Universidad de La Laguna

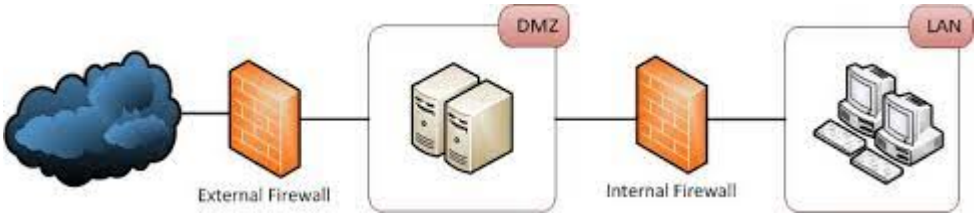
Práctica de Laboratorio 09. Shorewall: Doble firewall con DMZ

Vamos a realizar una configuración de nuestro Firewall con DMZ utilizando *Shorewall* y *firewalld*. Implementaremos un diseño con doble firewall (Interno con firewalld y Externo con shorewall) con dos interfaces para gestionar las zonas Internet, DMZ y Red Interna. La DMZ se localiza entre los dos firewalls configurados.

En el caso del firewall interno, utilizaremos otra implementación de firewalls basada en *nftables*. firewalld sobre una distribución Centos 8

Ejercicios:

Vamos a partir del siguiente diseño de red con dos firewalls, 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 dos firewalls y tres zonas:

La red tendrá tres zonas: *priv* para red interna, *fw* para el firewall y *dmz* para la DMZ con el siguiente direccionamiento:

- **Internet:** la red especificada por el servidor DHCP externo (IAAS de la ULL tiene 10.6.128.X)
- **Red Interna:** Clase C privada como subred de una clase B privada: 172.16.X.0/24
- **DMZ:** Case C privada 192.168.X.0/24

2. Habilitar NAT utilizando la configuración de *shorewall*

Hay que habilitar NAT utilizando la configuración del *shorewall* (fichero de configuración **snat**) del firewall externo (usando *shorewall*).

3. Configurar cliente en la red “Interna” y servidor en la DMZ

Configurar cliente en la red "Interna" y servidor en la DMZ. El servidor debe tener disponibles los servicios Web y FTP. Pueden utilizar proftpd server por ejemplo.

- Asignar al servidor la IP privada 192.168.X.100 y la IP pública (redirección de tráfico HTTP y FTP) que asigne el DHCP al Firewall.

4. Configurar el firewall con siguientes políticas por defecto:

- ACCEPT para tráfico FW a DMZ y FW a Red Interna.
- ACCEPT para tráfico Red Interna a DMZ.
- ACCEPT para tráfico Red Interna a Internet.
- REJECT para tráfico DMZ a Red Interna e Internet a DMZ.
- DROP para tráfico Internet a FW e Internet a Red Interna.

5. Configurar reglas utilizando Macros para permitir el siguiente tráfico:

- Tráfico DNS para la resolución de nombres al servidor DNS externo (tanto desde la red interna como de la DMZ
- Tráfico de cualquier tipo desde la red interna a servidores de Internet.
- Tráfico Web y FTP 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)

Escribir un breve informe comentando la configuración realizada, las pruebas realizadas y los archivos de configuración de Shorewall.