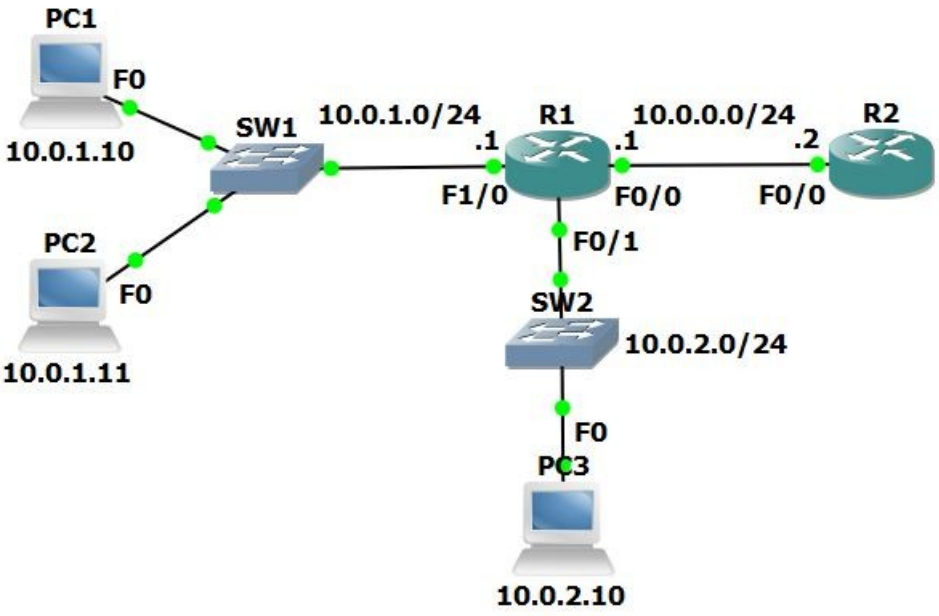
LABORATORIO

Access Control Lists (ACL)

En este laboratorio se configuraran ACLs de tipo Standard y Extended.

Topología



Los routes y las PCs ya fueron configurados con sus correspondientes direccionamientos IP, y R2 tiene configurado un enrutamiento estático hacia las redes 10.0.1.0/24 y 10.0.2.0/24.

Introducción

1. Conceptos básicos de ACLs

¿Qué hacen?

- Filtrado de paquetes evaluando cada paquete contra una lista de reglas.
- La evaluación se hace de manera ordenada. La **primera coincidencia** decide si un paquete se permite o se deniega.
- Si un paquete no coincide con ninguna, existe una **denegación implícita** al final de la ACL.

Casos de uso típicos

- Proteger la red de accesos no autorizados.
- Restringir los accesos a un servidor (ej. permitir sólo HTTP desde una determinada subred).
- Limitar quién puede administrar un router (aplicar ACLs a VTY).
- Filtrar tráfico entre zonas (DMZ, LAN, WAN).
- Mejorar la seguridad antes de llegar a un firewall.

Dirección de aplicación

Las ACLs se aplican en interfaces (físicas o virtuales) en dos direcciones:

- **In (inbound)**: Filtra paquetes que entran al dispositivo por esa interfaz (antes de procesarlos).
- **Out (outbound)**: Filtra paquetes que salen del dispositivo por esa interfaz (después de procesarlos).

Lógica de procesamiento

Las ACLs son listas secuenciales, es decir, el router revisa cada regla de arriba hacia abajo. La primera coincidencia decide si un paquete se permite (`permit`) o se deniega (`deny`). Si no hay coincidencia, se aplica la regla implícita "`deny ip any any`" al final.

2. Tipos de ACLs

Cisco clasifica las ACL de la siguiente manera:

Por funcionalidad

- **Standard**: filtran **sólo por dirección IP de origen.** No distinguen entre servicios (puertos). Simple, pero limitada.
- **Extended**: filtran por **origen, destino, protocolo** (TCP/UDP/ICMP/IP) y **puertos** (ej. TCP/80). Mucho más granulares y precisas.

