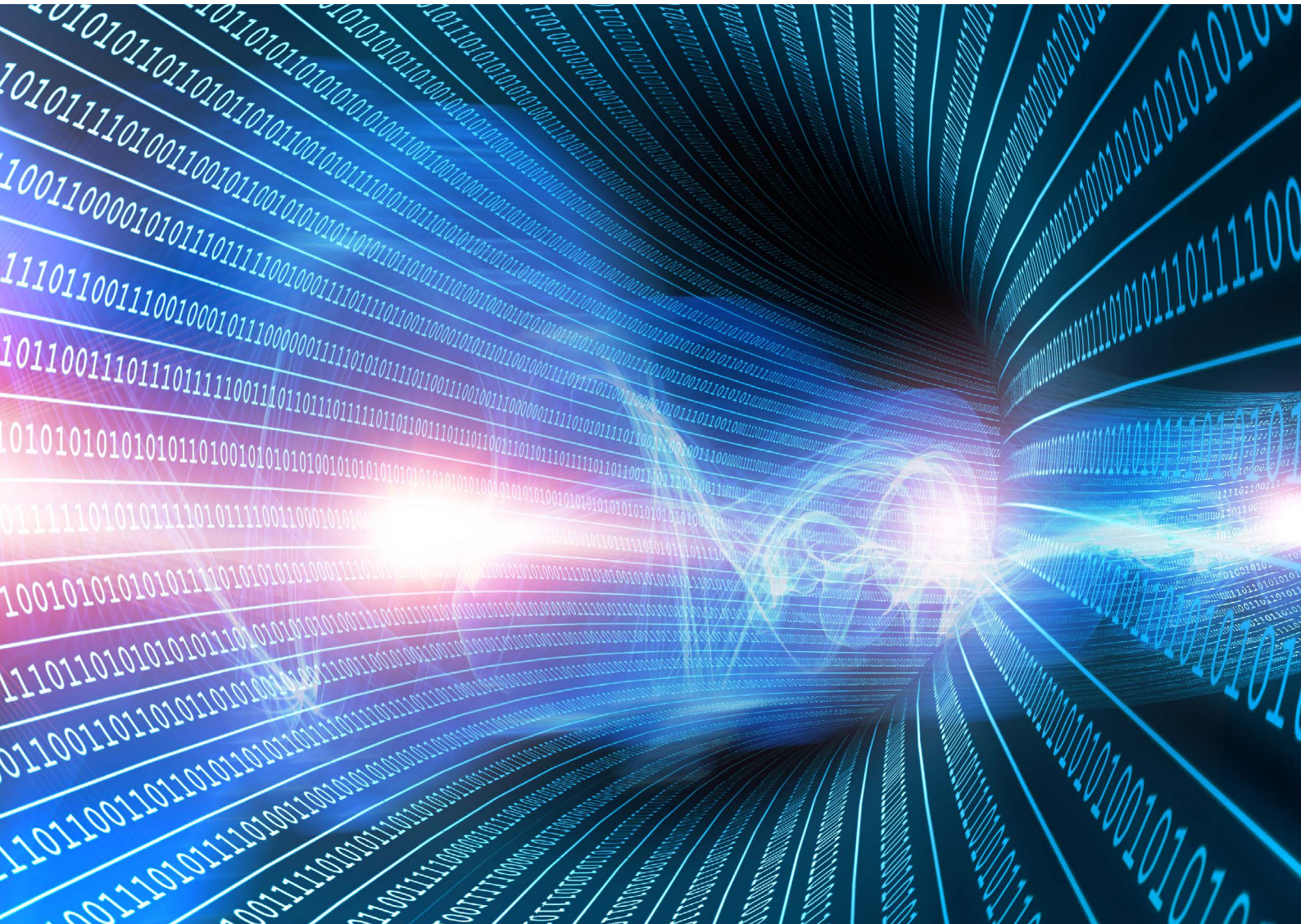
VPN: cos'è, come funziona e a cosa serve una Virtual Private Network

Testi a cura di Salvatore Lombardo,
Funzionario informatico, Esperto ICT, Socio Clusit e autore

LEGGI SUL SITO



INDICE DEGLI ARGOMENTI

Una **VPN (Virtual Private Network)** è una rete privata virtuale che **garantisce privacy, anonimato e sicurezza** attraverso un canale di comunicazione logicamente riservato (tunnel VPN) e creato sopra un'infrastruttura di rete pubblica.

