

Listas de control de acceso en routers CISCO

Álvaro González Sotillo

May 25, 2016

Contents

1 LISTAS DE CONTROL DE ACCESO	1
2 PROCESAMIENTO DE ACL	2
3 COMANDOS ÚTILES	2
3.1 Borrar una ACL	2
3.2 Mostrar las ACL existentes	3
3.3 ACL asociadas a una interfaz	3
3.4 Asociar una ACL a una interfaz	3
3.5 Eliminar una ACL de una interfaz	3
4 ACL ESTANDAR	3
4.1 Ejercicio	3
4.2 Solución propuesta al ejercicio	3
5 ACL AMPLIADAS	4
5.1 IP	4
5.2 Protocolo de mensajes de control de Internet (ICMP)	4
5.3 Protocolo de control de transporte (TCP)	4
5.4 Protocolo de datagrama de usuario (UDP)	4
5.5 Ejercicio	5
5.6 Solución propuesta	5
6 Práctica	5
6.1 Enunciado	5

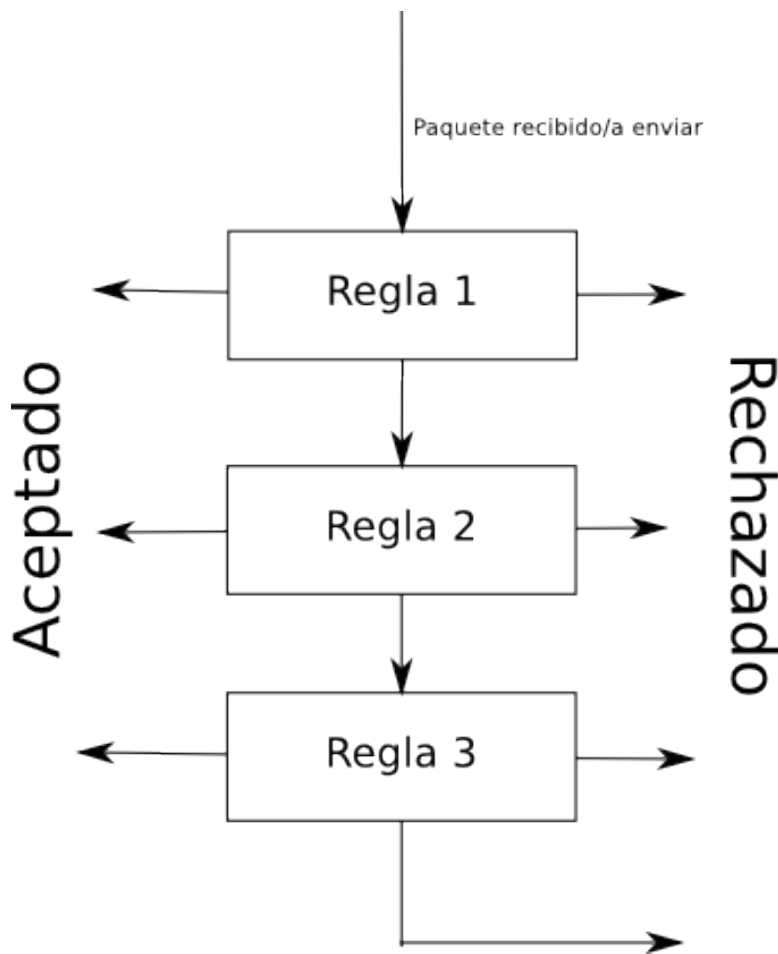
1 LISTAS DE CONTROL DE ACCESO

- Las ACL son listas con reglas.
 - Cada regla define una condición que puede cumplir un paquete
 - Cada regla define una acción (**permit**, **deny**) a ejecutar sobre el paquete que cumpla su condición
 - Siempre hay una regla al final que desecha cualquier paquete
- Se identifican por un número
 - Estándar:
 - * 1 a 99
 - * 1300 a 1999
 - Ampliadas:
 - * 100 a 199
 - * 2000 a 2699
- En versiones recientes de IOS (11.2) se pueden usar también nombres de ACL
- Una interfaz puede tener una ACL asociada en cada sentido

