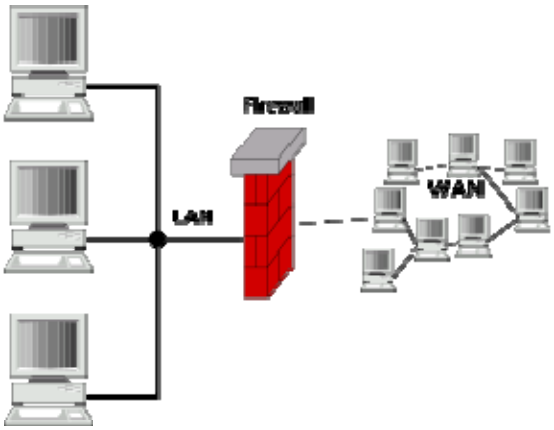
Firewall

Da Wikipedia, l'enciclopedia libera.



Schema semplificato di una rete con firewall collegata a una rete esterna

In Informatica, nell'ambito delle reti di computer, un **firewall** (termine inglese dal significato originario di *parete refrattaria, muro tagliafuoco', "muro ignifugo"'; in italiano anche* parafuoco *o* parafiamma*) è un componente passivo di difesa perimetrale che può anche svolgere funzioni di collegamento tra due o più tronconi di rete.* Usualmente la rete viene divisa in due sottoreti: una, detta esterna, comprende l'intera Internet mentre l'altra interna, detta LAN (Local Area Network), comprende una sezione più o meno grande di un insieme di computer locali. In alcuni casi è possibile che si crei l'esigenza di creare una terza sottorete detta DMZ (o zona demilitarizzata) atta a contenere quei sistemi che devono essere isolati dalla rete interna ma devono comunque essere protetti dal firewall.

Grazie alla sua posizione strategica, il firewall risulta il posto migliore ove imporre delle logiche di traffico per i pacchetti in transito e/o eseguire un monitoraggio di tali pacchetti. La sua funzionalità principale in sostanza è quella di creare un filtro sulle connessioni entranti ed uscenti, in questo modo il dispositivo innalza il livello di sicurezza della rete e permette sia agli utenti interni che a quelli esterni di operare nel massimo della sicurezza.

Indice

Principi di funzionamento

Una prima definizione chiusa di firewall è la seguente:

Apparato di rete hardware o software che filtra tutti i pacchetti entranti ed uscenti, da e verso una rete o un computer, applicando regole che contribuiscono alla sicurezza della stessa.

In realtà un firewall può essere realizzato con un normale computer (con almeno due schede di rete e software apposito), può essere una funzione inclusa in un router o può essere un apparato specializzato. Esistono inoltre i cosiddetti "firewall personali", che sono programmi installati sui normali calcolatori, che filtrano solamente i pacchetti che entrano ed escono da quel calcolatore; in tal caso viene utilizzata una sola scheda di rete.

La funzionalità principale in sostanza è quella di creare un filtro sulle connessioni entranti ed uscenti, in questo modo il dispositivo innalza il livello di sicurezza della rete e permette sia agli utenti interni che a quelli esterni di operare nel massimo della sicurezza. Il firewall agisce sui pacchetti in transito da e per la zona interna potendo eseguire su di essi operazioni di:

- controllo
- modifica
- monitoraggio

Questo grazie alla sua capacità di "aprire" il pacchetto IP per leggere le informazioni presenti sul suo header, e in alcuni casi anche di effettuare verifiche sul contenuto del pacchetto.

Personal Firewall o Firewall Software

*Per approfondire, vedi la voce **Personal firewall**.*

Oltre al firewall a protezione perimetrale ne esiste un secondo tipo, definito "*Personal Firewall*", che si installa direttamente sui sistemi da proteggere (per questo motivo è chiamato anche Firewall Software). In tal caso, un buon firewall effettua anche un controllo di tutti i programmi che tentano di accedere ad Internet presenti sul computer nel quale è installato, consentendo all'utente di impostare delle regole che possano concedere o negare l'accesso ad Internet da parte dei programmi stessi, questo per prevenire la possibilità che un programma malevolo possa connettere il computer all'esterno pregiudicandone la sicurezza.

Il principio di funzionamento differisce rispetto a quello del firewall perimetrale in quanto, in quest'ultimo, le regole che definiscono i flussi di traffico permessi vengono impostate in base all'indirizzo IP sorgente, quello di destinazione e la porta attraverso la quale viene erogato il servizio, mentre nel personal firewall all'utente è sufficiente esprimere il consenso affinché una determinata applicazione possa interagire con il mondo esterno attraverso il protocollo IP.

