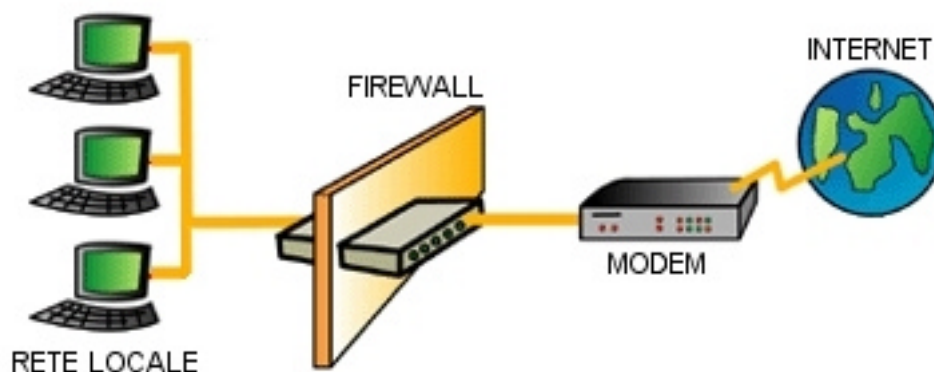


## FIREWALL

Il firewall è una apparecchiatura hardware/software che viene posizionata tra la Vostra rete interna (i Vostri computer) ed internet, ed ha la funzione di “filtrare” tutto il traffico in ingresso ed in uscita.



L'installazione e la configurazione di un firewall permette di controllare dettagliatamente tutto quanto “passa” tra la Vostra rete interna e l'immenso mondo di internet, permettendo di definire e controllare chi, e cosa, può entrare ed uscire.

Tipicamente, dalla Vostra rete interna sarà permesso collegarsi ad internet per scrivere o leggere posta e per navigare su determinati siti internet; sarà invece possibile impostare un filtro per i Vostri dipendenti per fare in modo che non possano collegarsi a siti di dubbio contenuto (siti pornografici, sito con dialer o altro), e sarà altresì possibile vietare l'accesso ad utenti malintenzionati che, da internet, tentino di collegarsi con la Vostra rete interna per carpire o danneggiare i Vostri dati.

➤ **Attraverso l'uso del firewall si ottengono le seguenti funzionalità:**

- **Protezione degli attacchi provenienti da internet alla Vostra rete interna**  
Un computer non protetto appartenente alla Vostra rete interna può “mettere a disposizione” dei malintenzionati tutti i Vostri archivi o servizi. Un malintenzionato potrebbe prendere totale possesso del Vostro computer, e da lì arrivare a tutti i Vostri computer, copiando, danneggiando o cancellando i Vostri dati personali e aziendali
- **Filtro sui siti visitati in uscita**  
E' possibile definire filtri su siti “proibiti”; ad esempio è possibile impedire l'accesso ai siti che contengono la parola “sex”

- **Accesso personalizzato**

Tutti i computer presenti nella Vostra rete possono essere catalogati, in modo da definire politiche di accesso ad internet personalizzate, sui singoli computer oppure “a gruppi” (amministrazione, contabilità, sviluppo...)

- **Server virtuali**

Se avete la necessità di “mettere a disposizione” determinati servizi agli utenti che provengono da Internet (ad esempio potreste mettere a disposizione dei venditori o dei clienti una cartella in cui posizionate i listini o le brochure), potete creare un Virtual Server che sarà “visibile” dall'esterno. Il pc che funge da Virtual Server rimarrà interno alla Vostra rete, e sarà dunque da Voi direttamente gestito pur essendo protetto. L'indirizzo fisico del server interno verrà “mappato e tradotto” per gli utenti internet, che non vedranno direttamente il pc, ma un suo indirizzo assegnato dal firewall in modo trasparente.

- **Controllo schedulato**

Potete definire una schedulazione sulle regole da applicare al firewall: per esempio potete definire che durante gli orari di lavoro non è possibile accedere ai siti che contengono videogiochi, mentre questo può essere permesso durante la pausa pranzo, oppure potete definire che è possibile accedere ai dati pubblicati sul Vostro server solamente durante gli orari di lavoro

- **DNS dinamico**

Quando Vi collegate ad internet, il Vostro provider vi assegna un indirizzo (del tipo 152.28.15.92). Tale indirizzo può cambiare di volta in volta, ad ogni connessione con internet. Attraverso il DNS dinamico, Vi verrà assegnato un nome “fisso” (ad esempio MiaAzienda.virtual.com), che permetterà di collegarvi alla Vostra rete da remoto facendo sempre riferimento allo stesso “nome”

- **PC in DMZ**

E' possibile lasciare un pc completamente accessibile ad internet (computer-civetta, oppure un pc “a disposizione” degli utenti internet)

- **LOG**

Il firewall genera un log del flusso di dati in passaggio: quali tentativi di intrusione alla Vostra rete interna sono stati bloccati, quali accessi verso siti internet non ammessi sono stati impediti, e da quale pc si è originato il tentativo di accesso. I files di log verranno inviati automaticamente via mail per permettere di prendere le eventuali contromisure.

Una volta installato e configurato, il firewall funziona automaticamente, senza la necessità di intervento da parte Vostra.

➤ **Tra le altre funzionalità offerte dal firewall ci sono:**

- **Switch**

Il firewall è anche uno switch 4 porte autosense 10/100Mb

- **Condivisione dell'accesso ad internet**

Con una singola connessione ad internet attraverso un normale provider (Alice, Libero, Ica-net o altri) si fornisce l'accesso a tutti i computer autorizzati presenti nella rete

- **(opzionale) VPN**

E' possibile collegare sedi remote, oppure singoli computer, alla rete interna, in totale sicurezza. I computer remoti entreranno a far parte della rete come se fossero fisicamente connessi alla rete interna, e dunque potranno accedere ai dati, utilizzare le stampanti eccetera

➤ **I Nostri servizi:**

- Analisi della attuale configurazione di rete
- Installazione e configurazione del firewall
- Modifica/aggiornamento delle regole aziendali di accesso ad internet
- Analisi periodica dei log, e definizione delle eventuali contromisure in caso di attacco
- Amministrazione e diagnostica, in locale o remota, del funzionamento del firewall
- Aggiornamento periodico del firmware e della logica del firewall