

Guía de actualización de PAN-OS

11.0

Contact Information

Corporate Headquarters:

Palo Alto Networks

3000 Tannery Way

Santa Clara, CA 95054

www.paloaltonetworks.com/company/contact-support

About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Palo Alto Networks, Inc.

www.paloaltonetworks.com

© 2022-2023 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

Last Revised

March 29, 2023

Table of Contents

Actualizaciones de software y contenido.....	7
Actualizaciones del software PAN-OS.....	8
Actualizaciones dinámicas de contenido.....	9
Instalación de actualizaciones de contenido.....	12
Actualización de contenido de aplicaciones y amenazas.....	15
Implementación de actualizaciones de contenido de aplicaciones y amenazas.....	16
Sugerencias para las actualizaciones de contenido.....	17
Prácticas recomendadas para las actualizaciones de contenido de aplicaciones y amenazas.....	19
Prácticas recomendadas para las actualizaciones de contenido: nivel crítico.....	19
Prácticas recomendadas para las actualizaciones de contenido: prioridad de seguridad.....	23
Infraestructura de red de entrega de contenido.....	27
 Cambio de Panorama a una versión posterior.....	 31
Instalación de actualizaciones de contenido y software para Panorama.....	32
Actualización de Panorama con una conexión a Internet.....	32
Cambio de la versión de Panorama sin una conexión a Internet a una versión posterior.....	39
Instalación automática de actualizaciones de contenido para Panorama sin conexión a Internet.....	46
Actualización de Panorama en una configuración de HA.....	51
Migración de los logs de Panorama al nuevo formato de log.....	54
Actualización de Panorama para aumentar la capacidad de gestión de dispositivos.....	55
Actualice Panorama y dispositivos gestionados en modo FIPS-CC.....	56
Cambio a versiones anteriores a Panorama 11.0.....	58
Solución de problemas del cambio a versiones posteriores de Panorama.....	62
Implementación de actualizaciones de cortafuegos, recopiladores de logs y dispositivos WildFire utilizando Panorama.....	63
¿Qué actualizaciones puede enviar Panorama a otros dispositivos?.....	64
Programación de una actualización de contenido mediante Panorama.....	64
Compatibilidad de versiones de Panorama, el recopilador de logs, el cortafuegos y WildFire.....	66
Actualización de recopiladores de logs cuando Panorama está conectado a internet.....	66
Actualización de recopiladores de logs cuando Panorama no está conectado a internet.....	70
Cambio de un clúster de WildFire a una versión posterior desde Panorama con conexión a Internet.....	75

Cambio de un clúster de WildFire a una versión posterior desde Panorama sin conexión a Internet.....	77
Actualización de los cortafuegos cuando Panorama está conectado a internet.....	80
Actualización de los cortafuegos cuando Panorama no está conectado a internet.....	89
Actualización de un cortafuegos de ZTP.....	96
Restablecimiento de las actualizaciones de contenido de Panorama.....	98
Cambio de PAN-OS a una versión posterior.....	101
Lista de control para actualizar PAN-OS.....	102
Consideraciones sobre el cambio a versiones anteriores/posteriores de complementos de Panorama.....	104
Cambio del cortafuegos a la versión posterior PAN-OS 11.0.....	111
Determine la ruta de actualización a PAN-OS 11.0.....	111
Cambio de un cortafuegos independiente a una versión posterior.....	115
Cambio de un par de cortafuegos de HA a una versión posterior.....	119
Actualización del cortafuegos a PAN-OS 11.0 desde Panorama.....	126
Actualización de los cortafuegos cuando Panorama está conectado a internet.....	126
Actualización de los cortafuegos cuando Panorama no está conectado a internet.....	134
Actualización de un cortafuegos de ZTP.....	141
Cambio a una versión anterior de PAN-OS.....	144
Cambio de un cortafuegos a una versión de mantenimiento anterior.....	144
Cambio de un cortafuegos a una versión de funciones anterior.....	145
Cambio de un agente de Windows a una versión anterior.....	146
Solución de problemas del cambio a versiones posteriores de PAN-OS.....	148
Actualización del cortafuegos VM-Series.....	151
Cambio del software PAN-OS VM-Series a una versión posterior (independiente).....	152
Cambio del software PAN-OS VM-Series a una versión posterior (par de HA).....	155
Cambio del software PAN-OS de VM-Series a una versión posterior mediante Panorama.....	161
Actualización de la versión de software de PAN-OS (VM-Series para NSX).....	166
Actualización de la serie VM para NSX durante una ventana de mantenimiento.....	167
Actualización de VM-Series para NSX sin interrumpir el tráfico.....	169
Actualización del modelo VM-Series.....	172
Actualización del modelo VM-Series en un par de HA.....	174
Cambio a versión posterior del cortafuegos VM-Series.....	176
Cambio complementos de Panorama a versiones posteriores.....	177
Consideraciones sobre el cambio a versiones anteriores/posteriores de complementos de Panorama.....	178

Actualice el complemento de DLP empresarial.....	181
Actualización del complemento Panorama Interconnect.....	182
Actualización del complemento de SD-WAN.....	184
Comandos de la CLI para realizar la actualización.....	185
Utilizar los comandos de la CLI para las tareas de cambio a versión posterior.....	186
API para realizar la actualización.....	191
Usar la API para tareas de actualización.....	192

Actualizaciones de software y contenido

PAN-OS es el software que ejecuta todos los cortafuegos de nueva generación de Palo Alto Networks. Además, Palo Alto Networks publica a menudo actualizaciones para dotar los cortafuegos de las últimas funciones de seguridad. Los cortafuegos pueden aplicar políticas basadas en las firmas de aplicaciones, amenazas, etc. que aportan las actualizaciones de contenido, sin que el usuario deba actualizar su configuración.

Después de descargar e instalar correctamente una actualización de software PAN-OS en el cortafuegos físico, la actualización de software se valida después de que el cortafuegos físico se reinicie como parte del proceso de instalación del software para garantizar la integridad del software PAN-OS. Esto garantiza que la nueva actualización de software en ejecución sea buena y que el cortafuegos no se vea comprometido debido a la explotación remota o física.

- > [Actualizaciones del software PAN-OS](#)
- > [Actualizaciones dinámicas de contenido](#)
- > [Instalación de actualizaciones de contenido](#)
- > [Actualización de contenido de aplicaciones y amenazas](#)
- > [Prácticas recomendadas para las actualizaciones de contenido de aplicaciones y amenazas](#)
- > [Infraestructura de red de entrega de contenido](#)

Actualizaciones del software PAN-OS

PAN-OS es el software que ejecuta todos los cortafuegos de nueva generación de Palo Alto Networks. La versión del software PAN-OS que ejecuta el cortafuegos se muestra en su pantalla **Dashboard (Panel)**.

Puede buscar las nuevas versiones de PAN-OS directamente en el cortafuegos o bien en el [portal de atención al cliente de Palo Alto Networks](#). Para actualizar el cortafuegos a la última versión de PAN-OS:

STEP 1 | Compruebe las novedades disponibles en las [notas de la versión de PAN-OS](#) más recientes. También consulte [Consideraciones sobre el cambio a versiones anteriores/posteriores de complementos de Panorama](#) para asegurarse de comprender todos los cambios posibles que podría incorporar la versión de PAN-OS.

STEP 2 | Compruebe si hay versiones de PAN-OS nuevas:

- **En el portal de atención al cliente** (support.paloaltonetworks.com), seleccione **Updates (Actualizaciones) > Software Updates (Actualizaciones de software)** en la barra de menús de la izquierda. Descargue y guarde la versión que desee usar para actualizar el cortafuegos.
- **En el cortafuegos**, seleccione **Device (Dispositivo) > Software** y haga clic en **Check Now (Buscar ahora)** para que busque versiones nuevas de PAN-OS en el servidor de actualizaciones de Palo Alto Networks.




¿Tiene dificultades para buscar actualizaciones de software? Consulte [este artículo](#) para obtener soluciones a algunos de los problemas comunes de conectividad.


STEP 3 | Una vez que haya decidido la versión de publicación que desea, siga el flujo de trabajo completo para [Cambio del cortafuegos a la versión posterior PAN-OS 11.0](#). Los pasos a seguir dependen de la versión que ejecute, de si tiene una implementación de alta disponibilidad (high availability, HA) y de si utiliza Panorama para gestionar los cortafuegos.

Actualizaciones dinámicas de contenido

Palo Alto Networks publica a menudo actualizaciones que el cortafuegos utiliza para aplicar políticas de seguridad sin que sea preciso actualizar el software PAN-OS ni modificar la configuración del cortafuegos. Estas actualizaciones permiten dotar los cortafuegos de la inteligencia contra amenazas y las funciones de seguridad más recientes.

Aparte de las actualizaciones de aplicaciones y algunas actualizaciones de antivirus, que reciben todos los cortafuegos, las actualizaciones de contenido dinámicas que tiene a su disposición pueden depender de sus [suscripciones](#). En **Device (Dispositivo) > Dynamic Updates (Actualizaciones dinámicas)**, puede configurar una programación para cada una de las actualizaciones dinámicas de contenido si quiere definir la frecuencia con la que el cortafuegos busca, descarga o instala actualizaciones nuevas.

Actualización dinámica de contenido	Contenido del paquete
Antivirus	<p>Las actualizaciones de antivirus se publican cada 24 horas e incluyen:</p> <ul style="list-style-type: none"> firmas WildFire para malware recién descubierto. Para obtener estas actualizaciones cada cinco minutos en lugar de una vez al día, debe tener una suscripción a WildFire. (Threat Prevention obligatorio) Firmas de comando y control (command-and-control, C2) generadas automáticamente para detectar ciertos patrones en el tráfico de C2. Estas firmas permiten que el cortafuegos detecte la actividad de C2 incluso cuando el host de C2 es desconocido o cambia con rapidez. (Threat Prevention obligatorio) Entradas nuevas y actualizadas de las listas dinámicas externas integradas. Estas listas incluyen direcciones IP malintencionadas, blindadas y de alto riesgo proporcionadas por hosts malintencionados, contra los que ofrecen protección. (Threat Prevention obligatorio) Actualizaciones del conjunto local de firmas de DNS que usa el cortafuegos para identificar los dominios malintencionados conocidos. Si configura el sinkholing de DNS, el cortafuegos puede identificar los hosts de su red que intentan conectarse a esos dominios. Si desea que el cortafuegos verifique los dominios con toda la base de datos de firmas de DNS, configure la seguridad de DNS.
applications	<p>Las actualizaciones de aplicaciones proporcionan firmas de aplicaciones o App-ID nuevos y modificados. Esta actualización no requiere suscripciones adicionales, pero sí un contrato de asistencia/mantenimiento en vigor. Las nuevas actualizaciones de la aplicación se publican solo el tercer martes de cada mes, para que tenga tiempo de preparar las actualizaciones de políticas necesarias con anticipación.</p> <p> <i>En casos excepcionales, la publicación de la actualización que contiene ID de aplicación nuevos puede demorarse uno o dos días.</i></p>

Actualización dinámica de contenido	Contenido del paquete
	<p>Las modificaciones de los ID de aplicaciones se publican con mayor frecuencia. Los App-ID nuevos y modificados permiten al cortafuegos aplicar la política de seguridad con una precisión cada vez mayor, lo que provoca cambios en la aplicación de dicha política que pueden afectar a la disponibilidad de las aplicaciones. Para aprovechar al máximo las actualizaciones de la aplicación, siga nuestros consejos para administrar ID de aplicaciones nuevos y modificados.</p>
Aplicaciones y amenazas	<p>Incluye firmas de aplicaciones y contra amenazas nuevas y actualizadas. Esta actualización está disponible si cuenta con una suscripción a Threat Prevention (en este caso, sustituye la actualización de aplicaciones). Las actualizaciones de amenazas nuevas se publican a menudo (en ocasiones, varias veces a la semana), junto con los App-ID actualizados. Los nuevos ID de aplicación se publican solo el tercer martes de cada mes.</p> <p> <i>En casos excepcionales, la publicación de la actualización que contiene ID de aplicación nuevos puede demorarse uno o dos días.</i></p> <p>El cortafuegos puede recuperar las últimas actualizaciones de amenazas y aplicaciones en tan solo 30 minutos de disponibilidad.</p> <p>Si desea saber cómo habilitar las actualizaciones de aplicaciones y amenazas del modo óptimo para garantizar la disponibilidad de las aplicaciones y su protección frente a las últimas amenazas, consulte Prácticas recomendadas para las actualizaciones de contenido de aplicaciones y amenazas.</p>
Diccionario de dispositivo	<p>El diccionario de dispositivos es un archivo XML para que los cortafuegos lo usen en las reglas de la política de seguridad basadas en ID de dispositivo. Contiene entradas para varios atributos del dispositivo y se actualiza completamente con frecuencia y se publica como un nuevo archivo en el servidor de actualización. Si hay algún cambio en una entrada del diccionario, se publicará un archivo revisado en el servidor de actualización para que Panorama y los cortafuegos lo descarguen e instalen automáticamente la próxima vez que comprueben el servidor de actualización, lo que hacen automáticamente cada dos horas.</p>
GlobalProtect Data File (Archivo de datos de GlobalProtect)	<p>Contiene información específica del proveedor para definir y evaluar los datos de perfiles de información de hosts (host information profile, HIP) que proporcionan las aplicaciones de GlobalProtect. Para recibir estas actualizaciones, debe tener una suscripción a las puertas de enlace de GlobalProtect. Además, para que GlobalProtect funcione, también debe crear una programación para estas actualizaciones.</p>
VPN sin cliente de GlobalProtect	<p>Contiene firmas de aplicaciones nuevas y actualizadas para franquear el acceso a aplicaciones web comunes desde el portal de GlobalProtect por VPN sin cliente. Para recibir estas actualizaciones, debe tener una suscripción a GlobalProtect.</p>

Actualización dinámica de contenido	Contenido del paquete
	Además, para que GlobalProtect Clientless VPN funcione, también debe crear una programación para estas actualizaciones. Como práctica recomendada, se recomienda instalar siempre las últimas actualizaciones de contenido para la VPN sin cliente de GlobalProtect.
WildFire	Proporciona acceso a firmas de malware y antivirus generadas por la nube pública de WildFire en tiempo real. Opcionalmente, puede configurar PAN-OS para recuperar los paquetes de actualización de firmas de WildFire. Puede configurar el cortafuegos de modo que busque actualizaciones nuevas incluso cada minuto para asegurarse de que obtiene las últimas firmas de WildFire en menos de un minuto desde que están disponibles. Si carece de la suscripción a WildFire, debe esperar al menos 24 horas para recibir las firmas con la actualización de antivirus.
WF-Private (Archivo específico de WildFire)	Proporciona, casi en tiempo real, las firmas contra malware y antivirus creadas como resultado del análisis realizado por un dispositivo de WildFire. Para recibir actualizaciones de contenido de un dispositivo de WildFire, tanto este como el cortafuegos deben ejecutar PAN-OS 6.1 o una versión posterior. Además, el cortafuegos debe estar configurado para reenviar archivos y enlaces de correo electrónico a la nube privada de WildFire.


Instalación de actualizaciones de contenido

Para garantizar una protección constante contra las amenazas más recientes (incluidas aquellas que aún no se han descubierto), debe asegurarse de mantener actualizados sus cortafuegos con las actualizaciones y el contenido más reciente de Palo Alto Networks. Los [Actualizaciones dinámicas de contenido](#) disponibles dependen de las [suscripciones](#) que tenga.

Siga estos pasos para instalar las actualizaciones de contenido. También puede configurar una programación si quiere definir la frecuencia con la que el cortafuegos obtiene e instala actualizaciones de contenido.

Las actualizaciones de contenido de aplicaciones y amenazas no funcionan exactamente igual que los demás tipos de actualizaciones. Para sacar el máximo partido de la prevención de amenazas y los conocimientos sobre aplicaciones más recientes, siga las directrices de [Implementación de actualizaciones de contenido de aplicaciones y amenazas](#) en lugar de estos pasos.

STEP 1 | Asegúrese de que el cortafuegos tenga acceso al servidor de actualización.

1. De forma predeterminada, el cortafuegos accede al **servidor de actualizaciones en `updates.paloaltonetworks.com`** para que el cortafuegos reciba actualizaciones de contenido del servidor más cercano. Si su cortafuegos tiene acceso limitado a Internet, podría ser necesario configurar su lista de permitidos a fin de permitir el acceso a los servidores involucrados en las descargas de actualizaciones. Para obtener más información sobre los servidores de actualización de contenido, consulte [Infraestructura de Red de entrega de contenido para actualizaciones dinámicas](#). Si desea obtener más información de referencia o tiene problemas de conectividad y descarga de actualizaciones, consulte <https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u00000001UtRCAU>.
-  *Si su dispositivo se encuentra en China continental, Palo Alto Networks recomienda utilizar el servidor **updates.paloaltonetworks.cn** para descargar actualizaciones.*
2. **(Opcional)** Haga clic en **Verify Update Server Identity** para obtener un nivel adicional de validación para habilitar el cortafuegos y comprobar que el certificado SSL del servidor esté firmado por una autoridad fiable. Esta opción está habilitada de manera predeterminada.
3. **(Opcional)** Si el cortafuegos necesita utilizar un servidor proxy para acceder a los servicios de actualización de Palo Alto Networks, en la ventana **Proxy Server (Servidor proxy)**, introduzca:
 - **Server:** dirección IP o nombre de host del servidor proxy.
 - **Port:** puerto para el servidor proxy. Intervalo: 1-65535.
 - **User:** nombre de usuario para acceder al servidor.
 - **Password (Contraseña):** contraseña para que el usuario acceda al servidor proxy. Vuelva a introducir la contraseña en **Confirm Password**.
4. **(Opcional)** Configure hasta tres intentos de reconexión si se produce un fallo en la conexión. Utilice **debug set-content-download-retry attempts** para establecer el número de intentos de conexión. El valor predeterminado es 0.

