

Liste de acces și NAT

Politica de securitate a unei firme se scrie în cuvinte, dar rețeaua înțelege doar reguli. Lucrarea aceasta face traducerea: cinci cerințe formulate de conducere devin liste de acces, plasate corect pe interfețe și pe direcții. Apoi toată firma iese în Internet - pe o singură adresă publică.

OBIECTIVELE CAPITOLULUI

- Construiți topologia și demonstrați conectivitate completă înainte de orice filtru
- Completați tabelul de referință al conectivității
- Implementați politicile P1-P4 și demonstrați efectul fiecăreia, prin teste
- Recompletați tabelul de conectivitate și explicați fiecare diferență
- Configurați PAT pentru toate segmentele interne
- Configurați NAT static pentru serverul web și demonstrați accesul din Internet
- Documentați traducerea adreselor, segment cu segment
- Provocați o regulă cu zero potriviri, explicați de ce și reparați-o

6.1 Cum se citește o listă de acces

O listă de acces este o listă de reguli, parcursă **de sus în jos**, până la prima potrivire. Ce se potrivește primul decide, iar restul listei nici măcar nu se mai citește. La final, dacă nimic nu s-a potrivit, există un *deny* invizibil care aruncă pachetul.

DEFINIȚIA 6.1 (LISTĂ STANDARD). Vede doar *adresa sursă*. Se numerează 1-99. Utilă când vreți să spuneți „de la aceste stații, nicăieri” sau „numai de la aceste stații”. Se plasează cât mai aproape de *destinație*, tocmai pentru că nu știe care este destinația.

DEFINIȚIA 6.2 (LISTĂ EXTINSĂ). Vede sursa, destinația, protocolul și portul. Se numerează 100-199, sau primește un nume. Se plasează cât mai aproape de *sursă*, ca traficul interzis să nu consume rețeaua degeaba.

DEFINIȚIA 6.3 (MASCĂ WILDCARD). Inversul măștii de rețea: 0 înseamnă „bitul acesta trebuie să coincidă”, 1 înseamnă „orice”. Pentru o rețea /24 se scrie 0.0.0.255. Scurtături: *host* 10.1.10.5 înseamnă 10.1.10.5 0.0.0.0, iar *any* înseamnă 0.0.0.0 255.255.255.255.

DEFINIȚIA 6.4 (DIRECȚIA). *in* filtrează pachetele care *intră* în ruter pe acea interfață, înainte de rutare. *out* filtrează pachetele care *ies*, după rutare. Aceeași listă pe aceeași interfață, dar pe direcții diferite, face lucruri complet diferite.

Trei greșeli care se fac de fiecare dată. 1. *Ordinea*. O regulă generală pusă deasupra uneia specifice o face pe a doua inutilă - nu se va potrivi niciodată.

2. *Deny-ul implicit*. O listă care conține numai reguli *deny* blochează absolut tot, inclusiv ce voiați să permiteți.

3. *Direcția*. Lista corectă, pusă pe direcția greșită, nu vede niciodată traficul pe care trebuia să îl filtreze - și are contorul la zero.

6.2 Echipamente necesare

Tabelul 6.1 Echipamente necesare.

Buc.	Echipament	Model	Categoria din Packet Tracer	La ce folosește aici
2	Ruter	4331	Network Devices → Routers	R-FIRMA (ruterul de margine) și ISP
1	Switch	2960	Network Devices → Switches	SW1, cu trei VLAN-uri
3	Calculator	PC-PT	End Devices	câte o stație de test per departament
2	Server	Server-PT	End Devices	SRV-WEB în DMZ și „Internetul” (8.8.8.8)
1	Cablu serial	Serial DCE	Connections	R-FIRMA ↔ ISP
6	Cablu drept	Copper Straight-Through	Connections	restul legăturilor

Topologia reia structura din laboratorul 3: trei VLAN-uri pe SW1, trunk spre ruter, subinterfețe pe G0/0/0. DMZ-ul se leagă pe o interfață fizică separată, G0/0/1.

