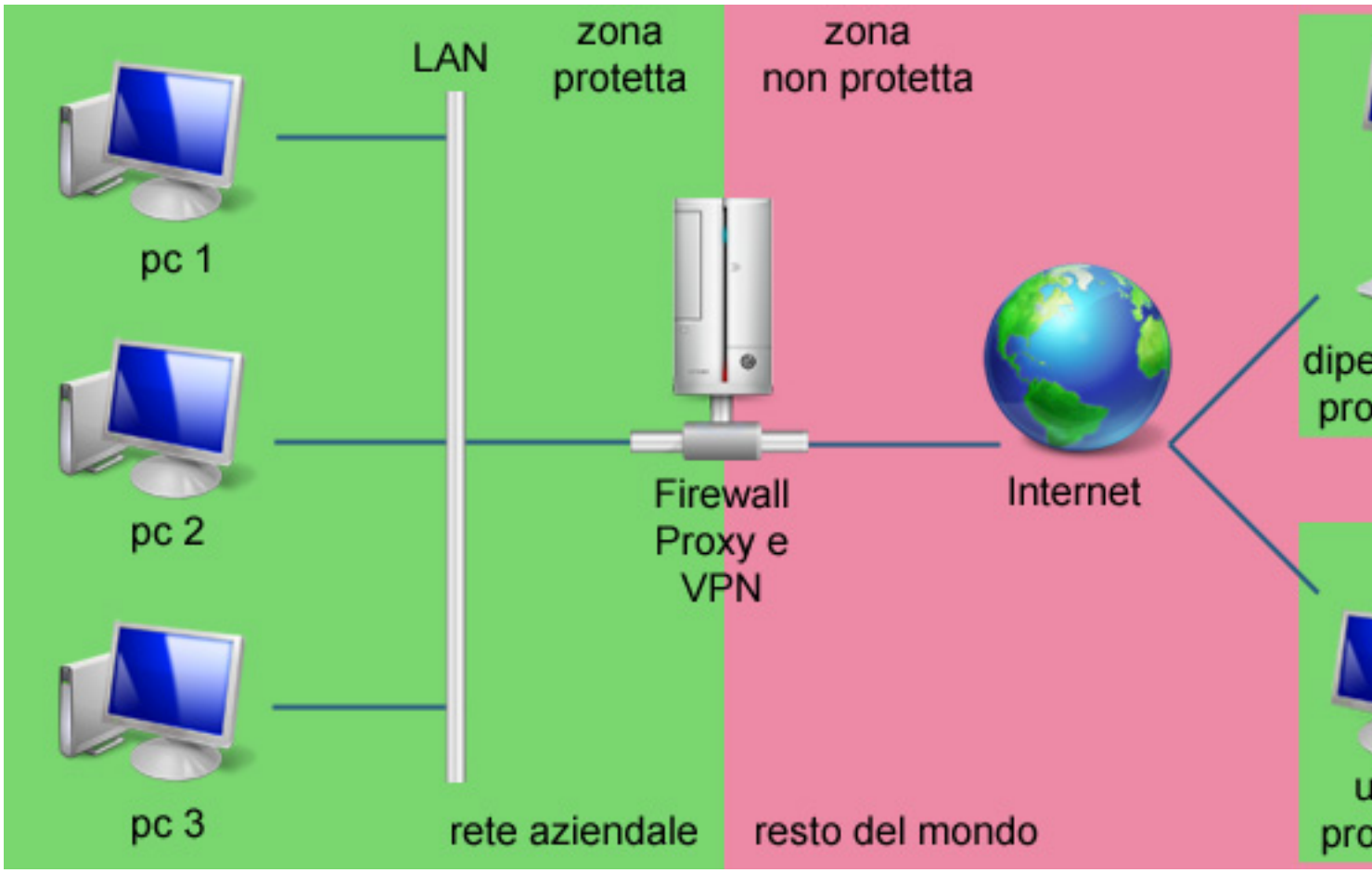
L' accesso sicuro da e verso Internet

L' accesso ad Internet è ormai una necessità quotidiana per la maggior parte delle imprese. Per garantire la miglior sicurezza mettiamo in opera **Firewall** sul traffico in ingresso ed in uscita per controllare ed impedire accessi non autorizzati,
Proxy
per ottimizzare, filtrare ed autorizzare la navigazione su Internet e
VPN Reti Private Virtuali
per il collegamento
sicuro e controllato
di più uffici remoti o per il collegamento di un dipendente in trasferta con la rete informatica del proprio ufficio.