- Entrada de paquetes (Inbound)
- Salida de paquetes (Outbound)

2 PROCESAMIENTO DE ACL

- Al llegar un paquete
 1. Si la interfaz no tiene ACL de entrada, se acepta
 2. Si tiene ACL, se revisan las reglas de la lista
 - (a) Se comprueban en orden
 - (b) Si alguna deniega el paquete, se rechaza
 - (c) Si alguna acepta el paquete, se acepta
 - (d) Si ninguna se aplica al paquete, se rechaza
- Antes de enviar un paquete
 1. Si la interfaz no tiene ACL de salida, se envía
 2. Si tiene ACL, se revisan las reglas de la lista
 - (a) Se comprueban en orden
 - (b) Si alguna deniega el paquete, se desecha
 - (c) Si alguna acepta el paquete, se envía
 - (d) Si ninguna se aplica al paquete, se desecha



3 COMANDOS ÚTILES

3.1 Borrar una ACL

```
no access-list <numero>
```

3.2 Mostrar las ACL existentes

```
show ip access-list
```

3.3 ACL asociadas a una interfaz

```
show ip interface <interfaz>
```

Es necesario mirar el apartado Inbound y Outbound

3.4 Asociar una ACL a una interfaz

```
interface <interfaz>
ip access-group <numero ACL> <out o in>
```

3.5 Eliminar una ACL de una interfaz

```
interface <interfaz>
no ip access-group <numero ACL> <in o out>
```

4 ACL ESTANDAR

```
access-list access-list-number {permit|deny}
{host|source source-wildcard|any}.
```

- Solo hacen referencia a las direcciones IP de origen.
- Se puede especificar:
 - Una Red: Se especifica con IP y WILDCARD (no IP y máscara). El WILDCARD es la máscara de red con ceros y unos invertidos.
 - * Ejemplo: La red 192.168.1.0/24 se especifica como 192.168.1.0 0.0.0.255
 - Una dirección IP: Las siguientes especificaciones son equivalentes
 - * 192.168.1.1
 - * 192.168.1.1 0.0.0.0
 - Todas las direcciones: Las siguientes especificaciones son equivalentes
 - * any
 - * 0.0.0.0 255.255.255.255

4.1 Ejercicio

Se desea que la red 10.0.0.0/15 no sea enrutada, excepto el equipo 10.0.1.1, que es del administrador.

4.2 Solución propuesta al ejercicio

1. Se elige un número libre de ACL (en este caso, el 1).
2. Se introducen en orden todas las reglas de la ACL
3. Se recomienda hacer explícita la regla final de denegación.
4. El resultado sería el siguiente:

- Permitir el host 10.0.1.1

```
access-list 1 permit host 10.0.1.1
```

- Prohibir la red 10.0.0.0/15

```
access-list 1 deny 10.0.0.0 0.1.255.255
```

- Permitir el resto de redes

```
access-list 1 permit any
```

- Explicitar la regla final de denegación (va a estar de todas formas, pero ayuda a no olvidarse de ella)

```
access-list 1 deny any
```

- Asociar esta ACL a la interfaz de entrada de la red 10.0.0.0/15

```
interface Fa0/0
ip access-group 1 in
```

5 ACL AMPLIADAS

Pueden hacer referencia a otras características del paquete:

- Dirección de origen y destino
- Protocolo ICMP, TCP o UDP
- Puerto
- Conexión previamente establecida

5.1 IP

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]]
{deny | permit} protocol source source-wildcard destination destination-wildcard
[precedence precedence] [tos tos] [log | log-input]
[time-range time-range-name][fragments]
```

5.2 Protocolo de mensajes de control de Internet (ICMP)

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]]
{deny | permit} icmp source source-wildcard destination destination-wildcard
[icmp-type [icmp-code] | [icmp-message]] [precedenceprecedence] [tos tos]
[log | log-input] [time-range time-range-name][fragments]
```