6.3 Topologia și politica

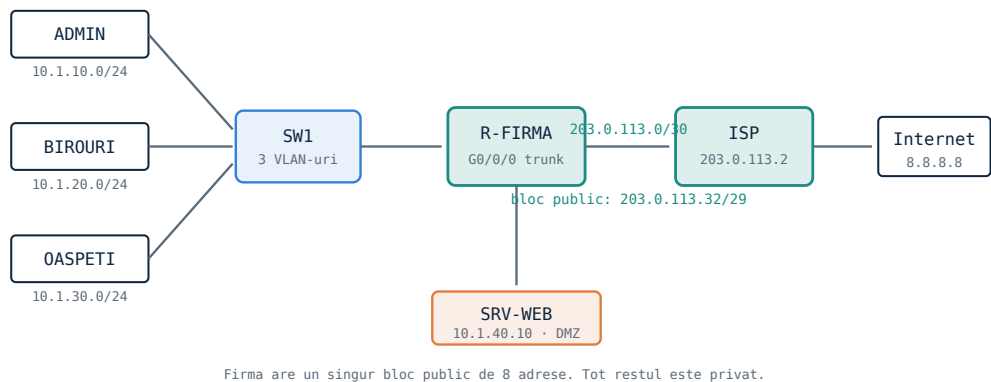


Figura 6.1 Rețeaua firmei, cu trei segmente interne, o zonă demilitarizată și o singură ieșire spre Internet.

Tabelul 6.2 Topologia și politica.

Segment	VLAN	Rețea	Gateway	Stație de test
ADMIN	10	10.1.10.0/24	10.1.10.1	PC-ADM 10.1.10.11
BIROURI	20	10.1.20.0/24	10.1.20.1	PC-BIR 10.1.20.11
OASPETI	30	10.1.30.0/24	10.1.30.1	PC-OSP 10.1.30.11
DMZ	-	10.1.40.0/24	10.1.40.1	SRV-WEB 10.1.40.10
Legătura spre ISP	-	203.0.113.0/30	-	R-FIRMA .1, ISP .2
Bloc public alocat	-	203.0.113.32/29	-	.33 – .38 utilizabile

DEFINIȚIA 6.5 (POLITICA DE SECURITATE, AȘA CUM A FORMULAT-O CONDUCEREA). P1. Oaspeții au acces la Internet și la serverul web din DMZ, dar la nicio altă resursă internă.

P2. Biroul are acces peste tot, cu excepția segmentului ADMIN.

P3. Serverul web din DMZ nu are voie să inițieze conexiuni spre rețeaua internă. Poate doar să răspundă.

P4. Ruterul poate fi administrat prin SSH doar de pe stațiile din ADMIN.

P5. Serverul web trebuie să fie accesibil din Internet, la o adresă publică fixă.

6.4 Pasul 0: rețeaua funcțională, fără filtre

Înainte de a filtra ceva, totul trebuie să funcționeze. Este o disciplină care se învață greu, dar economisește ore: dacă aplicați ACL-uri peste o rețea care nu merge, nu veți ști niciodată care problemă e a cui.

1. VLAN-uri pe switch

pe SW1

```
Switch> enable
Switch# configure terminal
Switch(config)# hostname SW1
SW1(config)# vlan 10
SW1(config-vlan)# name ADMIN
SW1(config-vlan)# vlan 20
SW1(config-vlan)# name BIROURI
SW1(config-vlan)# vlan 30
SW1(config-vlan)# name OASPETI
SW1(config-vlan)# exit

SW1(config)# interface fastEthernet 0/1
SW1(config-if)# switchport mode access
SW1(config-if)# switchport access vlan 10
SW1(config-if)# exit
SW1(config)# interface fastEthernet 0/2
SW1(config-if)# switchport mode access
SW1(config-if)# switchport access vlan 20
SW1(config-if)# exit
SW1(config)# interface fastEthernet 0/3
SW1(config-if)# switchport mode access
SW1(config-if)# switchport access vlan 30
SW1(config-if)# exit

SW1(config)# interface gigabitEthernet 0/1
SW1(config-if)# switchport mode trunk
SW1(config-if)# end
```

