Práctica 12 Redes de Computadores: Access Control List All (ACL)

Kevin Mateo Alvarado Suarez (kevin.alvarado@ucuenca.edu.ec),
Santiago Ariel Armijos Goercke (santiago.armijos@ucuenca.edu.ec),
Raúl Marcelo Ortiz Gaona (raul.ortiz@ucuenca.edu.ec)
Universidad de Cuenca
Redes de Computadores

Resumen

I. Introducción

II. Objetivos

1. Conocer el funcionamiento del servicio ACL.
2. Conocer la importancia del servicio ACL.
3. Conocer las ventajas del servicio ACL.
4. Simular el uso del servicio ACL.

III. Marco Teórico

III.1. Servicio ACL

Una lista de control de acceso a la red (ACL) consiste en reglas que determinan si se permite o se niega el acceso a un entorno informático. Puedes imaginar una ACL como la lista de invitados a un club exclusivo, donde solo aquellos que están en la lista tienen permiso para ingresar. Esta funcionalidad permite a los administradores garantizar que, a menos que el dispositivo presente las credenciales adecuadas, no podrá acceder al sistema. De esta manera, se establece un nivel de seguridad que controla cuidadosamente quién tiene acceso y quién no a través de las puertas de la red. [1]

III.2. Tipos de ACL

Las listas de control de acceso se pueden clasificar en dos categorías principales: [2]

- **ACL Estándar:**
  Una lista de control de acceso estándar se crea exclusivamente en función de la dirección IP de origen. Estas ACL permiten o bloquean todo el conjunto de protocolos sin distinguir entre tipos de tráfico IP como UDP, TCP o HTTPS. Se identifican mediante rangos numéricos 1-99 o 1300-1999, lo que facilita que el enrutador reconozca la dirección IP de origen.
- **ACL Extendida:**
  Una lista de control de acceso extendida se utiliza ampliamente debido a su capacidad para diferenciar el tráfico IP de manera exhaustiva. Considera tanto las direcciones IP de origen como de destino, junto con los números de puerto, para analizar y gestionar el tráfico IP de manera efectiva. Los usuarios pueden especificar qué tráfico IP se debe permitir o denegar. Las ACL extendidas se designan mediante los rangos numéricos 100-199 y 2000-2699.

III.3. Funcionamiento

Un ACL de sistema de archivos actúa como una tabla que informa al sistema operativo de una computadora sobre los privilegios de acceso que tiene un usuario a un objeto del sistema, ya sea un archivo individual o un directorio de archivos completo. Cada objeto tiene una propiedad de seguridad que lo vincula a su lista de control de acceso. La lista tiene una entrada para cada usuario con derechos de acceso al sistema.

Los privilegios típicos incluyen el derecho a leer un archivo único (o todos los archivos) en un directorio, ejecutar el archivo o escribir en el archivo o archivos. Los sistemas operativos que utilizan un ACL incluyen, por ejemplo, Microsoft Windows NT/2000, Netware de Novell, OpenVMS de Digital y sistemas basados en UNIX.

En el contexto de un modelo de seguridad basado en ACL, cuando un usuario solicita un objeto, el sistema operativo examina la ACL en busca de una entrada relevante y verifica si la operación solicitada es permisible.

Por otro lado, los ACL de red se instalan en enrutadores o conmutadores, donde actúan como filtros de tráfico. Cada ACL de red contiene reglas predefinidas que controlan qué paquetes o actualizaciones de enrutamiento se permiten o deniegan el acceso a una red.

Los enrutadores y conmutadores con ACL funcionan como filtros de paquetes que transfieren o niegan paquetes según criterios de filtrado. Como dispositivo de Capa 3, un enrutador de filtrado de paquetes utiliza reglas para determinar si se debe permitir o denegar el acceso al tráfico, teniendo en cuenta direcciones IP de origen y destino, puertos de destino y origen, y el procedimiento oficial del paquete. [1]

III.4. Ventajas de utilizar ACL

Existen varios beneficios al utilizar un ACL, que incluyen los siguientes: [3]

