UNIVERSITATEA
TRANSILVANIA
BRAȘOV
Electronics & Computers

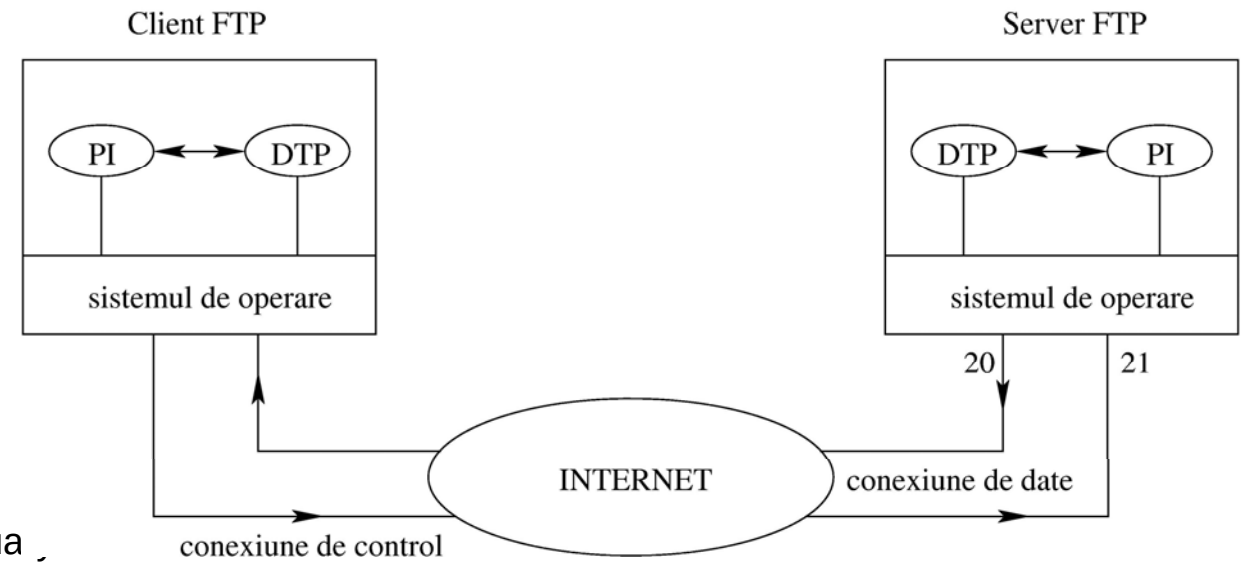
Servicii Internet II

FTP – File Transfer Protocol

- Este serviciul care transfera cea mai mare cantitate de date
- Download – copierea unui fsier de pe un host aflat la distanta pe calculatorul local
- Upload – copierea unui fisier de pe calculatorul local pe un host aflat la distanta
- Utilizarea serviciului necesita existenta unui cont de utilizator si a unei parole
  - Exista un cont generic- anonymous, email-ul ca si parola
  - Cu modul ftp anonymous oricine se pate conecta la un server ftp