2. Router-on-a-stick, DMZ și ieșirea spre ISP

pe R-FIRMA

```
Router(config)# hostname R-FIRMA

R-FIRMA(config)# interface gigabitEthernet 0/0/0
R-FIRMA(config-if)# no ip address
R-FIRMA(config-if)# no shutdown
R-FIRMA(config-if)# exit
```

```
R-FIRMA(config)# interface gigabitEthernet 0/0/0.10
R-FIRMA(config-subif)# encapsulation dot1Q 10
R-FIRMA(config-subif)# ip address 10.1.10.1 255.255.255.0
R-FIRMA(config-subif)# exit
R-FIRMA(config)# interface gigabitEthernet 0/0/0.20
R-FIRMA(config-subif)# encapsulation dot1Q 20
R-FIRMA(config-subif)# ip address 10.1.20.1 255.255.255.0
R-FIRMA(config-subif)# exit
R-FIRMA(config)# interface gigabitEthernet 0/0/0.30
R-FIRMA(config-subif)# encapsulation dot1Q 30
R-FIRMA(config-subif)# ip address 10.1.30.1 255.255.255.0
R-FIRMA(config-subif)# exit
```

```
R-FIRMA(config)# interface gigabitEthernet 0/0/1
R-FIRMA(config-if)# description DMZ
R-FIRMA(config-if)# ip address 10.1.40.1 255.255.255.0
R-FIRMA(config-if)# no shutdown
R-FIRMA(config-if)# exit
```

```
R-FIRMA(config)# interface serial 0/1/0
R-FIRMA(config-if)# ip address 203.0.113.1 255.255.255.252
R-FIRMA(config-if)# clock rate 128000
R-FIRMA(config-if)# no shutdown
R-FIRMA(config-if)# exit
```

```
R-FIRMA(config)# ip route 0.0.0.0 0.0.0.0 203.0.113.2
R-FIRMA(config)# end
pe ISP
```

```
Router(config)# hostname ISP
ISP(config)# interface serial 0/1/0
ISP(config-if)# ip address 203.0.113.2 255.255.255.252
ISP(config-if)# no shutdown
ISP(config-if)# exit
ISP(config)# interface gigabitEthernet 0/0/0
ISP(config-if)# ip address 8.8.8.1 255.255.255.0
ISP(config-if)# no shutdown
ISP(config-if)# exit
ISP(config)# ip route 203.0.113.32 255.255.255.248 203.0.113.1
ISP(config)# end
```

Observați ce **nu** are ISP-ul: nicio rută spre rețelele private ale firmei. Este chiar rostul NAT-ului, pe care îl configurăm la final.

3. Completați tabelul de referință

De pe fiecare stație internă, ping către toate celelalte și către SRV-WEB și Internet. Totul trebuie să funcționeze. Notați rezultatele - va fi referința față de care veți verifica efectul fiecărei liste.

De la \ către	ADMIN	BIROURI	OASPETI	DMZ	Internet
ADMIN	-				
BIROURI		-			
OASPETI			-		

DMZ

-

6.5 Traducerea politicii în reguli

Fiecare politică se traduce răspunzând, în ordine, la trei întrebări: **ce tip de listă** îmi trebuie, **pe ce interfață** o pun și **pe ce direcție**.

P1 - Oaspeții

Exemplul 6.1. Sursa este mereu aceeași (10.1.30.0/24), dar destinația decide dacă traficul e permis sau nu. O listă standard vede doar sursa, deci **nu poate exprima** politica. Ne trebuie o listă **extinsă**.

