Virtual Private Network

Da Wikipedia, l'enciclopedia libera.

Una **Virtual Private Network** o **VPN** è una rete privata instaurata tra soggetti che utilizzano un sistema di trasmissione pubblico e condiviso come per esempio Internet. Lo scopo delle reti VPN è di dare alle aziende le stesse possibilità delle linee private in affitto ad un costo inferiore sfruttando le reti condivise pubbliche.

Le reti VPN utilizzano collegamenti che necessitano di autenticazione per garantire che solo gli utenti autorizzati vi possano accedere; per garantire la sicurezza che i dati inviati in Internet non vengano intercettati o utilizzati da altri non autorizzati, esse utilizzano sistemi di crittografia.

Le reti VPN sicure adottano dunque protocolli che provvedono a cifrare il traffico transitante sulla VPN. Oltre alla cifratura, una VPN sicura deve prevedere nei suoi protocolli dei meccanismi che impediscano violazioni della sicurezza, come ad esempio il furto dell'identità digitale o l'alterazione dei messaggi.

Il termine VPN è un termine generico e non un marchio. In particolare, non esiste alcun ente che regoli la denominazione di un prodotto come VPN, che quindi ogni produttore può utilizzare a suo arbitrio.

Esistono tuttavia vari organismi indipendenti, largamente riconosciuti, che certificano interoperabilità e sicurezza dei sistemi informatici, come ad esempio ICSA Labs. Un apparato o un software, che riporti il marchio di ICSA Labs per le VPN IPSec, ha sicuramente superato una serie di test oggettivi e replicabili, che garantiscono la compatibilità con tutte le altre implementazioni certificate ed un adeguato livello di sicurezza. È oggi opinione comune che una VPN correttamente progettata abbia un grado di sicurezza comparabile con quello di una rete dedicata.

Per mezzo di una VPN, utilizzando una connessione Internet si è comunque in grado di effettuare una connessione al proprio ufficio, con una telefonata al numero telefonico dell'accesso Internet più vicino. Se si dispone di una connessione Internet ad alta velocità (ad esempio via cavo o ADSL) per il proprio computer e per i computer aziendali, è possibile connettersi in rete con il proprio ufficio alla velocità relativamente alta della connessione Internet utilizzata.

Generalmente una VPN comprende due parti: una *interna alla rete*, e quindi protetta, che preserva la trasmissione, e una meno affidabile e sicura che è *quella esterna alla rete private*, ad esempio via Internet.

Nelle VPN c’è in genere un firewall tra il computer del dipendente o di un cliente e il terminale della rete o del server. Il dipendente, per esempio, quando stabilisce la connessione con il firewall, deve autenticare i dati che vuole trasmettere, passando attraverso un servizio di autenticazione interno.

Un utente autenticato può essere provvisto di privilegi particolari per accedere a risorse che generalmente non sono accessibili a tutti gli utenti. La maggior parte dei programmi client richiede che tutto il traffico IP della VPN passi attraverso un “Tunnel” virtuale tra le reti utilizzando Internet come mezzo di collegamento. Dal punto di vista dell’utente ciò significa che, mentre la connessione VPN è attiva, tutti gli accessi esterni alla rete sicura devono passare per lo stesso firewall come se l’utente fosse fisicamente connesso all’interno della rete sicura. Questo riduce il rischio che utenti esterni possano accedere alla rete privata dell’azienda.

La sicurezza della connessione VPN è di importanza fondamentale, perché la rete su cui gli altri computer stanno lavorando potrebbe non essere sicura, o esserlo solo parzialmente. La VPN deve quindi garantire un livello di sicurezza tale da proteggere i computer dei dipendenti che stanno lavorando simultaneamente sulla stessa rete, tra i quali uno potrebbe essere stato infettato da un virus, un worm o un trojan.

Indice

[nascondi]

Tipologie di VPN

- TRUSTED VPN
- SECURED VPN
- HYBRID VPN

Trusted VPN

La garanzia che la rete Trusted VPN offre è la sicurezza che nessun terzo non autorizzato possa usufruire del circuito del cliente. Questo implica che il cliente abbia un proprio indirizzo IP e una propria politica di sicurezza.

