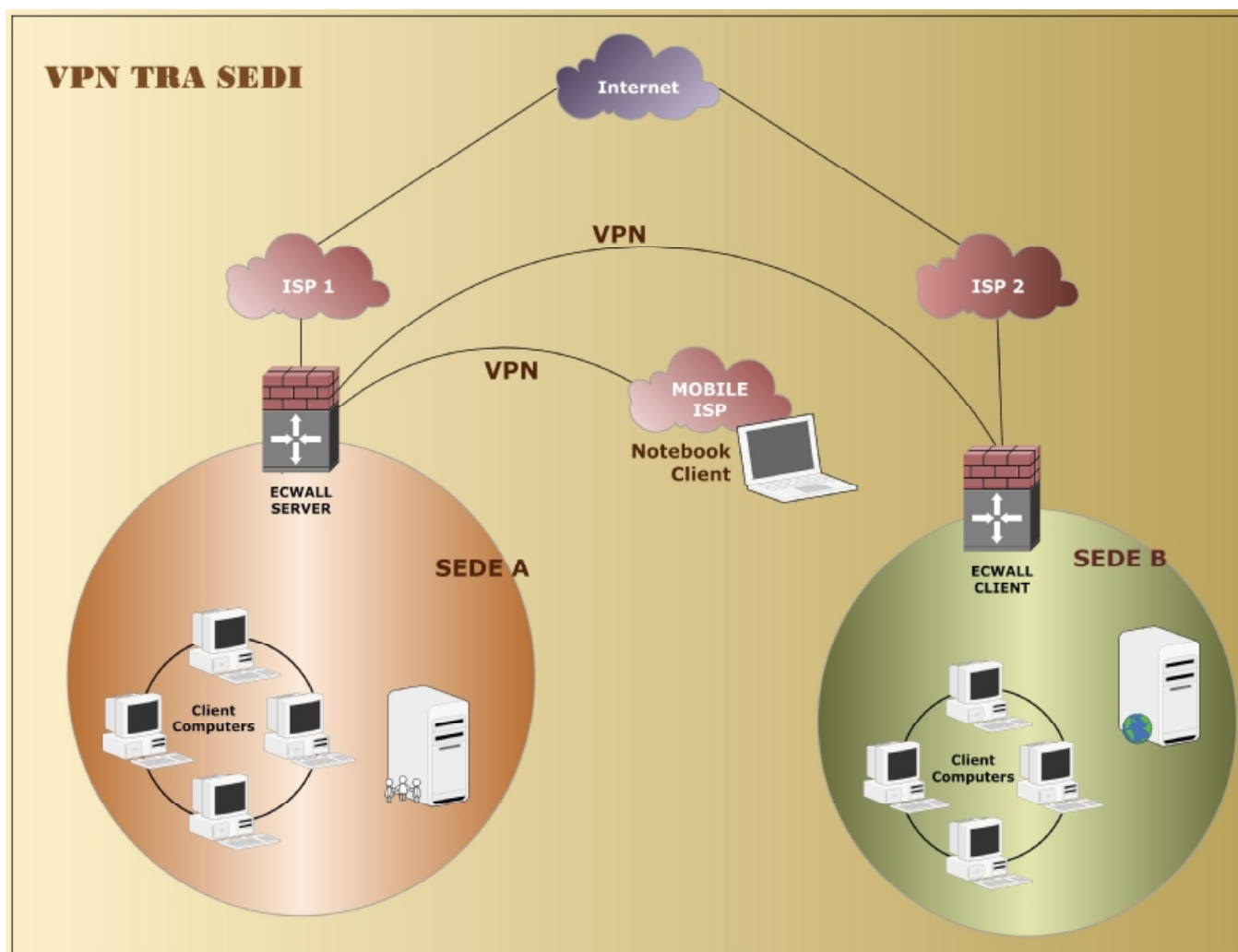


## 1 Caratteristiche generali

Nati dall'esperienza maturata nell'ambito della sicurezza informatica, gli **ECWALL** di e-creation rispondono in modo brillante alle principali esigenze di connettività delle aziende: sicurezza, affidabilità, duttilità, costi di start-up limitati, canone di noleggio e assistenza.



Gli **ECWALL** sono dei mini-pc con sistema operativo linux embedded in grado di svolgere quelle funzioni che la maggior parte delle aziende oggi giorno sente come essenziali: firewall avanzato, proxy, vpn server.

Alcune di queste funzionalità sono comprese anche nei comuni prodotti che passano sotto la categoria di firewall hardware. Prodotti che portano la connettività internet delle aziende "alla

portata di tutti" poiché con pochi click si è spesso in grado di dotare un'azienda degli strumenti base necessari per poter godere delle funzionalità offerte dalla banda larga.