Plasarea: lista extinsă se pune cât mai aproape de sursă, deci pe subinterfața `G0/0/0.30`, direcția `in` - traficul interzis nici măcar nu ajunge să fie rutat.

```
R-FIRMA(config)# ip access-list extended OASPETI-IN
R-FIRMA(config-ext-nacl)# remark permite accesul la serverul web din DMZ
R-FIRMA(config-ext-nacl)# 10 permit tcp 10.1.30.0 0.0.0.255 host 10.1.40.10 eq 80
R-FIRMA(config-ext-nacl)# remark blocheaza orice alta resursa interna
R-FIRMA(config-ext-nacl)# 20 deny ip 10.1.30.0 0.0.0.255 10.0.0.0 0.255.255.255
R-FIRMA(config-ext-nacl)# remark restul, adica Internetul, este permis
R-FIRMA(config-ext-nacl)# 30 permit ip 10.1.30.0 0.0.0.255 any
R-FIRMA(config-ext-nacl)# exit

R-FIRMA(config)# interface gigabitEthernet 0/0/0.30
R-FIRMA(config-subif)# ip access-group OASPETI-IN in
R-FIRMA(config-subif)# end
```

Listingul 6.1 P1 pe R-FIRMA copiază

Testați acum, de pe PC-OSP:

Tabelul 6.3 P1 - Oaspeții.

Test	Rezultat	De ce
ping 10.1.10.11	blocat	regula 20: destinație în 10.0.0.0/8
ping 10.1.40.10	blocat	tot regula 20 - regula 10 permite doar TCP portul 80 , iar ping-ul este ICMP
ping 8.8.8.8	permis	regula 30: orice altă destinație

Al doilea rând merită citit de două ori. Serverul web este accesibil oaspeților - dar *numai pe portul 80*. Ping-ul către el eșuează, și este corect să eșueze: politica spunea „acces la serverul web”, nu „acces la server”. O listă extinsă face exact distincția asta, iar un test cu ping v-ar face să credeți greșit că regula nu funcționează.

Ordinea celor trei reguli este întreaga soluție. Regula 10 este mai specifică decât 20, deci trebuie să fie deasupra ei; regula 30 este cea mai generală și încheie lista. Inversați regulile 10 și 30 și testați din nou: veți vedea exact cum se rupe politica.

P2 - Biroul

```
R-FIRMA(config)# ip access-list extended BIROURI-IN
R-FIRMA(config-ext-nacl)# 10 deny ip 10.1.20.0 0.0.0.255 10.1.10.0 0.0.0.255
R-FIRMA(config-ext-nacl)# 20 permit ip 10.1.20.0 0.0.0.255 any
R-FIRMA(config-ext-nacl)# exit
R-FIRMA(config)# interface gigabitEthernet 0/0/0.20
R-FIRMA(config-subif)# ip access-group BIROURI-IN in
```

Listingul 6.2 P2 copiază

Verificați: biroul nu mai ajunge la ADMIN, dar ajunge la DMZ și în Internet. Verificați și sensul invers - de pe PC-ADM către PC-BIR: **funcționează**, pentru că lista este aplicată doar pe traficul care *intră* dinspre birou.

P3 - DMZ-ul nu inițiază

Exemplul 6.2. „Poate doar să răspundă” înseamnă că traficul dinspre DMZ spre interior este permis **numai** dacă face parte dintr-o conversație pornită din interior. Un ACL clasic nu poate exprima asta - el vede pachete, nu conexiuni. Soluția minimală este cuvântul cheie *established*.

```
R-FIRMA(config)# ip access-list extended DMZ-IN
R-FIRMA(config-ext-nacl)# 10 permit tcp host 10.1.40.10 10.0.0.0 0.255.255.255 established
R-FIRMA(config-ext-nacl)# 20 deny ip host 10.1.40.10 10.0.0.0 0.255.255.255
R-FIRMA(config-ext-nacl)# 30 permit ip host 10.1.40.10 any
R-FIRMA(config-ext-nacl)# exit
R-FIRMA(config)# interface gigabitEthernet 0/0/1
R-FIRMA(config-if)# ip access-group DMZ-IN in
```

Listingul 6.3 P3 copiază

Limitele lui established. Verifică doar biții ACK și RST din antetul TCP, deci un pachet fabricat cu ACK setat trece. Nu funcționează pentru UDP și ICMP. Într-o rețea reală, aici s-ar folosi un firewall cu stare sau un ACL reflexiv, cu *reflect* și *evaluate*.

