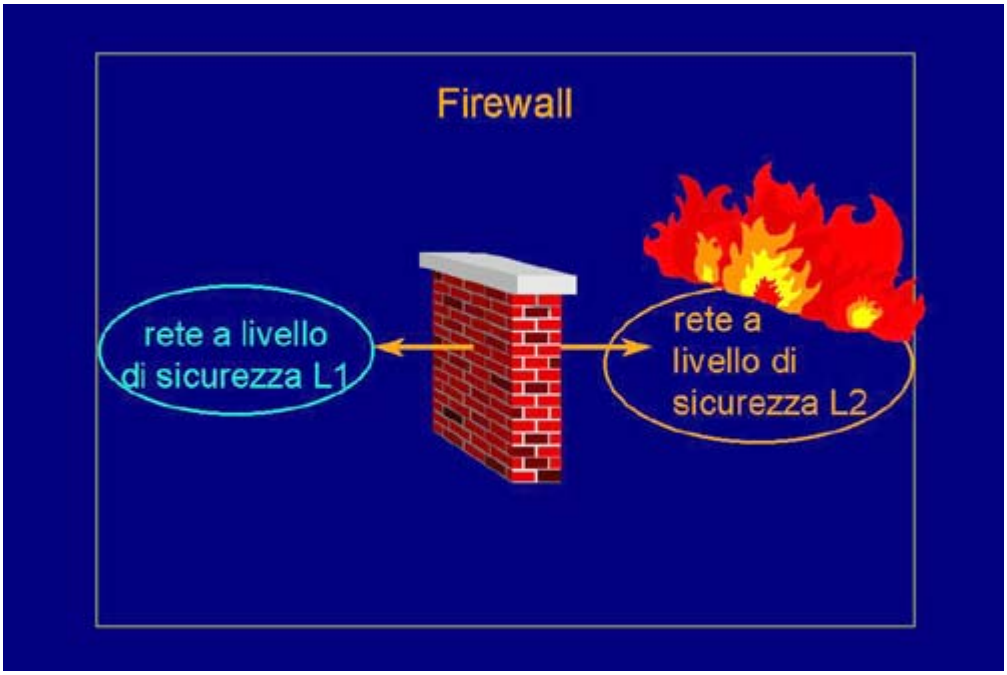
Autenticazione ed integrità dei dati
Firewall



Per proteggere una rete dagli attacchi provenienti dall'esterno si utilizza normalmente un sistema denominato Firewall. Firewall è un termine inglese che indica i muretti di mattoni che, tipicamente, vengono frapposti fra le case americane. Poiché le case americane sono normalmente costruite in legno, si vuole evitare che, se una casa prende fuoco, quindi c'è un incendio, questo si trasferisca automaticamente anche alla casa affianco. Perciò gli americani fanno le case in legno e i muretti di divisione tra una casa e l'altra in mattoni. Questo concetto è stato esteso anche alla sicurezza informatica: ossia nell'ipotesi che esista una rete con un livello di sicurezza L1 e una rete con un altro livello di sicurezza L2, inferiore, quindi più facilmente attaccabile, più facilmente bruciabile e che quindi può essere attaccata più facilmente, il firewall consiste in una sorta di muretto informatico che deve evitare che il fuoco si propaghi. Il firewall deve permettere la comunicazione fra le due reti solo, ed esclusivamente, se in quella esterna non c'è il fuoco, mentre deve bloccare automaticamente la comunicazione in caso di tentativi di attacco.

