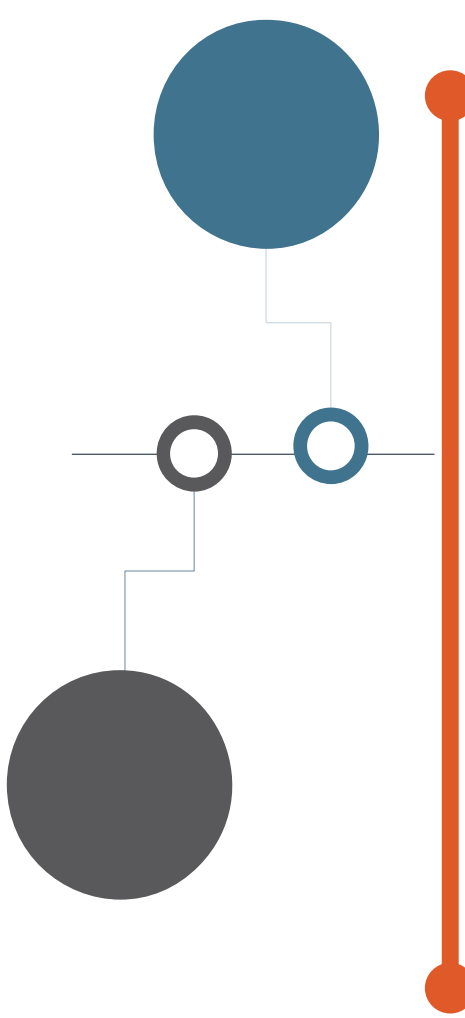
Servidores Web de Altas Prestaciones

Práctica 4: Seguridad (cortafuegos)

