5. Sisteme Firewall

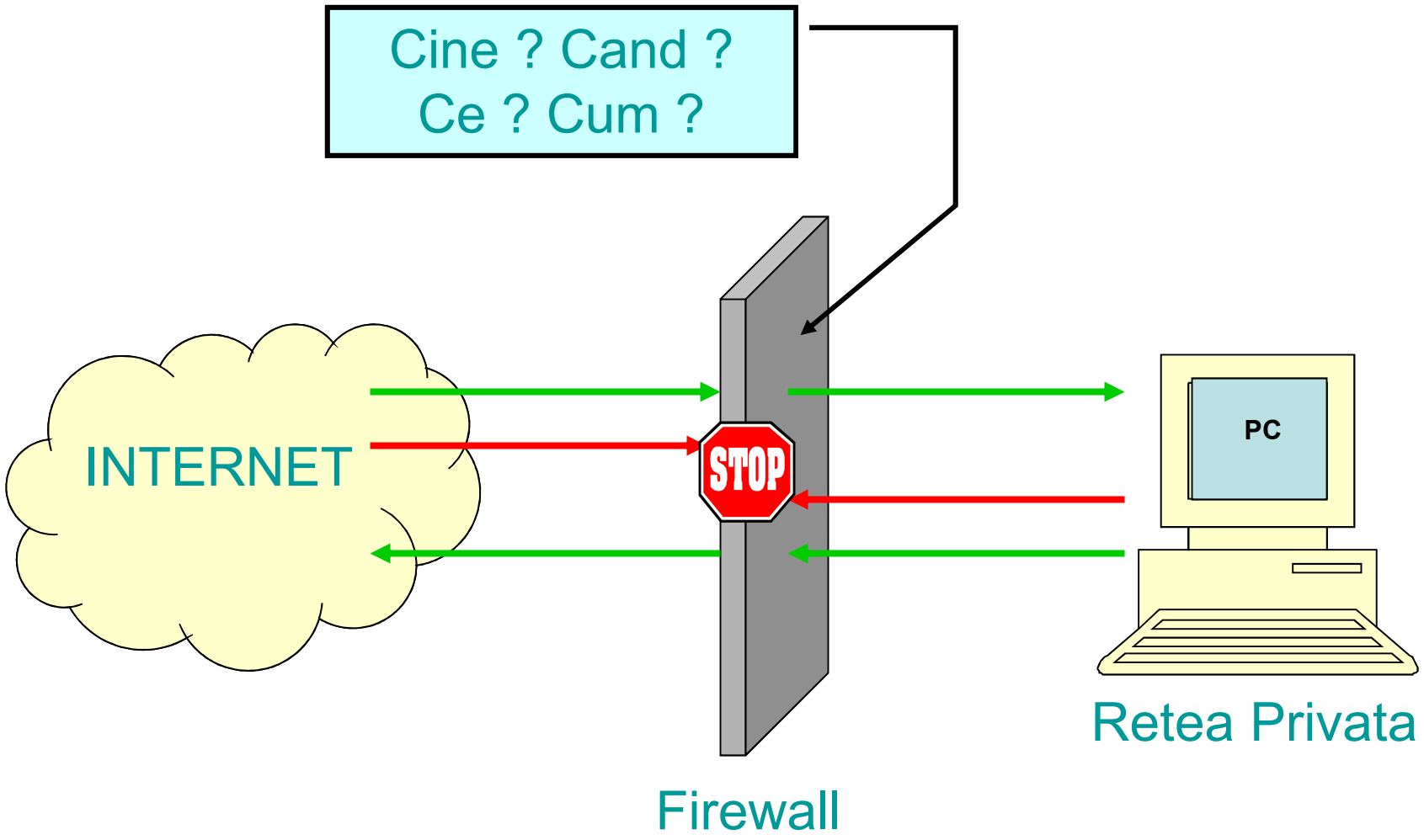
Sisteme Firewall

- Conectarea la Internet este o cerinţă de business pentru aproape toate organizaţiile
- Un calculator conectat direct la Internet este o ţintă posibilă pentru atacatori
- Orice disfuncţionalitate a sistemelor de calcul costă bani (direct sau indirect)
- Sunt necesare mecanisme de protecţie a reţelelor interne împotriva atacurilor externe

Rolul unui firewall

- O manifestare fizică a politicii de securitate în retea
- Punct de control şi monitorizare a traficului, între două reţele
- Mecanism pentru limitarea accesului la resursele/serviciile reţelei interne
- Similar unui “zid de apărare“

Rolul unui firewall (cont.)



