

Introduzione al Firewall e Principi Fondamentali

1. 📖 Spiegazione Approfondita

Il firewall rappresenta la prima linea di difesa (perimetro) in un'architettura di sicurezza di rete. Concettualmente, agisce come un "guardiano" o un filtro intelligente posizionato tra due reti con diversi livelli di fiducia (solitamente una rete interna fidata, LAN, e una rete esterna non fidata, Internet).

La sua funzione primaria è analizzare il traffico in transito (sia in ingresso che in uscita) e decidere, pacchetto per pacchetto, se consentire il passaggio (*Allow*) o bloccarlo (*Block/Drop*), basandosi su un set di regole predefinite chiamate **Policy di Sicurezza**.

Studiare i firewall è essenziale per quattro macro-obiettivi:

1. **Protezione della rete:** Difesa contro accessi non autorizzati.
2. **Prevenzione degli attacchi:** Mitigazione di minacce attive (exploit, malware).
3. **Gestione del traffico:** Ottimizzazione e controllo della banda (QoS).
4. **Conformità normativa:** Rispetto di standard come GDPR, PCI-DSS o ISO 27001 che richiedono perimetri di sicurezza definiti.

3. 🧠 Analisi Tecnica & Memorizzazione

- **Definizione Chiave:** Dispositivo hardware o software che regola il flusso di traffico tra segmenti di rete diversi applicando una politica di controllo degli accessi (ACL).
- **Contesto Reale:** In azienda, nessun dispositivo viene collegato direttamente a Internet senza un firewall intermedio. È il punto in cui si definisce "chi può parlare con chi" (es. il reparto Marketing non può accedere al database della contabilità).

5. ⚠️ Focus Esame

- **Domanda frequente:** Il firewall può bloccare *tutti* gli attacchi? No, il firewall tradizionale non vede bene dentro il traffico crittografato (senza decifrazione SSL) e non protegge da attacchi interni (Insider Threat) se non c'è segmentazione interna.

Componenti Architettureali del Firewall

1. 📖 Spiegazione Approfondita

Indipendentemente dal form factor (hardware o software), ogni firewall moderno si basa su tre componenti logici fondamentali:

1. **Motore di Ispezione del Traffico (Inspection Engine):** È il "cuore" del sistema. Analizza i dati grezzi. Le sue capacità determinano la potenza del firewall:
 - *Ispezione dei pacchetti (Stateless):* Legge solo l'intestazione (Header) IP/TCP/UDP (IP sorgente, destinazione, porta). Non ricorda il passato.
 - *Stateful Inspection:* Mantiene una tabella di stato (*State Table*). Sa se un pacchetto fa parte di una connessione già stabilita (es. la risposta di un server web a una nostra richiesta).

- **Deep Packet Inspection (DPI):** Esamina il *payload* (il contenuto vero e proprio) del pacchetto per trovare malware, firme di virus o dati sensibili, andando oltre le semplici intestazioni.

2. **Interfaccia di Gestione (Management Interface):** La console (GUI web, CLI o software dedicato) usata dall'amministratore per configurare regole, visualizzare log in tempo reale (monitoring) e generare reportistica.

3. **Database delle Regole (Rulebase):** L'archivio dove sono scritte le policy. Il motore interroga questo database per ogni pacchetto processato.

3. 🧠 Analisi Tecnica & Memorizzazione

- **Definizione Chiave:** La **State Table** (Tabella di Stato) è ciò che differenzia un firewall moderno da un router con semplici ACL. Memorizza lo stato della connessione (SYN, SYN-ACK, ESTABLISHED, FIN).
- **Contesto Reale:** Senza Stateful Inspection, bisognerebbe aprire manualmente tutte le porte effimere (alte) per permettere il traffico di ritorno, creando enormi buchi di sicurezza.

Logica di Filtraggio e "Top-Down Approach"

1. 📖 Spiegazione Approfondita

Il funzionamento decisionale del firewall si basa sul confronto dei pacchetti con il **Database delle Regole**. Questo processo segue rigorosamente un approccio sequenziale **Top-Down** (dall'alto verso il basso):

1. Il pacchetto arriva al firewall.
2. Il firewall legge la **Regola 1**. Se il pacchetto corrisponde ai criteri (Match), viene eseguita l'azione (es. ACCEPT o DROP) e l'analisi **si ferma**.
3. Se non corrisponde, passa alla **Regola 2**, e così via.
4. **Implicit Deny (Regola di Default):** Se il pacchetto scorre tutte le regole senza trovare corrispondenza, viene scartato dall'ultima regola invisibile, che è sempre un "Deny All" o "Drop All".

Le regole definiscono tipicamente:

- **Sorgente (Source):** IP, Subnet o Utente.
- **Destinazione (Destination):** IP, Server o FQDN (es. google.com).
- **Servizio/Porta:** TCP/80 (HTTP), TCP/22 (SSH), ecc.
- **Azione:**
 - **Allow/Accept:** Lascia passare.
 - **Drop:** Scarta il pacchetto silenziosamente (l'emittente non riceve nulla, simulando un "buco nero").
 - **Deny/Reject:** Scarta il pacchetto inviando un errore al mittente (es. ICMP Destination Unreachable o TCP RST).

