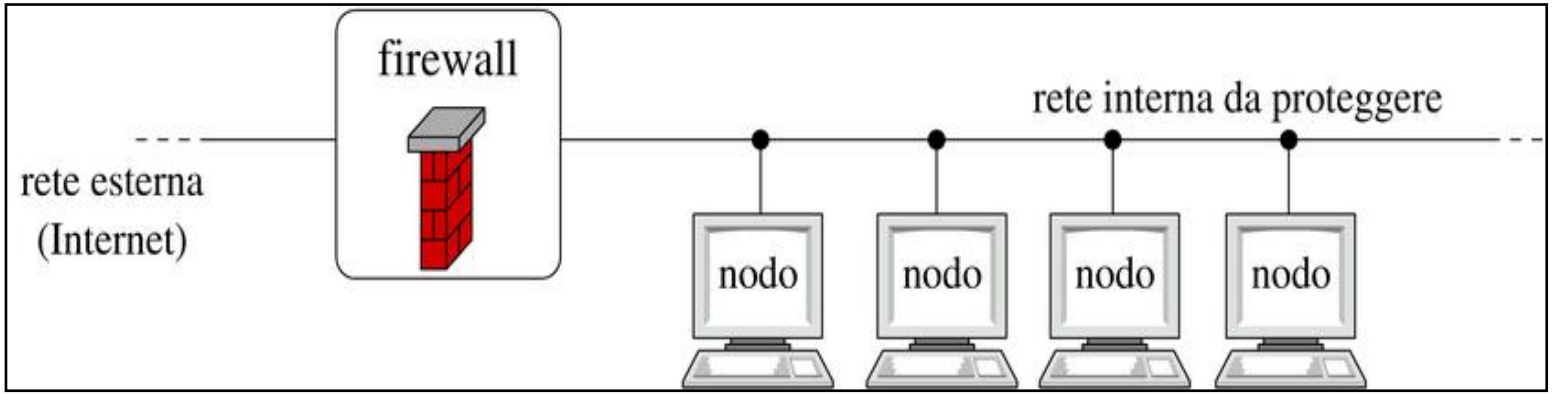
PARTE 8

Elementi di Sicurezza Informatica per reti di calcolatori

Modulo 2 – Firewall

Firewall

- **Il firewall è un dispositivo di sicurezza che si interpone tra due reti diverse per controllare e limitare il traffico**




Muraglia cinese:
Difesa perimetrale

Principi di firewalling

- **Il firewall deve essere l'unico punto di contatto tra la rete esterna e la rete interna**
- **Solo il traffico autorizzato o non vietato deve riuscire ad attraversare il firewall**
- **Il firewall deve essere, a sua volta, un sistema sicuro e tenuto sempre sotto controllo**

Unico punto di contatto

L'errore comune (pubblicità?)

- **"Compra un network appliance con tutte le funzioni (firewall, router, NAT) e così proteggi la tua organizzazione"**
- **In realtà, si comprano i componenti del firewall, ma non il firewall che invece richiede:**

  - Progetto delle regole sulla base di:
    - policy aziendali
    - scelte tecniche di sicurezza
  - Implementazione delle regole

Politiche per la sicurezza di rete

- **Le politiche si definiscono mediante Access Control List (ACL):**
  - quali servizi devono essere esplicitamente consentiti o proibiti
  - come devono essere utilizzati e da chi
  - eventuali eccezioni alle regole precedenti
- **Le ACL possono contenere migliaia di regole**

- **Due politiche contrapposte:**
  - Negazione implicita: “Non passa niente tranne ciò che è stato espressamente autorizzato”
  - Accesso implicito: “Passa tutto ciò che non è stato espressamente vietato”

Negazione implicita

- **“Tutto ciò che non è esplicitamente permesso è implicitamente proibito”**

- **Solo il traffico esplicitamente autorizzato può attraversare il firewall. Tutto il traffico non esplicitamente autorizzato viene bloccato.**
  - È il metodo più sicuro di firewalling
  - Dal punto di vista degli utenti è molto restrittivo
  - E’ più difficile da gestire

