

**Configura y verifica listas de control de acceso extendidas**

## Topology

Diagrama

Descripción generada automáticamente

**Objetivos**

**Parte 1: Configura dispositivos y verifica conectividad**

* Realizar configuración básica en PCs, ruteadores y switches.
* Configure OSPF en los ruteadores R1, ISP y R3.

**Parte 2: Configure y verifique listas de acceso extendidas numeradas y con nombre**

* Configurar, aplicar y verificar una ACL extendida numerada
* Configurar, aplicar y verificar una ACL extendida con nombre.

**Parte 3: Modifique y verifique ACLs extendidas**

**Tabla de direccionamiento**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Device** | **Interface** | **IP Address** | **Subnet Mask** | **Default Gateway** |
| R1 | G0/1 | 192.168.10.1 | 255.255.255.0 | N/A |
|  | Lo0 | 192.168.20.1 | 255.255.255.0 | N/A |
|  | S0/1/0 (DCE) | 10.1.1.1 | 255.255.255.252 | N/A |
| ISP | S0/1/0 | 10.1.1.2 | 255.255.255.252 | N/A |
|  | S0/1/1 (DCE) | 10.2.2.2 | 255.255.255.252 | N/A |
|  | Lo0 | 209.165.200.225 | 255.255.255.224 | N/A |
|  | Lo1 | 209.165.201.1 | 255.255.255.224 | N/A |
| R3 | G0/1 | 192.168.30.1 | 255.255.255.0 | N/A |
|  | Lo0 | 192.168.40.1 | 255.255.255.0 | N/A |
|  | S0/1/1 | 10.2.2.1 | 255.255.255.252 | N/A |
| S1 | VLAN 1 | 192.168.10.11 | 255.255.255.0 | 192.168.10.1 |
| S3 | VLAN 1 | 192.168.30.11 | 255.255.255.0 | 192.168.30.1 |
| PC-A | NIC | 192.168.10.3 | 255.255.255.0 | 192.168.10.1 |
| PC-C | NIC | 192.168.30.3 | 255.255.255.0 | 192.168.30.1 |

**Antecedentes / Escenario**

Las listas de control de acceso extendidas (ACL) son extremadamente poderosas. Ofrecen un grado de control mucho mayor que las ACL estándar en cuanto a los tipos de tráfico que se pueden filtrar, así como también dónde se originó el tráfico y hacia dónde se dirige.

En esta práctica de laboratorio, configurará reglas de filtrado para dos oficinas representadas por R1 y R3. La administración ha establecido algunas políticas de acceso entre las LAN ubicadas en R1 y R3, que debe implementar. El ruteador ISP entre R1 y R3 no tiene ninguna ACL colocada. No se le permitiría ningún acceso administrativo a un ruteador ISP, ya que solo puede controlar y administrar su propio equipo.

**Parte 1: Configura dispositivos y verifica conectividad**

### 1. Configura direcciones IP en PC-A y PC-C.

### 2. Realice configuración básica en R1, ISP y R3

### 3. Habilite SSH en el ruteador R3

R3(config)# **ip domain-name cisco.com**

R3(config)# **username admin privilege 15 secret class**

R3(config)# **crypto key generate rsa**

**Press enter and then type the value of 1024**

R3(config)# **line vty 0 4**

R3(config-line)# **login local**

R3(config-line)# **transport input ssh**

### 4. Configure OSPF en los ruteadores R1, ISP y R3

### Asigne 1 como ID de proceso OSPF y anuncie todas las redes en R1, ISP y R3.

R1(config)# **router ospf 1**

R1(config-router)# **network 192.168.10.0 0.0.0.255 area 0**

R1(config-router)# **network 192.168.20.0 0.0.0.255 area 0**

R1(config-router)# **network 10.1.1.0 0.0.0.3 area 0**

### 4. Verifique la conectividad entre los dispositivos

### De la PC-A realice ping a la PC-C y a todas las direcciones Loopback.

**Parte 2: Configure ACLs extendidas numeradas**

### Las ACL extendidas pueden filtrar el tráfico de muchas maneras diferentes. Las ACL extendidas pueden filtrar con direcciones IP de origen, puertos de origen, direcciones IP de destino, puertos de destino, así como varios protocolos y servicios.

