# Una rete di... sicurezza

## La sicurezza di una rete passa prima di tutto per gli elementi della sua infrastruttura

Massimo Giussani

Le reti di calcolatori che si incontrano nel mondo reale presentano tutta una serie di vulnerabilità dettate da esigenze di praticità, funzionalità o retrocompatibilità. La compensazione di queste debolezze richiede un'attenta opera di progettazione e configurazione, allo scopo di proteggere i nodi sprovvisti di difese adeguate, limitare l'accesso ai soli soggetti autorizzati, disabilitare i servizi di rete non indispensabili e assicurare la riservatezza delle comunicazioni. Gli strumenti a disposizione di chi progetta e amministra le reti sono molteplici: da un lato il posizionamento strategico di switch e router permette di confinare la diffusione dei dati ai soli soggetti o alle sottoreti pertinenti, dall'altro l'impiego di firewall e proxy consente di controllare lo scambio dei dati a vari livelli; i sistemi di rilevamento e prevenzione delle intrusioni permettono poi di analizzare in maniera coordinata il traffico di rete per isolare le eventuali anomalie, mentre il ricorso alle reti private virtuali accresce la sicurezza mediante opportuni meccanismi di cifratura.
Vediamo in che modo i diversi elementi dell'infrastruttura di rete possono rappresentare da un lato potenziali punti di accesso non autorizzato e dall'altro dei veri e propri bastioni per la protezione della rete.

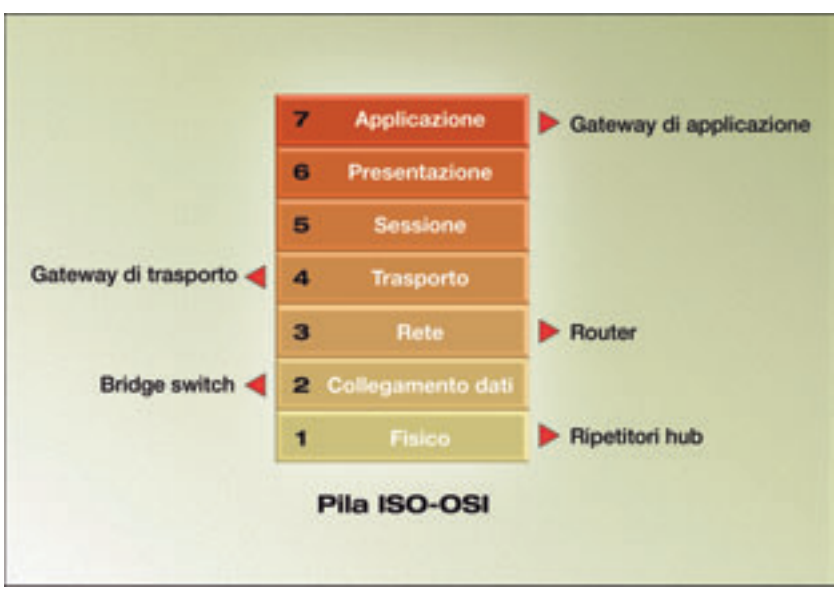


**Figura 1 - Collocazione dei principali dispositivi di rete nella pila ISO-OSI**

### Gli hub e gli switch

L'infrastruttura di rete gioca un ruolo fondamentale nell'implementazione delle politiche di sicurezza. Per capire come, è prima di tutto necessario sapere quali sono i compiti di 'hub', 'switch' e 'router' e come questi possono influire, positivamente o negativamente, sulla sicurezza delle rete nel suo complesso. Gli hub, o concentratori, lavorano al livello più basso della pila ISO/OSI e si limitano a replicare tutti i dati che ricevono sulle altre porte del dispositivo, con una condivisione delle risorse del canale in termini di banda e di probabilità di collisione dei pacchetti. Se da un lato non contribuiscono a migliorare la sicurezza della rete, dall'altro in genere non porgono il fianco agli attacchi degli hacker. Esistono tuttavia hub più avanzati che permettono di disabilitare alcune porte e di effettuare statistiche sui pacchetti in transito: questi sistemi sono dotati di un'interfaccia per la loro gestione (tipicamente Snmp, Telnet o http) che, se non viene adeguata-