Da sottolineare che l'aggiornamento di un firewall è importante ma non è così vitale come invece lo è l'aggiornamento di un antivirus, in quanto le operazioni che il firewall deve compiere sono sostanzialmente sempre le stesse. È invece importante creare delle regole che siano corrette per decidere quali programmi devono poter accedere alla rete esterna e quali invece non devono.

Vantaggi e svantaggi

Rispetto ad un firewall perimetrale, il personal firewall è eseguito sullo stesso sistema operativo che dovrebbe proteggere, ed è quindi soggetto al rischio di venir disabilitato da un malware che prenda il controllo del calcolatore con diritti sufficienti. Inoltre, la sua configurazione è spesso lasciata a utenti finali poco esperti.

A suo favore, il personal firewall ha accesso ad un dato che un firewall perimetrale non può conoscere, ovvero può sapere quale applicazione ha generato un pacchetto o è in ascolto su una determinata porta, e può basare le sue decisioni anche su questo, ad esempio bloccando una connessione SMTP generata da un virus e facendo passare quella generata da un client di posta elettronica autorizzato.

Inoltre, può essere installato rapidamente e indipendentemente dagli amministratori di rete.

Filtraggio dei contenuti

Una funzione che alcuni firewall prevedono è la possibilità di filtrare ciò che arriva da internet sulla base di diversi tipi di criteri non relativi alla sicurezza informatica, ma volti a limitare gli utilizzi della rete sulla base di decisioni "politiche", in particolare vietando la connessione a determinate categorie di siti internet:

- contenuti non adatto ai minori (ad esempio in una rete domestica, o destinata ai frequentatori di una scuola o biblioteca)
- contenuti non pertinente con l'attività lavorativa (in una rete aziendale)
- contenuti non ritenuti accettabili da organi di censura, su base politica o religiosa).
- siti che permettono di pubblicare informazioni sfuggendo alla censura di un regime totalitario (in particolare blog)

Alcune nazioni arrivano a filtrare tutto il traffico internet proveniente dal proprio territorio nazionale nel tentativo di controllare il flusso di informazioni .

Spesso l'attivazione di questa funzionalità è demandata a software e/ho hardware aggiuntivi appartenenti alla categoria dell'URL filtering. Ai firewall viene però richiesto di impedire che gli utenti aggirino tali limitazioni.

Limitazioni

Il firewall è solo uno dei componenti di una strategia di sicurezza informatica, e non può in generale essere considerato sufficiente:

- la sua configurazione è un compromesso tra usabilità della rete, sicurezza e risorse disponibili per la manutenzione della configurazione stessa (le esigenze di una rete cambiano rapidamente)
- una quota rilevante delle minacce alla sicurezza informatica proviene dalla rete interna (portatili, virus, connessioni abusive alla rete, dipendenti, accessi VPN, reti wireless non adeguatamente protette)

Tipologie

Tipologie di firewall, in ordine crescente di complessità:

- Il più semplice è il **packet filter**, che si limita a valutare gli header di ciascun pacchetto, decidendo quali far passare e quali no sulla base delle regole configurate. Ciascun pacchetto viene valutato solamente sulla base delle regole configurate, e per questo un firewall di questo tipo è detto anche **stateless**. Alcuni packet filter, analizzando i flag dell'header TCP, sono in grado di discriminare un pacchetto appartenente ad una "connessione TCP stabilita (established)" rispetto a quelli che iniziano una nuova connessione, ma non sono in grado di riconoscere un pacchetto malevolo che finga di appartenere ad una connessione TCP stabilita. Molti router posseggono una funzione di packet filter.
- Un firewall di tipo **stateful inspection**, tiene traccia di alcune relazioni tra i pacchetti che lo attraversano, ad esempio ricostruisce lo stato delle connessioni TCP. Questo permette ad esempio di riconoscere pacchetti TCP malevoli che non fanno parte di alcuna connessione. Spesso questo tipo di firewall sono in grado anche di analizzare i protocolli che aprono più connessioni (ad esempio FTP), inserendo nel payload dei pacchetti informazioni di livello rete e trasporto, permettendo così di gestire in modo puntuale protocolli di questo tipo.
- I firewall di tipo **deep inspection** effettuano controlli fino al livello 7 della pila ISO/OSI, ovvero valutano anche il contenuto applicativo dei pacchetti, ad esempio riconoscendo e bloccando i dati appartenenti a virus o worm noti in una sessione HTTP o SMTP.
- I cosiddetti **Application Layer Firewall** sono apparati che intercettano le connessioni a livello applicativo. A questa categoria appartengono i proxy. In tali casi, la configurazione della rete privata non consente connessioni dirette verso l'esterno, ma il proxy è connesso sia alla rete privata che alla rete pubblica, e permette alcune connessioni in modo selettivo, e solo per i protocolli che supporta.