5.3 Protocolo de control de transporte (TCP)

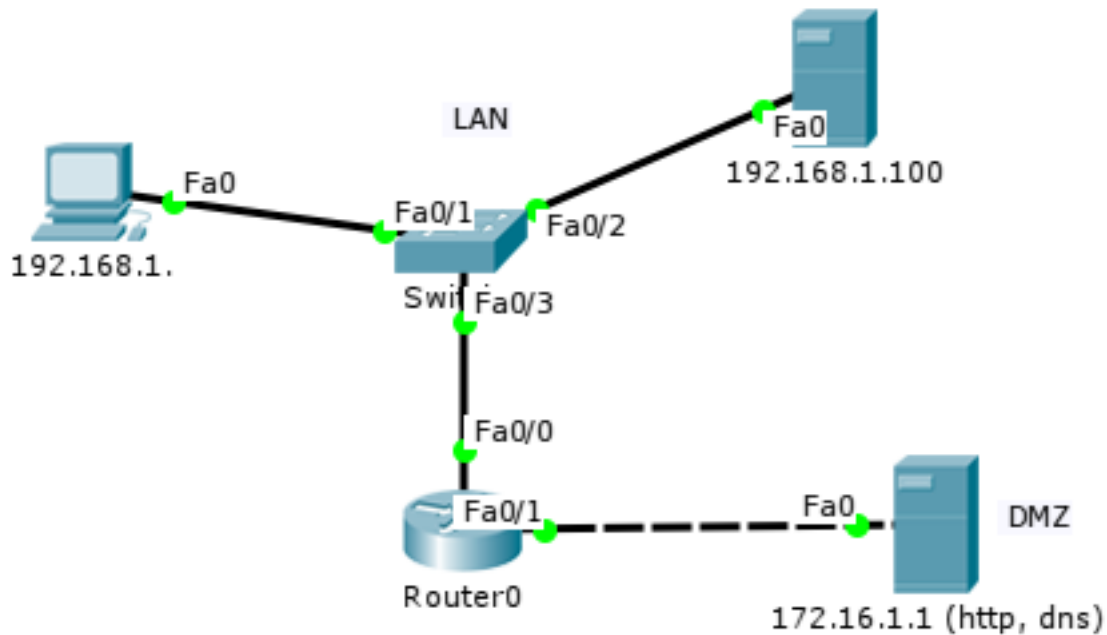
```
access-list access-list-number [dynamic dynamic-name [timeout minutes]]
{deny | permit} tcp source source-wildcard [operator [port]]
destination destination-wildcard [operator [port]] [established]
[precedence precedence] [tos tos] [log | log-input]
[time-range time-range-name][fragments]
```

5.4 Protocolo de datagrama de usuario (UDP)

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]]
{deny | permit} udp source source-wildcard [operator [port]]
destination destination-wildcard [operator [port]]
[precedence precedence] [tos tos] [log | log-input]
[time-range time-range-name][fragments]
```

5.5 Ejercicio

- Un router une las redes 192.168.1.0/24 (LAN) y 172.16.1.0/24 (DMZ). Se desea que:
 - Los usuarios de la LAN no puedan realizar PING hacia la DMZ.
 - El tráfico UDP está permitido por el puerto 53 (DNS)
 - Las únicas conexiones TCP permitidas entre LAN y DMZ serán las que tengan origen en la LAN.



5.6 Solución propuesta

Esta ACL debe colocarse en la tarjeta de la LAN, sentido inbound.

