Lab 4. Laboratori d'ACLs (Access Lists) i NAT amb IOS

1. Introducció

Les llistes d'accés (ACL) s'usen per al filtratge de paquets en funció de certs paràmetres com ara les adreces de xarxa origen o destinació, els ports origen o destinació, el tipus de protocol (ip, icmp, tcp, udp, etc.)). Una de les aplicacions on es fan servir més les llistes d'accés és a la seguretat de la xarxa. Amb les ACL es pot bloquejar el trànsit no desitjat en una interfície ja sigui de sortida o d'entrada. Les ACLs no només es fan servir per seguretat, sinó que també per identificar paquets en aplicacions com ara NAT (Network Address Translation), en BGP per filtrar rutes en crear polítiques d'encaminament, etc.

Hi ha ACLs per a diferents piles de protocols: TCP/IP, IPX/SPX, Apple, etc. Aquest document se centra en les ACL aplicades a seguretat a la xarxa per a la pila de protocols TCP/IP. Capa protocol té assignat un rang de ACLs. Per exemple les ACLs entre la 1 i la 199 s'usen en TCP/IP.

Quan creem una llista d'accés i l'apliquem a una interfície d'entrada o sortida, estem creant una seqüència d'instruccions que es revisen cada vegada que un paquet entra o surt per aquesta interfície. És important notar diverses característiques de les ACLs.

Primer, una ACL s'aplica a la interfície ja sigui d'entrada o de sortida. Es pot crear una ACL per a la interfície de sortida i una altra de diferent per la interfície d'entrada.

Segon, les ACL són seqüències d'instruccions que són revisades contra el paquet. L'ordre de les instruccions és important, ja que quan una línia de la seqüència dóna cert a la comprobació, es pren una acció i se surt de l'ACL, és a dir no es continua revisant per comprovar que hi hagi una altra línia de la seqüència que també resulta certa. Per tant, és molt important dissenyar l'ACL en la seqüència que ens interessi més.

Per exemple, no és el mateix aquestes dues línies d'una ACL:

- Si el paquet és ICMP rebutjar
- Si el paquet és IP acceptar

que la seqüència:

- Si el paquet és IP acceptar
- Si el paquet és ICMP rebutjar

Suposem que arribés un paquet ICMP. En el primer cas, el paquet es rebutjaria ja que la primera línia es compleix, el paquet és ICMP. En el segon cas el paquet ICMP s'acceptaria ja que la primera línia també es compleix, de manera que ja no es comprovaria la segona.

Un altre aspecte important és que no podem inserir línies a la seqüència. Si ens equivoquem en crear-la o volem inserir una línia, cal esborrar les línies fins al punt d'inserció.

Finalment, també **molt important**, l'última línia d'una llista d'accés **mai** apareix, és a dir, existeix de forma explicita i sempre és **denegar tot**.

Dins les llistes d'accés TCP/IP hi ha dos tipus d'ACLs

- Llistes d'accés IP estàndard (1-99)
- Llistes d'accés IP esteses (100-199)

2. Wildcard mask

La wildcard mask és una màscara de 32 bits que indica quins bits de l'adreça IP s'han de comprovar i quins no. Si els bits de la màscara estan a 0 aleshores es comproven, si estan a 1 aleshores no es comproven.

Per exemple, si volem que un paquet que entra es comprovi si pertany al host amb adreça IP `145.34.5.6`, volem que es comprovin tots els bits de l'adreça IP. Això significa que la wildcard mask seria `0.0.0.0`. En aquest cas se sol substituir la tupla *`@IP WildcardMask`* per *`host @IP`*. Per exemple la tupla *`145.34.5.6 0.0.0.0`* es pot expressar com a *`host 145.34.5.6`*.

Si volguéssim que no es comprovés cap bit, posaríem una wildcard mask de `255.255.255.255`. en aquest cas se sol substituir la tupla `@IP WildcardMask` per `any`. Per exemple la tupla `145.34.5.6 255.255.255.255` es pot expressar com a `any`.

També podem expressar xarxes. Per exemple, per comprovar tots els paquets que vinguin de la xarxa `145.34.5.0/24`. Això vol dir que hem de comprovar tots els paquets els primers 24 bits dels quals coincideixin amb els de l'adreça de xarxa. Després la WildcardMask corresponent hauria de ser `0.0.0.255`.