ICAR
INGENIERÍA DE COMPUTADORES, AUTOMÁTICA Y ROBÓTICA

UNIVERSIDAD DE GRANADA

Índice



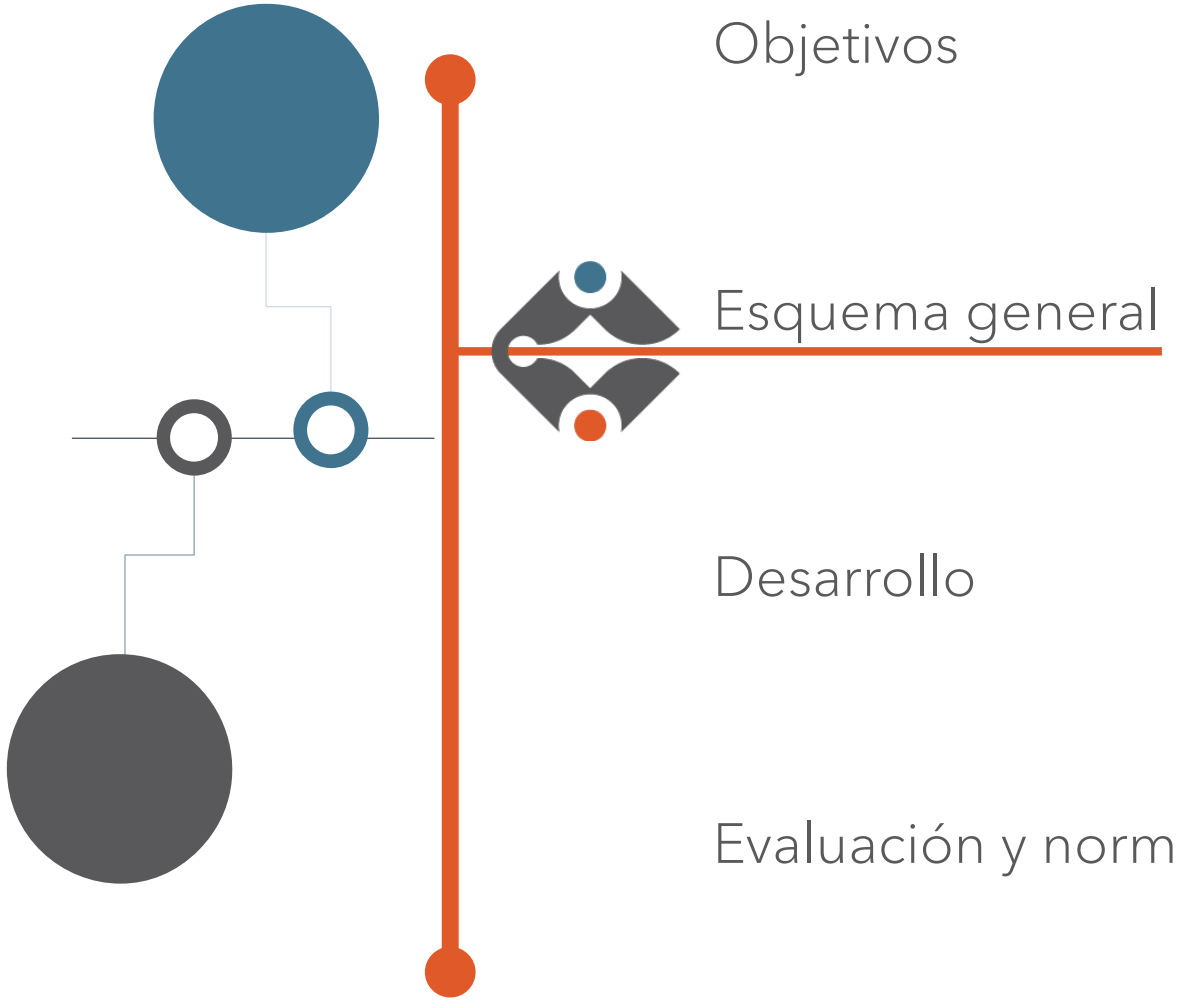
Objetivos

Esta práctica tiene como meta reforzar la seguridad de nuestra infraestructura web utilizando contenedores Docker y aplicando conceptos básicos de cortafuegos.

1. Implementar reglas básicas de IPTABLES para mejorar la seguridad del servidor.
2. Configurar políticas de IPTABLES para gestionar y filtrar el tráfico de red de forma eficiente.
3. Entender y aplicar prácticas de seguridad para proteger los servidores web.

La práctica se realizará de manera individual. Tiene un peso del **15%** del total de prácticas.

