


Ficha de mantenimiento técnico

pfSense SSPM

Sophie UNAM

Tarea	Actualización de la unidad de gestión de amenazas centralizada, pfSense
Detalles de la actualización	<p>Versión a instalar: 2.4.5.1-RELEASE Versión anterior: 2.5.0-RELEASE Medio de instalación: Descarga vía Internet. Arquitectura o Firmware: amd64 Servicios relacionados: firewall perimetral, sistema de prevención y detección de intrusiones, DNS, sistema de análisis de tráfico de red.</p>
Servicios críticos	<ul style="list-style-type: none"> • Salida a Internet para la SSPM. • Servicios web públicos de la SSPM. • Sistema de resolución de nombres, DNS, para la LAN SSPM. • Sistema de filtrado de contenidos para la LAN SSPM. • Firewall perimetral. • Sistema de detección y prevención de intrusiones.
Descripción	Dentro del convenio SSPM - UNAM, se actualizó el sistema operativo de la unidad de gestión de amenazas centralizadas, pfSense, de la SSPM a la última versión estable.
Impacto	La actualización resulta en una interrupción de todos los servicios críticos.
Evidencia	<p>1. Menú actualización.</p>  <p>The screenshot shows the pfSense dashboard with the following details:</p> <ul style="list-style-type: none"> Status / Dashboard System Information: <ul style="list-style-type: none"> Name: pfsense.drivemeca.com System: pfSense Netgate Device ID: af806684440989b61c23 BIOS: Vendor: SeeBIOS Version: rel-1.11.0-0-g63451fca13-prebuilt.qemu-project.org Release Date: Tue Apr 1 2014 Version: 2.4.3-RELEASE (amd64) built on Mon Mar 26 18:02:04 CDT 2018 FreeBSD 11.1-RELEASE p7 Version 2.4.3.1 is available. Version information updated on Tue Sep 11 11:53:40 CDT 2018 Interfaces: <ul style="list-style-type: none"> WAN: 1000baseT <full-duplex> 192 LAN: 1000baseT <full duplex> 192

2. Descarga de actualizaciones.

System / Update / System Update

Please wait while the system update completes
This may take several minutes. Do not leave or refresh the page!

System Update Update Settings

Updating System

```
sqlite3: 3.21.0 1 -> 3.22.0 1 [pfSense]
pfSense-rc: 2.4.3 -> 2.4.3 1 [pfSense-core]
pfSense-kernel-pfSense: 2.4.3 -> 2.4.3 1 [pfSense-core]
pfSense-default-config: 2.4.3 -> 2.4.3 1 [pfSense-core]
pfSense-base: 2.4.3 -> 2.4.3 1 [pfSense-core]
pfSense: 2.4.3 -> 2.4.3 1 [pfSense]
perl5: 5.24.3 -> 5.24.4 [pfSense]
libnghttp2: 1.29.0 -> 1.31.1 [pfSense]
```

Number of packages to be upgraded: 0

```
67 MiB to be downloaded
[1/8] Fetching sqlite3-3.22.0-1.txz: ..... done
[2/8] Fetching pfSense-rc-2.4.3-1.txz: .. done
```

3. Actualización terminada.

System / Update / System Update

System update successfully completed.

System Update Update Settings

Rebooting
Page will automatically reload in 76 seconds

Updating System

```
>>> Upgrading pfSense kernel...
Checking integrity... done (0 conflicting)
The following 1 package(s) will be affected (of 0 checked):

Installed packages to be UPGRADED:
  pfSense kernel pfSense: 2.4.3 > 2.4.3 1 [pfSense-core]

Number of packages to be upgraded: 1
[1/1] Upgrading pfSense-kernel-pfSense from 2.4.3 to 2.4.3 1...
[1/1] Extracting pfSense-kernel-pfSense-2.4.3-1: ..... done
==> Keeping a copy of current kernel in /boot/kernel.old
>>> Removing unnecessary packages... done
Upgrade is complete. Rebooting in 10 seconds.
Success
```

4. Reinicio con la nueva versión del sistema operativo.


Observaciones

- En atención a las recomendaciones de las autoridades sanitarias, este mantenimiento se llevó a cabo en modalidad de conexión remota, con personal de la SSPM en sitio.

Referencias

<https://www.netgate.com/blog/pfsense-2-4-5-release-now-available.html>

Firma responsable


Ulises M Alvarez.
Sophie UNAM.

