# Listas de control de acceso en routers CISCO

Álvaro González Sotillo

14 de mayo de 2019

## Índice



# 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

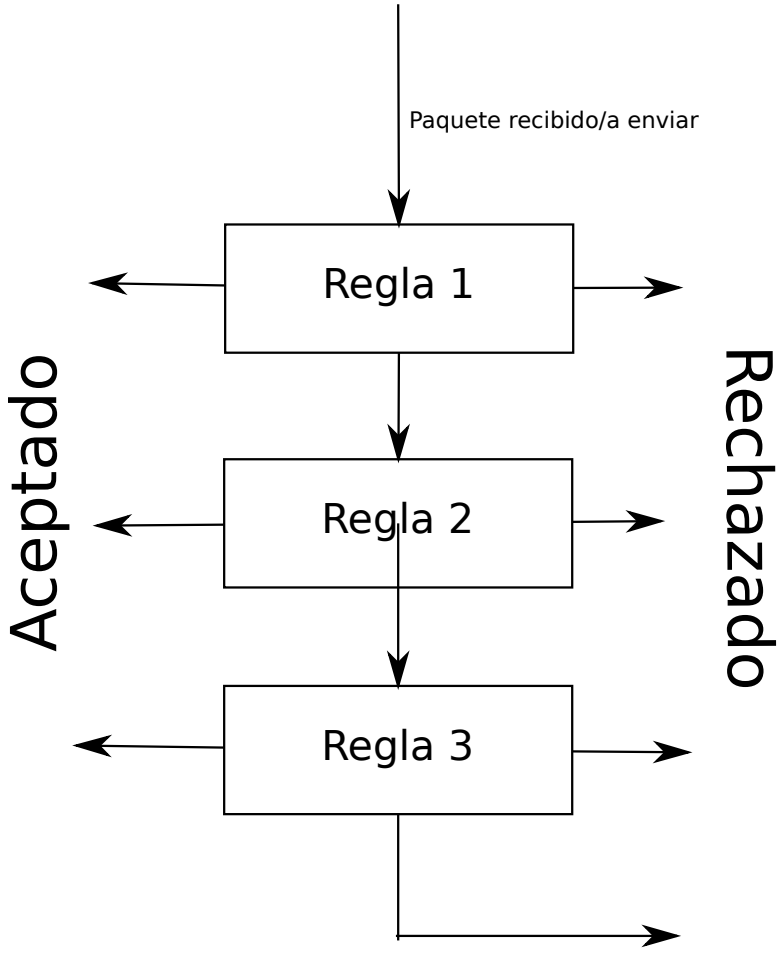
## 1.1. Numeración

- 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

- Una vez creada una ACL (más adelante) es necesario
  - Asignar y desasignar ACL a interfaces
  - Borrar y consultar ACL creadas

## 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`

Ejemplo: No dejes pasar el tráfico con origen en la red `192.168.1.0/8`

```
access-list 10 deny 192.168.1.0 0.0.0.255
```

### 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 regas 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. Operadores (para puertos TCP/UDP)

| Operador | Significa |
|---|---|
| eq | = igual |
| lt | < Menor |
| ne | No igual |
| gt | > Mayor |

### 5.2. 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]
```

Ejemplo: Prohíbe el tráfico hacia la red `172.16.0.0/12`

```
access-list 101 deny ip any 172.16.0.0 0.0.15.255
```

### 5.3. 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]
```

### 5.4. 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]
```

Ejemplo: Permite el protocolo **TCP** desde la red `172.16.3.0/24` con puerto de origen `21` hacia la red `172.16.1.0/24`

```
access-list 101 permit tcp 172.16.3.0 0.0.0.255 eq 21 172.16.1.0 0.0.0.255
```

Ejemplo: Permite la comunicación **TCP** hacia la red `10.0.0.0/8` si ya se ha establecido conexión (la red `10.0.0.0/8` es la que tiene el cliente)

```
access-list 102 permit tcp any 10.0.0.0 0.0.0.255 established
```

### 5.5. 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]
```

## 6. PROCESO DE DEFINICIÓN DE ACLs

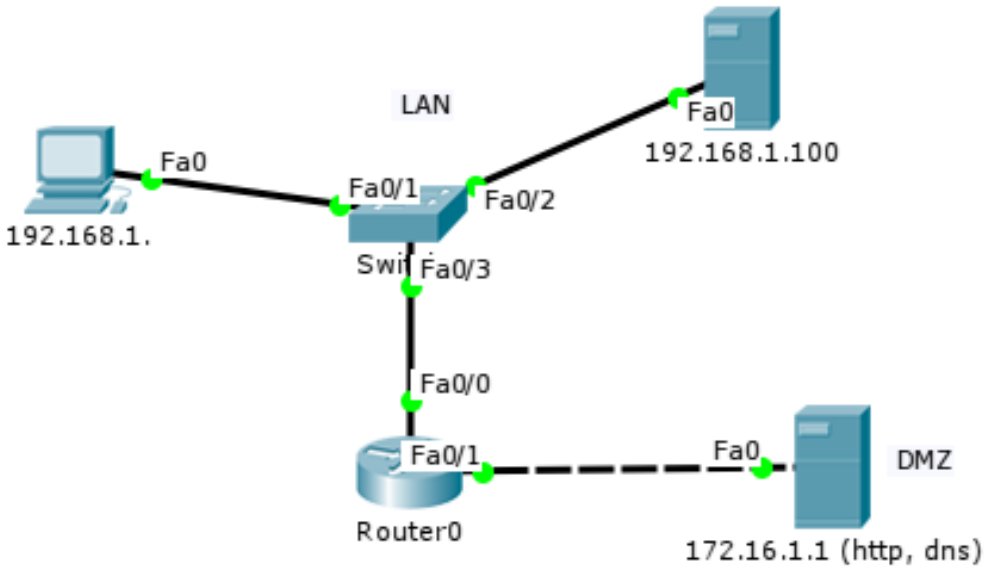
- Para definir las ACL de un router es necesario
  - Determinar las interfaces del router
  - Por cada interfaz:

