TAREA 06

CONFIGURACIÓN DE DISPOSITIVOS Y SISTEMAS INFORMÁTICOS I

BASTIONADO DE REDES Y SISTEMAS

ALBA MOREJÓN GARCÍA

2024/2025

Ciberseguridad en Entornos de las Tecnologías de la Información

La red de la organización tiene muchos "atajos" que los administradores y los usuarios conocen. Esto les permite poder acceder a los servicios que desean, sin que para ello necesiten tener permisos, como por ejemplo el servicio de impresión.

La compañía dispone de varios servicios:

- **Servicio Web con una base de datos asociada. Este es el servicio que presta a sus clientes, con una web que permite realizar la gestión del stock de almacenes.**
- **Gestor de contenidos de la Web**
- **Un servidor de directorio Activo**
- **Un servicio de resolución de nombres (DNS)**
- **Un servicio de impresión.**
- **Un servicio de ficheros.**
- **Portal para los empleados (Intranet). Este servicio se nutre de fuentes de noticias de información externas.**

El objetivo es que la arquitectura sea más segura, permitiendo controlar los flujos de información entre los diferentes servicios, y analizando los flujos que son necesarios y cuáles no.

a) Implementa las VLANS que consideres necesarias y justifica el por qué.

Las VLANs (redes de área local virtuales) son una manera de segmentar una red física en varias redes lógicas. Sirve para mejorar la seguridad y la eficiencia de la red de la organización, controlando el tráfico de información al aislar por sectores todo el tráfico de datos.

- VLAN 10: destinada a los administradores de red y sistemas.

Al separar los dispositivos y usuarios administradores que necesitan acceso a los sistemas administrativos (servidor de directorio activo y servicio de resolución de nombres) en su propia VLAN, permitimos una gestión más segura de la infraestructura de red y sistemas, pudiendo aplicar políticas de seguridad más estrictas y monitorear el tráfico de manera efectiva, reduciendo el riesgo de accesos no autorizados a recursos críticos.

- VLAN 20: los servidores de servicios como DNS, servicio de impresión y servicio de archivos.

Estos servicios son utilizados internamente y no necesitan estar expuestos a la red externa. Aislamos los servicios críticos del resto del tráfico para mejora la seguridad y el rendimiento de la red, asegurando que solo el tráfico necesario acceda a estos servicios.

- VLAN 30: para los servicios que necesitan estar accesibles desde el exterior, servidor web y el gestor de contenidos (DMZ).

Reduce el riesgo de que un ataque a uno de ellos afecte al resto. Además, aislar los servicios accesibles desde Internet como el servicio web y el gestor de contenidos de la web, permite proteger la red interna mientras se controla el tráfico entrante y saliente, evitando posibles ataques.

- VLAN 40: para el portal de empleados y las fuentes de noticias externas (Intranet).

Esto permite que el tráfico de la intranet esté separado del resto de la red, mejorando la seguridad y el rendimiento. Facilitar el acceso al portal para los empleados (intranet) y a las fuentes de noticias, separándolas en su propia VLAN, ayuda a controlar el acceso y a aplicar políticas de seguridad específicas.

La segmentación de la red en VLANs permite un mejor control del tráfico y una mayor seguridad. Aislar diferentes tipos de tráfico permite aplicar políticas de seguridad específicas a cada segmento, limitar el acceso no autorizado y reducir la superficie de ataque. Separar el tráfico de administración, del tráfico de usuarios y servicios críticos, optimiza el tráfico, mejora la gestión y la seguridad de la red.

b) Define los servicios que serán implementados en la DMZ.

La DMZ (Zona Desmilitarizada) es una subred que actúa como una zona intermedia entre la red interna de la organización y las redes externas, como Internet. Los servicios que deben estar en la DMZ son aquellos que necesitan ser accesibles desde el exterior pero que no deben comprometer la seguridad de la red interna.

