Contents

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 ???
  - Ampliadas: 100 a ???
- 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 ACL ESTANDAR

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

Solo hacen referencia a las direcciones IP de origen o destino. 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
  - host 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 ACL AMPLIADAS

Pueden hacer referencia a otras características del paquete: protocolo ICMP, TCP o UDP, puerto, conexión establecida...

4.1 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]
```

4.2 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]
```

4.3 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]
```

4.4 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 COMANDOS ÚTILES

5.1 Borrar una ACL

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

5.2 ACL existentes

```
show ip access-list
```

5.3 Interfaces asociadas a ACL

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

Es necesario mirar el apartado Inbound y Outbound

5.4 Asociar una ACL a una interfaz

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

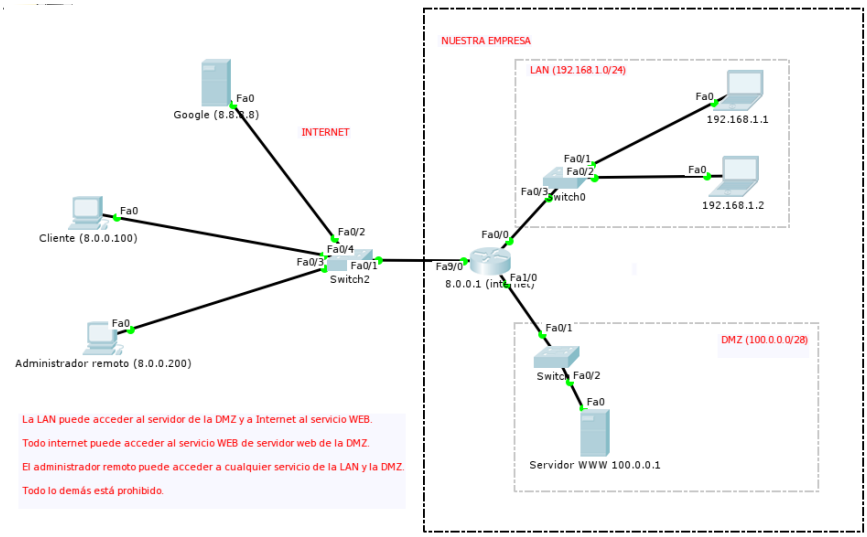
5.5 Desasociar una ACL a una interfaz

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

6 EJERCICIO PROPUESTO

6.1 Enunciado

```
ACL-inicial.pkt
```



- 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

6.2 Solución

Hay Muchas posibles soluciones. En esta se intenta que el Administrador tenga acceso IP completo (ICMP, TCP y UDP)

- Internet y la LAN pueden acceder al servidor web, se permite al administrador.

  Regla out en Fa1/0

  ```
  access-list 100 permit tcp any any eq www
  access-list 100 permit ip host 8.0.0.200 any
  access-list 100 deny ip any any
  interface fa1/0
  ip access-group 100 out
  ```

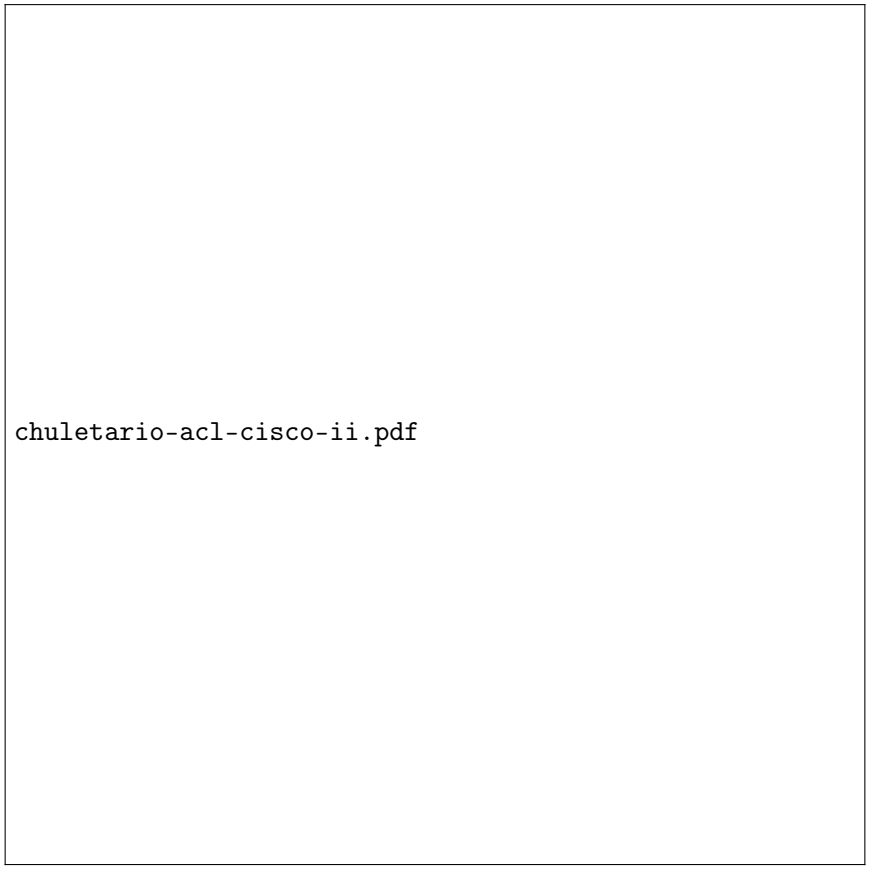
- La LAN solo puede acceder a los servicios WEB, se permite al administrador.

  Regla in en Fa0/0

  ```
  access-list 101 permit tcp any any eq www
  access-list 101 permit ip any 8.0.0.200 0.0.0.0
  access-list 101 deny ip any any
  interface fa0/0
  ip access-group 101 in
  ```

  Regla out en Fa0/0

  ```
  access-list 102 permit ip host 8.0.0.200 any
  access-list 102 permit tcp any any established
  access-list 102 deny ip any any
  interface fa0/0
  ip access-group 102 out
  ```


chuletario-acl-cisco-ii.pdf