LA SICUREZZA IN PRATICA

FIREWALL, ANTIVIRUS & NETWORK ASSET

Perché hanno colpito la mia Azienda? Cosa posso fare per tenere il mio lavoro al sicuro?

Internet è un potente strumento di comunicazione con un'utenza stimata di 300 milioni di utenti; ognuno di questi utenti può rappresentare un potenziale pericolo per la Vostra attività.

La diffusione di virus, attacchi informatici, violazioni della privacy etc., sono spesso argomento dei media internazionali; i rischi derivanti dall'utilizzo e dalla trasmissione di informazioni su Internet (e talvolta all'interno della propria rete locale), sono enormi.

Malgrado questo e gli obblighi previsti dalla legge italiana e comunitaria, gran parte delle aziende affrontano queste problematiche con superficialità o non le affrontano affatto; oggi più che mai le informazioni sulle problematiche della sicurezza si diffondono attraverso Internet e nella comunità degli hacker; software ed hardware, se non adeguatamente e velocemente aggiornati diventano obsoleti in breve tempo.

Assicurare l'inviolabilità della propria rete o delle proprie comunicazioni non è un compito semplice; per la natura intrinseca di molti software, non esiste un sistema che sia inviolabile o un software che sia sicuramente immune da problemi.

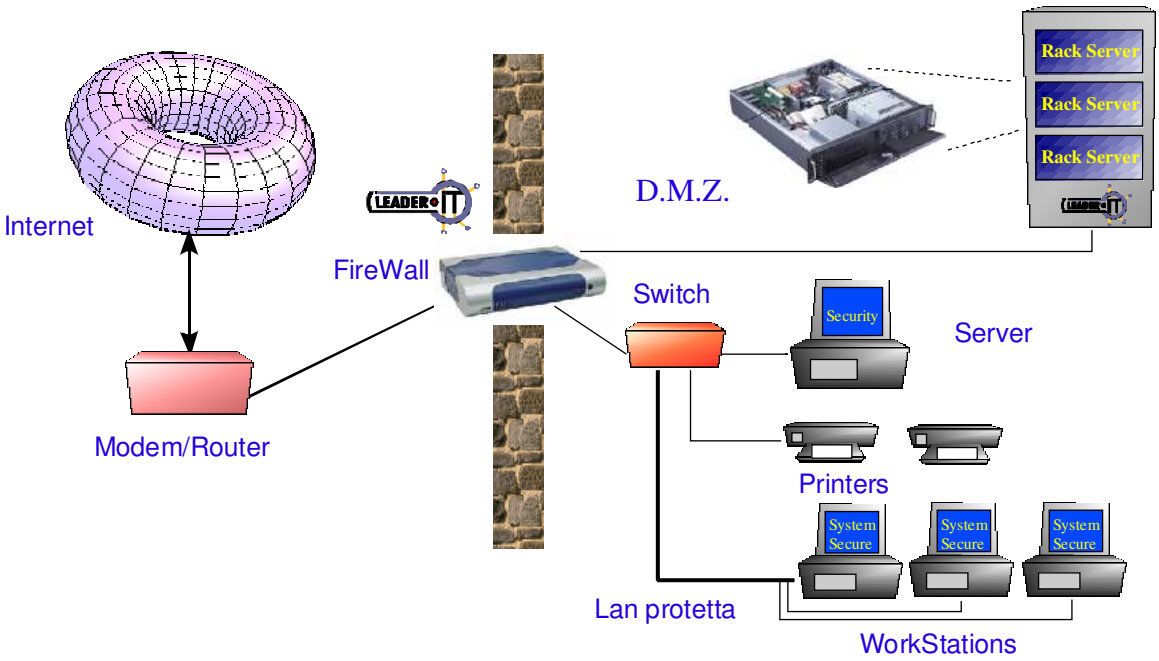
Negli ultimi tempi il continuo rilascio di patch software per problemi di sicurezza di numerosi sistemi operativi (Windows NT, 2000, Linux ed altri), indica che il "percorso" di protezione dei dati della propria attività non è solo un fatto che riguarda le grandi Aziende, ma anche la piccola e media impresa.

Un sistema considerato sicuro oggi, può diventare assolutamente insicuro domani!!

Pensare di non essere un bersaglio interessante per un attacco è un grave errore! Anche se la Vostra Azienda non si occupa di e-Commerce o non effettua transazioni commerciali di nessun tipo via Internet, le informazioni relative ad esempio alla Vostra contabilità, lista e dati sulla Vostra clientela potrebbero avere un grande valore per qualcuno (ad esempio un vostro concorrente).

Per questo motivo ogni specifica realtà deve essere analizzata attentamente per valutare i rischi, gli investimenti opportuni in relazione all'importanza delle risorse e dei dati da proteggere e gli strumenti necessari per raggiungere questi obiettivi.