Servicios a implementar en la DMZ:

1. **Servidor web**, este servidor aloja la página web de la empresa y permite a los clientes gestionar el stock de los almacenes. Al estar accesible desde Internet es crucial que el servidor web esté en la DMZ para proteger la red interna de posibles ataques.
2. Servidor de base de datos asociada, almacena y gestiona los datos necesarios para el funcionamiento del servidor web. Aunque la base de datos puede estar en la red interna, es importante que las conexiones desde el servidor web a la base de datos estén controladas y monitoreadas.
3. Gestor de contenidos de la web, permite la administración y actualización del contenido del sitio web. Al estar en la DMZ se asegura que cualquier acceso para la gestión de contenidos no compromete a la red interna.
4. Servidor DNS (Sistema de Nombres de Dominio), resuelve los nombres de dominio a direcciones IP. Colocar el servidor de DNS en la DMZ permite que las solicitudes de resolución de nombres desde Internet no afecten directamente a la red interna.
5. **Servidor de correo**, gestiona el envío y recepción de correos electrónicos. Al estar en la DMZ se protege la red interna de posibles amenazas que puedan llegar a través del correo electrónico.
6. Servidor FTP (Protocolo de Transferencia de Archivos), permite la transferencia de archivos entre la empresa y usuarios externos. Colocar este servidor en la DMZ asegura que las transferencias de archivos no comprometan la seguridad de la red interna.

Colocar estos servicios en la DMZ permite que sean accesibles desde Internet mientras se mantiene la red interna protegida. Implementar estos servicios en la DMZ proporciona una capa adicional de seguridad al aislarlos de la red interna, esto significa que incluso si un atacante logra comprometer uno de estos servicios, no tendrá acceso directo a los datos y sistemas internos de la empresa. Además, los firewalls y otras medidas de seguridad pueden monitorear y controlar el tráfico de la DMz, reduciendo el riesgo de ataques exitosos.

c) Implementa alguno de los servicios que tiene el sistema en la nube. Y define qué medidas de seguridad implementarías.

Para mejorar la seguridad y la eficiencia de la red de la organización, vamos a implementar el servicio web con base de datos asociada en la nube. Esto permitirá a los clientes gestionar el stock de almacenes a través de una página web alojada en la nube.

El primer paso para la implementación será elegir un proveedor de servicios en la nube que actualmente las mejores opciones estarán Amazon Web Service, Azure o Google Cloud, estos proveedores son confiables porque ofrecen infraestructura segura y escalable.
Una vez elegido, configuraremos el servidor web en la nube para alojar la página web y permitir que los clientes accedan al sistema de gestión de stock desde cualquier lugar. Seguiremos los siguientes pasos:

- Crear una instancia de servidor, deberemos seleccionar que tipo de instancia queremos, seleccionar el sistema operativo y configurar la red
- Instalación del software necesario, instalamos el servidor web (por ejemplo: Apache) y cualquier otro software necesario para la aplicación web.
- Desplegaremos la aplicación web, subimos los archivos de la aplicación web al servidor y configuraremos el servidor web para que sirva la aplicación a los usuarios.

Por último, configuraremos una base de datos en la nube para almacenar la información del stock y asegurar que los datos estén disponibles y protegidos, la base de datos también se encontrará en la nube para aprovechar la escalabilidad y las medidas de seguridad avanzadas que ofrecen los proveedores. Seguiremos los siguientes pasos:

- Crearemos una instancia de base de datos, en el servicio de bases de datos gestionado del proveedor.
- Configuraremos la base de datos, utilizando los parámetros necesarios, como el tipo de base de datos, el tamaño de almacenamiento y las políticas de backup.

- Migraremos los datos existentes a la nueva base de datos en la nube, asegurando que todos los datos estén correctamente transferidos.

Entre las medidas de seguridad que implementaremos estarán:

- El cifrado de datos, utilizaremos el cifrado HTTPS para todos los datos que se transmitan entre los clientes y el servicio web. El cifrado protege los datos contra accesos no autorizados y asegura que la información sensible no pueda ser interceptada durante la transmisión.
- La autentificación de multifactor, esto requerirá que los usuarios proporcionen dos o más formas de verificación para acceder al panel de administración del servicio web. El MFA añade una capa adicional de seguridad, reduciendo el riesgo de accesos no autorizados incluso si las credenciales de un usuario están comprometidas.
- Control de acceso basado en roles, se definirán permisos específicos para diferentes roles de usuario en el sistema de gestión de stock. Esto asegura que los usuarios solo tengan acceso a las funciones necesarias para su trabajo, minimizando el riesgo de accesos o modificaciones indebidas.
- Monitorizar y realizar auditorías de forma continua para rastrear los accesos y la actividad en el servicio. Para detectar y responder rápidamente a acciones sospechosas o no autorizadas.
- Implementar una configuración segura y la gestión de las vulnerabilidades, hay que asegurarse de que la configuración del servicio web siga las mejores prácticas de seguridad y realizar evaluaciones periódicas de las vulnerabilidades para prevenir ataques y brechas de seguridad.