STEP 2 | Compruebe las actualizaciones de contenido más recientes.

Seleccione **Device (Dispositivo) > Dynamic Updates (Actualizaciones dinámicas)** y haga clic en **Check Now (Comprobar ahora)** (ubicado en la esquina inferior izquierda de la ventana) para

comprobar las últimas actualizaciones. El enlace de la columna **Action (Acción)** indica si una actualización está disponible:

- **Download (Descargar)**: indica que hay disponible un nuevo archivo de actualización. Haga clic en el enlace para iniciar la descarga directamente en el cortafuegos. Tras descargarlo correctamente, el enlace en la columna **Action (Acción)** cambia de **Download (Descargar)** a **Install (Instalar)**.

WildFire	Last checked: 2020/09/21 09:45:42 PDT	Schedule: None
515237-522316	panupv3-all-wildfire-515237-522316.candidate	PAN OS 10.0 And Later
Full	8 MB	5a46cd783114c7627162...
2020/09/21 09:45:03 PDT		Download



No puede descargar la actualización de antivirus hasta que haya instalado la actualización de aplicaciones y amenazas.

- **Revert (Revertir)**: indica que hay disponible una versión previa la versión de software o contenido. Puede decidir revertir a la versión instalada anteriormente.

STEP 3 | Instale las actualizaciones de contenido.



La instalación puede tardar hasta 10 minutos en los cortafuegos PA-220 y hasta 2 minutos en los cortafuegos PA-5200 Series, PA-7000 Series o VM-Series.

Haga clic en el enlace **Instalar** de la columna **Acción**. Cuando se complete la instalación, aparecerá una marca de verificación en la columna **Currently Installed (Instalado actualmente)**.

WildFire	Last checked: 2020/09/21 09:48:44 PDT	Schedule: None
515238-522317	panupv3-all-wildfire-515238-522317.candidate	PAN OS 10.0 And Later
Full	8 MB	aed1502259d57604f288...
2020/09/21 09:50:06 PDT	✓	Install

STEP 4 | Programe cada actualización de contenido.

Repita este paso en cada actualización que desee programar.



Escalone las programaciones de actualizaciones, ya que el cortafuegos no puede descargar más de una actualización a la vez. Si ha programado la descarga de varias actualizaciones al mismo tiempo, solo la primera se realizará correctamente.

1. Establezca la programación de cada tipo de actualización haciendo clic en el enlace **Ninguna**.

WildFire	Last checked: 2020/09/21 09:48:44 PDT	Schedule: None
515238-522317	panupv3-all-wildfire-515238-522317.candidate	PA

2. Especifique la frecuencia de las actualizaciones seleccionando un valor en el menú desplegable **Recurrence (Periodicidad)**. Los valores disponibles varían según el tipo de contenido (las actualizaciones de WildFire están disponibles en **Real-time [Tiempo real]**, **Every Minute [Cada minuto]**, **Every 15 Minutes [Cada 15 minutos]**, **Every 30 minutes [Cada 30 minutos]** o **Every Hour [Cada hora]**, mientras que las actualizaciones de aplicaciones y amenazas pueden programarse **Weekly [Semanalmente]**, **Daily [Diariamente]**, **Hourly [Por hora]** o **Every 30 Minutes [Cada 30 minutos]**, y las actualizaciones de antivirus pueden programarse **Hourly [Cada hora]**, **Daily [Diariamente]** o **Weekly [Semanalmente]**).

También puede seleccionar de manera manual **None (Ninguno)** para aplicaciones y amenazas o para actualizaciones de antivirus. Esto significa que no hay una programación recurrente para este elemento y debe instalar las actualizaciones manualmente. Para eliminar por completo el nodo de programación, seleccione **Delete Schedule (Eliminar programación)**.

3. Especifique la **hora** (o los minutos que pasan de una hora en el caso de WildFire) y, si está disponible en función de la **Periodicidad** seleccionada, el **día** de la semana para realizar la actualización.
4. Especifique si desea que el sistema use la opción **Download Only (Únicamente descargar)** o, como opción recomendada, **Download And Install (Descargar e instalar)** la actualización.
5. Introduzca cuánto tiempo una publicación debe esperar antes de realizar una actualización de contenido en el campo **Threshold (Hours)**. En raras ocasiones puede haber errores en las actualizaciones de contenido. Por este motivo, tal vez desee retrasar la instalación de nuevas actualizaciones hasta que lleven varias horas publicadas.



Si tiene aplicaciones vitales que deben estar totalmente disponibles, configure el umbral de las actualizaciones de aplicaciones o las actualizaciones de aplicaciones y amenazas en un mínimo de 24 horas y siga el procedimiento [Prácticas recomendadas para las actualizaciones de contenido de aplicaciones y amenazas](#). Además, después de configurar la programación de las actualizaciones de contenido, tarea que solo se realiza una vez o con poca frecuencia, debe seguir [gestionando los App-ID nuevos y modificados](#) que se incluyen en las versiones de contenido, ya que pueden cambiar la manera de aplicar la política de seguridad.

6. **(Opcional)** Especifique los **nuevos umbrales de ID de aplicación** en horas para establecer la cantidad de tiempo que el cortafuegos debe esperar antes de instalar actualizaciones de contenido que contengan nuevos App-ID.

Applications and Threats Update Schedule ?

Recurrence

Weekly

Day

wednesday

Time

01:02

Action

download-and-install

☐

Disable new apps in content update

Threshold (hours)

24

A content update must be at least this many hours old for the action to be taken.

Allow Extra Time to Review New App-IDs

Set the amount of time the firewall waits before installing content updates that contain new App-IDs. You can use this wait period to assess and adjust your security policy based on the new App-IDs.

New App-ID Threshold (hours)

24

Delete Schedule

OK

Cancel

7. Haga clic en **OK (Aceptar)** para guardar estos ajustes de programación.
8. Haga clic en **Commit (Confirmar)** para guardar estos ajustes en la configuración actual.

STEP 5 | Actualización de PAN-OS.



Siempre actualice el contenido antes de actualizar PAN-OS. Cada versión de PAN-OS tiene una [versión de publicación de contenido compatible mínima](#).

1. Revise las [notas de versión](#).
2. [Actualice el software de PAN-OS](#).

Actualización de contenido de aplicaciones y amenazas

Las actualizaciones de contenido de aplicaciones y amenazas proporcionan las firmas de aplicaciones y prevención de amenazas más recientes al cortafuegos. La sección de aplicaciones del paquete incluye ID de aplicación nuevas y modificadas y no requiere una licencia. El paquete completo de contenido de aplicaciones y prevención de amenazas, que también incluye firmas de prevención de amenazas nuevas y modificadas, requiere una licencia de prevención de amenazas. Dado que el cortafuegos recupera e instala automáticamente las firmas de aplicaciones y prevención de amenazas más recientes (en función de los ajustes personalizados), puede comenzar a aplicar una política de seguridad en función de las ID de aplicación y la protección frente a amenazas más reciente sin una configuración adicional.

Las firmas de prevención de amenazas nuevas y modificadas y las ID de aplicación modificadas se publican, al menos, una vez a la semana y generalmente con mayor frecuencia. Los App-ID nuevos se publican el tercer martes de cada mes.



En casos excepcionales, la publicación de la actualización que contiene ID de aplicación nuevos puede demorarse uno o dos días.

Dado que las ID de aplicación nuevas pueden cambiar cómo la política de seguridad aplica el tráfico, esta liberación más limitada de ID de aplicación nuevas tiene como objetivo proporcionarle una ventana predecible para preparar y actualizar su política de seguridad. Además, las actualizaciones de contenido se acumulan; esto significa que la actualización de contenido más reciente siempre incluye las firmas de aplicaciones y de prevención de amenazas publicadas en las versiones anteriores.

Debido a que las firmas de aplicaciones y amenazas se entregan en un solo paquete (los mismos decodificadores que permiten que las firmas de aplicaciones identifiquen las aplicaciones también permiten que las firmas de prevención de amenazas inspeccionen el tráfico), debe considerar si desea implementar las firmas en conjunto o por separado. Cómo la elección de la implementación de las actualizaciones de contenido depende de los requisitos de seguridad de red y de disponibilidad de la aplicación de la organización. En primer lugar, identifique a su organización con una de las siguientes posturas (o quizás ambas según la ubicación del cortafuegos):

- Una organización que pone *la seguridad en primer lugar* prioriza la protección con las firmas contra amenazas más actualizadas por encima de la disponibilidad de la aplicación. Básicamente está utilizando el cortafuegos para las prestaciones de prevención de amenazas. Los cambios en la ID de aplicación que afectan cómo la política de seguridad aplica el tráfico de la aplicación son secundarios.
- Una red *crítica* prioriza la disponibilidad de la aplicación por encima de la protección con las firmas contra amenazas más actualizadas. Su red tiene una tolerancia cero de los periodos de inactividad. El cortafuegos se implementa en línea para aplicar la política de seguridad y, si está utilizando una ID de aplicación en la política de seguridad, todo cambio que introduja una versión de contenido que afecte la ID de aplicación podría causar un periodo de inactividad.

Usted puede adoptar un enfoque de red crítica o de seguridad en primer lugar para implementar las actualizaciones de contenido, o puede aplicar una combinación de ambos enfoques para satisfacer las necesidades de la empresa. Revise y considere [Prácticas recomendadas para las actualizaciones de contenido de aplicaciones y amenazas](#) para decidir cómo desea implementar las actualizaciones de aplicaciones y amenazas. A continuación:

- ❑ Siga el procedimiento [Implementación de actualizaciones de contenido de aplicaciones y amenazas](#).
- ❑ Siga los consejos de [Sugerencias para las actualizaciones de contenido](#).



Mientras que la programación de las actualizaciones de contenido es una tarea única o poco frecuente, después de establecer una programación, deberá continuar con la [Gestión de App-ID nuevas y modificadas](#) en las versiones de contenido, dado que estas App-ID pueden cambiar cómo se aplica la política de seguridad.

Implementación de actualizaciones de contenido de aplicaciones y amenazas

Antes de seguir los pasos para configurar las actualizaciones de contenido de amenazas y aplicaciones, conozca cómo funciona [Actualización de contenido de aplicaciones y amenazas](#) y decida cómo desea implementar [Prácticas recomendadas para las actualizaciones de contenido de aplicaciones y amenazas](#).

Además, Panorama le permite implementar actualizaciones de contenido en los cortafuegos con facilidad y rapidez. Si utiliza Panorama para gestionar los cortafuegos, siga [estos pasos para implementar las actualizaciones de contenido](#), en lugar de seguir los pasos a continuación.

STEP 1 | Para desbloquear el paquete completo de contenido de aplicaciones y prevención de amenazas, obtenga una licencia de prevención de amenazas y [active la licencia](#) en el cortafuegos.

1. Seleccione **Device (Dispositivo) > Licenses (Licencias)**.
2. Cargue manualmente la clave de la licencia o recupérela del servidor de licencias de Palo Alto Networks.
3. Verifique que la licencia de prevención contra amenazas esté activa.

STEP 2 | Establezca una programación para que el cortafuegos recupere e instale actualizaciones de contenido.

Cuando complete los siguientes pasos, reviste especial importancia tener en cuenta si la organización [se centra en los objetivos o en la seguridad](#) (o en una combinación de ambos) y leer [Prácticas recomendadas para las actualizaciones de contenido de aplicaciones y amenazas](#).

1. Seleccione **Device > Dynamic Updates** (Dispositivo > Actualizaciones dinámicas).
2. Seleccione la **Schedule (Programación)** de las actualizaciones de contenido de aplicaciones y prevención de amenazas.
3. Establezca la frecuencia (**Recurrence [Periodicidad]**) con la que el cortafuegos comprueba el servidor de actualización de Palo Alto Networks para buscar nuevas versiones de contenido de aplicaciones y prevención de amenazas, y el **Day (Día)** y la **Time (Hora)**.
4. Establezca la **Action (Acción)** que realizará el cortafuegos cuando descubra y recupere una nueva versión de contenido.
5. Establezca el **Threshold (Umbral)** de instalación para las versiones de contenido. Las versiones de contenido deben estar disponibles en el servidor de actualización de Palo Alto Networks al menos durante este período de tiempo antes de que el cortafuegos recupere la licencia y realice la acción que configuró en el último paso.
6. Si su red es crítica, con tolerancia cero a los periodos de inactividad de la aplicación (la disponibilidad de la aplicación es casi tan importante como la prevención de amenazas más reciente), puede establecer un **New App-ID Threshold (Umbral de App-ID nueva)**. El cortafuegos únicamente recupera actualizaciones de contenido que contienen App-ID nuevas luego de que haya estado disponible durante este período de tiempo.
7. Haga clic en **OK (Aceptar)** para guardar la programación de actualizaciones de contenido de aplicaciones y prevención de amenazas, y haga clic en **Commit (Confirmar)**.

- STEP 3 |** Realice la [Configuración del reenvío de logs](#) para enviar alertas de contenido crítico de Palo Alto Networks a servicios externos que utiliza para supervisar la actividad de la red y el cortafuegos. Esto le permite garantizar que el personal adecuado reciba la notificación sobre problemas de contenido críticos, de modo que se puedan tomar las medidas necesarias. Las alertas críticas de actualización de contenido también se guardan como entradas en el log del sistema con Type (Tipo) y Event (Evento): (subtype eq dynamic-updates) y (eventid eq palo-alto-networks-message).
- STEP 4 |** Mientras que la programación de las actualizaciones de contenido es una tarea única o poco frecuente, después de establecer una programación, deberá continuar con la [Gestión de App-ID nuevas y modificadas](#) en las versiones de contenido, dado que estas App-ID pueden cambiar cómo se aplica la política de seguridad.

Sugerencias para las actualizaciones de contenido

Las versiones de contenido de aplicaciones y prevención de amenazas de Palo Alto Networks experimentan evaluaciones estrictas de rendimiento y calidad. Sin embargo, debido a que existen demasiadas variables posibles en el entorno de un cliente, rara vez una versión de contenido afecta una red de manera inesperada. Siga estas sugerencias para mitigar o solucionar un problema relacionado con una versión de contenido, de modo que su red se vea afectada lo menos posible.

- ❑ **Siga las prácticas recomendadas para las actualizaciones de contenido de aplicaciones y amenazas.**

Lea e implemente las [Prácticas recomendadas para las actualizaciones de contenido de aplicaciones y amenazas](#). Cómo la elección de la implementación de las actualizaciones de contenido depende de sus requisitos de seguridad de red y de disponibilidad de la aplicación.

- ❑ **Compruebe si está ejecutando el contenido más reciente.**

Obtenga la actualización de contenido más reciente si no configuró el cortafuegos para descargarla e instalarla automáticamente.

El cortafuegos valida que Palo Alto Networks aún recomiende las actualizaciones de contenido descargadas en el momento de la instalación. Esta comprobación, que el cortafuegos realiza de manera predeterminada, es útil cuando las actualizaciones de contenido se descargan del servidor de actualización de Palo Alto Networks (manualmente o de manera programada) antes de la instalación. Debido a que en contadas ocasiones Palo Alto Networks elimina una actualización de contenido, esta opción evita que el cortafuegos instale una actualización de contenido que Palo Alto Networks eliminó, incluso si el cortafuegos ya la descargó. Si observa un mensaje de error que indica que la actualización de contenido que intenta instalar ya no es válida, haga clic en **Check Now (Comprobar ahora)** para obtener la actualización de contenido más reciente e instale esa versión (**Device [Dispositivo] > Dynamic Updates [Actualizaciones dinámicas]**).

- ❑ **Active la telemetría de inteligencia contra amenazas.**

Active la [telemetría de inteligencia contra amenazas](#) que el cortafuegos envía a Palo Alto Networks. Utilizamos datos de telemetría para identificar y solucionar problemas de las actualizaciones de contenido.

Los datos de telemetría nos ayudan a reconocer con rapidez una actualización de contenido que afecta el rendimiento del cortafuegos o la aplicación de una política de seguridad de manera inesperada en

la base de clientes de Palo Alto Networks. Cuanto más rápido identificamos un problema, con mayor rapidez podemos ayudarte a evitar el problema o mitigar el impacto en su red.

Para permitir que el cortafuegos recopile y comparta datos de telemetría con Palo Alto Networks:

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Telemetry (Telemetría)**.
2. Edite los ajustes de **Telemetry (Telemetría)** y haga clic en **Select All (Seleccionar todos)**.
3. Haga clic en **OK (Aceptar)** y seleccione **Commit (Confirmar)** para guardar los cambios.

