PROYECTO FINAL.

Valor: 25%
Fecha de entrega: junio 2025

El proyecto se realizará en equipos de máximo 4 personas.

DESCRIPCIÓN

Proxy. Es un dispositivo o prograa que hace de intermediario en las peticiones de recursos que realiza un cliente a otro servidor.

Host Virtuales. Es una de las modalidades más utilizadas por las empresas dedicadas al negocio del alojamiento web. Dependiendo de los recursos disponibles, permite tener una cantidad variable de dominios y sitios web en la misma máquina.

DNS. Domain Name System o Sistema de Nombres de Dominio y además de apuntar los dominios al servidor correspondiente

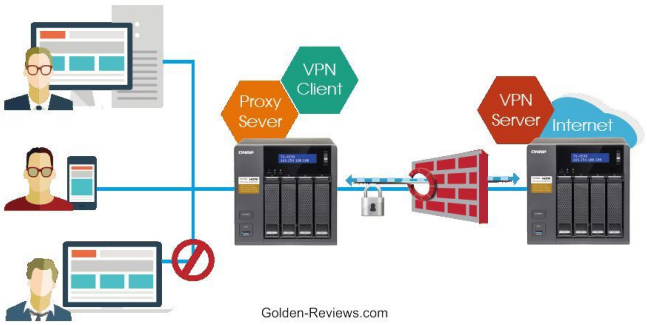
Iptables. Es una utilidad de línea de comandos para configurar un firewall del kernel de linux implementado como parte del proyecto NetFilter. El término se utiliza para referirse a dicho firewall del kernel.

CARACTERÍSTICAS GENERALES

- **PROXY**. Se deberá configurar un **servidor proxy utilizando SQUID**, el cual deberá incluir una **lista negra de palabras clave** para filtrar contenido no deseado. Esta lista estará almacenada en un archivo dentro del sistema de archivos del servidor.

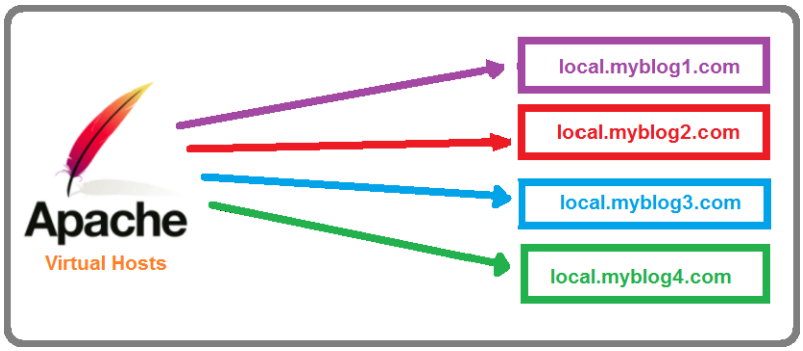
  Adicionalmente, se deberán **restringir al menos cinco sitios web específicos**, los cuales no podrán ser accedidos por los clientes a través del proxy.

  Cada equipo cliente deberá ser configurado manualmente en su **navegador web para utilizar el servidor proxy**, permitiendo así que todo el tráfico web pase por el control de SQUID y se apliquen las restricciones establecidas.



- **Host virtuales.** Para facilitar el acceso y despliegue de los distintos entornos o sitios web del proyecto, se solicita configurar Hosts Virtuales (Virtual Hosts) directamente en el servidor web (Apache o Nginx), evitando el uso del archivo local hosts de los sistemas clientes.

  Se deberá configurar un servidor web con la capacidad de soportar host virtuales (una o más páginas) que responderán en el mismo servidor. Habrá que configurar al menos 3 host virtuales diferentes con al menos una página de diferente para distinguir su acceso.



