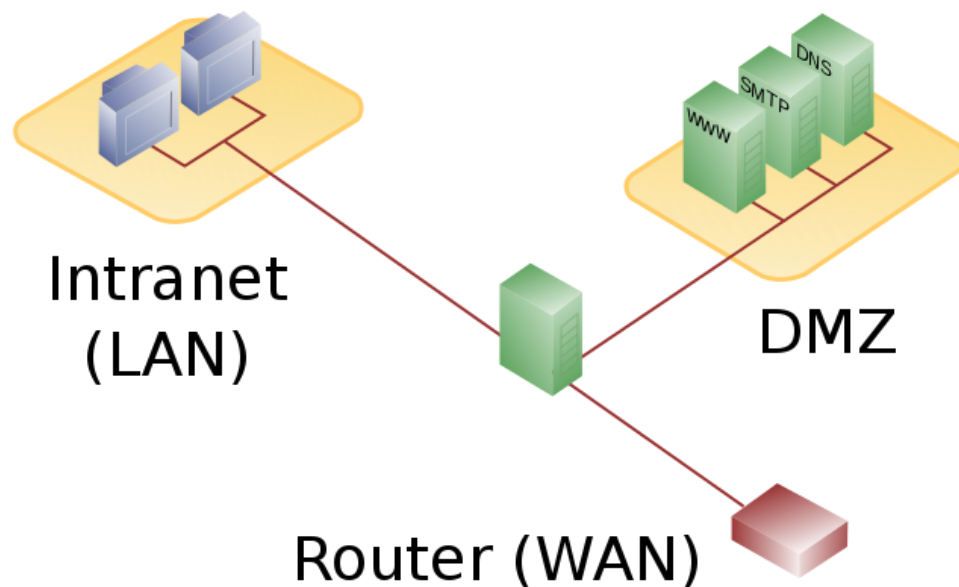


Práctica de Laboratorio 08. Configurando un Firewall con DMZ

En esta práctica vamos a configurar un Firewall con DMZ, de forma que tengamos conectadas a este dispositivo tres redes: Internet, la red Interna y una "Zona Desmilitarizada" (DMZ) en la que se instalarán hosts con los servicios habituales de internet de cara al exterior (por ejemplo, web, DNS o correo electrónico).

Ejercicios:

Vamos a partir del siguiente diseño de red con un sólo firewall, una red privada y una DMZ.



Diseñar el conjunto de reglas para IPtables de forma que se cumplan las siguiente Políticas de Seguridad.

1. Configuración de red con un sólo firewall, zona privada y DMZ con el siguiente direccionamiento:

- Internet: la red especificada por el servidor DHCP externo
- Red Interna: Clase C privada como subred de una clase B privada: 172.16.X.0/24 (X es la red asignada a cada alumno: 1,2,3,...)
- DMZ: Clase C privada 192.168.X.0/24 (X es la red asignada a cada alumno: 1,2,3,...)



2. Configurar un cliente en la red "Interna" y un servidor en la DMZ.

El cliente debe disponer de un navegador links o similar para las pruebas. El servidor debe disponer de un servicio HTTP (con [apache](#) o [nginx](#), a elegir). Aquí disponen de una [configuración de Apache para Debian](#) y una [configuración de nginx para Debian](#)

- Asignar al servidor Web la IP privada 192.168.X.100 y la IP pública (redirección de tráfico del puerto 80) que asigna el DHCP al Firewall.

3. Configurar el Firewall con políticas por defecto DROP y que permita:

- Tráfico DNS para la resolución de nombres al servidor DNS externo (tanto desde la red interna como de la DMZ)
- Tráfico Web desde la red interna a servidores web de Internet.
- Tráfico Web desde Internet al servidor web que tenemos en la DMZ. En este caso, redirigir el tráfico del puerto 80 de la IP pública de Internet del FW (en este caso de la ETSII) al servidor Web en la DMZ (comprobar con un navegador en el PC del CC).
- Tráfico Web desde la red Interna al servidor web de la DMZ (comprobar que se puede acceder tanto a la IP privada como a la pública)