Por formato

- **Numeradas**: creadas con números (ej. `access-list 10`, `access-list 101`).
  - Rangos para IPv4:
    - Standard: 1–99, 1300–1999
    - Extended: 100–199, 2000–2699

- **Nombradas** (recomendadas): Se usan nombres en lugar de números, son creadas con: `ip access-list standard <name>` o `ip access-list extended <name>`. Más fáciles de mantener, recordar y editar.

Nota: Las ACLs numeradas se configuran en configuración global, mientras que las nombradas tienen su propio submodo (`std-nacl` o `ext-nacl`), lo que permite editar reglas individuales (agregar, mover o eliminar por número de secuencia).

3. Estructura de una regla

Lógica de evaluación

- **El orden importa**: primera regla que coincide, se aplica la acción.
- **Acción**: permit o deny.
- **Match**: direcciones (origen o destino), protocolo (TCP/UDP/ICMP/IP), puerto (eq/gt/lt/range) y wildcard mask.

Wildcard mask

En Cisco se usa la wildcard mask (inversa de la máscara de red).

- Regla: bit **0** = debe coincidir; bit **1** = "no importa".
  - Ejemplos:
    - 10.1.1.0**/24** → 10.1.1.0 **0.0.0.255**.
    - `host 10.0.0.5` es equivalente a `10.0.0.5 0.0.0.0` (todos los bits deben coincidir).
    - `10.0.1.0 0.0.0.255` (cualquier host en la red **10.0.1.0/24**).
    - `0.0.0.0` = coincidencia exacta
    - `255.255.255.255` = coincide con cualquier dirección.

Comparación con máscara de red:

- Máscara de red (/24) **255.255.255.0** → wildcard **0.0.0.255**.

4. Reglas especiales

Palabras claves útiles

- `any`: equivale a `0.0.0.0 255.255.255.255`.
- `host x.x.x.x`: coincidencia exacta.
- `remark`: se utiliza para agregar un comentario

Operadores de puerto (para extended ACLs):

- `eq`: igual a
- `gt`: mayor que
- `lt`: menor que
- `range a b`: rango de `a` hasta `b`
  - Ejemplo
    - `permit tcp any host 192.168.1.10 eq 22` (permitir SSH desde cualquier origen al host 192.168.1.10).

Implicit deny

Al final de cada ACL hay una entrada `deny ip any any` implicita.

5. Dónde aplicar las ACLs

En interfaces

- Interface GigabitEthernet0/0: `ip access-group <name> in|out`.
  - `in`: filtra tráfico entrante hacia el router.
  - `out`: filtra tráfico que sale de la interfaz del router.

Controlar acceso a líneas VTY (administración remota)

- Líneas vty 0 a 4: `access-class ACL_NAME in`. (Útil para permitir sólo el acceso a administradores).

Buenas Prácticas

- **Extended ACLs**: aplicar **lo más cerca posible del origen,** para evitar que tráfico no deseado cruce la red.
- **Standard ACLs**: aplicar **lo más cerca posible del destino,** porque filtran solo por origen (si se coloca cerca del origen se podría bloquear tráfico legítimo hacia otras redes).

ACTIVIDADES

ACL Standard Numerada

1) Configurar y aplicar una ACL standard numerada en R1 que:

- Deniegue el tráfico de todos los hosts de la red 10.0.2.0/24 hacia R2.
- Las PCs en las redes 10.0.1.0/24 y 10.0.2.0/24 deben mantener la conectividad entre ellas.
- Las PCs en la red 10.0.1.0/24 deben mantener conectividad con R2.

La actividad especifica que se debe usar una ACL standard numerada en R1. Este tipo de ACL solamente chequea la dirección de origen, por lo tanto, la única forma de realizar esta tarea es aplicando la ACL de forma saliente (outbound) en la interfaz f0/0.

```
R1> enable
R1# configure terminal
R1(config)# access-list 1 deny 10.0.2.0 0.0.0.255
R1(config)# access-list 1 permit 10.0.1.0 0.0.0.255
```

Aplicación de la ACL:

```
R1(config)# interface f0/0
R1(config-if)# ip access-group 1 out
R1(config-if)# end
```

2) Verificar que las PCs 1 y 2 pueden realizar ping a R2, la PC3 no puede realizar ping a R2 pero si a las PCs 1 y 2.

