Curso de Especialización de Ciberseguridad en Entornos de Tecnología de la Información (CETI)

Bastionado de redes y sistemas

UD06. Configuración de dispositivos y sistemas informáticos I.
Tarea Online.

JUAN ANTONIO GARCIA MUELAS

INDICE

1.- Descripción de la tarea.

¿Qué te pedimos que hagas?

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.

- ✓ Implementa las VLANS que consideres necesarias y justifica el por qué.
- ✓ Define los servicios que estará implementados en la DMZ.
- ✓ Implementa alguno de los servicios que tiene el sistema en la nube. Y define qué medidas de seguridad implementarías.
- ✓ 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.
- ✓ Indica dónde colocarías los siguientes dispositivos que implementan medidas de seguridad en la red: switch, firewall, router, proxy, IDS.

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 dispones para el control de la ciberseguridad son dos personas: un técnico de ciberseguridad y un analista de ciberseguridad.

1. Implementa y justifica las VLANS que consideres necesarias.
   Vistos los servicios disponibles, implementaría las siguientes VLANs:
   - ✓ VLAN 10: Para la red interna (intranet) de la empresa, que incluye los servicios de portal para empleados y fuentes de noticias. Protegemos así esta parte de la estructura, que necesita de información desde fuentes externas.
   - ✓ VLAN 20: Gestor de contenidos de la Web. Queda así aislado de la red externa y comunicado con la interna mediante un túnel VPN.
   - ✓ VLAN 30: Servicio de resolución de nombres (DNS). Podría haberse incluido junto al servidor de directorio Activo, pero creo que los beneficios de la segmentación sobre estos dos elementos vitales priman sobre cualquier otro factor.
   - ✓ VLAN 40: Servicio de impresión.
   - ✓ VLAN 50: en esta ubicamos el servicio de ficheros. Pensé en unificarla con el servicio de impresión, pero al final he creído que, aislándola, eliminaba un posible vector de ataque que pudiera propagarse hacia ese otro servicio.

2. Define los servicios implementados en la DMZ.

El **servicio web**, expuesto a ataques externos, queda aislado de la red interna desde la DMZ. Lo mismo pasa con el **servidor proxy**, que podría filtrar tráfico malicioso y proteger los recursos de la DMZ.

El **servidor de correo**, puede ser un objetivo. Su ubicación en la DMZ permitiría que fuera accesible desde la red externa, pero estando aislado de la red interna.

3. Implementa alguno de los servicios del sistema en la nube. Y define qué medidas de seguridad implementarías.

El servicio de directorio Activo es un servicio crítico para la gestión de usuario, que podemos implementar en la nube, mediante un servicio de plataforma (PaSS), que se ofrecen desde grandes operadores como AWS o Microsoft Azure y que permitirá una reducción de los costes por hardware y mantenimiento.

Algunas de las medidas a implementar desde ahí, serían:

- ✓ Encriptado del disco para proteger sus datos.
- ✓ Firewall para restringir el tráfico.
- ✓ Autenticación con doble factor.
- ✓ Copia de seguridad para poder restaurar datos llegado el momento.
- ✓ Monitorización con la que detectar actividad maliciosa.

4. Detalle del 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.

Podemos controlar los flujos de información mediante la implementación de dos Firewalls:

- ✓ **Firewall perimetral.** Ubicado entre la red externa y la DMZ, para controlar y proteger el tráfico entre ambas.

  Por ejemplo:

  - ➢ Permitir el tráfico HTTP y HTTPS desde la red externa a la DMZ.

IP origen	IP destino	Puerto	Protocolo	Acción
Red Externa 0.0.0.0/0	DMZ 192.168.1.0/24	80,443	tcp	Permitir

  - ➢ Permitir el tráfico DNS desde la red externa a la DMZ.

IP origen	IP destino	Puerto	Protocolo	Acción
Red Externa 0.0.0.0/0	DMZ 192.168.1.0/24	53	udp	Permitir

  - ➢ Denegar todo el tráfico restante desde la red externa a la DMZ.

IP origen	IP destino	Puerto	Protocolo	Acción
Red Externa 0.0.0.0/0	DMZ 192.168.1.0/24	cualquiera	cualquiera	Denegar

- ✓ **Firewall interno**. Controla los flujos de información entre la DMZ y la red interna.
  Por ejemplo:
  - ➢ Permitir el tráfico HTTP y HTTPS desde la DMZ a la red interna.

IP origen	IP destino	Puerto	Protocolo	Acción
DMZ 192.168.1.0/24	Red interna 192.168.2.0/24	80,443	tcp	Permitir

  - ➢ Permitir el tráfico DNS desde la DMZ a la red interna.

IP origen	IP destino	Puerto	Protocolo	Acción
DMZ 192.168.1.0/24	Red interna 192.168.2.0/24	53	udp	Permitir

  - ➢ Permitir el tráfico entre los servicios de la red interna.

IP origen	IP destino	Puerto	Protocolo	Acción
Red interna 192.168.2.0/24	Red interna 192.168.2.0/24	cualquiera	cualquiera	Permitir

  - ➢ Denegar todo el tráfico restante desde la DMZ a la red interna.

