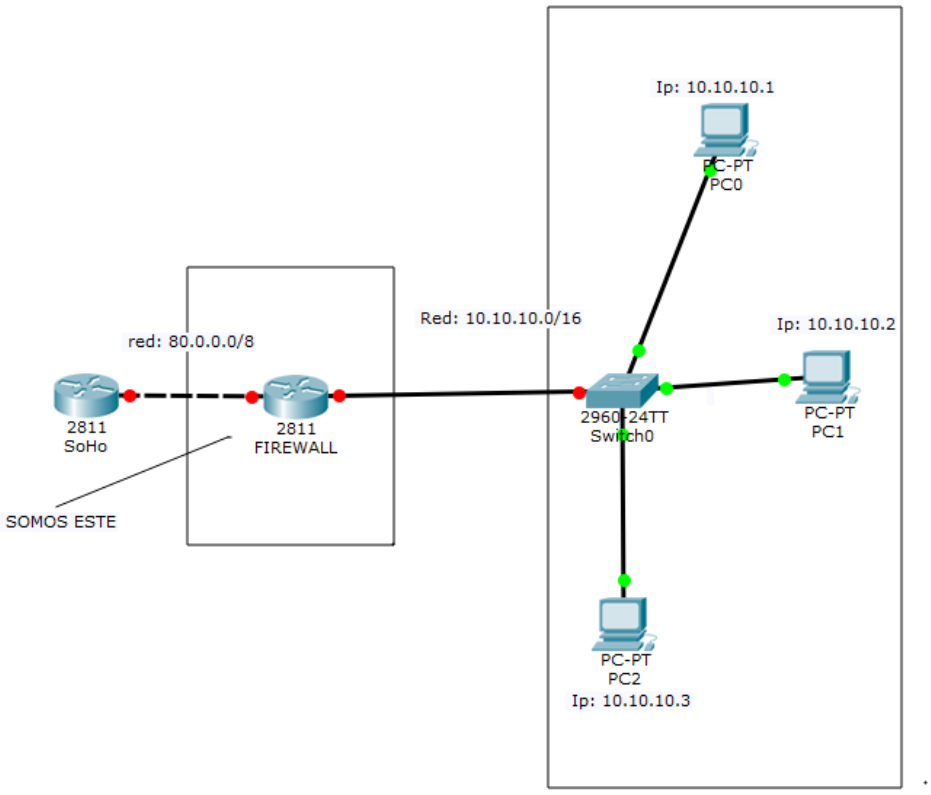
PRÁCTICA SEGURIDAD EN REDES

En un primer escenario, tenemos una máquina conectada a internet, y queremos protegerla con un cortafuego.

Reglas que debes de definir:

- Políticas por defecto para tablas filter y nat en ACCEPT.
- Localhost permite conexiones
- A nuestra IP le dejamos todo
- A un compañero de trabajo, le dejamos acceder a mysql (3306)
- A un proveedor le permitimos acceso ftp
- El puerto 80 debe de estar abierto
- El resto de puertos los cerramos, incluso los abiertos, para el resto de usuarios.

En un segundo escenario, tenemos una red local que se conecta a internet a través de un router SoHo, y queremos configurar un cortafuego que ponemos en el medio.