Cerinţe pe care trebuie să le satisfacă un firewall

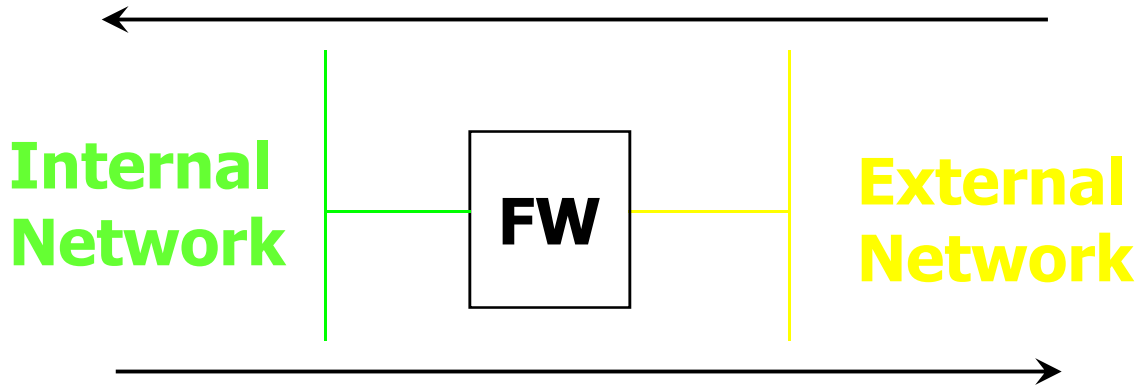
1. Tot traficul din interior spre exterior şi vice versa, trebuie să treacă prin firewall
   - nu trebuie să existe puncte de acces în reţea necontrolate (backdoors)
2. Numai traficul autorizat, stabilit prin politica de securitate internă, poate să treacă prin firewall
   - reguli de acces stricte
3. Firewall-ul însuşi trebuie să fie imun la atacuri. Aceasta presupune folosirea unui sistem de încredere care a fost supus în prealabil unui proces de securizare (hardening)
   - maşini dedicate pe care nu trebuie să mai ruleze alte servicii

Terminologie

- **Pachet** – unitatea de informaţie creată de un protocol de reţea, pentru a transporta date şi informaţii de control. În contextul stivei TCP/IP se mai numeşte şi datagramă.
- **DMZ (DeMilitarized Zone)** – un segment de reţea dispus între exterior (o reţea neprotejată, Internet) şi reţeaua internă (protejată), având rolul de a intermedia schimbul de informaţii. Este reţeaua în care, de regula, sunt dispuse serviciile publice şi gateway-urile de aplicaţie.
- Reţele protejate şi neprotejate
  - **Reţelele protejate** sunt localizate în spatele unui firewall, fiind protejate prin politicile acestuia
  - **Reţelele neprotejate**, cum ar fi Internet-ul, stau în fata unui firewall şi nu sunt protejate de către politicile acestuia
- Direcţii ale traficului
  - **Inbound** = spre interiorul zonei protejate de firewall
  - **Outbound** = spre exteriorul zonei protejate de firewall

