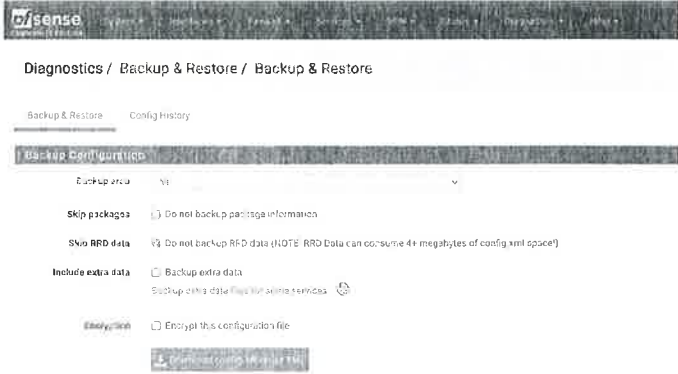


# Ficha de mantenimiento técnico

## pfSense SSPM

Sophie UNAM

Tarea	Actualización pfSense a 2.5.0-release en un nuevo hardware.
Detalles de la tarea	Objetivo: Actualizar el sistema de seguridad pfSense a la última versión estable en hardware nuevo. Versión pfSense: 2.5.0. Medio de instalación: USB. Arquitectura o Firmware: amd64. Servicios relacionados: Firewall y sistema de detección y prevención de intrusiones, Snort.
Servicios críticos	<ul style="list-style-type: none"><li>Firewall perimetral</li><li>Sistema de prevención y detección de intrusiones</li><li>Publicaciones web de la SSPM</li></ul>
Descripción	Dentro del convenio SSPM - UNAM, se programó la actualización del sistema de seguridad pfSense a la última versión estable, 2.5.0.
Impacto	Todas las conexiones hacia, y desde, Internet se interrumpieron durante la actualización.
Evidencia	<p>Se siguió el procedimiento estándar para actualizar el sistema:</p> <ol style="list-style-type: none"><li>En el sistema de producción, se descargó un respaldo completo de la configuración del pfSense en Diagnósticos &gt; Respaldos: <p>The screenshot shows the pfSense web interface for the 'Backup &amp; Restore' section. It includes options for 'Skip packages', 'Skip RRD data', 'Include extra data', and 'Encryption'. The 'Backup &amp; Restore' breadcrumb is visible at the top.</p></li><li>Se descargó una imagen de pfSense 2.5.0: <a href="https://www.pfsense.org/download/">https://www.pfsense.org/download/</a></li></ol>

3. Se instaló el sistema en el nuevo hardware.

**System Information**   

<b>Name</b>	pfSense.sspmqro.gob.mx
<b>User</b>	uma@132.248.185.74 (Local Database)
<b>System</b>	pfSense Netgate Device ID: <b>3d2ff136407ea79b003d</b>
<b>BIOS</b>	Vendor: Dell Inc. Version: 2.7.7 Release Date: <b>Wed May 6 2020</b>
<b>Version</b>	<b>2.5.0-RELEASE (amd64)</b> built on Tue Feb 16 08:56:29 EST 2021 FreeBSD 12.2-STABLE
	<small>The output is on <a href="#">pfSense Wiki</a>.</small> Version information updated at Mon Mar 29 9:05:11 CST 2021 
<b>CPU Type</b>	Intel(R) Xeon(R) Silver 4210 CPU @ 2.20GHz 40 CPUs; 2 package(s) x 10 core(s) x 2 hardware threads AES-NI CPU Crypto: Yes (inactive)

4. Se procedió a restaurar la configuración del servidor de producción en el nuevo hardware en, Diagnósticos > Respaldos:

**Restore Backup**

Open a pfSense configuration XML file and click the button below to restore the configuration.

Restore area: All 

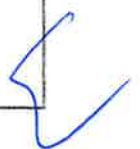
Configuration file:  config-pfSen..2192028.xml

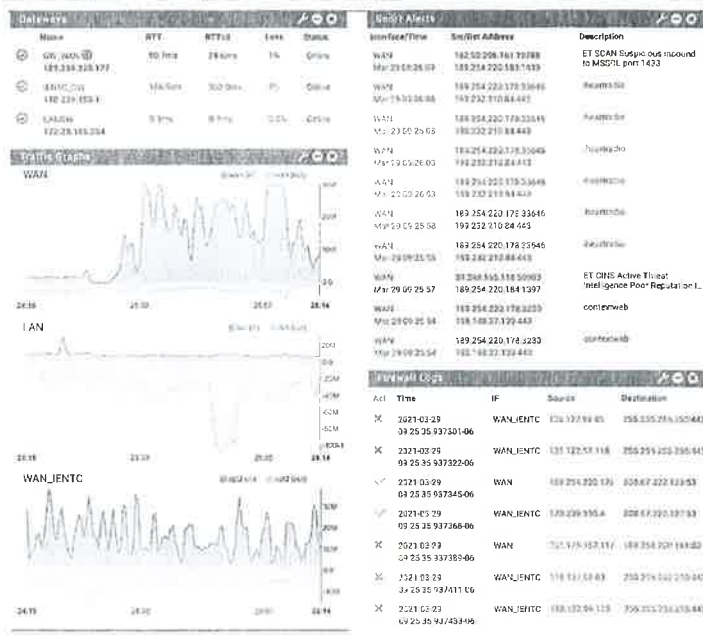

Encryption:  Configuration file is encrypted.

The firewall will reboot after restoring the configuration.

5. Se transfirieron las conexiones físicas al nuevo hardware.

6. Se evaluó la conectividad y funcionalidad del pfSense.



	 <p>The screenshot displays network monitoring data. On the left, a 'Gateways' table shows three WAN interfaces: WAN0 (191.224.220.177), WAN1 (191.224.220.178), and WAN2 (191.224.220.179). The WAN0 interface is marked as 'Online' with 80% RTT, 28% loss, and 1% CPU. Below this are three line graphs: 'WAN' showing traffic volume, 'LAN' showing local network activity, and 'WAN_JENTC' showing WAN traffic volume. On the right, a 'Security Alerts' table lists various alerts such as 'ET SCAN Suspicious inbound to MSSQL port 1433', 'Reassembly', 'Denial of Service', and 'ET DNS Active Threat Intelligence Poor Reputation L'. At the bottom right, a table shows 'Intranet Logs' with columns for Action, Time, IP, Source, and Destination.</p>
Observaciones	<ul style="list-style-type: none"> <li>• Dado el impacto en la conectividad y la necesidad de conectar un nuevo hardware, este mantenimiento se llevó a cabo en sitio. Con personal de la SSPM y de la UNAM.</li> </ul>
Referencias	<ul style="list-style-type: none"> <li>• <a href="https://docs.netgate.com/pfsense/en/latest/install/upgrade-guide-versions.html">https://docs.netgate.com/pfsense/en/latest/install/upgrade-guide-versions.html</a></li> </ul>
Firma responsable	 <p>Ulises M Alvarez. Sophie UNAM.</p>

*[Handwritten signature]*