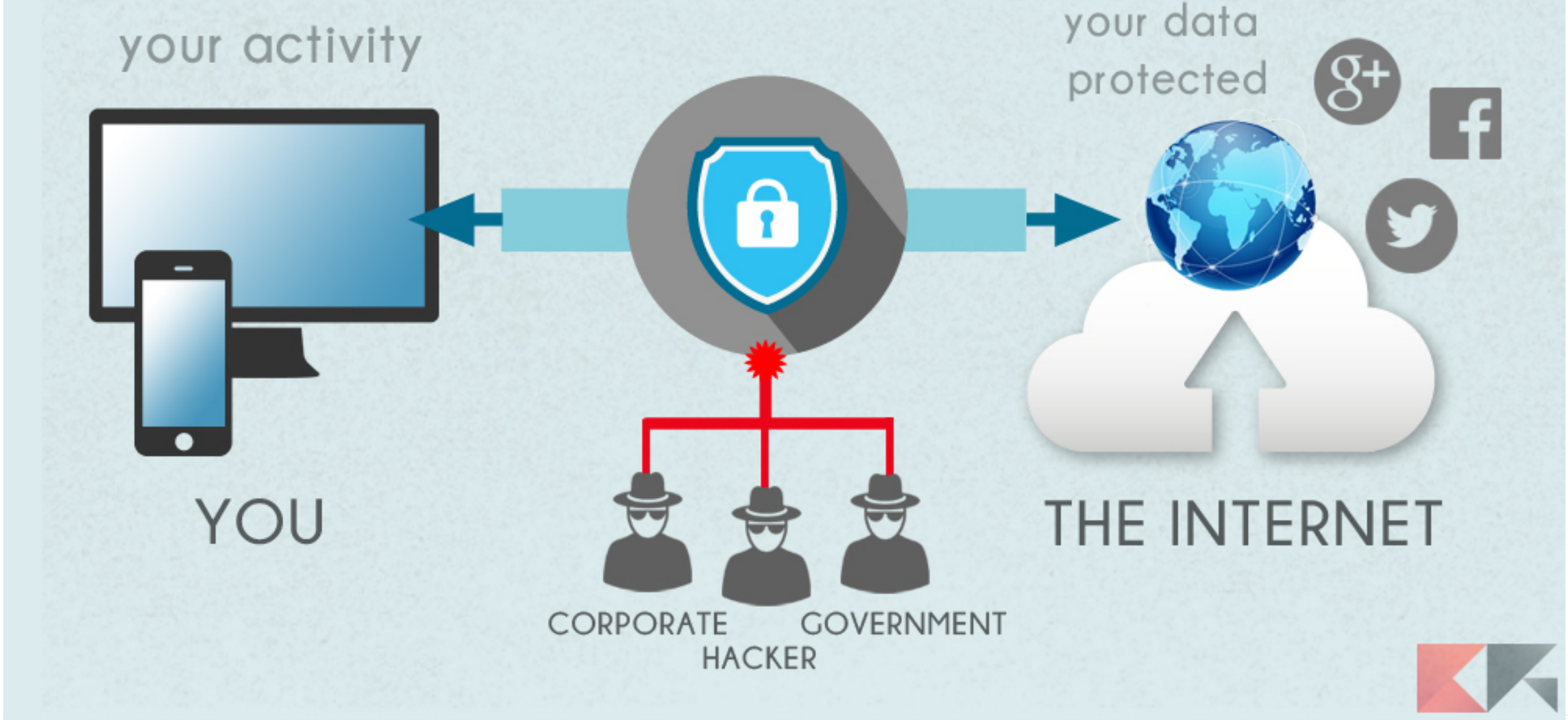
WHAT IS A VPN?


your activity
your data protected
YOU
THE INTERNET
CORPORATE
GOVERNMENT
HACKER

LE CARATTERISTICHE DI UNA VIRTUAL PRIVATE NETWORK

Per un'azienda con diverse sedi, dislocate anche a grande distanza tra loro, l'ideale sarebbe poterle trattare tutte come un'unica rete locale aziendale. In pratica, estendere in ambito geografico la propria rete LAN privata, realizzando, cioè, una WAN privata per il business di tutta l'azienda.
Gli sviluppi possibili sono molteplici: non solo sedi dislocate, ma anche la possibilità di includere nella rete postazioni di *homeworking* e *teleworking*, come pure eventuali LAN di partner consociati. Mediante la realizzazione di reti private, ogni LAN non è più un'isola nell'oceano (Internet) ma si collega con le altre in un arcipelago (WAN) con regole comuni e condivise.

