# Trey Research Corporation

Reti private virtuali: panoramica tecnica per Fabrikam, Inc.

**15 dicembre 2023**

Le **reti private virtuali (VPN)** sono una soluzione di sicurezza di rete molto diffusa che consente di crittografare il traffico di rete. [Le VPN agiscono come un tunnel sicuro e crittografano il traffico Internet, rendendo difficile a terzi tracciare le attività e rubare i dati.](https://bing.com/search?q=Virtual+Private+Networks+pros+and+cons)[1](https://bing.com/search?q=Virtual+Private+Networks+pros+and+cons).

## Vantaggi dell'implementazione delle VPN:

* Le VPN offrono un livello di privacy e di sicurezza crittografando il traffico Internet. In questo modo sarà più difficile per terzi tracciare le attività e rubare i dati.
* Le VPN possono aiutare a evitare di subire violazioni durante l'uso del Wi-Fi pubblico in un aeroporto o in una biblioteca. Questo perché le VPN agiscono come un tunnel sicuro e criptano il traffico Internet.
* [Le VPN impediscono al provider di servizi Internet di monitorare i siti web visitati, in quanto il traffico in entrata e in uscita dal computer viene indirizzato tramite i server della VPN, o tramite i relativi server a pagamento](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/).
* [Le VPN possono aggirare le restrizioni geografiche sui contenuti 2](https://privacysavvy.com/vpn/guides/pros-and-cons-of-vpn/)nascondendo l'indirizzo IP e crittografando la connessione a Internet.. Durante la connessione a un server VPN, il traffico Internet viene instradato tramite il server VPN, che assegna un nuovo indirizzo IP. [Ciò fa sembrare che l'accesso a Internet avvenga da un'altra posizione, consentendo di aggirare le restrizioni geografiche sui contenuti.](https://www.bing.com/aclk?ld=e8YiIMdr2QtA2Sk-u0-9k1uDVUCUwZqJo7k-TZ_u3VURZI-3jr14Tl4u2r6BKbbALVRPh16htACtOCb2UysS_OGSA02FnjNda5d_7Dsl3j4em0VxQmLB5dYQ9xV9_8fwf4GatF_vLHO4kWLTXLy2sWMccuzGxta13Ki3OpGEZizfm9Lnk7&u=aHR0cHMlM2ElMmYlMmZ3d3cuZXhwcmVzc3Zwbi5jb20lMmZ3aGF0LWlzLXZwbiUyZnVuYmxvY2std2Vic2l0ZXMlM2ZvZmZlciUzZDNtb250aHNmcmVlJTI2b2ZmZXJfY29kZSUzZDNjNmhqb29yNjklMjZyZWZJRCUzZEJJX2NhbXBhaWduaWQlM2Q0MDU1NDQ1ODUlMjZtc2Nsa2lkJTNkNjU2NzIxOTRkNjRkMWQ1Y2UwNjc0NDMzYTMxNGNjMTE&rlid=65672194d64d1d5ce0674433a314cc11)

## Svantaggi dell'implementazione delle VPN:

* La velocità di connessione può essere inferiore a quella dell'ISP. [Questo perché le VPN aggiungono un ulteriore livello di crittografia e di instradamento al traffico Internet 2](https://privacysavvy.com/vpn/guides/pros-and-cons-of-vpn/).
* L'uso della VPN è vietato in alcuni paesi autoritari. [In alcuni paesi, le VPN sono vietate o fortemente regolamentate](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/).
* L'uso di VPN gratuite rischia di esporre l'utente a pubblicità, malware e fughe. [Le VPN gratuite possono vendere i dati degli utenti a inserzionisti terzi o inserire annunci nelle pagine 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/).