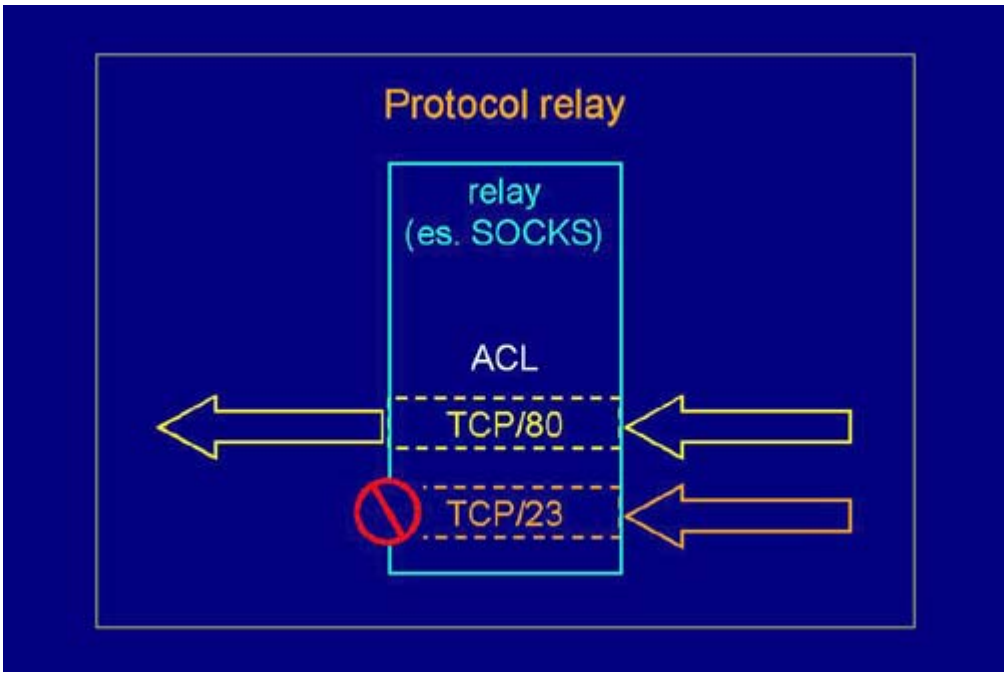
I tre comandamenti dei firewall

Esistono tre principi fondamentali per costruire un buon firewall. Il primo principio dice che il firewall deve essere l'unico punto di contatto tra le due reti a diverso livello di sicurezza. Questo è un punto fondamentale. Molto spesso capita che nelle aziende, nelle organizzazioni, esista un firewall che protegge il collegamento principale fra la rete aziendale e Internet, ma poi esistono dei collegamenti secondari che non sono protetti; esistono, ad esempio, dei modem collocati direttamente negli uffici per fare funzioni ausiliarie, a volte anche soltanto per comodità degli utenti. Questa è una cosa assolutamente sbagliata e contraria a tutti i principi. Equivale ad aver blindato la porta di casa e aver lasciato una semplice zanzariera sul giardino: è chiaro che i ladri tenteranno di entrare non dalla porta più robusta, ma da quella più debole. Quindi si ribadisce il concetto: il firewall deve essere l'unico punto di contatto tra la rete da proteggere e la rete esterna. Un secondo principio inderogabile dice che soltanto il traffico autorizzato può attraversare il firewall. Si noti che ho messo autorizzato fra virgolette, per evidenziare il fatto che nel caso in cui manchi una politica di autorizzazione, ossia non sia stato definito quali sono i tipi di pacchetti, i tipi di protocolli, le operazioni lecite tra la rete interna e la rete esterna, non è possibile creare un buon firewall. Come spesso capita, ubbidire alle direttive che arrivano dall'alto, che dicono: comprate un firewall perché in questo modo avremmo fatto sicurezza, non aiuta assolutamente, anzi, genera confusione se prima non è stata fatta una analisi di quali sono i requisiti di sicurezza, quindi non sono stati definiti quali sono i tipi di traffico autorizzati ad attraversare il firewall. Infine, il terzo punto dice che un firewall deve essere un sistema sicuro esso stesso. Quindi, deve essere implementato tramite una serie di sistemi protetti, dei sistemi che sono diversi dai normali router,o nodi di elaborazione, nelle configurazioni standard, perché queste configurazioni standard sono normalmente attaccabili e, ovviamente, costruire un castello con dei massi che si sbriciolano è una pessima idea.