- Simplificación de la identificación de usuarios: Una lista de control de acceso simplifica la forma en que se identifican los usuarios. Los ACL aseguran que solo los usuarios y el tráfico autorizados tengan acceso a un sistema, facilitando así el proceso de identificación de usuarios.
- Mejora del rendimiento: Los ACL proporcionan ventajas de rendimiento en comparación con otras tecnologías que realizan funciones similares. Se configuran directamente en el hardware de reenvío de dispositivos de enrutamiento, minimizando cualquier impacto negativo en el rendimiento. Esto se diferencia de los firewalls de inspección de estado, que son componentes de software independientes que pueden provocar degradación del rendimiento. Además, al controlar el tráfico de la red, los ACL contribuyen a la eficiencia general de las redes.
- Mayor control: Los ACL otorgan a los administradores un control más preciso sobre los permisos de usuarios y tráfico en diferentes puntos de una red. Juegan un papel crucial en la gestión del acceso a los puntos finales de la red y en la regulación del flujo de tráfico entre las redes internas.

III.5. ¿Dónde implementar una ACL?

Las listas de control de acceso (ACL) pueden ser aplicadas a prácticamente cualquier dispositivo de seguridad o enrutamiento, y el uso de múltiples ACL en diferentes partes de la red puede ser beneficioso. Las ACL son especialmente adecuadas para puntos finales de red, como aplicaciones o servidores, que requieren alta velocidad y rendimiento, además de una seguridad sólida. Los administradores de red pueden optar por colocar una lista de control de acceso en diferentes puntos de la red según la arquitectura de la misma. Las ACL se suelen colocar con frecuencia en los enrutadores de borde de una red porque limitan con Internet público. Esto brinda a la ACL la oportunidad de filtrar el tráfico antes de que llegue al resto de la red. Los enrutadores de borde con ACL se pueden colocar en la zona desmilitarizada (DMZ) entre Internet público y el resto de la red. Una DMZ es una zona intermedia con un enrutador orientado hacia el exterior que proporciona seguridad general contra todas las redes externas. También cuenta con un enrutador interno que separa la DMZ de la red protegida. Las DMZ pueden contener diversos recursos de red, como servidores de aplicaciones, servidores web, servidores de nombres de dominio o redes privadas virtuales. La configuración de la ACL en el dispositivo de enrutamiento es diferente según los dispositivos que tiene detrás y las categorías de usuarios que necesitan acceso a esos dispositivos. [3]

IV. DESARROLLO

IV.1. Explicación de la Práctica

Para esta practica se pidió conectar dos routers, en el uno estarán las redes LAN privadas y en el otro los servidores WEB y FTP, la conexión entre routers debería tener una IP publica y seria necesario usar NAT.

Pero esto generaría problemas con las IPs de las ACL entonces se decidió documentar la practica realizada en clases. La cual consta de lo ya explicado antes con la única diferencia de que todo esta conectado a un mismo router.

IV.2. Disposición de los dispositivos

Se conectó cada router a cada uno de los switches mediante un cable de par trenzado directo. Luego, se procedió a conectar dos computadoras en 2 de los switches y dos servidores en el switch restante, totalizando 3 switches, 4 computadoras, 2 servidor y 1 laptop. Este paso se realizó con el propósito de configurar cada dispositivo a través de la consola, facilitando así la posterior prueba de comunicación en la red. A continuación se muestra la disposición de estos dispositivos.

