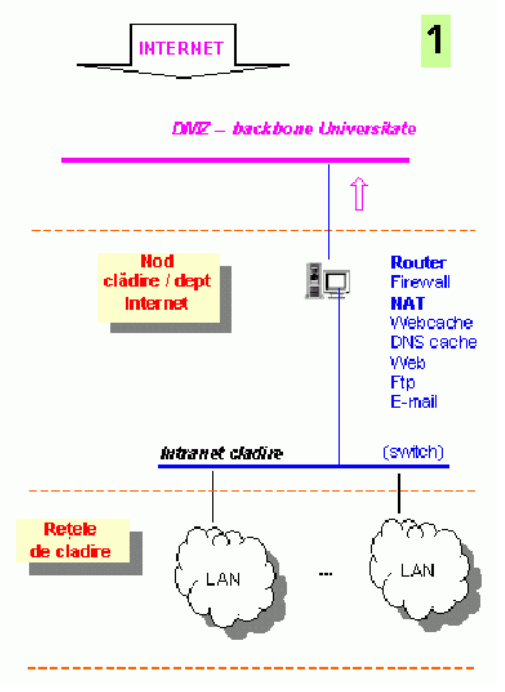
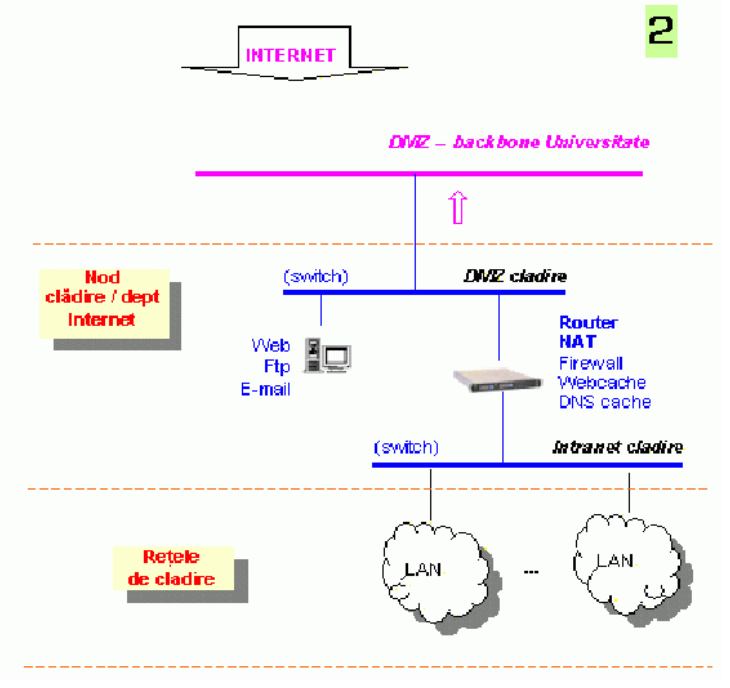
Scheme de conectare

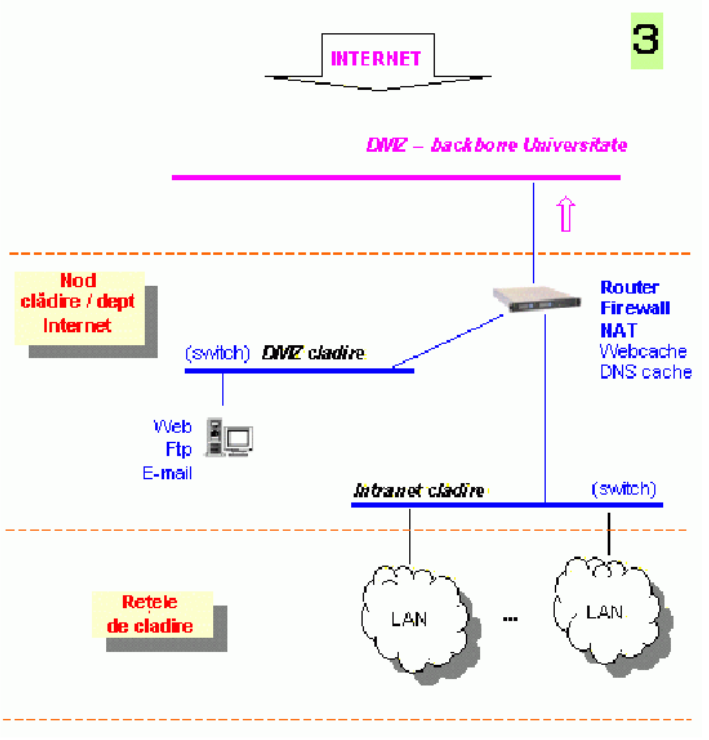
1. Cea mai simpla schema, dar si cea mai nesigura si neperformanta, este a unui singur server care realizeaza toate serviciile necesare:



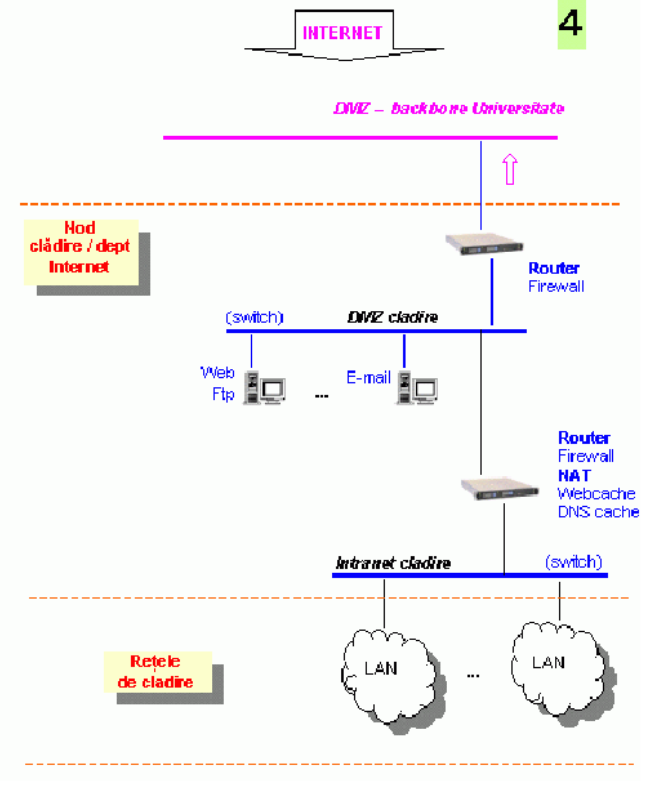
2. O schema recomandata, este cea cu protectie prin firewall si server separat de servicii Internet, scos in afara retelei interioare:



3. O schema eleganta se poate realiza prin folosirea unui router firewall cu 3 interfete:



4. Schema urmatoare, are 2 straturi de protectie firewall:



Date de configurare

*Reteaua primara (*backbone*)*

Toate host-urile conectate direct in reteaua primara a Universitatii trebuie sa fie in raspunderea unui administrator de retea; datele principale de configurare sunt:

- **IP address:** primita de la **ISP (Internet Service Provider)**
- **IP mask:**
- **Default gateway:**
- **Primary DNS:**
- **Secondary DNS:**
- **DNS host name:** discutat cu Centrul Internet
- **DNS domain name:** **univ-ovidius.ro**
- **NO WINS**
- **DHCP: NO -** pentru host-urile independente

- **Server principal e-mail -** *SMTP/POP3:***mail.univ-ovidius.ro***webmail:* **http://mail.univ-ovidius.ro**
- **Downloads: http://www.univ-ovidius.ro/downloads**

Pentru testarea caii de acces Internet, se poate folosi **ping**, dat atat pe adresa IP (numerica), cat si pe adresa FQDN (literala), pentru cateva noduri importante din reteaua Centrului Internet:

Fully Qualified Domain Name

	IP	FQDN	Descriere	
y		**ns.univ-ovidius.ro**	server DNS retea primara	**Indicatie: http://dnscheck.pingdom.com/**
x		.....	server DNS **retea secundara**	
x		.....	poarta iesire	
x		**www.univ-ovidius.ro**	server web	

Daca toate adresele de mai sus se verifica ok, se poate presupune ca problemele nu sunt la nivelul Centrului Internet.