❑ **Reenvíe las alertas de actualizaciones de contenido de Palo Alto Networks a las personas indicadas.**

Habilite el reenvío de logs para las alertas de contenido crítico de Palo Alto Networks, de modo que los mensajes importantes sobre los problemas en la versión de contenido se dirijan directamente al personal adecuado.

Ahora, Palo Alto Networks puede emitir alertas sobre problemas de actualización de contenido directamente en la interfaz web del cortafuegos o (si habilitó el reenvío de logs) en el servicio externo que utiliza para la supervisión. Las alertas de contenido crítico describen el problema, de modo que pueda comprender cómo lo afectan e incluyen medidas a tomar de ser necesario.

En la interfaz web del cortafuegos, las alertas críticas sobre problemas de contenido se muestran de manera similar al [mensaje del día](#). Cuando Palo Alto Networks emite una alerta crítica sobre una actualización de contenido, la alerta se muestra de manera predeterminada cuando inicia sesión en la interfaz web del cortafuegos. Si ya inició sesión en la interfaz web del cortafuegos, observará que aparece un signo de exclamación sobre el icono de mensaje en la barra de menú ubicada en la parte inferior de la interfaz web; haga clic en el icono de mensaje para ver la alerta.

Las alertas críticas de actualización de contenido también se guardan como entradas en el log del sistema con Type (Tipo) **dynamic-updates** y Event (Evento) **palo-alto-networks-message**. Utilice el siguiente filtro para ver esas entradas del log: (subtype eq dynamic-updates) y (eventid eq palo-alto-networks-message).

❑ **Use Panorama para revertir la versión del contenido a una anterior si es necesario.**

Tras recibir la notificación de un problema en una actualización de contenido, puede utilizar Panorama para restablecer con rapidez los cortafuegos gestionados a la última versión de actualización de contenido, en lugar de restablecer de forma manual la versión de contenido en los cortafuegos individuales: [Restablecimiento de las actualizaciones de contenido de Panorama](#).

Prácticas recomendadas para las actualizaciones de contenido de aplicaciones y amenazas

Las prácticas recomendadas para implementar actualizaciones de contenido ayudan a garantizar una aplicación correcta de la política a medida que se introducen aplicaciones y firmas contra amenazas nuevas y modificadas en el cortafuegos. A pesar de que las firmas de aplicaciones y amenazas se entregan en una única actualización de contenido (conozca más sobre [Actualización de contenido de aplicaciones y amenazas](#)), usted cuenta con la flexibilidad para implementarlas de manera diferente en función de los requisitos de seguridad y disponibilidad de su red:

- Una organización que pone *la seguridad en primer lugar* prioriza la protección con las firmas contra amenazas más actualizadas por encima de la disponibilidad de la aplicación. Básicamente está utilizando el cortafuegos para las prestaciones de prevención de amenazas.
- Una red *crítica* prioriza la disponibilidad de la aplicación por encima de la protección con las firmas contra amenazas más actualizadas. Su red tiene una tolerancia cero de los periodos de inactividad. El cortafuegos se implementa en línea para aplicar la política de seguridad y, si está usando una ID de aplicación en la política de seguridad, todo cambio del contenido que afecte la ID de aplicación podría causar un periodo de inactividad.

Usted puede adoptar un enfoque de red crítica o de seguridad en primer lugar para implementar las actualizaciones de contenido, o puede aplicar una combinación de ambos enfoques para satisfacer las necesidades de la empresa. Considere su enfoque mientras aplica las siguientes prácticas recomendadas para aprovechar mejor las firmas de aplicaciones y contra amenazas nuevas y modificadas:

- [Prácticas recomendadas para las actualizaciones de contenido: nivel crítico](#)
- [Prácticas recomendadas para las actualizaciones de contenido: prioridad de seguridad](#)

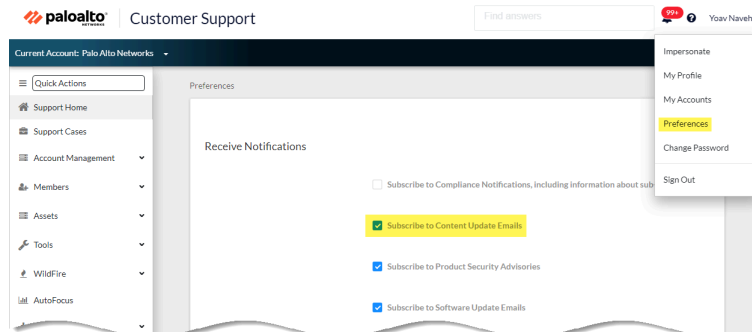
Prácticas recomendadas para las actualizaciones de contenido: nivel crítico

Las [Prácticas recomendadas para las actualizaciones de contenido de aplicaciones y amenazas](#) permiten garantizar la correcta aplicación de las políticas a medida que se publican firmas nuevas de aplicaciones y contra amenazas. Respete estas prácticas recomendadas para implementar las actualizaciones de contenido en una *red crítica*, donde tiene una tolerancia cero a los periodos de inactividad de la aplicación.

- ❑ Siempre revise las notas de la versión de contenido para conocer la lista de las aplicaciones identificadas y modificadas recientemente, y las firmas de amenazas que introduce la versión de contenido. Las notas de la versión de contenido también describen de qué manera la actualización

puede afectar la aplicación de la política de seguridad existente y ofrece recomendaciones sobre cómo puede modificar su política de seguridad para aprovechar mejor lo nuevo.

Para suscribirse y recibir notificaciones de las nuevas actualizaciones de contenido, visite el [portal de asistencia al cliente](#), edite **Preferences (Preferencias)** y seleccione **Subscribe to Content Update Emails (Suscribirse para recibir actualizaciones de contenido por correo electrónico)**.



También puede revisar las [notas de la versión de contenido para aplicaciones y prevención de amenazas](#) en el portal de asistencia técnica de Palo Alto Networks o directamente en la interfaz web del cortafuegos: seleccione **Device (Dispositivo) > Dynamic Updates (Actualizaciones dinámicas)** y abra la **Release Note (Nota de la versión)** de una versión de contenido específica.

PA-3260											
DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE											
22 items											
VERSION	FILE NAME	FEATURES	TYPE	SIZE	SHA256	RELEASE DATE	DOWNLOADED	CURRENTLY INSTALLED	ACTION	DOCUMENTATION	
> Antivirus Last checked: 2020/09/21 09:45:41 PDT Schedule: None > Applications and Threats Last checked: 2020/09/21 09:45:38 PDT Schedule: Every Wednesday at 01:02 (Download only)											
8292-6181	panupv2-all-apps-8292-6181	Apps	Full	47 MB		2020/07/13 11:46:39 PDT	✓ previously		Revert	Release Notes	
8317-6296	panupv2-all-apps-8317-6296	Apps	Full	48 MB		2020/09/08 17:55:10 PDT		✓	Review Policies Review Apps	Release Notes	
8320-6303	panupv2-all-contents-8320-6303	Apps, Threats	Full	56 MB	84bec4d9ccecfd164e0ae...	2020/09/11 12:04:40 PDT			Download	Release Notes	
8320-6305	panupv2-all-contents-8320-6305	Apps, Threats	Full	56 MB	8a562c6d8472feb9a0356...	2020/09/11 16:36:04 PDT			Download	Release Notes	
8320-6307	panupv2-all-contents-8320-6307	Apps, Threats	Full	57 MB	137eb5f7637306c8c1e...	2020/09/11 20:10:13 PDT			Download	Release Notes	
8320-6308	panupv2-all-contents-8320-6308	Apps, Threats	Full	57 MB	2ca4a4e1afc6292a1cd1b...	2020/09/14 17:27:56 PDT			Download	Release Notes	
8320-6309	panupv2-all-contents-8320-6309	Apps, Threats	Full	56 MB	192cf08c2f0058c188d0...	2020/09/14 18:13:54 PDT			Download	Release Notes	
8320-6310	panupv2-all-contents-8320-6310	Apps, Threats	Full	57 MB	2436f79a8f02aef137b82...	2020/09/15 10:19:15 PDT			Download	Release Notes	
8321-6311	panupv2-all-contents-8321-6311	Apps, Threats	Full	56 MB	603a71e854a0e0e0e0e...	2020/09/15 13:44:29 PDT			Download	Release Notes	

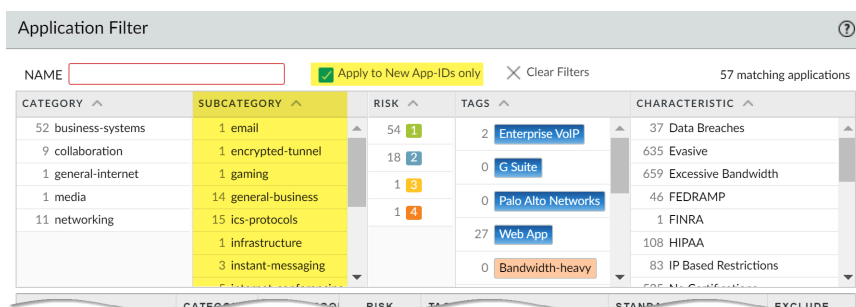


La sección Notes (Notas) de las notas de versión de contenido resalta las futuras actualizaciones que Palo Alto Networks ha identificado como posibles impactos considerables para la cobertura; por ejemplo, nuevas ID de aplicación o decodificadores. Verifique estas futuras actualizaciones, de manera que pueda prever con antelación cualquier impacto de la versión en la política.

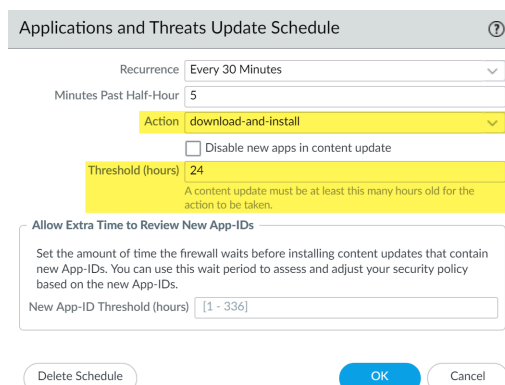
- ❑ Cree una regla en la política de seguridad para siempre [permitir ciertas categorías de App-ID nuevos](#), como aplicaciones de autenticación o desarrollo de software en las que confían las funciones empresariales críticas. Esto significa que cuando una versión de contenido introduce o cambia la cobertura de una aplicación empresarial importante, el cortafuegos continúa permitiendo sin inconvenientes la aplicación sin requerir una actualización en la política de seguridad. Esto elimina el posible impacto en la disponibilidad de los App-ID de categorías críticas y ofrece treinta días (los

App-ID nuevos se liberan una vez al mes) para ajustar su política de seguridad de modo que permita los App-ID críticos.

Para hacerlo, cree un [filtro de aplicación para App-ID nuevas en categorías críticas application \(Objects \[Objetos\] > Application Filters \[Filtros de aplicación\]\)](#),



- ❑ Para mitigar el impacto en la aplicación de la política de seguridad asociada con la habilitación de nuevas firmas de aplicaciones y amenazas, puede alternar la implementación del contenido nuevo. Proporcione el nuevo contenido a las ubicaciones con menos riesgo comercial (menor usuarios en sucursales) antes de implementarlo en las ubicaciones con mayor riesgo comercial (tal como las ubicaciones con aplicaciones críticas). El confinamiento de las actualizaciones de contenido más recientes a ciertos cortafuegos antes de implementarlas en toda la red también facilita la detección de problemas e inconvenientes que puedan surgir. Puede utilizar Panorama para enviar programaciones escalonadas y umbrales de instalación para los cortafuegos y los grupos de dispositivos en función de la organización o ubicación ([Utilización de Panorama para implementar actualizaciones en los cortafuegos](#)).
- ❑ Programe las actualizaciones de contenido, de modo que se puedan **download-and-install (descargar e instalar)** automáticamente. Luego, establezca un **Threshold (Umbral)** que determine la cantidad de tiempo que espera el cortafuegos antes de instalar el contenido más reciente. En una red crítica, programe un umbral de hasta 48 horas.



La demora en la instalación garantiza que el cortafuegos únicamente instale contenido que ha estado disponible y que funciona en los entornos del cliente durante ese período de tiempo específico. Para [programar actualizaciones de contenido](#), seleccione **Device (Dispositivo) > Dynamic Updates (Actualizaciones dinámicas) > Schedule (Programar)**.

- ❑ Proporcione tiempo adicional para ajustar su política de seguridad en función de las App-ID antes de instalarlas. Para hacerlo, establezca un umbral de instalación que se aplique únicamente a las actualizaciones de contenido que contienen nuevas App-ID. Las actualizaciones de contenido con nuevas App-ID se liberan únicamente una vez al mes y el umbral de instalación se activa únicamente

en ese momento. [Programa actualizaciones de contenido](#) para configurar un **New App-ID Threshold (Umbral de nueva App-ID) (Device [Dispositivo] > Dynamic Updates [Actualizaciones dinámicas] > Schedule [Programar])**.

Applications and Threats Update Schedule

Recurrence: Every 30 Minutes

Minutes Past Half-Hour: 5

Action: download-and-install

☐ Disable new apps in content update

Threshold (hours): 24
A content update must be at least this many hours old for the action to be taken.

Allow Extra Time to Review New App-IDs

Set the amount of time the firewall waits before installing content updates that contain new App-IDs. You can use this wait period to assess and adjust your security policy based on the new App-IDs.

New App-ID Threshold (hours): 48

Delete Schedule OK Cancel

- Siempre revise las App-ID nuevas y modificadas que introduce una versión de contenido para evaluar cómo estos cambios afectan su política de seguridad. El siguiente tema describe las opciones que puede utilizar para actualizar su política de seguridad antes y después de instalar nuevas App-ID: Realice la [Gestión de ID de aplicación nuevas y modificadas](#).

Applications and Threats Last checked: 2020/09/21 09:45:38 PDT Schedule: Every Wednesday at 01:02 (Download only)

Name	App	Full	Size	Last Checked	Actions
8292-6181	panupv2-all-apps-8292-6181	Apps	47 MB	2020/07/13 11:46:39 PDT	✓ previously Revert
8317-6296	panupv2-all-apps-8317-6296	Apps	48 MB	2020/09/08 17:55:10 PDT	✓ Review Policies Review Apps

New and Modified Applications since last installed content

25 items

Content Version: 8320

Search: []

Left sidebar: New Apps, Content Version: 8320, List of apps (apache-guacamole, assa-abloy-r3, comodo-itm, conx-meeting, creo-model-manager, ether-s-bus, google-messages, nihon-kohden-patient-monitoring, paloalto-device-telemetry, smtp-starttis, stomp, streamyard, vmware-carbon-black, wargaming.net)

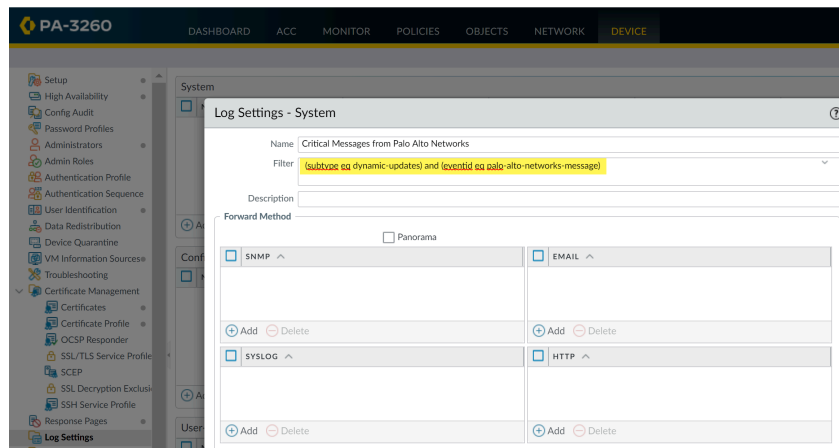
Right pane details for 'apache-guacamole':

- Name: apache-guacamole
- Standard Ports: tcp/8080
- Depends on: web-browsing, websocket
- Implicitly Uses: web-browsing, websocket
- Previously Identified As: web-browsing, websocket
- Deny Action: drop-reset
- Additional Information: Apache Guacamole, Google, Yahoo!
- Characteristics: Evasive: no, Excessive Bandwidth Use: no, Used by Malware: no, Capable of File Transfer: no, Has Known Vulnerabilities: yes
- Classification: Category: networking, Subcategory: remote-access, Risk: []

Bottom right: Install Review Policies Review Apps

- Realice la [Configuración del reenvío de logs](#) para enviar alertas de contenido crítico de Palo Alto Networks a servicios externos que utiliza para supervisar la actividad de la red y el cortafuegos. Esto le permite garantizar que el personal adecuado reciba la notificación sobre problemas de contenido críticos, de modo que se puedan tomar las medidas necesarias. Las alertas críticas de actualización de contenido también se guardan como entradas en el log del sistema con Type (Tipo) y Event

(Evento): (**subtype eq dynamic-updates**) y (**eventid eq palo-alto-networks-message**).



PAN-OS 8.1.2 modificó el tipo de log para las alertas de contenido críticas de **general** a **dynamic-updates**. Si utiliza PAN-OS 8.1.0 o PAN-OS 8.1.1, el contenido crítico se registra como entradas de log del sistema con el siguiente Type (Tipo) y Event (Evento), y debe configurar el reenvío para estas alertas con el siguiente filtro: (**subtype eq general**) y (**eventid eq palo-alto-networks-message**).

