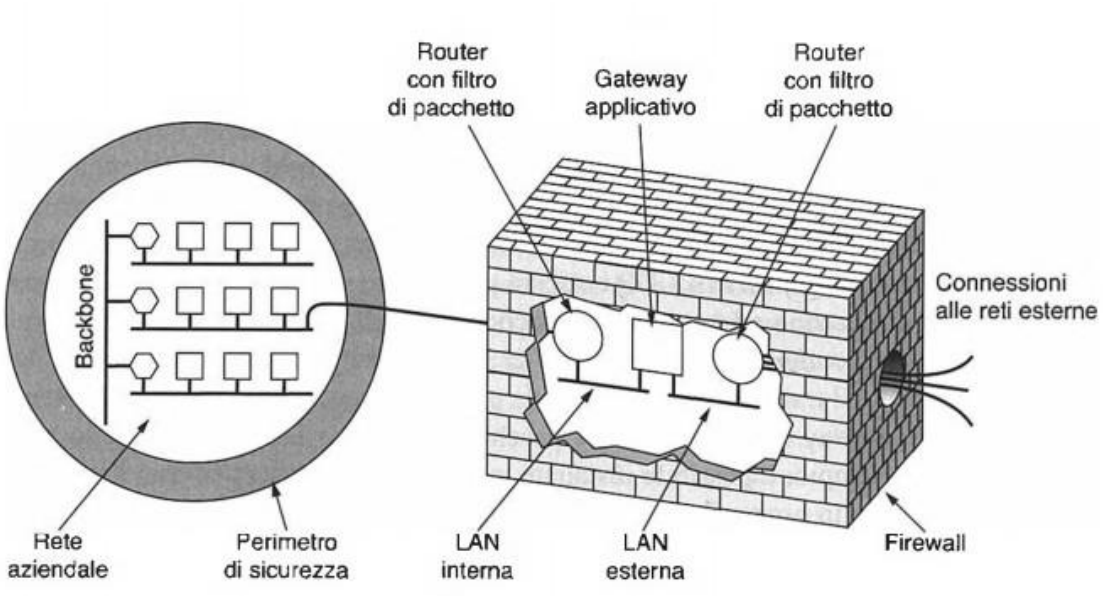
In questo modulo saranno presentati i principi di funzionamento dei moderni firewall presenti agli estremi di una rete per la sua protezione.

Firewall

Prof. Michele Tarantino

La possibilità di connettere qualunque computer che si trova in qualunque posto a qualunque altro computer in una qualsiasi località, può essere visto allo stesso tempo come una comodità e come una fonte di problemi. Per le persone che si collegano da casa e navigano suInternet, si tratta di un divertimento. Per i manager della sicurezza nelle aziende è invece un incubo. La maggior parte delle aziende possiede una gran quantità di informazioni online e queste devono essere garantite e protette soprattutto se parliamo di sistemi distribuiti su cui i dati viaggiano in continuazione: segreti industriali, piani di sviluppo di prodotti, strategie di marketing, analisi finanziarie, ecc. La divulgazione di queste informazioni alla concorrenza può avere pesanti ripercussioni. Oltre al pericolo di vedere fuoriuscire delle informazioni, ci sono anche i pericoli legati alla diffusione di informazioni verso l'interno. In particolare, *virus*, *worm* e altre "pesti digitali" possono aprire una falla nella sicurezza e distruggere dati importanti, oppure far sprecare una gran quantità del tempo agli amministratori di sistema chedevono rimediare ai danni. La conseguenza è la necessità di instaurare dei meccanismi di protezione che garantiscano la sicurezza. Come già detto, un metodo è quello di usare IPsec. Questo approccio protegge i dati in transito fra i siti sicuri. IPsec non riesce però a fare nulla per tenere alla larga dalle LAN aziendali le pesti digitali e gli intrusi. Per vedere come si può realizzare questo obiettivo, dobbiamo parlare di *firewall*.