3. 🧠 Analisi Tecnica & Memorizzazione

- **Definizione Chiave: Best Practice dell'Ordine:** Le regole più specifiche (es. "L'host A può accedere al Server B sulla porta 80") devono essere messe **PRIMA** delle regole generali (es. "Tutta la rete può navigare su Internet").

- **Contesto Reale:** Un errore comune è mettere una regola "Block All" prima di una regola "Allow HTTP". Risultato: nessuno naviga, perché il firewall si ferma alla prima corrispondenza.

5. 🚩 Focus Esame

- **Trabocchetto:** "Cosa succede se un pacchetto non matcha nessuna regola scritta dall'admin?" -> Viene bloccato dalla **Implicit Deny** finale.

Tipologie Avanzate: WAF, Proxy e NGFW

1. 📖 Spiegazione Approfondita

Oltre al firewall di rete standard, esistono tipologie specializzate:

- **WAF (Web Application Firewall):** Opera a livello 7 (Applicazione) del modello ISO/OSI. Non guarda solo porte e IP, ma analizza il traffico HTTP/HTTPS. Protegge specificamente le applicazioni web da attacchi come **SQL Injection**, **XSS (Cross-Site Scripting)** e **File Inclusion**.
 - *Esempio:* Se un utente prova a caricare un file **.php** (potenziale webshell) in un modulo di upload immagini, il firewall di rete lo lascerebbe passare (è traffico HTTP lecito), ma il WAF lo blocca analizzando il contenuto.
- **Proxy Server:** Agisce come intermediario. Interrompe la connessione diretta tra client e server.
 - **Forward Proxy:** Usato dai client interni per uscire su Internet (nasconde l'IP del client, fa caching, filtra contenuti).
 - **Reverse Proxy:** Si posiziona davanti ai server web aziendali. Protegge i server, fa bilanciamento del carico (Load Balancing) e offloading SSL.
- **NGFW (Next-Generation Firewall):** È l'evoluzione moderna che unifica tutto in un solo dispositivo. Include: Firewall stateful + IPS/IDS + Controllo Applicativo (riconosce "Facebook" non solo come traffico porta 80, ma come app) + VPN + Antimalware + Threat Intelligence.

3. 🧠 Analisi Tecnica & Memorizzazione

- **Definizione Chiave:** Il **Reverse Proxy** protegge i server nascondendoli all'esterno; il **Forward Proxy** protegge i client nascondendoli al server di destinazione.
- **Contesto Reale:** Per soddisfare lo standard PCI-DSS (pagamenti con carta di credito), l'uso di un WAF davanti ai server di e-commerce è praticamente obbligatorio.

IDS vs IPS (Intrusion Detection/Prevention System)

1. 📖 Spiegazione Approfondita

Questi sistemi sono specializzati nell'individuare pattern di attacco complessi che un semplice firewall a regole statiche non vedrebbe.

- **IDS (Intrusion Detection System):** È un sistema di monitoraggio **passivo**. Ascolta il traffico (spesso tramite una porta SPAN/Mirror dello switch), rileva un attacco e genera un **allarme** (log/email). **NON**

ferma l'attacco direttamente.

- **Modalità: NIDS** (Network-based, analizza i pacchetti sulla rete) o **HIDS** (Host-based, installato sul singolo server, analizza log e integrità file).
- **IPS (Intrusion Prevention System):** È un sistema **attivo**. È posizionato "in-line" (in linea) sul cavo di rete. Il traffico deve attraversarlo. Se rileva un attacco, lo **blocca** istantaneamente scartando i pacchetti.

Tecniche di Rilevamento:

1. **Signature-based (Pattern Matching):** Confronta il traffico con un database di "firme" di attacchi noti. Preciso, pochi falsi positivi, ma cieco contro attacchi nuovi (Zero-Day).
2. **Anomaly-based (Comportamentale):** Crea un profilo "normale" della rete (baseline). Se il traffico devia dalla norma (es. picco di traffico alle 3 di notte), scatta l'allarme. Rileva Zero-Day, ma genera molti falsi positivi.

3. 🧠 Analisi Tecnica & Memorizzazione

- **Definizione Chiave:** La differenza sostanziale è l'azione. IDS = "Telecamera di sorveglianza" (registra il ladro ma non lo ferma). IPS = "Guardia armata" (interviene fisicamente).
- **Contesto Reale:** Si inizia spesso con un IDS in modalità "promiscua" per capire il traffico senza bloccare servizi legittimi (tuning), per poi passarlo a IPS (blocking) una volta stabilizzati i falsi positivi.

4. 🔗 Cross-Connection Master

- **Integrazione SIEM:** Sia IDS che IPS inviano i loro log a un SIEM (Security Information and Event Management) per la correlazione degli eventi.