IP origen	IP destino	Puerto	Protocolo	Acción
DMZ 192.168.1.0/24	Red interna 192.168.2.0/24	cualquiera	cualquiera	Denegar

Algún Firewall más (como para controlar los flujos entre VLANs), si bien puede añadir capas de seguridad, aumentaría costes y haría todavía más compleja la red. Teniendo en cuenta que la empresa no quiere gastar más dinero del necesario, descarto añadirlo.

5. Colocación de dispositivos que implementan medidas de seguridad en la red: switch, firewall, router, proxy, IDS.

Los dispositivos de seguridad comentados quedarían ubicados de la siguiente forma:

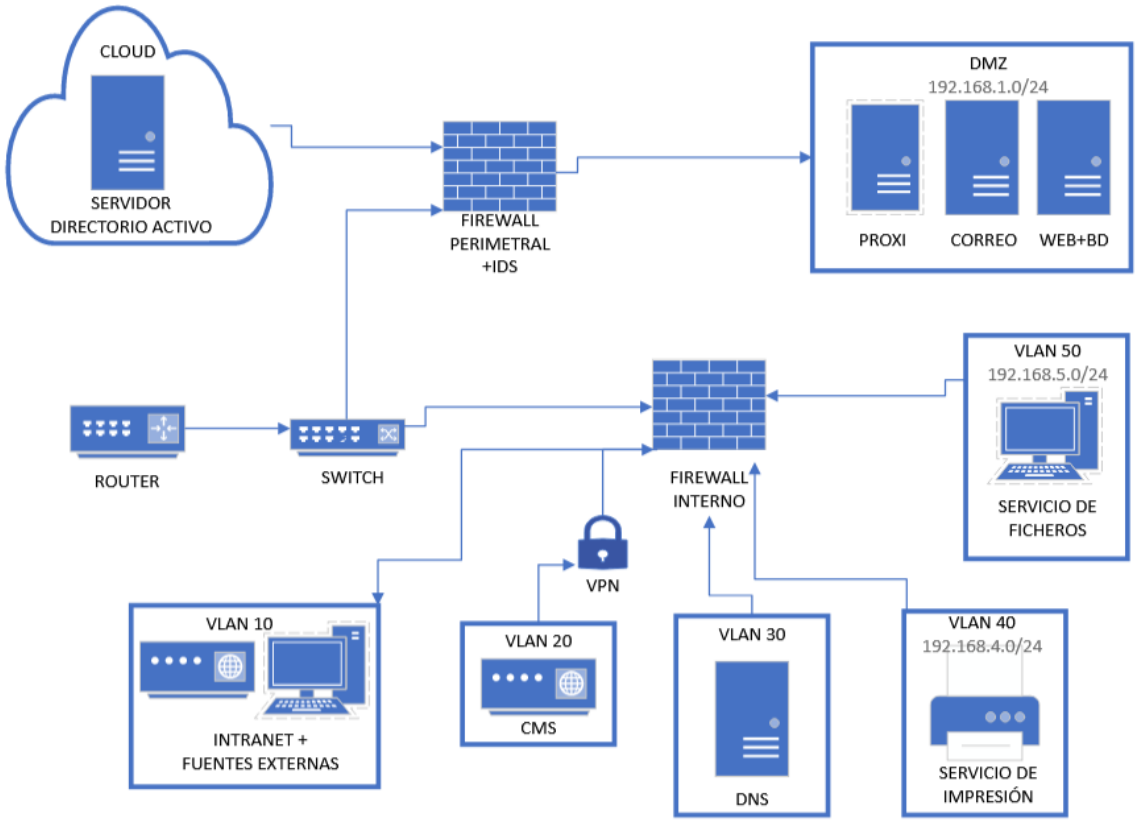
- ✓ Switch: Se colocaría en el centro de la red, para conectar todos los dispositivos.
- ✓ Firewall perimetral: Como se comentaba en el punto anterior, se ubicaría entre la red externa y la DMZ.
- ✓ Firewall interno: Se ubicaría entre la DMZ y la red interna.
- ✓ Router: Se ubicaría entre la red interna y la red externa.
- ✓ Proxy: Se ubica en la DMZ, como se señala en el punto dos.
- ✓ IDS: Ubicado en el firewall perimetral, para detectar ataques.

Diagrama de red para mostrar los puntos anteriores.

El esquema de la red queda definido de la siguiente manera:

Router
|
|Switch
| |Firewall perimetral
| |Servidor Directorio Activo
| |DMZ
| |Proxy
| |Servidor de correo
| |Servicio web + base de datos
| |Firewall interno
| |VLAN 10: Intranet + fuentes externas
VPN |VLAN 20: CMS
|VLAN 30: DNS
|VLAN 40: Servicio de impresión
|VLAN 50: Servicio de ficheros

Y el diagrama de red:



Webgrafía.

https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/521-ccn-stic-811-interconexion-en-el-ens/file.html.

https://www.incibe.es/protege-tu-empresa/blog/dmz-y-te-puede-ayudar-proteger-tu-empresa

https://www.ncsc.gov.uk/blog-post/drawing-good-architecture-diagrams

https://www.mecd.es/cidead/aulavirtual/course/view.php?id=2368#section-6