Per questo crediamo che per proteggere i Vostri investimenti non dovete solo installare un firewall, ma dovete pensare ad una infrastruttura sicura che coinvolge gli Utenti forse più degli apparati di rete.



IL FIREWALL LEADER.IT

La nostra soluzione firewall, frutto di esperienza quinquennale, si articola nei seguenti servizi:

- protezione rete interna
- DMZ con ip privati o pubblici
- servizi di tunnelling pptp (linux-win)
- servizi di tunnelling CIPE (linux-linux e linux-win2k)
- servizi di tunnelling OpenSSH (seishell win2k-linux) per soluzioni tipo “Application Tunnel”
- smtp forwarder
- dns pubblico (yaku-ns)
- servizi NAT per rete interna
- servizi DHCP per rete interna
- servizio di backup-restore
- monitoraggio real-time del traffico

La rete interna viene protetta tramite politiche restrittive di accesso basate su iptables e iproute2, ciò consente di discriminare le regole di transito dei pacchetti e di utilizzo dei servizi.

Le politiche di accesso ai servizi pubblici sono limitate ai servizi posti a dimora nella DMZ e sono limitabili a loro volta tramite regole ad-hoc sul filtraggio dei pacchetti in transito.

Per i servizi PPTP (PointoPoint Tunneling Protocol) che permettono l'accesso alla rete delle macchine windows tramite microsoft VPN viene utilizzato il relativo server per linux (PopTOP), ed è in aggiornamento la distribuzione per l'utilizzo di IPSEC onde fornire l'accesso tramite il protocollo già installato sulle macchine win2k.

In caso di collegamenti attraverso internet di più sedi della stessa ditta utilizziamo il protocollo CIPE (Crypto IP Protocol Encapsulation di Olaf Titz) che fornisce alte caratteristiche di performance anche con dispositivi hardware di basso calibro. Il suddetto protocollo permette la gestione di tunnel nel numero di 99 per nodo in maniera del tutto trasparente al resto del sistema.

Per quello che riguarda la gestione dei classici Application-Tunnel la scelta si è orientata verso l'utilizzo di OpenSSH sul lato server e l'accoppiata SeiShell+Plink dal lato client, in questo modo si permette di attivare un tunnel senza installare nessun software sul lato client (win*).

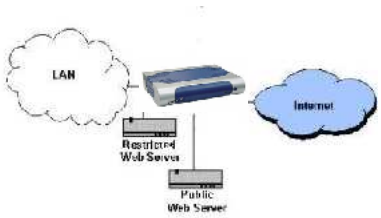
Questo tipo di soluzione si utilizza generalmente in presenza di servizi che non necessitano l'accesso alla rete in generale.

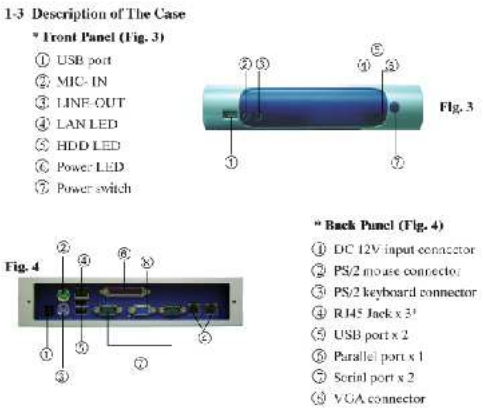
Onde evitare l'accesso dall'esterno alla rete interna, per il trasporto dei servizi di posta viene utilizzata una configurazione minimale di Qmail che si occupa del trasporto verso il destinatario (in-out) di eventuali messaggi di posta elettronica bloccando eventuali tentativi di relay attraverso il nostro server.

Nel caso di dns pubblico si utilizza yaku-ns che garantisce da un lato la semplicità di configurazione e dall'altro la sicurezza essendo totalmente chrooted.

Vengono inoltre forniti i seguenti servizi:

- servizi di NAT alla rete interna discriminando le regole in base agli IP di chiamata e le porte-IP di destinazione.
- servizi di DHCP statico e dinamico alle macchine della rete interna. Questa soluzione permette di settare delle regole specifiche per le macchine con ip assegnato staticamente rispetto alle altre in maniera semplice e immediata.
- servizi di backup in remoto delle configurazioni e installazione automatica di patch di sicurezza tramite il nostro server senza bisogno di interazione da parte del cliente.




1-3 Description of The Case

* Front Panel (Fig. 3)

① USB port
② MIC- IN
③ LINE-OUT
④ LAN LED
⑤ HDD LED
⑥ Power LED
⑦ Power switch

Fig. 3

Fig. 4

* Back Panel (Fig. 4)

① DC 12V input connector
② PS/2 mouse connector
③ PS/2 keyboard connector
④ RJ45 Jack x 1
⑤ USB port x 2
⑥ Parallel port x 1
⑦ Serial port x 2
⑧ VGA connector

Versione Rack 19”
o
compatta