- **Favorisce la sicurezza rispetto all’usabilità**

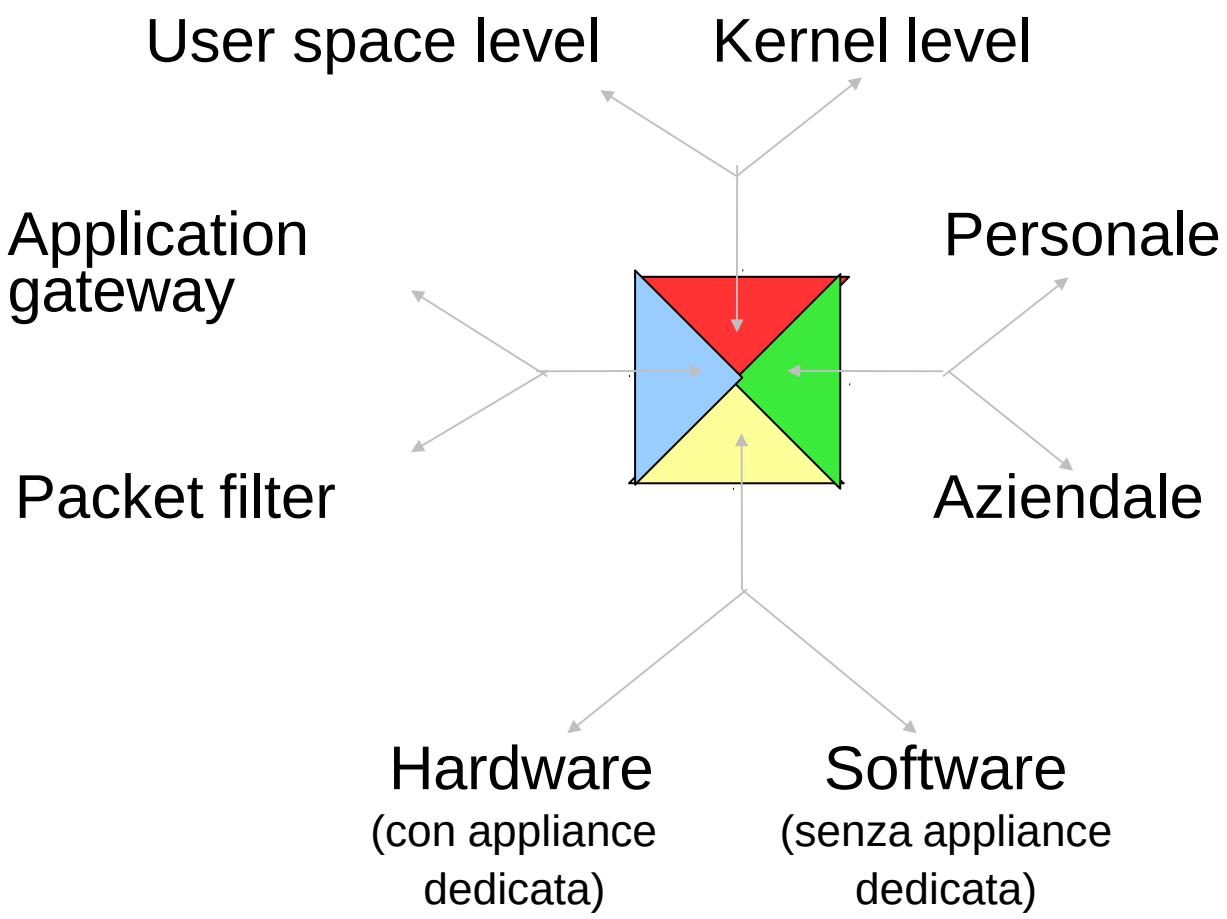
Accesso implicito

- **“Tutto ciò che non è esplicitamente proibito è implicitamente consentito”**

- **Solo il traffico esplicitamente vietato viene bloccato dal firewall. Tutto il traffico non vietato esplicitamente può attraversare il firewall:**
  - Garantisce la massima usabilità della rete
  - E’ più facile da gestire
  - Espone la rete a rischi di sicurezza

- **Favorisce l’usabilità rispetto alla sicurezza**

Tassonomia dei firewall



Tassonomia dei Firewall

- **Livello di esecuzione**
  - Kernel level: controlli a livello 3 e 4 (supporto a livello applicazione assente o solo parziale)
  - User space level: controlli a livello applicazione
- **Ambito di azione**
  - Personale (personal firewall installato su PC. Es., ZoneAlarm, Norton personal firewall, ...)
  - Aziendale (installato su rete)
- **Realizzazione**
  - Hardware (appliance, possibilmente integrato con altre funzioni, quali routing, natting, patting, ecc.)
  - Software (ad esempio, le distribuzioni Linux con netfilter/iptables mettono a disposizione funzionalità di packet filtering oltre che di NAT/PAT)

