

# Guía de Configuración de Portal Cautivo en pfSense

El portal cautivo es un sistema que controla el acceso a la red y permite gestionar la velocidad de conexión, normalmente utilizado en redes públicas para autenticar a los usuarios y registrar su actividad. Aquí te explico cómo configurarlo en pfSense, detallando cada paso y los beneficios que aporta.

## ¿Qué es un Portal Cautivo?

Un portal cautivo intercepta el tráfico de una red y redirige a los usuarios a una página de inicio de sesión donde deben autenticarse. Solo después de autenticarse podrán acceder a la red y a Internet. Puede emplearse en redes cableadas e inalámbricas.

## Beneficios del Portal Cautivo

1. **Identificación de usuarios:** Permite rastrear quién accede a la red.
2. **Registro y trazabilidad:** Facilita el monitoreo del uso de la red.
3. **Versatilidad:** Compatible con redes cableadas e inalámbricas.

## Configuración en pfSense

### 1. Configuración de Usuarios Locales

- **Acceso:** Ve a [System / User Manager / Users](#).
- **Crear un Usuario:** Crea un usuario con nombre y contraseña para la autenticación.
- **Crear un Grupo:** Asigna a los usuarios el privilegio de autenticarse en el portal cautivo.

### 2. Creación de un Certificado Autofirmado

- **Acceso:** Dirígete a [System / Certificate Manager / CAs](#) y selecciona "Add".
- **Configuración del Certificado:**
  - **Nombre descriptivo:** Escribe un nombre para el certificado.
  - **Método:** Selecciona "Create an internal Certificate Authority".
  - **Longitud de clave:** 2048 bits (por defecto).
  - **Algoritmo de digestión:** SHA-1.
  - **Tiempo de vida:** 365 días o el tiempo deseado.
  - **Nombre común:** Ingresa el nombre de dominio configurado previamente, que puedes ver en el "dashboard" de pfSense.

Luego, crea un certificado de servidor usando el CA creado.

### 3. Configuración del DNS

- **Acceso:** Ve a [Services / DNS Resolver / General Settings](#).
- **Configuración del DNS:**
  - Activa el [DNS Resolver](#).
  - En "Host Overrides", selecciona "Add" y configura:
    - **Host:** Nombre del host.

- **Dominio:** Nombre del dominio.
- **Dirección IP:** IP de la LAN.

#### 4. Configuración del Portal Cautivo

- **Acceso:** Ve a [Services](#) / [Captive Portal](#) y selecciona "Add".
- **Parámetros principales:**
  - **Enable Captive Portal:** Activa el portal cautivo.
  - **Interface:** Elige la interfaz de la red.
  - **Hard Timeout:** Define el tiempo máximo de conexión.
  - **Redirection URL:** Establece la URL a la que se redirigirá al usuario después de autenticarse.
  - **MAC Filtering:** Desactívalo para facilitar el acceso sin filtro de MAC.
  - **Authentication:** Selecciona "Local" para usar usuarios de pfSense.
  - **Portal Page Contents:** Personaliza el contenido de la página de inicio de sesión.

Puedes también habilitar el certificado previamente configurado para una conexión segura.

#### 5. Pruebas de Funcionamiento

- Prueba la conectividad desde un cliente haciendo [ping](#) para verificar que está funcionando.
- Al acceder a un navegador, el portal cautivo redirigirá al usuario a la página de autenticación. Si el certificado no está instalado en el equipo, mostrará un aviso de seguridad.

#### Seguridad y Restricciones del Portal Cautivo

- **Seguridad:** El portal cautivo impide el acceso directo a Internet, pero no a la red local, lo cual podría ser un riesgo de seguridad (ej., ataques Man-in-the-Middle).
- **IDS Recomendado:** Para mayor seguridad, considera instalar un sistema IDS (Intrusion Detection System) y aislar el portal cautivo del resto de la red de la empresa.

#### Personalización Adicional

- Puedes personalizar la página del portal cargando plantillas HTML en [HTML Page Contents](#) y archivos adicionales en [File Manager](#).