TI testará as limitações da VPN na preparação para o uso em massa](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/).
* Evite VPNs gratuitas. [O uso de VPNs gratuitas traz risco de exposição a anúncios, malware e vazamentos 3](https://forti1.com/en/ssl-vpn-best-practices-7-security-tips/).