### Las políticas de seguridad son las siguientes:

### Permita que el tráfico web que se origina en la red 192.168.10.0/24 vaya a cualquier red.

### Permita una conexión SSH a la interfaz serial de R3 desde la PC-A.

### Permita que los usuarios de la red 192.168.10.0/24 accedan a la red 192.168.20.0/24.

### Al observar las políticas de seguridad enumeradas anteriormente, necesitará al menos dos ACL para cumplir con las políticas de seguridad. Una mejor práctica es colocar las ACL extendidas lo más cerca posible de la fuente. Seguiremos esta práctica para estas políticas.

### access-list 111 permit tcp 192.168.10.0 0.0.0.255 any eq 80

### access-list 111 permit tcp host 192.168.10.3 host 10.2.2.1 eq 22

### access-list 111 permit ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255

### int g0/1

### ip access-group 111 in

**Parte 3: Verifique las listas de control de acceso extendidas numeradas**

### Realice un acceso por web desde la PC-A hasta la PC-C.

### Realice una conexión ssh a la interfaz serial de R3 desde la PC-A.

### Packet tracer:

* Desde la **PC-A** inicie **Comand Prompt**.
* Establezca una conexión SSH a la interface serial del ruteador R3. Utilice el nombre de usuario **admin** y la contraseña **class**.

C:\> ssh -l admin 10.2.2.1

### Tera Term

* Desde la **PC-A** inicie **Tera term**.
* Establezca una conexión SSH a la interface serial del ruteador R3. Utilice el nombre de usuario **admin** y la contraseña **class**.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Calendario

Descripción generada automáticamente con confianza media

**NOTA:** La primera vez que establece una sesión de SSH con un dispositivo, se genera una **SECURITY WARNING** (ADVERTENCIA DE SEGURIDAD) para comunicarle que no se conectó a ese dispositivo anteriormente. Este mensaje es parte del proceso de autenticación. Lea la advertencia de seguridad y, luego, haga clic en **Continue** (Continuar).

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

### Realice un ping de la PC-A a la interfaz Loopbak 192.168.20.1

### Realice un ping de la PC-A a la interfaz serial del ruteador R3 (10.2.2.1)

**Parte 4: Configure ACLs extendidas con nombre**

### Configure la política en R3. Asigne un nombre a la ACL WEB-POLICY

### Permita que el tráfico web que se origine en la red 192.168.30.0/24 acceda a R1 (s0/1/0) y a la red 209.165.200.224 /27 en el ISP. NO se debe permitir que la red 192.168.30.0/24 acceda a ninguna otra red a través de la web.

R3(config)# **ip access-list extended WEB-POLICY**

R3(config-ext-nacl)# **permit tcp 192.168.30.0 0.0.0.255 host 10.1.1.1 eq 80**

R3(config-ext-nacl)# **permit tcp 192.168.30.0 0.0.0.255 209.165.200.224**

**0.0.0.31 eq 80**

### Aplicar la ACL WEB-POLICY a la interfaz S0/1/1 de R3

R3(config-ext-nacl)# **interface g0/1**

R3(config-if)# **ip access-group WEB-POLICY in**

**Parte 5: Verifique las listas de control de acceso extendidas con nombre**

### Realice un ping de la PC-C a la PC-A: 192.168.10.3.

### Realice un ping de la PC-C al ISP: 209.165.201.1.

### Realice un ping de la PC-C a R1: 10.1.1.1.

### Realice un ping de la PC-C al ISP: 209.165.200.225.

### NOTA: Los ping fallaron, ya que solo el tráfico web puede salir de la red 192.168.30.0 /24 hacia el host 10.1.1.1 y hacia la red 209.165.200.224 solamente.

**Parte 6: Modifique y verifique ACLs extendidas**

Debido a que las ACL aplicadas en **R1** y **R3**, no se permiten pings ni ningún otro tipo de tráfico entre las redes LAN en **R1** y **R3**. La administración ha decidido que se debe permitir todo el tráfico entre las redes **192.168.10.0/24** y **192.168.30.0/24**. Debe modificar ambas ACL en **R1** y **R3**.

### En R1 ejecuta el comando show access-lists

### Modifica la ACL en R1

R1(config)# **ip access-list extended 100**

R1(config-ext-nacl)# 4**0 permit ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255**

R1(config-ext-nacl)# **end**

### En R3 ejecuta el comando show access-lists

### Modifica la ACL en R1

R3(config)# **ip access-list extended WEB-POLICY**

R3(config-ext-nacl)# **30 permit ip 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255**

R3(config-ext-nacl)# **end**

### Verifique las ACLs

### De la PC-A haga un ping a la PC-C

### De la PC-C haga un ping a la PC-A