- ❑ Pruebe las actualizaciones nuevas de contenido de aplicaciones y amenazas en un entorno de prueba dedicado antes de habilitarlas en su entorno de producción. La manera más fácil de comprobar las nuevas aplicaciones y contenido contra amenazas es usar un cortafuegos de prueba para acceder al tráfico de producción. Instale el contenido más reciente en el cortafuegos de prueba y contrólole a medida que procesa el tráfico copiado de su entorno de producción. También puede usar clientes de prueba y un cortafuegos de prueba, o capturas de paquetes (packet captures, PCAP) para simular el tráfico de producción. El uso de PCAP funciona bien para simular el tráfico de distintas implementaciones en las que la política de seguridad del cortafuegos varía según la ubicación.

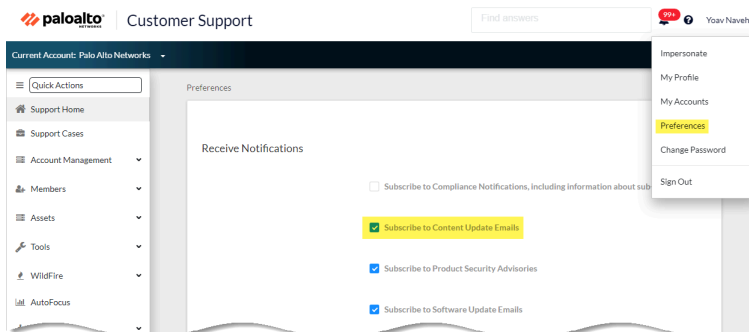
Prácticas recomendadas para las actualizaciones de contenido: prioridad de seguridad

Las [Prácticas recomendadas para las actualizaciones de contenido de aplicaciones y amenazas](#) permiten garantizar la correcta aplicación de las políticas a medida que se publican firmas nuevas de aplicaciones y contra amenazas. Respete estas prácticas recomendadas para implementar las actualizaciones de contenido en una *red con prioridad de seguridad*, donde utiliza principalmente el cortafuegos para las capacidades de prevención de amenazas y su primera prioridad es la defensa frente al ataque.

- ❑ Siempre revise las notas de la versión de contenido para conocer la lista de las aplicaciones identificadas y modificadas recientemente, y las firmas de amenazas que introduce la versión de contenido. Las notas de la versión de contenido también describen de qué manera la actualización

puede afectar la aplicación de la política de seguridad existente y ofrece recomendaciones sobre cómo puede modificar su política de seguridad para aprovechar mejor lo nuevo.

Para suscribirse y recibir notificaciones de las nuevas actualizaciones de contenido, visite el [portal de asistencia al cliente](#), edite **Preferences (Preferencias)** y seleccione **Subscribe to Content Update Emails (Suscribirse para recibir actualizaciones de contenido por correo electrónico)**.



También puede revisar las [notas de la versión de contenido para aplicaciones y prevención de amenazas](#) en el portal de asistencia técnica de Palo Alto Networks o directamente en la interfaz web del cortafuegos: seleccione **Device (Dispositivo) > Dynamic Updates (Actualizaciones dinámicas)** y abra la **Release Note (Nota de la versión)** de una versión de contenido específica.

VERSION	FILE NAME	FEATURES	TYPE	SIZE	SHA256	RELEASE DATE	DOWNLOADED	CURRENTLY INSTALLED	ACTION	DOCUMENTATION
<div>Antivirus</div> <div>Applications and Threats</div>										
8292-6181	panupv2-all-apps-8292-6181	Apps	Full	47 MB		2020/07/13 11:46:39 PDT	✓ previously		Revert	Release Notes
8317-6296	panupv2-all-apps-8317-6296	Apps	Full	48 MB		2020/09/08 17:55:10 PDT		✓	Review Policies Review Apps	Release Notes
8320-6303	panupv2-all-contents-8320-6303	Apps, Threats	Full	56 MB	84bec4d9ccecfd1640ae...	2020/09/11 12:04:40 PDT			Download	Release Notes
8320-6305	panupv2-all-contents-8320-6305	Apps, Threats	Full	56 MB	8a562c6d8472feb9a035e...	2020/09/11 16:36:04 PDT			Download	Release Notes
8320-6307	panupv2-all-contents-8320-6307	Apps, Threats	Full	57 MB	137eb5f763730f6c8c1e...	2020/09/11 20:10:13 PDT			Download	Release Notes
8320-6308	panupv2-all-contents-8320-6308	Apps, Threats	Full	57 MB	2ca4a4e1afc6292a1cd1b...	2020/09/14 17:27:56 PDT			Download	Release Notes
8320-6309	panupv2-all-contents-8320-6309	Apps, Threats	Full	56 MB	192cf8c2f0058c1884d...	2020/09/14 18:13:54 PDT			Download	Release Notes
8320-6310	panupv2-all-contents-8320-6310	Apps, Threats	Full	57 MB	2436f79a8f02aef137b82...	2020/09/15 10:19:15 PDT			Download	Release Notes
8321-6311	panupv2-all-contents-8321-6311	Apps, Threats	Full	56 MB	63ca71e854e0e0e0e0e...	2020/09/15 13:44:29 PDT			Download	Release Notes



La sección Notes (Notas) de las notas de versión de contenido resalta las futuras actualizaciones que Palo Alto Networks ha identificado como posibles impactos considerables para la cobertura; por ejemplo, nuevas ID de aplicación o decodificadores. Verifique estas futuras actualizaciones, de manera que pueda prever con antelación cualquier impacto de la versión en la política.

- ❑ Para mitigar el impacto en la aplicación de la política de seguridad asociada con la habilitación de nuevas firmas de aplicaciones y amenazas, puede alternar la implementación del contenido nuevo. Proporcione el nuevo contenido a las ubicaciones con menos riesgo comercial (menor usuarios en sucursales) antes de implementarlo en las ubicaciones con mayor riesgo comercial (tal como las ubicaciones con aplicaciones críticas). El confinamiento de las actualizaciones de contenido más recientes a ciertos cortafuegos antes de implementarlas en toda la red también facilita la detección de problemas e inconvenientes que puedan surgir. Puede utilizar Panorama para enviar programaciones escalonadas y umbrales de instalación para los cortafuegos y los grupos de dispositivos en función de la organización o ubicación ([Utilización de Panorama para implementar actualizaciones en los cortafuegos](#)).
- ❑ Programe las actualizaciones de contenido, de modo que se puedan **download-and-install (descargar e instalar)** automáticamente. Luego, establezca un **Threshold (Umbral)** que determine la cantidad de

tiempo que espera el cortafuegos antes de instalar el contenido más reciente. En una red con prioridad de seguridad, programe un umbral de seis a doce horas.

Applications and Threats Update Schedule

Recurrence: Every 30 Minutes

Minutes Past Half-Hour: 5

Action: download-and-install

☐ Disable new apps in content update


Threshold (hours): 6
A content update must be at least this many hours old for the action to be taken.

Allow Extra Time to Review New App-IDs
Set the amount of time the firewall waits before installing content updates that contain new App-IDs. You can use this wait period to assess and adjust your security policy based on the new App-IDs.

New App-ID Threshold (hours): [1 - 336]

Buttons: Delete Schedule, OK, Cancel

La demora en la instalación garantiza que el cortafuegos únicamente instale contenido que ha estado disponible y que funciona en los entornos del cliente durante ese período de tiempo específico. Para [programar actualizaciones de contenido](#), seleccione **Device (Dispositivo) > Dynamic Updates (Actualizaciones dinámicas) > Schedule (Programar)**.

 *No programe un **New App-ID Threshold (Umbral de nueva App-ID)**. Este umbral brinda a las organizaciones críticas tiempo adicional para ajustar la aplicación de la política de seguridad en función de las nuevas App-ID. Sin embargo, debido a que este umbral también demora la entrega de las actualizaciones de contenido de prevención de amenazas más recientes, no se recomienda a las organizaciones que ponen la seguridad en primer lugar.*

- Revise las App-ID nuevas y modificadas que introduce una versión de contenido para evaluar cómo estos cambios afectan su política de seguridad. El siguiente tema describe las opciones que puede utilizar para actualizar su política de seguridad antes y después de instalar nuevas App-ID: [Realice la Gestión de ID de aplicación nuevas y modificadas](#).

Applications and Threats

Last checked: 2020/09/21 09:45:38 PDT Schedule: Every Wednesday at 01:02 (Download only)

App-ID	Name	Version	Size	Last Checked	Action
8292-6181	panupv2-all-apps-8292-6181	Apps	Full	47 MB	2020/07/13 11:46:39 PDT
8317-6296	panupv2-all-apps-8317-6296	Apps	Full	48 MB	2020/09/08 17:55:10 PDT

New and Modified Applications since last installed content

25 items

Content Version: 8320

- apache-guacamole
- assa-abloy-r3
- comodo-itsm
- conv-meeting
- creo-model-manager
- ether-s-bus
- google-messages
- nhon-kohen-patient-monitoring
- paloalto-device-telemetry
- smtp-startis
- stomp
- streamyard
- vmware-carbon-black
- wargaming.net

Content Version: 8321-6313

Application Details: apache-guacamole

Name: apache-guacamole

Standard Ports: tcp/8080

Depends on: web-browsing, websocket

Implicitly Uses:

Previously Identified As: web-browsing, websocket

Deny Action: drop-reset

Additional Information: Apache Guacamole, Google, Yahoo!

Characteristics:

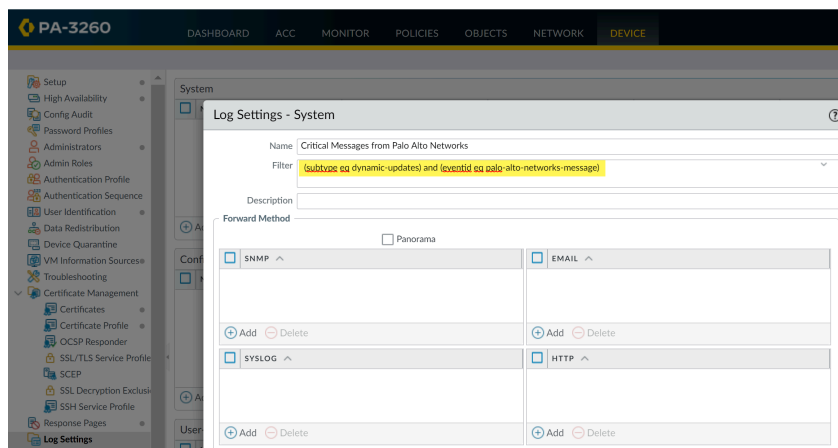
- Evasive: no
- Excessive Bandwidth Use: no
- Used by Malware: no
- Capable of File Transfer: no
- Has Known Vulnerabilities: yes

Classification:

- Category: networking
- Subcategory: remote-access
- Risk: 1

- Realice la [Configuración del reenvío de logs](#) para enviar alertas de contenido crítico de Palo Alto Networks a servicios externos que utiliza para supervisar la actividad de la red y el cortafuegos. Esto le permite garantizar que el personal adecuado reciba la notificación sobre problemas de contenido críticos, de modo que se puedan tomar las medidas necesarias. Las alertas críticas de actualización de contenido también se guardan como entradas en el log del sistema con Type (Tipo) y Event

(Evento): (subtype eq dynamic-updates) y (eventid eq palo-alto-networks-message).





PAN-OS 8.1.2 modificó el tipo de log para las alertas de contenido críticas de **general** a **dynamic-updates**. Si utiliza PAN-OS 8.1.0 o PAN-OS 8.1.1, el contenido crítico se registra como entradas de log del sistema con el siguiente Type (Tipo) y Event (Evento), y debe configurar el reenvío para estas alertas con el siguiente filtro: **(subtype eq general) y (eventid eq palo-alto-networks-message)**.

Infraestructura de red de entrega de contenido

Palo Alto Networks mantiene una infraestructura de red de entrega de contenidos (Content Delivery Network, CDN) para entregar actualizaciones de contenido a los cortafuegos de Palo Alto Networks. Estos cortafuegos acceden a los recursos web en la CDN para realizar diferentes funciones de identificación de contenido y aplicaciones.

La siguiente tabla enumera los recursos de Internet a los que accede el cortafuegos para una función o aplicación:

Recurso	URL	Direcciones estáticas (si se requiere un servidor estático)
Base de datos de aplicaciones	<ul style="list-style-type: none"> updates.paloaltonetworks.com (Global, excepto China continental) 	us-static.updates.paloaltonetworks.com
Base de datos amenazas/antivirus	<ul style="list-style-type: none"> updates.paloaltonetworks.cn (solo China continental) <p>Añada las siguientes URL a su lista de permisos de cortafuegos si su cortafuegos tiene acceso limitado a Internet:</p> <ul style="list-style-type: none"> downloads.paloaltonetworks.com:443 proditpdownloads.paloaltonetworks.com:443 <p>Como práctica recomendada, configure el servidor de actualizaciones para que acceda a updates.paloaltonetworks.com. Esto permite que el cortafuegos de Palo Alto Networks reciba actualizaciones de contenido del servidor más cercano en la infraestructura CDN.</p>	<p>Agregue los siguientes conjuntos de direcciones de servidor estático IPv4 o IPv6 a la lista de permitidos de su cortafuegos:</p> <ul style="list-style-type: none"> IPv4: 35.186.202.45:443 and 34.120.74.244:443 IPv6: [2600:1901:0:669::]:443 y [2600:1901:0:5162::]:443

Recurso	URL	Direcciones estáticas (si se requiere un servidor estático)
	<p> Si desea información de referencia adicional o está experimentando problemas de descarga de actualizaciones y de conectividad, consulte: https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u0000001UtRCAU</p> <p>La base de datos de Threat Vault de Palo Alto Networks incluye información sobre vulnerabilidades, exploits, virus y amenazas de spyware. Las funciones del cortafuegos, incluida la seguridad de DNS y el perfil de antivirus, utilizan el siguiente recurso para recuperar información de identificación de amenazas para crear excepciones:</p> <ul style="list-style-type: none"> data.threatvault.paloaltonetworks.com 	<p> Ambas direcciones IP proporcionadas para un tipo de protocolo determinado deben agregarse a la lista de permitidos para disfrutar de una funcionalidad adecuada.</p>
Filtrado de URL de PAN-DB Filtrado avanzado de URL	<p>*.urlcloud.paloaltonetworks.com</p> <p>Se resuelve como la dirección URL principal s0000.urlcloud.paloaltonetworks.com y, a continuación, se redirige al servidor regional más próximo:</p> <ul style="list-style-type: none"> s0100.urlcloud.paloaltonetworks.com s0200.urlcloud.paloaltonetworks.com s0300.urlcloud.paloaltonetworks.com s0500.urlcloud.paloaltonetworks.com 	Las direcciones IP estáticas no están disponibles. No obstante, puede resolver manualmente una dirección URL como una dirección IP y permitir el acceso a la dirección IP del servidor regional.
Servicios en la nube	<p>Se resuelve en hawkeye.services-edge.paloaltonetworks.com y luego se redirige al servidor regional más cercano:</p> <ul style="list-style-type: none"> EE. UU.: us.hawkeye.services-edge.paloaltonetworks.com Europa: eu.hawkeye.services-edge.paloaltonetworks.com Reino Unido: uk.hawkeye.services-edge.paloaltonetworks.com APAC: apac.hawkeye.services-edge.paloaltonetworks.com 	Las direcciones IP estáticas no están disponibles.

Recurso	URL	Direcciones estáticas (si se requiere un servidor estático)
DNS Security	<ul style="list-style-type: none"> Nube: dns.service.paloaltonetworks.com:443 Telemetría: io.dns.service.paloaltonetworks.com:443 <p>Al descargar una lista de permisos, dns.service.paloaltonetworks.com se resuelve en el siguiente servidor:</p> <ul style="list-style-type: none"> static.dns.service.paloaltonetworks.com:443 data.threatvault.paloaltonetworks.com (utilizado para crear excepciones DNS) 	Las direcciones IP estáticas no están disponibles.
Aprendizaje automático en línea basado en cortafuegos: <ul style="list-style-type: none"> ML en línea de URL Filtering WildFire Inline ML 	<ul style="list-style-type: none"> ml.service.paloaltonetworks.com:443 	Las direcciones IP estáticas no están disponibles.
WildFire	<ul style="list-style-type: none"> Nube (recuperación de informes): wildfire.paloaltonetworks.com:443 <p>Regiones de nube de WildFire:</p> <ul style="list-style-type: none"> Global: wildfire.paloaltonetworks.com Unión Europea: eu.wildfire.paloaltonetworks.com Japón: jp.wildfire.paloaltonetworks.com Singapur: sg.wildfire.paloaltonetworks.com Reino Unido: uk.wildfire.paloaltonetworks.com Canadá: ca.wildfire.paloaltonetworks.com Australia: au.wildfire.paloaltonetworks.com Alemania: de.wildfire.paloaltonetworks.com India: in.wildfire.paloaltonetworks.com 	Las direcciones IP estáticas no están disponibles.