Trasladar el servicio web con base de datos asociada de local a la nube ofrece numerosas ventajas, la principal es la accesibilidad, ya que permite a los clientes acceder y gestionar desde cualquier lugar. Además, la escalabilidad en la nube permite ajustar los recursos según la demanda, la seguridad también mejora ya que los proveedores ofrecen medidas avanzadas como el cifrado de datos y la autenticación de doble factor. Implementar este servicio en la nube, en comparación con otros servicios como el de ficheros o el de impresión, tiene mejor impacto en la operación diaria y la interacción con los clientes, ya que facilita el acceso remoto, reduce el costo operativo y asegura tanto la alta disponibilidad como la recuperación ante desastres.

d) Explica en detalle el número de Firewalls que implementaría y qué flujos de información controlaría. Indica una regla basada en IP de origen - IP destino - puerto - protocolo que tendrías que implementar en cada uno de los firewalls que has colocado.

Para mejorar la seguridad de la red de la organización y controlar los flujos de información, se recomienda implementar del firewalls

- **Firewall externo,** se encontrará entre la red externa (Internet) y la zona DMZ. Se va a utilizar para controlar el tráfico entrante y saliente de la DMZ, protegiendo la red interna de conexiones no autorizadas desde Internet.
    - Regla 1, permitiremos el tráfico HTTP y HTTPs
        - Origen: Cualquier IP externa
        - Destino: Ip del servidor web en la DMZ
        - Puertos: 80 (HTTP) y 443 (HTTPS)
        - Protocolo: TCP
        - Acción: Permitir
    - Regla 2, permitiremos el tráfico DNS
        - Origen: Cualquier IP externa
        - Destino: Ip del servidor DNS en la DMZ
        - Puertos: 53
        - Protocolo: UDP
        - Acción: Permitir

Este firewall actúa como primera línea de defensa contra amenazas externas, filtrando el tráfico entrante y saliente de la DMZ. Esto protege la red interna de accesos no autorizados y ataques de seguridad.

- Firewall interno, se encuentra entre la DMZ y la red interna. Se va a utilizar para controlar el tráfico entre la DMZ y la red interna, asegurando que solo el tráfico necesario tenga acceso a los recursos internos.
    - Regla 1, permitiremos el tráfico HTTP y HTTPs
        - Origen: Ip del servidor web en la DMZ
        - Destino: Ip del servidor de base de datos de la red interna
        - Puertos: 80 (HTTP) y 443 (HTTPS)
        - Protocolo: TCP
        - Acción: Permitir
    - Regla 2, permitiremos el tráfico LDAP
        - Origen: Ip del servidor de directorio activo de la DMZ
        - Destino: Ip del servidor de datos de la red interna
        - Puertos: 389 (LDAP)
        - Protocolo: TCP
        - Acción: Permitir

Con el firewall interno aseguramos que esté permitido el tráfico necesario entre la DMZ y la red interna esté permitido. Esto ayudará a proteger los recursos internos y a controlar los flujos de información entre los diferentes servicios.

e) Indica dónde colocarías los siguiente dispositivos que implementan medidas de seguridad en la red: switch, firewall, router, proxy, IDS.

Para mejorar la seguridad de la red de la organización y controlar los flujos de información, es fundamental colocar correctamente los dispositivos de red.

- Switch

Se colocará un switch en cada VLAN para segmentar el tráfico de red. Esto mejora la seguridad y el rendimiento al aislar el tráfico de diferentes segmentos de la red.
Los switches conectan dispositivos dentro de cada VLAN, permitiendo la comunicación interna. También pueden implementar políticas de seguridad, como listas de control de acceso para filtrar el tráfico no deseado.

- Firewall
    - Firewall perimetral, se ubicará entre la red externa (Internet) y DMZ. Su función será controlar el tráfico entrante y saliente de la DMZ, protegiendo la red interna de accesos no autorizados y ataques cibernéticos. Los firewalls aplican reglas de seguridad para permitir o denegar el tráfico basado en IP de origen, IP de destino, puerto y protocolo.
    - Firewall interno, se localizará entre la DMZ y la red interna. Su función es controlar el tráfico entre la DMZ y la red interna, asegurando que solo el tráfico necesario tenga acceso a los recursos internos.
- Router

Entre diferentes VLANs y entre la red interna y la red externa. Su función será enrutar el tráfico entre diferentes segmentos de la red y hacia Internet. Los routers también pueden implementar políticas de seguridad para controlar el tráfico y prevenir accesos no autorizados.