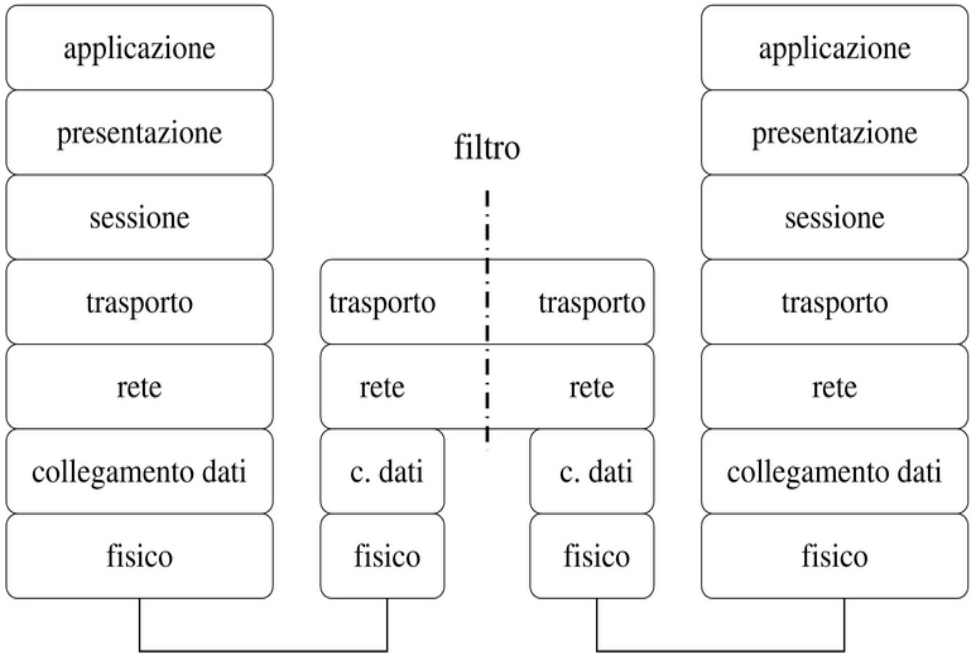
Firewall: funzionalità

- **Si possono identificare due tipologie principali di firewall sulla base delle funzionalità offerte:**
- **Packet filter**
- **Application gateway (Proxy firewall) ← Non trattato**

Filtri di pacchetto

Packet filter

- **Il firewall packet filter agisce a livello 3 (packet filter vero e proprio) e a livello 4 (circuit gateway) dello stack TCP/IP**



Packet filter

- **Bloccano o lasciano passare il traffico che attraversa il firewall definendo i protocolli, gli indirizzi IP e le porte che si possono o non possono utilizzare**

- **Spesso viene completato da funzionalità di routing (router firewall) per permettere l'instradamento dei pacchetti accettati all'interno della rete**

- **Quando un pacchetto arriva al packet filter, il firewall estrae alcune informazioni dall'header e, in base alle regole definite, o lo inoltra o lo scarta**

Packet Filter

- **Informazioni comunemente utilizzate:**
  - interfaccia di ingresso dei pacchetti interfaccia di uscita dei pacchetti protocolli di livello 3 (IP, ARP, OSPF, ...)
  - valori dell'header dei protocolli di livello 3 (indirizzi IP, tipo di messaggio ICMP, ...)
  - protocolli di livello 4 (TCP, UDP, SCTP, ...)
  - valori dell'header dei protocolli di livello 4 (numeri di porta, valori dei flag, ...)

Packet Filter

- **Due tecniche di filtraggio dei pacchetti:**

- **Static Packet Filtering**
  - la prima tecnica ad essere implementata
  - considera i singoli pacchetti come entità individuali, non correlate tra loro

- **Stateful Packet Filtering (o Inspection)**
  - capace di esaminare i gruppi di pacchetti correlati tra loro (es. pacchetti appartenenti alla stessa connessione)

Static Packet Filter

- **È realizzato mediante una lista di regole**
  - Ogni regola è composta da una espressione di confronto, seguita da un'azione
  - L'espressione di confronto ed è utilizzata per identificare i pacchetti che rispondono a certe descrizioni
  - Le espressioni di confronto considerano solo le informazioni contenute negli header dei pacchetti
  - Possibili azioni: Accetta – Rifiuta – Ignora – Log
  - Esempio di firewall con static packet filter: ipchains
  - (prima di iptables)

Static Packet Filter - vantaggi

- **Tutti i pacchetti vengono analizzati come unità di informazione non correlate tra loro**