P4 - Accesul de administrare

Traficul spre liniile VTY ale ruterului nu se filtrează pe interfață, ci direct pe linii, cu *access-class*. Aici este suficientă o listă **standard**: conține doar de unde vine conexiunea.

```
R-FIRMA(config)# ip domain-name firma.local
R-FIRMA(config)# crypto key generate rsa
R-FIRMA(config)# username admin privilege 15 secret Admin123
R-FIRMA(config)# access-list 10 remark doar statiile ADMIN
R-FIRMA(config)# access-list 10 permit 10.1.10.0 0.0.0.255

R-FIRMA(config)# line vty 0 4
R-FIRMA(config-line)# transport input ssh
R-FIRMA(config-line)# login local
R-FIRMA(config-line)# access-class 10 in
R-FIRMA(config-line)# exec-timeout 5 0
```

Listingul 6.4 P4 copiază

Verificați-vă înțelegerea



Figura 6.2 Lista OASPETI-IN, testată pe cinci pachete.

Ultimul pachet este important: vine din BIROURI, deci nu se potrivește cu nicio regulă din această listă și cade pe deny implicit. Nu are însă nicio consecință - lista este aplicată pe 0/0/0.30, iar acel pachet nu trece niciodată pe acolo. Un ACL contează doar acolo unde este aplicat.

6.6 Contorul, cel mai bun instrument de depanare

```
R-FIRMA# show access-lists
R-FIRMA# clear access-list counters
```

Listingul 6.5 verificare copiază

Ieșirea arată, pentru fiecare regulă, de câte ori s-a potrivit:

```
Extended IP access list OASPETI-IN
 10 remark permite accesul la serverul web din DMZ
 20 permit tcp 10.1.30.0 0.0.0.255 host 10.1.40.10 eq 80
 40 deny ip 10.1.30.0 0.0.0.255 10.0.0.0 0.255.255.255 (8 match(es))
 60 permit ip 10.1.30.0 0.0.0.255 any (4 match(es))
```

Listingul 6.6 ce trebuie să apară

Cum se citește. Dacă o regulă are **zero potriviri**, traficul nu ajunge la ea: fie lista e pe interfața greșită, fie pe direcția greșită, fie o regulă de deasupra prinde deja traficul. Dacă are potriviri, dar rezultatul nu e cel dorit, atunci regula e scrisă greșit. *Cele două cazuri se repară complet diferit*, iar contorul vă spune în care sunteți.

Recompletați acum tabelul de conectivitate de la secțiunea 5 și comparați cu referința. Fiecare celulă care s-a schimbat trebuie să corespundă unei politici - dacă s-a schimbat ceva neprevăzut, aveți o regulă prea largă.

6.7 NAT: ieșirea în Internet

Toate adresele interne sunt private, deci nerutabile în Internet. ISP-ul nici măcar nu are rute spre ele. Ne trebuie traducere.