Pentru testarea accesului in Internet ping-ul nu e suficient. Trebuie testat tipul de serviciu cu care se lucreaza prin aplicatiile respective: browser, client ftp, client pop3/smtp, etc.

Cand accesul IP si DNS se verifica OK, daca sunt totusi probleme de vizibilitate Internet, se pot folosi comenzile:

tracert, **pathping** (Win), sau **traceroute** (Linux, Unix)

pentru a vedea problemele care sunt de regula la nivelele superioare de furnizori Internet.

De asemenea se pot folosi informatiile furnizate de servicii din exterior (ping, traceroute).

Pentru un diagnostic de detaliu trebuie insa tinut cont de conditiile particulare in care sunt rezolvate rutele de acces pentru fiecare aplicatie si nod interior (rugam contactati admin). Astfel de ex., un traceroute (icmp, udp) nu va reflecta neaparat calea reala pentru acces www, sau acces ftp.

Reteaua de campus Mamaia

O parte din statiile de lucru de pe **Mamaia** au ramas conectate la o retea locala interioara, si mai departe printr-un router Cisco la reteaua primara (*backbone*) a Universitati. Routerul are functiuni *firewall, NAT, traffic mngmnt*.
Toate statiile conectate direct in reteaua interioara **Mamaia** trebuiesc setate **cu DHCP (Dynamic Host Configuration Protocol)**

Obs: Campurile de mai jos se vor completa pentru fiecare statie de lucru

- **IP address:**
- **IP mask:**
- **Default gateway:**
- **Primary DNS:**
- **DNS host name:** nu e important pentru conectivitate externa
- **DNS domain name:** nu e important pentru conectivitate externa
- **NO WINS**
- **DHCP**
- **E-mail server (POP3/SMTP):** cu interfata Web:
- **Downloads:**

Testarea accesului Internet de la o statie conectata in reteaua interioara Colina, include cateva adrese importante pe calea de iesire in reteaua primara:

IP	Descriere
.....	poarta iesire din LAN (*default gateway*) **Mamaia**
.....	poarta intrare *backbone*
.....	server DNS *bacbone*

Retele de cladire, departament

Configurarea retelelor de cladire/facultate/departament este in intregime in responsabilitatea administratorilor de sisteme.

Reteaua locala interioara este conectata la reteaua primara printr-un router, sau server Linux/Windows, cu functia de translatare adrese (NAT), astfel ca intreaga retea locala se 'vede' spre exterior ca o singura adresa IP rutabila (sau un set de cateva asemenea adrese).

Observatie **Obs. Pe Mmaia - clasa B: 172.....**

In reteaua interioara se folosesc adrese nerutabile in Internet, de obicei o clasa C cu adresa de retea 192.168.x.0/24, unde x este adresa de host din adresa IP exterioara a routerului (de ex., la un router conectat in reteaua primara cu adresa IP 193.254.231.171, adresa de retea interioara este 192.168.171.0/24, iar 192.168.171.98 de ex., este o adresa de host in LAN-ul interior).

