https://doi.org/10.22201/dgtic.30618096e.2026.4.3.190 Vol. 4, Núm. 3. julio-septiembre 2026, págs. 74 - 82

Uso de la herramienta OPNsense para la gestión de seguridad unificada de un centro de datos

Use of the OPNsense tool for unified threat management in a data center

Pedro Temachti Pérez Santillán
Dirección General de Cómputo y de Tecnologías de Información y Comunicación
Universidad Nacional Autónoma de México
ptsantillan@unam.mx
ORCID: 0009-0000-2626-9073

Información del reporte:

Para citar este reporte técnico:

Pérez Santillán, P. T. (2026). Uso de la herramienta OPNsense para la gestión de seguridad unificada de un centro de datos. *Cuadernos Técnicos Universitarios de la DGTIC, 4*(3), páginas (74 - 82). https://doi.org/10.22201/dgtic.30618096e.2026.4.3.190

Resumen

La seguridad de la infraestructura tecnológica en los centros de datos requiere esquemas robustos que controlen el acceso y protejan los servicios críticos contra amenazas externas. Ante la exposición directa de servidores de administración con direcciones públicas y la falta de conexiones remotas seguras en una organización, se planteó la necesidad de implementar una solución de gestión unificada de amenazas que permitiera centralizar el tráfico de red, ocultar los equipos internos y habilitar accesos cifrados para el personal técnico.

La metodología se desarrolló a través de un enfoque que abarcó el diseño lógico de una arquitectura segmentada y la posterior instalación de una plataforma de código abierto sobre un entorno virtualizado. Se configuraron reglas estrictas para aislar los segmentos de operación, se habilitó la traducción de direcciones uno a uno para gestionar las salidas a la red externa y se crearon servidores virtuales independientes de red privada para el acceso remoto. Finalmente, se ejecutaron pruebas de conectividad y auditoría de eventos para validar la efectividad de las políticas establecidas antes de la puesta en marcha definitiva. Una limitación del estudio fue la imposibilidad de validar empíricamente el bloqueo geográfico, debido a la falta de acceso a direcciones IP de origen extranjero durante la etapa de pruebas.

https://doi.org/10.22201/dgtic.30618096e.2026.4.3.190 Vol. 4, Núm. 3. julio-septiembre 2026, págs. 75 - 82

Los resultados demostraron un ocultamiento de los equipos internos y un control del tráfico saliente. Los intentos de acceso no autorizado fueron mitigados de manera automática y registrados para su posterior auditoría, mientras que las conexiones de red privada funcionaron de forma estable en diversos sistemas operativos. Se concluyó que la solución adoptada resolvió las vulnerabilidades iniciales al reducir la superficie de ataque, recomendando para el futuro la integración de sistemas de inspección profunda y la centralización de registros.

Palabras clave: OPNsense, OpenVPN, *firewall*, VPN, ciberseguridad.

Abstract

The security of technological infrastructure in data centers requires robust frameworks that control access and protect critical services against external threats. Given the direct exposure of administration servers with public addresses and the lack of secure remote connections in an organization, the need arose to implement a unified threat management solution to centralize network traffic, hide internal equipment, and enable encrypted access for technical personnel.

The methodology was developed through a structured approach that encompassed the logical design of a segmented architecture and the subsequent installation of an open-source platform within a virtualized environment. Strict filtering rules were configured to isolate operational segments, one-to-one address translation was enabled to regulate outbound traffic to the external network, and independent virtual private network servers were created for remote access. Finally, connectivity tests and event auditing were executed to validate the effectiveness of the established policies before final deployment. One limitation of this study was the inability to empirically validate the geographic blocking feature, due to the lack of access to foreign-origin IP addresses during the testing phase.