LE CARATTERISTICHE DI UNA VIRTUAL PRIVATE NETWORK

Esistono reti private vere e proprie e reti private virtuali. Le reti private vere e proprie sono quelle che collegano più sedi in una rete aziendale attraverso canali dedicati, a uso esclusivo, pagandone l'affitto al proprietario o al gestore.
I vantaggi sono molti:

- larghezza di banda sempre disponibile;
- nessun problema di accesso;
- nessuna congestione del traffico (almeno non a livello di rete);
- prestazioni garantite;
- sicurezza garantita.

Gli svantaggi tuttavia non mancano:

- alti costi di installazione;
- costi ricorrenti di manutenzione;
- tempi lunghi per la configurazione e la riconfigurazione;
- mancanza di scalabilità;
- rischio di blocco della rete in caso di grave guasto su un canale (non c'è ridondanza).

LESSICO

L'**homeworking** è la tipologia di lavoro svolta da casa (ufficio domestico), collegandosi alla rete aziendale.

Il **teleworking** è la tipologia di lavoro svolta collegandosi alla rete aziendale da qualsiasi luogo col proprio dispositivo mobile.

LE CARATTERISTICHE DI UNA VIRTUAL PRIVATE NETWORK

Una VPN (Virtual Private Network)

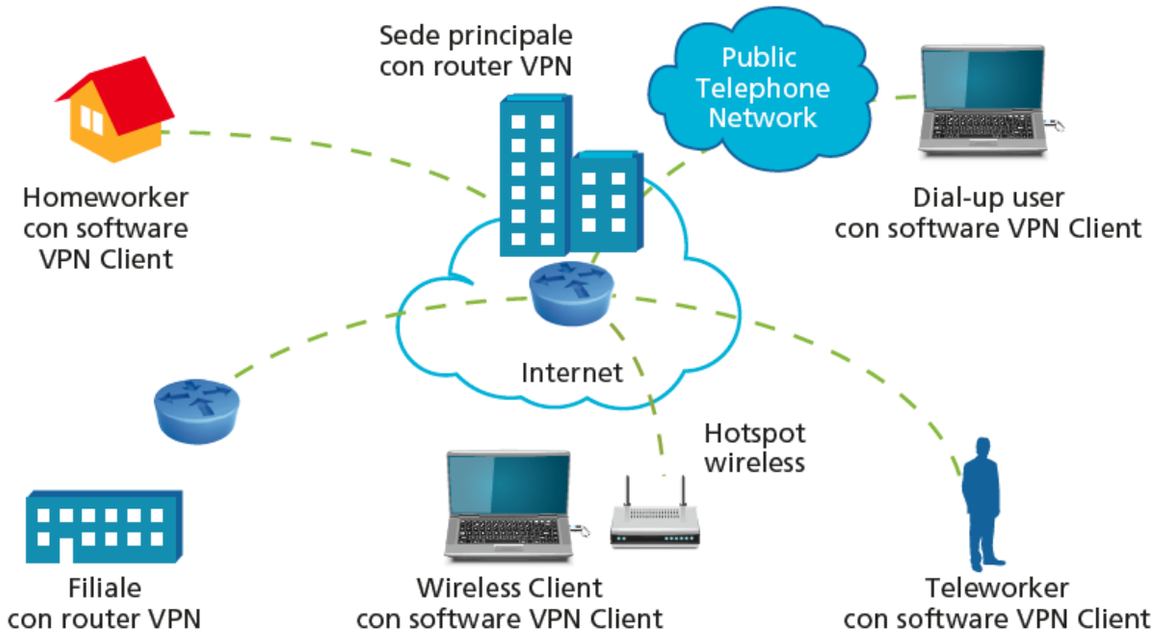
è una rete privata

creata all'interno

di un'infrastruttura

di rete pubblica,

per esempio Internet.



LE CARATTERISTICHE DI UNA VIRTUAL PRIVATE NETWORK

Rispetto a una normale rete privata, le VPN sono configurabili e riconfigurabili facilmente, sono scalabili e offrono un valido rapporto tra costi e funzionalità.
Dal momento che una VPN utilizza una rete pubblica, l'alto grado di ridondanza è garantito e dunque il rischio di blocco della rete è pressoché nullo.
La sua natura condivisa implica però il dover affrontare tre grossi problemi:

- la variabilità del tempo di trasferimento (traffico, congestione, latenza, velocità variabili, jitter, perdita di pacchetti, ecc.);
- il controllo degli accessi (autenticazione);
- la sicurezza delle trasmissioni (cifratura e tunneling).