Il termine virtuale sta a significare che tutti i dispositivi appartenenti alla rete non devono essere necessariamente collegati ad una stessa LAN locale ma possono essere dislocati in qualsiasi punto geografico del mondo.

1

COS'È UNA VPN

Una VPN è dunque un particolare servizio di rete che può **essere utilizzato per criptare il traffico Internet** e, di conseguenza, proteggere la propria identità online.

In ambito prettamente aziendale, una VPN **può essere paragonata ad una estensione geografica della rete locale privata (LAN)** e che, quindi, permette di collegare tra loro, in maniera sicura, i siti della stessa azienda dislocati sul territorio.

Per farlo, viene sfruttato l'instradamento dei pacchetti di dati tramite il protocollo IP per il trasporto su scala geografica: questo permette, di fatto, di realizzare una LAN "virtuale" e "privata" ma del tutto equivalente ad un'infrastruttura fisica di rete dedicata.

2. A COSA SERVE UNA VPN

Le VPN sono utilizzate soprattutto in ambito aziendale e dalle amministrazioni pubbliche, soprattutto per la possibilità di abbattere i costi nella realizzazione di una propria rete protetta e creata, per l'appunto, sfruttando l'infrastruttura della rete pubblica.

Sono comunque anche molti gli utenti privati che preferiscono navigare in rete tramite VPN per poter esplorare e scambiare dati su Internet in maniera sicura e senza restrizioni o geoblocking.

Tra i vari servizi disponibili, alcuni provider offrono anche la possibilità di scegliere quali protocolli utilizzare per la connessione, optando per un server VPN allestito all'interno della propria rete (aziendale/privata) oppure collegandone uno gestito da terzi.

È bene tenere a mente che, poiché i dati su Internet, se non adeguatamente protetti, possono essere intercettati da chiunque si trovi sul loro percorso (tramite tecniche di sniffing), i soggetti interessati a conoscere i dettagli delle attività di rete svolte dagli utenti potrebbero essere diversi e con scopi differenti: investigativi, commerciali o fraudolenti.

Di seguito analizziamo in dettaglio le tipologie, i principi di funzionamento e i protocolli che caratterizzano una VPN.

3 CLASSIFICAZIONE DELLE VPN

Le reti VPN si dividono in reti ad accesso remoto e reti site-to-site:

CONNESSIONE VPN AD ACCESSO REMOTO

Le connessioni ad accesso remoto consentono agli utenti (ad esempio in smart working) di accedere a un server su una rete privata per il tramite della rete Internet. Questo tipo di connessione può essere vista come un collegamento tra un PC client VPN e il server dell'azienda. Come già detto, dal punto di vista logico è come se si disponesse di un collegamento dedicato e privato.

CONNESSIONE VPN SITE-TO-SITE

Una connessione site-to-site è utilizzata per connettere in una rete privata, sempre con l'ausilio di una rete pubblica, uffici dislocati in più sedi o di altre organizzazioni, consentendo il routing ed una comunicazione sicura. In questo scenario, ogni sede avrà un router dedicato, ovvero un nodo della rete VPN che instraderà i pacchetti dati verso i destinatari omologhi secondo un modello client/server, condividendo le informazioni con le sedi remote in modo del tutto trasparente. Concettualmente si possono distinguere due sotto classi di VPN site-to-site:

1. una classe VPN-Intranet quando si uniscono più sedi della stessa azienda;
2. una classe VPN-Extranet quando si uniscono aziende e/o uffici esterni all'organizzazione.

All'interno di questa distinzione, in base ai livelli di sicurezza e affidabilità del circuito virtuale le VPN possono essere ulteriormente classificate in:

- **Trusted.** L'ISP (Internet Service Provider) garantisce la creazione di una serie di percorsi dotati di precise caratteristiche di sicurezza, assegnando un determinato indirizzo IP fisso e applicando una corretta politica di sicurezza delle informazioni;
- **Secure.** Questo tipo di VPN, attraverso protocolli di crittografia, garantisce la creazione di un tunnel tra i nodi della rete privata. I dati che viaggiano all'interno del tunnel risultano pertanto inaccessibili a tentativi d'intercettazione;
- **Hybrid.** Come specificato dal nome si tratta di una particolare tipologia di rete privata mista. Si applica nei casi in cui una azienda dotata di una Trusted VPN avesse bisogno anche di una Secure VPN. Con una VPN ibrida si garantisce così una buona sicurezza ed un certo livello di qualità del servizio dei circuiti di tunneling.