- **Vantaggi**
  - Basso costo computazionale e economico
  - Non richiede il mantenimento di informazioni di stato Semplice da implementare e gestire
  - Ottima scalabilità (facilmente parallelizzabile)
- **Basso costo computazionale e economico**
- **Non richiede il mantenimento di informazioni di stato Semplice da implementare e gestire**
- **Ottima scalabilità (facilmente parallelizzabile)**

Static Packet Filter - svantaggi

- **Svantaggi**
  - Non è in grado di riconoscere pacchetti appartenenti ad una connessione già aperta (ESTABLISHED)
  - Non è in grado di riconoscere pacchetti correlati ad una connessione già aperta (RELATED)
  - Occorre aprire numerosi “buchi” nel firewall per garantire una comunicazione bidirezionale valida per tutti i protocolli

Static Packet Filter - esempio

- **Un client (rete interna) stabilisce una connessione ad un server esterno**

- **Client invia pacchetti alla porta 80 di Server**
- **Server risponde con pacchetti a una porta effimera di Client (1024 < numero porta < 65535)**

- **Occorre abilitare traffico in ingresso verso tutte le porte effimere dei client nella rete protetta**

Stateful Packet Filter

- **Conosciuto anche come Dynamic Packet Filtering**
- **Analizza gli header di livello 3 e 4, non analizza header/payload a livello applicazione**
- **La dinamicità consiste nella capacità di:**
  - distinguere le connessioni già aperte da quelle nuove
  - mantenere tabelle di stato con le informazioni relative alle connessioni attive
  - adattare dinamicamente le regole utilizzate per il filtraggio in base alle informazioni di stato
- **Es., iptables (+ CONNTRACK)**

Stateful Packet Filter - vantaggi

- **Riconosce pacchetti appartenenti ad una connessione già aperta (ESTABLISHED)**
- **Le risposte provenienti dall'esterno a connessioni legittime vengono autorizzate da regole temporanee, istanziate dinamicamente e automaticamente**
- **Le regole temporanee sono attive solo per il tempo strettamente necessario (durata della connesione + timeout)**
- **Non è necessario aprire "buchi" permanenti Più resistente al firewalking**

Stateful Packet Filter - esempio

- **Un client (rete interna) stabilisce una connessione ad un server esterno**
  - Firewall rileva un TCP three-way-handshake completo tra Client e Server (una nuova connessione è stata aperta)
  - Firewall aggiunge regole temporanee che consentono il passaggio ai pacchetti appartenenti alla connessione aperta (ESTABLISHED)
- **Non occorre abilitare esplicitamente traffico in ingresso verso porte effimere dei client nella rete protetta**

Stateful Packet Filter - svantaggi

- **Non è in grado di riconoscere pacchetti correlati ad una connessione già aperta (RELATED)**

  → problemi con i protocolli che si discostano dal paradigma client/server (es: FTP)

- **Richiede maggiori quantità di memoria per mantenere informazioni relative alle connessioni**

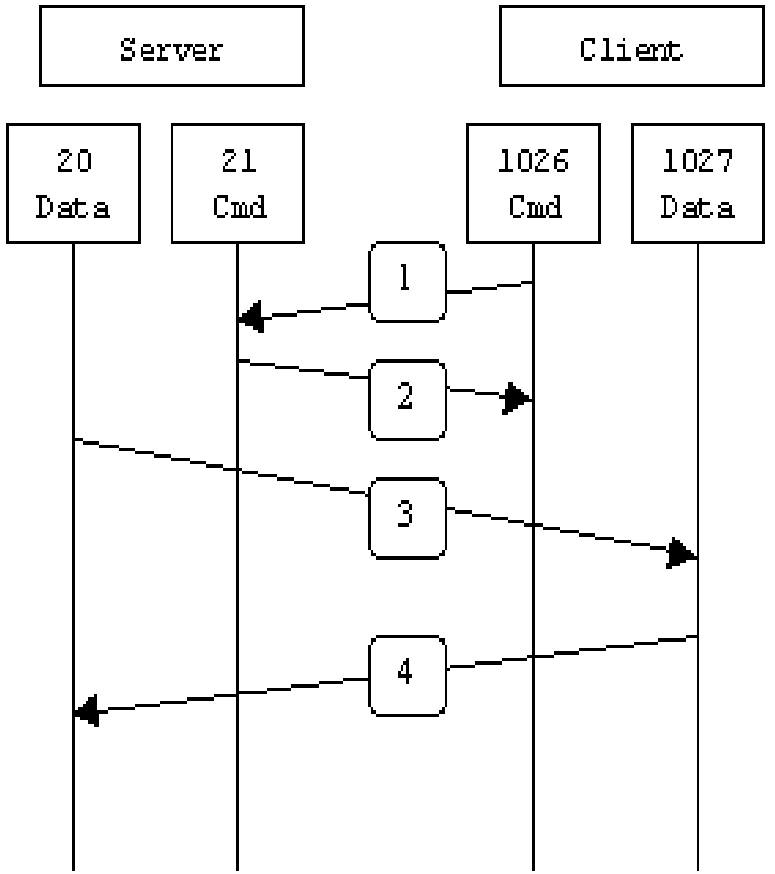
- **Richiede maggiore capacità computazionale**