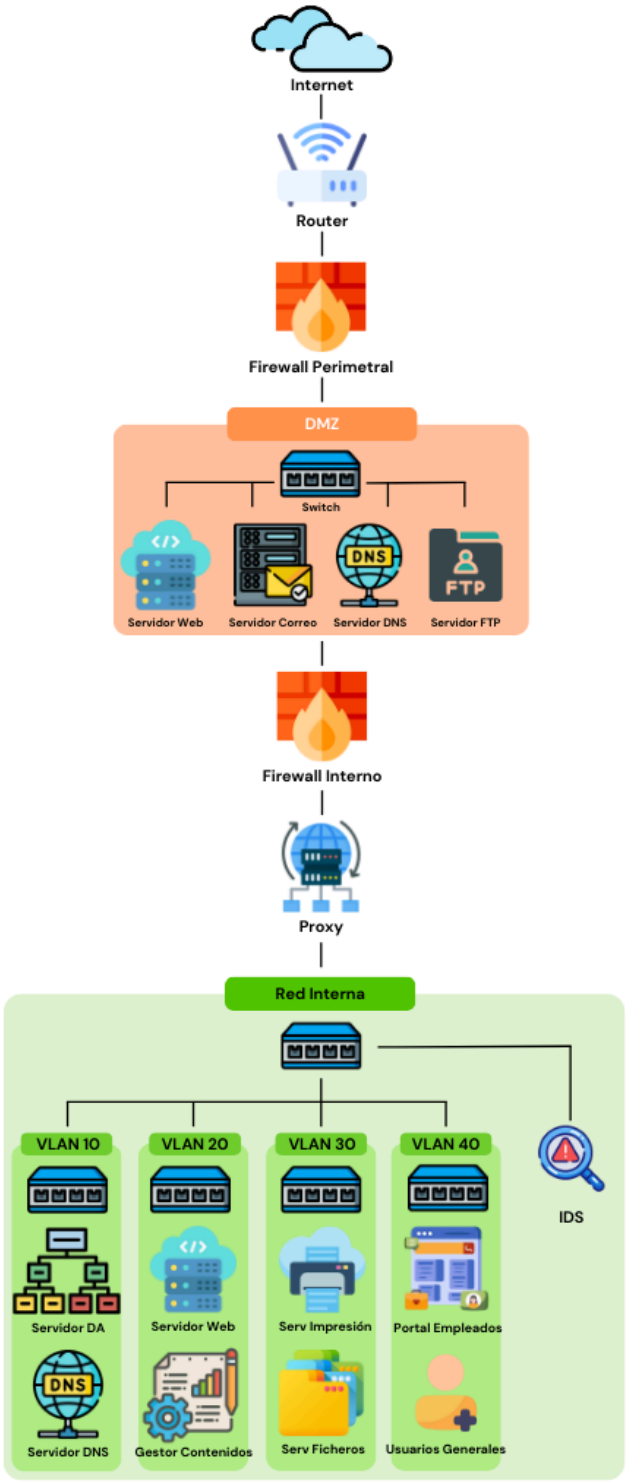
- Proxy

Se ubicará en la DMZ. Servirá para filtrar y controlar el acceso web, actuando como intermediario entre los usuarios y los recursos de Internet. Los proxies pueden bloquear sitios web maliciosos y registrar el tráfico para auditorías de seguridad.

- IDS

Lo situaremos en la red interna y su función será monitorear el tráfico de red en busca de actividades sospechosas o no autorizadas. Los IDs pueden alertar a los administradores de red sobre posibles ataques y ayudar a identificar y mitigar amenazas. Monitorean el tráfico de la DMZ y la red interna, detectando y alertando sobre aplicaciones peligrosas

Todo esto será reflejado en un diagrama de red en el que se pueda visualizar la información indicada en los puntos anteriores.



La empresa no quiere gastarse más del dinero necesario y los recursos humanos que dispone para el control de la ciberseguridad son dos personas: un técnico de ciberseguridad y un analista de ciberseguridad.