ACCESS CONTROL LIST (ACL)

CUPRINS

- Definiție ACL
- Funcționarea ACL-urilor
- Tipuri de liste de acces
- Mod de configurare

ACL – generalități

Ce este un Access List?

- Listele de acces sunt un set de condiții specificate de administrator pentru gestionarea unor anumite tipuri de trafic
- Pot fi folosite atât pentru **filtrarea traficului**, cât și în diverse alte procese ce au nevoie de selecția doar unei părți a traficului ce trece prin ruter

Ce oferă ACL-urile

- Mecanisme pentru controlul și monitorizarea traficului
- Identificarea pachetelor cu prioritate diferită (QoS)
- Identificarea pachetelor pentru criptarea traficului
- Controlul actualizărilor protocoalelor de rutare

Dezavantaje?

- Timp de latență mai mare
- Încărcare suplimentară a echipamentului

Ruter dedicat

• principala funcție: **rutare**
• permit implementarea de funcții de filtrare
• nu oferă implicit criptare
• folosește protocoale de nivel 3 și 4 pentru a lua decizii.

VS

Firewall dedicat

• principala funcție: **filtrare**
• poate ruta, dar suporta mult mai putine facilități
• oferă criptare HW la rate foarte mari
• ia decizii pe baza protocoalelor de nivel 3-7
• server ssh integrat

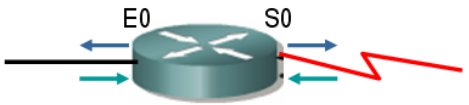
Filtarea traficului cu ACL

Definiție ACL

- O listă de acces este un set de reguli
- **ACL**-urile pot fi create pentru multiple protocoale de layer 3, cum ar fi IP, IPX sau AppleTalk
- Poate fi folosit pentru filtrarea traficului, permițând obținerea **accesului sigur** în și dintr-o rețea
- O regula are doua părți: o parte de testare și una de acțiune
- Regulile sunt testate secvențial. Dacă o regulă face match, se aplică acțiunea specificată
- Dacă s-au epuizat toate regulile, pachetul este respins

Filtrarea traficului folosind ACL

- Dacă este aplicat pe o interfață, regulile din ACL vor filtra traficul pe respectiva interfață
- O interfață suportă ACL-uri atât pentru traficul ce este primit pe interfată **(inbound)** cât și pentru traficul ce este trimis pe interfață **(outbound)**
- Pentru fiecare protocol rutat configurat pe o interfață, un router suportă câte o pereche de ACL-uri
  - 1 ACL inbound
  - 1 ACL outbound