## Specifiche dell'installazione:

* [Una VPN crea un tunnel crittografato tra il dispositivo che esegue il client VPN e un server VPN, il quale successivamente instrada il traffico attraverso il tunnel, permettendo l'accesso sicuro al resto della rete aziendale](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/). I passaggi includono
  1. Sul dispositivo dell'utente viene installato un client VPN che crittografa tutto il traffico tra il dispositivo e il server VPN.
  2. Il server VPN decrittografa il traffico e lo inoltra alla destinazione desiderata.
  3. Il server di destinazione risponde alla richiesta inviando nuovamente il traffico al server VPN.
  4. Il server VPN crittografa il traffico e lo invia nuovamente al client VPN.
  5. [Il client VPN decrittografa il traffico e lo invia al dispositivo dell'utente](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).
* Per installare e configurare un server VPN, seguire questa procedura:
  1. Creare un profilo VPN sul computer.
  2. Fare clic su Start e quindi su Impostazioni per aprire il menu delle impostazioni.
  3. Nel menu delle impostazioni, fare clic su Rete e Internet, quindi su VPN.
  4. Selezionare Aggiungi una connessione VPN.
  5. Nella finestra Aggiungi una connessione VPN sono presenti diverse operazioni da completare.
  6. [Salvare le modifiche apportate](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).

## Rischi e mitigazioni:

* Gli utenti malintenzionati sono da tempo consapevoli del lavoro da remoto come potenziale vettore di minacce. L'ambiente di lavoro remoto è particolarmente attraente per gli utenti malintenzionati per diversi motivi. In primo luogo, l'ambiente della rete domestica non è gestito in modo professionale. Il problema principale risiede nel fatto che molti altri dispositivi sulle reti domestiche non vengono aggiornati regolarmente, e molti di essi non sono equipaggiati con le necessarie misure di mitigazione delle vulnerabilità. Per mantenere la presenza su una rete aziendale, un utente malintenzionato che ha sfruttato un sistema deve evitare il rilevamento e resistere alle azioni di rimedio. Anche in questo caso, la rete domestica risulta più favorevole per l'utente malintenzionato; la rilevazione delle minacce è generalmente quasi assente e le azioni di rimedio sono occasionali, come nel caso in cui un PC venga reinstallato o dismesso perché lento. Per garantire la sicurezza dell'ambiente di lavoro remoto, è fondamentale estendere ulteriormente i principi di zero-trust. [Non è solo la rete a dover essere considerata un ambiente ostile, ma qualsiasi elemento che sfugga al controllo diretto dell'azienda](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/).
* [Aggiornare le VPN, i dispositivi dell'infrastruttura di rete e i dispositivi usati per l'accesso remoto agli ambienti di lavoro con le patch software e le configurazioni di sicurezza più recenti](https://bing.com/search?q=Virtual+Private+Networks+pros+and+cons) [6](https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-073a).

## Procedure consigliate per l'implementazione:

Le procedure consigliate per l'implementazione di una VPN in una rete aziendale includono:

* [Selezionare una VPN che utilizza standard accettati, come Internet Key Exchange/Internet Protocol Security (IKE/IPSec), che sono generalmente meno rischiosi e più sicuri delle VPN Secure Sockets Layer/Transport Layer Security (SSL/TLS) che utilizzano codice personalizzato per inviare il traffico su 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/).
* Usare una VPN con crittografia avanzata. Verificare che gli algoritmi di crittografia, gli algoritmi di autenticazione e i protocolli utilizzati da una VPN siano forti e convalidati da FIP. [Configurare tutte le VPN per usare l'autenticazione a più fattori (MFA), e, quando possibile, sostituire l'autenticazione basata su password con un sistema di autenticazione client tramite certificati digitali (memorizzati su smartcard)](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/).
* Gestire le vulnerabilità del software. Lo sfruttamento delle vulnerabilità delle VPN è un vettore di attacco comune per i criminali informatici. Selezionare un fornitore VPN con una comprovata esperienza di applicazione di patch per la vulnerabilità e richiedere una distinta base del software (SBOM) per convalidare che il codice di terze parti è aggiornato e sicuro. Cercare anche un prodotto in grado di eseguire la convalida del codice durante l'esecuzione per rilevare potenziali intrusioni. [Dopo aver distribuito una VPN, verificare regolarmente e applicare tempestivamente gli aggiornamenti 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/).
* Prepararsi per i picchi d'uso. [Il personale addetto alla sicurezza IT deve testare le limitazioni VPN in preparazione all'utilizzo di 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/).
* Evitare VPN gratuite. [L'uso di VPN gratuite rischia l'esposizione ad annunci, malware e perdite 3](https://forti1.com/en/ssl-vpn-best-practices-7-security-tips/).