mente protetta o disabilitata, può portare alla compromissione del dispositivo.
Gli switch, o commutatori, sono nella loro accezione più comune dei dispositivi di livello due nella pila ISO/OSI. Lavorando al livello di collegamento dati, capiscono gli indirizzi MAC dei nodi di origine e destinazione e provvedono di conseguenza a smistare il traffico. I dati vengono inviati solo alle porte direttamente collegate alle sottoreti che contengono gli indirizzi di destinazione. L'enorme vantaggio offerto dai commutatori è rappresentato dalla separazione dei flussi di informazione: due nodi che comunicano tramite uno switch vedono il canale come se fosse a loro dedicato, a banda piena e senza rischi di collisione con altri pacchetti. Gli switch offrono dei vantaggi anche dal punto di vista della sicurezza, dato che impediscono l'intercettazione delle comunicazioni da parte dei nodi estranei alle sottoreti direttamente interessate. Per contro, come già per gli hub intelligenti, le interfacce per la configurazione e la gestione rappresentano un punto debole da proteggere.

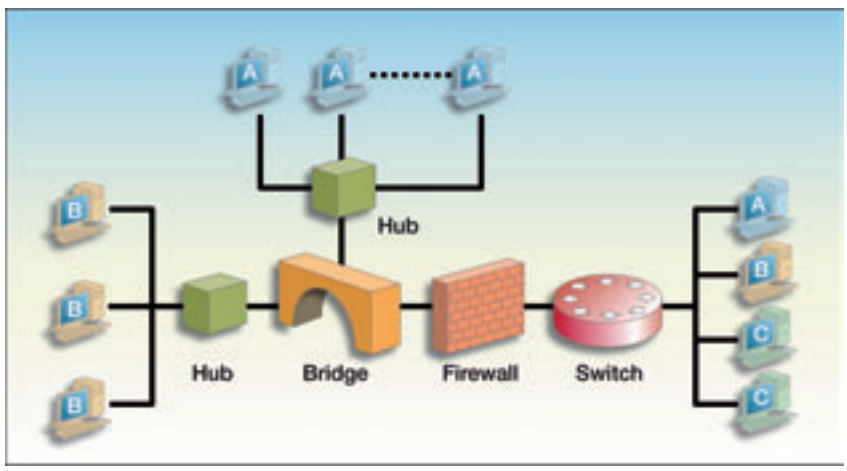


**Figura 2 - Switch e bridge possono essere impiegati per suddividere le reti fisiche in reti virtuali con traffico separato, in modo da impedire o rendere difficoltosa l'intercettazione delle comunicazioni**

## I router

I router, che potremmo chiamare instradatori, operano a un livello ancora più alto della pila ISO-OSI, nella fattispecie al livello di rete. Sono in grado di capire gli indirizzi IP e usano questa informazione per stabilire a quale porta di uscita inviare i pacchetti in transito. La decisione viene presa in base a tabelle di instradamento configurate manualmente o aggiornate dinamicamente in base alle informazioni raccolte durante il funzionamento del dispositivo ed elaborate da sofisticati algoritmi. All'interno di una rete aziendale, i router sono generalmente collocati nei punti di accesso alla rete pubblica. Rappresentando i primi e gli ultimi bastioni di difesa dell'azienda dagli attacchi esterni, devono essere configurati ponendo particolare attenzione alle problematiche di sicurezza. Un malintenzionato che dovesse guadagnare l'accesso al router di frontiera potrebbe dirottare il traffico in ingresso e in uscita verso i propri sistemi (intercettando comunicazioni riservate o fornendo false informazioni sotto mentite spoglie) semplicemente riconfigurando la tabella di instradamento. L'esclusione di protocolli di controllo poco sicuri (come l'ormai antiquato Telnet) e l'adozione di protocolli dotati di metodi sicuri di autenticazione e cifratura delle comunicazioni (come SSH), uniti all'impostazione di password 'forti', possono ridurre i rischi di compromissione dei router. L'adozione di protocolli di instradamento che implementano funzioni di sicurezza rappresenta un altro passo in questa direzione, ad esempio, sostituendo i router con protocollo RIP (Router Information Protocol) con la variante RIP-2, dotata di supporto dell'autenticazione sicura, o con il protocollo Ospf (Open Shortest Path First).