OSSERVAZIONI

VPN SOFTWARE

Funzionano attraverso l'installazione di un software client sui dispositivi interessati, accedendo con delle credenziali fornite e autenticate dai rispettivi provider e server VPN.

VPN HARDWARE

Sono dei dispositivi di rete, solitamente dei router dotati di software client VPN proprietari preinstalati.

DIFFERENZE

Le differenze fondamentali tra le due tipologie di VPN consistono nella praticità e trasparenza della fruibilità del servizio. Per le VPN basate su software occorre installare e configurare manualmente su ogni dispositivo client con le relative credenziali e attivarle ogni volta per il corretto utilizzo.
Con le VPN basate su hardware si ha il vantaggio di avere il servizio sempre attivo con l'operatività su Internet costantementeprotetta e criptata, indipendentemente dal dispositivo in uso e connesso in rete.

4 COME FUNZIONA UNA VPN

Poiché l'infrastruttura di rete utilizzata dai meccanismi VPN è Internet (rete più economicamente vantaggiosa, capillarmente diffusa ma intrinsecamente insicura) occorrono delle misure che superino i limiti caratteristici di una rete pubblica non protetta: il tunneling, l'autenticazione e la crittografia.

IL TUNNELING

Tale meccanismo prevede di **instaurare un tunnel sicuro tra due entità remote finali ed abilitate a realizzare una VPN**. Non esiste nessun tunnel tecnicamente, ma piuttosto solo un collegamento logico attraverso una rete IP. Le due estremità del tunnel, anche se distanti e collegati attraverso molti nodi intermedi, durante il processo logico diventano virtualmente adiacenti.

Facendo riferimento allo standard protocollare ISO/OSI ed all'architettura TCP/IP in particolare, possiamo affermare che **con il tunneling si compie un incapsulamento multi-protocollare dei dati**.
I pacchetti di dati, anche se appartenenti a protocolli differenti una volta giunti all'ingresso del tunnel, vengono ulteriormente imbustati dal protocollo di tunneling e successivamente spediti sulla rete verso l'uscita del tunnel, dove dopo avere rimosso l'imbustamento raggiungono la destinazione.

L'AUTENTICAZIONE ED IL PROCESSO DI COMUNICAZIONE

Il processo di autenticazione, che dipende dal tipo di protocollo adottato, è necessario alfine di **autorizzare l'accesso, assicurare la trasmissione, garantire il non ripudio.**

Indipendentemente dalla tipologia VPN usata (accesso remoto/site-to-site) per instaurare una connessione tra un client ed il relativo server i passi che sono richiesti possono essere così riassunti:

1. il client contatta il server;
2. il server notifica la propria presenza;
3. il client richiede al server di essere identificato;
4. il server verifica che il tentativo di connessione sia autorizzato previa autenticazione riuscita;
5. il server risponde alla richiesta di autenticazione e autorizza la comunicazione con il client;
6. inizia la comunicazione tra le due entità.

LA CRITTOGRAFIA

La crittografia, tecnica che assicura la riservatezza delle informazioni, trasforma il dato leggibile mediante un algoritmo digitale in un dato codificato e incomprensibile per i non autorizzati.

La funzione di decifratura effettua il processo inverso. Il tipo di cifratura adoperata, come per il tipo di autenticazione usata, dipende dal protocollo di comunicazione adottato dal fornitore del servizio. Gli algoritmi di cifratura possono essere classificati in simmetrici, asimmetrici e basati sull'hashing:

