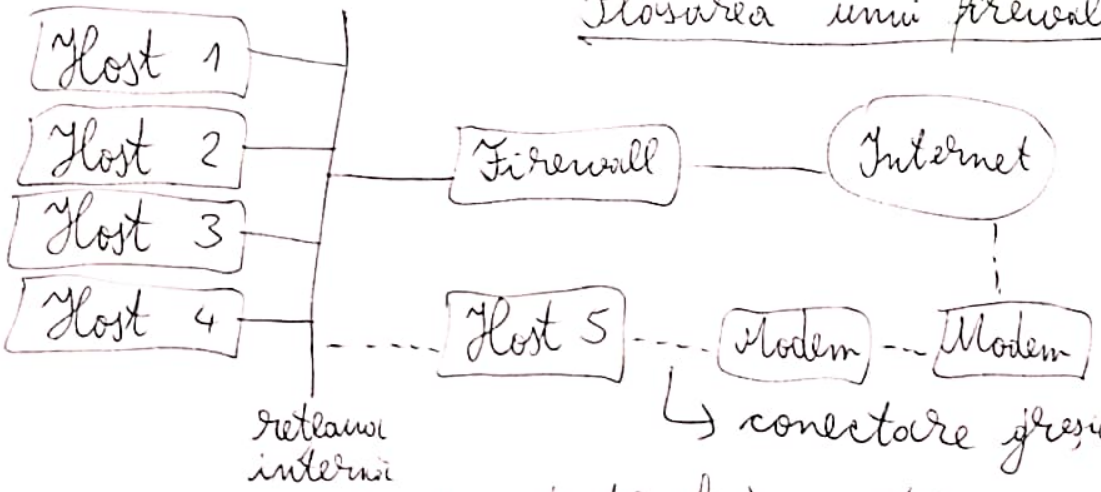
C14

Firewall

- ansamblu de componente hardware și soft care se interpune între două rețele pt. a restrânge și controla traficul între ele.

Plasarea unui firewall

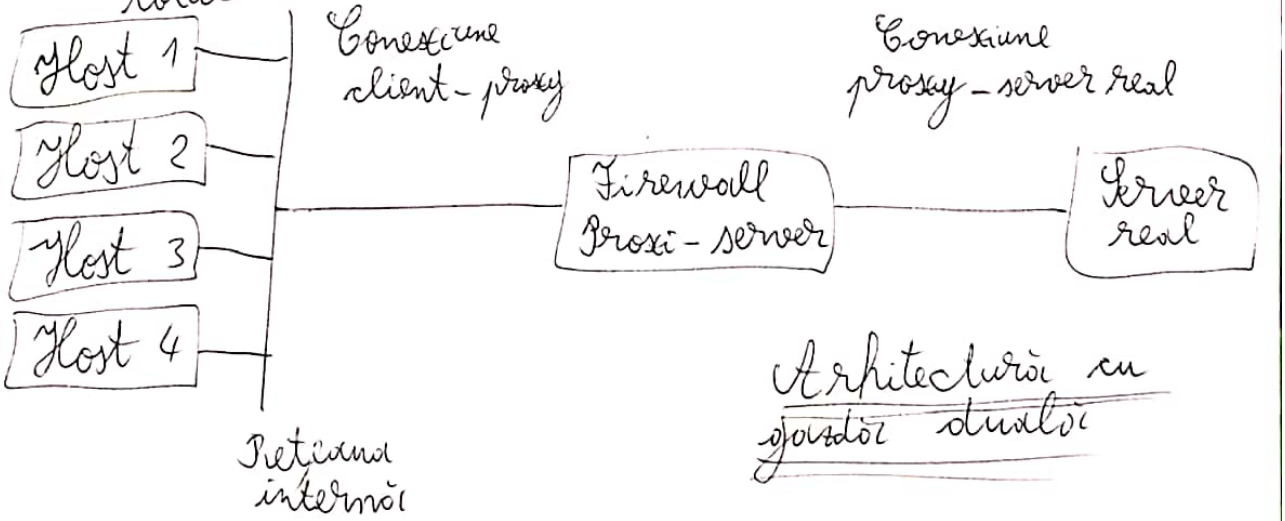


- sniffer (analizator de trafic) monitorizează date confidențiale și parole.
- servicii de securitate:
  - acces controlat la/de la gazdele interne și externe.
  - filtrarea protocoalelor.
  - autentificare centralizată.
  - monitorizarea rețelei.

- principii de bază:
  - filtrarea pachetelor
  - sisteme proxy.
- filtrarea pachetelor (packet filtering) este realizată prin intermediul unei componente a firewall-ului numită router protector (screening router).
- avantajul filtrării de pachete: transparența sa.

Servicii Proxy

- proxy-server = program care rulează pe o mașină, componentă a firewall-ului numită gazdă bastion, datorită rolului de „portăreață" pe care îl îndeplinește în apărarea rețelei.
- lucrează la nivelul aplicației.
- gazda bastion = gateway.
- comunicația:
  1. clientul emite cererea către proxy-server
  2. proxy-serverul analizează cererea, și dacă este totul ok, o trimite serverului real.
  3. serverul răspunde cererii cu un răspuns către proxy
  4. proxy-serverul analizează răspunsul, și dacă este totul ok, o trimite clientului.



Arhitectură cu gazdă dual

- avantaje.
  - autentificare.
  - filtrarea individuală.
  - monitorizarea.
- dezavantaje: prin existența a 2 conexiuni se modifică procedura de utilizare a serviciilor, iar pt. fiecare protocol care trb. inspectat trb. să existe un proxy-server diferit.

C14

Arhitectura cu subrețea protejată (screened subnet)

- DMZ (Demilitarized Zone) = zonă din jurul firewall-ului în care sunt situate calculatoarele pe care sunt scrise/instalate serverele cu caracter public.

Linux

- IPChains → setare, menținere și inspectare reguli de firewall din nucleul Linux.
  - IP input chain
  - IP output chain
  - IP forwarding chain
  ] built-in
  - chain-uri definite de utilizator.
- cuvinte rezervate: ACCEPT, DENY, REJECT, MASQ, REDIRECT și RETURN (pt. starea unui pachet).
- argumentul "!" înaintea adresei inversează sensul adr. IP
- chain-urile input, output și forward sunt predefinite și nu pot fi șterse. Regulile se pot adăuga și se pot șterge din oricare chain. Operații: creare/ștergere chain, schimbare politică chain, golire chain, etc.