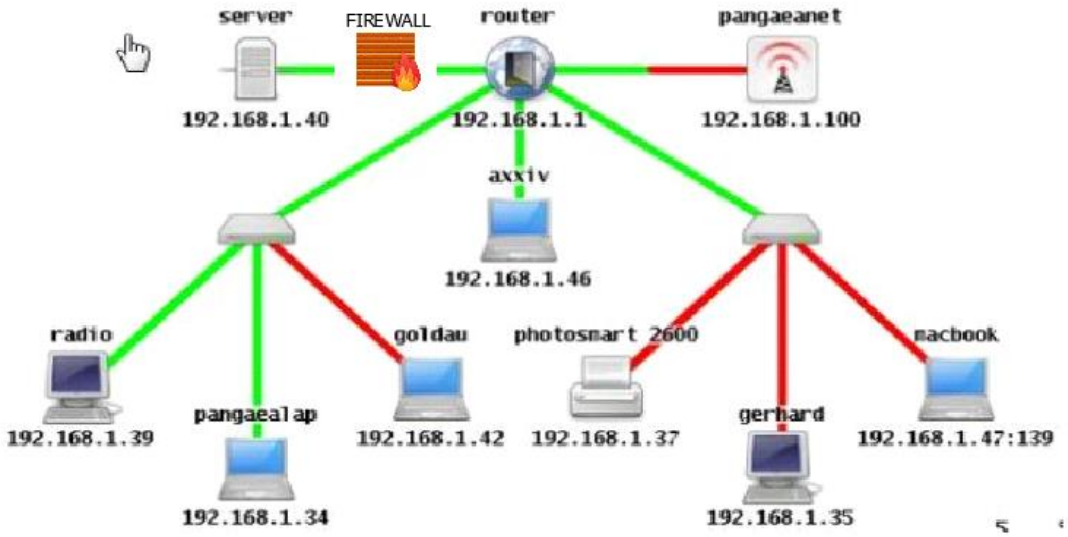
Alumno: Rodrigo Vila

Ejercicio número 1 - Unidad 4

A continuación, se expondrá un gráfico, donde el alumno/a será el que tome la decisión de dónde ubicar un Firewall. Sabiendo que los enlaces rojos, tienen prioridad de salida a Internet por la antena, y los verdes prioridad de acceso al servidor más importante de la topología.

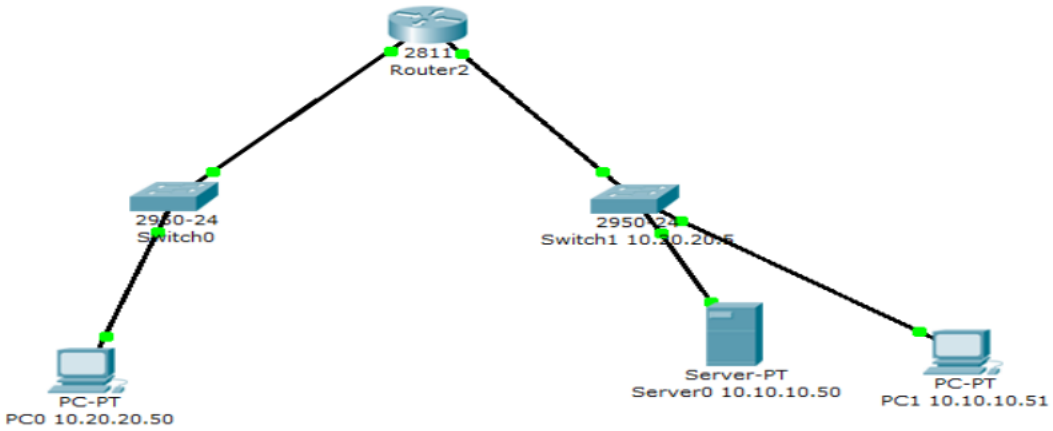


En este caso yo pondría el Firewall justo antes del SERVER, que es el dispositivo más importante a proteger. Teniendo en cuenta que todo el tráfico de la red tendría que pasar obligadamente a través del Firewall para contactar al Servidor.

Ejercicio número 2 - Unidad 4

EJERCICIO 1

Escribir un ACL que permita el tráfico de la PC0 a la PC1 y otro ACL que permita el tráfico de la PC0 al server.



ACL para permitir el tráfico de PC0 a PC1:

access-list 1 permit 10.20.20.50 0.0.0.255 10.10.10.51 0.0.0.0

Explicación:

Esta ACL permite todo el tráfico desde la PC0 (10.20.20.50) a la PC1 (10.10.10.51).

La máscara de red 0.0.0.255 se utiliza para especificar que solo se permite el tráfico desde la PC0.

La máscara de red 0.0.0.0 se utiliza para especificar que se permite todo el tráfico desde la PC1.