1. Marcați interfețele

fiecare interfață e „inside” sau „outside”

```
R-FIRMA(config)# interface gigabitEthernet 0/0/0.10
R-FIRMA(config-subif)# ip nat inside
R-FIRMA(config-subif)# exit
R-FIRMA(config)# interface gigabitEthernet 0/0/0.20
R-FIRMA(config-subif)# ip nat inside
R-FIRMA(config-subif)# exit
R-FIRMA(config)# interface gigabitEthernet 0/0/0.30
R-FIRMA(config-subif)# ip nat inside
R-FIRMA(config-subif)# exit
R-FIRMA(config)# interface gigabitEthernet 0/0/1
R-FIRMA(config-if)# ip nat inside
R-FIRMA(config-if)# exit
R-FIRMA(config)# interface serial 0/1/0
R-FIRMA(config-if)# ip nat outside
R-FIRMA(config-if)# exit
```

Fără aceste marcaje, NAT-ul nu face absolut nimic - indiferent cât de corecte sunt regulile. Este prima verificare atunci când „NAT-ul nu merge”.

2. **PAT pentru toate stațiile interne**

PAT cu adresa interfeței de ieșire

```
R-FIRMA(config)# access-list 100 remark ce se translateaza
R-FIRMA(config)# access-list 100 permit ip 10.1.10.0 0.0.0.255 any
R-FIRMA(config)# access-list 100 permit ip 10.1.20.0 0.0.0.255 any
R-FIRMA(config)# access-list 100 permit ip 10.1.30.0 0.0.0.255 any
```

```
R-FIRMA(config)# ip nat inside source list 100 interface serial 0/1/0 overload
```

Iată a doua utilizare a listelor de acces, promisă în cursul 7: aici lista nu filtrează nimic - doar **descrie** traficul care trebuie translatat. Aceeași sintaxă, alt rol.

3. **NAT static pentru serverul web (P5)**

o adresă publică fixă pentru SRV-WEB

```
R-FIRMA(config)# ip nat inside source static 10.1.40.10 203.0.113.33
```

Testați din „Internet”: de pe serverul NET, `ping 203.0.113.33` - răspunde serverul din DMZ. Iar `ping 10.1.40.10` de acolo nu merge și nu are cum: adresa privată nu există în Internet. Alternativ, dacă vreți să publicați doar portul 80 și să păstrați adresa publică pentru altceva: port forwarding

```
R-FIRMA(config)# ip nat inside source static tcp 10.1.40.10 80 203.0.113.1 80
```

4. **Priviți traducerea cu ochii voștri**

verificare NAT

```
R-FIRMA# show ip nat translations
R-FIRMA# show ip nat statistics
R-FIRMA# clear ip nat translation *
```

În bancul din pagină: dați de pe PC-BIR `ping 8.8.8.8` și citiți tabelul *Traseul ultimului pachet*. Coloana *IP sursă* se schimbă exact la trecerea prin R-FIRMA: până acolo este 10.1.20.11, după aceea 203.0.113.1.

Poziție	IP sursă	IP destinație
între SW1 și R-FIRMA	10.1.20.11	8.8.8.8
între R-FIRMA și ISP	203.0.113.1	8.8.8.8
răspunsul, între ISP și R-FIRMA		
răspunsul, între R-FIRMA și SW1		

Completați ultimele două rânduri singuri, apoi verificați în Packet Tracer, în *Simulation*.

Excepția de la regula celor două adrese În laboratorul 1 ați învățat că adresa IP nu se schimbă niciodată pe drum. NAT este exact încălcarea acelei reguli - și motivul pentru care este criticat de puriști. Este, în același timp, motivul pentru care IPv4 mai trăiește.



Figura 6.3 PAT, ca reper: cum arată tabela.

6.8 Provocare

Exemplul 6.3. Conducerea revine cu trei cerințe suplimentare. Implementați-le pe toate, fără a strica politicile existente.

1. **Oaspeții nu au voie la Internet în afara programului de lucru** (luni-vineri, 8:00–18:00).
2. **Un singur calculator din BIROURI**, cel de la contabilitate (10.1.20.50), **trebuie să ajungă la segmentul ADMIN** - dar numai pe portul 3389.
3. **Descărcările prin FTP sunt interzise pentru toată lumea, mai puțin pentru ADMIN.**

Pentru fiecare cerință, precizați: tipul de listă, poziția exactă a regulii în lista existentă, interfața și direcția.