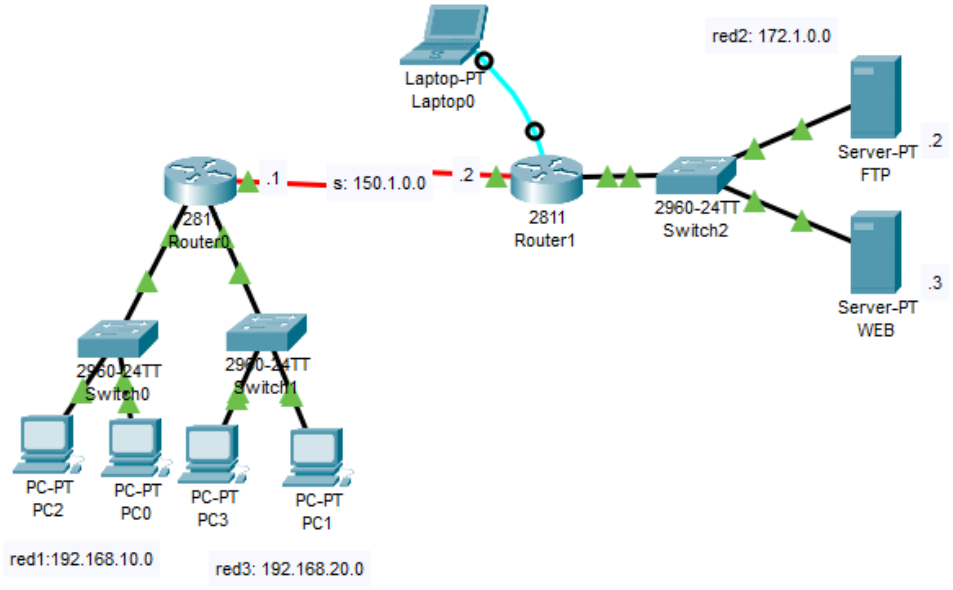

Figura 1: Disposición Dispositivos.

IV.3. Programación Router0 (Puertos FastEthernet)

```
Router(config)#interface fa 0/1
Router(config-if)#ip address 192.168.10.1 255.255.255.0
Router(config-if)#no sh
Router(config-if)#exit

Router(config)#interface fa 1/0
Router(config-if)#ip address 192.168.20.1 255.255.255.0
Router(config-if)#no sh
Router(config-if)#exit

Router(config)#interface fa 0/0
Router(config-if)#ip address 172.1.0.1 255.255.0.0
Router(config-if)#no sh
Router(config-if)#exit
```

IV.4. Programación Router1 (Puertos FastEthernet)

```
Router(config)#interface fa 0/0
Router(config-if)#ip address 172.1.0.1 255.255.0.0
Router(config-if)#no sh
Router(config-if)#exit
```

IV.5. Programación Router0 (Puertos Seriales)

```
Router(config)#interface s 0/0/0
Router(config-if)#ip address 150.1.0.1 255.255.0.0
Router(config-if)#no sh
Router(config-if)#exit
```

IV.6. Programación Router1 (Puertos Seriales)

```
Router(config)#interface s 0/0/0
Router(config-if)#ip address 150.1.0.2 255.255.0.0
Router(config-if)#no sh
Router(config-if)#exit
```

IV.7. Programación Router0 (RIP)

```
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#no auto summary
Router(config-router)#network 150.1.0.0
Router(config-router)#network 192.168.10.0
Router(config-router)#network 192.168.20.0
Router(config-router)#exit
```

IV.8. Programación Router1 (RIP)

```
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#no auto summary
Router(config-router)#network 150.1.0.0
Router(config-router)#network 172.1.0.0
Router(config-router)#exit
```

IV.9. Programación Router1 (ACL)

```
Router(config)#access-list 110 deny tcp 192.168.10.0 0.0.0.255
host 172.1.0.3 eq 80
Router(config)#access-list 110 permit tcp 192.168.20.0 0.0.0.255
host 172.1.0.3 eq 80

Router(config)#access-list 110 permit tcp 192.168.10.0 0.0.0.255
host 172.1.0.2 eq 21
Router(config)#access-list 110 permit tcp 192.168.20.0 0.0.0.255
host 172.1.0.2 eq 21

Router(config)#interface fa 0/0
Router(config-if)#ip access-group 110 out
Router(config-if)#exit
```

IV.10. Configuración de las direcciones IP, máscaras de red y Gateway a cada dispositivo

Por ultimo, toca configurar cada uno de los dispositivos (computadoras de escritorio y servidores) con una IP, mascara de red y Gateway correspondiente.

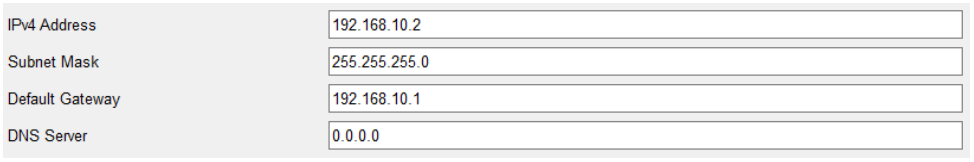

Figura 2: Configuración Dispositivo LAN A.

