

VERSION PUBLICA Y ANONIMIZADA

Memoria publica del proyecto

Infraestructura segura con Proxmox VE, IPFire y aplicacion web

Mois0n - Moises Cuevas Gomez

Area	Administracion de sistemas, redes, virtualizacion e infraestructura segura
Tecnologias	Proxmox VE, IPFire, Linux, Apache, MySQL, phpMyAdmin, Python
Enfoque	Documento publico orientado a empleabilidad y portfolio profesional
Privacidad	Se omiten IPs, dominios, credenciales, reglas sensibles y capturas internas

Documento generado a partir de la memoria tecnica academica del proyecto integrado. Esta version esta preparada para publicacion en portfolio profesional.

Indice

1. Resumen ejecutivo
2. Objetivos del proyecto
3. Alcance y requisitos
4. Arquitectura general
5. Segmentacion de red
6. Servicios desplegados
7. Automatizacion con Python
8. Seguridad aplicada
9. Problemas encontrados y soluciones
10. Competencias demostradas
11. Mejoras futuras
12. Conclusion
13. Nota de publicacion segura

1. Resumen ejecutivo

Este documento presenta una version publica, reducida y anonimizada del proyecto "Infraestructura segura con Proxmox VE, IPFire y aplicacion web". La finalidad es mostrar de forma profesional el trabajo realizado sin exponer configuraciones reales, datos internos ni informacion sensible.

El proyecto se basa en el diseño e implantacion de una infraestructura virtualizada que integra Proxmox VE como plataforma de virtualizacion, IPFire como firewall, segmentacion de red en zonas diferenciadas, despliegue de servicios web y base de datos, y automatizacion mediante Python para el control de stock.

Elemento	Descripcion publica
Proyecto	Infraestructura virtualizada orientada a seguridad, servicios web y automatizacion
Base	Servidor fisico con Proxmox VE
Seguridad perimetral	IPFire como firewall y gestor de zonas de red
Servicios	Apache/PHP, MySQL, phpMyAdmin y contenedor Python
Resultado	Entorno funcional documentado, con separacion de funciones y enfoque de seguridad

2. Objetivos del proyecto

El objetivo principal fue construir un laboratorio tecnico que integrara varias areas clave de administracion de sistemas y redes: virtualizacion, firewall, servicios web, base de datos, automatizacion y documentacion tecnica.

- Diseñar una infraestructura virtualizada sobre Proxmox VE.
- Separar funciones mediante una arquitectura por zonas de red.
- Desplegar una aplicacion web con base de datos.
- Utilizar IPFire como firewall y punto de control del trafico.
- Automatizar comprobaciones de stock mediante Python.
- Documentar problemas encontrados, decisiones tecnicas y mejoras futuras.

3. Alcance y requisitos

El alcance del proyecto cubre desde la instalacion del entorno base hasta la puesta en funcionamiento de los servicios principales. La memoria academica original incluia capturas y configuraciones detalladas; esta version publica se centra en la arquitectura, las tecnologias y las competencias demostradas.

Categoria	Requisito o decision
Hardware	Equipo fisico usado como servidor de laboratorio
Virtualizacion	Uso de maquinas virtuales y contenedores para separar servicios
Red	Segmentacion en zonas RED, GREEN y ORANGE
Servicios	Servidor web, base de datos, administracion y automatizacion
Seguridad	Filtrado de trafico, aislamiento y publicacion anonimizada

4. Arquitectura general

La arquitectura se planteo como una infraestructura modular. Proxmox VE actua como capa de virtualizacion y permite desplegar de forma separada el firewall, los servicios web, la base de datos y los procesos de automatizacion.

Arquitectura logica simplificada

Servidor fisico

- > Proxmox VE
 - > IPFire Firewall
 - > RED: salida/red externa
 - > GREEN: red interna/administracion
 - > ORANGE: servicios web/DMZ
 - > Contenedor Servidor Apache/PHP
 - > Contenedor Base de datos MySQL
 - > Contenedor phpMyAdmin
 - > Contenedor Python para automatizacion

Este enfoque permite aislar funciones, controlar comunicaciones entre zonas y documentar cada componente de manera independiente.

5. Segmentacion de red

La segmentacion de red fue una de las partes mas importantes del proyecto. En lugar de trabajar sobre una red plana, se definieron zonas diferenciadas para separar salida exterior, administracion interna y servicios.

Zona	Funcion
RED	Zona de salida o conexion exterior. Se considera la zona menos confiable.
GREEN	Zona interna de confianza para administracion y gestion de servicios.
ORANGE	Zona tipo DMZ orientada a servicios web o componentes separados de la red interna.