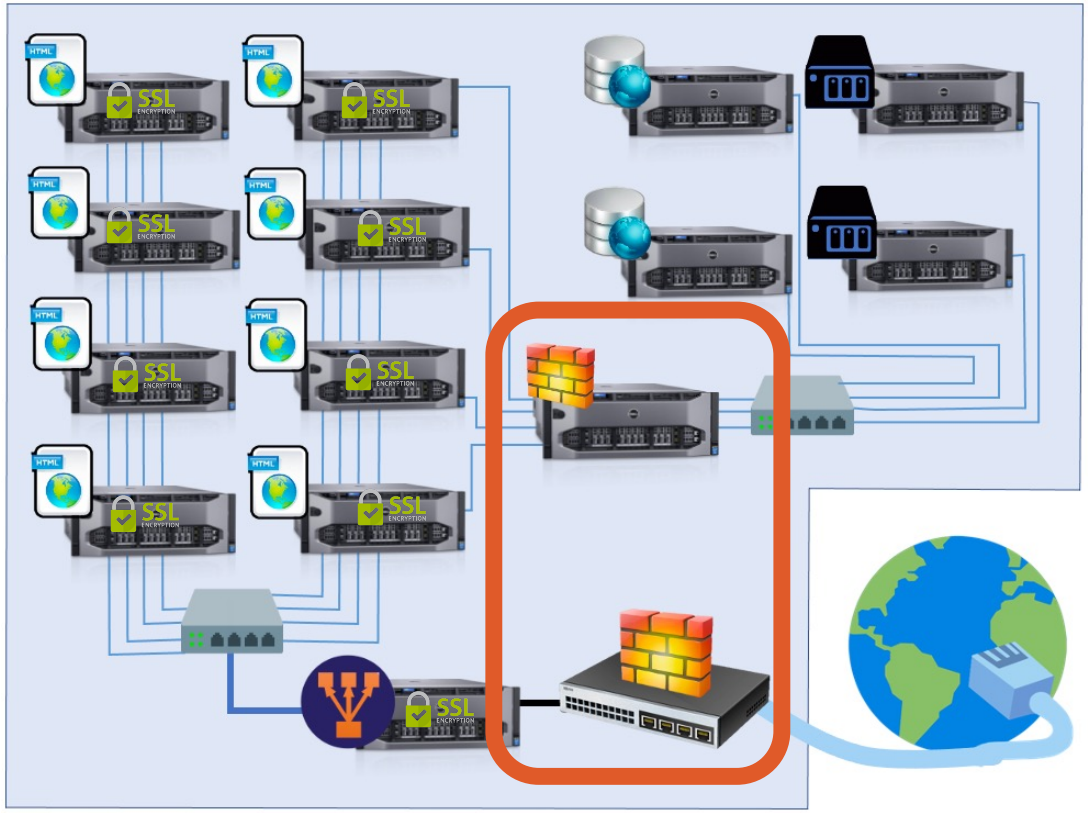
Índice



Esquema general

- Configuración de cortafuegos
- Creación de reglas personalizadas

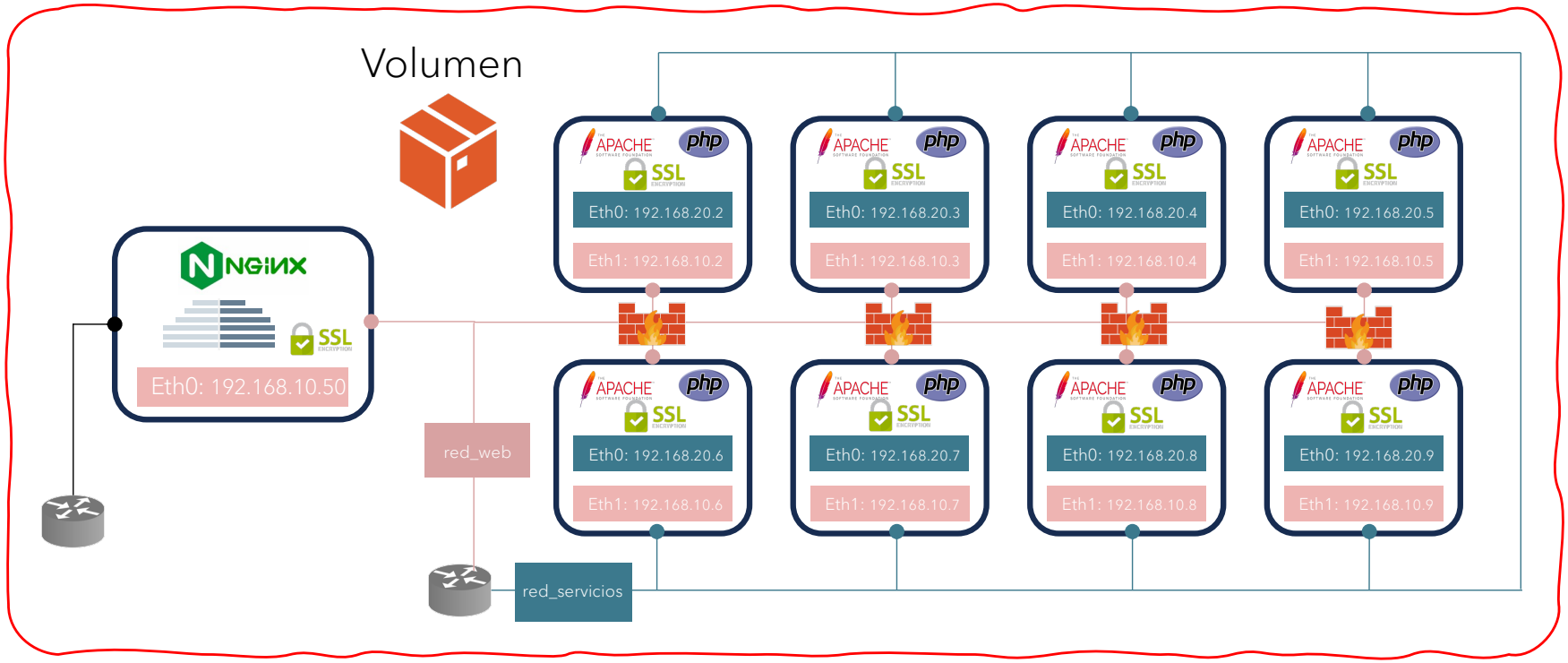
2 sesiones



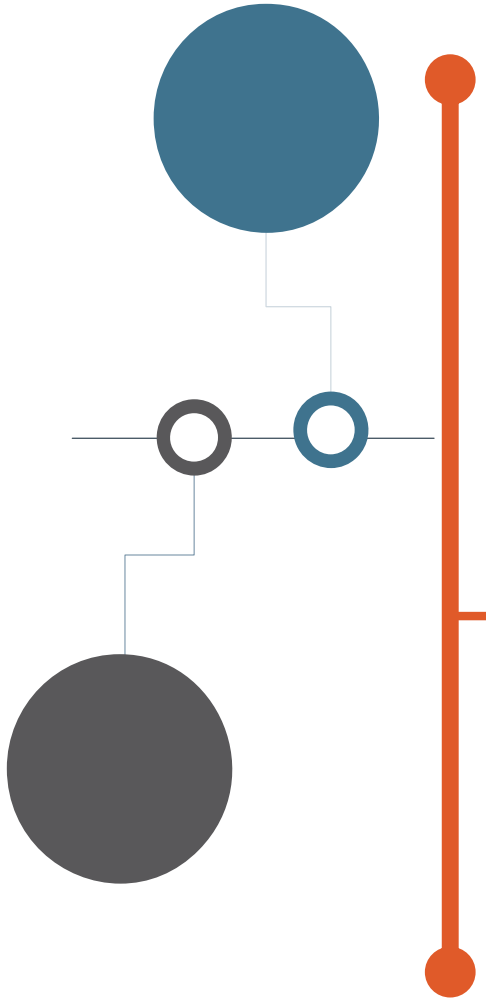
Requisitos Previos:

- Haber completado satisfactoriamente las Prácticas 1, 2 y 3 o tener experiencia equivalente en configuración de balanceadores de carga y certificados SSL con Docker.
- Conocimientos básicos sobre seguridad web y cortafuegos.

Esquema general de la práctica



Índice



Desarrollo

Se explorará el uso de IPTABLES para incrementar la seguridad de una granja web, diseñando e implementando políticas de defensa que permitan un control preciso del tráfico de red. Se crearán scripts para aplicar estas políticas, que incluyen medidas contra accesos no deseados y ataques externos, y se integrarán en los servidores web mediante Dockerfile y docker-compose.yml.

Se comenzará por desarrollar scripts específicos para definir y administrar políticas de seguridad, enfocándonos en controlar y filtrar tanto el tráfico entrante como el saliente hacia los servidores web. Posteriormente, se integrarán en los servidores mediante ajustes en Dockerfile y docker-compose.yml.

Parte 0: Creación del espacio de trabajo IPTABLES

En esta parte se establecerá el espacio de trabajo a través de directorios específicos para el conjunto de reglas y script necesarios para la configuración de cortafuegos. Partiendo de la estructura de directorios de la práctica anterior:

- Crea un directorio en tu máquina local llamado P4-tuusuariougr-certificados donde incluirá los certificados SSL que creaste en la práctica 3 así como directorios llamados P4-tuusuariougr-nginx y P4-tuusuariougr-apache para trabajar con los archivos de configuración de nginx y apache al igual que en la práctica 3.