## I firewall

Senza dubbio gli strumenti più diffusi per implementare le politiche di sicurezza in una rete aziendale sono i firewall. Come indicato dal nome, che significa letteralmente 'muro tagliafiamme', questi componenti hardware e software servono a impedire la propagazione di dati indesiderati oltre un certo punto della rete, tanto in entrata quanto in uscita.
I firewall possono essere sostanzialmente di due tipi: firewall personali, tipicamente agenti software installati sui singoli terminali che si occupano di monitorare le comunicazioni a livello di pacchetti e di applicazioni, e firewall di rete, che gestiscono il traffico da e verso un'intera area protetta e possono presentarsi sotto forma di dispositivi separati (ma più frequentemente integrati nei router) o di applicativi software eseguiti dal sistema operativi di un server di rete (ad esempio IPTables sotto Linux o MS ISA Server sotto Windows). Scopo del firewall è controllare il traffico in transito, a diversi livelli di astrazione, per far sì che lo scambio dei dati sia sottoposto a un rigido controllo di sicurezza, a partire dall'autenticazione degli interlocutori, passando per la cifratura dei dati sensibili, celando per quanto possibile l'architettura della rete interna e consentendo l'accesso solo a determinati applicativi e servizi. La registrazione degli eventi anomali in un log permette agli amministratori di rete di verificare il comportamento del sistema protetto e identificare le fonti di potenziali intrusioni. Nel corso degli anni i firewall si sono evoluti dando alla luce modelli ibridi, dotati di un numero crescente di funzionalità, a partire dalla conversione NAT (Network Address Translation) degli indirizzi di rete, passando per l'aggiunta di antivirus e filtri antispam, per arrivare alla gestione di reti private virtuali (VPN).

## Dai bridge trasparenti ai proxy

A seconda della tecnologia utilizzata, i firewall sono in grado di agire a diversi livelli della pila ISO-OSI. Alcuni operano su un solo strato, altri esercitano la loro azione su più strati, come illustrato schematicamente dalla figura 3. I firewall a filtraggio di pacchetti, ad esempio, utilizzano le informazioni dello strato di rete per esercitare un controllo del traffico basato sugli indirizzi IP di arrivo e partenza e su altre informazioni accessorie, come il numero delle porte interessate. Conoscere queste variabili può non essere sufficiente a distinguere uno scambio illegittimo, ad esempio con un indirizzo IP contraffatto, da un pacchetto originato da un corrispondente di fiducia. Un controllo a un livello superiore, quello di sessione, permette di verificare l'esistenza di una sessione di comunicazione tra due soggetti legittimi e consente di filtrare pacchetti spuri che non appartengono a tale scambio. A un livello ancora più alto, quello di applicazione, troviamo i firewall proxy che realizzano un vero e proprio intermediario in grado di comprendere nella loro interezza le informazioni veicolate con un dato protocollo applicativo. I dati vengono analizzati su un sistema robusto e vengono inviati al destinatario solo se ritenuti non nocivi e conformi alle politiche di sicurezza in atto. Un firewall di questo tipo deve poter eseguire tutti i servizi necessari a gestire i protocolli di comunicazione ammessi. In particolare dovrà disporre di un proxy http per gestire la navigazione sul Web, di un proxy Smtp per gli scambi di posta elettronica, di un proxy ftp per il trasferimento dei file e così via. Non sono possibili comunicazioni con protocolli applicativi diversi da quelli implementati. Esistono anche firewall che agiscono a livello di collegamento dati e si comportano da bridge trasparenti tra due nodi di rete: ricevono le trame del livello 'data link', estraggono il contenuto a livello collegamento dati ed effettuano il filtraggio. Il traffico che soddisfa i requisiti di sicurezza viene inoltrato al nodo di destinazione. Uno dei principali vantaggi di questi dispositivi, che vanno sotto il nome di 'bridging firewall', è rappresentato dal fatto che, operando al secondo livello della pila OSI, non presentano alcun indirizzo IP e sono pertanto trasparenti al livello di rete, rendendo estremamente difficile poterli attaccare dall'esterno.