ACL Extended Numerada

3) Configurar y aplicar una ACL extended numerada en R1 que:

- Permita acceso mediante Telnet desde la PC1 a R2.
- La conexión mediante Telnet a R2 debe ser denegada al resto de las PCs en la red.
- Todas las demás conexiones deben ser permitidas.
- Telnet ya fue configurado en R2, el password es “Cisco”.

Todo el tráfico desde la red 10.0.2.0/24 hacia R2 es denegado por la ACL standard numerada configurada anteriormente. Es necesario crear una nueva ACL que permita el tráfico Telnet hacia R2 (10.0.0.2) desde la PC1 (10.0.1.10) y denegar el tráfico del resto de hosts en la red 10.0.1.0/24. La regla implícita deny all al final

de la ACL bloqueará el tráfico Telnet del resto de hosts hacia R2, pero también bloqueará todo el tráfico desde la red 10.0.1.0/24, incluso el tráfico hacia la red 10.0.2.0/24. Por esta razón, es necesario bloquear explícitamente el tráfico Telnet y permitir otro tipo de tráfico.

Router R1

```
R1# configure terminal
R1(config)# access-list 100 permit tcp host 10.0.1.10 host 10.0.0.2 eq telnet
R1(config)# access-list 100 deny tcp 10.0.1.0 0.0.0.255 host 10.0.0.2 eq telnet
R1(config)# access-list 100 permit ip any any
```

Aplicación de la ACL:

```
R1(config)# interface f1/0
R1(config-if)# ip access-group 100 in
R1(config-if)# end
```

4) Verificar el funcionamiento de la ACL relizando pruebas de conectividad.

PC1 a R2:

```
PC1:\> telnet 10.0.0.2
Trying 10.0.0.2 ...Open
User Access Verification
Password: (Cisco)
R2>
```

PC2 a R2:

```
PC2:\> telnet 10.0.0.2
Trying 10.0.0.2 ...
% Connection timed out; remote host not responding

PC2:\> ping 10.0.0.2
Pinging 10.0.0.2 with 32 bytes of data:
Reply from 10.0.0.2: bytes=32 time<1ms TTL=254
Reply from 10.0.0.2: bytes=32 time=2ms TTL=254
Reply from 10.0.0.2: bytes=32 time<1ms TTL=254
Reply from 10.0.0.2: bytes=32 time<1ms TTL=254
Ping statistics for 10.0.0.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 2ms, Average = 0ms
```

PC3 a R2:

```
PC3:\> telnet 10.0.0.2
Trying 10.0.0.2 ...
% Connection timed out; remote host not responding

PC3:\> ping 10.0.0.2
Pinging 10.0.0.2 with 32 bytes of data:
Reply from 10.0.2.1: Destination host unreachable.
Reply from 10.0.2.1: Destination host unreachable.
Reply from 10.0.2.1: Destination host unreachable.
Reply from 10.0.2.1: Destination host unreachable.
Ping statistics for 10.0.0.2:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

PC3 a PC1:

```
PC3:\> ping 10.0.1.10
Pinging 10.0.1.10 with 32 bytes of data:
Reply from 10.0.1.10: bytes=32 time<1ms TTL=127
Reply from 10.0.1.10: bytes=32 time=1ms TTL=127
Reply from 10.0.1.10: bytes=32 time<1ms TTL=127
Reply from 10.0.1.10: bytes=32 time<1ms TTL=127
Ping statistics for 10.0.1.10:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

5) ¿Cuál fue la cantidad de paquetes Telnet permitidos por la ACL?