- Dentro del directorio P4-tuusuariougr-apache, crea un directorio llamado P4-tuusuariougr-iptables-web donde se crearán los scripts necesarios para IPTABLES.
- Copia el directorio que creaste en la práctica 1 llamado web_tuusuariougr para que los servidores web sirvan el `index.php` que creaste en la práctica 1.

Parte 1: Definición de políticas de seguridad a los servidores web

En esta parte definiremos e implementaremos las políticas de seguridad que vamos a utilizar en la práctica para las réplicas de los servidores web. Trabajaremos en el directorio P4-tuusuariougr-iptables-web y se deberá crear un script llamado **`tuusuariougr-iptables-web.sh`** que implemente reglas IPTABLES con las siguientes especificaciones:

- **Denegación implícita de todo el tráfico.** Política por defecto de cualquier paquete entrante, saliente o reenvío que no cumpla con una regla explícita será descartado automáticamente. Esta política ayuda a proteger el sistema contra accesos no autorizados. Es una práctica de seguridad conservadora y restrictiva.

```
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
```

NOTA: No olvides darle permisos de ejecución al script tuusuariougr-iptables-web.sh

Parte 1: Definición de políticas de seguridad a los servidores web

En esta parte definiremos e implementaremos las políticas de seguridad que vamos a utilizar en la práctica para las réplicas de los servidores web. Trabajaremos en el directorio P4-tuusuariougr-iptables-web y se deberá crear un script llamado **`tuusuariougr-iptables-web.sh`** que implemente reglas IPTABLES con las siguientes especificaciones:

- Manejar el tráfico de red entrante basado en el estado de las conexiones. Permitir conexiones establecidas y relacionadas al tráfico entrante para permitir paquetes que sean parte de una conexión ya existente o paquetes que estén iniciando una nueva conexión pero que estén asociados a una ya existente. Es una configuración común para asegurar que las respuestas a solicitudes iniciadas por el sistema local sean permitidas.

```
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

NOTA: No olvides darle permisos de ejecución al script tuusuariougr-iptables-web.sh

Parte 1: Definición de políticas de seguridad a los servidores web

En esta parte definiremos e implementaremos las políticas de seguridad que vamos a utilizar en la práctica para las réplicas de los servidores web. Trabajaremos en el directorio P4-tuusuariougr-iptables-web y se deberá crear un script llamado **`tuusuariougr-iptables-web.sh`** que implemente reglas IPTABLES con las siguientes especificaciones:

- Manejar el tráfico de red saliente basado en el estado de las conexiones. Permitir conexiones nuevas al tráfico saliente para que el host envíe paquetes asociados con nuevas solicitudes, así como aquellos que forman parte de conexiones ya establecidas o relacionadas. Esto es crucial para permitir que las aplicaciones en el host inicien y mantengan conexiones de red sin interrupción.

```
iptables -A OUTPUT -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
```

NOTA: No olvides darle permisos de ejecución al script tuusuariougr-iptables-web.sh

Parte 1: Definición de políticas de seguridad a los servidores web

En esta parte definiremos e implementaremos las políticas de seguridad que vamos a utilizar en la práctica para las réplicas de los servidores web. Trabajaremos en el directorio P4-tuusuariougr-iptables-web y se deberá crear un script llamado **`tuusuariougr-iptables-web.sh`** que implemente reglas IPTABLES con las siguientes especificaciones:

- Manejar tráfico de red de la misma máquina. Permitir el tráfico que el host envía a sí mismo, tanto entrante como saliente. Es una configuración común para la operación normal del sistema, ya que muchos procesos internos del sistema operativo y aplicaciones usan esta interfaz para comunicarse entre sí.

```
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT
```

NOTA: No olvides darle permisos de ejecución al script tuusuariougr-iptables-web.sh

Parte 1: Definición de políticas de seguridad a los servidores web

En esta parte definiremos e implementaremos las políticas de seguridad que vamos a utilizar en la práctica para las réplicas de los servidores web. Trabajaremos en el directorio P4-tuusuariougr-iptables-web y se deberá crear un script llamado **tuusuariougr-iptables-web.sh** que implemente reglas IPTABLES con las siguientes especificaciones:

- Manejar tráfico HTTP y HTTPS. Permitir el tráfico TCP entrante al puerto 80 y 443 respectivamente pero solo proveniente del balanceador de carga.

```
iptables -A INPUT -p tcp -s 192.168.10.50 --dport 80 -j ACCEPT
iptables -A INPUT -p tcp -s 192.168.10.50 --dport 443 -j ACCEPT
```

NOTA: No olvides darle permisos de ejecución al script tuusuariougr-iptables-web.sh

Parte 2: Configuración de Servidores Web con las reglas IPTABLES

En esta parte configuraremos los servidores web finales para implementar las políticas de seguridad definidas en la parte 1. Trabajaremos en el directorio P4-tuusuariougr-apache.

Parte 2.1 – Script de entrada – `entrypoint.sh`

Crea un script llamado `entrypoint.sh` dentro del directorio P4-tuusuariougr-**iptables-web** que ejecute el script con las reglas IPTABLES y luego ejecute el comando principal del contenedor: exec "$@".

Ejemplo básico de entrypoint.sh

```
#!/bin/bash
# Ejecuta el script de iptables
./tuusuariougr-iptables-web.sh

# Luego, ejecuta el comando principal del contenedor
exec "$@"
```

NOTA: No olvides darle permisos de ejecución al script entrypoint.sh

Parte 2: Configuración de Servidores Web con las reglas IPTABLES

En esta parte configuraremos los servidores web finales para implementar las políticas de seguridad definidas en la parte 1. Trabajaremos en el directorio P4-tuusuariougr-apache.

Parte 2.2 – DockerFile con ENTRYPOINT – **`DockerFileApacheP4`**

El archivo DockerFileApacheP4 debe crearse en el directorio P4-tuusuariougr-apache y llamarse tuusuariougr-apache-image:p4. Debe contener instrucciones para:

1. Partir de la imagen para Apache creada en la práctica 3.
2. Instalar IPTABLES.
3. Copia el script de entrada entrypoint.sh y el script de reglas tuusuariougr-iptables-web.sh al contenedor.
4. Da permisos de ejecución a los scripts en el contenedor.
5. Configura el ENTRYPOINT con el script de entrada.

Parte 2: Configuración de Servidores Web con las reglas IPTABLES

En esta parte configuraremos los servidores web finales para implementar las políticas de seguridad definidas en la parte 1. Trabajaremos en el directorio P4-tuusuariougr-apache.

Parte 2.2 – DockerFile con ENTRYPOINT – **`DockerFileApacheP4`**

Ejemplo básico de DockerFile