Firewall

In Informatica, nell'ambito delle reti di computer, un firewall (termine inglese dal significato originario di parete refrattaria, muro tagliafuoco, muro ignifugo; in italiano anche parafuoco o parafiamma) è un componente passivo di difesa perimetrale che può anche svolgere funzioni di collegamento tra due o più tronconi di rete. Usualmente la rete viene divisa in due sottoreti: una, detta esterna, comprende l'intera Internet mentre l'altra interna, detta LAN (Local Area Network), comprende una sezione più o meno grande di un insieme di computer locali. In alcuni casi è possibile che si crei l'esigenza di creare una terza sottorete detta DMZ (o zona demilitarizzata) atta a contenere quei sistemi che devono essere isolati dalla rete interna ma devono comunque essere protetti dal firewall.

Vantaggi di avere un Firewall

La funzionalità principale in sostanza è quella di creare un filtro sulle connessioni entranti ed uscenti, in questo modo il dispositivo innalza il livello di sicurezza della rete e permette sia agli utenti interni che a quelli esterni di operare nel massimo della sicurezza. Il firewall agisce sui pacchetti in transito da e per la zona interna potendo eseguire su di essi operazioni di:

- controllo
- modifica
- monitoraggio

Proxy

Un proxy è un programma che si interpone tra un client ed un server, inoltrando le richieste e le risposte dall'uno all'altro. Il client si collega al proxy invece che al server, e gli invia delle richieste. Il proxy a sua volta si collega al server e inoltra la richiesta del client, riceve la risposta e la inoltra al client.

Un caso in cui viene spesso usato un proxy è la navigazione web (denominato proxy HTTP dal nome del protocollo usato).

Per utilizzare un proxy è possibile configurare il client in modo che si colleghi al proxy invece che al server, oppure definire un proxy trasparente; in questo caso, a seconda della configurazione, alcune connessioni (ad esempio quelle HTTP) vengono automaticamente indirizzate al proxy senza che sia necessario configurare un client (quindi l'impostazione rimane attiva anche cambiando client).

Vantaggi di avere un Proxy

- connettività
  per permettere ad una rete privata di accedere all'esterno è possibile configurare un computer in modo che faccia da proxy tra gli altri computer e Internet, in modo da mantenere un unico computer connesso all'esterno, ma permettere a tutti di accedere. In questa situazione, solitamente il proxy viene usato anche come firewall.

- caching
  un proxy può immagazzinare per un certo tempo i risultati delle richieste di un utente, e se un altro utente effettua le stesse richieste può rispondere senza dover consultare il server originale. Collocando il proxy in una posizione "vicina" agli utenti, questo permette un miglioramento delle prestazioni ed una riduzione del consumo di ampiezza di banda.

- monitoraggio
  un proxy può permettere di tenere traccia di tutte le operazioni effettuate (ad esempio, tutte le pagine web visitate), consentendo statistiche ed osservazioni dell'utilizzo della rete.

- controllo
  un proxy può applicare regole definite dall'amministratore di sistema per determinare quali richieste inoltrare e quali rifiutare, oppure limitare l'Ampiezza di banda utilizzata dai client, oppure filtrare le pagine Web in transito, ad esempio bloccando quelle il cui contenuto è ritenuto offensivo in base a determinate regole.

- privacy
  un proxy può garantire un maggiore livello di privacy mascherando il vero indirizzo IP del client in modo che il server non venga a conoscenza di chi ha effettuato la richiesta.

VPN Reti Private Virtuali

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.

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.

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.

Vantaggi delle VPN

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

- Permette la connessione sicura alla propria rete aziendale fra uffici remoti o fra dipendenti in trasferta ed ufficio
- Migliora la sicurezza dove le linee di dati non sono state crittate
- Fornisce una più veloce ROI (tempo di ritorno dell'investimento) rispetto al trasporto tradizionale delle linee WAN

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.

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.

articolo derivato da Wikipedia Firewall
articolo derivato da Wikipedia Proxy
articolo derivato da Wikipedia Virtual Private Network