TIPI DI VPN

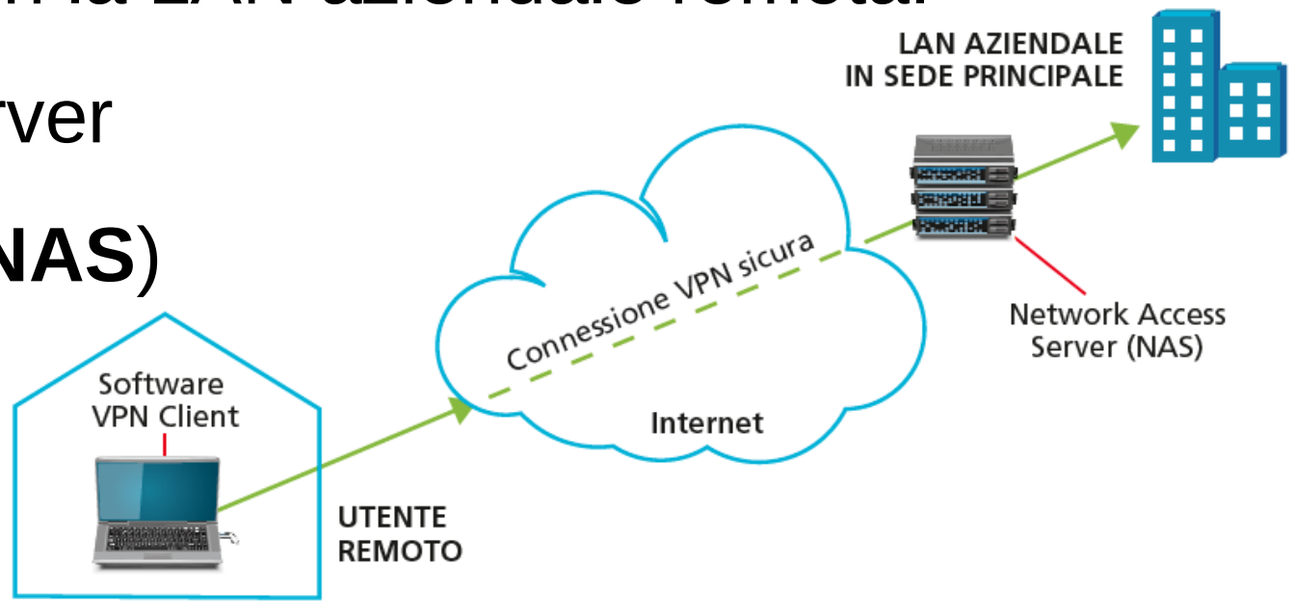
Tipi di VPN

Esistono due principali tipi di VPN in commercio:

- **Remote-access VPN**: porta qualsiasi applicazione dati, voce o video al desktop remoto, emulando il desktop dell'ufficio principale;
- **Site-to-site VPN**: è l'alternativa alle WAN e consente alle aziende di ampliare le risorse di rete alle filiali, agli uffici domestici e alle sedi di partner.

TIPI DI VPN

Remote-access VPN: consente ai singoli utenti di stabilire connessioni sicure con la LAN aziendale remota. Realizzata con un server di accesso alla rete (**NAS**) e un **software VPN Client**.



TIPI DI VPN

LO SAI CHE

RADIUS (*Remote Authentication Dial In User Service*) è un protocollo AAA molto diffuso, standardizzato da IETF, che si basa sul modello Client/Server. IETF ha standardizzato un secondo protocollo AAA, DIAMETER, di tipo peer-to-peer.

Ci sono due componenti indispensabili per realizzare un accesso remoto VPN.
La prima è un server di accesso alla rete, ovvero un **NAS** (*Network Access Server*, colloquialmente *Nazz*).
Un NAS può essere un server dedicato oppure un'applicazione software in esecuzione su un server condiviso. Attraverso di esso, un utente si connette a Internet al fine di utilizzare una VPN. Il NAS richiede all'utente di fornire credenziali valide per accedere alla VPN. Per autenticare le credenziali dell'utente, il NAS utilizza il proprio processo di autenticazione o, in alternativa, si avvale di un server di autenticazione separato in esecuzione sulla rete, come per esempio un **Server AAA**.
L'acronimo indica i tre compiti: per ogni connessione VPN, il Server AAA conferma chi sei (*authentication*), identifica ciò a cui ti è permesso accedere tramite la connessione (*authorization*) e tiene traccia di ciò che fai mentre sei loggato (*accounting*).

TIPI DI VPN

L'altra componente indispensabile è un **software VPN Client**. La maggior parte dei sistemi operativi oggi sono dotati di software in grado di connettersi alle reti Remote-access VPN, anche se alcune VPN potrebbero richiedere agli utenti di installare un'applicazione specifica. Inoltre è necessario anche un **firewall**, che fornisce una barriera tra la LAN privata e Internet.