L'esperienza con i firewall hardware porta però ad una considerazione fondamentale; una considerazione a dire il vero ovvia, tanto ovvia, però, da essere spesso assolutamente taciuta o dimenticata: **nessun firewall o IDS (Intrusion Detection System) potrà mai proteggere un sistema mal configurato (o in generale una applicazione "bacata")**.

Un firewall hardware mal configurato, o configurato da personale inesperto, può rivelarsi assolutamente inutile, lasciando la rete aziendale in balia di tutti i pericoli che arrivano dalla rete internet: intrusioni da parte di hacker, attacchi DoS (**denial of service**, con i quali si cerca di portare il funzionamento di un sistema informatico che fornisce un servizio, ad esempio un sito web, al limite delle prestazioni), infezioni da parte di virus o di worm, o quant'altro. È per questo che e-creation ha pensato a **ECWALL**, una soluzione che unisce la praticità di installazione e di collocazione di un firewall hardware, all'assistenza di personale qualificato, in grado di identificare correttamente le esigenze di sicurezza di un'azienda.

## 2 ECWALL: versione base

**ECWALL** è disponibile in due versioni: base e pro.

Queste sono le funzionalità disponibili in **ECWALL versione base**:

### ◆ Firewall con SPI.

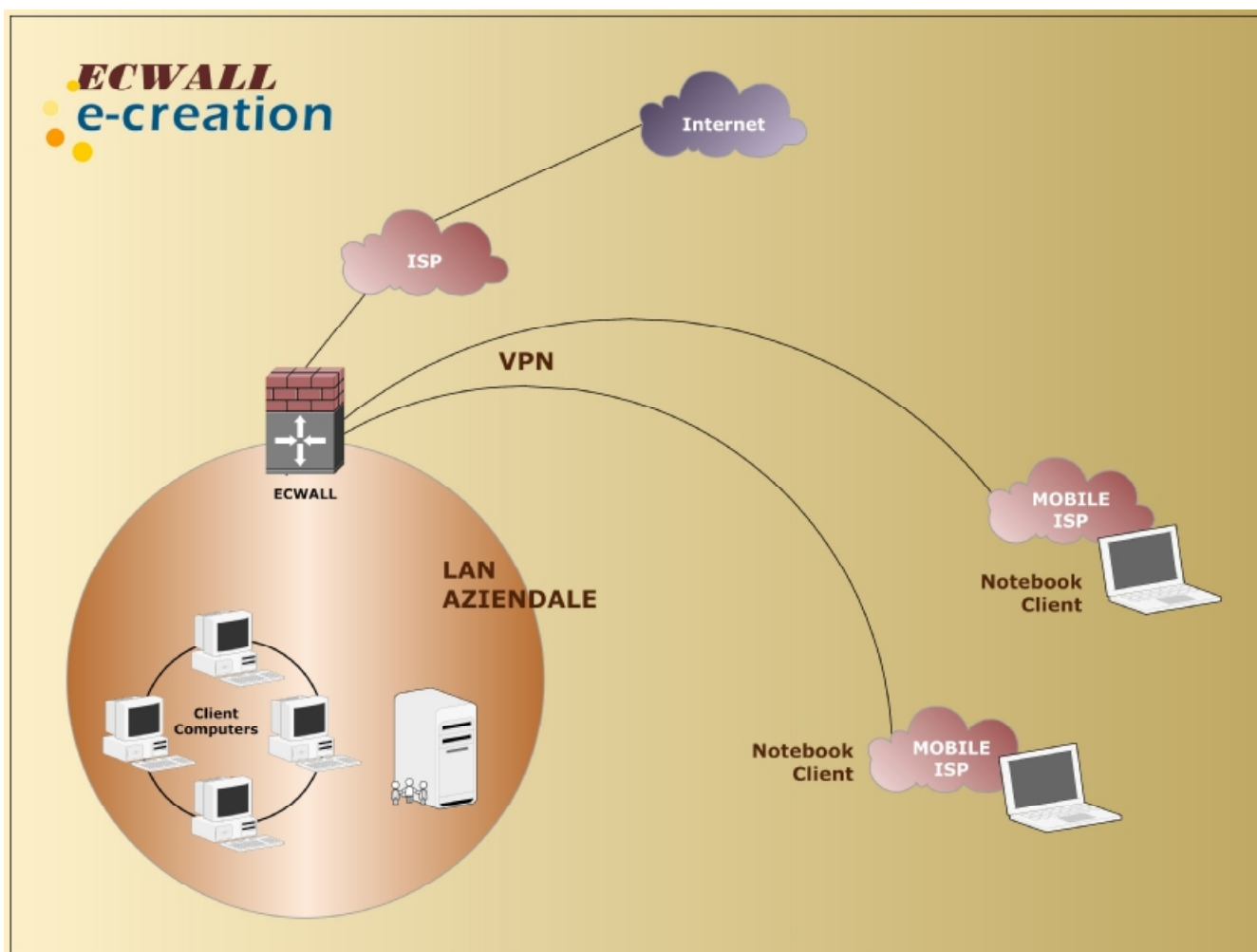
**ECWALL** sfruttando il Netfilter e l'iptables di Linux, può essere configurato per agire da firewall proteggendo la LAN da attacchi e port scan provenienti da internet. **ECWALL** può operare sia da Packet Filter, cioè filtrare basandosi su delle condizioni (regole) imposte sugli header dei pacchetti (ad esempio accettare o rifiutare connessioni in base all'indirizzo IP di provenienza o di destinazione, al protocollo e alla porta di comunicazione, all'interfaccia di rete utilizzata, all'indirizzo fisico – MAC address – della scheda di rete, ed altro ancora), sia da Stateful Packet Inspection (SPI) cioè filtrando i pacchetti basandosi sulla loro correlazione con connessioni già attive o altri pacchetti già transitati (ad esempio accettare o rifiutare i pacchetti che richiedono di stabilire una connessione nuova, che appartengono ad una connessione già esistente, ed altro ancora).