I ***firewall*** (letteralmente, muro di fuoco) sono una versione moderna del vecchio rimedio medievale per le emergenze di sicurezza: scavare un profondo fossato attorno al proprio castello. Questa struttura obbligava chiunque volesse entrare o uscire dal castello a passareper un singolo ponte levatoio, dove la polizia poteva facilmente eseguire le sue ispezioni. Con le reti è possibile realizzare lo stesso trucco: un'azienda può avere molte LAN connesse in modo arbitrario, ma tutto il traffico da e per l'azienda viene convogliato attraverso un ponte levatoio (il *firewall*), come mostrato nella Figura seguente:

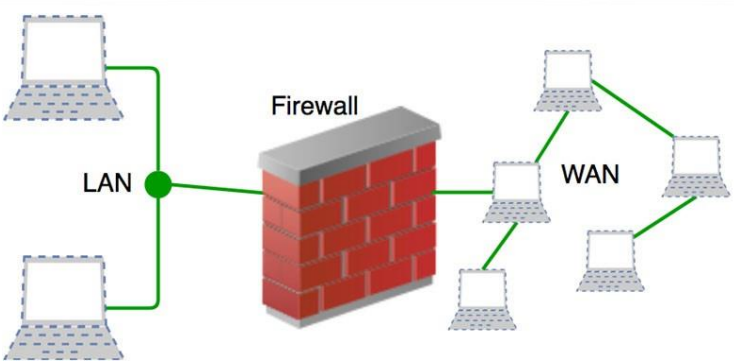


In questa configurazione il *firewall* ha due componenti: due *router* che fanno il **filtraggio** dei pacchetti e un ***gateway* applicativo**. Esistono anche delle configurazioni più semplici, ma questa struttura ha il vantaggio di obbligare ogni pacchetto a transitare attraverso due filtri e un *gateway* applicativo sia per entrare sia per uscire.

Ogni ***packet filter*** (filtro di pacchetti) è un *router* standard equipaggiato con funzionalità extra. Queste funzionalità permettono di ispezionare ogni pacchetto in arrivo o in uscita. I pacchetti che rispondono a certi criteri vengono fatti passare normalmente, quelli che falliscono il test vengono scartati. Nella Figura è molto probabile che il *packet filter* verso l'interno della LAN controlli i pacchetti in uscita, mentre quello sul lato esterno della LAN controlli i pacchetti in ingresso. I pacchetti, dopo aver attraversato il primo ostacolo, proseguono verso il *gateway* applicativo per un'ulteriore ispezione. Si utilizzano due *packet filter* su LAN differenti per essere sicuri che nessun pacchetto possa entrare o uscire senza essere passato attraverso il *gateway* applicativo: non c'è nessun percorso che gli passaintorno.

I *packet filter* sono tipicamente gestiti tramite delle tabelle configurate dall'amministratore di sistema. Queste tabelle elencano sorgenti e destinazioni accettabili e quelle bloccate, inoltre gestiscono le regole predefinite riguardo a cosa fare con i pacchetti che vengono o vanno verso altre macchine. Nel caso comune delle impostazioni TCP/IP, la sorgente e la destinazione consistono di un indirizzo IP e di una porta. Le porte indicano quale servizio è desiderato. Per esempio, la porta TCP 23 è per il telnet, la porta 79 è per il *finger*. Un'aziendapuò bloccare tutti i pacchetti entranti per tutti gli indirizzi IP in combinazione con una o tutte queste porte. In questo modo, nessuno al di fuori dell'azienda può effettuare una login con telnet oppure cercare le persone con il *daemon finger*.

Bloccare i pacchetti in uscita è più difficile in quanto, sebbene molti siti si attengano alle convenzioni sui numeri standard delle porte, non c'è l'obbligo di farlo. Inoltre, per alcuni servizi come l'FTP (*File Transfer Protocol*), i numeri di porta vengono assegnati dinamicamente. Bloccare le connessioni UDP è ancora più difficile rispetto a quelle TCP, questo perché a priori si riescono ad avere troppo poche informazioni sull'attività delle connessioni UDP. Per questo motivo, molti *packet filter* sono configurati semplicemente per bandire completamente il traffico UDP. La seconda parte del *firewall* è costituita dal *gateway* applicativo. Il *gateway* non guarda più i pacchetti in quanto tali, ma opera allo stratoapplicativo. Per esempio, è possibile installare un *gateway* di posta, per esaminare tutti i messaggi in arrivo o in uscita. Il *gateway* esamina ciascun messaggio e decide se trasmetterlo o scartarlo in base ai campi di