The results demonstrated a total concealment of internal servers and precise control of outbound traffic. Unauthorized access attempts via remote administration protocols were automatically mitigated and logged for subsequent auditing, while the private network connections functioned stably across various operating systems. It was concluded that the adopted solution resolved the initial vulnerabilities by reducing the attack surface, recommending for the future the integration of deep inspection systems and the centralization of logs

Keywords: *OPNsense, OpenVPN, firewall, VPN, cibersecurity.*

1. INTRODUCCIÓN

La seguridad de la información constituye uno de los pilares fundamentales en la operación de cualquier infraestructura tecnológica moderna. La protección de los sistemas que soportan servicios críticos dejó de ser opcional para convertirse en una prioridad. Las oficinas del centro de datos de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación (DGTIC) albergan la administración de servicios que requieren un esquema robusto de control de acceso, segmentación de red y conectividad remota segura.

La gestión unificada de amenazas, conocida por sus siglas en inglés como UTM (*Unified Threat Management*), surgió porque la diversidad de herramientas de seguridad tradicionales requería administrar de forma separada múltiples sistemas como *firewalls*, sistemas de detección de intrusos, segmentación de redes,

https://doi.org/10.22201/dgtic.30618096e.2026.4.3.190 Vol. 4, Núm. 3. julio-septiembre 2026, págs. 76 - 82

entre otras. Según la página de Zscaler (2024), los sistemas UTM integran estas capacidades en una sola plataforma de administración centralizada, simplificando la operación y reduciendo la superficie de ataque. En este mismo sentido, investigaciones recientes publicadas en el *International Journal of Research Publication and Reviews* (Purvant y Sowmya, 2024) señalaron que el análisis de tráfico y la automatización en los *firewalls* se están convirtiendo en herramientas de seguridad indispensables. Paralelamente, el trabajo de Majid (2025) demostró que herramientas como OPNsense son capaces de prevenir accesos no autorizados, registrar eventos de seguridad y bloquear ataques en entornos de red, confirmando su eficacia como plataforma de seguridad.

Ante la ausencia de un mecanismo centralizado para regular el tráfico saliente de las máquinas de administración del centro de datos de la DGTIC, se identificó la necesidad de implementar una solución que proporcionara salida controlada mediante direcciones IP privadas, así como acceso remoto cifrado para el personal técnico.

El objetivo del trabajo es implementar la herramienta OPNsense como solución de gestión unificada de amenazas (UTM) para regular el tráfico saliente de las máquinas de administración del centro de datos de la DGTIC, mediante el control de acceso basado en direcciones IP privadas y el establecimiento de un mecanismo de conectividad remota cifrada para el personal técnico.

2. DESARROLLO TÉCNICO

Selección de la solución

Previo a la implementación descrita en este documento, las máquinas de administración de servicios del centro de datos operaban con una asignación directa de direcciones IP públicas. Adicionalmente, no existía un mecanismo formal para que el personal técnico se conectara de forma cifrada desde ubicaciones remotas.

Ante esta situación, se evaluaron distintas alternativas. A pesar de que las soluciones comerciales, como FortiGate y Cisco ASA, ofrecen capacidades avanzadas de inspección de tráfico, sus costos elevados de licenciamiento pueden representar una limitación. Por tal motivo, pfSense constituyó una opción viable al ser una plataforma de código abierto.

Huda *et al.* (2023) realizaron una comparativa de calidad de servicio entre pfSense y OPNsense y concluyeron que ambas plataformas ofrecen un desempeño equiparable. OPNsense fue seleccionado gracias a que ofrece una interfaz web más moderna, ciclos de actualización de seguridad más frecuentes y complementos que pueden aumentar sus capacidades y alcance, como la integración con sistemas de detección de intrusiones como Suricata y soporte nativo para múltiples protocolos VPN. En investigaciones recientes, Tymoshchuk *et al.* (2024) confirmaron la eficiencia de OPNsense para entornos de producción y realizaron pruebas que demostraron su capacidad para detectar y prevenir accesos no autorizados, evidenciando su efectividad en aplicaciones reales de seguridad de redes.