I criteri di packet filter possono operare contemporaneamente a quelli SPI rendendo molto flessibili le regole del firewall. La corretta impostazione di queste regole permette di garantire un isolamento della rete aziendale dai pericoli provenienti dalla rete internet. Allo stesso modo permette di poter interagire con tutti i servizi che sono necessari per la produttività aziendale.

### ◆ VPN Host-to-LAN e LAN-to-LAN

La crescente mobilità degli utenti di un'organizzazione, unita alla necessità di questi ultimi di poter accedere alla propria LAN come se vi fossero fisicamente connessi anche quando sono distanti dalla sede, ha portato allo sviluppo delle VPN **host to LAN** (VPN Roadwarrior). Questo tipo di collegamento consiste in un tunnel criptato che, attraverso Internet, connette il client esterno al server VPN presente su **ECWALL**. Dentro tale tunnel si instaura un collegamento point to point sulle cui due estremità vengono assegnati indirizzi IP appartenenti all'organizzazione. Così facendo, il client remoto appare interno nei confronti del firewall e pertanto potrà dialogare con gli host della LAN senza il rischio di essere filtrato.

Allo stesso modo, la presenza in un'organizzazione di sedi distaccate, unita al costo elevato delle linee di comunicazione dedicate ha portato alla necessità di usare Internet come mezzo per lo scambio di dati. D'altra parte, la rete pubblica, essendo aperta ed insicura, non fornisce garanzie di confidenzialità per i dati che la attraversano. Una VPN lan-to-lan (o site-to-site) è un tunnel crittografato che unisce due LAN (geograficamente distanti) attraverso Internet. Concettualmente si potrebbe pensare alla VPN come ad un cavo virtuale che unisce due LAN: non importa quanti router sia necessario attraversare su Internet, le due LAN appariranno separate da un unico segmento di rete.