La sintassi della configurazione di un firewall in molti casi è basata su un meccanismo di lista di controllo degli accessi (ACL), che possono essere statiche (quindi modificabili solo tramite configurazione esplicita) o dinamiche (cioè che possono variare in base allo stato interno del sistema, come ad esempio nel Port knocking).

Una funzione spesso associata al firewall è quella di NAT (traduzione degli indirizzi di rete), che può contribuire a rendere inaccessibili i calcolatori sulla rete interna.

Molti firewall possono registrare tutte le operazioni fatte (logging), effettuare registrazioni più o meno selettive (ad esempio, registrare solo i pacchetti che violano una certa regola, non registrare più di N pacchetti al secondo), e tenere statistiche di quali regole sono state più violate.

La registrazione integrale dell'attività di un firewall può facilmente assumere dimensioni ingestibili, per cui spesso si usa il logging solo temporaneamente per diagnosticare problemi, o comunque in modo selettivo (logging dei soli pacchetti rifiutati o solo di alcune regole). Tuttavia, l'analisi dei log di un firewall (o anche dei contatori delle varie regole) può permettere di individuare in tempo reale tentativi di intrusione.

Talvolta ad un firewall è associata anche la funzione *rilevamento delle intrusioni (IDS)*, un sistema basato su euristiche che analizza il traffico e tenta di riconoscere possibili attacchi alla sicurezza della rete, e può anche scatenare reazioni automatiche da parte del firewall (Intrusion prevention system).

Vulnerabilità

Una delle vulnerabilità più conosciute di un firewall di fascia media è l'HTTP tunneling, che consente di bypassare le restrizioni Internet utilizzando comunicazioni HTTP solitamente concesse dai firewall. Altra tipica vulnerabilità è la dll injection, ovvero una tecnica utilizzata da molti trojan, che sovrascrive il codice maligno all'interno di librerie di sistema utilizzate da programmi considerati *sicuri*. L'informazione riesce ad uscire dal computer in quanto il firewall, che di solito controlla i processi e non le librerie, crede che l'invio ad Internet lo stia eseguendo un programma da lui ritenuto sicuro, ma che di fatto utilizza la libreria contaminata. Alcuni firewall hanno anche il controllo sulla variazione delle librerie in memoria ma è difficile capire quando le variazioni sono state fatte da virus.

Implementazioni

- Software
  - Firestarter, *frontend* di iptables
  - shorewall, *frontend* di iptables
  - Netfilter/iptables: l'infrastruttura di *packet filtering* integrata nei kernel Linux versione 2.4 e superiori
  - ipchains: l'infrastruttura di *packet filtering* integrata nei kernel Linux versione 2.2
  - ipfw: l'infrastruttura di *packet filtering* integrata nel kernel FreeBSD versione 2
  - ipfw2: l'infrastruttura di *packet filtering* integrata nel kernel FreeBSD versione 4
  - IPFilter (ipf)
  - pf
  - Untangle Software gateway basata su Linux e disponibile anche come hardware appliance. Versione 5.1
  - m0n0wall progetto basato su FreeBSD
  - Distribuzione GNU/Linux che include firewall amministrabile via web
  - Distribuzione Endian Firewall Il software di Endian Firewall è open source al 100%

- Appliance
  - .vantronix basata su OpenBSD
  - Cisco PIX
  - Check Point FireWall 1
  - Juniper Netscreen
  - Endian Firewall
  - GIGASYS S110
  - Stonegate

- Personal firewalls
  - Online Armor
  - Agnitum Outpost
  - Comodo Personal Firewall
  - Core Force
  - Jetico
  - intelliGuard Antivirus
  - Look 'n' Stop
  - Norton Personal Firewall
  - Sunbelt Kerio
  - Sygate Personal Firewall
  - ZoneAlarm
  - OpenFirewall progetto basato su tdifw e WIPFW
  - GhostWall