Packet filter

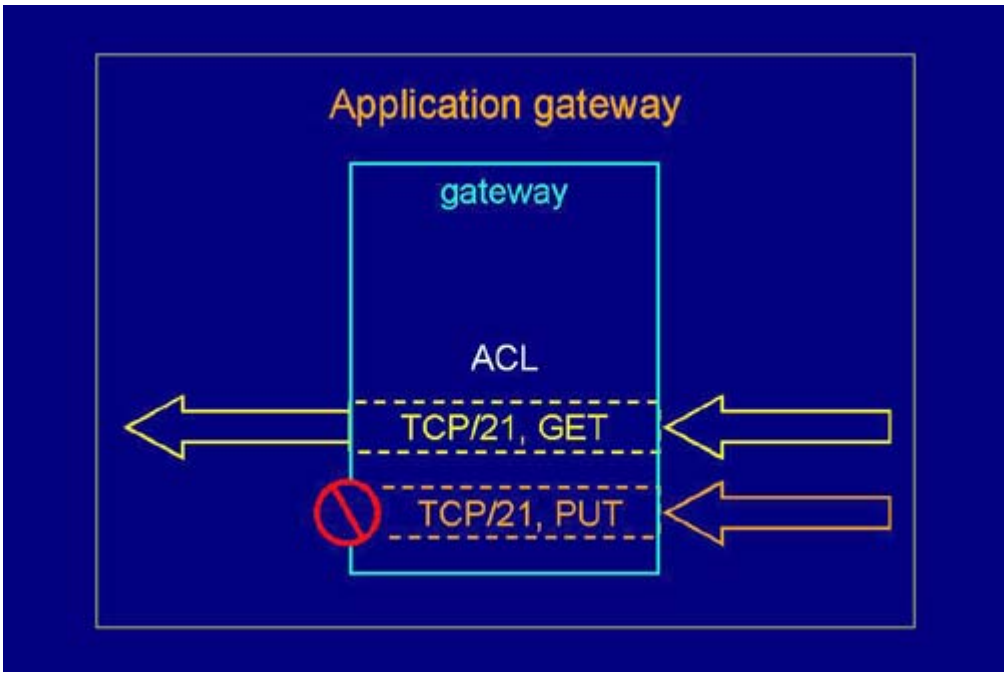
Esaminiamo quindi i principali tipi di componenti che vengono utilizzati per creare il sistema firewall. Il primo tipo di componente che esaminiamo è un cosiddetto packet filter. Il packet filter è una sorta di setaccio che ha il compito di scremare i pacchetti, ossia di buttare via, non lasciar transitare, i pacchetti che hanno delle caratteristiche sconvenienti, non aderenti la nostra politica di sicurezza. Si parla di packet filter quando si vanno ad esaminare gli indirizzi di rete, ad esempio l'indirizzo sorgente e l'indirizzo destinazione, o quando si vanno ad esaminare i protocolli e le porte, ossia quando, in generale, si effettua un filtraggio a livello 3 o 4, eventualmente anche a livello 2. Un packet filter può essere implementato tramite apparecchiature hardware, ad esempio un router sulle quali siano state attivate le ACL (liste di controllo degli accessi), oppure può essere realizzato un software, tramite un gateway su un nodo di elaborazione dotato, ad esempio, di due interfacce di rete. Il packet filter è un componente molto utilizzato all'interno dei firewall, ma deve essere molto chiaro che, trattandosi di un controllo effettuato a livello 3 o 4, si tratta di un controllo poco raffinato. Quindi, il compito di un packet filter è fare un filtro a grana grossa, scremare il grosso dei pacchetti, toglierci dai piedi gli attacchi più banali. Ben difficilmente un packet filter potrà essere in grado di andare ad identificare gli utenti, o le applicazioni, o i comandi, che noi vogliamo far passare o controllare attraverso il firewall.

Protocol relay



Un secondo componente talvolta usato nella creazione di un sistema firewall è il protocol relay. Il protocol relay è tipicamente un software dotato di una lista di controllo degli accessi basata sui livelli tre e quattro, in particolare sul livello 4. Ad esempio, supponiamo che arrivi una richiesta di collegamento destinata ad un nodo Web esterno, ossia un nodo con protocollo TCP porta 80. Se l'ACL prevede la possibilità per gli utenti interni di collegarsi a Web esterni, questo pacchetto verrà lasciato transitare. Supponiamo però che arrivi un altro tipo di pacchetto, un altro tipo di richiesta di apertura di un canale logico, in questo caso si richiede l'apertura di un canale TCP destinato alla porta 23 di un nodo esterno. Questa è una richiesta per un collegamento in emulazione di terminale secondo il protocollo telnet. Supponendo che la ACL non permetta questo tipo di collegamento: sarà compito del protocol relay impedire il collegamento. Nel caso precedente in cui invece il collegamento era permesso, il compito del protocol relay è quello di accettare l'apertura di questo canale, aprire un altro canale esterno e far transitare automaticamente i dati fra i due canali. Uno dei sistemi più utilizzati per realizzare un protocol relay è il sistema chiamato SOCKS, che tra l'altro è un sistema di public domain.