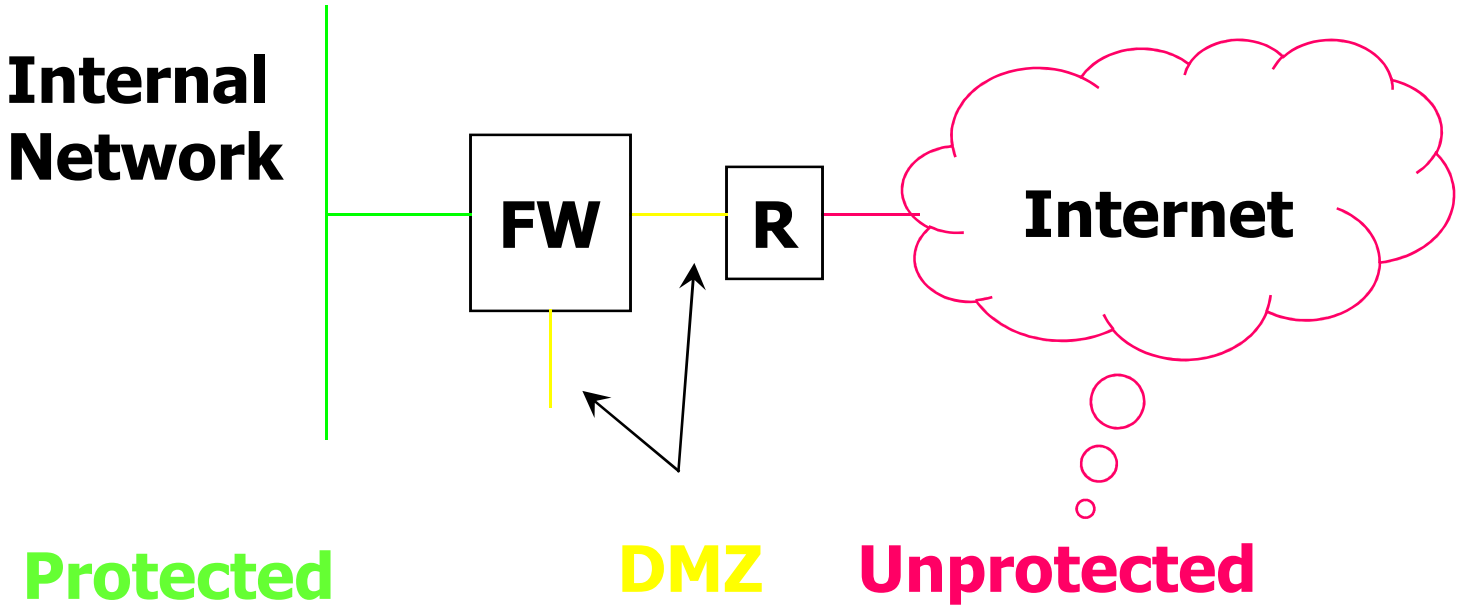
Terminologie (cont.)

- **Inbound sau Outbound**
  - **Inbound** = spre interiorul zonei protejate de firewall