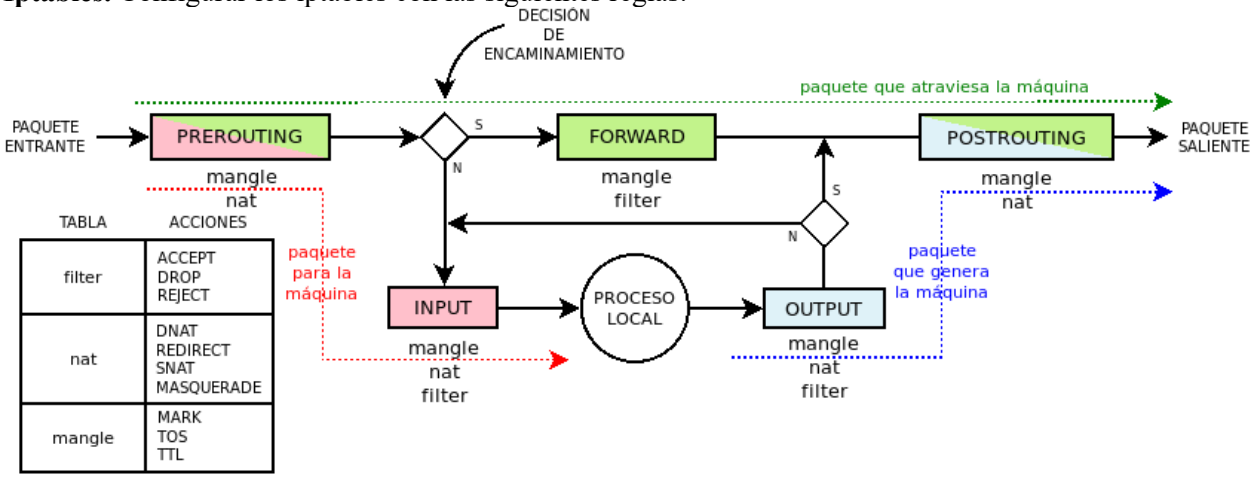
- **DNS.** Para el funcionamiento correcto de los hosts virtuales definidos en el proyecto, se establece como requerimiento la configuración de un **servidor DNS utilizando BIND**. Este servidor será el encargado de resolver los nombres de dominio (ficticios) asociados a cada uno de los servicios web implementados.

  Centralizar la resolución de nombres mediante BIND, evitando configuraciones manuales en archivos locales (`/etc/hosts`) y permitiendo el acceso a los distintos módulos del sistema desde cualquier equipo cliente conectado a la red.

Ejemplo de dominios definidos:

Dominio DNS	Función
`app1.midominio.local`	Sitio web principal
`admin.midominio.local`	Panel de administración
`api.midominio.local`	API del sistema

- **Iptables.** Configurar los iptables con las siguientes reglas:



Se debe configurar el firewall del sistema utilizando **iptables**, estableciendo un conjunto de reglas que controlen el tráfico de red según políticas de seguridad predefinidas. Las reglas deberán ser aplicadas de forma precisa, considerando tanto el tráfico de entrada como de salida.

Reglas solicitadas:

1. **Denegar el acceso al puerto 80 (HTTP)** para un equipo específico de la subred.
   Objetivo: Restringir el acceso a sitios web desde dicho equipo.
2. **Bloquear el acceso al puerto 21 (FTP)** para un equipo determinado de la subred.
   Objetivo: Impedir la transferencia de archivos mediante el protocolo FTP por razones de seguridad.
3. **Denegar el tráfico de salida** para el rango de direcciones IP comprendido entre `192.168.X.10` y `192.168.X.100`.
   Objetivo: Bloquear el tráfico hacia 90 equipos de la red por motivos de control o segmentación.
4. **Bloquear las respuestas ICMP tipo "ping" (echo-reply)** para todas las máquinas de la red.
   Objetivo: Hacer que los equipos no respondan a solicitudes de eco, ocultando su presencia en la red.
5. **Bloquear el acceso al puerto 25 (SMTP)** para un equipo identificado por su dirección MAC.
   Objetivo: Evitar el envío de correos no autorizados o spam desde ese dispositivo.

Reglas adicionales propuestas:

6. **Limitar el número de conexiones simultáneas por equipo a un máximo de 20.**
   Justificación: Evitar abusos de servicios por parte de usuarios o posibles ataques DoS internos.
7. **Bloquear todo tráfico saliente a sitios con destino al puerto 443 (HTTPS)** desde una estación de prueba.
   Justificación: Simular entornos sin navegación segura para pruebas de interceptación o monitoreo de tráfico.
8. **Permitir únicamente tráfico SSH (puerto 22) desde una IP autorizada.**
   Justificación: Restringir el acceso administrativo remoto solo al personal autorizado.
9. **Proponer al menos 3 servicios mas a denegar.**

NOTAS: • Puede instalar servicios extra para realizar la prueba.

NOTAS:
• Entregar el proyecto en equipos, en el apartado de aula virtual.
• Entregar documentación:

- Portada
- Descripción del proyecto.
- Temas investigados para la realización del proyecto.
  - Configuraciones
- Bitácora de trabajo.
- Conclusiones
- Referencias consultadas

• **Proyecto copiado de Internet o de alguna otra fuente causará anulación de la calificación final del curso, así como proyectos con errores de compilación o que no se realice lo que se pide.**

TEMAS A EVALUAR:

• Se evaluará que el proyecto funcione de acuerdo a lo descrito anteriormente. Además debe cumplir con los temas que marca el programa de la materia.