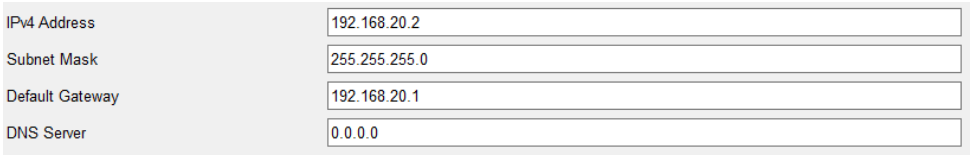

Figura 3: Configuración Dispositivo LAN B.

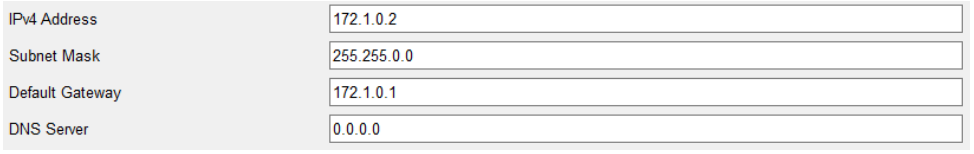

Figura 4: Configuración Dispositivo Servidor FTP.

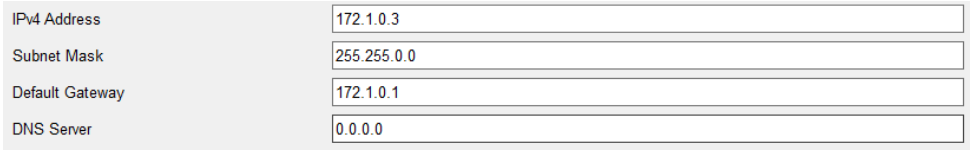

Figura 5: Configuración Dispositivo Servidor WEB.

IV.11. Diseño final de la red

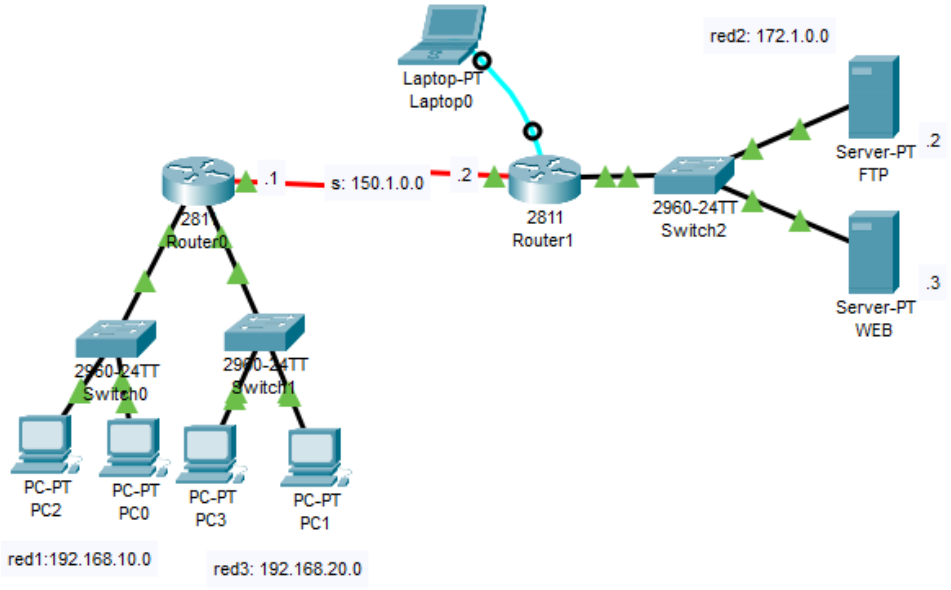

Figura 6: Diseño Final de la Red

IV.12. Pruebas de comunicación

A continuación, se muestran las pruebas de comunicación.

```
C:\>ftp 172.1.0.2
Trying to connect...172.1.0.2
Connected to 172.1.0.2
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>quit

221- Service closing control connection.
C:\>
```

