Instituto Politécnico Nacional

Escuela Superior de Cómputo

Administración de Servicios en Red

Práctica 8: Desafio ACLs

Alumnos:
Pimentel González Carlos
Hernández Castellanos César Uriel

Docente:
Henestrosa Carrasco Leticia

Grupo: 4CV3

Fecha: 20 de septiembre de 2019

Índice

1. Introducción

1.1. Lista de Control de Acceso

Una lista de control de acceso es un concepto de seguridad informática usado para fomentar la separación de privilegios. Es una forma de determinar los permisos de acceso apropiados a un determinado objeto.

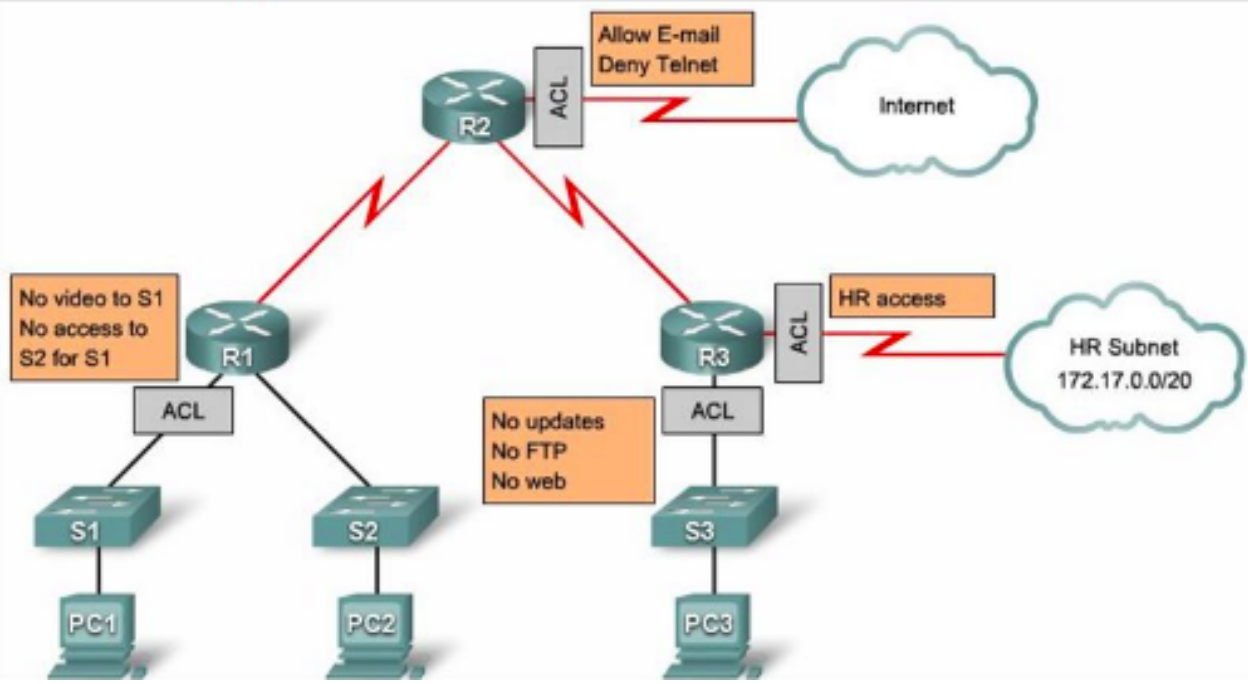

Figura 1: Aplicación de ACL en diferentes interfaces

1.2. Subneteo

El término subneteo hace referencia a la subdivisión de una red en varias subredes. El subneteo permite a los administradores de red, dividir una red más grande en varias subredes sin la necesidad de hacerlo público en internet

2. Objetivo

Reforzar los diferentes conocimientos adquiridos con anterioridad (ACL nombradas y subneteo), para esto se configurará de acuerdo a las politicas de red que se establece.

3. Objetivos específicos

1. Dividir 172.16.128.0/19 en dos subredes iguales.
2. Asignar la última dirección utilizable de la primera subred en la interfaz GE 0/1
3. Configurar HQ y Branch con enrutamiento RIPv2
4. Diseñar las listas de acceso para HQ y Branch de acuerdo a las politicas planteadas.

4. Tabla de direccionamiento

En la tabla siguiente es posible apreciar las rutas de los diferentes nodos en la red.

Device	Interface	IP Address	Subnet Mask	Default Gateway
HQ	G0/0	172.16.127.254	255.255.192.0	N/A
	G0/1	172.16.63.254	255.255.192.0	N/A
	S0/0/0	192.168.0.1	255.255.255.252	N/A
	S0/0/1	64.104.34.2	255.255.255.252	64.104.34.1
Branch	G0/0			N/A
	G0/1			N/A
	S0/0/0	192.168.0.2	255.255.255.252	N/A
HQ1	NIC	172.16.64.1	255.255.192.0	172.16.127.254
HQ2	NIC	172.16.0.2	255.255.192.0	172.16.63.254
HQServer.pka	NIC	172.16.0.1	255.255.192.0	172.16.63.254
B1	NIC			
B2	NIC	172.16.128.2	255.255.240.0	172.16.143.254
BranchServer.pka	NIC	172.16.128.1	255.255.240.0	172.16.143.254