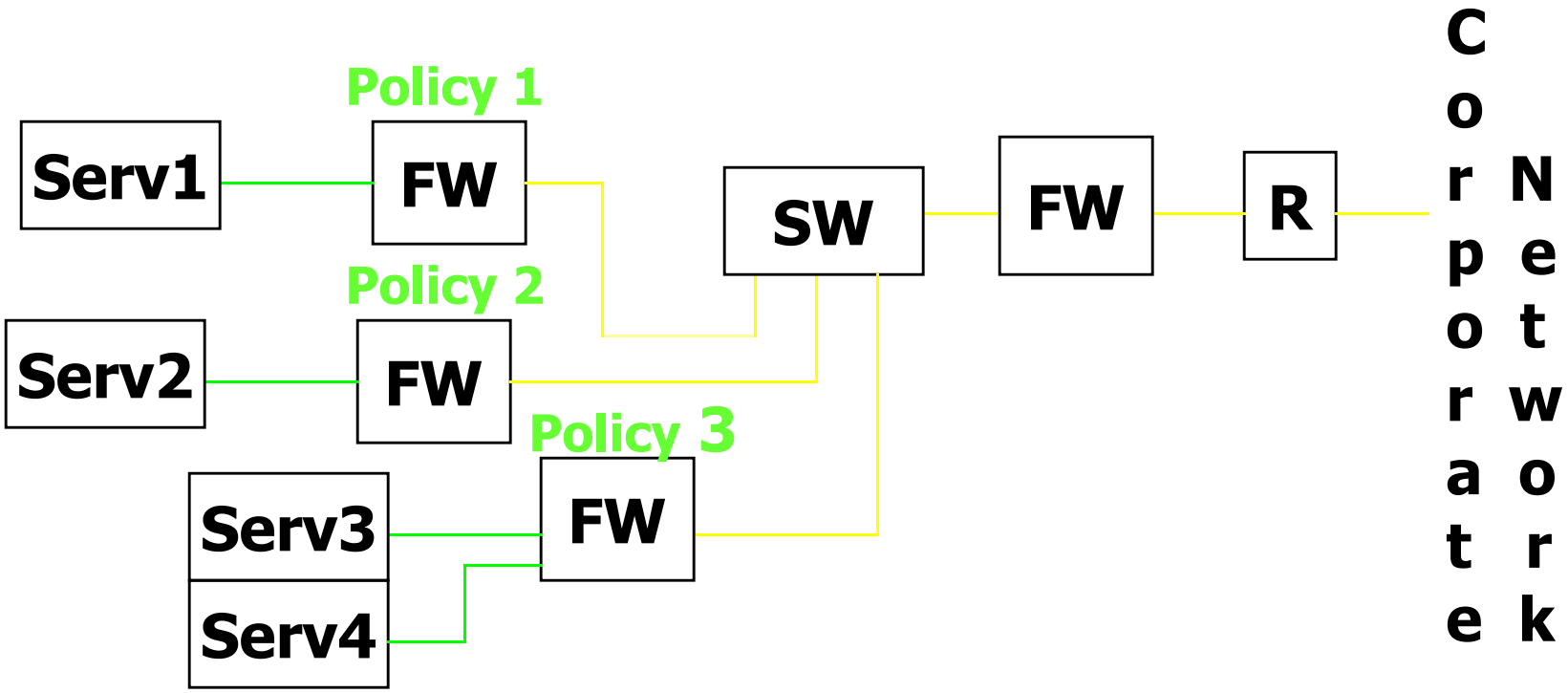


  - **Outbound** = spre exteriorul zonei protejate de firewall

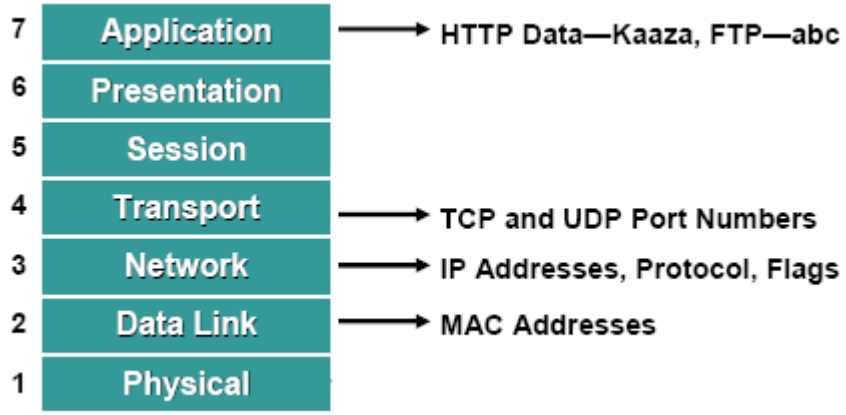
Exemplu de firewall



Exemplu de firewall (cont.)



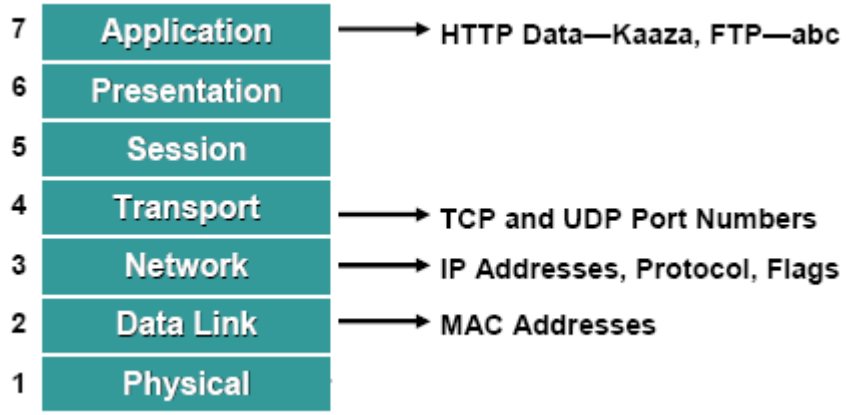
Parametri de control al accesului



Exemple de politici (reguli):