Se recomanda folosirea atribuirii dinamice de adrese IP si DNS prin DHCP. Aici e un exemplu de configurare pentru Windows XP.
Atat routerele broadband, cat si serverele Linux sau Windows, permit configurarea unui server DHCP care sa actioneze in reteaua interioara.
Parametrii principali ce se configureaza sunt:
- set de adrese atribuite serverului DHCP, din domeniul de adrese IP interioare ales de administrator (de ex., 32 de adrese, de la 192.168.171.33 pana la 192.168.171.64)
- adresele IP de servere DNS primar (193.254.231.2) si secundar (193.254.230.2), atribuite de serverul DHCP statiilor din retea

Daca routerul gateway este un sistem Linux, sau daca un asemenea server se gaseste in reteaua interioara, acesta trebuie configurat sa asigure si functia de *DNS cache*, dar si alte functii de gateway: *proxy, filtrare virus/antispam*, etc.

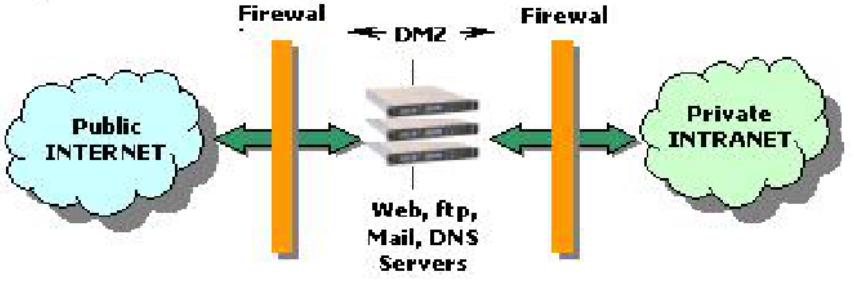
Configurarea firewall cu DMZ

DMZ este o prescurtare pentru ***demilitarized zone***. In contextul *firewall Internet*, aceasta se refera la o parte separata a retelei, care nu apartine nici retelei interne, nici nu e conectata direct la Internet. De obicei in DMZ se plaseaza serverele WEB, E-MAIL, FTP, DNS, etc., accesibile din Internet.

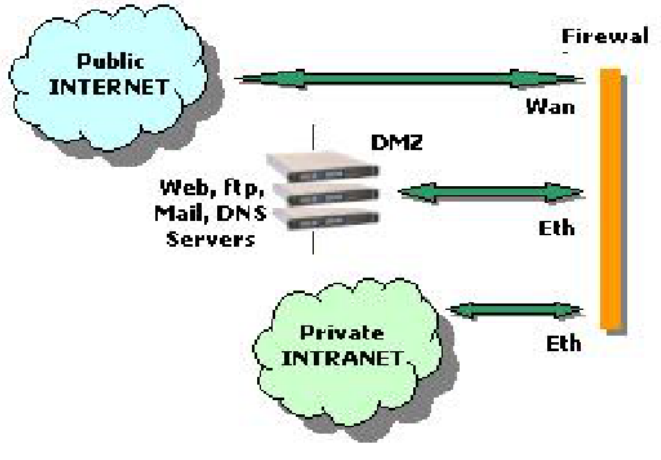
Exemple de configurare firewall cu DMZ:

- O abordare uzuala este prin utilizarea a 2 firewall-uri , unul extern, intre Internetul public si DMZ, si unul intern, intre DMZ si reteaua interioara, asa cum e ilustrat in fig. a). Astfel, Intranetul este protejat in spatele unui strat dublu firewall.
- Simplu, se poate utiliza un router firewall cu 3 interfete: una externa spre Internet, una interna spre Intranet si una spre DMZ, asa cum arata fig. b). Asemenea configuratii se pot realiza cu routere dedicate, sau cu servere, de ex. Linux (chiar dedicat, cum este Astaro Security Linux, disponibil si la noi in situl ftp).

a)

