ADMINISTRACIÓN Y CONFIGURACIÓN DE REDES (EI 1019) - CURSO 2020-2021
BOLETÍN DE PROBLEMAS P8

INTRODUCCIÓN.

En este boletín vamos a configurar diferentes listas de acceso para limitar el tráfico en la configuración de red de la figura 1.

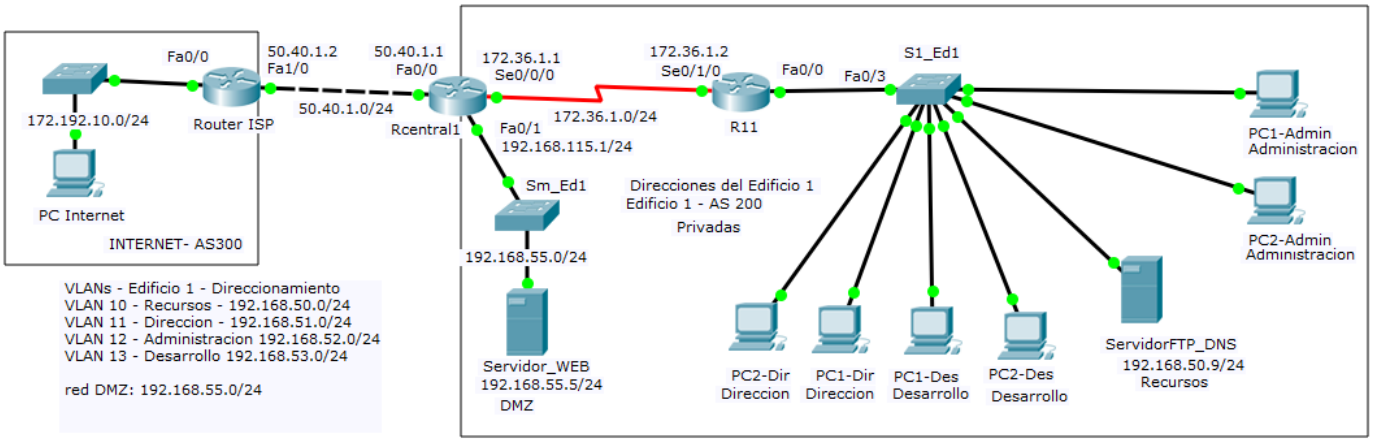

Figura 1. Configuración de la red.

EJERCICIO 1. Configuración de listas de control de acceso.

En la figura se han configurado 4 VLANs conectadas a las subinterfaces Fa0/0.10, Fa0/0.11, Fa0/0.12 y Fa0/0.13 del router R11.

VLANs - Edificio 1 - Direccionamiento
VLAN 10 - Recursos - 192.168.50.0/24
VLAN 11 - Direccion - 192.168.51.0/24
VLAN 12 - Administracion 192.168.52.0/24
VLAN 13 - Desarrollo 192.168.53.0/24

Nat web: 50.40.1.5
Nat ftp: 50.40.1.9

Queremos realizar las siguientes limitaciones de tráfico:

Todas las vlans pueden comunicarse con recursos.

Todas las vlans pueden ir al servidor web solo con tráfico http menos recursos que no puede acceder.

Recursos se comunica con todos.

Las vlans no pueden comunicarse entre sí (salvo con recursos que hemos dicho ya).

Dirección tenga acceso a internet solo para los protocolos: http (web), ftp (bajarse ficheros), dns (servicio de nombres en el puerto 53) y smtp (salida de correo electrónico).

Administración no debe tener acceso a internet.

Desarrollo debe tener acceso pleno a internet.

Se puede acceder al servidor ftp desde el exterior solo para servicio ftp y al servidor web solo para servicio http.

1) Piensa donde definir la lista y en que interfaces aplicarla.
   Por ejemplo, podemos hacer una lista para cada vlan y aplicarla en su subinterfaz. Para la última restricción necesito una lista aparte. ¿Dónde aplicarías esta lista?

SOLUCION

Direccion

interface Fa0/0.11
ip access-group 101 in
exit

cómo se debe permitir tráfico a cualquier destino (any) a los puertos www, ftp, 53 y smtp, pero no tráfico ip (de cualquier tipo) a las otras vlans, hay que negar primero el acceso a otras vlans y después permitir el tráfico concreto, porque sino se podría acceder a desarrollo o administración con tráfico web, ftp, dns o smtp.