Cambio de Panorama a una versión posterior

- > Instalación de actualizaciones de contenido y software para Panorama
- > Solución de problemas del cambio a versiones posteriores de Panorama
- > Implementación de actualizaciones de cortafuegos, recopiladores de logs y dispositivos WildFire utilizando Panorama

Instalación de actualizaciones de contenido y software para Panorama

Una suscripción válida a la asistencia técnica permite acceder a la imagen de software y las notas de versión de Panorama. Para aprovechar las correcciones y las mejoras de seguridad más recientes, actualice a la versión de software y contenido más reciente siguiendo las recomendaciones de implementación de su distribuidor o un ingeniero de sistemas de Palo Alto Networks. El procedimiento para instalar actualizaciones de software y contenido depende de si Panorama tiene una conexión directa a internet y si tiene una configuración de alta disponibilidad (high availability, HA).

- [Actualización de Panorama con una conexión a Internet](#)
- [Cambio de la versión de Panorama sin una conexión a Internet a una versión posterior](#)
- [Instalación automática de actualizaciones de contenido para Panorama sin conexión a Internet](#)
- [Actualización de Panorama en una configuración de HA](#)
- [Migración de los logs de Panorama al nuevo formato de log](#)
- [Actualización de Panorama para aumentar la capacidad de gestión de dispositivos](#)
- [Actualice Panorama y dispositivos gestionados en modo FIPS-CC](#)
- [Cambio a versiones anteriores a Panorama 11.0](#)

Actualización de Panorama con una conexión a Internet

Si Panorama™ tiene una conexión directa a internet, realice los siguientes pasos para instalar las actualizaciones de contenido y software de Panorama según sea necesario. Si Panorama se ejecuta en una configuración de alta disponibilidad (HA), actualice el software de Panorama en cada par (consulte [Actualización de Panorama en una configuración de HA](#)). Si está actualizando Panorama y los dispositivos gestionados en modo FIPS-CC a PAN-OS® 11.0 desde PAN-OS 10.2 o una versión anterior, debe realizar los pasos adicionales para restablecer el estado de conexión segura de los dispositivos en modo FIPS-CC si se agregan a la gestión de Panorama mientras se ejecuta una versión PAN-OS 10.2. Ver [Actualice Panorama y dispositivos gestionados en modo FIPS-CC](#) para obtener más detalles sobre la actualización de dispositivos Panorama y FIPS-CC en modo FIPS-CC.

Pasar el software del dispositivo virtual Panorama a una versión posterior no cambia el modo del sistema; cambiar al modo Panorama o al modo solo de gestión es una tarea manual que requiere configuraciones adicionales, como se describe cuando realiza la [Configuración del dispositivo virtual Panorama con recopiladores de logs locales](#).



Palo Alto Networks introdujo nuevos formatos de datos de logs en diferentes puntos de la ruta de actualización según la versión de PAN-OS desde la que se está actualizando.

- **Actualización de PAN-OS 8.1 a PAN-OS 9.0:** PAN-OS 9.0 introdujo un nuevo formato de datos de logs para recopiladores de logs dedicados y locales. En la ruta de actualización para PAN-OS 11.0, los datos de logs existentes se migran de forma automática al nuevo formato cuando actualiza de PAN-OS 8.1 a PAN-OS 9.0.
- **Actualización de PAN-OS 10.0 a PAN-OS 10.1:** PAN-OS 10.1 introdujo un nuevo formato de registro para recopiladores de registros dedicados y locales. En la ruta de actualización a PAN-OS 11.0, los logs generados en PAN-OS 8.1 o versiones anteriores ya no están disponibles. Esto incluye logs migrados como parte de la actualización a PAN-OS 9.0. Después de actualizar a PAN-OS 10.1, tiene la opción de recuperar y migrar estos logs al formato de log de PAN-OS 10.1.

Para evitar que se pierdan datos de logs, debe actualizar todos los recopiladores del grupo. Los logs no se reenvían ni se recopilan si no se ejecuta la misma versión de PAN-OS en todos ellos. Además, los datos de logs de los recopiladores del mismo grupo no se ven en las pestañas **ACC** ni **Monitor (Supervisión)** hasta que todos ejecuten la misma versión de PAN-OS. Por ejemplo, si el grupo tiene tres recopiladores de logs y actualiza dos de ellos, no se reenvía ningún log a ninguno de los recopiladores del grupo.

Antes de actualizar Panorama, consulte las [Notas de la versión](#) para obtener la versión de contenido mínima necesaria para PAN-OS® 11.0.

STEP 1 | Verifique que las actualizaciones que planea instalar sean apropiadas para su implementación de Panorama.



Palo Alto Networks recomienda encarecidamente que Panorama, los recopiladores de logs y todos los cortafuegos gestionados ejecuten la misma versión de publicación de contenido.

- ❑ Consulte las [notas de versión](#) para obtener la versión de contenido mínimas necesarias para una versión de software de Panorama. Si va a [actualizar los cortafuegos y recopiladores de logs](#) a una versión determinada, primero deberá actualizar Panorama a esa versión o una superior.
- ❑ Si el dispositivo virtual Panorama se ejecuta en un hipervisor, compruebe que la instancia cumple los [requisitos de configuración del dispositivo virtual Panorama](#).

STEP 2 | [Determine la ruta de actualización a PAN-OS 11.0.](#)

No puede omitir la instalación de ninguna versión de función publicada en la ruta de la versión de PAN-OS en ejecución a PAN-OS 11.0.

Revise [Lista de control para actualizar PAN-OS](#), los problemas conocidos y los cambios en el comportamiento predeterminado en las [Notas de la versión](#) y [Consideraciones sobre el cambio a versiones anteriores/posteriores de complementos de Panorama](#) para cada versión a través de la cual pase como parte de la ruta de actualización.

STEP 3 | Guarde una copia de seguridad del archivo de configuración actual de Panorama que puede usar para restaurar la configuración si tiene problemas con la actualización.



Aunque Panorama crea automáticamente una copia de seguridad de la configuración, se recomienda crear y almacenar de manera externa una copia de seguridad antes de la actualización.

1. [Inicie sesión en la interfaz web de Panorama.](#)
2. **Guarde la instantánea de configuración de Panorama con nombre (Panorama [Panorama] > Setup [Configuración] > Operations [Operaciones]),** introduzca un **Name (Nombre)** para la configuración y haga clic en **OK (Aceptar)**.
3. **Export named Panorama configuration snapshot (Exportar instantánea de configuración de Panorama con nombre),** seleccione el **Name (Nombre)** de la configuración que acaba de guardar, haga clic en **OK (Aceptar)** y guarde el archivo exportado en una ubicación que sea externa a Panorama.

STEP 4 | ([Prácticas recomendadas](#)) Si está aprovechando Cortex Data Lake (CDL), [instale el certificado de dispositivo Panorama.](#)

Panorama cambia de forma automática al uso del certificado de dispositivo para la autenticación con ingestión de CDL y endpoints de consulta al actualizar a PAN-OS 11.0.



Si no instala el certificado de dispositivo antes de pasar a la versión posterior PAN-OS 11.0, Panorama continúa utilizando el certificado de servicio de creación de logs existente para la autenticación.

STEP 5 | Instale las últimas actualizaciones de contenido.



Si Panorama no ejecuta las versiones de contenido mínimas requeridas para la versión de Panorama a la que desea actualizar, debe actualizar las versiones de contenido a la versión mínima (o posterior) antes de instalar las actualizaciones de software. Consulte las [notas de versión](#) para obtener la versión de contenido mínima necesaria para una versión de Panorama.



Palo Alto Networks® recomienda encarecidamente que Panorama, los recopiladores de logs y todos los cortafuegos gestionados ejecuten la misma versión de publicación de contenido. También se recomienda programar actualizaciones periódicas automáticas para que siempre se ejecuten las últimas versiones de contenido (consulte el paso 14).

1. Seleccione **Panorama (Panorama)**Dynamic Updates (Actualizaciones dinámicas) y **busque ahora** las actualizaciones más recientes. Si el valor de la columna Acción es **Download (Descargar)**, hay una actualización disponible.



Asegúrese de que Panorama ejecute la misma versión de publicación de contenido, pero no una posterior, que la que se ejecuta en los cortafuegos gestionados y los recopiladores de logs.

2. (Antes de actualizar la versión de lanzamiento de contenido en Panorama, asegúrese de [Actualizar el cortafuegos a PAN-OS 11.0 desde Panorama](#) y luego los recopiladores de logs

(consulte [Actualización de recopiladores de logs cuando Panorama está conectado a internet](#)) a la misma versión de lanzamiento de contenido (o posterior).

Si no necesita instalar actualizaciones de contenido en este momento, vaya al siguiente paso.

3. Instale las actualizaciones de contenido restantes que considere. Cuando se complete la instalación, la columna Instalado actualmente mostrará una marca de verificación.
 1. Haga clic en **Download (Descargar)** e **Install (Instalar)** para descargar e instalar la actualización de aplicaciones o de aplicaciones y amenazas. Independientemente de su suscripción, Panorama instala y solo necesita la actualización del contenido de Aplicaciones, no el contenido de Amenazas. Para obtener más información, consulte [Compatibilidad de versiones de Panorama, el recopilador de logs, el cortafuegos y WildFire](#).
 2. Haga clic en **Download (Descargar)** e **Install (Instalar)** para descargar e instalar otras actualizaciones (antivirus, WildFire® o filtrado de URL) una a la vez en cualquier secuencia.

STEP 6 | Seleccione **Panorama > Plugins (Complementos)** y **Download (Descargar)** para descargar la versión del complemento compatible con PAN-OS 11.0 para todos los complementos instalados actualmente en Panorama.

Consulte la [Matriz de compatibilidad](#) para la versión del complemento de Panorama compatible con la versión de PAN-OS 11.0 de destino.

Esto es necesario para actualizar Panorama de PAN-OS 10.2 a PAN-OS 11.0. La actualización a PAN-OS 11.0 se bloquea si no se descarga la versión de complemento compatible.



Los complementos descargados necesarios para actualizar a PAN-OS 11.0 se instalan automáticamente después de que Panorama se actualice correctamente a PAN-OS 11.0. Si un complemento descargado no se instala automáticamente, debe instalar manualmente el complemento afectado después de actualizar a PAN-OS 11.0.

STEP 7 | Actualice Panorama a las versiones de PAN-OS junto con la ruta de actualización a PAN-OS 11.0.

1. [Cambie Panorama con una conexión a Internet a la versión posterior PAN-OS 8.1.](#)
2. [Cambie Panorama con una conexión a Internet a la versión posterior PAN-OS 9.0.](#)

En PAN-OS 9.0, se incorporó un nuevo formato de log. Si se configura un recopilador de logs local, los logs se migran de forma automática al nuevo formato después de cambiar la versión de Panorama con éxito a la versión posterior PAN-OS 9.0.



No continúe en su ruta de actualización hasta que verifique que la migración automática de logs se haya completado con éxito.

3. [Cambie Panorama con una conexión a Internet a la versión posterior PAN-OS 9.1.](#)
4. [Cambie Panorama con una conexión a Internet a la versión posterior PAN-OS 10.0.](#)



(Panorama en modo heredado solamente) Descargue PAN-OS 10.0.0 y luego descargue e instale PAN-OS 10.0.8 o una versión posterior antes de continuar con la ruta de actualización.

Esto es necesario para conservar todos los logs almacenados en la partición de almacenamiento NFS. Algunos logs almacenados en la partición de almacenamiento NFS de Panorama en modo heredado se eliminan si instala PAN-OS 10.0.7 o una versión anterior de PAN-OS 10.0.

5. [Actualice Panorama con una conexión a Internet](#) a la versión posterior PAN-OS 10.1.

PAN-OS 10.1 incorpora un nuevo formato de log. En la actualización de PAN-OS 10.0 a PAN-OS 10.1, puede optar por migrar los logs generados en PAN-OS 8.1 o una versión anterior. De lo contrario, estos logs se eliminan de forma automática cuando se actualiza correctamente a PAN-OS 10.1. Durante la migración, no se ven los datos de logs en las pestañas ACC ni Monitor (Supervisión). Mientras se lleva a cabo la migración, los datos de log continúan reenviándose al recopilador de log correspondiente, pero el rendimiento puede verse afectado.



(Panorama en modo heredado solamente) Descargue PAN-OS 10.1.0 y luego descargue e instale PAN-OS 10.1.3 o una versión posterior.

Esto es necesario para conservar todos los logs almacenados en la partición de almacenamiento NFS. Algunos logs almacenados en la partición de almacenamiento NFS de Panorama en modo heredado se eliminan si instala PAN-OS 10.1.2 o una versión anterior de PAN-OS 10.1.

6. [Actualice Panorama con una conexión a Internet](#) a la versión posterior PAN-OS 10.2.

STEP 8 | Actualice Panorama a la versión posterior PAN-OS 11.0.

1. Seleccione **Panorama > Software** y haga clic en **Check Now (Buscar ahora)** para buscar las últimas versiones. Si hay disponible alguna versión de software, aparece **Download (Descargar)** en la columna Action (Acción).
2. Localice y **descargue** la imagen de PAN-OS 11.0.0. Después de una descarga correcta, la columna Acción cambia de **Download (Descargar)** a **Install (Instalar)** para instalar la imagen descargada.
3. Instale la imagen descargada y luego reinicie el dispositivo.
 1. Instalación de la imagen.
 2. Una vez que la instalación se realiza completamente, reinicie mediante uno de los siguientes métodos:
 - Si se le pide que reinicie, haga clic en **Yes (Sí)**. Si aparece un mensaje para iniciar sesión en el sistema de gestión de contenidos (content management system, CMS), pulse Intro sin escribir ningún nombre de usuario ni ninguna contraseña. Cuando aparezca el mensaje para iniciar sesión en Panorama, introduzca el nombre de usuario y contraseña que especificó durante la configuración inicial.
 - Si no se le solicita que reinicie, seleccione **Reboot Panorama (Reiniciar Panorama)** desde la sección Device Operations (Operaciones del dispositivo) (**Panorama > Setup [Configuración] > Operations [Operaciones]**)

STEP 9 | Después de reiniciar Panorama, verifique que las versiones del complemento Panorama sean compatibles con PAN-OS 11.0.

Debe verificar e instalar la versión del complemento de Panorama compatible con PAN-OS 11.0 después de actualizar Panorama correctamente. Consulte la [Matriz de compatibilidad](#) para obtener más información sobre los complementos de Panorama admitidos en PAN-OS 11.0.

1. [Inicie sesión en la interfaz web de Panorama](#) y revise el widget de Información general en el **Panel** para verificar que las versiones del complemento compatible con PAN-OS 11.0 se hayan instalado correctamente.

También puede [iniciar sesión en la CLI de Panorama](#) e introducir el comando `show plugins installed` (mostrar los complementos instalados) para ver la lista de complementos actualmente instalados.
2. Seleccione **Panorama > Plugins (Complementos)** y busque el complemento que no se instaló.
3. **Instale** la versión del complemento compatible con PAN-OS 11.0.
4. Repita los pasos anteriores hasta que todos los complementos instalados en Panorama ejecuten la versión compatible con PAN-OS 11.0.

STEP 10 | (Si el recopilador de logs local pertenece a un grupo de recopiladores) Actualice todos los demás recopiladores de logs del grupo.

- [Actualización de recopiladores de logs cuando Panorama está conectado a internet](#)
- [Actualización de recopiladores de logs cuando Panorama no está conectado a internet](#)

STEP 11 | (Panorama y dispositivos gestionados en modo FIPS-CC) [Actualice Panorama y dispositivos gestionados en modo FIPS-CC.](#)

Actualizar Panorama y los dispositivos gestionados en modo FIPS-CC requiere que restablezca el estado de conexión segura de los dispositivos en modo FIPS-CC, si se agregan a la gestión de Panorama mientras se ejecuta una versión de PAN-OS 11.0. Debe volver a incorporar los siguientes dispositivos gestionados a la gestión de Panorama:

- Dispositivos gestionados en modo FIPS-CC agregados a Panorama mediante la clave de autenticación de registro de dispositivo.
- Dispositivos gestionados en el modo de operación normal agregados a Panorama mediante la clave de autenticación de registro de dispositivo

No necesita volver a incorporar los dispositivos gestionados agregados a la gestión de Panorama mientras el dispositivo gestionado ejecutaba PAN-OS 10.0 o una versión anterior.

STEP 12 | (PAN-OS 10.2 y versiones posteriores) [Vuelva a generar o a importar todos los certificados para cumplir con el nivel de seguridad 2 de OpenSSL.](#)

Este paso es necesario si actualiza desde PAN-OS 10.1 o una versión anterior a PAN-OS 11.0. Omita este paso si actualiza desde PAN-OS 10.2 y ya volvió a generar o a importar los certificados.

Se requiere que todos los certificados cumplan con los siguientes requisitos mínimos:

- RSA de 2048 bits o superior, o ECDSA de 256 bits o superior
- Resumen de SHA256 o superior

Consulte la [Guía del administrador de PAN-OS](#) o la [Guía del administrador de Panorama](#) para obtener más información sobre cómo volver a generar o a importar los certificados.

