Universidad Rafael Landívar
Facultad de Ingeniería
Ingeniería en Informática y Sistemas
Curso: Redes I
Ing. Manuel Santizo / Ing. Fernando Girón

Tarea 06 – DMZ

Lester Andrés García Aquino
1003115

Guatemala, 28 de octubre de 2020

¿Qué es una DMZ?

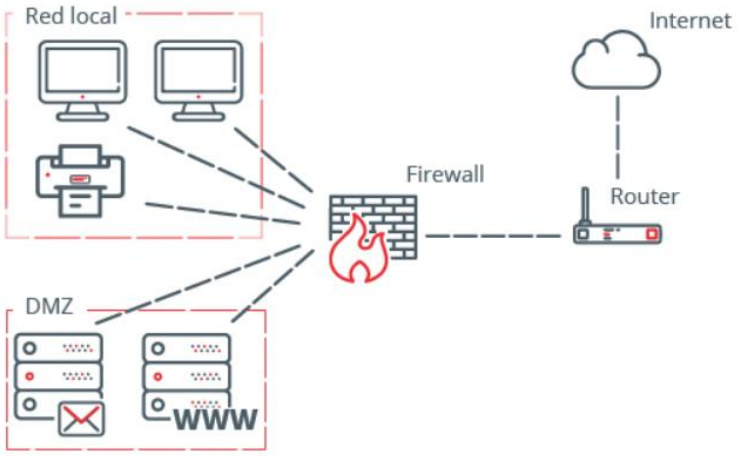
En seguridad informática, una red DMZ (a veces denominada “zona desmilitarizada”) funciona como una subred que contiene los servicios externos expuestos de una organización. Actúa como el punto expuesto a redes que no son de confianza, comúnmente Internet debido a la gran cantidad de usuarios que existen en esta, y como se sabe, entra mayor sea la cantidad de usuarios, mayor es la probabilidad de que existan robos o pérdidas de información.

El objetivo de una DMZ es agregar una capa adicional de seguridad a la red de área local (LAN) de una organización. Un nodo de red protegido y monitoreado que se enfrenta al exterior de la red interna puede acceder a lo que está expuesto en la DMZ, mientras que el resto de la red de la organización está a salvo detrás de un firewall, y como yo lo entiendo, es como un tipo cebo para los ataques, pensarán que no lograron su objetivo y desistirán posteriormente.

Cuando se implementa correctamente, una red DMZ brinda a las empresas o entidades protección adicional para detectar y mitigar las brechas de seguridad antes de que lleguen a la red interna, donde se almacenan datos e información valiosa.

El objetivo principal de las redes o implementaciones DMZ es para proteger a los hosts más vulnerables a los ataques. Estos hosts generalmente involucran servicios que se extienden a usuarios fuera de la red de área local, siendo los ejemplos más comunes el correo electrónico, los servidores web y los servidores DNS. Debido al mayor potencial de ataque, se colocan en la subred monitoreada para ayudar a proteger el resto de la red si se ve comprometida.

Los hosts en la DMZ tienen permisos de acceso estrictamente controlados a otros servicios dentro de la red interna, porque los datos que pasan a través de la DMZ no son tan seguros. Además de eso, las comunicaciones entre los hosts en la DMZ y la red externa también están restringidas para ayudar a aumentar la zona fronteriza protegida. Esto permite que los hosts de la red protegida interactúen con la red interna y externa, mientras que el firewall separa y administra todo el tráfico compartido entre la DMZ y la red interna. Por lo general, un firewall adicional será responsable de proteger la DMZ de la exposición a todo en la red externa.



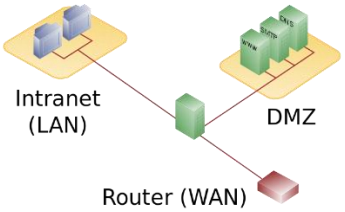
Cualquier servicio que se proporcione a los usuarios en la red externa se puede colocar en la DMZ. Los más comunes de estos servicios son:

- Servidores web
- Servidores de correo
- Servidores FTP
- Servidores VoIP

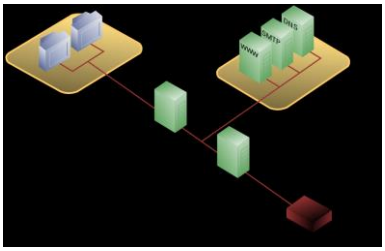
Por motivos de seguridad, cumplimiento de normas legales como HIPAA y motivos de supervisión, en un entorno empresarial, algunas empresas instalan un servidor proxy dentro de la DMZ. Esto tiene los siguientes beneficios:

- Obliga a los usuarios internos (generalmente empleados) a utilizar el servidor proxy para acceder a Internet.
- Requisitos de ancho de banda de acceso a Internet reducidos, ya que el servidor proxy puede almacenar en caché parte del contenido web.
- Simplifica el registro y el seguimiento de las actividades de los usuarios.
- Filtrado de contenido web centralizado.

1) Single firewall



2) Dual firewall



3) DMZhost