Il circuito viaggia attraverso uno o più “interruttori” di comunicazione che possono essere compromessi da chi vuole disturbare il traffico della rete. Il cliente di una VPN si aspetta quindi che il fornitore (provider) della VPN mantenga l’integrità del circuito in modo da impedire l'accesso di intrusi.

Le aziende che utilizzano la Trusted VPN vogliono avere la sicurezza che i loro dati si muovano attraverso una serie di percorsi che hanno proprietà specifiche e che sono controllati da un ISP. Il cliente ha quindi fiducia che i percorsi attraverso i quali questi dati si muovono siano mantenuti sicuri secondo i criteri di un precedente accordo, anche se generalmente il cliente non conosce quali siano i percorsi utilizzati dal fornitore della VPN Trusted.

Requisiti Necessari

- ***nessuno al di fuori del fornitore della VPN Trusted può influire sulla creazione o la modificazione del percorso VPN.***

Nessuno al di fuori del rapporto di fiducia può cambiare nessuna parte della VPN.

- ***nessuno al di fuori del fornitore della VPN Trusted può modificare i dati in entrata o quelli eliminati dal percorso della VPN.***

I dati viaggiano all'interno dei vari percorsi che sono condivisi da più clienti del fornitore, il percorso deve quindi essere specificato dal VPN e nessuno a parte il fornitore di fiducia può modificare i vari dati.

- ***Il percorso e l'indirizzo usati in una VPN Trusted devono essere stabiliti prima che il VPN venga creato.***

Il cliente deve sapere ciò che si aspetta dal fornitore, così che entrambi possano pianificare e creare la rete per la quale stanno collaborando.

Tecnologie utilizzate dal VPN

Le tecnologie utilizzate si suddividono in *Layer 2* e *Layer 3*;

Layer 2

- circuiti ATM
- circuiti di trasmissione
- trasporto del layer 2 sopra l'MPLS

Layer 3

- MPLS con distribuzione limitata delle informazioni del percorso attraverso l'BGP (Border Gateway Protocol).

Secure VPN

Da quando Internet si è diffusa ed è diventato un importante mezzo di comunicazione, la sicurezza è diventata sempre più importante, sia per i clienti, sia per i provider. Visto che la VPN non offriva una sicurezza completa, i fornitori di connettività hanno cominciato a creare protocolli che permettessero l'encrittazione dei dati da parte della rete o da parte del computer di provenienza, in modo da essere trasportati in Internet come qualsiasi altro dato, per poi essere decriptati all'arrivo nella rete dell'azienda o nel computer ricevente.

Questo traffico criptato agisce come un *"Tunnel"* tra due reti: anche se un intruso cercasse di leggere i dati non potrebbe decifrarne il contenuto né modificarli, dato che eventuali modifiche sarebbero immediatamente rilevate dal ricevente e quindi respinte. Le reti costruite utilizzando la criptazione dei dati sono chiamate Secure VPN.

Più recentemente i fornitori di servizio hanno cominciato ad offrire un nuovo tipo di Trusted VPN, questa volta usando Internet invece della rete telefonica come substrato di comunicazione. Queste nuove Trusted VPN non offrono sicurezza, ma danno ai clienti un modo di creare facilmente segmenti di rete su vasta scala (WAN), inoltre i segmenti Trusted VPN possono essere controllati da un posto unico e spesso con una qualità di servizio garantita (QoS - quality of service) dal provider.

Il motivo principale per cui le società usano una Secure VPN è che possono trasmettere informazioni delicate su Internet senza temere che vengano spiate. Tutta l'informazione che viaggia attraverso una Secure VPN è criptato ad un tale livello che, anche se una persona catturasse una copia del traffico, non potrebbe leggerlo anche se usasse computer di alte prestazioni (supercomputer). Inoltre una Secure VPN permette all'azienda di avere la sicurezza che nessun intruso può alterare i contenuti delle trasmissioni.