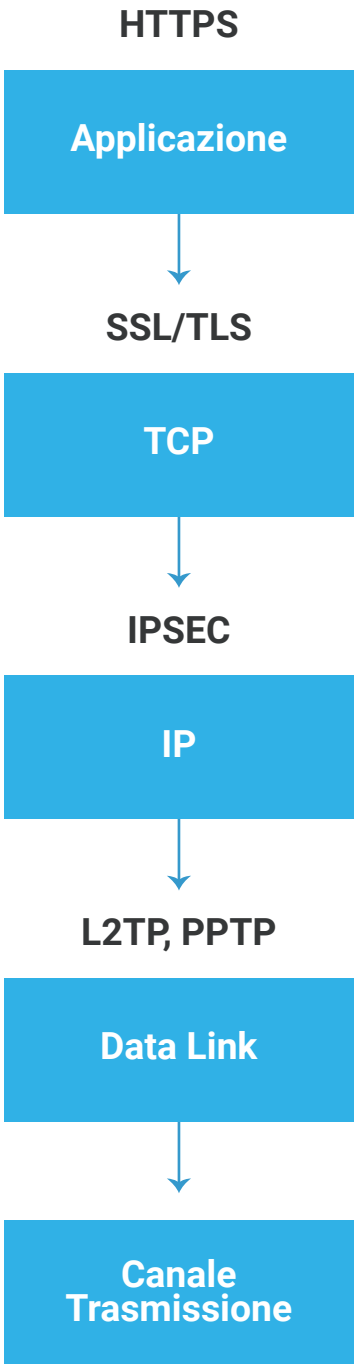
- **algoritmo simmetrico:** tecnica che utilizza la medesima chiave per cifrare e per decifrare i dati. Algoritmi comunemente usati sono: DES (Data Encryption Standard) e AES (Advanced Encryption Standard);
- **algoritmo asimmetrico:** tecnica che utilizza una chiave diversa per cifrare e decifrare i dati. Algoritmi comunemente usati sono: RSA (Rivest, Shamir e Adleman), ECC (Elliptic Curve Cryptography), DSA (Digital Signature Algorithm) e Diffie-Hellman;
- **hashing:** tecnica che utilizza una funzione (hash) non reversibile (univoca) per proteggere oltre la riservatezza anche l'integrità dei dati. Algoritmi comunemente usati sono: MD5, SHA 2 (Secure Hash Algorithm), Argon 2.

5 PROTOCOLLI PER RETI VPN

Per la trasmissione VPN esistono opportuni protocolli la cui scelta d'utilizzo dovrebbe dipendere dalle necessità e dai requisiti desiderati. Ognuno di questi protocolli con la loro specificità, contribuisce alla protezione dei pacchetti dati in trasmissione.

Tra i protocolli più comuni si possono citare PPTP, L2PT, IPSEC, L2TP/IPSEC, SSL/TLS e HTTPS:

- **PPTP.** Il Point to Point Tunneling Protocol è un protocollo di livello 2 che si basa sul protocollo PPP (Point to Point Protocol) e viene solitamente utilizzato in combinazione con il protocollo di livello 3 GRE (Generic Routing Encapsulation);



- **L2TP.** Il Layer 2 Tunneling Protocol è un protocollo di livello 2 che non prevede alcuna forma di autenticazione e cifratura ma solamente permette di realizzare un tunnel virtuale;
- **IPSEC.** L'Internet Protocol Security è un protocollo di livello 3 che permette una comunicazione sicura sulle reti IP. La riservatezza, l'integrità e l'autenticità del traffico dati vengono assicurate attraverso meccanismi di cifratura e autenticazione;
- **L2TP / IPsec.** L'implementazione dei protocolli L2TP su IPsec è un modo per ottenere le migliori caratteristiche di entrambi gli standard. Il risultato è un protocollo con un certo livello di sicurezza, che consente la trasmissione crittografata dei pacchetti dati (IPSEC) su un tunnel virtuale (L2TP);
- **SSL/TLS.** Il Secure Sockets Layer (TLS – Transport Layer Security è una versione aggiornata e più sicura di SSL) è un protocollo di livello 4 la cui tecnologia può essere usata anche per garantire la sicurezza di una connessione VPN. Una delle soluzioni software per la configurazione di una VPN per mezzo di SSL è OpenVPN;
- **HTTPS.** L'Hyper Text Transfer Protocol Secure è un protocollo di livello applicazione per il trasferimento ipertestuale sicuro che si appoggia sul protocollo di trasporto SSL/TLS. Può essere utilizzato attraverso l'installazione di applicativi ad hoc e/o di estensioni browser.

6 ALCUNI SERVIZI PREMIUM VPN

Esistono innumerevoli servizi VPN offerti in rete. La ricerca e la scelta deve essere fatta secondo le proprie reali esigenze e valutando opportunamente le varie funzioni opzionali proposte, tenendo bene in mente che per usufruire di tutte le peculiarità di una buona VPN, ovvero riservatezza, sicurezza e protezione delle informazioni conviene optare sempre verso soluzioni premium (a pagamento) ed affidabili.