Origen dirección:
//permito tráfico www al servidor web y después niego el tráfico de cualquier tipo (ip) hacia el servidor web
//permito tráfico a recursos
//deniego tráfico a las otras vlans
//permito tráfico especifico (www,ftp,53,smtp) hacia any
//se deniega el resto

access-list 101 permit tcp 192.168.51.0 0.0.0.255 host 192.168.55.5 eq www
access-list 101 deny ip 192.168.51.0 0.0.0.255 host 192.168.55.5
access-list 101 permit ip 192.168.51.0 0.0.0.255 192.168.50.0 0.0.0.255
access-list 101 deny ip 192.168.51.0 0.0.0.255 192.168.52.0 0.0.0.255
access-list 101 deny ip 192.168.51.0 0.0.0.255 192.168.53.0 0.0.0.255
access-list 101 permit tcp 192.168.51.0 0.0.0.255 any eq www
access-list 101 permit tcp 192.168.51.0 0.0.0.255 any eq ftp
access-list 101 permit udp 192.168.51.0 0.0.0.255 any eq 53
access-list 101 permit tcp 192.168.51.0 0.0.0.255 any eq smtp
access-list 101 deny ip any any

Administracion

interface Fa0/0.12
ip access-group 102 in
exit

Con origen administración

//permito www al servidor web,
//permito a recursos
//resto denegado

access-list 102 permit tcp 192.168.52.0 0.0.0.255 host 192.168.55.5 eq www
access-list 102 deny ip 192.168.52.0 0.0.0.255 host 192.168.55.5
access-list 102 permit ip 192.168.52.0 0.0.0.255 192.168.50.0 0.0.0.255
access-list 102 deny ip 192.168.52.0 0.0.0.255 192.168.51.0 0.0.0.255
access-list 102 deny ip 192.168.52.0 0.0.0.255 192.168.53.0 0.0.0.255
access-list 102 deny ip any any

las líneas en azul no son necesarias porque estaría incluido en la condición de la última línea de denegar todo.

Desarrollo

interface Fa0/0.13
ip access-group 103 in
exit

//como debe tener acceso pleno a internet deniego lo que no toque

access-list 103 permit tcp 192.168.53.0 0.0.0.255 host 192.168.55.5 eq www
access-list 103 deny ip 192.168.53.0 0.0.0.255 host 192.168.55.5
access-list 103 deny ip 192.168.53.0 0.0.0.255 192.168.51.0 0.0.0.255
access-list 103 deny ip 192.168.53.0 0.0.0.255 192.168.52.0 0.0.0.255
access-list 103 permit ip 192.168.53.0 0.0.0.255 192.168.50.0 0.0.0.255
access-list 103 permit ip any any

la línea en azul no es necesaria porque está incluida en la condición permitir todo.

Recursos

interface Fa0/0.10
ip access-group 100 in
exit

//recursos se comunica con todos menos con el servidor web
access-list 100 deny ip 192.168.50.0 0.0.0.255 host 192.168.55.5
access-list 100 permit ip any any

RESTO: acceso al servidor ftp desde el exterior → 2 soluciones posibles

Una: En Rcentral1 tráfico que entra en Fa0/0 in y usando la dirección externa del servidor ftp, origen any destino el servidor.

```
interface Fa0/0
ip access-group 104 in
exit
access-list 104 permit tcp any host 50.40.1.9 eq ftp
access-list 104 deny ip any host 50.40.1.9
access-list 104 permit tcp any host 50.40.1.5 eq www
access-list 104 deny ip any host 50.40.1.5
access-list 104 permit ip any any
```

OTRA SOLUCION es aplicar en Rcentral1 de salida de los interfaces Se0/0/0 y Fa0/1 y tendré que usar las direcciones privadas de los servidores. Origen any destino los servidores.

```
interface Se0/0/0
ip access-group 105 out
exit
interface Fa0/1
ip access-group 106 out
exit

access-list 105 permit tcp any host 192.168.50.9 eq ftp
access-list 105 deny ip any host 192.168.50.9
access-list 105 permit ip any any

access-list 106 permit tcp any host 192.168.55.5 eq www
access-list 106 deny ip any host 192.168.55.5
access-list 106 permit ip any any
```

O podría usar una única lista aplicada a los dos interfaces

```
interface Se0/0/0
ip access-group 107 out
exit
interface Fa0/1
ip access-group 107 out
exit
```

access-list 107 permit tcp any host 192.168.50.9 eq ftp
access-list 107deny ip any host 192.168.50.9
access-list 107 permit tcp any host 192.168.55.5 eq www
access-list 107 deny ip any host 192.168.55.5
access-list 106 permit ip any any