Application gateway

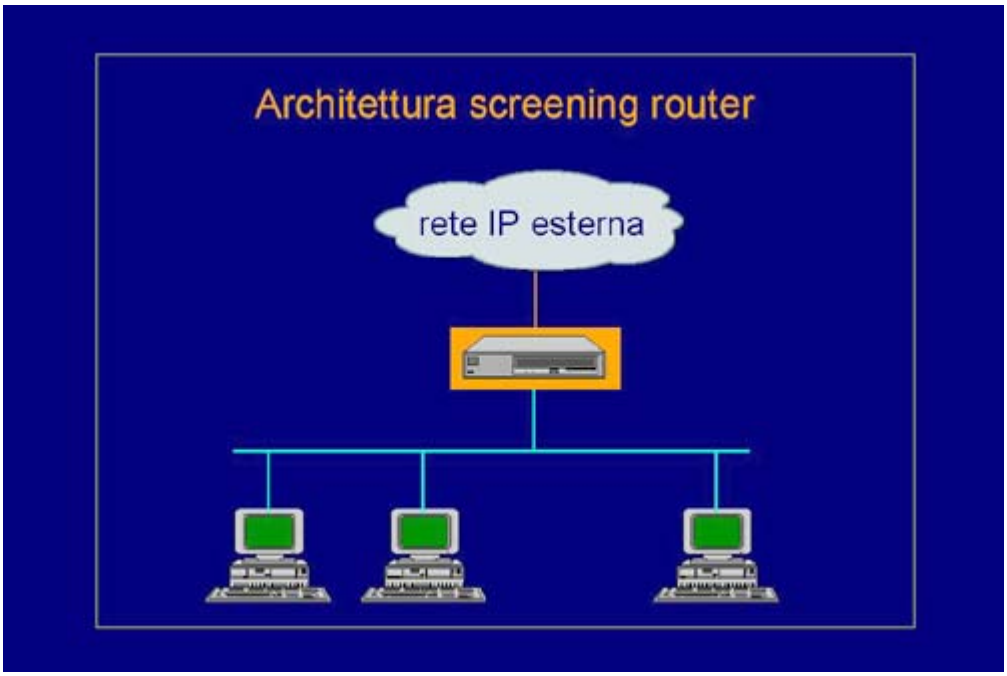


Se vogliamo effettuare dei controlli più raffinati, che non siano solo a livello 3 o a livello 4, dobbiamo salire fino a livello 7. A livello 7 abbiamo a disposizione come sistemi di sicurezza per un firewall i cosiddetti application gateway. Un application gateway è un punto di controllo dotato anch'esso di una ACL, che è però in grado di andare ad effettuare i controlli in base ai dati, o ai comandi applicativi, contenuti nel payload di livello 7. Ad esempio, supponiamo di ricevere una richiesta di transito, attraverso il firewall, relativa all'apertura di un canale TCP, porta 21. Questo ci indica che si tratta di un trasferimento di file secondo il protocollo FTP, ma in particolare l'utente richiede un operazione di GET. Questa operazione di GET è visibile perché noi siamo un application gateway e non siamo un semplice protocol relay o un packet filter. Se l'ACL permette che gli utenti interni prendano dei documenti dall'esterno, lascerà transitare questo comando e quindi l'utente potrà ottenere il documento desiderato. Se però una successiva richiesta evidenzia sempre un trasferimento di dati del protocollo FTP, ma in cui la direzionalità questa volta è quella determinata dal comando PUT, ossia l'utente interno desidera mandare fuori un documento, la nostra ACL potrebbe in questo caso vietare il trasferimento. Si noti che la decisione se far transitare i dati oppure no è stata presa in base al comando a livello applicativo: GET oppure PUT. Questo è un tipo di funzionalità che non poteva in nessun modo essere assolta né da un packet filter, né da un protocol relay.