Ficha de mantenimiento técnico

pfSense SSPM

Sophie UNAM

Tarea	Actualización SecurityOnion a 2.3.40.
Detalles de la tarea	Objetivo: Actualizar el sistema monitoreo de seguridad en red SecurityOnion a la última versión estable. Versión SecurityOnion: 2.3.40. Medio de instalación: Internet. Arquitectura o Firmware: amd64. Servicios relacionados: Monitor de eventos de seguridad de red.
Servicios críticos	<ul style="list-style-type: none"> Monitor de eventos de seguridad de red.
Descripción	Dentro del convenio SSPM - UNAM, se programó la actualización del sistema de monitoreo de eventos de seguridad SecurityOnion a la última versión estable, 2.3.40.
Impacto	Durante la descarga de actualizaciones se interrumpió la captura de paquetes de red.
Evidencia	<p>Se siguió el procedimiento estándar para actualizar el sistema:</p> <ol style="list-style-type: none"> En la consola, se ejecutó: sudo soup <pre> ##### ##### ### UNAUTHORIZED ACCESS PROHIBITED ### ### ### ##### ##### uma@132.248.185.246's password: Last failed login: Mon Mar 29 16:26:54 UTC 2021 from nodo50.geociencias.unam.mx on ssh:not There was 1 failed login attempt since the last successful login. Last login: Mon Mar 29 16:16:23 2021 from nodo50.geociencias.unam.mx Access the Security Onion web interface at https://132.248.185.246 (You may need to run so-allow first if you haven't yet) [uma@monitor ~]\$ sudo soup █ </pre>

2. En la consola, se actualizó el sistema operativo: sudo yum update, y se volvió a ejecutar: sudo soup

```
[user@monitor ~]$ sudo yum update
[sudo] password for user:
Failed to set locale, defaulting to C
Loaded plugins: fastestmirror, versionlock
Loading mirror speeds from cached hostfile
 * base: mirrors.unifiedlayer.com
 * epel: o212k17pfbg9m.cloudfront.net
 * extras: mirrors.centos.las1.serverforge.org
 * updates: repos.forthought.net
Excluding A updates due to versionlock (use "yum versionlock status" to show them)
No packages marked for updates
[user@monitor ~]$ sudo soup

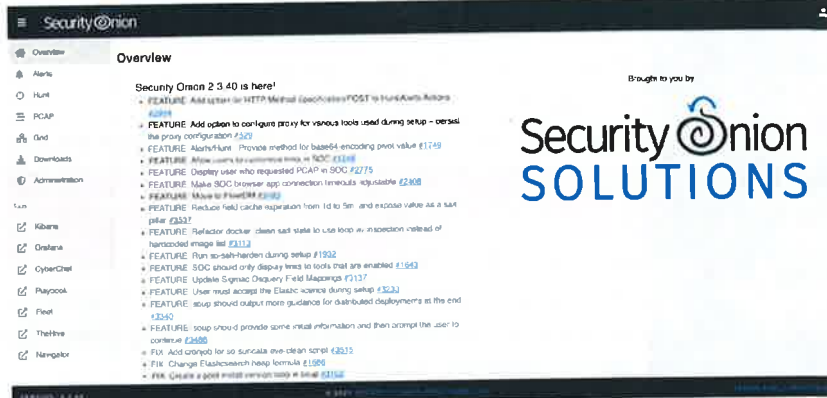
SOUP - Security Onion Updater

Please review the following for more information about the update process and recent updates:
https://docs.securityonion.net/soup
https://blog.securityonion.net

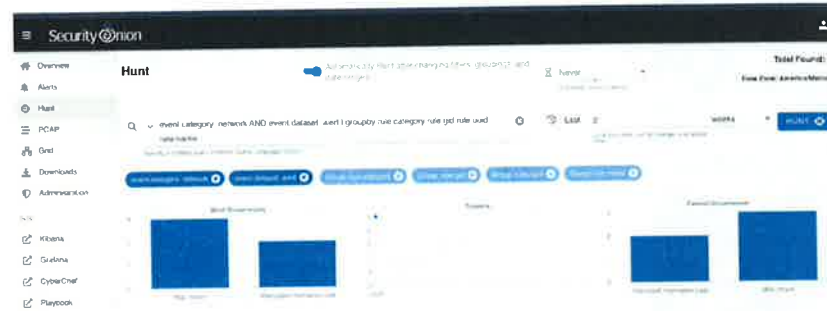
Please note that soup only updates Security Onion components and does NOT update the underlying operating system (OS). When you installed Security Onion, there was an option to automatically update the OS packages. If you did not enable this option, then you will want to ensure that the OS is fully updated before running soup.

Press Enter to continue or Ctrl-C to cancel.
```

3. Se comprobó actualización.



4. Se comprobó funcionalidad.



Una vez finalizadas las pruebas, se declaró la actualización como exitosa.

Observaciones

- Este mantenimiento se llevó a cabo en el sitio. Con personal de la SSPM y de la UNAM.

Referencias

- <https://docs.securityonion.net/en/2.3/updating.html>

Firma
responsable



Ulises M Alvarez.
Sophie UNAM.