- Determinar qué tráfico será permitido
- Determinar qué tráfico debe ser prohibido
- Ordenar las reglas para que no entren en conflicto (generalmente, de más concreta a más general)

- Es posible que se generen reglas redundantes
  - Pueden eliminarse, teniendo en cuenta que el tráfico prohibido es mejor eliminarlo cuanto antes de la red

## 6.1. 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.




(Fichero PKT)

## 6.2. Planteamiento

Interfaz Fa0/0 (LAN)

| | Entrada | | Salida |
|---|---|---|---|
| *X* | PING (ICMP) | *X* | PING (ICMP) |
| *V* | *DNS (UDP con destino 53)* | *V* | *DNS (UDP con origen 53)* |
| *V* | *TCP si se ha establecido desde la LAN* | *V* | *TCP si se ha establecido desde la LAN* |
| | | *X* | TCP si es una conexión entrante de la DMZ |
| *X* | Todo | *X* | Todo |

Interfaz Fa0/1 (DMZ)

| | Entrada | | Salida |
|---|---|---|---|
| *X* | PING (ICMP) | *X* | PING (ICMP) |
| *V* | *DNS (UDP con origen 53)* | *V* | *DNS (UDP con destino 53)* |
| *V* | *TCP si se ha establecido desde la LAN* | *V* | *TCP* |
| *X* | Todo | *X* | Todo |

- En el planteamiento anterior hay bastante redundancia, así que pueden agruparse muchas de esas reglas.
  - Basta con prohibir ICMP en una sola interfaz, en un solo sentido
  - Basta con controlar el tráfico TCP en una sola interfaz
  - Basta con controlar el tráfico DNS en una sola interfaz

### 6.3. Solución propuesta

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

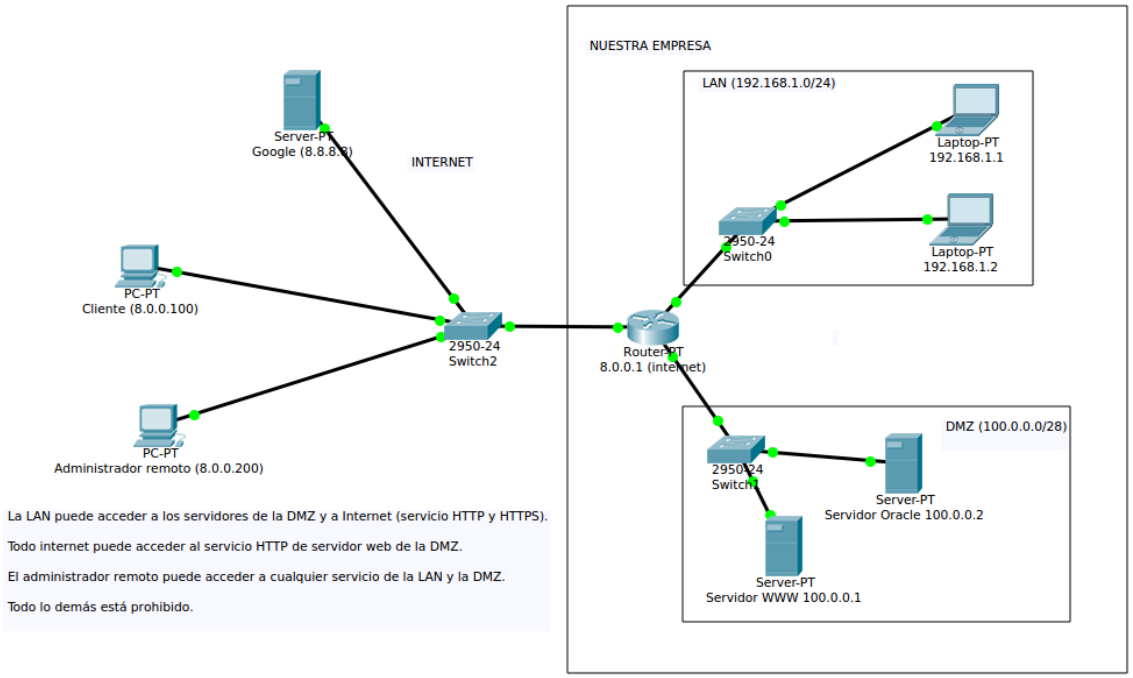
```
access-list 100 deny icmp any any
access-list 100 permit udp any any eq domain
access-list 100 permit tcp any any
access-list 100 deny ip any any
interface Fa0/0
ip access-group 100 in
```

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
```

## 7. Práctica

Fichero PKT inicial (adjunto al PDF)
Enlace al fichero PKT inicial




- La LAN puede acceder completamente a los servidores de la DMZ
- La LAN puede acceder a Internet al servicio HTTP, HTTPS y DNS.
- Todo internet puede acceder al servicio HTTP y HTTPS del servidor web de la DMZ.
- El administrador remoto puede acceder a cualquier servicio de la LAN y la DMZ.
- Todo lo demás está prohibido
  - En particular, conexiones entrantes de Internet a la LAN o a Oracle
- 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`

## 8. Referencias

- Formatos:
  - Transparencias
  - PDF
- Creado con:
  - Emacs
  - org-reveal
  - Latex