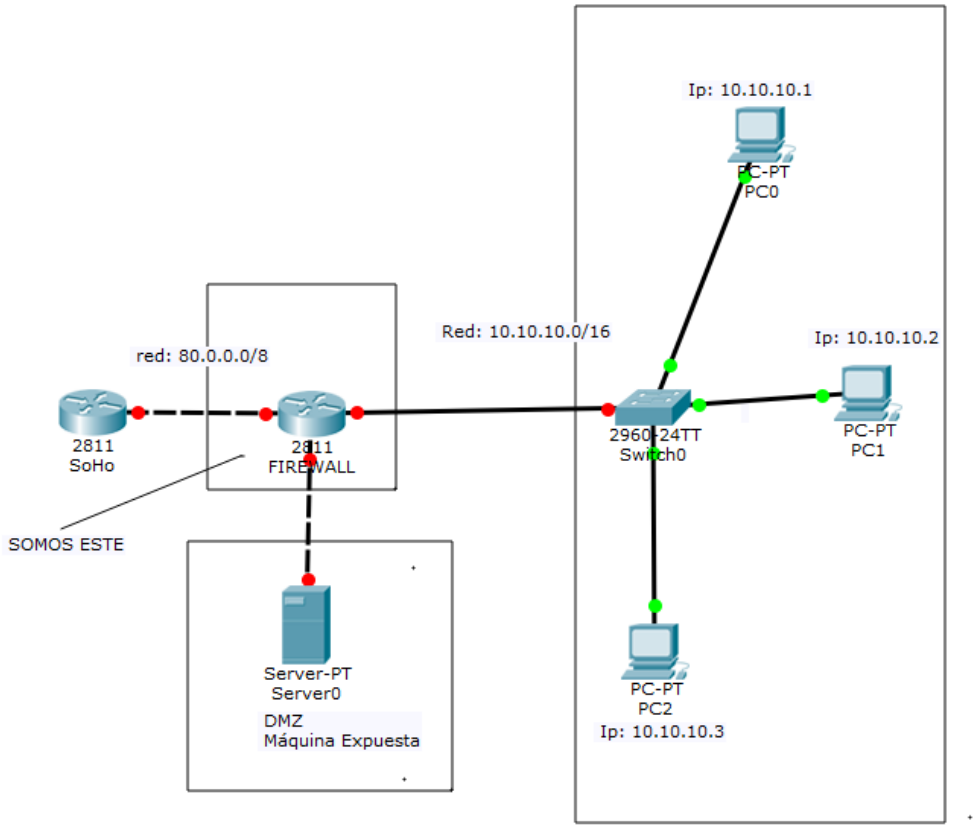


Reglas que debes de definir:

- Elminia cualquier regla que pueda existir

- Políticas por defecto para tablas filter y nat en ACCEPT.
- Enp0s3 es una NIC conectada al Soho y enp0s8 es una NIC conectada a la LAN.
- Al cortafuego se tiene acceso desde la red local
- Activa el bit de FORWARDING
- Al cortafuego NO se tiene acceso desde la red pública
- Se cierra el puerto de gestión webmin (10000)
- Por otro lado, queremos que los trabajadores sólo puedan navegar por internet, pero no accedan, ni a Kazza o Edonkey
- Se abre el acceso a puertos del correo
- El resto se deniega

En un tercer escenario, se agrega al escenario anterior, una DMZ, cómo sigue:



En este tipo de escenarios el cortafuego debe de permitir:

- Acceso de la red local a internet
- Acceso público a los puertos 80 y 443
- Acceso del servidor DMZ desde una máquina concreta de la LAN con fines administrativos, eso sí, comunicación cifrada y segura.

Reglas que debes de definir:

- Elimina cualquier regla que pueda existir
- Políticas por defecto para tablas filter y nat en ACCEPT.
- Enp0s3 es una NIC conectada al Soho y enp0s8 es una NIC conectada a la LAN y enp0s9 a la DMZ
- Todo lo que venga del exterior y vaya al puerto 80 y al puerto 443, lo redirigimos al bastión de la dmz
- Al cortafuego se tiene acceso desde la red local
- Tanto firewall como red local, tienen acceso al exterior.
- Se permite, con fines administrativos, el acceso desde el exterior a una máquina de la LAN.
- De la misma forma, se permiten, con fines administrativos el acceso desde la misma máquina de la LAN a la DMZ
- (Las dos últimas acciones se deben de permitir exclusivamente con conexiones seguras y con la máxima seguridad)
- El resto de la LAN se cierra a la DMZ
- El resto de la DMZ se cierra al cortafuego
- Se cierran el resto de puertos por debajo del 1024 para acceso del exterior