3. ACL estàndard

Les ACL estàndard només usen les adreces origen per fer la comprovació. Les llistes d'accés estàndard tenen números (`acl#`) compresos entre l'1 i el 99. La ordre té el format següent:

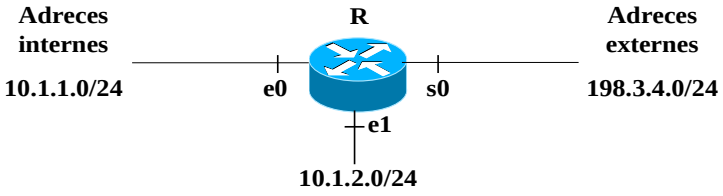
```
access-list acl# {deny|permit} {@IPsource WildcardMask | host @IPsource | any}
ip access-group acl# {in |out}
```

La primera ordre, access-list, crea la llista d'accés amb número `acl#` i amb condició denega o permet sobre l'adreça IP origen especificada amb la corresponent wildcard mask. Recordeu que la darrera línia d'una ACL mai no apareix però sempre és "`access-list acl# deny any`".

La segona ordre, `access-group`, assigna la llista d'accés acl# sobre el protocol IP sobre la interfície d'entrada o de sortida on s'executa aquesta ordre.
Per esborrar una ACL executar l'ordre:

```
no access-list acl#
```

Exemple: Volem denegar a la interfície s0 de sortida qualsevol paquet IP que provingui de la xarxa `10.1.1.0/24.`




```
R# configure terminal
R(config)# access-list 1 deny 10.1.1.0 0.0.0.255
R(config)# access-list 1 permit any
R(config)# interface s0
R(config-if)# ip access-group 1 out
R(config-if)# exit
R# show access-lists
```

Primer creem la llista d'accés amb número igual a 1 i deneguem tot el trànsit que vingui de la xarxa `10.1.1.0/24.` Com que l'última línia seria denegar tota la resta (ex.; la xarxa `10.1.2.0/24`), permetem la resta d'adreces. Apliquem aquesta ACL sobre la interfície de sortida s0 perquè si ho féssim sobre l'e0 d'entrada aleshores bloquejaríem els paquets de la xarxa `10.1.1.0/24` cap a la xarxa `10.1.2.0/24.`

4. ACLs esteses

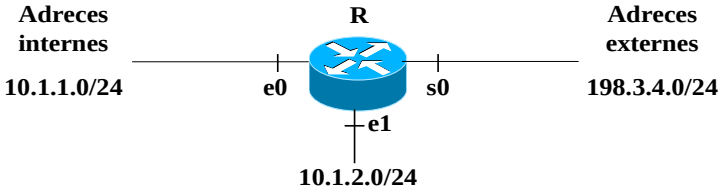
Les ACLs esteses permeten utilitzar tant les adreces origen com a destinació per fer la comprovació. A més, permeten especificar el protocol sobre el qual es vol fer la comprovació i en el cas que sigui TCP o UDP especificar el port. Les llistes d'accés esteses tenen números (`acl#`) compresos entre el 100 i el 199. La ordre té el format següent:

```
access-list acl# {deny|permit} protocol {@IPsource WildcardMask | host @IPsource | any}
[operador portsource] {@IPdest WildcardMask | host @IPdest | any} [operador portdest ]
[established]
ip access-group acl# {in |out}
```

La primera ordre, access-list, crea la llista d'accés estesa amb número acl# i amb condició de negatiu o permet sobre l'adreça IP origen i/o destinació especificades amb les corresponents wildcard masks. *`protocol`* pot ser ip, icmp. tcp, udp, etc. *`Operador`* pot ser *{lt, gt, eq, neq}* (less than, greater than, equal, non equal) i `port` és un port TCP o UDP. `established` només és vàlid amb tcp i, quan es fa servir, captura el trànsit tcp d'una connexió establerta. Per això el router mira els paquets amb el bit ACK o RST activats (el primer paquet de SYN sempre té aquests dos bits desactivats).

Recordeu que l'última línia d'una ACL no apareix però és "`access-list acl# deny ip any any`".