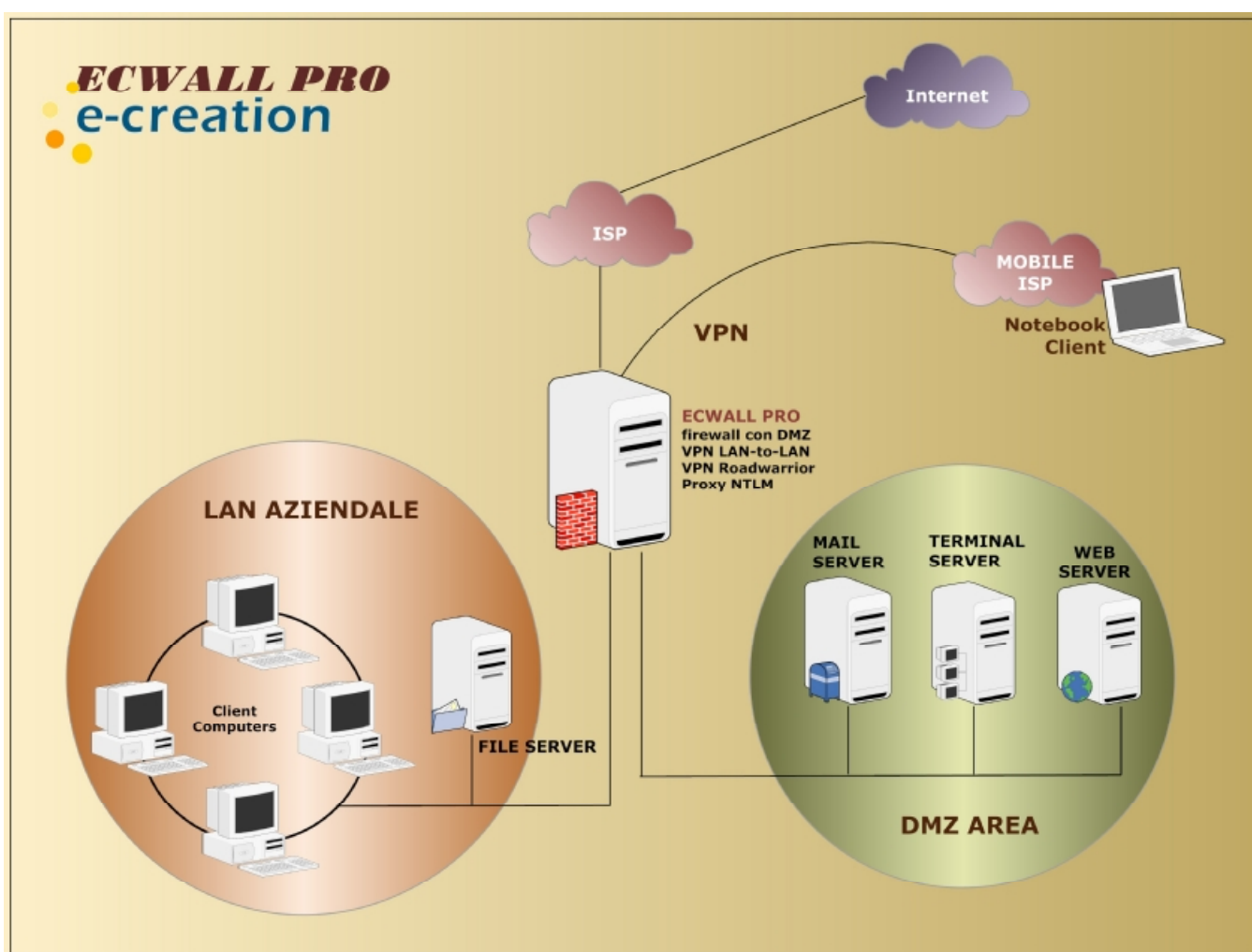
ECWALL utilizza il supporto di OpenVPN per le VPN di tipo Host-to-LAN. E LAN-to-LAN: OpenVPN è un sistema molto forte dal punto di vista della sicurezza. Oltre ad utilizzare gli algoritmi crittografici più robusti messi a disposizione da OpenSSL, è stato scritto con

un'attenzione particolare, nel tentativo di evitare quanto più è possibile falle di sicurezza dovute ad errori di programmazione.

### 3 ECWALL: versione pro

In **ECWALL versione pro** sono presenti tutte le funzionalità di **ECWALL versione base**.

In aggiunta la **versione pro** va incontro alle esigenze delle aziende più strutturate, che cercano una valida difesa per gli utenti della rete ma anche per un'ampia gamma di servizi offerti: server web, server ftp, server di posta, terminal server e altro ancora.



#### ◆ Firewall con SPI e DMZ.

In questa versione **ECWALL** è già configurato per la gestione di una rete privata e una DMZ (De-Militarized Zone, Zona De-Militarizzata), sia a livello di script di configurazione

per il firewall, che a livello hardware (per gestire correttamente un'area DMZ sono infatti necessarie tre schede di rete invece delle due usuali).

A chi serve una firewall con SPI e DMZ? A tutte quelle aziende particolarmente strutturate che hanno bisogno di rendere disponibile su internet una gamma di servizi, cioè hanno bisogno di gestire sia una rete pubblica che una rete privata: una rete pubblica è quel tratto di rete visibile da tutto il "mondo". In questa rete possono essere situati un web server, un mail server, un ftp server, un terminal server, ecc...

La rete pubblica in gergo tecnico viene appunto chiamata DMZ ed è un tratto di rete in cui il firewall permette l'accesso a tutti. La rete privata è una rete in cui i computer possono accedere a internet ma non vengono visti dal "mondo".