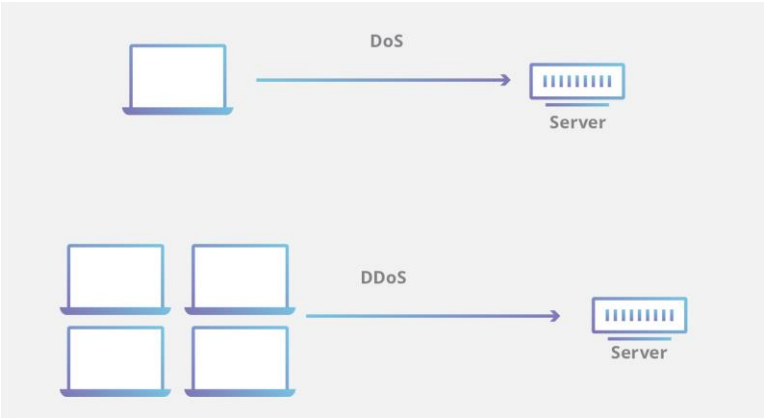


intestazione, alla dimensione del messaggio, o anche a seconda del contenuto. Ogni sito è libero di installare uno o più *gateway* applicativi per applicazioni specifiche. È prassi comune, per le organizzazioni molto sensibili alla sicurezza, permettere l'ingresso e l'uscita della postaelettronica e l'uso del Web, ma di proibire tutto il resto, in quanto considerato tropporischioso. Questa soluzione, in combinazione con la crittografia e il *packet filtering*, offre unacerta sicurezza, al costo di qualche scomodità.

Anche quando il *firewall* è configurato perfettamente, rimangono ancora molti problemi di sicurezza. Per esempio, se un *firewall* è configurato per permettere l'ingresso dei pacchetti solo da alcune specifiche reti (per esempio le altre sedi dell'azienda), un intruso dall'esterno del *firewall* può inserire un indirizzo di sorgente falso e quindi aggirare il controllo. Se un utente, dall'interno, vuole spedire all'esterno dei documenti segreti, li può cifrare oppure fotografare per poi spedirli come file JPEG, che aggirano qualunque filtro sulle parole. Non acaso il 70% degli attacchi arrivano da dentro il *firewall*.

Inoltre, esiste un'intera classe di attacchi che i *firewall* non riescono a trattare. L'idea alla basedei *firewall* è quella di prevenire l'ingresso degli intrusi e l'uscita dei dati segreti. Sfortunatamente, ci sono persone che non hanno niente di meglio da fare che cercare di bloccare la funzionalità di certi siti. Questo viene fatto inviando una grande quantità di pacchetti legittimi ai siti bersaglio, finché questi non collassato sotto il peso del carico di lavoro. Per esempio, per "azzoppare" un sito, un intruso può inviare un pacchetto TCP SYN, per stabilire una connessione. Il sito allocherà quindi uno slot per la connessione e invierà come risposta un pacchetto SYN + ACK. Se l'intruso non risponde, lo slot viene mantenuto per alcuni secondi finché non si ottiene un *timeout*. Se l'intruso invia migliaia di richieste di connessione, tutti gli slot vengono riempiti e le connessioni legittime non possono più essere aperte. Gli attacchi che hanno come scopo quello di fermare l'operatività dell'obiettivo, e nonquello di rubare dei dati, sono chiamati DoS (*Denial o f Service*)(*SYN flood*).

Normalmente i pacchetti con le richieste hanno un indirizzo sorgente falso, in questo modo l'intruso non può essere identificato facilmente. Unavariante più pericolosa è possibilequando un intruso è già penetrato in centinaia di macchine sparse per il mondo, e ordina a tutte queste macchine di attaccare simultaneamente un solo obiettivo.Attacchi di questo tipo sono detti attacchi DDoS (*Distributed Denial of Service)*. È difficile proteggersi contro questo tipo di attacchi. Anche se la macchina attaccata identifica le false richieste, ci vuole sempre un po' di tempo per elaborarle e poi scartarle. Se questo tipo di richieste arrivano con una frequenza abbastanza alta, la CPU della macchina attaccata sarà costretta a spendere tutto il suo tempo per gestirle.



Resta connesso e informato sui prossimi eventi, corsi e seminari:

Web
www.profmicheletarantino.com

Email
profmicheletarantino@gmail.com

Telefono
349 83 54 521

Facebook
@micheletarantinodocente

Instagram
@profmicheletarantino

Hai bisogno di un modulo personalizzato? Non esitare a contattarmi!