Bastion host

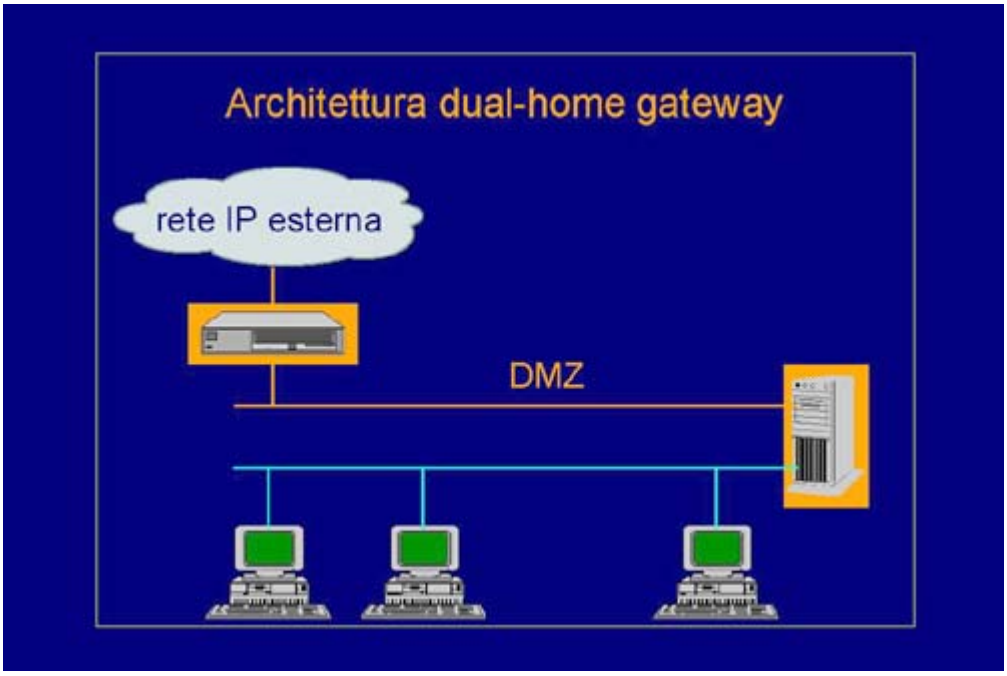
Abbiamo detto che un sistema firewall deve essere dotato di misure di sicurezza interne, esso stesso. In questo senso normalmente si parla di bastion host. Un bastion host è un sistema fortificato, o come talvolta si suol dire blindato, questo significa che si tratta di un normale sistema operativo e di un normale hardware, a cui sono state assegnate funzioni di controllo o di filtraggio. Ad esempio, su questa macchina può essere ospitato un gateway a livello 4 o a livello 7. Ma soprattutto sul bastion host è stata fatta una configurazione particolare. Ad esempio, è stato installato solo ed esclusivamente il software indispensabile per le funzionalità di sicurezza. Analogamente, sono stati installati solo i servizi indispensabili. Bisogna ricordarsi che qualunque processo presente su uno dei nodi che costituiscono il firewall, costituisce un potenziale punto di attacco per gli hacker. Ecco quindi che bisogna cercare di minimizzare il software sia installato sia effettivamente attivo sul firewall, per minimizzare le possibilità di attacco dall'esterno. Inoltre, sul nostro bastion host bisognerà cercare di non avere nessun utente: la cosa ideale sarebbe gestire le macchine che compongono il firewall direttamente dalla loro console. Sono ammesse gestioni remote solo ed esclusivamente attraverso canali molto forti, ben autenticati con crittografia e protezione di integrità dei dati. Siccome non esiste la certezza di aver configurato in modalità effettivamente molto sicura un qualunque nodo di elaborazione, neanche il miglior esperto di sicurezza potrà mai garantirlo, ecco che un sistema fortificato deve fare un log molto estensivo di tutto ciò che capita sul sistema stesso. In questo caso il log ci serve per verificare che effettivamente il sistema non sia stato attaccato. Poiché i log possono diventare molto grossi, è molto importante che sul sistema siano attivati anche dei sistemi di allarme automatico, ossia dei sistemi che controllano i dati contenuti nei file di log e evidenzino automaticamente, lanciando degli allarmi, se il sistema firewall è sotto attacco.