**Figura 3 - Esistono diverse tipologie di firewall, ciascuna delle quali agisce a livelli differenti della pila ISO-OSI**

## Ispezioni di stato

I 'firewall stateful' controllano le comunicazioni a più livelli nel tentativo di filtrare dinamicamente i pacchetti in base allo stato delle connessioni di rete. Ad esempio, il diffuso protocollo TCP, che interessa lo strato di rete della pila OSI, è un protocollo di comunicazione orientato alla connessione. Questo significa che per poter trasferire dati da un punto all'altro della rete è prima necessario stabilire una connessione tra i due interlocutori con una forma di 'handshake'. Lo stato della connessione viene tracciato per mezzo di opportuni flag nel pacchetto TCP; queste informazioni vengono usate dal firewall stateful

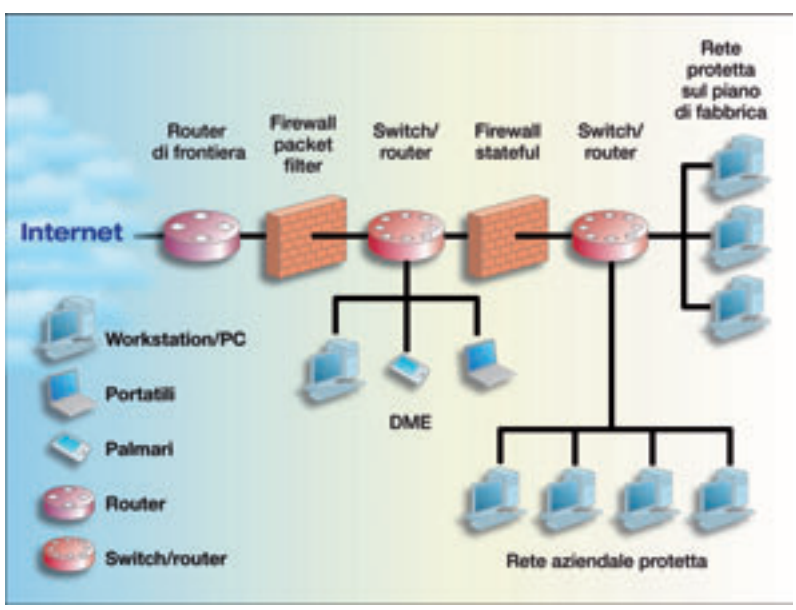


**Figura 4 - La sicurezza di una rete richiede l'integrazione di vari dispositivi per separare le reti esposte agli attacchi da quelle protette**

per creare delle tabelle di connessione sulle quali basare le decisioni per filtrare le comunicazioni. Ogni volta che un nodo esterno alla rete richiede di comunicare con un terminale all'interno del perimetro protetto, il firewall stateful crea una voce nella tabella di connessione associata agli indirizzi IP e alle porte di mittente e destinatario e lascia passare solo quei pacchetti che sono associabili a stati di connessione ritenuti legittimi, bloccando tutti gli altri. L'ispezione dei pacchetti a livello di stato (SPI, Stateful Packet Inspection) rappresenta dunque un passo avanti rispetto al filtraggio dei pacchetti al mero livello di rete e costituisce una scelta comunque efficiente rispetto alle soluzioni di firewall realizzate con proxy. Ulteriori informazioni sul tipo di comunicazione in atto possono essere dedotte, senza troppo compromettere le prestazioni, da una sommaria analisi dei dati a livello di applicazione; il risultato è una maggior flessibilità decisionale che permette di gestire flussi di dati basati su protocolli di trasporto che si comportano diversamente dal tradizionale TCP/IP (come ftp) o su protocolli di livello superiore che devono essere opportunamente interpretati (ad esempio http). I protocolli senza connessione, come UDP, presentano delle difficoltà aggiuntive per l'assenza di flag di stato. A questo si può porre parziale rimedio utilizzando dei contatori da associare a sessioni virtuali da disabilitare dopo un tempo predeterminato; il firewall deve inoltre ritenere legittimo il transito di pacchetti di controllo Icmp che servono a segnalare eventuali problemi di trasmissione in una comunicazione basata su UDP.