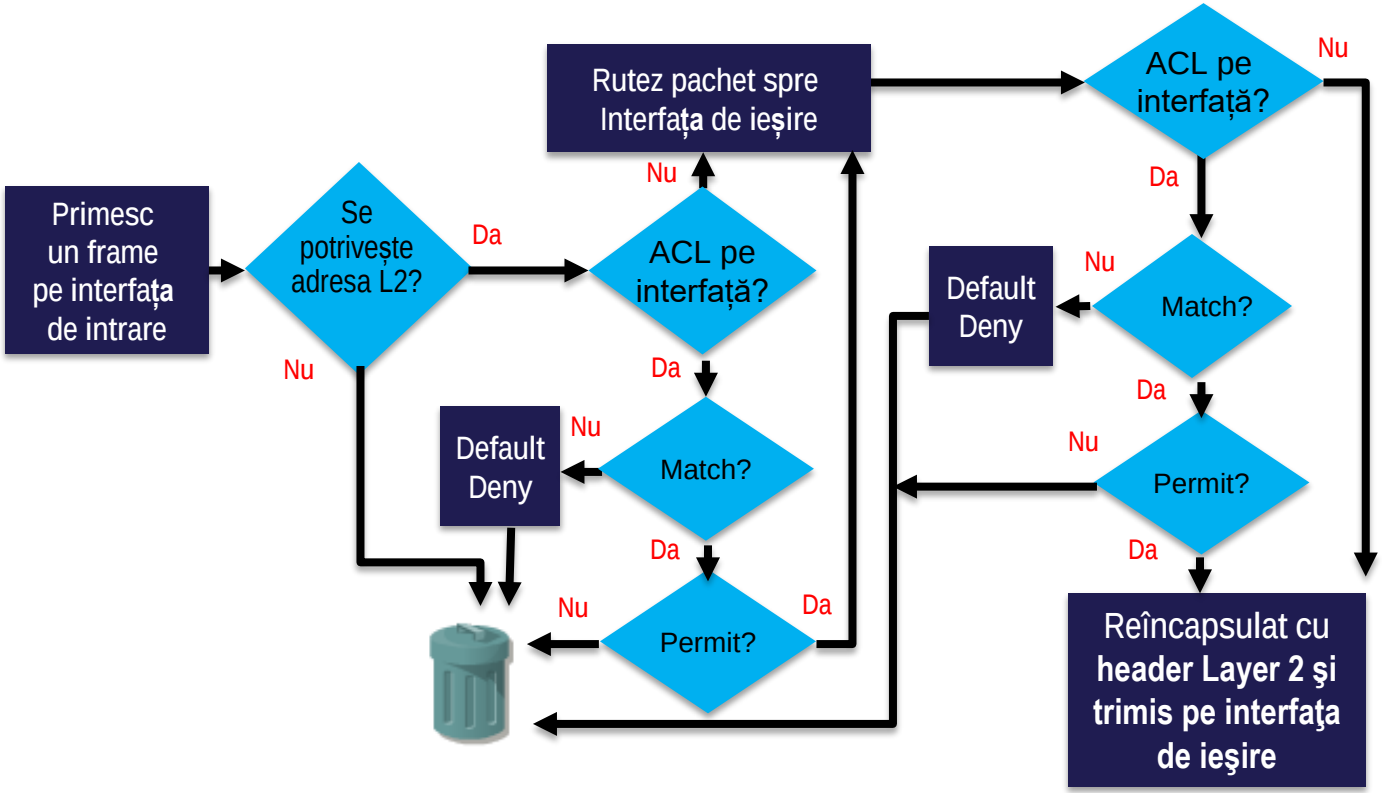


- Pentru un router ce are 2 interfețe și 3 protocoale rutate configurate (IP, IPX, AppleTalk), nr. maxim de ACL-uri ce pot fi configurate:
  - 2 (interfețe) x 3 (protocoale rutate) x 2 (in și out)

Funcționarea ACL-urilor

- Deciziile de forward-are se pot face pe baza:
  - adresa sursei (IP-ul sursei)
  - adresa destinatiei (IP-ul destinației)
  - protocol
  - numărul portului
- Declarațiile care compun un ACL sunt rulate secvențial **de la prima declarație până la ultima**
- Dacă o condiție din ACL este indeplinită pachetului afectat îi este permis sau refuzat accesul, în funcție de respectiva declarație, iar **restul ACL-ului nu se mai verifică**
- **La sfarșitul** oricărui ACL se găsește o declarație **"deny any" implicită**
- Aceasta declarație "deny any" nu este vizibilă, dar nu va permite accesul nici unui pachet care nu a corespuns condițiilor din celelalte declarații ale ACL-ului

Funcționarea ACL-urilor



Tipuri de liste de access

- Liste de acces standard

```
R(config)#access-list 50 permit 172.16.0.0 0.0.255.255
```

- Liste de acces extinse

```
R(config)#access-list 100 permit tcp 172.16.0.0 0.0.255.255
 192.168.10.0 0.0.0.255 eq 23
```

Wildcard mask

- Folosit pentru a identifica biții ce doresc să fie verificați dintr-o adresă IP
- Un șir de 32 de biți
  - biţii de 0 fac match
  - biţii de 1 sunt ignoraţi

```
Rio(config)#access-list 10 permit 172.16.0.0 0.0.255.255
```

Se pot folosi 2 cuvinte cheie in ACL-uri:

- **any** - înseamnă adresa IP 0.0.0.0 și WM 255.255.255.255, toate IP-urile vor face match
- **host** – testează egalitatea cu o adresă de host, echivalent cu WM 0.0.0.0