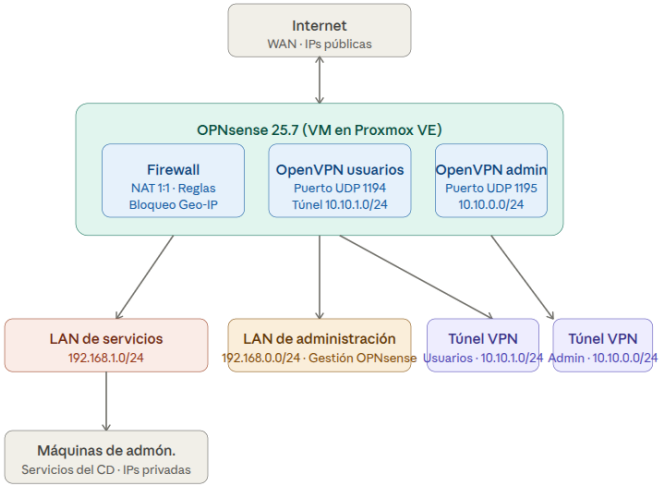
https://doi.org/10.22201/dgtic.30618096e.2026.4.3.190 Vol. 4, Núm. 3. julio-septiembre 2026, págs. 77 - 82

Arquitectura de red diseñada

La arquitectura implementada se fundamentó en la segmentación de red mediante el uso de OPNsense como punto centralizado de control del tráfico. Se definieron las siguientes interfaces lógicas dentro del sistema, representadas en el diagrama de la Figura 1.

Figura 1

Diagrama de la arquitectura de red implementada con OPNsense



WAN: Interfaz de cara a Internet, a través de la cual OPNsense recibe el tráfico externo y gestiona la salida de las máquinas internas hacia la red pública.

LAN de servicios: Red privada a la que se conectan las máquinas de administración del centro de datos. Las máquinas de esta red dejan de tener exposición directa en Internet y obtienen salida controlada a través de OPNsense.

LAN de administración: Segmento exclusivo para la gestión del propio OPNsense, separado lógicamente de la red de servicios para impedir que usuarios puedan acceder a la consola de administración del *firewall*.

Interfaces VPN: Interfaces virtuales creadas por OpenVPN para la conexión remota cifrada del personal técnico.

2.1 METODOLOGÍA

La implementación se llevó a cabo en cinco etapas: diseño, instalación, configuración, pruebas y puesta en producción.

Etapa 1 – Diseño

La etapa de diseño consistió en la definición de la arquitectura lógica de red que daría soporte a los servicios de *firewall* y VPN. A partir del análisis de los requerimientos de seguridad del centro de datos, se

https://doi.org/10.22201/dgtic.30618096e.2026.4.3.190 Vol. 4, Núm. 3. julio-septiembre 2026, págs. 78 - 82

elaboró un diagrama conceptual de red en el que se identificaron los segmentos de red necesarios, los flujos de tráfico permitidos y los filtros de seguridad entre ellos.

Se definió el esquema de direccionamiento IP privado como se muestra en la Tabla 1.

Tabla 1

Esquema de direccionamiento IP de la infraestructura implementada

Segmento	Red	Propósito
LAN de servicios	192.168.1.0/24	Máquinas de administración de servicios
LAN de administración	192.168.0.0/24	Gestión de OPNsense
Túnel VPN de usuarios	10.10.1.0/24	Acceso remoto cifrado para usuarios
Túnel VPN de administración	0.10.0.0/24	Acceso remoto cifrado para administradores
WAN	Direcciones IP públicas	Salida a Internet de los usuarios

La separación de los segmentos de red cubre la necesidad de mantener aislados entre sí a los usuarios de la administración para limitar el impacto de un eventual incidente de seguridad. Asimismo, la definición de dos instancias VPN independientes —una para usuarios y otra para administradores— siguió la premisa de que cada usuario debe tener acceso únicamente a los recursos estrictamente necesarios para el cumplimiento de sus funciones.