Tra le varie funzioni di un certo livello qualitativo, alle quali prestare attenzione, se la privacy e l'anonimato sono le principali prerogative desiderate si possono indicare le seguenti:

- **split tunneling:** questo servizio di rete consente di accedere contemporaneamente e in modo trasparente a domini di sicurezza diversi (Internet/LAN) per il tramite delle stesse o diverse connessioni di rete, senza predite di connessioni o zone d'ombra che possano inficiare anonimato e privacy;
- **gestione delle perdite DNS.** I servizi VPN più affidabili devono garantire oltre che la riservatezza anche la privacy, ad esempio mascherando l'indirizzo IP di navigazione. L'uso di un server proprietario per le richieste DNS diverso da quello fornito dal provider dei servizi Internet ISP, può consentire di evitare la rintracciabilità dei movimenti sul web. Una corretta gestione deve sapere risolvere gli errori DNS salvaguardando la riservatezza di navigazione;
- **kill switch.** Questo servizio consente di mantenere sempre aperta una connessione VPN anche nel caso di un'interruzione del servizio Internet. Il tunnel virtuale rimane aperto e la connessione VPN verrà ripristinata solo in seguito al ripristino del servizio Internet.

7 CONSIDERAZIONI FINALI

I principali fattori che devono fare propendere verso l'uso di una VPN sono quindi:

1. per il privato:
   a) la privacy e l'anonimato;
   b) la possibilità di poter accedere senza restrizioni a servizi e siti web;
   c) una migliore protezione dalle minacce informatiche, se impiegata con cognizione di causa, una certa prudenza ed un buon antivirus.

2. per le aziende, oltre a quelli validi per i privati:
   a) l'abbattimento dei costi. Grazie all' uso di Internet come infrastruttura di collegamento remoto delle VPN i costi di mantenimento di una rete si riducono significativamente;
   b) migliore fruibilità delle comunicazioni. Gli utenti remoti si possono connettere in sicurezza alle risorse della rete aziendale o tra loro da qualunque posto e h24;
   c) adattabilità. Un'infrastruttura basata su VPN è facilmente adattabile alle necessità di cambiamento delle reti ed è molto flessibile in quanto può realizzare una rete privata sia tra sedi fisse e remote che tra terminali remoti;
   d) sicurezza. La sicurezza e l'affidabilità di una VPN derivano dall'utilizzo di protocolli di tunneling per l'implementazione di una topologia punto-punto.

Valgono comunque le solite regole di buona pratica. Nell'avere consapevolezza che nessun strumento hardware e software è sicuro al 100%, per evitare spiacevoli inconvenienti, occorre che amministratori e

utenti recepiscano ogni security advisory ed applichino le patch rese disponibili dai fornitori (prima che sia troppo tardi!) per porre rimedio allo sfruttamento di ogni possibile vulnerabilità.

È sempre consigliabile consultare la documentazione del servizio VPN che si ha intenzione di adoperare per conoscere anzitempo gli algoritmi ed i protocolli adottati, facendo attenzione ai provider che offrono VPN gratis, perché solitamente il conto si paga alla fine in termini di prestazioni e per i rischi e le vulnerabilità che si possono celare o trascurare.

Pubblicato il 13 Marzo 2020

NETWORK DIGITAL 360

Network Digital360 è il più grande network in Italia di testate e portali B2b dedicati ai temi della Trasformazione Digitale e dell'Innovazione Imprenditoriale, con oltre 50 fra portali, canali e newsletter.
Ha la missione di diffondere la cultura digitale e imprenditoriale nelle imprese e pubbliche amministrazioni italiane e di fornire a tutti i decisori che devono valutare investimenti tecnologici informazioni aggiornate e approfondite.
Il Network è parte integrante di Digital360HUB, il polo di Demand Generation di Digital360, che mette a disposizione delle tech company un'ampia gamma di servizi di comunicazione, storytelling, pr, content marketing, marketing automation, inbound marketing, lead generation, eventi e webinar.

VIA COPERNICO, 38
20125 - MILANO
TEL. 02 92852785
MAIL: MARKETING@DIGITAL4.BIZ