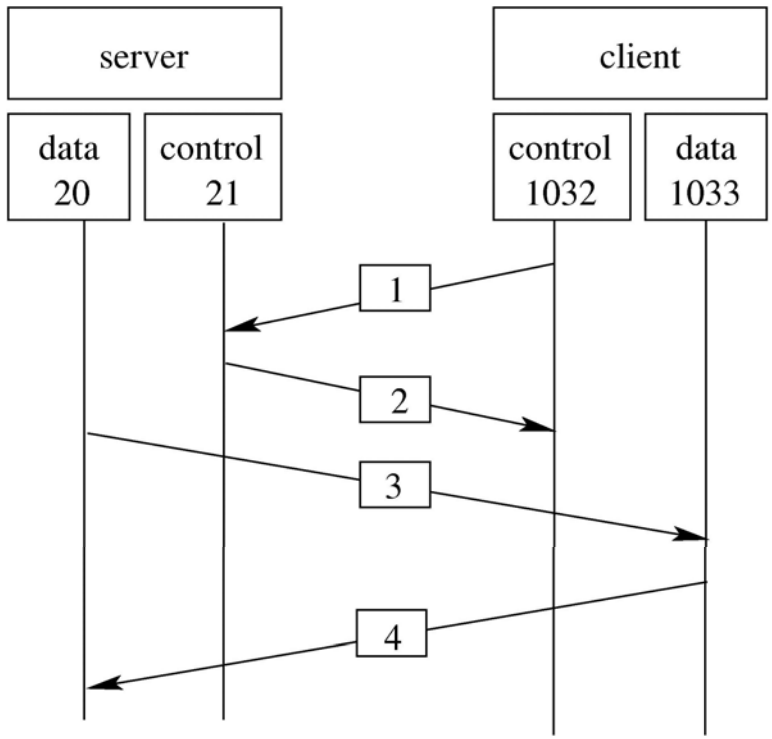
Modelul FTP

- Conexiunea de control
  - Conexiune acctiva pe toata durata sesiunii
  - Se stabileste pe portul 21 al serverului
  - Initiata de client
- Conexiunea de date
  - Initiata de server dupa primirea unei conexiuni de control
  - Conectarea de pe portul 20 al serverului
  - Este activa doar pe durata transferului fisierului



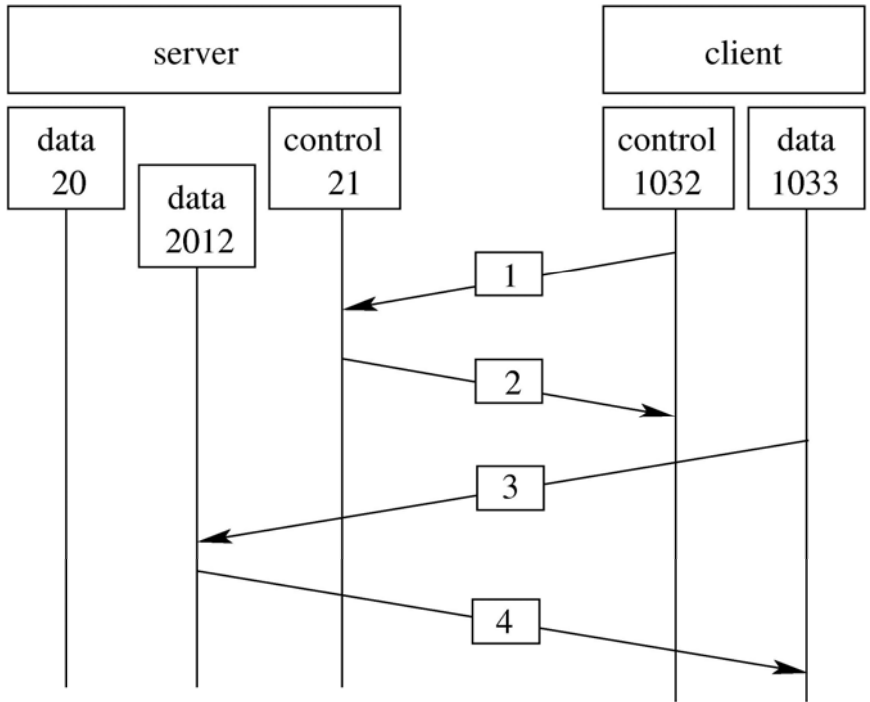
FTP Activ

- Serverul foloseste porturile 21si 20
- Conexiune de control initiata de client
- Conexiune de date initiata de server
- Existenta firewall-urilor a dus la limitarea acestui mod de functionare si aparitia modului pasiv de functionare