STEP 13 | (Recomendado para el modo Panorama) [Aumente la memoria del dispositivo virtual Panorama a 64 GB.](#)

Después de actualizar correctamente el dispositivo virtual Panorama en el modo Panorama a PAN-OS 11.0, Palo Alto Networks recomienda aumentar la memoria del dispositivo virtual Panorama a 64 GB para cumplir con los [requisitos del sistema adicionales](#) y evitar cualquier problema relacionado con la creación de logs, la gestión y el rendimiento operativo relacionados con un dispositivo virtual Panorama con carencias.

STEP 14 | (Recomendación) Programe actualizaciones de contenido recurrentes y automáticas.



Panorama no sincroniza las actualizaciones de contenido programadas entre peers de HA. Debe llevar a cabo esta tarea en el Panorama activo y pasivo.

En la fila del encabezado de cada tipo de actualización [**Panorama > Dynamic Updates (Actualizaciones dinámicas)**], el **Schedule (Programa)** está inicialmente establecido en **None (Ninguno)**. Lleve a cabo los siguientes pasos para cada tipo de actualización.

1. Haga clic en **None (Ninguno)** y seleccione la frecuencia de actualización (**Recurrence [Frecuencia]**). Las opciones de frecuencia dependen del tipo de actualización.
2. Seleccione la acción de programación:
 - **Download And Install (Descargar e instalar) (recomendado)**: Panorama instala automáticamente las actualizaciones después de descargarlas.
Download Only (Solo descargar): debe instalar las actualizaciones manualmente después de que Panorama las descargue.
3. Basado en la [estrategia de mejores prácticas para la seguridad](#) de su organización, configure un periodo de tiempo (**Threshold [Umbral]**) tras el cual Panorama descarga la actualización que se había anunciado como disponible con anterioridad.
4. Haga clic en **OK (Aceptar)** para guardar los cambios.
5. Seleccione **Commit (Confirmar) > Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** sus cambios.

STEP 15 | (Solo DLP empresarial) [Edite la configuración de filtrado de datos de DLP empresarial](#) para reducir el **tamaño máximo de archivo** a 20 MB o menos.

Esto es necesario cuando se actualiza desde el complemento Panorama para DLP empresarial 3.0.3 o versiones posteriores a DLP empresarial 4.0.0, ya que esta versión del complemento no admite una [inspección de archivos de gran tamaño](#).

Cambio de la versión de Panorama sin una conexión a Internet a una versión posterior

Si Panorama™ no tiene una conexión directa a internet, realice los siguientes pasos para instalar las actualizaciones de contenido y software de Panorama según sea necesario. Si Panorama se implementa en una configuración de alta disponibilidad (HA), debe actualizar cada peer (consulte [Actualización de Panorama en una configuración de HA](#)). Si está actualizando Panorama y los dispositivos gestionados en modo FIPS-CC a PAN-OS 11.0 desde PAN-OS 10.2 o una versión anterior, debe realizar los pasos adicionales para restablecer el estado de conexión segura de los dispositivos en modo FIPS-CC si se agregan a la gestión de Panorama mientras se ejecuta una versión PAN-OS 10.2. Ver [Actualice Panorama y dispositivos gestionados en modo FIPS-CC](#) para obtener más detalles sobre la actualización de dispositivos Panorama y FIPS-CC en modo FIPS-CC.

Pasar el software del dispositivo virtual Panorama a una versión posterior no cambia el modo del sistema; cambiar al modo Panorama o al modo solo de gestión es una tarea manual que requiere configuraciones adicionales, como se describe cuando realiza la [Configuración del dispositivo virtual Panorama con recopiladores de logs locales](#).



Palo Alto Networks introdujo nuevos formatos de datos de logs en diferentes puntos de la ruta de actualización según la versión de PAN-OS desde la que se está actualizando.

- **Actualización de PAN-OS 8.1 a PAN-OS 9.0:** PAN-OS 9.0 introdujo un nuevo formato de datos de logs para recopiladores de logs dedicados y locales. En la ruta de actualización para PAN-OS 11.0, los datos de logs existentes se migran de forma automática al nuevo formato cuando actualiza de PAN-OS 8.1 a PAN-OS 9.0.
- **Actualización de PAN-OS 10.0 a PAN-OS 10.1:** PAN-OS 10.1 introdujo un nuevo formato de logs para recopiladores de logs dedicados y locales. En la ruta de actualización a PAN-OS 11.0, los logs generados en PAN-OS 8.1 o versiones anteriores ya no están disponibles. Esto incluye logs migrados como parte de la actualización a PAN-OS 9.0. Después de actualizar a PAN-OS 10.1, tiene la opción de recuperar y migrar estos logs al formato de logs de PAN-OS 10.1.

Para evitar que se pierdan datos de logs, debe actualizar todos los recopiladores del grupo. Los logs no se reenvían ni se recopilan si no se ejecuta la misma versión de PAN-OS en todos ellos. Además, los datos de logs de los recopiladores del mismo grupo no se ven en las pestañas **ACC** ni **Monitor (Supervisión)** hasta que todos ejecuten la misma versión de PAN-OS. Por ejemplo, si el grupo tiene tres recopiladores de logs y actualiza dos de ellos, no se reenvía ningún log a ninguno de los recopiladores del grupo.

Antes de actualizar Panorama, consulte las [Notas de la versión](#) para comprobar la versión de contenido mínima que exige PAN-OS® 11.0.

STEP 1 | Verifique que las actualizaciones que planea instalar sean apropiadas para su implementación de Panorama.



Palo Alto Networks recomienda encarecidamente que Panorama, los recopiladores de logs y todos los cortafuegos gestionados ejecuten la misma versión de publicación de contenido.

- ❑ Consulte las [notas de versión](#) para obtener la versión de contenido mínima que debe instalar para una versión de software de Panorama. Si va a [actualizar los cortafuegos y recopiladores de logs](#) a una versión determinada, primero deberá actualizar Panorama a esa versión o una superior.
- ❑ Si utiliza dispositivos virtuales Panorama, compruebe que la instancia cumple los [requisitos de configuración del dispositivo virtual Panorama](#).

STEP 2 | Determine la ruta de actualización a PAN-OS 11.0.

No puede omitir la instalación de ninguna versión de función publicada en la ruta de la versión de PAN-OS en ejecución a PAN-OS 11.0.

Revise [Lista de control para actualizar PAN-OS](#), los problemas conocidos y los cambios en el comportamiento predeterminado en las [Notas de la versión](#) y [Consideraciones sobre el cambio a versiones anteriores/posteriores de complementos de Panorama](#) para cada versión a través de la cual pase como parte de la ruta de actualización.

STEP 3 | Guarde una copia de seguridad del archivo de configuración actual de Panorama que puede usar para restaurar la configuración si tiene problemas con la actualización.



Aunque Panorama crea automáticamente una copia de seguridad de la configuración, se recomienda crear y almacenar de manera externa una copia de seguridad antes de la actualización.


1. [Inicie sesión en la interfaz web de Panorama.](#)
2. **Guarde la instantánea de configuración de Panorama con nombre (Panorama [Panorama] > Setup [Configuración] > Operations [Operaciones]),** introduzca un **Name (Nombre)** para la configuración y haga clic en **OK (Aceptar)**.
3. **Export named Panorama configuration snapshot (Exportar instantánea de configuración de Panorama con nombre),** seleccione el **Name (Nombre)** de la configuración que acaba de guardar, haga clic en **OK (Aceptar)** y guarde el archivo exportado en una ubicación que sea externa a Panorama.

STEP 4 | Descargue las actualizaciones de contenido a un host que pueda conectarse y cargar contenido en Panorama a través de SCP o HTTPS.


Si no necesita instalar actualizaciones de contenido en este momento, vaya al paso 6.

1. Use un host que tenga acceso a internet para iniciar sesión en el [Sitio web de atención al cliente de Palo Alto Networks](#).
2. Descargue las actualizaciones de contenido que considere:
 1. Haga clic en **Updates (Actualizaciones) > Dynamic Updates (Actualizaciones dinámicas)** en la sección Resources (Recursos).
 2. Haga clic en **Download (Descargar)** para descargar las actualizaciones de contenido adecuadas y guarde los archivos en el host. Lleve a cabo este paso para cada tipo de contenido que necesite actualizar.

STEP 5 | Instale las últimas actualizaciones de contenido.

-  *Debe instalar las actualizaciones de contenido antes que las actualizaciones de software y debe [Actualizar el cortafuegos a PAN-OS 11.0 desde Panorama](#) primero y luego [actualice los recopiladores de logs](#) antes de instalarlos en el servidor de gestión Panorama.*

Instale la actualización de aplicaciones o de aplicaciones y amenazas en primero lugar y, luego, las demás actualizaciones (de antivirus, WildFire® o URL Filtering), de una en una y en cualquier orden.

-  *Independientemente de si su suscripción incluye contenido de aplicaciones y amenazas, Panorama instala y necesita solo el contenido de aplicaciones. Para obtener más información, consulte [Compatibilidad de versiones de Panorama](#), [el recopilador de logs](#), [el cortafuegos](#) y [WildFire](#).*


[Inicie sesión en la interfaz web de Panorama](#) y realice los siguientes pasos para cada tipo de contenido:

1. Seleccione **Panorama (Panorama) > Dynamic Updates (Actualizaciones dinámicas)**.
2. Haga clic en **Upload (Cargar)**, seleccione el **Type (Tipo)** de contenido, seleccione **Browse (Examinar)** y vaya a la ubicación en el host donde descargó la actualización, seleccione la actualización y haga clic en **OK (Aceptar)**.
3. Seleccione **Install From File (Instalar desde archivo)**, seleccione el **Package Type (Tipo de paquete)** y haga clic en **OK (Aceptar)**.

STEP 6 | Cargue la versión del complemento compatible con PAN-OS 11.0 para todos los complementos actualmente instalados en Panorama.

Consulte la [Matriz de compatibilidad](#) para la versión del complemento de Panorama compatible con la versión de PAN-OS 11.0 de destino.

Esto es necesario para actualizar Panorama de PAN-OS 10.2 a PAN-OS 11.0. La actualización a PAN-OS 11.0 se bloquea si no se descarga la versión de complemento compatible.

-  *Los complementos descargados necesarios para actualizar a PAN-OS 11.0 se instalan automáticamente después de que Panorama se actualice correctamente a PAN-OS 11.0. Si un complemento descargado no se instala automáticamente, debe instalar manualmente el complemento afectado después de actualizar a PAN-OS 11.0*

1. Descargue la versión del complemento compatible con PAN-OS 11.0.
 1. Inicie sesión en el [Portal de soporte de Palo Alto Networks](#).
 2. Seleccione **Updates (Actualizaciones) > Software Updates (Actualizaciones de software)** y seleccione el complemento en el menú desplegable.
 3. **Descargue** la versión del complemento compatible con PAN-OS 10.2.
 4. Repita este paso para todos los complementos actualmente instalados en Panorama.
2. [Inicie sesión en la interfaz web de Panorama](#)
3. Seleccione **Panorama > Plugins (Complementos)** y **cargue** la versión del complemento que descargó en el paso anterior.

Repita este paso para todos los complementos actualmente instalados en Panorama.

STEP 7 | Actualice Panorama a las versiones de PAN-OS junto con la ruta de actualización a PAN-OS 10.2.

1. [Pase Panorama cuando no esté conectado a Internet a la versión posterior PAN-OS 8.1.](#)
2. [Pase Panorama cuando no esté conectado a Internet a la versión posterior PAN-OS 9.0.](#)

En PAN-OS 9.0, se incorporó un nuevo formato de log. Si se configura un recopilador de logs local, los logs se migran de forma automática al nuevo formato después de cambiar la versión de Panorama con éxito a la versión posterior PAN-OS 9.0.



No continúe en su ruta de actualización hasta que verifique que la migración automática de logs se haya completado con éxito.

3. [Pase Panorama cuando no esté conectado a Internet a la versión posterior PAN-OS 9.1.](#)
4. [Pase Panorama cuando no esté conectado a Internet a la versión posterior PAN-OS 10.0.](#)



(Panorama en modo heredado solamente) Descargue PAN-OS 10.0.0 y luego descargue e instale PAN-OS 10.0.8 o una versión posterior antes de continuar con la ruta de actualización.

Esto es necesario para conservar todos los logs almacenados en la partición de almacenamiento NFS. Algunos logs almacenados en la partición de almacenamiento NFS de Panorama en modo heredado se eliminan si instala PAN-OS 10.0.7 o una versión anterior de PAN-OS 10.0.

5. [Actualice Panorama cuando no esté conectado a Internet a la versión posterior PAN-OS 10.1.](#)

PAN-OS 10.1 incorpora un nuevo formato de log. En la actualización de PAN-OS 10.0 a PAN-OS 10.1, puede optar por migrar los logs generados en PAN-OS 8.1 o una versión anterior. De lo contrario, estos logs se eliminan de forma automática cuando se actualiza correctamente a PAN-OS 10.1. Durante la migración, no se ven los datos de logs en las pestañas ACC ni Monitor (Supervisión). Mientras se lleva a cabo la migración, los datos de log continúan reenviándose al recopilador de log correspondiente, pero el rendimiento puede verse afectado.



(Panorama en modo heredado solamente) Descargue PAN-OS 10.1.0 y luego descargue e instale PAN-OS 10.1.3 o una versión posterior.

Esto es necesario para conservar todos los logs almacenados en la partición de almacenamiento NFS. Algunos logs almacenados en la partición de almacenamiento NFS de Panorama en modo heredado se eliminan si instala PAN-OS 10.1.2 o una versión anterior de PAN-OS 10.1.

6. [Actualice Panorama cuando no esté conectado a Internet a la versión posterior PAN-OS 10.2.](#)

STEP 8 | Descargue la imagen de la versión PAN-OS 11.0 más reciente en un host que pueda conectarse y cargar contenido en Panorama a través de SCP o HTTPS.

1. Use un host con acceso a internet para iniciar sesión en el [sitio web de Atención al cliente de Palo Alto Networks](#).
2. Descargue las actualizaciones de software:
 1. En la página principal del sitio web de Atención al cliente de Palo Alto Networks, haga clic en **Updates (Actualizaciones) > Software Updates (Actualizaciones de software)**.
 2. Busque la imagen de versión específica del modelo para la versión más reciente de PAN-OS 11.0. Por ejemplo, para actualizar un dispositivo M-Series a Panorama 11.0.0, descargue la imagen **Panorama_m-11.0.0**; para actualizar un dispositivo virtual Panorama a Panorama 11.0.0, descargue la imagen **Panorama_pc-11.0.0**.



*Puede localizar rápidamente imágenes de Panorama seleccionando **Panorama M Images (Imágenes M de Panorama)** (Dispositivos de la serie M) o **Panorama Updates (Actualizaciones de Panorama)** (dispositivos virtuales) del menú desplegable **Filter By (Filtrado por)**.*

3. Haga clic en el nombre de archivo y guarde el archivo en el host.

STEP 9 | Actualice Panorama a la versión PAN-OS 11.0.

1. [Inicie sesión en la interfaz web de Panorama](#).
2. Seleccione **Panorama (Panorama) > Software (Software)** y **cargue** la imagen PAN-OS 11.0 que descargó en el paso anterior.
3. Seleccione **Browse (Examinar)** para navegar hasta la ubicación del host donde descargó la actualización, seleccione la actualización, seleccione **Sync to peer (Sincronizar en el peer)** si Panorama tiene una configuración de HA (para enviar la imagen de software al peer secundario) y haga clic en **OK (Aceptar)**.
4. Instale la imagen del software y reinicie.

Para una configuración de HA, [Actualización de Panorama en una configuración de HA](#); de lo contrario:

1. **instale** la imagen cargada.
2. Después de completar la instalación correctamente, reinicie usando uno de los siguientes métodos:
 - Si se le pide que reinicie, haga clic en **Yes (Sí)**. Si aparece un mensaje para iniciar sesión en el sistema de gestión de contenidos (content management system, CMS), pulse Intro sin escribir ningún nombre de usuario ni ninguna contraseña. Cuando aparezca el mensaje para iniciar sesión en Panorama, introduzca el nombre de usuario y contraseña que especificó durante la configuración inicial.
 - Si no se le solicita que reinicie, seleccione **Reboot Panorama (Reiniciar Panorama)** desde la sección Device Operations (Operaciones del dispositivo) (**Panorama > Setup [Configuración] > Operations [Operaciones]**)

STEP 10 | Después de reiniciar Panorama, verifique que las versiones del complemento Panorama sean compatibles con PAN-OS 11.0.

Debe verificar e instalar la versión del complemento de Panorama compatible con PAN-OS 11.0 después de actualizar Panorama correctamente. Consulte la [Matriz de compatibilidad](#) para obtener más información sobre los complementos de Panorama admitidos en PAN-OS 11.0.

1. [Inicie sesión en la interfaz web de Panorama](#) y revise el widget de Información general en el **Panel** para verificar que las versiones del complemento compatible con PAN-OS 11.0 se hayan instalado correctamente.
También puede [iniciar sesión en la CLI de Panorama](#) e introducir el comando `show plugins installed` (mostrar los complementos instalados) para ver la lista de complementos actualmente instalados.
2. Seleccione **Panorama > Plugins (Complementos)** y busque el complemento que no se instaló.
3. **Instale** la versión del complemento compatible con PAN-OS 11.0.
4. Repita los pasos anteriores hasta que todos los complementos instalados en Panorama ejecuten la versión compatible con PAN-OS 11.0.