ACL-uri standard

- ACL-urile standard pot fi folosite pentru a filtra pachete doar în functie de **sursă**.
- Identificate printr-un număr între 1 si 99, sau, în versiunile mai recente de IOS, între 1300 si 1999.
- Reguli noi pot fi adăugate numai la finalul ACL-ului.

```
Rio(config)#access-list 50 deny 172.16.1.1
Rio(config)#access-list 50 permit 172.16.0.0 0.0.255.255
```

ACL standard pentru remote connections

- Aplicarea ACL standard pe liniile VTY:

```
R(config)#line vty 0 4
R(config-line)#access-class  access-list-number
{in [vrf-also]|out}
```

Editarea unui acces list

- Pentru a edita un ACL trebuiesc făcuți pașii:
  - copiați ACL-ul într-un fișier text
  - ștergeți ACL-ul din fișierul de configurare al router-ului folosind ‘no’ și declarația ACL-ului
  - faceți modificările necesare în fișierul text
  - copiați pe ruter ACL-ul modificat, în global configuration mode

Named ACLs

- Nu mai sunt folosite numere pentru a identifica ACL-uri, ci nume.
- Este posibilă numerotarea regulilor ce sunt adăugate, pentru ca apoi să se poată face modificări fără a șterge complet lista.

Configurarea Named ACLs

```
Mirana(config)#ip access-list extended Bugs
Mirana(config-ext-nacl)#20 permit ip any anyc
```

Am uitat 2 reguli ce trebuiau puse înainte!!!

```
Mirana(config-ext-nacl)#5 permit icmp host 10.0.0.0 any
Mirana(config-ext-nacl)#10 deny icmp any any
```

Am gresit o regulă!!!

```
Mirana(config-ext-nacl)#no 5
Mirana(config-ext-nacl)#5 permit icmp host 10.0.0.1 any
```

Aplicarea pe interfată

```
Mirana(config)#interface fastEthernet 0/1
Mirana(config-if)#ip access-group Bugs
```

Comentarii despre ACL

- Permit trafic către reţeaua A şi opresc trafic către host B

```
R(config)#access-list 50 remark permit traficul spre A
R(config)#access-list 50 permit 172.16.0.0 0.0.255.255
R(config)#access-list 50 remark opresc traficul spre B
R(config)#access-list 50 deny 192.168.10.15
```

- Un comentariu este limitat la 100 de caractere

Alți parametri ai listelor de acces

- **established** – filtrează pachetele TCP care folosesc o conexiune deja stabilită (au bitul ACK setat). Se poate folosi doar pentru liste extinse.
- **log** – generează un mesaj ce cuprinde: nr. listei, dacă a fost acceptat/respins pachetul, sursa, nr. de pachete. Mesajul este generat pentru primul pachet care corespunde unei reguli, iar apoi la intervale de 5 minute

Verificarea ACL-urilor

- Aceste comenzi **show** verifica **continutul** si **pozitionarea** ACL-urilor:

Comanda	Descriere
`show ip interface`	Informații privind numărul de ACL-uri de intare și ieșire
`show access-list`	Afișează conținutul ACL-urilor configurate pe router
`show running-config`	Afișează, printre altele, poziționarea și conținutul ACL-urilor configurate

Log-uri

```
R(config)#access-list 50 permit 172.16.0.0 0.0.255.255 log
```

- Generează un mesaj ce cuprinde
  - nr. listei
  - dacă a fost acceptat/respins pachetul
  - sursa
  - nr. de pachete
- Mesajul este generat pentru primul pachet care corespunde unei reguli, iar apoi la intervale de 5 minute

Exemple de ACL-uri

- Construiți o listă de acces care să permită doar traficul de la stația 193.230.2.1

```
#access-list 1 permit host 193.230.2.1
#access-list 2 permit 193.230.2.1 0.0.0.0
#access-list 3 permit 193.230.2.1
```

- Soluție folosind ACL extins

```
#access-list 101 permit ip host 193.230.2.1 any
```

Exemple de ACL-uri

- Care este efectul următoarelor linii?

```
#interface ethernet 4
      #ip access-group 199 out
#access-list 199 permit ip any any
#access-list 199 deny ip 106.45.0.0 0.0.255.255 any
#access-list 199 deny tcp any 44.7.12.224 0.0.0.15 eq
ftp
#access-list 199 deny udp 23.145.64.0 0.0.0.255 host
1.2.3.4 eq rip
```