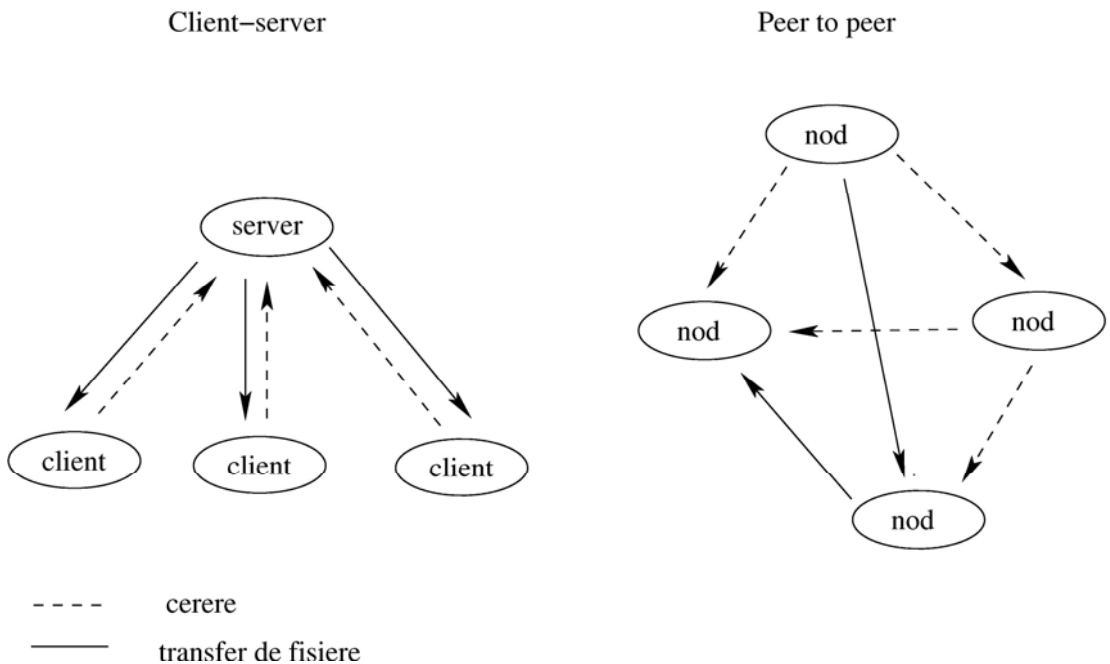
FTP Pasiv

- Clientul foloseste comanda PASV
- Acest mod rezolva problema blacarii conexiunii de date de catre firewall
  - Clientul initiaza si conexiune de date
- Serverul este entitatea pasiva acre asteapta comenzi



File sharing

- O modalitate noua de transfer a fisierelor
- Arhitectura distribuita – toate nodurile sint si server si client in acelasi timp
- Se rezolva problema supraincarcarii unor servere cu continut cautat
  - Cu cit o resursa este mai cautata cu atit este mai disponibila



Probleme (1)

- Conectivitatea
  - Pentru a incepe transferul trebuie sa exista o cenexiune la cel putin unnod
  - Pseudo-servere ofera liste cu nodurile active la un moment dat
- Cautarea
  - Gasirea unei anumite resurse se bazeaza pe doua componente ale modelului de cautare
    - Algoritmul de transmitere a mesajului
    - Gasirea fisierului

Probleme (2)

- Algoritm de transmitere a mesajului
  - se urmareste maximizarea numarului de noduri chestionate
  - Difuzare – fiecare not transmite mai departe cererea catre toate nodurile la care este conecatat
    - Utilizarea cimpului TTL pentru a distruge o cerere veche
    - Necesita o largime de banda considerabila
  - Mentinerea unei liste cu vecini si fisierele lor disponibile si selectarea doar a vecinului cu latimea de banda cea mai mare
- Gasirea fisierului
  - Identificarea un mod unic a unui fisier indiferent de numele lui pe baza continutului – algoritmi de hashing MD5

Probleme (3)

- Transferul fisierelor
  - Variatii mari a latimii de banda a diferitilor clienti
  - Raspindirea canalelor asimetrice
  - Probleme legate de upload-area fisierelor in mod rapid
  - Solutia : transferul fisierului din surse multiple
  - Transferurile se realizeaza prin protocol HTTP implementat peste TCP/IP
    - Orice nod implementeaza un client si un server HTTP

Retele existente (1)