Architettura screening router



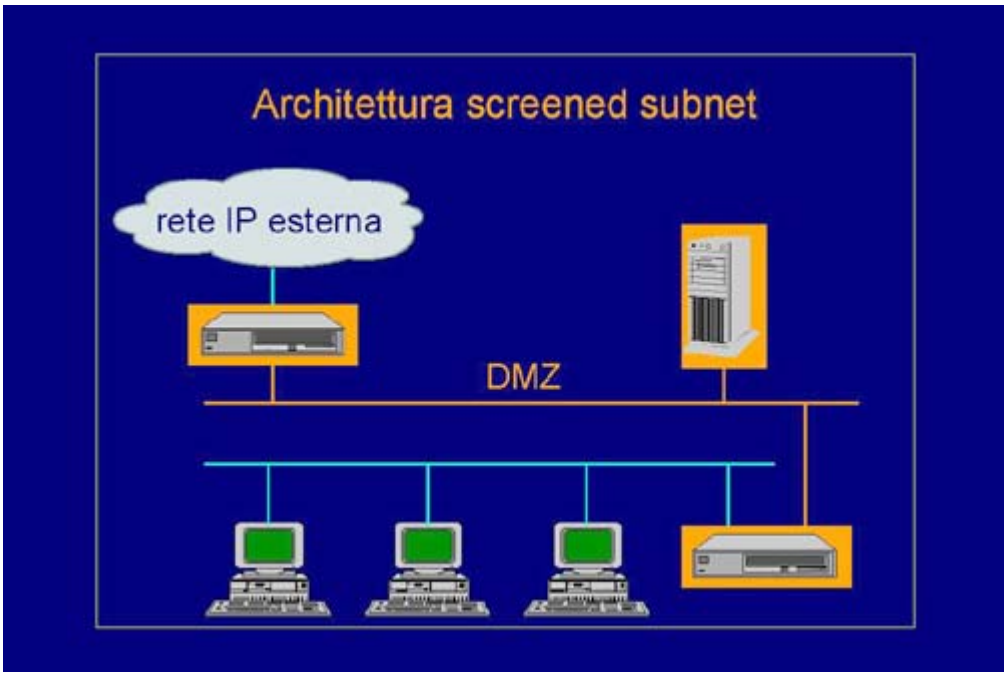
A questo punto siamo in grado di andare a delineare alcune delle tipiche architetture di firewall che vengono utilizzate, componendo insieme i vari sistemi base che abbiamo visto fino adesso. L'architettura cosiddetta screening router è quella che protegge un'intera rete, nei confronti delle reti esterne, solo ed esclusivamente tramite il router. Ossia, il router, che già avrebbe il compito di instradare i pacchetti tra la nostra rete e la rete esterna, ha un compito supplementare: quello di effettuare dei filtraggi, ovviamente al livello che gli è possibile, ossia tipicamente ai livelli 3 e 4. A questo punto tutta la sicurezza del nostro sistema è demandata al router stesso: se il router effettua un buon lavoro saremo sicuri, se non effettua un buon lavoro, come purtroppo non può fare visto che non può salire fino ai livelli applicativi, la nostra rete sarà esposta. L'architettura screening router, quindi, si presta ad essere utilizzata, come soluzione di firewall, solo ed esclusivamente in casi di reti con pochissimi protocolli che transitano tra la rete e l'esterno e soltanto per reti con livello di sicurezza medio-basso.

Architettura dual-home gateway



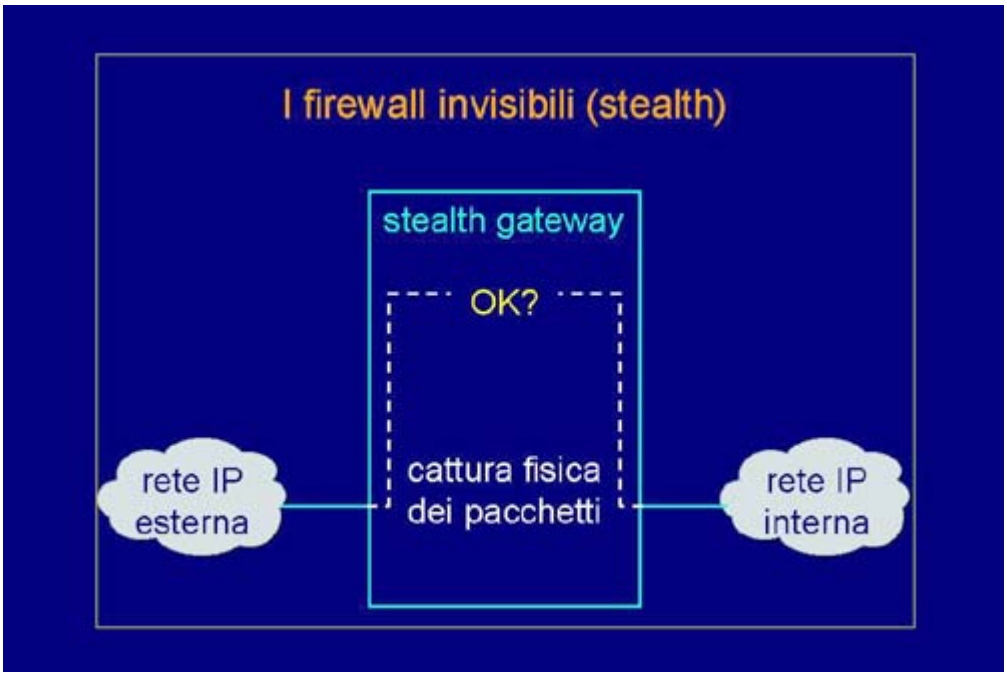
Se si desidera migliorare il livello di sicurezza offerto da un'architettura di quel genere, conviene introdurre un secondo elemento in grado di effettuare dei controlli ad un livello più elevato. Si parla, allora, di un'architettura di tipo dual-home gateway nel caso in cui, oltre al router, il controllo venga effettuato anche da un nodo di elaborazione dotato di due schede di rete. Questo nodo di elaborazione separerà, obbligatoriamente, la rete interna, non soltanto da una rete esterna, ma anche da una rete intermedia. Questa rete intermedia prende il nome di zona demilitarizzata, ossia terra di nessuno, perché è quella entro cui dovrebbero passare solo un sottoinsieme dei pacchetti provenienti dall'esterno. Il router fa un primo filtro a livello basso, 3 e 4, il gateway effettua un controllo più raffinato a livello 5, 6 o 7. Sulla zona demilitarizzata sono normalmente ospitati quei server che hanno necessità di frequenti contatti con l'esterno. Ad esempio, il server Web aziendale rivolto all'esterno troverebbe logicamente posto qui, all'interno della DMZ.