STEP 11 | (Si el recopilador de logs local pertenece a un grupo de recopiladores) Actualice todos los demás recopiladores de logs del grupo.

- [Actualización de recopiladores de logs cuando Panorama está conectado a internet](#)
- [Actualización de recopiladores de logs cuando Panorama no está conectado a internet](#)

STEP 12 | (Panorama y dispositivos gestionados en modo FIPS-CC) [Actualice Panorama y dispositivos gestionados en modo FIPS-CC.](#)

Actualizar Panorama y los dispositivos gestionados en modo FIPS-CC requiere que restablezca el estado de conexión segura de los dispositivos en modo FIPS-CC, si se agregan a la gestión de Panorama mientras se ejecuta una versión de PAN-OS 11.0. Debe volver a incorporar los siguientes dispositivos gestionados a la gestión de Panorama:

- Dispositivos gestionados en modo FIPS-CC agregados a Panorama mediante la clave de autenticación de registro de dispositivo.
- Dispositivos gestionados en el modo de operación normal agregados a Panorama mediante la clave de autenticación de registro de dispositivo

No necesita volver a incorporar los dispositivos gestionados agregados a la gestión de Panorama mientras el dispositivo gestionado ejecutaba PAN-OS 10.0 o una versión anterior.

STEP 13 | (PAN-OS 10.2 y versiones posteriores) Vuelva a generar o a importar todos los certificados para cumplir con el nivel de seguridad 2 de OpenSSL.

Este paso es necesario si actualiza desde PAN-OS 10.1 o una versión anterior a PAN-OS 11.0. Omita este paso si actualiza desde PAN-OS 10.2 y ya volvió a generar o a importar los certificados.

Se requiere que todos los certificados cumplan con los siguientes requisitos mínimos:

- RSA de 2048 bits o superior, o ECDSA de 256 bits o superior
- Resumen de SHA256 o superior

Consulte la [Guía del administrador de PAN-OS](#) o la [Guía del administrador de Panorama](#) para obtener más información sobre cómo volver a generar o a importar los certificados.


STEP 14 | (Recomendado para el modo Panorama) Aumente la memoria del dispositivo virtual Panorama a 64 GB.

Después de actualizar correctamente el dispositivo virtual Panorama en el modo Panorama a PAN-OS 11.0, Palo Alto Networks recomienda aumentar la memoria del dispositivo virtual Panorama a 64 GB para cumplir con los [requisitos del sistema adicionales](#) y evitar cualquier problema relacionado con la creación de logs, la gestión y el rendimiento operativo relacionados con un dispositivo virtual Panorama con carencias.

Instalación automática de actualizaciones de contenido para Panorama sin conexión a Internet

Descargue de forma automática actualizaciones de contenido para cortafuegos, recopiladores de logs y dispositivos WildFire® en redes con espacios abiertos donde el servidor de gestión Panorama™, los cortafuegos gestionados, los recopiladores de logs y los dispositivos WildFire no están conectados a Internet. Para lograr esto, debe implementar un Panorama adicional con acceso a Internet y un servidor SCP. Después de implementar Panorama con acceso a Internet, configure Panorama conectado a Internet para descargar de forma automática actualizaciones de contenido al servidor SCP. Desde el servidor SCP, Panorama con espacios abiertos está configurado para descargar e instalar de forma automática actualizaciones de contenido según su programación de actualizaciones de contenido. Panorama genera un log del sistema cuando Panorama con acceso a Internet descarga actualizaciones de contenido al servidor SCP o cuando Panorama con espacios abiertos descarga e instala actualizaciones de contenido desde el servidor SCP.


Solo se admiten los siguientes programas de actualización de contenido desde un dispositivo Panorama conectado a Internet a un Panorama sin una conexión a Internet:

-  *No manipule ni cambie el nombre del archivo de contenido después de descargarlo con éxito al servidor SCP. Panorama no puede descargar e instalar actualizaciones de contenido con nombres de archivo alterados. Además, para que la actualización de contenido automática tenga éxito, debe asegurarse de que haya suficiente espacio de disco en el servidor SCP, que el servidor SCP esté ejecutándose cuando una descarga esté a punto de comenzar, y que ambos dispositivos Panorama estén encendidos y no a mitad de un procedimiento de reinicio.*

En este ejemplo, se muestra cómo configurar las actualizaciones de contenido automáticas para las actualizaciones de aplicaciones y amenazas.

STEP 1 | Implemente un servidor SCP.

Actualizaciones de contenido para cortafuegos gestionados, recopiladores de logs y descargas de dispositivos WildFire desde el dispositivo Panorama conectado a Internet. El dispositivo Panorama con espacios abiertos descarga las actualizaciones de contenido del servidor SCP y, luego, instala las actualizaciones en los cortafuegos gestionados, los dispositivos WildFire y los recopiladores de logs.

-  *Cuando crea el directorio de carpetas para actualizaciones de contenido, es recomendable crear una carpeta para cada tipo de tipo de actualización de contenido. Este es el inconveniente que implica gestionar un gran volumen de actualizaciones de contenido y se reduce la posibilidad de eliminar actualizaciones de contenido que no deben eliminarse del servidor SCP.*

STEP 2 | Implemente el dispositivo Panorama conectado a Internet.

Este dispositivo Panorama se comunica con el servidor de actualización de Palo Alto Networks y descarga las actualizaciones de contenido al servidor SCP.

1. Configure el servidor de gestión de Panorama.
 - [Configuración del dispositivo de la serie M](#)
 - [Configuración del dispositivo virtual Panorama](#)
2. Realice la configuración inicial de Panorama.
 - [Realización de la configuración inicial del dispositivo de la serie M](#)
 - [Realización de la configuración inicial del dispositivo virtual Panorama](#)

STEP 3 | Implemente el dispositivo Panorama sin una conexión a Internet.

Este dispositivo Panorama se comunica con el servidor SCP para descargar e instalar actualizaciones de contenido en cortafuegos gestionados, recopiladores de logs y dispositivos WildFire.

1. Configure el servidor de gestión de Panorama.
 - [Configuración del dispositivo de la serie M](#)
 - [Configuración del dispositivo virtual Panorama](#)
2. Realice la configuración inicial de Panorama.
 - [Realización de la configuración inicial del dispositivo de la serie M](#)
 - [Realización de la configuración inicial del dispositivo virtual Panorama](#)
3. Añada sus cortafuegos gestionados, recopiladores de logs y dispositivos WildFire.
 - [Cómo añadir un cortafuegos como dispositivo gestionado](#)
 - [Configuración de recopiladores gestionados](#)
 - [Agregue un dispositivo WildFire independientes para gestionar con Panorama](#)

STEP 4 | Configure el dispositivo Panorama conectado a Internet para descargar actualizaciones de contenido en su servidor SCP.

1. [Inicio de sesión en la interfaz web de Panorama.](#)
2. Cree un perfil de servidor SCP.
 1. Seleccione **Panorama > Server Profiles (Perfiles de servidor) > SCP** y luego **Add (Añadir)** para añadir un nuevo perfil de servidor HTTP.
 2. Introduzca un nombre descriptivo en **Nombre** para el perfil de servidor SCP.
 3. Especifique la dirección IP de **servidor SCP**.
 4. Introduzca el **puerto**.
 5. Especifique el **nombre de usuario** del servidor SCP.
 6. Especifique la **contraseña** del servidor SCP y seleccione **Confirm Password (Confirmar contraseña)**.
 7. Haga clic en **OK (Aceptar)** para guardar los cambios.

3. Cree una programación de actualización de contenido para descargar con regularidad actualizaciones de contenido al servidor SCP.

Debe crear una programación para cada tipo de actualización de contenido que desee descargar e instalar de forma automática en los cortafuegos gestionados, recopiladores de logs y dispositivos WildFire.

1. Seleccione **Panorama (Panorama) > Device Deployment (Implementación del dispositivo) > Dynamic Updates (Actualizaciones dinámicas)**, seleccione **Schedules (Programaciones)** y añada una programación de actualizaciones de contenido.
2. Especifique un **nombre** descriptivo para la programación de actualizaciones de contenido.
3. En **Download Source (Origen de descarga)**, seleccione **Update Server (Servidor de actualizaciones)**.
4. Seleccione el **tipo** de actualización de contenido.
5. Seleccione **Recurrence (Recurrencia)** para establecer el intervalo en el que Panorama verifica en el servidor de actualización de Palo Alto Networks si hay nuevas actualizaciones de contenido.



Para configurar un programa de recurrencia más preciso, especifique la cantidad de minutos después del intervalo de recurrencia seleccionado. Si tiene varias actualizaciones de contenido programadas para descargar mediante el mismo intervalo de recurrencia, escalónelas para evitar sobrecargar el servidor Panorama y SCP.

6. En **Action (Acción)**, seleccione **Download And SCP (Descarga y SCP)**.
7. Seleccione el **perfil SCP** que configuró en el paso anterior.
8. Escriba la **ruta de acceso de SCP** para el tipo de actualización de contenido.
9. **(Opcional)** Ingrese el **umbral** en horas para las actualizaciones de contenido. Panorama descarga solo actualizaciones de contenido que tengan esta cantidad de horas (o más).
10. Haga clic en **OK (Aceptar)** para guardar los cambios.

Schedule

Name

Pano29-APT-Download-SCP

☐ Disabled

Download Source

☒ Update Server ☐ SCP

Type

App and Threat

Recurrence

Every 30 Mins

Minutes Past Half-Hour

2

☐ Disable new applications after installation

Action

Download And SCP

SCP Profile

SCP21

SCP Path

~/APT

Threshold (hours)

3

Content must be at least this many hours old for any action to be taken

Allow Extra Time to Review New App-IDs

Set the amount of time the firewall waits before installing content updates that contain new App-IDs. You can use this wait period to assess and adjust your security policy based on the new App-IDs.

New App-ID Threshold (hours)

[1 - 336]

OK

Cancel

4. Haga clic en **Commit (Confirmar)** para compilar los cambios.

STEP 5 | Configure Panorama con espacios abiertos para descargar actualizaciones de contenido del servidor SCP y, a continuación, instale las actualizaciones en sus cortafuegos gestionados, recopiladores de logs y dispositivos WildFire.

1. [Inicio de sesión en la interfaz web de Panorama.](#)
2. Cree un perfil de servidor SCP.
 1. Seleccione **Panorama > Server Profiles (Perfiles de servidor) > SCP** y luego **Add (Añadir)** para añadir un nuevo perfil de servidor HTTP.
 2. Introduzca un nombre descriptivo en **Nombre** para el perfil de servidor SCP.
 3. Especifique la dirección IP de **servidor SCP**.
 4. Introduzca el **puerto**.
 5. Especifique el **nombre de usuario** del servidor SCP.
 6. Especifique la **contraseña** del servidor SCP y seleccione **Confirm Password (Confirmar contraseña)**.
 7. Haga clic en **OK (Aceptar)** para guardar los cambios.

SCP Server Profile

Name: SCP21

Server:

Port: 22

User Name: admin

Password:

Confirm Password:

OK Cancel

3. Cree una programación de actualizaciones de contenido para descargar e instalar con regularidad actualizaciones de contenido del servidor SCP.

Debe crear una programación para cada tipo de actualización de contenido que desee descargar e instalar de forma automática en los cortafuegos gestionados, recopiladores de logs y dispositivos WildFire.

1. Seleccione **Panorama (Panorama) > Device Deployment (Implementación del dispositivo) > Dynamic Updates (Actualizaciones dinámicas)**, seleccione **Schedules (Programaciones)** y **añada** una programación de actualizaciones de contenido.
2. Especifique un **nombre** descriptivo para la programación de actualizaciones de contenido.
3. En **Download Source (Origen de descarga)**, seleccione **SCP**.
4. Seleccione el **perfil SCP** que configuró en el paso anterior.
5. Escriba la **ruta de acceso de SCP** para el tipo de actualización de contenido.
6. Seleccione el **tipo** de actualización de contenido.
7. Seleccione **Recurrence (Recurrencia)** para establecer el intervalo en el que Panorama verifica en el servidor de actualización de Palo Alto Networks si hay nuevas actualizaciones de contenido.



Para configurar un programa de recurrencia más preciso, especifique la cantidad de minutos después del intervalo de recurrencia seleccionado. Si tiene varias actualizaciones de contenido programadas para descargar mediante el mismo intervalo de recurrencia, escalónelas para evitar sobrecargar el servidor Panorama y SCP.

8. En **Action (Acción)**, seleccione **Download (Descargar)** o **Download And Install (Descargar e instalar)**.



Solo se admiten **Download (Descargar)** y **Download and Install (Descargar e instalar)** cuando **Download Source (Origen de descarga)** es **SCP**.

Si selecciona **Download (Descargar)**, debe iniciar de forma manual la instalación de la actualización de contenido en sus cortafuegos gestionados.

9. Seleccione los **dispositivos** en los que instalar las actualizaciones de contenido.
10. (Opcional) Ingrese el **umbral** en horas para las actualizaciones de contenido. Panorama descarga solo actualizaciones de contenido que tengan esta cantidad de horas (o más).
11. Haga clic en **OK (Aceptar)** para guardar los cambios.

Schedule

Name

SCP21-PRA-APT

☐ Disabled

Download Source

☐ Update Server
 ☒ SCP

SCP Profile

SCP21

SCP Path

~/APT

Type

App and Threat

Recurrence

Hourly

Minutes Past Hour

25

☐ Disable new applications after installation

Action

Download And Install

Devices

FILTERS

☐ Platforms

☐ PA-850 (1)
 ☐ PA-3250 (1)
 ☐ PA-VM (5)

☐ Device Groups

☐ DG-VM (5)
 ☐ DG2vsys (2)
 ☐ DGvsys3 (1)

☐ Tags

7 items

☒ PA-850-8
 ☒ PA-3250-5
 ☒ PA-VM-6
 ☒ PA-VM-73
 ☒ PA-VM-92
 ☒ PA-VM-95
 ☒ PA-VM-96

☐ Group HA Peers

Threshold (hours)

[1 - 336]

Content must be at least this many hours old for any action to be taken

Allow Extra Time to Review New App-IDs

Set the amount of time the firewall waits before installing content updates that contain new App-IDs. You can use this wait period to assess and adjust your security policy based on the new App-IDs.

New App-ID Threshold (hours)

[1 - 336]

4. **Commit (Confirmar)** los cambios.

Actualización de Panorama en una configuración de HA

Para garantizar una conmutación por error sin fisuras cuando actualiza el software de Panorama en una configuración de alta disponibilidad (HA), los peers activo y pasivo de Panorama deben ejecutar la misma

versión de Panorama con la misma versión de la base de datos de Aplicaciones. El siguiente ejemplo describe cómo actualizar un par de HA (peer activo es Primary_A y peer pasivo es Secondary_B).

Si está actualizando Panorama y los dispositivos gestionados en modo FIPS-CC a PAN-OS 11.0 desde PAN-OS 10.2 o una versión anterior, debe realizar los pasos adicionales para restablecer el estado de conexión segura de los dispositivos en modo FIPS-CC si se agregan a la gestión de Panorama mientras se ejecuta una versión PAN-OS 10.2. Ver [Actualice Panorama y dispositivos gestionados en modo FIPS-CC](#) para obtener más detalles sobre la actualización de dispositivos Panorama y FIPS-CC en modo FIPS-CC.

Antes de actualizar Panorama, consulte las [Notas de la versión](#) para obtener la versión de contenido mínima necesaria para PAN-OS 11.0.

STEP 1 | Actualice el software de Panorama en peer Secondary_B (pasivo).

Realice una de las siguientes tareas en el peer Secondary_B:

- [Actualización de Panorama con una conexión a Internet](#)
- [Cambio de la versión de Panorama sin una conexión a Internet a una versión posterior](#)

Después de la actualización, este Panorama pasa a un estado no funcional porque la versión de los peers ya no coincide con la versión del software.

STEP 2 | (Prácticas recomendadas) Si está aprovechando Cortex Data Lake (CDL), [instale el certificado de dispositivo Panorama](#) en cada par de HA de Panorama.

Panorama cambia de forma automática al uso del certificado de dispositivo para la autenticación con ingestión de CDL y endpoints de consulta al actualizar a PAN-OS 11.0.



Si no instala el certificado de dispositivo antes de actualizar a PAN-OS 11.0, Panorama continúa utilizando los certificados de servicio de creación de logs existentes para la autenticación.

STEP 3 | Suspenda el peer Primary_A para forzar una conmutación por error.

En el peer Primary_A:

1. En la sección **Operational Commands (Comandos operativos)** (**Panorama > High Availability (Alta disponibilidad)**), haga clic en **Suspend local Panorama (Suspend local Panorama)**.
2. Verifique que el estado es suspendido **suspended** (se muestra en la esquina inferior derecha de la interfaz web).

La conmutación por fallo resultante debe hacer que el peer Secondary_B haga la transición al estado **active**.

STEP 4 | Actualice el software de Panorama en el peer Primary_A (actualmente pasivo).