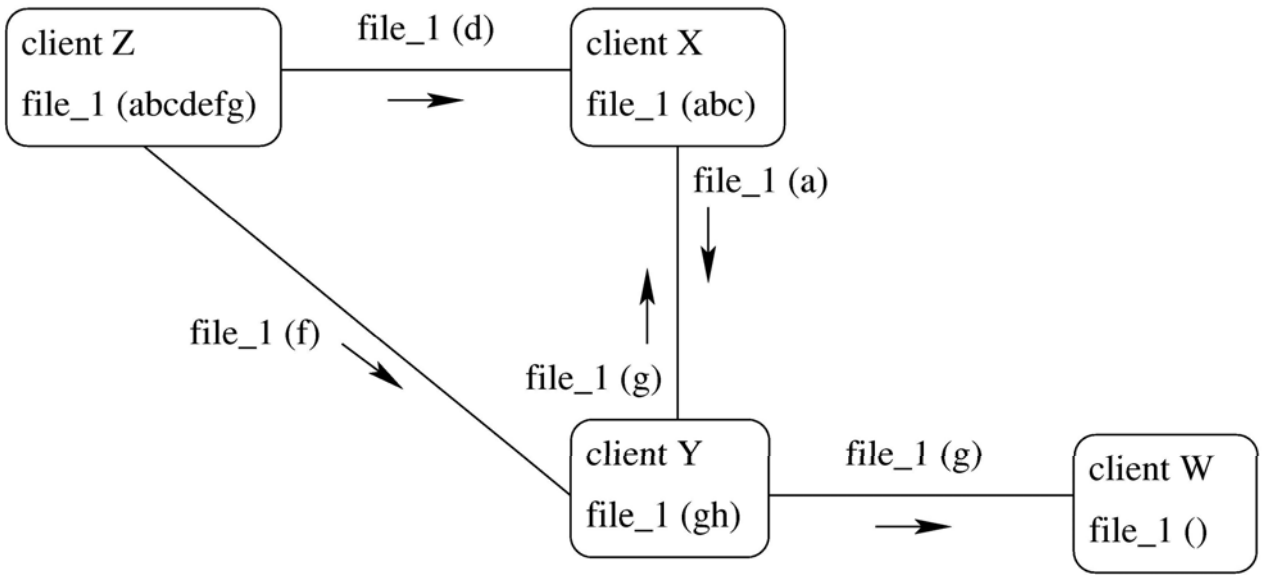
- Kazza/Morpheus
  - Tehnologia FastTrack
    - Ierarhizarearetelei in fucntie de latimea de banda
    - Super-noduri – calculatoare cu latime de banda considerabila
    - Administrarea retelei in mod automat si dinamic
  - Transferuri inteligente
    - Impartirea fisierelor in bucati mici si transferul simultan de la mai multe surse
    - Verificarea ciclica a tuturor surselor existente
  - AMDA (Automatic Meta Data Assignment)
    - Extragere de informatie relevanta
      - Titlu piesa, interpret, album (fisiere audio)
      - Rezolutie, codec, subtitrare, actori (fisiere video)
    - Folsirea acestor date pentru rafinarea cautarii

Retele existente (2)

- eDonkey – folseste un client si un server
  - Clientul permite partajarea si transmiterea fisierelor
  - Serverul permite cautarea utilizatorilor activi si a fisierelor
  - Serverul nu transmite nici un fisier
- Cautarea
  - Clientul se conecteaza la un server si trimite lista fisierelor pertajate
  - Server-ul mentine liste cu toate fisierele tuturor clientilor
  - La o cerere serverul va cautain baza de date proprie si va returna lista clientilor care au acea resursa
  - Se foloseste protocolul UDP pentru minimizarea traficului de date

Retele existente (3)

- Transferul
  - Se creaza o lista cu toti clientii care au acea resursa
    - Clientii obtinuti de la serverul local
    - Clientii obtinuti de la serverele distante
  - Se fac cereri multiple catre toti cei care au acel fisier



Firewall - Definitie

- "fire wall" (zid de foc) - zid ignifug cu rolul de a preveni extinderea focului dintr-o incapere catre restul zonelor.
- Internetul - mediu volatil si nesigur din punct de vedere al securitatii calculatoarelor => necesitatea izolarii prin intermediul unui "firewall“