  → rischio di attacchi DoS

  → difficile parallelizzazione

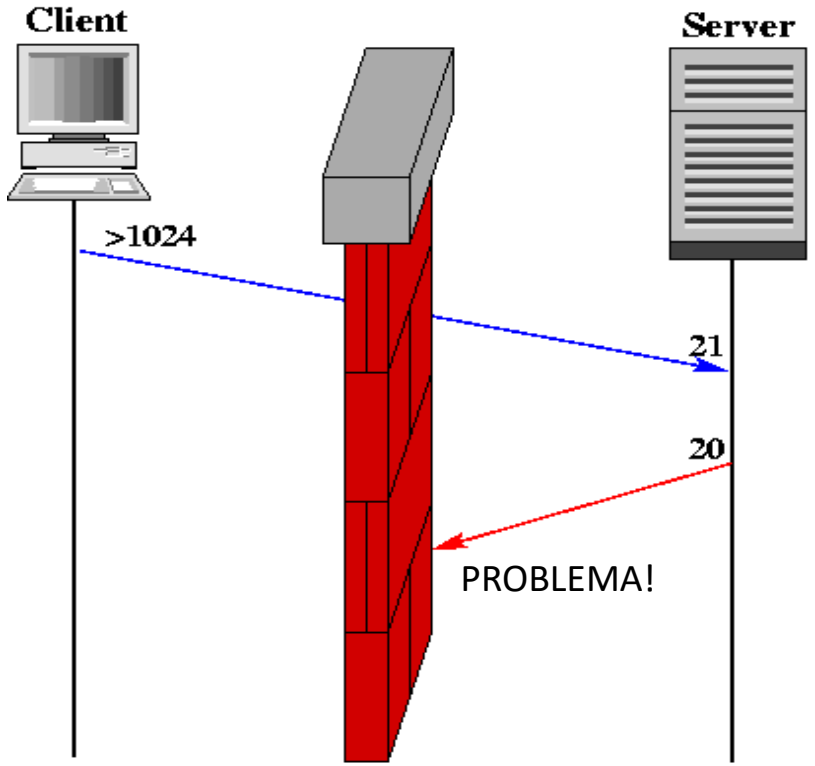
Stateful Packet Filter – esempio FTP

- **FTP Active**
  - 1,2: il client inizia la connessione di controllo sulla porta 21 del server. In questa connessione trasmette il comando PORT N
  - 3,4: il server inizia la connessione dati sulla porta N del client
  - la seconda connessione è correlata (RELATED) a traffico autorizzato



Stateful packet filter – esempio FTP

- **Politica**
  - Negazione implicita (blocca il traffico non esplicitamente autorizzato)
  - Autorizza connessioni iniziate dalla rete interna
  - Autorizza (dinamicamente) risposte a connessioni iniziate dalla rete interna



Stateful Packet Filter + Ispezione del payload

- **Ulteriore evoluzione dell'analisi stateful**
- **I pacchetti non vengono valutati solo sulla base dei suoi header, ma anche sulla base dei dati del payload del pacchetto**
- **Es., IPTables + CONNTRACK + moduli applicazioni**

- **Consente di interpretare i comandi di livello applicativo contenuti nel payload dei pacchetti di livello 4 (es., il comando PORT del protocollo FTP)**
- **Questa funzione, tuttavia, non implica l'analisi completa del protocollo applicativo!**

Stateful Packet Filter + Ispezione del payload

- **Vantaggi**
  - Riconosce anche pacchetti correlati ad una connessione già aperta (RELATED)
  - Il traffico correlato a connessioni legittime viene autorizzate da regole temporanee
  - Gestione efficace e sicura di protocolli complessi

- **Svantaggi**
  - Ulteriore appesantimento dell'onere computazionale (pattern matching sul payload dei pacchetti)