La separacion por zonas facilita aplicar reglas de filtrado, reducir superficie de exposicion y limitar el impacto si un servicio queda comprometido o mal configurado.

6. Servicios desplegados

El proyecto integra servicios necesarios para disponer de una aplicacion web funcional y administrable. La version publica agrupa estos servicios por funcion, sin exponer configuraciones internas.

Servicio	Papel dentro del proyecto
Apache/PHP	Servidor web y ejecucion de la aplicacion desarrollada.
MySQL	Base de datos para usuarios, productos, compras y stock.
phpMyAdmin	Administracion visual de la base de datos durante pruebas y desarrollo.
Python	Automatizacion de comprobaciones de stock y generacion de avisos.
IPFire	Firewall, segmentacion de red y control del trafico entre zonas.

7. Automatizacion con Python

Una parte relevante del proyecto fue la automatizacion del control de stock. Se planteo un script que consulta la base de datos y detecta productos por debajo de un umbral definido, generando un aviso para facilitar la gestion.

Base de datos MySQL

- > Script Python
- > Consulta de productos
- > Deteccion de bajo stock
- > Registro o aviso

Esta parte demuestra integracion entre scripting y base de datos, asi como la capacidad de automatizar tareas repetitivas de administracion.

8. Seguridad aplicada

El proyecto se oriento a construir una infraestructura con criterios basicos de seguridad. La seguridad se trabajo desde varias capas: red, servicios, acceso, documentacion y publicacion responsable.

- Uso de IPFire como firewall dedicado.
- Separacion de zonas de red para servicios internos y servicios expuestos.
- Aplicacion de reglas de filtrado y control de trafico.
- Uso de HTTPS/certificados en el contexto del proyecto original, presentado aqui de forma resumida.
- Aislamiento de procesos mediante maquinas o contenedores.
- No publicacion de credenciales, IPs reales, dominios, usuarios o reglas sensibles.

9. Problemas encontrados y soluciones

Durante el proyecto se documentaron incidencias tecnicas relacionadas con instalacion, comunicacion entre servicios, acceso desde zonas de red, dependencias y publicacion de servicios. Estos problemas forman parte del valor del proyecto, porque muestran capacidad de diagnostico y resolucion.

Problema	Enfoque de solucion
Instalacion de Python en contenedor	Separar el entorno de ejecucion y resolver dependencias sin afectar al sistema base.
Acceso a servicios en DMZ	Revisar reglas, rutas, interfaces y registros para localizar problemas de comunicacion.
Conectividad entre servicios	Comprobar puertos, rutas, firewall y dependencias de aplicacion.
Administracion de base de datos	Validar permisos, usuarios tecnicos y comunicacion entre aplicacion y MySQL.

10. Competencias demostradas

- Instalacion y administracion de un entorno de virtualizacion con Proxmox VE.
- Diseño de una arquitectura segmentada con firewall dedicado.
- Despliegue de servicios web y base de datos en Linux.
- Integracion de aplicacion web, MySQL y automatizacion con Python.
- Diagnostico de conectividad y resolucion de incidencias.
- Documentacion tecnica de un proyecto completo.
- Criterio de seguridad al preparar una version publica para portfolio.

11. Mejoras futuras

Como evolucion del proyecto, se pueden plantear mejoras orientadas a hacerlo mas cercano a un entorno profesional.

- Incorporar monitorizacion de servicios y recursos.
- Centralizar logs y alertas de seguridad.
- Aplicar hardening mas completo sobre servicios expuestos.
- Documentar reglas de firewall de forma anonima y visual.
- Añadir diagramas tecnicos limpios para el portfolio.

- Ampliar la parte de ciberseguridad con pruebas controladas de laboratorio.

12. Conclusion

Este proyecto representa una base solida para demostrar competencias en administracion de sistemas, redes, virtualizacion, despliegue de servicios, automatizacion y seguridad. La combinacion de Proxmox VE, IPFire, Linux, Apache, MySQL y Python permite mostrar una vision practica e integrada de una infraestructura IT.

La version publica resume los aspectos mas importantes del proyecto sin exponer informacion sensible, por lo que puede utilizarse como material de apoyo dentro del portfolio profesional.

13. Nota de publicacion segura

Esta memoria es una version publica y anonimizada. Se han omitido deliberadamente datos tecnicos sensibles como IPs reales, dominios, credenciales, nombres internos, reglas completas de firewall, configuraciones de VPN/PPPoE, capturas de administracion y cualquier informacion que pudiera comprometer un entorno real o ya desplegado.

Portfolio tecnico: <https://mois0n.pages.dev>