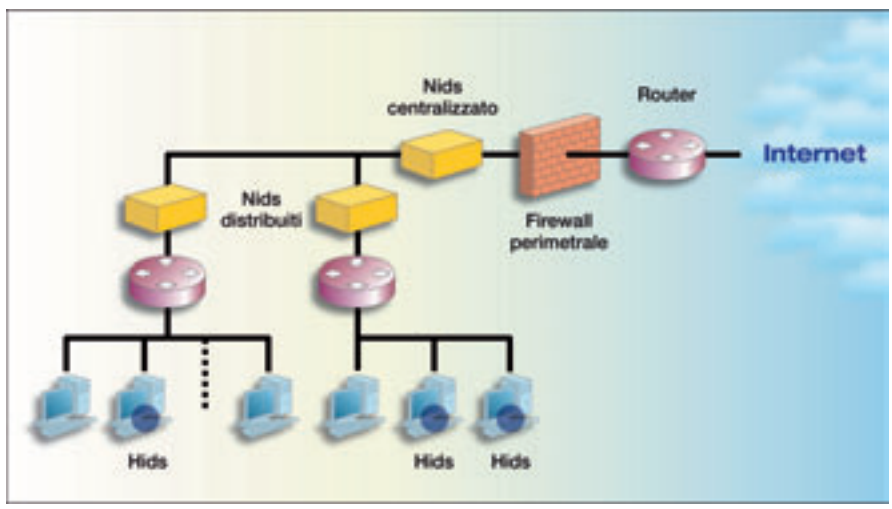


**Figura 5 - L'implementazione di sistemi di rilevamento delle intrusioni, nelle versioni di rete (Nids) e da terminale (Hids) permette di tenere sotto controllo il traffico di rete, registrando tutte le potenziali anomalie**

## Rilevare e prevenire le intrusioni

'Packet filtering', 'stateful inspection' e proxy sono i termini più frequentemente usati quando si ha a che fare con i firewall di rete. I primi sono generalmente posizionati nei punti di frontiera con le reti esterne e operano una prima cernita dei pacchetti, eliminando quelli dichiaratamente non pertinenti; i firewall stateful trovano posto all'interno della rete e lasciano passare solo i pacchetti che riguardano comunicazioni riconosciute come legittime; al livello più elevato, in termini di intelligenza e di carico, si posizionano i proxy che esercitano un controllo a livello di applicazione.

Oltre che per proteggere la rete dalla minacce esterne, i firewall possono essere utilizzati per isolare dei segmenti di rete con un livello di protezione volutamente ridotto. Si tratta delle cosiddette zone demilitarizzate o DMZ (DeMilitarized Zone), entro i cui confini è possibile accedere a Internet senza limitazioni troppo stringenti, ma anche senza conseguenze per il resto della rete. Altri dispositivi affiancano i firewall nell'arsenale dell'amministratore di rete: i sistemi di rilevamento delle intrusioni (IDS, Intrusion Detection System) e i sistemi di prevenzione delle intrusioni (IPS, Intrusion Prevention System). Un IDS è un sistema che analizza i dati scambiati su una rete protetta alla ricerca di anomalie o tracce di schemi di attacco noti. Una volta che il motore ha identificato una potenziale falla (che potrebbe essere un eccesso di traffico con un certo tipo di protocollo da o verso una determinata stazione, o la presenza di dati malformati all'interno dei pacchetti in transito), l'IDS provvede a tenerne traccia in opportuni log e, nei casi più urgenti, ad allertare l'amministratore nei casi più urgenti. Un sistema IDS è solitamente costituito da più sensori hardware o software posizionati nei punti strategici della rete (tipicamente in corrispondenza dei firewall), da un motore di analisi accoppiato a un database degli schemi di attacco noti e da una console per la gestione. Come i firewall, anche gli IDS possono operare a diversi livelli di astrazione della pila OSI, utilizzando un insieme di regole e algoritmi per discernere il traffico normale da quello potenzialmente malevolo. Un IDS non prende misure attive nei confronti degli attacchi: si comporta piuttosto come un sistema di allarme che segnala la presenza di intrusi, tenendo traccia della strada usata per penetrare le difese del sistema. Queste informazioni possono essere successivamente usate per identificare i problemi di sicurezza e irrobustire la rete.

Un'ulteriore evoluzione dei dispositivi di sicurezza è rappresentata dagli IPS, che agiscono direttamente nei confronti delle minacce e mettono in pratica le misure necessarie per bloccare il traffico anomalo non appena questo viene rilevato. ■