```
#Instalar iptables
RUN apt-get update && apt-get install -y iptables

# Copiar script de entrada entrypoint y script de reglas iptables
COPY ./P4-tuusuariougr-iptables-web/entrypoint.sh /entrypoint.sh
COPY ./P4-tuusuariougr-iptables-web/tuusuaruiougr-iptables-web.sh
/tuusuariougr-iptables-web.sh

# Dar permisos de ejecución a los scripts
RUN chmod +x /entrypoint.sh /tuusuaruiougr-iptables-web.sh

# Configurar el script de entrada
ENTRYPOINT ["/entrypoint.sh"]
```

Parte 3: Configuración de Docker Compose para la Granja Web con IPTABLES

Parte de **docker-compose.yml** de la **práctica 3** y añade capacidades de administración de red a los servicios web.

Definir un servicio para cada instancia de Apache que incluya:

- Imagen construida a partir del DockerFileApacheP4 y que se llame tuusuarioUGR-apache-image:p4.
- Nombre del contendedor: webX donde X es el número de contenedor del 1 al 8.
- Volumen para montar el directorio local **web_**tuusuarioUGR en la ruta por defecto de Apache para servir el index.php.
- Volumen para montar el directorio local **certificados_**tuusuarioUGR en la carpeta /etc/apache2/ssl/.
- Conexión a las redes red_web y red_servicios con las IP indicadas en el esquema de la práctica.
- Capacidades de administración de red para poder ejecutar IPTABLES.