Le Secure VPN sono particolarmente utili per permettere accessi remoti da parte di utilizzatori connessi ad Internet da zone non controllate dall'amministratore della rete.

Requisiti Necessari

- ***Tutto il traffico su una Secure VPN deve essere criptato e autenticato.***

Molti dei protocolli utilizzati per creare Secure VPN permettono la creazione di reti autenticate, ma non criptate. Anche se una simile rete è più sicura di una rete senza autenticazione, non potrebbe essere considerata una VPN perché non protegge la privacy.

- ***Le proprietà di sicurezza di una VPN devono essere concordate da tutte le parti della VPN.***

VPN sicure hanno uno o più *"tunnel"* e ogni tunnel ha due estremità. Gli amministratori delle due estremità di ogni Tunnel devono essere in grado di accordarsi sulle proprietà di sicurezza del tunnel.

- ***Nessuno al di fuori della VPN può compromettere le proprietà di sicurezza della VPN.***

Deve essere impossibile per un intruso cambiare le proprietà di sicurezza di una o più parti della VPN, in modo da indebolire la criptazione o di compromettere le chiavi di criptazione usate.

Tecnologie utilizzate dai Secured VPN

- IPsec con criptazione in ogni Tunnel.
- IPsec interne al L2TP.
- SSL 3.0 o TLS con criptazione

Queste tecnologie sono standardizzate nel IETF (Internet Engineering Task Force Sito IETF).

Hybrid VPN

Una Secure VPN può essere adoperata come parte di una Trusted VPN creando un terzo tipo di VPN, recentemente introdotta sul mercato:

Hybrid VPN

Le parti sicure di una Hybrid VPN possono essere controllate da un cliente o dallo stesso provider che fornisce la parte di fiducia dell'Hybrid VPN.

Qualche volta un'intera Hybrid VPN è resa sicura grazie ad una Secure VPN, ma più comunemente solo una parte dell’Hybrid VPN è sicura.

È chiaro che le Secure VPN e le Trusted VPN hanno proprietà molto differenti.

- Le *Secure VPN* danno sicurezza, ma non assicurano i percorsi.
- Le *Trusted VPN* assicurano le proprietà dei percorsi come QoS, ma non la sicurezza da intrusioni.

A causa di questi punti di forza e di debolezza sono state introdotte le Hybrid VPN. Gli scenari di utilizzazione sono tuttavia ancora in evoluzione. Una situazione tipica per il dispiegamento di un Hybrid VPN è quando un’azienda ha gia una Trusted VPN e desidera sicurezza su una parte della VPN. Fortunatamente nessuna delle tecnologie Trusted VPN inpedisce la creazione di Hybrid VPN, e qualche produttore sta creando sistemi che supportano esplicitamente la creazione di servizi Hybrid VPN.

Requisiti Necessari

- ***Gli indirizzi di confine tra la Secured VPN e la Trusted VPN devono essere estremamente chiari.***

In una Hybrid VPN, la Secure VPN dovrebbe essere un sottoinsieme della Trusted VPN. Per ogni paio di indirizzi dati in una Hybrid VPN, l'amministratore della VPN deve essere in grado di sapere con certezza se il traffico tra i due indirizzi è o meno parte della Secure VPN.

Tecnologie utilizzate dall’Hybrid VPN

- ***Ogni tecnologia supportata dalla Secure VPN si muove attraverso ogni tecnologia supportata dalla Trusted VPN.***

I protocolli

Le Secure VPN utilizzano protocolli crittografici a tunnel per offrire l’autenticazione del mittente e l’integrità del messaggio, allo scopo di difendere la privacy. Una volta scelte, implementate ed usate, alcune tecniche possono fornire comunicazioni sicure su reti non sicure.

Le tecnologie delle Secure VPN dovrebbero essere utilizzate come “*security overlay*” attraverso infrastrutture di rete dedicate.