Segmentazione di Rete & Zoning

1. 📖 Spiegazione Approfondita

La segmentazione è la pratica di dividere una rete piatta in sottoreti (subnet) isolate logicamente o fisicamente, controllate da firewall. Questo limita il "movimento laterale" degli attaccanti.

Zone tipiche:

- **LAN (Intranet):** Zona ad alta fiducia (PC dipendenti).
- **DMZ (Demilitarized Zone):** Zona a fiducia intermedia esposta verso Internet. Contiene i servizi pubblici (Server Web, Mail, DNS). **Regola d'oro:** Internet può accedere alla DMZ. La DMZ *non* dovrebbe poter accedere liberamente alla LAN interna.
- **Server Farm / Applicativi Critici:** Zona ad altissima sicurezza (Database), accessibile solo dai server della DMZ o dagli amministratori, mai direttamente da Internet.

5. ⚠️ Focus Esame

- **Concetto critico:** Se un server web nella DMZ viene compromesso, l'hacker si trova isolato nella DMZ e non ha accesso diretto ai PC degli impiegati o al database interno (se le regole del firewall sono corrette).

Strumento Pratico: iptables (Linux Firewall)

1. 📖 Spiegazione Approfondita

iptables è lo strumento storico da riga di comando per gestire il firewall integrato nel kernel Linux (Netfilter). Funziona tramite **Catene (Chains)**:

- **INPUT:** Controlla i pacchetti destinati al computer stesso (in entrata).
- **OUTPUT:** Controlla i pacchetti generati dal computer stesso (in uscita).
- **FORWARD:** Controlla i pacchetti che attraversano il computer (se funge da router/gateway).

2. ✂ Sintassi & Comandi (Cleaning)

Ecco i comandi corretti e standardizzati per l'uso di iptables (spesso soggetti a errori OCR):

- **Visualizzare le regole esistenti:**

```
sudo iptables -L -v -n
```

- **-L:** List (elenca).
- **-v:** Verbose (dettagli).
- **-n:** Numeric (mostra IP e porte numeriche senza risolvere i nomi DNS, più veloce).

- **Aggiungere una regola (Append):**

```
sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT
```

- **-A INPUT:** Aggiungi in coda alla catena INPUT.
- **-p tcp:** Protocollo TCP.
- **--dport 22:** Porta di destinazione 22 (SSH).
- **-j ACCEPT:** Jump to Action (Azione: Accetta).

- **Bloccare un IP specifico:**

```
sudo iptables -A INPUT -s 192.168.1.50 -j DROP
```

- **-s:** Source (sorgente).

- **Policy di Default (Importante!):**

```
sudo iptables -P INPUT DROP
```

- Imposta la politica di default a DROP (tutto ciò che non è esplicitamente permesso viene bloccato). **Attenzione:** Farlo solo dopo aver permesso SSH, altrimenti ci si chiude fuori!

5. ⚠ Focus Esame

- **Ordine delle regole:** **iptables** legge le regole in ordine sequenziale. Se usi **-A** (Append), la regola va in fondo. Se vuoi inserirla in cima, devi usare **-I** (Insert).

1. 📖 Spiegazione Approfondita

PfSense è una distribuzione firewall open-source basata su **FreeBSD**. È estremamente popolare perché offre funzionalità di livello enterprise (NGFW) gratuitamente. Si gestisce interamente tramite interfaccia Web (WebGUI), rendendolo più accessibile rispetto a **iptables**.

Processo di Installazione e Setup:

1. **VM Setup:** Richiede solitamente due schede di rete virtuali:
 - Adapter 1: **NAT** o **Bridged** (simula l'interfaccia WAN, connessa a Internet).
 - Adapter 2: **Internal Network** (simula l'interfaccia LAN, dove collegheremo i client da proteggere).
2. **Configurazione IP:** Durante il boot, PfSense rileva le interfacce. L'interfaccia LAN ha di default IP **192.168.1.1**.
3. **Accesso Web:** Da un client nella rete interna, si apre il browser all'indirizzo del gateway PfSense.
4. **Wizard:** Si configura hostname, DNS, e si cambiano le password di default (admin/pfsense).

3. 🧠 Analisi Tecnica & Memorizzazione

- **Contesto Reale:** PfSense è usato non solo per firewalling, ma spesso come router di bordo, terminatore VPN e Load Balancer in piccole e medie imprese (PMI).
- **Sicurezza di Default:** Appena installato, PfSense blocca tutto il traffico in ingresso sulla WAN (nessuno entra) e permette tutto il traffico in uscita dalla LAN (tutti escono).

5. ⚠️ Focus Esame

- **Scenario Lab:** Se installi PfSense su VirtualBox e non riesci ad accedere alla WebGUI, verifica che il client sia nella stessa "Rete Interna" dell'interfaccia LAN del firewall e che abbia ricevuto un IP via DHCP (PfSense ha un server DHCP attivo di default sulla LAN).