```
cap_add:
 -NET_ADMIN
```

Parte 3: Configuración de Docker Compose para la Granja Web con IPTABLES

Parte de **docker-compose.yml** de la **práctica 3** y añade capacidades de administración de red a los servicios web.

Definir un servicio llamado balanceador-nginx que incluya:

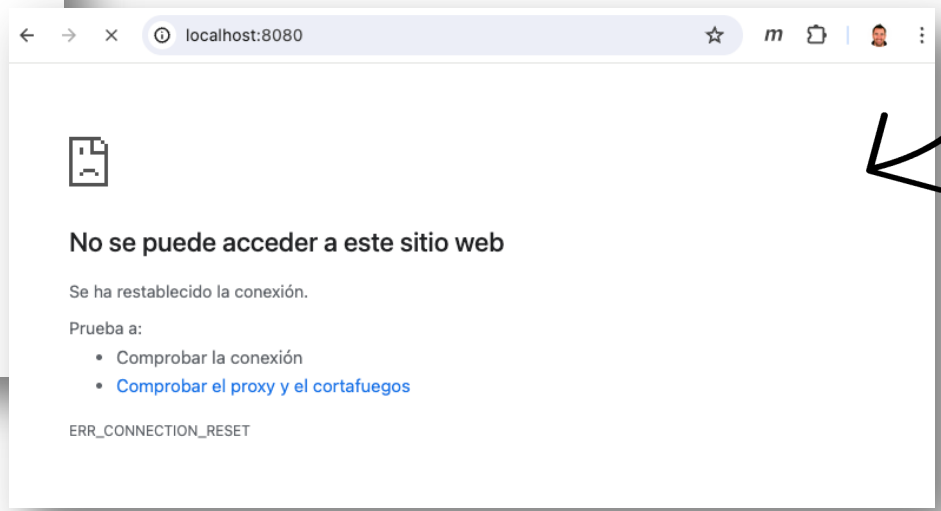
- Construcción de la imagen a partir del DockerFileNginxP4 y que se llame tuusuarioUGR-nginx-image:p4.
- Volumen para montar el archivo tuusuariougr-nginx-ssl.conf en el contenedor en /etc/nginx/nginx.conf.
- Volumen para montar el directorio local certificados_tuusuarioUGR en la carpeta /etc/nginx/ssl/.
- Asignación de dirección IP estática 192.168.10.50 en la red red_web.
- Dependencia establecida con los servicios de Apache para garantizar el orden correcto de despliegue.

Parte 4: Verificación y pruebas del escenario con IPTABLES

En esta sección realizará el despliegue del escenario y se verificará.

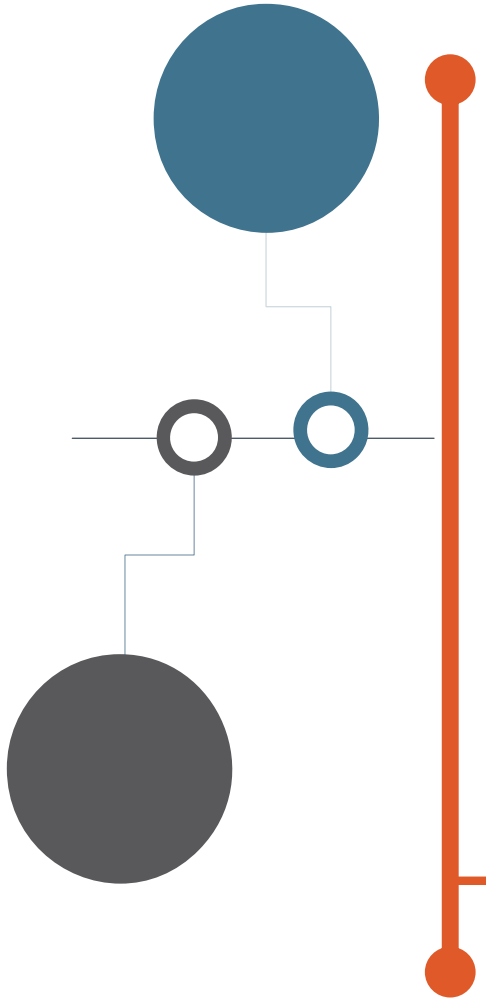
- **Verificación y Pruebas:**
  - Verifica que Nginx distribuya adecuadamente las solicitudes HTTP y HTTPS entre los diferentes servidores Apache y que no puedas acceder directamente a los servidores web.

Peticiones a un servidor web apache:



Peticiones al balanceador:

Índice



Evaluación

Para superar la práctica se deben realizar las siguientes tareas básicas:

B1. Preparación del Entorno de Trabajo

- Crear y preparar directorios específicos para los archivos de configuración de IPTABLES y certificados SSL previamente generados. Esto incluye:
  - Un directorio para scripts IPTABLES específicos.

B2. Creación y Configuración de Scripts IPTABLES

- Desarrollar y escribir un script tuusuariougr-iptables-web.sh que establecerá las reglas de IPTABLES en los servidores web. Este script debe:
  - Establecer políticas por defecto para rechazar todo tráfico no explícitamente permitido.
  - Permitir conexiones entrantes y salientes específicas necesarias para la operación normal de los servidores web.
  - Asegurar que las conexiones entre el balanceador de carga y los servidores web estén adecuadamente configuradas para permitir solo tráfico HTTP y HTTPS.

Evaluación

Para superar la práctica se deben realizar las siguientes tareas básicas:

B3. Implementación de Scripts IPTABLES en Docker

- Integrar el script IPTABLES en la configuración de Docker de los servidores web Apache. Esto implica:
  - Modificar los Dockerfiles para incluir y ejecutar el script IPTABLES al iniciar los contenedores.
  - Asegurar que los scripts tienen los permisos adecuados para ejecutarse y modificar las reglas de IPTABLES dentro de los contenedores.

B4. Configuración de Docker Compose

- Modificar y adaptar el archivo docker-compose.yml de la práctica anterior para incluir los cambios necesarios que permitan la ejecución de IPTABLES dentro de los contenedores de Apache y Nginx. Esto incluirá:
  - La configuración para montar los scripts y directorios necesarios dentro de los contenedores.
  - Asegurar que los contenedores tienen las capacidades de red necesarias (CAP_NET_ADMIN) para modificar IPTABLES.

Evaluación

Para superar la práctica se deben realizar las siguientes tareas básicas:

B5. Verificación y Pruebas

- Ejecutar y verificar el entorno configurado. Esto implica:
  - Desplegar los servicios usando Docker Compose.
  - Verificar que las reglas de IPTABLES están activas y funcionando como se espera dentro de los contenedores.
  - Confirmar que el tráfico no permitido está siendo correctamente bloqueado, mientras que el tráfico legítimo fluye según lo esperado.

Evaluación

Se proponen, opcionalmente, las siguientes tareas avanzadas:

A1: Definir e implementar políticas de seguridad en el balanceador de carga

- Definir e implementar políticas de seguridad en el balanceador de carga. Podría incluir, además de denegación implícita:
  - Limitar el número de conexiones simultáneas.
  - Bloquear escaneo de puertos.
  - Usar módulo string para mitigar ataques de inyección SQL o XSS a través de las peticiones HTTP.
  - Etc.

Se proponen, opcionalmente, las siguientes tareas avanzadas:

A2. Configuración Avanzada de IPTABLES para DDoS