ACL para permitir el tráfico de PC0 al servidor:

access-list 2 permit 10.20.20.50 0.0.0.255 10.10.10.50 0.0.0.0

Explicación:

Esta ACL permite todo el tráfico desde la PC0 (10.20.20.50) al servidor (10.10.10.50).

La máscara de red 0.0.0.255 se utiliza para especificar que solo se permite el tráfico desde la PC0.

La máscara de red 0.0.0.0 se utiliza para especificar que se permite todo el tráfico desde el servidor.

Aplicación de las ACL:

La ACL 1 se debe aplicar a la interfaz del router que conecta con la PC0 (Ethernet0/0).

La ACL 2 se debe aplicar a la interfaz del router que conecta con el servidor (Ethernet0/1).

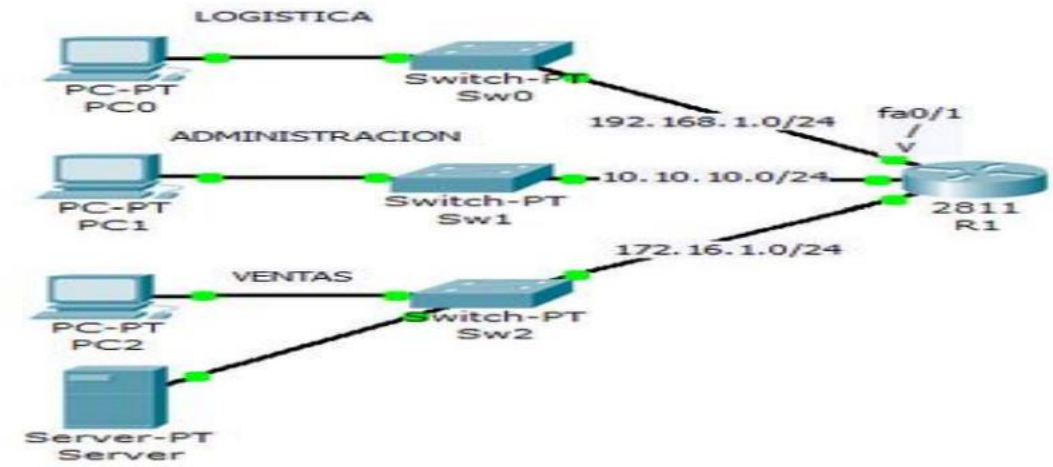
Bibliografía investigada:

Cisco: Configuración de ACL de IP de uso general:
https://www.cisco.com/c/es_mx/support/docs/ip/access-lists/26448-ACLsamples.html

Packet Tracer: Configuración de ACL extendidas, situación 1:
http://giret.ufps.edu.co/cisco/modulos/5.0/m2/course/files/9.3.2.10%20Configuring%20Extended%20ACLs%20Scenario%201%20Instructions.pdf

EJERCICIO 2

Consigna: Logística y Ventas pueden verse entre sí, pero no pueden ver a Administración, sin embargo Administración puede ver a todas.



ACL para la red:

Información de la red:

- Subredes:
  - Administración: 192.168.1.0/24
  - Logística: 10.10.10.0/24
  - Ventas: 172.16.1.0/24
- Routers:
  - R1: 192.168.1.1

- R2: 10.10.10.1
- R3: 172.16.1.1

- Switches:
- Switch-PT: 192.168.1.254
- Switch-Ventas: 172.16.1.254

ACLs:

R1 (Interfaz Ethernet 0/0):

access-list 1 permit 192.168.1.0 0.0.0.255 10.10.10.0 0.0.0.255

access-list 1 permit 192.168.1.0 0.0.0.255 172.16.1.0 0.0.0.255

access-list 1 deny 192.168.1.0 0.0.0.255 any

access-list 2 permit 10.10.10.0 0.0.0.255 192.168.1.0 0.0.0.255

access-list 2 permit 10.10.10.0 0.0.0.255 172.16.1.0 0.0.0.255

access-list 2 deny 10.10.10.0 0.0.0.255 any

access-list 3 permit 172.16.1.0 0.0.0.255 192.168.1.0 0.0.0.255

access-list 3 permit 172.16.1.0 0.0.0.255 10.10.10.0 0.0.0.255

access-list 3 deny 172.16.1.0 0.0.0.255 any

R2 (Interfaz Ethernet 0/1):

access-list 1 permit 10.10.10.0 0.0.0.255 192.168.1.0 0.0.0.255

access-list 1 deny 10.10.10.0 0.0.0.255 any

R3 (Interfaz Ethernet 0/2):

access-list 1 permit 172.16.1.0 0.0.0.255 192.168.1.0 0.0.0.255

access-list 1 deny 172.16.1.0 0.0.0.255 any

Explicación:

En R1:

- Permitir el tráfico desde la subred de Administración hacia las subredes de Logística y Ventas.
- Denegar cualquier otro tráfico desde la subred de Administración.
- Permitir el tráfico desde la subred de Logística hacia la subred de Administración y de Ventas.
- Denegar cualquier otro tráfico desde la subred de Logística.
- Permitir el tráfico desde la subred de Ventas hacia las subredes de Administración y Logística.
- Denegar cualquier otro tráfico desde la subred de Ventas.