Architettura screened subnet



Infine, l'architettura migliore è quella cosiddetta screened subnet. In un architettura di tipo screened subnet noi siamo in grado di nascondere completamente l'esistenza della rete interna, al mondo esterno. Questo è possibile perché, rispetto alla soluzione precedente, la zona demilitarizzata è stata completamente nascosta tramite un secondo router. In questo modo il primo router ignorerà completamente l'esistenza della rete interna. Un eventuale attaccante dovrà in ogni caso superare almeno due sistemi, prima di penetrare all'interno della nostra rete aziendale. Anche in questo caso, questa rete su cui non sono attestati nodi aziendali, si chiama zona demilitarizzata ed analogamente qua sopra vengono attestati i server esterni. Notate che nel caso che il nostro sistema informatico preveda la disponibilità di modem collegati direttamente alla nostra rete aziendale, tali modem e il relativo NAS (Network Access Server) devono essere posizionati sulla zona demilitarizzata. In nessun caso bisogna permettere che delle apparecchiature di collegamento insicure, quali sono i modem, siano collegati direttamente alla rete aziendale.

I firewall invisibili (stealth)



Infine, concludiamo con un concetto innovativo ed interessante, che è emerso in anni recenti nel campo dei firewall. Uno dei problemi dei firewall è che essi stessi potrebbero essere oggetto di attacco da parte di un hacker. Ma un hacker, per attaccare un sistema, ha bisogno di potergli indirizzare dei pacchetti. Il concetto che è stato sviluppato è quello di firewall invisibile, ossia un firewall, quindi un nodo di elaborazione, privo di indirizzo di rete. Se un nodo non è dotato di indirizzo di rete non gli si possono indirizzare dei pacchetti e non è quindi virtualmente attaccabile. Ma allora come riesce a sviluppare le proprie funzionalità di sicurezza? Il concetto è molto semplice, il firewall invisibile, il cosiddetto stealth firewall o stealth gateway, è costituito da un nodo di elaborazione che interrompe fisicamente il cavo tra la rete interna e la rete esterna. Dopodiché effettua cattura fisica dei pacchetti, perché nessuna delle sue interfacce è dotata di indirizzo di rete, ma grazie al fatto che il cavo entra fisicamente dentro l'interfaccia è possibile catturare tutti i bit. Questi bit sono sottoposti a un controllo di livello opportuno, secondo le funzionalità di sicurezza richieste e se il controllo da esito positivo i bit vengono inoltrati inalterati. Quindi, in nessun modo avviene una modifica dei dati: un osservatore esterno non può in nessun modo accorgersi del fatto che i dati sono stati controllati. I dati subiscono soltanto un lieve ritardo nel momento in cui attraversano il gateway. L'azione del gateway a tutti gli effetti è invisibile, i pacchetti passano o non passano, sembra in modo magico. Questo è un concetto interessante che mi aspetto di vedere applicato sempre più estesamente in futuro.