```
access-list 100 deny icmp any any
access-list 100 permit udp any any eq domain
access-list 100 permit tcp any any
access-list 100 deny ip any any
interface Fa0/0
ip access-group 100 in
```

Esta ACL debe colocarse en la tarjeta de la LAN, sentido outbound

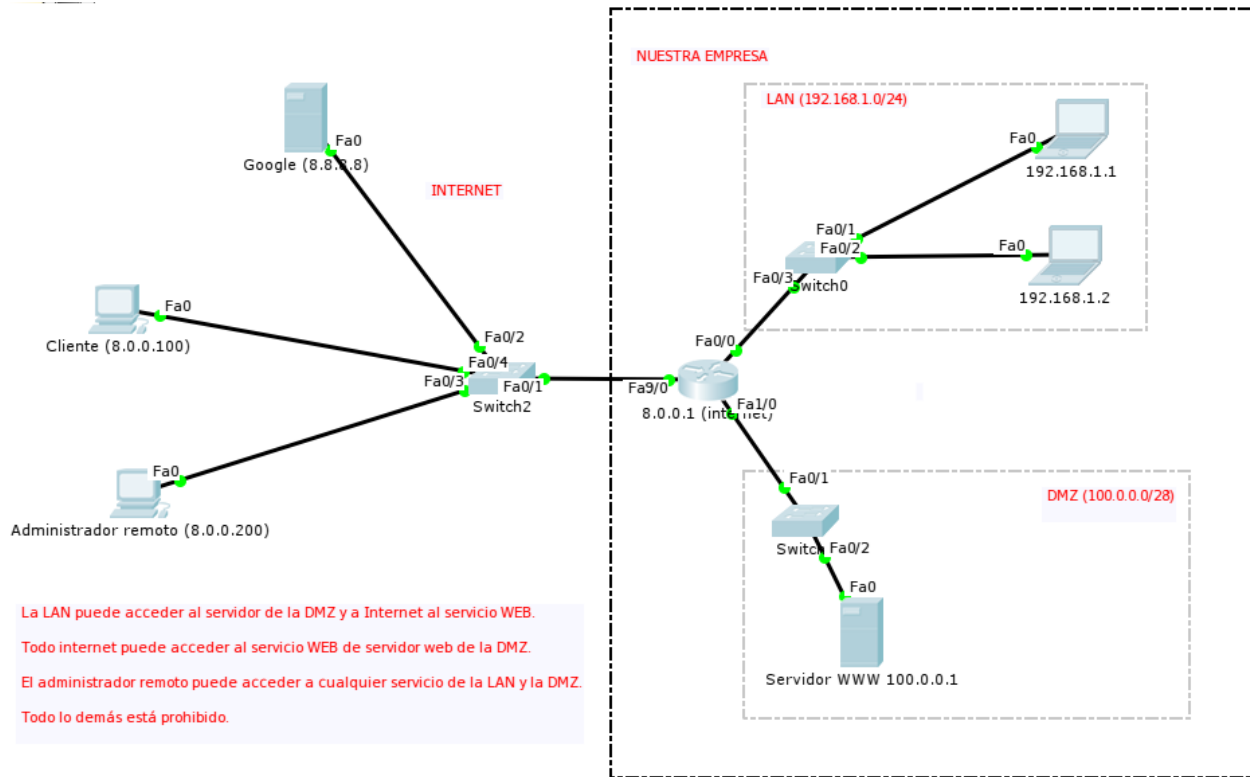
```
access-list 101 permit udp any eq 53 any
access-list 101 permit tcp any any established
access-list 101 deny ip any any
interface Fa0/0
ip access-group 101 out
```

6 Práctica

6.1 Enunciado

Fichero PKT inicial (adjunto al PDF)

[Enlace al fichero PKT inicial](#)



- La LAN puede acceder al servidor de la DMZ y a Internet al servicio WEB.
- Todo internet puede acceder al servicio WEB de servidor web de la DMZ.
- El administrador remoto puede acceder a cualquier servicio de la LAN y la DMZ.
- Todo lo demás está prohibido.
- Router
 - Internet: Fa9/0 8.0.0.1/8
 - DMZ: Fa1/0 100.0.0.14/28
 - LAN: Fa0/0 192.168.1.254/24
- Servidor Web:
 - DMZ: 100.0.0.1/28
- Administrador remoto:
 - 8.0.0.200