- **La nivel legatură de date**
  - **Interzice toate pachetele de la adresa MAC 00-1c-bf-01-02-03**
  - **Nu cere autentificarea daca adresa MAC este 00-1c-2b-aa-bb-cc**
- **La nivel reţea**
  - **Interzice orice trafic, cu excepţia pachetelor de ieşire ce vin de la reţeaua 10.10.10.0/24**
  - **Permite numai trafic ESP (IPsec)**
  - **Interzice orice trafic, cu excepţia traficului de la reţeaua 172.16.30.0/24, spre reţeaua 192.168.10.0/24**

Parametri de control al accesului (cont.)



Exemple de politici (reguli):

- **La nivel transport**
  - **Permite traficul de Web de oriunde (inclusiv Internet), cu condiţia ca adresa destinaţie să fie a serverului propriu – 192.168.0.10**
  - **Permite traficul FTP de oriunde, spre propriul server – 192.168.0.11**
- **La nivel aplicaţie**
  - **Interzice tot traficul de tip "peer-to-peer"**
  - **Nu permite trafic HTTP în al cărui header există comanda "POST"**
  - **Nu permite opţiunea "DEBUG" în comenzile SMTP (e-mail)**

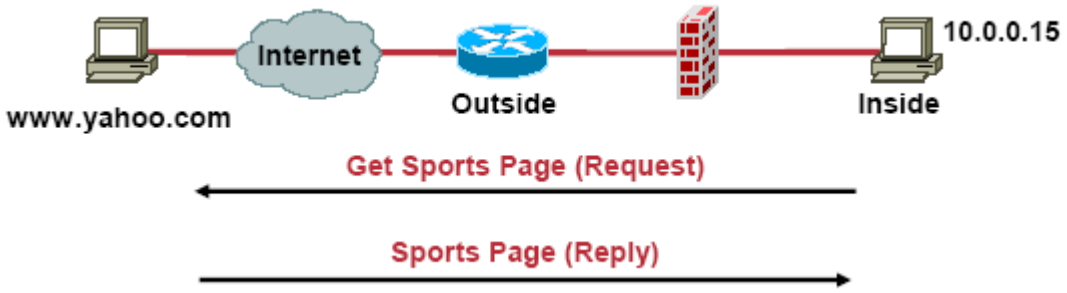
Tipuri de firewall

1. Packet filtering firewall
2. Stateful inspection firewall
3. Application firewall
4. Proxy gateway
5. Personal firewall

Packet filtering firewall

- Permite sau interzice pachetele, funcţie de adresa IP sau portul sursa/destinaţie
  - reguli de filtrare (ACL – Access Control List): deny / allow
  - *deny all* – regula default
- Verificarea pachetelor se face în ambele direcţii (*inbound* respectiv *outbound* trafic)
- Payload-ul pachetelor (zona de date) nu este inspectat
- Nu memorează informaţii de stare; pachetele sunt tratate individual, fară a ţine cont de context
- Funcţie suportată de majoritatea ruterelor actuale
- Avantaje
  - simplu, rapid, transparent pentru utilizatori
- Dezavantaje
  - nu poate bloca toate tipurile de trafic
  - ineficient împotriva atacurilor care exploatează vulnerabilitățile protocoalelor din stiva TCP/IP
  - eficiență scăzută în cazul fragmentării pachetelor

Packet filtering firewall (cont.)