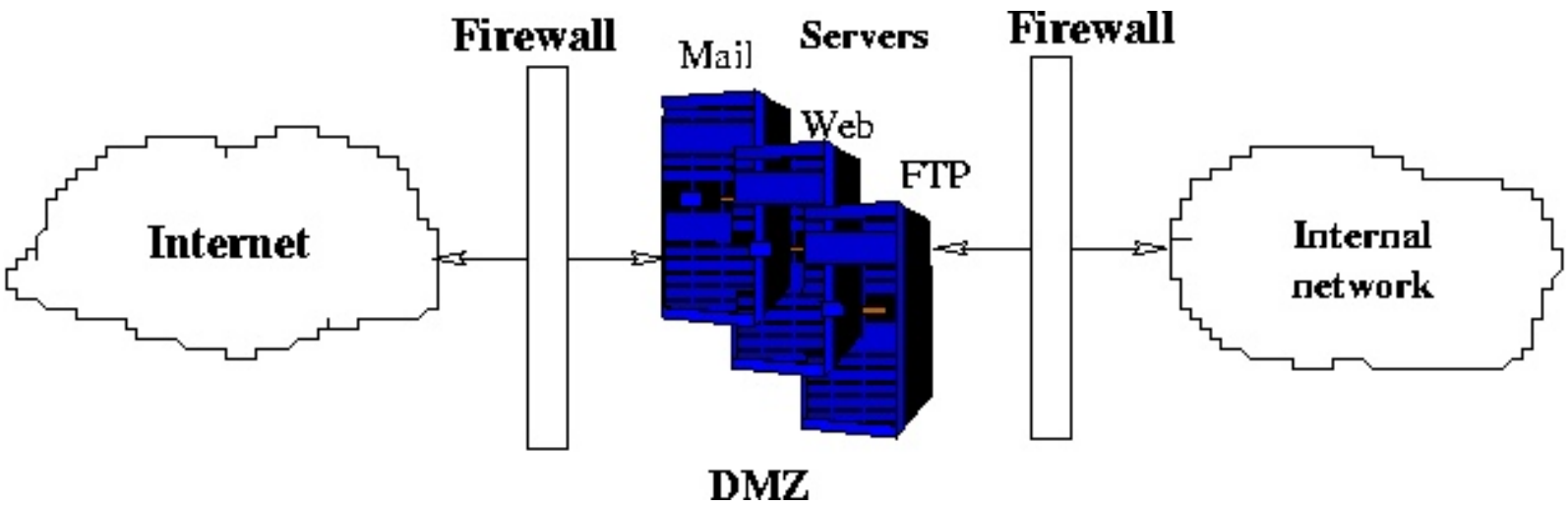
- Un firewall receptioneaza, analizeaza si ia decizii pentru toate pachetele sosite inainte ca acestea sa ajunga ın celelalte parti ale retelei interne.

Firewall - Topologie

- Firewall-ul - primul program care receptioneaza si prelucreaza traficul de intrare si ultimul care prelucreaza traficul de iesire.
- Firewall-ul este plasat intre reteaua interna si internet

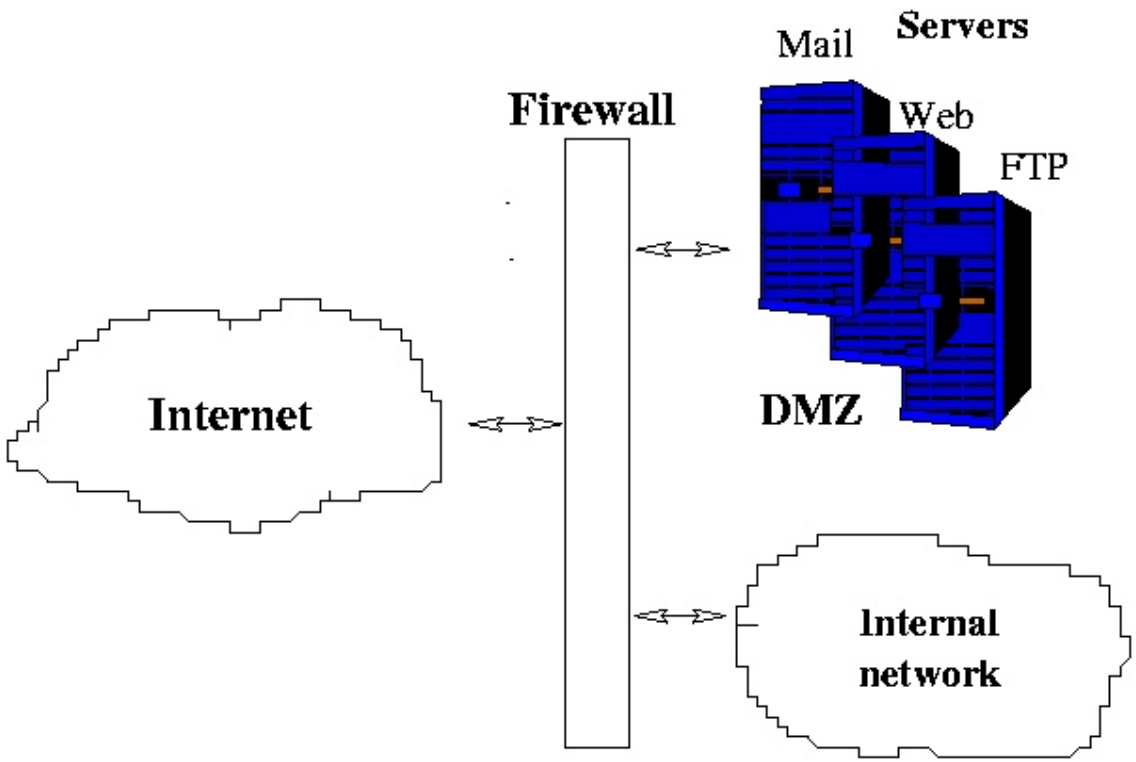
Firewall – DMZ (1)