Exemple: Volem denegar a la interfície s0 de sortida qualsevol paquet ICMP que provingui de la xarxa `10.1.1.0/24` i l'accés a qualsevol port telnet (port 23) per part d'un host d'aquesta xarxa.



```
R# configure terminal
R(config)# access-list 101 deny icmp 10.1.1.0 0.0.0.255 any
R(config)# access-list 101 deny tcp 10.1.1.0 0.0.0.255 any eq 23
R(config)# access-list 101 permit ip any any
R(config)# interface s0
R(config-if)# ip access-group 101 out
R(config-if)# exit
R# show access-lists
```

Primer creem la llista d'accés estesa 101, denegant l'accés de paquets ICMP, segon una altra línia denegant l'accés a qualsevol host amb port 23, finalment permetem qualsevol altre tipus de trànsit. A continuació, apliquem la llista d'accés a la interfície de sortida s0.

5. Verificació

`R# show ip interface`	Mostra si hi ha alguna ACL a la interfície.
`R# show access-lists`	Mostra les ACL definides
`R# show running-config`	Per comprovar la configuració.

6. NAT

NAT (Network Address Translation) és el procés que permet la translació d'adreces privades a públiques mitjançant la substitució o alteració de les adreces IP o ports a les capçaleres IP i TCP del paquet transmès. Perquè NAT funcioni hem de disposar d'un router que implementi NAT en alguna o diverses variants: NAT estàtic, NAT dinàmic i NAT per ports (PAT).
No sempre es fa servir NAT per traslladar adreces privades a públiques. Hi ha ocasions en què es traslladen adreces privades a privades o adreces públiques a adreces públiques. Les adreces internes poden ser tant privades com a públiques. El cas més típic és aquell en què la direcció interna és una adreça privada i la direcció externa és una adreça pública. IOS utilitza la següent nomenclatura genèrica a l'hora de fer servir NAT:

- **Adreces locals internes (Inside local addresses):** l'adreça IP interna assignada a un host a la xarxa interna
- **Adreces globals internes (Inside global addresses):** l'adreça IP d'un host a la xarxa interna tal com apareix a una xarxa externa
- **Adreces locals externes (Outside local addresses):** l'adreça IP d'un host extern tal com apareix a la xarxa interna
- **Adreces globals externes (Outside global addresses):** l'adreça IP assignada a un host extern en una xarxa externa

Veure que la diferència entre una adreça local i global interna és que la direcció local interna és la direcció que volem traslladar mentre que la direcció global interna és la direcció ja traslladada.

7. NAT estàtic

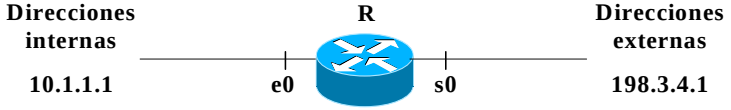
Fem servir NAT estàtic quan les adreces estan emmagatzemades en una taula de consulta del router i s'estableix un mapatge directe entre les adreces internes locals i les adreces internes globals. Això vol dir que per cada adreça interna local existeix una adreça interna global. Aquest mecanisme se sol utilitzar quan es vol canviar un esquema d'adreces d'una xarxa a un altre esquema d'adreces o quan es tenen servidors que han de mantenir una adreça IP fixa de cara a l'exterior com ara DNS o servidors web.

7.1. Configuració de NAT estàtic

Per configurar NAT estàtic seguirem els passos següents:

- Definir el mapeig de les adreces estàtiques:
  ip nat inside source static *local-ip global-ip*
  ip nat inside source static network *local-network global-network mask*
- Especificar la interfície interna
  ip nat inside
- Especificar la interfície externa
  ip nat outside

Exemple:




```
R# configure terminal
R(config)# ip nat inside source static 10.1.1.1 198.3.4.1
R(config)# interface e0
```

```
R(config-if)# ip nat inside
R(config-if)# exit
R(config)# interface s0
R(config-if)# ip nat outside
R(config-if)# exit
R(config)# exit
```

8. NAT dinàmic

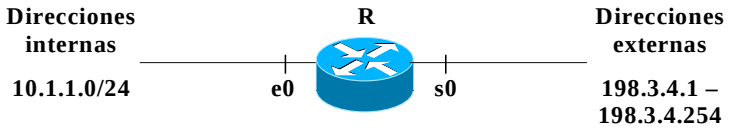
Fem servir NAT dinàmic quan disposem d'un conjunt d'adreces globals internes que s'assignaran de manera dinàmica i temporal a les adreces locals internes. Aquesta assignació s'efectuarà quan es rep trànsit al router i té un temporitzador assignat.