Con la ayuda del comando `show access-list <number>` se puede chequear la cantidad de paquetes permitidos.

```
R1# show access-lis 100
Extended IP access list 100
 permit tcp host 10.0.1.10 host 10.0.0.2 eq telnet (17 match(es))
 deny tcp 10.0.1.0 0.0.0.255 host 10.0.0.2 eq telnet (12 match(es))
 permit ip any any (8 match(es))
```

ACL Extended Nombrada

6) Remover la ACL extendida numerada recientemente aplicada a la interfaz f1/0. No es necesario borrar la ACL.

```
R1# configure terminal
R1(config)# interface f1/0
R1(config-if)# no ip access-group 100 in
R1(config-if)# exit
```

7) Configurar y aplicar una ACL extended nombrada en R1 de la siguiente manera:

- Permitir Telnet desde la PC1 hacia R2.
- El tráfico Telnet hacia R2 debe ser denegado para las otras PCs en la red.
- Permitir ping desde la PC2 hacia R2.
- Ping hacia R2 debe ser denegado para las otras PCs en la red.
- El resto de la conectividad se debe mantener tal como está.

Todo el tráfico desde la red 10.0.2.0/24 está denegado por la ACL standard numerada configurada anteriormente. Por lo tanto, es necesario configurar una ACL para asegurar el tráfico desde la red 10.0.1.0/24.

```
R1(config)# ip access-list extended Interface_f1/0_in
R1(config-ext-nacl)# permit tcp host 10.0.1.10 host 10.0.0.2 eq telnet
R1(config-ext-nacl)# deny tcp 10.0.1.0 0.0.0.255 host 10.0.0.2 eq
telnet
R1(config-ext-nacl)# permit icmp host 10.0.1.11 host 10.0.0.2 echo
R1(config-ext-nacl)# deny icmp 10.0.1.0 0.0.0.255 host 10.0.0.2 echo
R1(config-ext-nacl)# permit ip any any
R1(config-ext-nacl)# exit
```

Aplicación de la ACL:

```
R1(config)# interface f1/0
R1(config-if)# ip access-group Interface_f1/0_in in
R1(config-if)# end
```

8) Verificar el funcionamiento de la ACL

PC1 ping R2:

```
PC1:\> ping 10.0.0.2
Pinging 10.0.0.2 with 32 bytes of data:
Reply from 10.0.1.1: Destination host unreachable.
Reply from 10.0.1.1: Destination host unreachable.
Reply from 10.0.1.1: Destination host unreachable.
Reply from 10.0.1.1: Destination host unreachable.
Ping statistics for 10.0.0.2:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

PC1 Telnet R2:

```
PC1:\> telnet 10.0.0.2
Trying 10.0.0.2 ...Open
User Access Verification
```

Password: (Cisco)

R2>

PC2 ping R2:

PC2:\> **ping 10.0.0.2**

Pinging 10.0.0.2 with 32 bytes of data:

Reply from 10.0.0.2: bytes=32 time<1ms TTL=254

Reply from 10.0.0.2: bytes=32 time<1ms TTL=254

Reply from 10.0.0.2: bytes=32 time<1ms TTL=254

Reply from 10.0.0.2: bytes=32 time=1ms TTL=254

Ping statistics for 10.0.0.2:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

PC2 Telnet R2:

PC2:\> **telnet 10.0.0.2**

Trying 10.0.0.2 ...

% Connection timed out; remote host not responding

PC3 ping R2

PC3:\> **ping 10.0.0.2**

Pinging 10.0.0.2 with 32 bytes of data:

Reply from 10.0.2.1: Destination host unreachable.

Reply from 10.0.2.1: Destination host unreachable.

Reply from 10.0.2.1: Destination host unreachable.

Reply from 10.0.2.1: Destination host unreachable.

Ping statistics for 10.0.0.2:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC3 Telnet R2:

PC3:\> **telnet 10.0.0.2**

Trying 10.0.0.2 ...

% Connection timed out; remote host not responding

PC3 ping PC1:

PC3:\> **ping 10.0.1.10**

Pinging 10.0.1.10 with 32 bytes of data:

Reply from 10.0.1.10: bytes=32 time<1ms TTL=127

Reply from 10.0.1.10: bytes=32 time=1ms TTL=127

Reply from 10.0.1.10: bytes=32 time<1ms TTL=127

Reply from 10.0.1.10: bytes=32 time<1ms TTL=127

Ping statistics for 10.0.1.10:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),