Figura 7: Comunicación Servidor FTP y Red 1

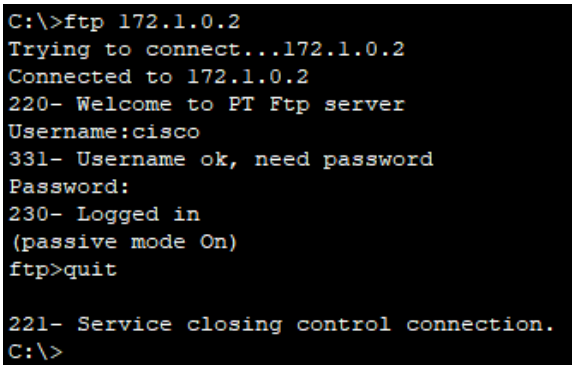

Figura 8: Comunicación Servidor FTP y Red 3

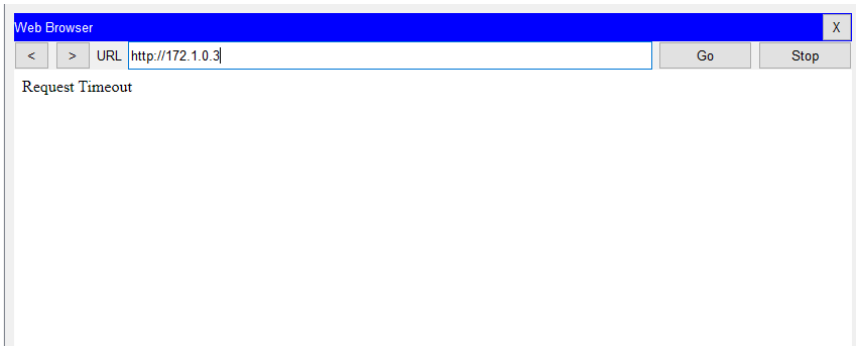

Figura 9: Comunicación Servidor WEB y Red 1

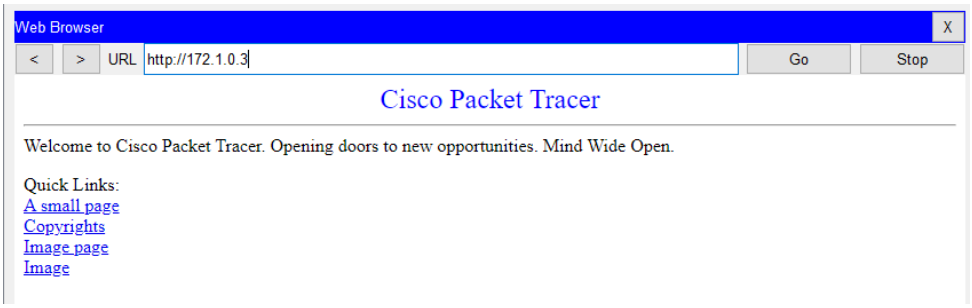

Figura 10: Comunicación Servidor WEB y Red 3

V. Conclusiones

Esta práctica sobre Listas de Control de Acceso (ACL) en Cisco Packet Tracer fue fundamental para comprender la importancia de estas herramientas en la seguridad de las redes de computadoras. A lo largo de la simulación, se evidenció la necesidad de configurar ACL de manera precisa utilizando la sintaxis específica de Cisco. La capacidad para filtrar el tráfico basado en criterios como direcciones IP, protocolos y puertos se destacó como una habilidad esencial. La práctica también subrayó la importancia de la verificación y solución de problemas, así como la consideración del impacto en el rendimiento de la red al implementar ACL. Además se debe aclarar que no se hizo uso de NAT debido a que resultaría imposible crear una ACL para bloquear cada red privada, ya que NAT encapsula a estas dos redes en una sola ip pública.

Referencias

[1] “What Is a Network Access Control List (ACL)?” [Online]. Available: https://www.fortinet.com/resources/cyberglossary/network-access-control-list

[2] “What is Access Control List | ACL Types & Linux vs Windows | Imperva.” [Online]. Available: https://www.imperva.com/learn/data-security/access-control-list-acl/
[3] “What is Access Control List (ACL)? - SearchSoftwareQuality.” [Online]. Available: https://www.techtarget.com/searchnetworking/definition/access-control-list-ACL