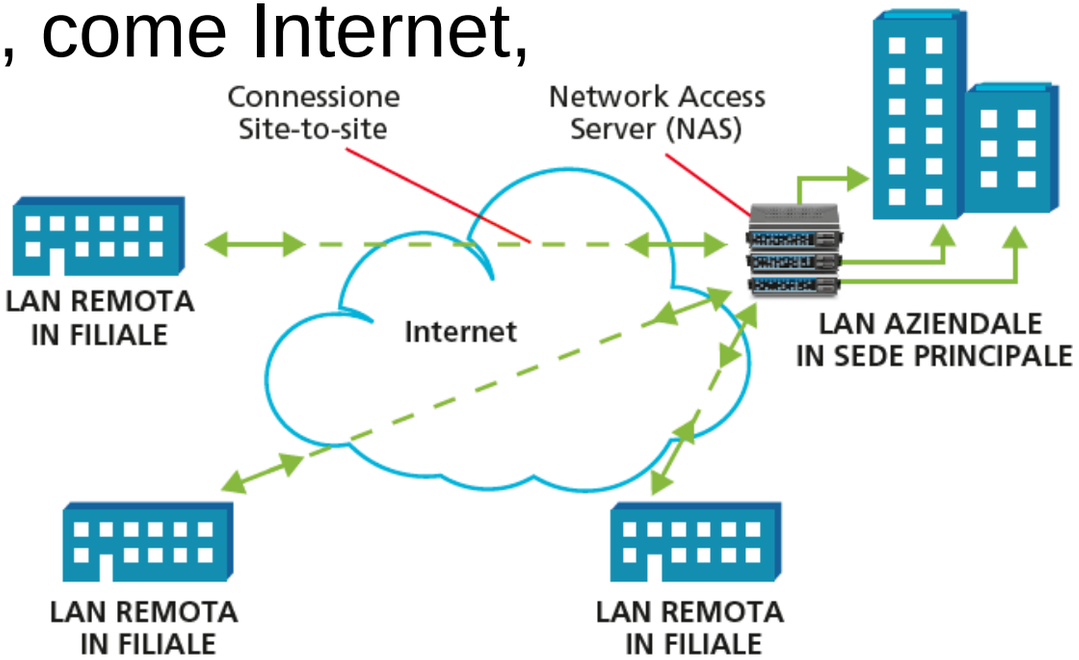
Le grandi aziende, o le aziende con personale IT esperto, in genere scelgono di acquistare, implementare e gestire in proprio la VPN ad accesso remoto. Viceversa, le imprese possono anche scegliere di esternalizzare (*outsourcing*) i propri servizi di accesso remoto VPN tramite un **provider di servizi enterprise** (ESP, *Enterprise Service Provider*). L'ESP configura un NAS per il business aziendale e ne garantisce il funzionamento.

Una **Remote-access VPN** è adatta per i singoli dipendenti/utenti o per aziende con filiali costituite da piccoli uffici.

In caso di aziende con filiali grandi, con centinaia di dipendenti occorre affidarsi a un altro tipo di VPN, utilizzate per mantenere le aziende collegate LAN-to-LAN.

TIPI DI VPN

Site-to-site VPN: permette di stabilire connessioni sicure attraverso una rete pubblica, come Internet, ad aziende con tante sedi. Realizzata come **Intranet-based** oppure **Extranet-based**.



TIPI DI VPN

Ci sono due tipi di Site-to-site VPN:

- **Intranet-based**: se una società desidera unire le reti delle sedi remote in un'unica rete privata, può creare una VPN *intranet* per collegare ogni LAN separata in una singola rete WAN;
- **Extranet-based**: se una società ha un rapporto stretto con un'altra società (per esempio un partner fornitore o un'azienda cliente), è possibile costruire una VPN *extranet* che collega le LAN di queste imprese. La VPN extranet permette alle aziende di lavorare insieme in un ambiente sicuro, condividendo le risorse e senza l'accesso preventivo alla propria intranet.

Anche se lo scopo di una Site-to-site VPN è diverso da quello di una Remote-access VPN, i due tipi di VPN potrebbero utilizzare parte dello stesso software e gli stessi dispositivi. Idealmente, però, una Site-to-site VPN dovrebbe eliminare la necessità di eseguire il software VPN Client come se l'host fosse su una Remote-access VPN.

LESSICO

La rete **intranet** è una rete interna aziendale (LAN), che impiega le tecnologie e i protocolli di Internet (modello TCP/IP).

La rete **extranet** impiega le tecnologie e i protocolli di Internet per collegare un'azienda ai propri fornitori o clienti o ad aziende consociate.