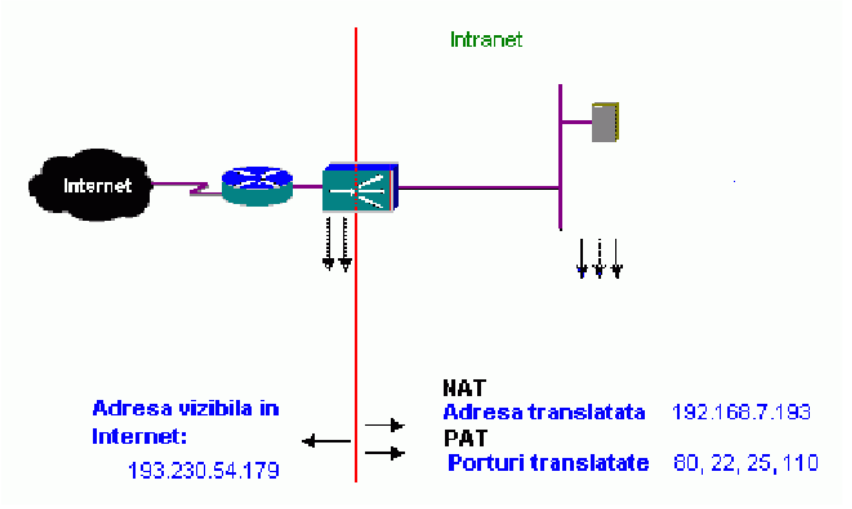


b)



NAT / PAT

Network Address Translation/Port Address Translation



NAT si PAT sunt 2 tehnologii care permit unui echipament - server, router - sa schimbe una sau ambele adrese IP folosite in tranzactie. In Internet, doua masini interconectate prin protocolul TCP/IP au fiecare adrese unice, ceea ce permite rutarea traficului intre ele. Adresele se regasesc in antetul fiecarui pachet rutat in Internet.

Prin NAT se schimba la plecare, una din adrese, in alta adresa unica. La returul traficului, adresa schimbata, se reface pentru a ajunge la masina originala. Se poate astfel:

- asigura un prim nivel de securitate - adresa reala IP a unei masini, nu e cunoscuta in afara
- economisi adrese pretioase IP, ascunzand in spatele routerului care face NAT, o intreaga retea, translatata in exterior printr-o singura adresa, sau un grup de adrese.

Prin PAT, se schimba portul TCP/IP adresat unei masini din spatele routerului, in alt port, cunoscut numai in interiorul retelei. Se realizeza astfel:

- un al doilea nivel de redirectare, ca masura de securitate
- se permite accesul din Internet, la o masina aflata in spatele routerului, pe anumite porturi

Folosite combinat, cele 2 tehnologii permit ascunderea unei intregi retele interioare, in spatele unei singure adrese IP, sau grup de adrese IP, vizibile in Internet, cu asigurarea accesului dinspre Internet, spre anumite masini din reteaua interioara, pentru care se permite accesul (servere Web, E-mail, Ftp, etc.).

DNS - Domain Name System

DNS este un serviciu de registru Internet distribuit. Este folosit pentru translatarea intre nume de domeniu si adrese IP. Cele mai multe servicii Internet se bazeaza pe DNS si daca acesta cade, siturile web nu pot fi gasite iar livrarea mail se blocheaza.

Fiecare calculator trebuie sa 'stie' de existenta a cel putin un server DNS pentru a rezolva corelatia intre un nume calificat de domeniu (FQDN, sau nume de domeniu DNS), adica o adresa literala (gen www.google.com, sau mail. univ-ovidius)ro si adresa sa numerica (IP address, de tipul 193.254.230.3); aceasta pentru ca o conexiune TCP/IP intre 2 calculatoare in Internet se face la nivel de adrese numerice IP.

Daca procesul 'resolver' din calculatorul propriu nu reuseste sa faca o cautare valida DNS (acel *DNS lookup*), atunci veti primi o eroare pentru orice pagina web sau server mail, apelate prin numele lor de domeniu.
Va puteti convinge ca exista o problema DNS - nu neaparat la nivel central - daca primind o eroare pentru www. univ-ovidius.ro puteti totusi aduce homepage-ul Universitatii cu adresa IP echivalenta: .....