I protocolli che implementano una VPN sicura più conosciuti sono:

- IPsec (IP security), comunemente usate su IPv4 (parte obbligatoria dell'IPv6).
- PPTP (point-to-point tunneling protocol), sviluppato da Microsoft.
- SSL/TLS, utilizzate sia per il “Tunneling” dell’intera rete, come nel progetto OpenVPN, o per assicurarsi che è essenzialmente un Web Proxy. L’SSL è un framework, molto spesso associato con il commercio elettronico, che si è rivelato di grande flessibilità ed è quindi usato come strato di sicurezza per varie implementazioni (più o meno standard) di reti private virtuali.
- VPN Quarantine: La macchina del cliente terminale della VPN potrebbe essere una fonte di attacco, cosa che non dipende dal progetto della VPN. Ci sono soluzioni che forniscono servizi di VPN Quarantine che controllano il computer remoto. Il il cliente viene tenuto in quarantena fino a che l'infezione non è stata rimossa.
- MPVPN (Multi Path Virtual Private Network), un trademark registrato di proprietà della Ragula System Development Company.

- L'ISPs ora offre un servizio VPN per aziende che vogliono la sicurezza e la convenienza di un VPN. Oltre a fornire ai dipendenti remoti un accesso sicuro alla rete interna, a volte vengono inclusi altri servizi di sicurezza e gestione.

Questi meccanismi non implementano di per sé una rete virtuale, ma solo un colloquio sicuro tra due terminali. In questi casi il meccanismo di rete virtuale deve essere realizzato mediante un protocollo apposito che viene poi incapsulato. Esiste oggi un discreto numero di approcci alternativi (ed ovviamente mutuamente incompatibili) a questo schema, tra i quali possiamo citare i seguenti.

- Protocollo SOCKS: questo approccio è il più "standard", in quanto SOCKS è uno standard IETF per Generic Firewall Traversal definito nella RFC 1928.
- OpenVPN mette a disposizione un eseguibile che crea un tunnel cifrato con un'altra istanza del medesimo programma su un computer remoto, e può trasportare l'intero stack TCP/IP.
- Un altro approccio molto usato utilizza il protocollo SSH, che è in grado, come OpenVPN, di creare dei tunnel tra due macchine collegate. Questa caratteristica è nata per trasportare XWindow, ma è stata implementata in modo generale, ed è quindi possibile utilizzarla per trasportare un protocollo qualsiasi. Una implementazione molto diffusa, in quanto open source e gratuita, è OpenSSH.
- L'approccio di ormai tutti i fornitori di firewall è invece quello di usare TLS per rendere sicura la comunicazione con un proxy al quale si accede via browser. Il canale cifrato viene realizzato in realtà generalmente tramite un'applet Java od un oggetto ActiveX, che quindi può essere installata in modo quasi trasparente per l'utente finale. La conseguente facilità di gestione fa sì che questo approccio sia particolarmente apprezzato nelle organizzazioni complesse.

Alcune reti VPN sicure non usano algoritmi di cifratura ma partono dal presupposto che un singolo soggetto fidato gestisca l'intera rete condivisa e che quindi l'impossibilità di accedere al traffico globale della rete renda i singoli canali sicuri dato che il gestore della rete fornisce ad ogni soggetto solamente la sua VPN.

I protocolli che utilizzano questa filosofia includono:

- L2F (Layer 2 Forwarding), sviluppato da Cisco.
- L2TP (Layer 2 Tunnelling Protocol), sviluppato in collaborazione tra Microsoft e Cisco.
- L2TPv3 (Layer 2 Tunnelling Protocol version 3). Le Trusted VPNs non usano un “Tunneling” crittografico e invece contano sulla sicurezza di una singola rete di provider per proteggere il traffico. In un certo senso, questa è un’elaborazione di una rete tradizionale.
- Multi- Protocol Label Switching (MPLS) è spesso usato per costruire una Trusted VPN.