- **Filtru de pachete fără stare (stateless) – sunt necesare doua liste de control al accesului:**
  1. **Permite traficul HTTP de la 10.0.0.0/24, spre www.yahoo.com**
  2. **Permite traficul HTTP de la www.yahoo.com, spre 10.0.0.0/24**

Stateful inspection firewall

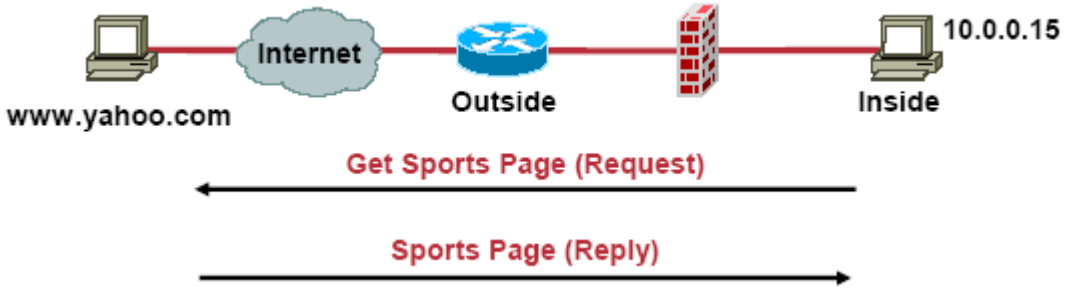
- Bazat tot pe filtrarea de pachete
- Inspectează pachetele şi memorează informaţii de stare pentru fiecare conexiune în parte
  - odată ce un pachet este identificat ca făcând parte dintr-o conexiune stabilită, procesarea acestuia poate fi optimizată (lua o cale mai scurtă)
  - informaţia de stare ce se memorează diferă de la producător la producător
- Cel mai popular tip de firewall
- Performanţe ridicate

Stateful inspection firewall (cont.)

Source Address	Source Port	Destination Address	Destination Port	Connection State
192.168.1.100	1030	192.0.2.71	80	Initiated
192.168.1.102	1031	10.12.18.74	80	Established
192.168.1.101	1033	10.66.32.122	25	Established
192.168.1.106	1035	10.231.32.12	79	Established

- Fiecare pachet primit este analizat în conformitate cu conținutul tabelei de stare:
  - daca starea pachetului corespunde stării din tabel, atunci pachetul este lăsat să treacă
- Maşini de stare pentru fiecare protocol (TCP, UDP, etc)
  - blocarea pachetelor care nu aderă strict la starea maşinii din momentul respectiv (de exemplu, numărul de secvenţă TCP este în afara ordinii)
- Ce se întâmplă în cazul protocoalelor de tip connectionless (UDP)?
  - se urmărește doar adresele și porturile sursă și destinație
  - un răspuns DNS va fi lăsat să treacă numai dacă a existat în prealabil o interogare DNS
  - intrările din tabelă sunt șterse automat după un interval de timp

Stateful inspection firewall (cont.)



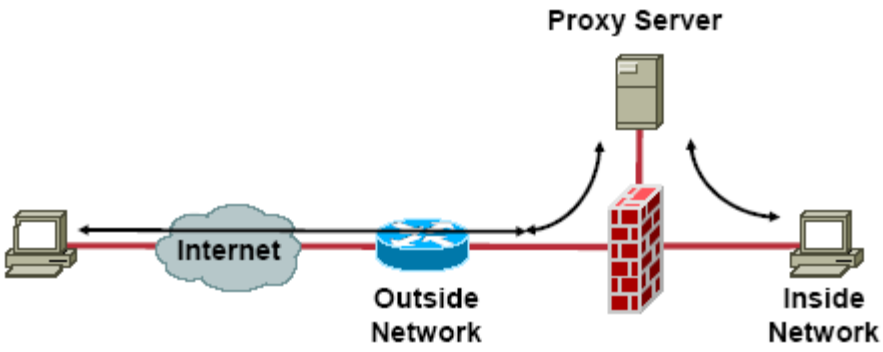
- **Este suficientă o singură listă de control al accesului:**
  1. **Permite traficul HTTP de la 10.0.0.0/24, spre www.yahoo.com**

Application firewall

- *Deep pachet inspection*
- Filtrare funcție de datele / comenzile transmise la nivel aplicație:
  - blocarea tuturor e-mailurilor care conțin fișiere executabile ca atașament, blocarea paginilor de Web cu conținut activ (Java, ActiveX), blocarea comenzii FTP ”put”
- Produse specializate funcție de protocolul de nivel aplicație:
  - Web Application Firewall (WAF)