8.1. Configuració de NAT dinàmic

Per configurar NAT dinàmic seguirem els passos següents:

- Crear un conjunt d'adreces globals:
  ip nat pool *name start-ip end-ip {***netmask** *mask* | **prefix-length** *prefix-length}*
- Crear una ACL que identifiqui els hosts per a la translació
  access-list *access -list-number* **permit** *source {source-wildcard}*
- Configurar NAT dinàmic basat en la direcció origen
  ip nat inside source list *access-list-number* **pool** *name*
- Especificar la interfície interna
  ip nat inside
- Especificar la interfície externa
  ip nat outside

Exemple:




```
R# configure terminal
R(config)# ip nat pool fib-xc 198.3.4.1 198.3.4.254 netmask 255.255.255.0
R(config)# access-list 2 permet 10.1.1.0 0.0.0.255
R(config)# ip nat inside source list 2 pool fib-xc
R(config)# interface e0
R(config-if)# ip nat inside
R(config-if)# exit
R(config)# interface s0
R(config-if)# ip nat outside
R(config-if)# exit
R(config)# exit
R# show ip nat translations
```

Les entrades s'assignen per defecte 24 hores. Si es vol modificar el temporitzador, utilitzar la següent ordre:

```
R(config)# ip nat translation timeout seconds
```

On seconds és el temps que s'assignarà al temporitzador.

9. NAT overload o PAT (Port Address Translation)

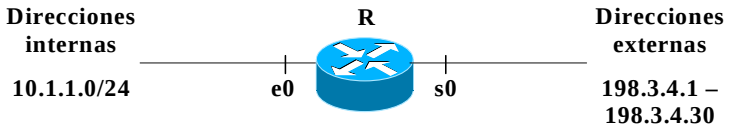
Fem servir PAT (NAT per ports) quan disposem d'una adreça global interna que pot direccionar tot un conjunt gran (centenars) d'adreces locals internes. Aquesta assignació la fa amb el parell direcció global/port. Encara que disposem de 65535 ports (16 bits) en realitat el router PAT només pot fer servir un subconjunt d'aquests ports (depèn del router, però aproximadament unes 4000 ports per adreça global). PAT es pot utilitzar en conjunció amb NAT dinàmic de manera que diverses adreces globals amb múltiples ports direccionen un nombre més gran d'adreces locals internes.

9.1. Configuració de PAT

Per configurar PAT seguirem els passos següents:

- Crear un conjunt d'adreces globals (pot ser una sola adreça):
  ip nat pool *name start-ip end-ip {***netmask** *mask* | **prefix-length** *prefix-length}*
- Crear una ACL que identifiqui els hosts per a la translació
  access-list *access -list-number* **permit** *source {source-wildcard}*
- Configurar PAT basat en la direcció origen
  ip nat inside source list *access-list-number* **pool** *name* **overload**
- Especificar la interfície interna
  ip nat inside
- Especificar la interfície externa
  ip nat outside

Exemple: farem servir fins a 30 adreces internes globals, cadascuna de les quals fa PAT




```
R# configure terminal
R(config)# ip nat pool fib-xc 198.3.4.1 198.3.4.30 netmask 255.255.255.0
R(config)# access-list 2 permet 10.1.1.0 0.0.0.255
R(config)# ip nat inside source list 2 pool fib-xc overload
R(config)# interface e0
R(config-if)# ip nat inside
R(config-if)# exit
R(config)# interface s0
R(config-if)# ip nat outside
R(config-if)# exit
R(config)# exit
R# show ip nat translations
```

En cas que no hi hagi un conjunt d'adreces globals podem fer servir l'adreça assignada a la interfície “s0” de la següent manera:

```
R(config)# ip nat inside source list 2 interfície s0 overload
```