Benefici per le Aziende

Una ben strutturata VPN può offrire grandi benefici per un’azienda:

- Estende la connettività geografica
- Migliora la sicurezza dove le linee di dati non sono state crittate
- Riduce i costi di operazione
- Riduce il tempo di transito e i costi di trasporto per i clienti remoti
- Semplifica la topologia di rete, almeno in determinati scenari
- Fornisce la possibilità di reti globali
- Fornisce supporto di rete
- Fornisce compatibilità con le reti a banda larga
- Fornisce una più veloce ROI (tempo di ritorno dell'investimento) rispetto al trasporto tradizionale delle linee WAN
- Mostra una buona economia di scala

Comunque, da quando la VPN ha così esteso la “mother network” con una dovizia di macchine e dispositivi, alcune implementazioni di sicurezza devono ricevere una attenzione particolare:

- La sicurezza nei confronti del cliente deve essere stretta e rafforzata. Questo è stato determinato dal Central Client Administration e dal Security Policy Enforcement.

È necessario che una azienda che abbia bisogno che ogni collaboratore possa usare la loro VPN fuori degli uffici, prima di tutto installi un firewall certificato. Alcune organizzazioni con dati particolarmente delicati fanno si che gli impiegati utilizzino due diverse connessioni WAN: una per lavorare ai dati delicati e l’altra per tutti gli altri usi.

- La scala di accesso al target di rete deve essere limitata
- Le politiche di registrazione devono essere valutate e nella maggior parte dei casi riviste

In situazioni in cui le aziende, o individui, hanno obblighi legali per la tenuta di informazioni confidenziali, ci possono essere problemi legali o penali. Due esempi sono i regolamenti HIPAA negli USA con riguardo ai dati sicuri, e i regolamenti generali dell’Unione europea che si applicano ad ogni informazione comerciale e contabile, e si estende a coloro che condividono questi dati.

Un modo per ridurre le conseguenze di un furto di un portatile è quello di usare un portatile Thin client, ora disponibili sul mercato. Questo permette ai dipendenti di accedere in remoto a database sicuri e confindeziali con minore rischio di perdere o compromettere la confidenzialità dei dati.

Tunneling

Il Tunneling è la trasmissione di dati attraverso una rete pubblica, che fa sì che i nodi di routing della rete pubblica non siano in grado di rilevare che la trasmissione è parte di una rete privata. In genere il Tunneling viene creato incapsulando i dati e il protocollo nel protocollo di rete pubblica, così che i dati che transitano per il tunnel non siano comprensibili a terzi che stiano eventualmente esaminando i dati trasmessi.

Il Tunneling permette di usare la rete pubblica per trasportare dati per conto di clienti autorizzati all'accesso alla rete privata.

Soluzione per la Sicurezza di una VPN

La parte più importante della soluzione VPN.

La vera natura della VPN - fare transitare dati privati in reti pubbliche - richiede attenzione verso le minacce potenziali ai dati stessi e l’impatto di quelli persi. Una VPN si preoccupa di tutti i tipi di minacce alla sicurezza, offrendo servizi di sicurezza nella aree di: **Autenticazione (*controllo all’accesso*)** :

l’autenticazione è un processo per assicurarsi che un cliente o un sistema siano effettivamente coloro che dichiarano di essere. Ci sono molti tipi di meccanismi di autenticazione, ma i più usati sono:

- *qualcosa che sai*: (una ID, password, PIN)
- *qualcosa che hai*: (un simbolo leggibile dal computer es. SmartCard)
- *qualcosa che sei*: (la retina, le impronte digitali)

La login o la password sono considerate generalmente autenticazioni *deboli*. *Forti* autenticazioni si ottengono combinando tra loro due diversi tipi di autenticazione. L'effettivo livello di sicurezza dipende ovviamente dal contesto, perché un SmartCard può essere rubata, e le credenziali di login possono non essere difficili da individuare.

Dati di sicurezza rubati o persi possono consentire più attacchi e necessitano di più schemi di autenticazione.

Nessuna tecnica offre completa sicurezza di autenticazione, neanche quelle Biometriche (impronte digitali, impronte vocali, mappatura della retina).