Proxy gateways

- Application Level Gateway - control la nivel de protocol
- Toate cererile şi răspunsurile trec prin proxy server unde sunt validate
- Exista doua conexiuni separate: client-proxy, proxy-server
- Avantaje:
  - adresele IP interne nu sunt vizibile în exterior
  - permit autentificarea utilizatorilor care accesează Internet-ul
  - permit analiza traficului SSL
- Fiecare serviciu are nevoie de un proxy separat
  - nu toate serviciile suportă proxy
- HTTP proxy
  - filtrare, loggare, caching pagini Web
  - forward vs reverse proxy



Personal firewall

- Versiune simplificată a unui firewall de reţea, destinată staţiilor de lucru
- Interzice conexiunile de intrare, daca nu au fost explicit permise
- Inspectează traficul de intrare/ieşire şi protejează staţiile de lucru de atacuri
- Management centralizat pentru impunerea politicilor de securitate la nivel organizaţional
- Exemple de personal firewall
  - Windows XP Firewall (SP2)
  - ZoneAlarm (www.zonelabs.com)
  - Norton Personal Firewall (www.symantec.com)
  - Comodo Firewall (www.comodo.com)

Alte tehnologii firewall

- Network Access Control (NAC) / Network Acces Protection (NAP)
  - verificarea calculatoarelor utilizatorilor înainte de a le da accesul în rețeaua internă
  - calculatorul este pus inițial într-o ”zonă de carantină” (rețea specială), verificat din punct de vedere al securității (antivirus, update-uri, etc) și apoi i se permite accesul în rețeaua internă
- Unified Threat Management (UTM)
  - implementarea mai multor funcționalități de securitate (firewall, IPS, antivirus, VPN, DLP) pe un singur echipament
  - reduce efortul de administrare
  - limitări din punct de vedere al performanței
- Firewall pentru infrastructuri virtuale
  - rețele virtualizate
  - filtrarea traficului între mașini virtuale

Implementare firewall

Dedicated Appliances

- Sistem de operare specializat, securizat
- Diferite niveluri de performanta/pret
- Uşor de instalat şi administrat

Software (Network and Personal)

- Rulează pe sisteme de uz general
- Nivel de performanţă mediu

Firewall Switch Module

- Nivel foarte ridicat de performanţă
- Se integrează în infrastructura de reţea existentă

Integrated in Router Software

- Protecţia investiţiei existente
- Dedicat conexiunilor WAN/Internet
- Influenţează performanţele de rutare a pachetelor ale ruterului

Caracteristici cheie pentru un firewall

- Performanţa
  - viteza de procesare (bps, pps, cps)
  - scalabilitatea
  - ASIC vs NP vs CPU (uz general)
- Politici de filtrare suportate
  - pe bază de adrese şi protocoale
  - funcţie de aplicaţiile de reţea utilizate
  - pe baza identităţii utilizatorilor
- Disponibilitatea
  - activ-pasiv
  - activ-activ
- Integrarea cu infrastructura existentă
  - cu serviciile de autentificare (Radius, Tacacs+)
  - cu serviciile de logging şi monitorizare
- Management
  - SSH, HTTPS

Limitările unui firewall

- Nu asigură protecţie împotriva atacurilor interne
  - 70 % din atacuri sunt din interior!
- Nu asigură protecţie împotriva viruşilor transmişi prin e-mail sau Web
  - traficul SMTP şi HTTP este permis de firewall!
- Nu pot inspecta traficul criptat / tunelat
- Sisteme complexe
  - configurarea şi administrarea unui firewall nu este simplă!

Produse firewall

- Cisco ASA
- Check Point FireWall-1
- Juniper NetScreen
- Palo Alto Networks PA/VM
- Fortinet FortiGate
- McAfee Firewall Enterprise
- Stonesoft NGFW
- Linux netfilter/iptables

Gartner Magic Quadrant for Enterprise Network Firewalls