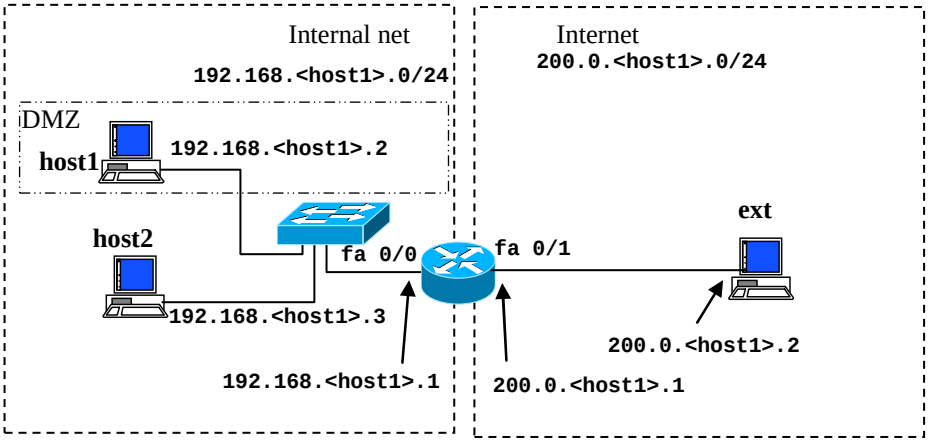
10. Verificació d'una configuració NAT

Fem servir les següents ordres per verificar que la configuració NAT és correcta (des de manera privilegiada):

```
R# show ip nat translations
R# show ip nat translations verbose
R# show ip nat statistics
R# debug ip nat (no debug ip nat)
R# clear ip nat translation *                    → elimina totes les translacions NAT
```

11. Realització de la pràctica

11.1. NAT



1) Configurar la xarxa de la figura. La xarxa de l'esquerra representa una xarxa privada i la de la dreta representa Internet. Fixeu-vos que la xarxa privada té adreces privades (no enrutables a Internet): Recordeu que els rangs d'adreces privades són 10.0.<host1>.0/8, 172.16.<host1>.0/12 i 192.168.<host1>.0/16. Configurar host1 i host2 perquè tinguin una ruta per defecte usant el router. Configurar el host que representa Internet (ext) perquè només sàpiga arribar a les adreces públiques: És a dir, no afegir a la taula d'encaminament d'ext cap ruta per defecte. D'aquesta manera, ext només podrà arribar a la xarxa directament connectada, que representa Internet. Apuntar les adreces IP configurades a la taula següent:

host1/e1	
host2/e1	
R1/fa0/0	
R1/fa0/1	
ext/e1	

2) Comprovar fent *pings* que hi ha connectivitat entre host1-host2-router i entre ext-router. Comprovar que no hi ha connectivitat entre host1/2-ext (ja que ext no pot contestar els datagrames que arriben amb una adreça font privada).
3) Configurar PAT (sense canviar la configuració anterior) perquè tots els hosts de la xarxa interna accedeixin a Internet amb l'adreça pública de la interfície fa0/1 del router (200. 0.< host1>.1):
   - Comprovar que tots dos hosts de la xarxa interna poden accedir a Internet.
   - Comprovar el funcionament de NAT amb `debug ip nat` (executa `no debug ip nat` per desactivar l'ordre).
   - Comprovar la taula NAT (`show ip nat translations`).
   - Comprovar que ext no pot accedir als hosts de la xarxa Interna (host1/2). Raonar perquè no és possible.
4) Configurar un static NAT de 200.0.< host1>.1 cap al host1. Comprovar amb "debug ip nat" al router que ext té connectivitat amb host1 (amb ping des d'ext).

11.2. ACLs

Continuant amb la configuració anterior:

5) Configurar una llista d'accés estàndard perquè només pugui accedir a Internet host2. Tindre en compte que l'ordre en què s'aplica NAT i ACL en una interfície és: primer ACL in, després NAT i finalment ACL out. Què passa amb ext? Es té accés a host1? Per què?
6) Esborrar l'ACL estàndard anterior i fer servir una ACL estesa per crear una configuració que permeti accedir des d'Internet només al servei ssh (port 22) de host1. Per comprovar-ho connectar des d'ext al servidor ssh de host1, i després intentar connectar des d'ext amb telnet a host1. Desitgem que host2 continuï amb accés a Internet, però des de host1 no ha de ser possible iniciar una connexió amb Internet. Comprovar-ho confirmant que és possible connectar amb telnet des de host2 a ext, però no des de host1.

12. Informe previ

1. Digues les comandes que permeten la configuració PAT del punt 3) del guió.
2. Digues les comandes que permeten la configuració NAT estàtic del punt 4) del guió.
3. Digues les comandes que permeten la configuració de les ACL del punt 5) del guió.
4. Digues les comandes que permeten la configuració de les ACL del punt 6) del guió.