- Implementar reglas avanzadas en IPTABLES para mitigar ataques de Denegación de Servicio Distribuido (DDoS). Esto podría incluir:
  - Limitación de la tasa de conexiones nuevas por IP para evitar la saturación de los recursos del servidor.
  - Uso de módulos como recent para detectar y bloquear rápidamente el tráfico anómalo y prevenir inundaciones de IPs.
  - Configuración de umbrales y reglas específicas que identifiquen patrones de tráfico asociados a ataques comunes de DDoS.
  - Protección Contra Ataques de Fragmentación.
  - Etc.

Evaluación

Se proponen, opcionalmente, las siguientes tareas avanzadas:

A3: Simular ataques a la granja web y configuraciones de seguridad realizadas

- Simular un ataque DDoS para probar la configuración de seguridad de la granja web.
- Simular un ataque de inyección SQL o XSS
- Simular otros ataques.

- Se debe demostrar la efectividad de la implementación ante las simulaciones de ataques.

Normas de entrega

Se desarrollará un documento siguiendo el guion de la práctica y **detallando** e indicando, en su caso, los **aspectos básicos y avanzados realizados**, comandos de terminal ejecutados, resultados de ejecución, etc.

- Por ejemplo, si se ha realizado la tarea básica de configuración del entorno, el documento .pdf con la memoria de prácticas debe aparecer una sección titulada: *Tareas Básicas - Tareas Básicas - B2. Creación y Configuración de Scripts IPTABLES* donde aparezcan detalladas las configuraciones. De igual forma, si por ejemplo, se han realizado tareas avanzadas sobre automatizaciones con Scripts, debe aparecer *Tareas Avanzadas – A2. Configuración Avanzada de IPTABLES para DDoS,* detalles de las configuraciones, explicaciones sobre ellas y resultados.

Se recomienda utilizar herramientas de control de Tiempo (por ejemplo, clockify) para contabilizar el tiempo de dedicado a la realización de la práctica.

Se deja a **libre elección** la **estructura y formato** del documento el cual reflejará el correcto desarrollo de la práctica a modo de diario/tutorial siguiendo los puntos descritos anteriormente. Asimismo, se recomienda incluir capturas de pantalla que reflejen el correcto desarrollo de los distintos apartados de la práctica. La **primera página** del documento debe incluir, al menos, **nombre**, **apellidos** y **tiempo dedicado a la práctica** medido con herramientas de control de tiempo.

Normas de entrega

Para la entrega se habilitará una tarea en PRADO cuya entrega debe seguir OBLIGATORIAMENTE el formato especificado.

1. Un archivo **.pdf** con el documento desarrollado siguiendo el formato ApellidosNombreP4.pdf
2. Un archivo **.zip** con los distintos archivos de configuraciones, carpetas, etc. necesarios para la ejecución de la práctica siguiendo el formato ApellidosNombreP4.zip

Uso de Inteligencia Artificial Generativa

Para cada práctica es OBLIGATORIO usar herramientas de IA generativa (ChatGPT, Copilot u otras) e incluir enlace al chat/prompt utilizado. También se debe analizar y justificar el resultado que proporciona la herramienta con el resultado final que opta el estudiante para la práctica.

Es OBLIGATORIO incluir en el guion una sección titulada: "**Análisis propuesta IA**" donde se incluya enlace al chat/prompt con las consulta/as realizada/as, resultado que proporciona la IA y un párrafo con un análisis crítico y detallado del resultado proporcionado.

Normas de entrega

La práctica se realizará de manera individual. Tiene un peso del **15%** del total de prácticas.

La práctica se evaluará mediante el uso de rúbrica específica (accesible por el estudiante en la tarea de entrega) y una defensa final de prácticas.

Cuestiones sobre la calificación obtenida en cada práctica se realizarán **UNICAMENTE** en la sesión dedicada a recuperación/defensa al final de curso.

La detección de prácticas copiadas implicará el suspenso inmediato de todos los implicados en la copia (tanto del autor del original como de quien las copió). OBLIGATORIO ACEPTAR LICENCIA EULA DE TURNITIN en la entrega. Si la memoria supera un 40% de copia Turnitin implicará el suspenso automáticamente.

Servidores Web de Altas Prestaciones

Práctica 4: Seguridad (cortafuegos)

ICAR
INGENIERÍA DE COMPUTADORES, AUTOMÁTICA Y ROBÓTICA

UNIVERSIDAD DE GRANADA