- O configuratie tipica consta intr-o zona neutra DMZ (**D**e**M**ilitarized **Z**one) care contine serverele care se doresc protejate
- DMZ-ul nu apartine retelei interne si nu este conectata direct la Internet si este protejata de firewall-uri



Firewall – DMZ(2)

- O configuratie mai practica cu un singur firewall necesita doar o singura resursa HW (router + firewall)



Firewall – Filtrare de pachete

- Doua tipuri de firewall
  - la nivel aplicatie - proxy-uri
  - la nivel ret¸ea - filtrare de pachete

- Firewall-ul proxy este mai eficienta pentru ca restrictioneaza aplicatii dar mai greu de implementat.
- Filtrarea de pachete este cea mai raspindita metoda datorita simplitatii in implemetare.
- Filtrarea lor se face pe baza:
  - Adresei sursa/destinatie
  - Portului destinatie al accesului
  - Protocolului utilizat in comunicare

Firewall – Filtrare de pachete

- Doua tipuri de firewall
  - la nivel aplicatie - proxy-uri
  - la nivel ret¸ea - filtrare de pachete

- Firewall-ul proxy este mai eficienta pentru ca restrictioneaza aplicatii dar mai greu de implementat.
- Filtrarea de pachete este cea mai raspindita metoda datorita simplitatii in implemetare.

- Filtrarea - acceptarea sau rejectarea pachetelor in urma examinarii pechetelor sosite sau trimise, pe baza regulilor de configurare - **politici de filtrare**.

Firewall – Politici de filtrare

- Filtrarea pachetelor lor se face pe baza unor reguli care se refera la:
  - Adresa sursa/destinatie a pachetului
  - Portului destinatie al accesului (20, 22, 53, etc)
  - Protocolului utilizat in comunicare (TCP, UDP)

- In Linux firewall-ul este implementat cu comanda ***iptables***

Firewall – Exemplu minimal

- Exemplu de firewall pt work-station (fara servere care ofera servicii in Internet) care ruleaza Linux:

```
// stergem toate regulile existente
iptables –F
iptables -X

// acceptam toate cererile catre exterior
iptables -P OUTPUT ACCEPT
// restrictionam toate cererile din exterior
iptables -P FORWARD DROP
iptables -P INPUT DROP

// din exterior acceptam doar raspunsurile cererilor
// facute in interiorul firewall-ului
iptables -A INPUT -i eth0 -m state --state
ESTABLISHED,RELATED -j ACCEPT
```

Firewall – Pro si contra

- Pro:
  - Simplitate in implementarea firewall-urilor
  - Simplitate in configurarea politicilor de filtrare
- Contra
  - Nu asigura securitate absoluta
  - Datorita modalitatii de implementarea a politicilor de filtrare datele esential din pachete pot fi falsificate (adrese, poturi)
  - Odata acceptat un pachet (conexiune) orice vulnerabilitate a aplicatiei sursa poate fi exploatata