Rezolvare. 1. Vă trebuie un `time-range` și o regulă condiționată temporal:

indicație

```
R-FIRMA(config)# time-range PROGRAM
R-FIRMA(config-time-range)# periodic weekdays 8:00 to 18:00
! apoi, în lista OASPETI-IN, regula 30 devine:
R-FIRMA(config-ext-nacl)# no 30
R-FIRMA(config-ext-nacl)# 30 permit ip 10.1.30.0 0.0.0.255 any time-range PROGRAM
```

2. Regula trebuie să fie **deasupra** regulii 10 din `BIROURI-IN`, care blochează tot traficul spre ADMIN. Aici se vede de ce numerotarea explicită a regulilor este esențială - puteți insera la poziția 5, fără să rescrieți lista:

indicație

```
R-FIRMA(config)# ip access-list extended BIROURI-IN
R-FIRMA(config-ext-nacl)# 5 permit tcp host 10.1.20.50 10.1.10.0 0.0.0.255 eq 3389
```

3. FTP folosește portul de control 21 și, în modul activ, portul de date 20. O regulă care blochează doar `eq 21` oprește stabilirea sesiunii, deci este suficientă în practică - dar gândiți-vă ce se întâmplă cu FTP pasiv, unde portul de date este negociat dinamic și poate fi oricare peste 1024. Este exact limitarea despre care vorbea cursul 7 și motivul pentru care firewall-urile moderne inspectează conținutul, nu doar anteturile.

6.9 Ce se predă

Tabelul 6.4 Ce se predă.

Livrabil	Format	Punctaj
Fișierul Packet Tracer cu politicile P1–P5 implementate	.pkt	35 %
Cele două tabele de conectivitate, înainte și după, cu explicarea diferențelor	document	25 %
Documentarea translatării NAT, segment cu segment	document	20 %
Provocarea: cele trei cerințe noi, cu regulă, poziție, interfață și direcție	document	20 %

Exerciții

1. Ce vede o lista de acces standard?
 - a. Sursa și destinația
 - b. Doar adresa sursă
 - c. Doar portul
 - d. Adresa MAC

2. O lista contine doar reguli deny. Ce trece prin ea?
 - a. Tot ce nu e mentionat explicit
 - b. Nimic: la final exista un deny implicit
 - c. Doar traficul ICMP
 - d. Depinde de directie
3. O regula din ACL are contorul la zero, desi traficul respectiv exista. Ce verificati?
 - a. Ca regula e scrisa gresit
 - b. Ca lista e aplicata pe interfata si directia corecta, sau ca o regula de deasupra prinde deja traficul
 - c. Adresa MAC a sursei
 - d. Masca de subretea
4. De ce se plaseaza o lista extinsa cat mai aproape de sursa?
 - a. Ca sa fie mai usor de scris
 - b. Ca traficul interzis sa fie oprit inainte de a consuma resursele retelei
 - c. Pentru ca IOS o cere
 - d. Nu conteaza plasarea
5. Ce face comanda ip nat inside source list 100 interface serial 0/1/0 overload?
 - a. Filtreaza traficul din lista 100
 - b. Translateaza adresele descrise de lista 100 spre adresa interfetei seriale, folosind porturi distincte
 - c. Creeaza o ruta statica
 - d. Blocheaza NAT-ul
6. Un oaspete poate deschide site-ul din DMZ, dar ping-ul catre acelasi server esueaza. E o problema?
 - a. Da, ceva e configurat gresit
 - b. Nu: regula permite doar TCP portul 80, iar ping-ul este ICMP
 - c. Da, lipseste NAT-ul
 - d. Nu, ping-ul nu functioneaza niciodata prin ruter

Extras din volumul „Rețele Locale - Note de curs și lucrări de laborator”. Varianta online a acestui capitol conține figurile în formă interactivă.