Etapa 2 – Instalación

Se creó una máquina virtual en Proxmox VE con los recursos necesarios para ejecutar OPNsense, asignando interfaces de red virtuales correspondientes a los segmentos WAN y LAN. Se descargó la imagen ISO oficial de OPNsense y se procedió a la instalación del sistema. Una vez completada, se accedió a la interfaz web de administración para iniciar la configuración del sistema.

Etapa 3 – Configuración

En esta etapa, se configuraron las principales funcionalidades que se requerían del sistema.

- *Configuración de NAT 1 a 1.* Se implementó traducción de direcciones de red uno a uno (*one-to-one NAT*) para que cada máquina mantuviera su dirección IP pública al salir hacia Internet, conservando los accesos asociados a su dirección IP, pero eliminando la exposición directa de los equipos Internet.
- *Reglas de firewall y bloqueo regional.* Se definieron reglas de filtrado para separar el tráfico de la LAN de servicios respecto de la LAN de administración, impidiendo que, desde la red de servicios, se pudiera acceder a la interfaz de gestión de OPNsense. Adicionalmente, se configuró el bloqueo regional de IPs utilizando las listas de geolocalización MaxMind GeoLite2 disponibles para OPNsense, de modo que todo el tráfico entrante proveniente de rangos de direcciones IP fuera del territorio mexicano se descartara en la interfaz WAN. El bloqueo geográfico constituye una de las múltiples herramientas de una estrategia de ciberseguridad integral cuando opera como parte de las reglas del *firewall*, brindando una mayor protección (Miller, 2025).
- *Configuración de OpenVPN.* Se desplegó un servidor OpenVPN dentro de OPNsense para proveer acceso remoto cifrado al personal del centro de datos. Se generó una infraestructura de llave pública dentro de OPNsense para emitir certificados de servidor y de cliente, garantizando que únicamente

https://doi.org/10.22201/dgtic.30618096e.2026.4.3.190 Vol. 4, Núm. 3. julio-septiembre 2026, págs. 79 - 82

usuarios autenticados mediante un certificado válido y contraseña pudieran establecer una conexión.

Etapa 4 – Pruebas

Las pruebas funcionales se diseñaron para validar cada uno de los componentes configurados. Éstas se describen con detalle en la sección de Resultados.

3. RESULTADOS

La implementación de OPNsense como plataforma de seguridad unificada en el centro de datos produjo resultados satisfactorios en todos los puntos dentro del alcance del proyecto. A continuación, se presentan los resultados y su respectivo análisis.

Segmentación de red y ocultamiento de equipos

Una vez desplegada la arquitectura de red, se migraron todas las máquinas de administración de servicios a un esquema de direccionamiento con direcciones IP privadas. Como resultado, ninguno de los equipos quedó "visible" desde Internet, dado que sus direcciones privadas no son enrutables. Esto resolvió el problema de tener expuestos los equipos a actores externos.

NAT uno a uno y salida controlada a Internet

Se verificó desde cada equipo, mediante una consulta a la página web *ifconfig.me*, que cada uno salía a Internet con su dirección IP pública correspondiente. Esto validó que la traducción de direcciones operaba correctamente.

La consola de OPNsense proporcionó visibilidad en tiempo real del tráfico que atravesaba el *firewall*, permitiendo identificar los flujos activos y los eventos de seguridad registrados. Esta capacidad de observabilidad representó una gran mejora de seguridad.