En R2:

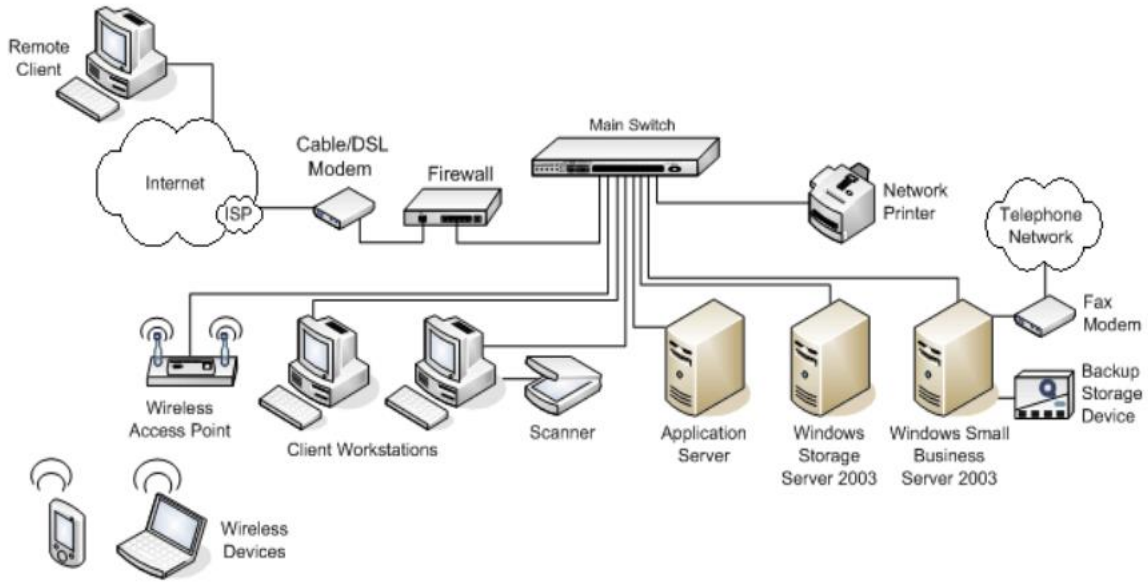
- Permitir el tráfico desde la subred de Logística hacia la subred de Administración.
- Denegar cualquier otro tráfico desde la subred de Logística.

En R3:

- Permitir el tráfico desde la subred de Ventas hacia la subred de Administración.
- Denegar cualquier otro tráfico desde la subred de Ventas.

Ejercicio Número 3 Unidad 4

De acuerdo a la metodología enseñada, poner en práctica los 6 puntos en este dibujo de red, Exponer en el foro.



1. Relevamiento:

La imagen muestra una red compuesta por los siguientes dispositivos:

Router: Dispositivo que conecta la red interna con Internet.

Switch: Dispositivo que conecta los diferentes dispositivos de la red interna.

PC0: Computadora personal.

PC1: Computadora personal.

Servidor: Dispositivo que proporciona servicios a la red interna.

Impresora: Dispositivo de impresión.

Punto de acceso inalámbrico: Dispositivo que permite la conexión inalámbrica a la red.

2. Dispositivos a proteger:

Servidores: Contienen información confidencial y crítica para la empresa.

Client Workstations: Contienen información personal y de trabajo de los usuarios.

Impresora: Puede ser utilizada para imprimir documentos confidenciales.

Backup Storage Device: Contiene backups de almacenamiento.

3. Posicionamiento de los dispositivos:

Los dispositivos se encuentran bien posicionados dentro de la topología. El router se encuentra en la frontera de la red, protegiendo la red interna de accesos no autorizados desde Internet. El switch se encuentra en el centro de la red, conectando los diferentes dispositivos.

4. Medidas de seguridad adicionales:

Utilizar un IPS: El IPS permite detectar patrones de comportamiento sospechosos en la red y bloquear ataques o intentos de intrusión conocidos.

Utilizar un IDS: Permite detectar intrusiones y realizar análisis forense de actividades maliciosas o no autorizadas en la red.

Utilizar una red privada virtual (VPN): La VPN permite a los usuarios conectarse a la red interna de forma segura desde cualquier lugar.

Utilizar una solución de antivirus y antimalware: El antivirus y antimalware protege los dispositivos de malware y virus.

5. Medidas de backup en caso de caída de la red:

Utilizar un sistema de alimentación ininterrumpida (UPS): El UPS protege los dispositivos de cortes de energía.

Utilizar un router de respaldo: El router de respaldo permite mantener la conexión a Internet en caso de fallo del router principal.

Utilizar un servidor de respaldo: El servidor de respaldo permite mantener la disponibilidad de los servicios en caso de fallo del servidor principal.

Rodrigo Vila.-