Figura 2: Tabla de direccionamiento

5. Topología

Se trabajará en la siguiente topologia:

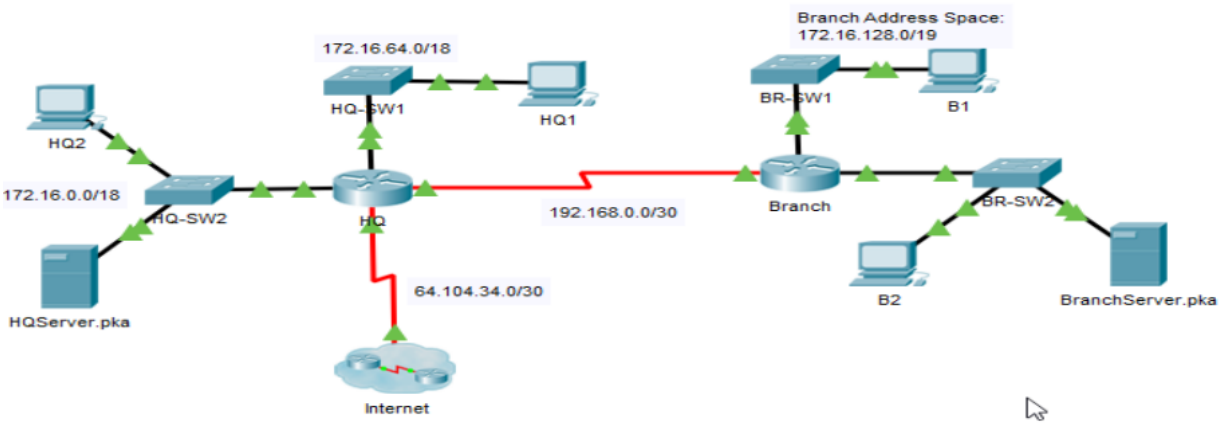

Figura 3: Topologia

6. Escenario

En esta actividad de desafío, finalizará el esquema de direccionamiento, configurará el enrutamiento e implementará listas de control nombradas.

7. Requerimientos

1. Divida 172.16.128.0/19 en dos subredes iguales para usar en Branch.
2. Asigne la última dirección utilizable de la segund asubred a la interfaz Gigabit Ethernet 0/0
3. Asigne la última dirección utilizable de la primera sub red a la interfaz Gigabit Ethernet 0/1
4. Documente el direccionamiento en la tabla de direccionamiento.
5. Configurar Branch con un apropiado direccionamiento.
6. Configurar B1 con el direccionamient apropiado utilizando la primera dirección disponible de la red la que se encuentre conectado
7. Configurar HQ y Branch con enrutamiento RIPv2 de acuerdo a lo siguiente:
   a) Anuncie las tres redes conectadas, no dando a conocer el enlace a internet.
   b) Configurar las interfaces adecuadas como pasivas.

c) Establezca una ruta determina en HQ que diriga el tráfico a la interfaz S/0/1.

d) Diseñe una ACL con nombre HQServer para evitar que cualquier computadora conectada a la interfaz Gigabit Ethernet 0/0 del enrytador Branch acceda a HQServer.pka, cualquier otro tráfico está permitido

e) Configure la lista de acceso en el enrutaor apropiado, aplique a la interfaz y dirección que corresponda.

8. Desarrollo

La práctica, lo primero que nos pedía, era dividir 172.16.128.0/19 en dos subredes iguales para usarlo en **Branch**. Para esto, pedimos un bit mas prestado por lo que las subredes quedaron asi:

ID de red	Rango usable		Mascara	Broadcast
172.16.128.0	172.16.128.1	172.16.143.254	255.255.240.0	172.16.143.255
172.16.144.0	172.16.144.1	172.16.159.254	255.255.240.0	172.16.159.255

Figura 4: Subneteo

El siguiente paso era asignar la ultima dirección usable de la segunda subred a la interfaz G0/0 y la ultima dirección usable de la primer subred a la interfaz G0/1. En la siguiente captura vemos esta configuración.

```
Branch(config-if)#int g0/0
Branch(config-if)#ip add 172.16.159.254 255.255.240.0
Branch(config-if)#int g0/1
Branch(config-if)#ip add 172.16.143.254 255.255.240.0
```

Figura 5: Configuración de interfaces

Luego había que configurar la computadora B1 con usando la primera dirección usable de la red a la que esta conectada. En la siguiente captura mostramos los datos ingresados, los cuales tomamos de nuestra tabla de subneteo previa.