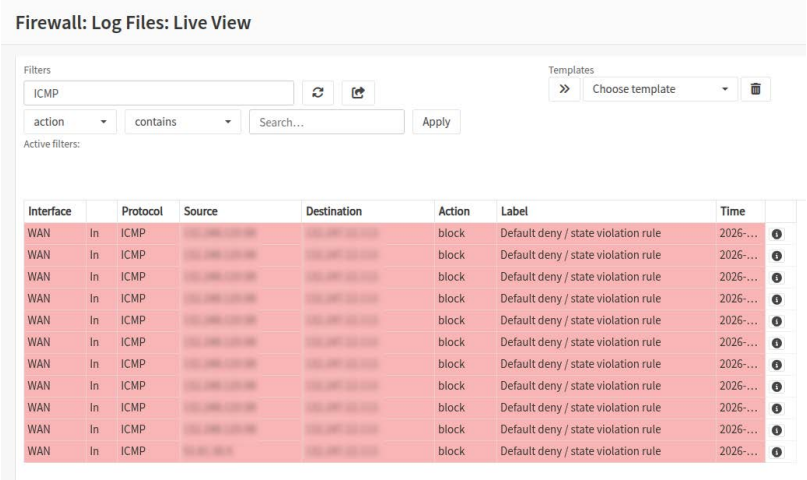
Reglas de *firewall* y bloqueo de accesos externos

Los *gateways* de los segmentos de red configurados dejaron de responder a solicitudes ICMP. Como se puede ver en la Figura 2, se confirmó que las reglas de filtrado aplicadas sobre las interfaces correspondientes operaron conforme a lo diseñado.

https://doi.org/10.22201/dgtic.30618096e.2026.4.3.190 Vol. 4, Núm. 3. julio-septiembre 2026, págs. 80 - 82

Figura 2

Verificación de que las solicitudes ICMP son bloqueadas y registradas en los logs



Los intentos de conexión SSH realizados desde direcciones IP externas fueron bloqueados y registrados automáticamente en el log del *firewall*, lo que demostró tanto la efectividad del filtrado de tráfico entrante como la capacidad de auditoría de la plataforma. Este comportamiento es consistente con lo reportado por Majid (2025), quien documentó que OPNsense es capaz de detectar, registrar y bloquear accesos no autorizados en entornos de red reales.

El aislamiento entre la LAN de usuarios y la LAN de administración fue verificado mediante intentos de acceso a la consola web de OPNsense desde equipos en la red de usuarios. En todos los casos, los intentos de conexión fueron bloqueados y reportados en el *firewall*.

Respecto al bloqueo geográfico mediante las listas MaxMind GeoLite2, no fue posible realizar pruebas funcionales directas porque no se cuenta con acceso a direcciones IP de origen extranjero durante el período de validación; no obstante, se verificó que los alias fueron creados correctamente en OPNsense y que las reglas asociadas se encontraban activas en la interfaz WAN.

Conectividad VPN y acceso remoto cifrado

Ambas instancias de OpenVPN funcionaron correctamente en plataformas Linux y Windows. El sistema exigió la contraseña de usuario para completar el proceso de autenticación. Cada intento de conexión, tanto exitoso como fallido, quedó registrado en el log de la VPN, lo que garantiza la visibilidad de todos los intentos de acceso a la misma.

Análisis de resultados

Los resultados obtenidos demuestran que OPNsense resolvió la situación planteada inicialmente. Las máquinas de administración de sistemas dejaron de estar expuestas directamente a Internet, el tráfico saliente quedó centralizado y controlado, los accesos no autorizados fueron bloqueados y registrados, así como el personal técnico dispuso de un mecanismo de acceso remoto cifrado y autenticado.

https://doi.org/10.22201/dgtic.30618096e.2026.4.3.190 Vol. 4, Núm. 3. julio-septiembre 2026, págs. 81 - 82

La capacidad de observabilidad aportada por el *firewall* constituye una mejora significativa, ya que permite a los administradores detectar actividad sospechosa, auditar accesos y fundamentar decisiones de ajuste de políticas de seguridad con base en evidencia.

