1. **Diseño de Modelo de Seguridad para una Red Empresarial**

Una empresa de seguros maneja información confidencial, como datos de clientes y documentos internos, está conformada por diferentes departamentos, incluyendo ventas, marketing, desarrollo y recursos humanos.

**Modelo de Seguridad:**

Identificar que tipo de Modelo de seguridad esta implementado en cada sector de la empresa: *Abierto, Restrictivo, Cerrado.*

**Ventas:**

La red de ventas es de acceso libre y se utiliza para comunicarse con clientes y socios externos.

Se implementará un firewall con reglas específicas para permitir el tráfico de comunicación con los clientes a través de los protocolos necesarios (por ejemplo, HTTP, HTTPS, correo electrónico).

**Marketing:**

La red de marketing necesita un nivel de seguridad más alto debido a la manipulación de campañas publicitarias y datos de clientes.

Se implementará un firewall más estricto que solo permita tráfico específico, como acceso a servidores de publicidad y bases de datos de clientes.

Además, se aplicarán políticas de filtrado de contenido para prevenir descargas no autorizadas.

**Desarrollo:**

La red de desarrollo contendrá servidores y sistemas críticos utilizados por el equipo de desarrollo.

Solo se permitirá el acceso a este segmento desde direcciones IP y sistemas autorizados.

Se utilizarán listas de control de acceso (ACL) y autenticación de múltiples factores para garantizar un alto nivel de seguridad.

**Recursos Humanos:**

La red de recursos humanos almacena información altamente confidencial sobre empleados y procesos de contratación.

Se implementará un firewall con reglas específicas para permitir el acceso solo a sistemas y bases de datos necesarios para el equipo de recursos humanos.

Se aplicarán políticas de seguridad de contraseñas y se utilizará encriptación para proteger la información.

1. **Actividad a resolver con Packet Tracer: Configurar ACL en el/los router/s para controlar el tráfico entre estos segmentos de red.**

En una empresa que emplea tres modelos de seguridad distintos para diferentes segmentos de su red, se enfrenta al desafío de restringir el acceso a ciertas aplicaciones, servicios y hosts basados en la clasificación de seguridad de cada área. El departamento de desarrollo requiere inicialmente un entorno abierto para acceder libremente a recursos y aplicaciones de la empresa. Por otro lado, el equipo ventas necesita un modelo de seguridad restrictivo para garantizar la protección de información confidencial. Finalmente, el área de marketing utiliza un modelo de seguridad cerrada para gestionar un sistema crítico que no debe estar expuesto al acceso externo.

La red de una empresa está dividida en:

Departamento **de Ventas** (192.168.1.1/30)

Departamento **de Marketing** (192.168.1.6/30)

Departamento **de Desarrollo** (30.0.0.1)

Antes de realizar los ejercicios, compruebe el tráfico de red entre los hosts de Ventas, Marketing y desarrollo.

Utilizar ACLs para la implementación de políticas de seguridad y control el flujo de tráfico en la red. Implementar diferentes conjuntos de reglas de ACL en los routers de la empresa para cada segmento de red, de acuerdo con los requisitos de seguridad de cada departamento. Esto permitirá establecer políticas de acceso personalizadas para cada área, cumpliendo con los modelos de seguridad abierta, restrictiva y cerrada requeridos. De esta manera, se asegura un entorno de red seguro y adecuado para cada departamento, manteniendo la integridad y confidencialidad de la información.

1. Permitir que solo el host Laptop0 salga de Ventas
2. Evitar (denegar) que el tráfico de todos los demás hosts de la red de ventas abandone la red 192.168.1.1/30

**ACL Estándar**

**Paso 1:** Crear Listas de Control de Acceso

Crea una ACL, uno para permitir o denegar el tráfico específico.

*Ingresar al modo enable:*

Router>enable

Router#

Router#config t

Router(config)#access-list 10 permit 10.0.0.10

Router(config)#access-list 10 deny 10.0.0.1 0.255.255.255

Router(config)#access-list 10 permit any

**Paso 2: Aplicar ACL en Interfaces**

Luego de haber creado la ACL para que funcione debemos asignarla a una interfaz del router e indicarle el sentido de entrada o salida (in/out)

**Aplicar las ACL en las interfaces correspondientes.**

Compruebe si ACL creada funciona, haga ping para corroborar el tráfico, y ejecute nuevamente show Access-lists

Router(config)#interface

Router(config)#interface GibabitEthernet 0/0

Router(config-if)#ip access-group 10 out

Router(config-if)#

Router(config-if)#exit

Router(config)#

Router(config)#exit

Router#

**Paso 3: Mostrar lista:**

Router#show access-lists

Comprobar si ACL creada funciona, haga ping para corroborar el tráfico, y ejecute nuevamente show access-lists



Podemos volver a aplicar show access-lists y ver la cantidad de coincidencias que tuvo cada una de las entradas:



**ACL Extendida**

Se solicita bloquear el acceso de PC1 a un sitio web del servidor, deberá bloquear el trafico utilizado por el protocolo http que utiliza el puerto 80. Deberá comprobar inicialmente que pueda acceder al servidor y que en el servidor estén configurados el puertos http.

1. Denegar que el host PC1 acceda a la página web del servidor.

Ver que en el servidor este configurado el servicio HTTP



Comprobar que tenemos acceso al servidor con un ping

Comprobar desde el navegador que ingresa a la página web del servidor

<http://30.0.0.10>



Router(config)# access-list 101 deny tcp host 20.0.0.20 host 30.0.0.10 eq 80

Router(config)# access-list 101 permit ip any any

Router(config)#exit

Router(config)#interface fa

Router(config-if)#interface GigabitEthernet 0/0

Router(config-if)#ip access-group 101 in

Corroborar la conexión entre PC1 PC0 al servidor

Corroborar el acceso desde el navegador de PC1 PC0 a <http://30.0.0.10>





**Preguntas:**

¿Qué tipos de ataques en la red utilizaríamos ACL?

¿Cómo deshabilitamos una ACL?

En el ejercicio de la configuración de la ACL estándar ¿Por qué es mejor colocar la ACL 10 en el Router0 en lugar del Router0?

En el ejercicio de la configuración de la ACL estándar ¿Qué tipo de tráfico se bloqueará desde la red de Ventas hacia el servidor?

En el ejercicio de la configuración de la ACL estándar ¿Qué tipo de tráfico se permitirá desde la red de Ventas hacia el servidor?

En el ejercicio de la configuración de la ACL estándar: Si un dispositivo en la red de Desarrollo intenta acceder a una red de Ventas, ¿será permitido o bloqueado?

En el ejercicio de la configuración de la ACL extendida ¿Qué sucederá si se intenta realizar una solicitud TCP (puerto 80) desde la PC1 hacia el servidor?

En el ejercicio de la configuración de la ACL extendida ¿Porque agregamos la segunda regla permit any any?

En el ejercicio de la configuración de la ACL extendida: ¿En que router se crea ACL 101? ¿Porque?

En el ejercicio de la configuración de la ACL extendida: Si un dispositivo en la red de Desarrollo intenta acceder a una red de Marketing ¿será permitido o bloqueado?

**Observación**

Recuerde que esta configuración es un ejemplo básico y en un entorno real, se deben considerar otras medidas de seguridad y ajustes específicos según los requisitos de la red empresarial.