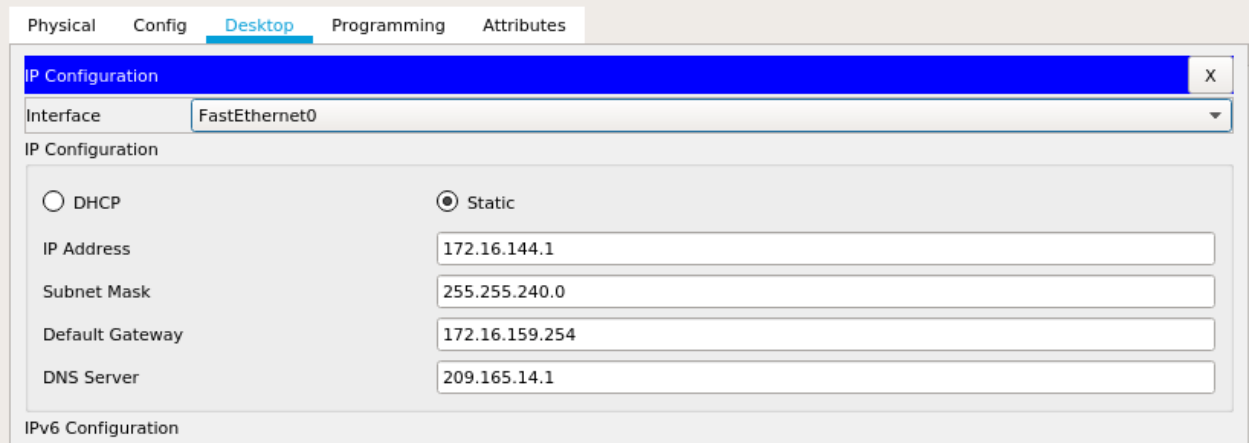

Figura 6: Configuración B1

El siguiente paso es configurar HQ y Branch con RIPv2 de acuerdo a los siguientes criterios:

- Configurar las interfaces apropiadas como pasivas
- No notificar el enlace a internet
- Redireccionar el trafico a S0/0/1 en HQ

Primero configuramos **Branch**, en la siguiente captura mostramos las configuraciones hechas.

```
Branch(config)#router rip
Branch(config-router)#version 2
Branch(config-router)#no auto-summ
Branch(config-router)#no auto-summary
Branch(config-router)#network 172.16.128.0
Branch(config-router)#network 172.16.144.0
Branch(config-router)#network 192.168.0.0
Branch(config-router)#passive
Branch(config-router)#passive-interface g0/0
Branch(config-router)#passive-interface g0/1
```

Figura 7: Configuración de rip en Branch

Y finalmente configuramos HQ.

```
HQ(config)#router rip
HQ(config-router)#version 2
HQ(config-router)#no auto
HQ(config-router)#no auto-summary
HQ(config-router)#network 172.16.0.0
HQ(config-router)#network 172.16.64.0
HQ(config-router)#network 192.168.0.0
HQ(config-router)#passi
HQ(config-router)#passive-interface g0/0
HQ(config-router)#passive-interface g0/1
HQ(config-router)#passive-interface s0/0/1
HQ(config-router)#defa
HQ(config-router)#default-information ori
HQ(config-router)#default-information originate
HQ(config-router)#exit
HQ(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1
```

Figura 8: Configuración de rip en HQ

El siguiente paso es crear una lista de acceso llamada **HQServer** para prevenir que cualquier computadora conectada a G0/0 de **Branch**, pueda acceder a **HQServer**. Todo el demás trafico es permitido. En la siguiente captura mostramos la configuración pertinente.

```
HQ(config)#ip access-list sta
HQ(config)#ip access-list standard HQServer
HQ(config-std-nacl)#deny 172.16.144.0 0.0.15.255
HQ(config-std-nacl)#permit any
HQ(config-std-nacl)#exit
HQ(config)#int g0/1
HQ(config-if)#ip ac
HQ(config-if)#ip access-group HQ
HQ(config-if)#ip access-group HQServer out
```

Figura 9: Configuración de la ACL HQServer

Por ultimo, nos pide que configuremos una lista de acceso de nombre **BranchServer** que evite que cualquier computadora en G0/0 del router **HQ**, acceda a **BranchServer**. Todo el demás trafico es permitido.

```
Branch(config)#ip access-list standard BranchServer
Branch(config-std-nacl)#deny 172.16.64.0 0.0.63.255
Branch(config-std-nacl)#permit any
Branch(config-std-nacl)#exit
Branch(config)#inter g0/1
Branch(config-if)#ip acces
Branch(config-if)#ip access-group BranchServer out
```

Figura 10: Configuración de la ACL BranchServer

9. Conclusión

Las ACL nos sirven como mecanismo para extender/reducir los privilegios de diferentes dispositivos y como mecanismo de tráfico entrante y saliente en dispositivos router. Pero en ambos casos el objetivo es la separación de privilegios y asi establecer los permisos idóneos para cada caso.

A diferencia de las ACL estándar, las ACL extendidas permiten obtener una mayor granulidad, siendo posible el filtrar el tráfico de la red ya sea por protocolo, puerto, host, etc.

En conclusión las ACL son de gran ayuda cuando no se cuenta con un gran presupuesto para nuestra red y con éste mecanismo es posible controlar nuestro tráfico de red.

Referencias

[1] Cisco Networking Academy Builds IT Skills Education For Future Careers", Netacad.com, 2019. [Online]. Available: https://www.netacad.com/es. [Accessed: 20 - Sep- 2019].