Implementaciones a futuro

En una etapa futura, se buscará incorporar un sistema de detección y prevención de intrusiones (IDS/IPS) mediante Suricata, complemento nativo de OPNsense, para añadir una capa de inspección profunda de paquetes que permita identificar patrones de ataque más sofisticados que los contemplados por el *firewall* con reglas estáticas. Veerasingam *et al*. (2023) demostraron la viabilidad de Suricata como sistema de detección y prevención de intrusiones incluso en entornos con recursos limitados, confirmando que su integración con plataformas de *firewall* existentes añade una capa de inspección profunda de tráfico que amplía significativamente las capacidades de detección frente a amenazas más sofisticadas que las cubiertas por reglas estáticas.

4. CONCLUSIONES

El centro de datos presentaba un esquema de red en el que las máquinas de administración de servicios operaban con direcciones IP públicas. Esta condición representaba una superficie de ataque mayor, situación por la que se decidió implementar OPNsense como plataforma de seguridad unificada.

La implementación de OPNsense brinda servicios integrados de *firewall* y VPN que resolvieron los planteamientos originales, el ocultamiento de las máquinas de administración respecto a Internet mediante el uso de direcciones IP privadas y NAT uno a uno, el control y filtrado del tráfico entrante y saliente mediante reglas basadas en el principio de mínimo privilegio, y el acceso remoto cifrado y autenticado para el personal técnico a través de dos instancias independientes de OpenVPN. Los intentos de conexión SSH no autorizados desde el exterior fueron bloqueados y registrados, el aislamiento entre los segmentos de red de usuarios y de administración se verificó correctamente, y ambas instancias VPN operaron de forma estable en plataformas Linux y Windows.

El único componente que no pudo validarse empíricamente fue el bloqueo geográfico mediante listas MaxMind GeoLite2. Su configuración fue completada, pero la prueba funcional quedó pendiente debido a que no se contó con direcciones IP extranjeras.

Para etapas posteriores se considera la implementación de un sistema centralizado de gestión de *logs* que consolide los registros del *firewall* y de las instancias VPN en una plataforma de análisis externa. Esto facilitaría la detección de patrones anómalos y la respuesta ante incidentes de seguridad a medida que la infraestructura del centro de datos crezca.

REFERENCIAS

Huda, A. S., Prihantoro, C., y Pranata, M. (2023). *Analisis perbandingan QoS pfSense dan OPNsense menggunakan metode load balancing* [Comparative analysis of QoS in pfSense and OPNsense using the load balancing method]. *Media Informatika, 22*(2), 87–95. https://doi.org/10.37595/mediainfo.v22i2.196

https://doi.org/10.22201/dgtic.30618096e.2026.4.3.190 **Vol. 4, Núm. 3.** julio-septiembre 2026, págs. 82 - 82

Majid, J. (2025). Building a firewall and intrusion detection system based network security system using OPNsense tools. *Iraqi Journal of Intelligent Computing and Informatics (IJICI)*, *4*(1), 66–76. https://doi.org/10.52940/ijici.v4i1.96

Miller, J. (2025). *Enhancing network security: Can geo-blocking be the answer?* BitLyft. https://www.bitlyft.com/resources/enhancing-network-security-can-geo-blocking-be-the-answer

Purvant, S., y Sowmya, K. S. (2024). Advancements in network security. *International Journal of Research Publication and Reviews*, *5*(1), 5122–5126. https://ijrpr.com/uploads/V5ISSUE1/IJRPR22156.pdf

Tymoshchuk, V., Pakhoda, V., Dolinskyi, A., y Karnaukhov, A. (2024). Modelling cyber threats and evaluating the performance of intrusion detection systems. *Grail of Science*, (46), 638–646. https://doi.org/10.36074/grail-of-science.29.11.2024.081

Veerasingam, P., Abd Razak, S., Abidin, A. F. A., Mohamed, M. A., y Mohd Satar, S. D. (2023). Intrusion detection and prevention system in SME's local network by using Suricata. *Malaysian Journal of Computing and Applied Mathematics*, *6*(1), 21–30. https://doi.org/10.37231/myjcam.2023.6.1.88

Zscaler. (2024). *What is unified threat management?* https://www.zscaler.com/zpedia/what-unified-threat-management