Realice una de las siguientes tareas en el peer Primary_A:

- [Actualización de Panorama con una conexión a Internet](#)
- [Cambio de la versión de Panorama sin una conexión a Internet a una versión posterior](#)

Después de reiniciar, el peer Primary_A está todavía en estado pasivo. A continuación, como la preferencia está habilitada de forma predeterminada, Primary_A cambia automáticamente al estado activo y el peer Secondary_B vuelve al estado pasivo.

Si deshabilitó la preferencia, [restaure el Panorama principal al estado activo](#) de forma manual.

STEP 5 | Verifique que ambos peers ahora estén ejecutando cualquier versión de lanzamiento de contenido recién instalada y la versión de Panorama recién instalada.

En el **Dashboard (Panel)** de cada peer de Panorama, compruebe la versión de software de Panorama y la versión de la aplicación, y confirme que son iguales en ambos peers y que la configuración en ejecución está sincronizada.

STEP 6 | [\(Solo con recopiladores de logs locales pertenecientes a un grupo de recopiladores\)](#) Actualice todos los demás recopiladores de logs del grupo.

- [Actualización de recopiladores de logs cuando Panorama está conectado a internet](#)
- [Actualización de recopiladores de logs cuando Panorama no está conectado a internet](#)

STEP 7 | [\(Panorama y dispositivos gestionados en modo FIPS-CC\)](#) [Actualice Panorama y dispositivos gestionados en modo FIPS-CC.](#)

Actualizar Panorama y los dispositivos gestionados en modo FIPS-CC requiere que restablezca el estado de conexión segura de los dispositivos en modo FIPS-CC, si se agregan a la gestión de Panorama mientras se ejecuta una versión de PAN-OS 11.0. Debe volver a incorporar los siguientes dispositivos gestionados a la gestión de Panorama:

- Dispositivos gestionados en modo FIPS-CC agregados a Panorama mediante la clave de autenticación de registro de dispositivo.
- Dispositivos gestionados en el modo de operación normal agregados a Panorama mediante la clave de autenticación de registro de dispositivo

No necesita volver a incorporar los dispositivos gestionados agregados a la gestión de Panorama mientras el dispositivo gestionado ejecutaba PAN-OS 10.0 o una versión anterior.

STEP 8 | [\(PAN-OS 10.2 y versiones posteriores\)](#) Vuelva a generar o a importar todos los certificados para cumplir con el nivel de seguridad 2 de OpenSSL.

Este paso es necesario si actualiza desde PAN-OS 10.1 o una versión anterior a PAN-OS 11.0. Omita este paso si actualiza desde PAN-OS 10.2 y ya volvió a generar o a importar los certificados.

Se requiere que todos los certificados cumplan con los siguientes requisitos mínimos:

- RSA de 2048 bits o superior, o ECDSA de 256 bits o superior
- Resumen de SHA256 o superior

Consulte la [Guía del administrador de PAN-OS](#) o la [Guía del administrador de Panorama](#) para obtener más información sobre cómo volver a generar o a importar los certificados.

STEP 9 | (Recomendado para el modo Panorama) **Aumente la memoria del dispositivo virtual Panorama a 64 GB.**

Después de actualizar correctamente el dispositivo virtual Panorama en el modo Panorama a PAN-OS 11.0, Palo Alto Networks recomienda aumentar la memoria del dispositivo virtual Panorama a 64 GB para cumplir con los [requisitos del sistema adicionales](#) y evitar cualquier problema relacionado con la creación de logs, la gestión y el rendimiento operativo relacionados con un dispositivo virtual Panorama con carencias.

Migración de los logs de Panorama al nuevo formato de log

Después de actualizar a una versión de Panorama 8.0 o posterior, los recopiladores de logs de Panorama utilizan un nuevo formato de almacenamiento de logs. Debido a que Panorama no puede generar informes o datos ACC de logs en el formato de log pre-8.0-release después de que actualice, debe migrar los logs existentes tan pronto como actualice Panorama y sus Recopiladores de logs de un PAN-OS® 7.1 o una versión anterior a una versión PAN-OS 8.0 o posterior, y debe hacerlo antes de actualizar sus cortafuegos gestionados. Panorama continuará recopilando logs de dispositivos gestionados durante la migración de logs, pero almacenará los logs entrantes en el nuevo formato de log después de actualizar a PAN-OS 8.0 o una versión posterior. Por este motivo, verá solo datos parciales en el ACC y en Informes hasta que Panorama complete el proceso de migración de logs.



La migración de logs al nuevo formato es una tarea única que debe realizar al actualizar a PAN-OS 8.0 (o cuando actualiza a PAN-OS 8.0 o a una versión posterior como parte de su ruta de actualización); no necesita realizar esta migración nuevamente cuando actualice a una versión posterior de PAN-OS.

El tiempo que Panorama requiere para completar el proceso de migración de logs depende del volumen de los nuevos logs que se escriben en Panorama y del tamaño de la base de datos de logs que está migrando. Debido a que la migración de log es un proceso intensivo de CPU, comience la migración durante un tiempo en el que la velocidad de logging sea menor. Es posible detener la migración durante las horas punta, si observa que las tasas de utilización de la CPU son altas, y reanudarla cuando la tasa de logs entrantes sea menor.

Después de realizar la [Instalación de actualizaciones de contenido y software de Panorama](#) y actualizar los recopiladores de logs, migre los logs de la siguiente manera:

- Visualice la tasa de entrada de logs.

Para obtener los mejores resultados, inicie la migración de logs cuando la tasa de logs entrantes sea baja. Para verificar la velocidad, ejecute el siguiente comando desde la CLI del Recopilador de logs:

```
admin@FC-M500-1> debug log-collector log-collection-stats show incoming-logs
```



Se espera una alta utilización de la CPU (cerca del 100%) durante la migración de logs y las operaciones continuarán realizándose con normalidad. La migración de logs se acelera a favor de los logs entrantes y otros procesos en caso de la contención de recursos.

- Comience a migrar los logs en cada Recopilador de logs al nuevo formato.

Para empezar la migración, introduzca el siguiente comando en la CLI de cada recopilador de logs.

```
admin@FC-M500-1> request logdb migrate lc serial-number <ser_num>
start
```

- Vea el estado de la migración de logs para estimar la cantidad de tiempo que le tomará finalizar la migración de todos los logs existentes al nuevo formato.

```
admin@FC-M500-1> request logdb migrate lc serial-number <ser_num>
status Slot: all Migration State: Porcentaje en curso completo:
0,04 Tiempo restante estimado: 451 horas 47 minutos
```

- Detenga el proceso de migración de log.

Para detener temporalmente el proceso de migración de logs, introduzca el siguiente comando en la CLI de los recopiladores de logs:

```
admin@FC-M500-1 request logdb migrate lc serial-number <ser_num>
stop
```

Actualización de Panorama para aumentar la capacidad de gestión de dispositivos

Actualice a PAN-OS 9.1 o versiones posteriores para usar la licencia de gestión de dispositivos existente en el dispositivo M-600 para administrar hasta 5000 cortafuegos o el dispositivo virtual Panorama™ para hasta 2500 cortafuegos.

STEP 1 | [Aumente las CPU y la memoria para el dispositivo virtual Panorama](#) si el dispositivo virtual Panorama aún no cumple los requisitos mínimos de recursos para una mayor administración de dispositivos.

Revise los [requisitos de capacidad para una mayor administración de dispositivos](#) a fin de verificar si el dispositivo virtual Panorama existente cumple los requisitos mínimos antes de cambiar a una versión posterior.

STEP 2 | [Inicio de sesión en la CLI de Panorama.](#)

STEP 3 | Si el servidor de gestión de Panorama no está todavía en el modo de solo gestión, cámbielo.

- [\(Solo en el caso de dispositivos M-600\)](#) Comience por el paso 5 para [configurar un dispositivo M-Series en modo solo administración](#).

O

- [Configure un dispositivo virtual Panorama en modo solo administración.](#)

STEP 4 | [Inicie sesión en la interfaz web de Panorama.](#)

STEP 5 | Actualice el servidor de gestión de Panorama.

- [Actualización de Panorama con una conexión a Internet.](#)
- [Cambio de la versión de Panorama sin una conexión a Internet a una versión posterior.](#)
- [Actualización de Panorama en una configuración de HA.](#)

STEP 6 | Seleccione **Panorama > Licenses (Licencias)** y verifique si está activada la licencia de gestión de dispositivos.

Device Management License	
Date Issued	January 22, 2020
Date Expires	Never
Description	Device management license to manage up to 1000 devices



*Si ha activado la licencia de gestión de dispositivos y, a continuación, ha actualizado a PAN-OS 9.1 o versiones posteriores, puede gestionar hasta 5000 cortafuegos con un dispositivo M-600 y hasta 2500 cortafuegos con un dispositivo virtual Panorama a pesar de que la descripción indique **Device management license to manage up to 1000 devices** (Licencia para gestionar hasta 1000 dispositivos).*

Actualice Panorama y dispositivos gestionados en modo FIPS-CC

En una actualización exitosa a PAN-OS 11.0, todos los dispositivos gestionados en modo FIPS-CC y cualquier dispositivo gestionado agregado a Panorama mientras el dispositivo ejecutaba una versión de PAN-OS 11.0 deben volver a incorporarse a la gestión de Panorama. Esto requiere que restablezca el estado de conexión segura para Panorama en modo FIPS-CC y para cualquier dispositivo gestionado en modo FIPS-CC. Después de restablecer el estado de conexión segura, debe agregar el cortafuegos, el recopilador de logs y el dispositivo WildFire agregados a Panorama [mediante la clave de autenticación de registro del dispositivo](#) nuevamente a la gestión de Panorama. Este procedimiento no es necesario y no afecta a los dispositivos gestionados agregados a Panorama mientras se ejecuta PAN-OS 10.0 o una versión anterior. Esto es necesario para todos [los modelos Panorama](#) admitidos y [los modelos de hardware de cortafuegos de nueva generación y VM-Series](#) en modo FIPS-CC.

STEP 1 | Cree una lista de los dispositivos gestionados en modo FIPS-CC y cualquier dispositivo gestionado agregado a Panorama mediante la clave de autenticación de registro del dispositivo. Esto lo ayudará más adelante a concentrar sus esfuerzos cuando vuelva a incorporar sus dispositivos gestionados a la gestión de Panorama.

STEP 2 | Actualice Panorama y los dispositivos gestionados a PAN-OS 11.0.

- [Actualización de Panorama con una conexión a Internet](#)
- [Cambio de la versión de Panorama sin una conexión a Internet a una versión posterior](#)
- [Actualización de Panorama en una configuración de HA](#)

STEP 3 | Después de una actualización exitosa a PAN-OS 11.0, revise los logs del sistema en Panorama para identificar qué dispositivos gestionados en modo FIPS-CC no pueden conectarse a Panorama.

STEP 4 | Restablezca el estado de conexión segura en Panorama.

Este paso restablece la conectividad para cualquier dispositivo gestionado agregado a la gestión de Panorama mientras se ejecuta una versión de PAN-OS 11.0 y es irreversible. Este paso no afecta el estado de conectividad de los cortafuegos agregados cuando se ejecuta PAN-OS 10.0 o una versión anterior que se actualiza a PAN-OS 11.0.

1. [Inicio de sesión en la CLI de Panorama.](#)
2. Restablezca el estado de conexión segura.

```
admin> request sc3 reset
```

3. Reinicie el servidor de gestión en Panorama.

```
admin> software restart process management-server
```

4. (Solo HA) Repita este paso para cada peer en la configuración de alta disponibilidad (HA).

STEP 5 | Restablezca el estado de conexión segura en el dispositivo gestionado en modo FIPS-CC.

Este paso restablece la conexión del dispositivo gestionado y es irreversible.

1. Inicie sesión en la CLI del dispositivo gestionado.
 - [Inicie sesión en la CLI del cortafuegos](#)
 - [Inicie sesión en la CLI del recopilador de logs](#)
 - [Inicie sesión en la CLI del dispositivo WildFire](#)
2. Restablezca el estado de conexión segura.

```
admin> request sc3 reset
```

3. Reinicie el servidor de administración en el dispositivo gestionado.

```
admin> software restart process management-server
```

STEP 6 | Vuelva a agregar los dispositivos gestionados, que fueron afectados, a Panorama.

- [Cómo añadir un cortafuegos como dispositivo gestionado](#)
- [Configuración de recopiladores gestionados](#)
- [Agregue dispositivos independientes WildFire para gestionar con Panorama](#)

STEP 7 | Vuelva a generar o a importar todos los certificados para cumplir con el nivel de seguridad 2 de OpenSSL.

Al actualizar a PAN-OS 11.0, se requiere que todos los certificados cumplan con los siguientes requisitos mínimos:

- RSA de 2048 bits o superior, o ECDSA de 256 bits o superior
- Compendio de SHA256 o superior

Consulte la [Guía del administrador de PAN-OS](#) o la [Guía del administrador de Panorama](#) para obtener más información sobre la regeneración o reimportación de los certificados.

Cambio a versiones anteriores a Panorama 11.0

PAN-OS® 11.0 presenta un soporte avanzado de prevención de amenazas para la prevención de exploits de día cero que aprovecha el aprendizaje profundo en línea, la actualización y degradación de software simplificada para Panorama y de los dispositivos gestionados para reducir la carga operativa de actualizar dispositivos gestionados en múltiples versiones de PAN-OS, la proactiva evaluación de prácticas recomendadas (BPA) mediante AIOps para eliminar aún más la exposición de una estrategia de seguridad comprometida, el proxy web local para ayudar a la transición a la nube sin sacrificar la seguridad o la eficiencia, el soporte de cortafuegos para un cliente DHCPv6 con estado para obtener direcciones IPv6, la visibilidad mejorada para el contexto de usuario para el motor de identidad en la nube (CIE), el soporte TLSv1.3 para el acceso de la gestión y las recomendaciones mejoradas de la regla de la política de seguridad de IoT para que sea más fácil escalar y administrar las recomendaciones de la regla de políticas. Siga el flujo de trabajo a continuación para cambiar la versión del cortafuegos a una anterior antes de cambiar la versión de los recopiladores de logs y Panorama que ejecutan Panorama 11.0 a una versión de función anterior. El procedimiento es el mismo tanto si Panorama gestiona un recopilador de logs local como si gestiona un recopilador de logs dedicado o varios.



Para degradar de PAN-OS 11.0 a una versión anterior de PAN-OS, debe descargar e instalar la versión preferida de PAN-OS 10.2 o una versión posterior de PAN-OS 10.2 antes continuar la ruta de degradación a la versión de PAN-OS de destino. La versión anterior de PAN-OS 11.0 falla si intenta cambiar a PAN-OS 10.1 o una versión anterior de PAN-OS.



Consulte la [matriz de compatibilidad de Palo Alto Networks](#) para confirmar que los cortafuegos y los dispositivos que desea cambiar son compatibles con la versión anterior de PAN-OS. En el caso de los cortafuegos y dispositivos que puede cambiar a una versión anterior, también debe revisar [Consideraciones sobre el cambio a versiones anteriores/posteriores de complementos de Panorama](#) para asegurarse de tener en cuenta todos los ajustes de funciones y configuración que serán diferentes o no estarán disponibles después de cambiar a una versión anterior.

STEP 1 | Inicie sesión en la interfaz web de Panorama.

STEP 2 | Guarde una copia de seguridad de los archivos de configuración de Panorama y de los dispositivos gestionados.

1. Asegúrese de **Export Panorama and device configuration snapshot (Exportar panorama e instantánea de configuración del dispositivo)** (**Panorama > Setup (Configuración) > Operations (Operaciones)**).
2. Guarde el archivo .tgz exportado en una ubicación externa a Panorama, los recopiladores de logs y los cortafuegos. Puede usar esta copia de seguridad para restaurar la configuración si tiene problemas que le obligan a volver a empezar.

STEP 3 | Si ha [configurado la autenticación para un recopilador de logs dedicado](#) y ha eliminado el `admin` del administrador, configure y envíe un nuevo usuario `admin` a sus recopiladores de logs dedicados.

Los recopiladores de logs dedicados deben tener el usuario `admin` configurado para cambiar a PAN-OS 9.1 y versiones anteriores.

STEP 4 | Seleccione **Panorama > Plugins (Complementos) y Download (Descargar)** para descargar la versión del complemento compatible con PAN-OS 10.2 para todos los complementos instalados actualmente en Panorama.

Consulte la [matriz de compatibilidad de complementos de Panorama](#) para la versión de complemento de Panorama compatible con PAN-OS 10.2 y versiones anteriores.

Esto es necesario para degradar correctamente Panorama de PAN-OS 11.0 a PAN-OS 10.2 y versiones anteriores. La versión descargada del complemento se instala automáticamente durante la actualización a PAN-OS 10.2. La degradación a PAN-OS 10.2 se bloquea si no se descarga la versión del complemento compatible.



*(Solo complemento de ZTP) Para degradar correctamente Panorama a PAN-OS 10.2, debe **desinstalar el complemento de ZTP** antes de comenzar el proceso de degradación. Después de degradar correctamente a PAN-OS 10.2, debe volver a instalar el complemento de ZTP en Panorama.*

STEP 5 | Cambie a una versión anterior todos los cortafuegos que ejecuten una versión de PAN-OS 11.0.



La degradación de PAN-OS 11.0 a una versión de función anterior requiere que primero degrade a la versión preferida de PAN-OS 10.2 o a una versión posterior de PAN-OS 10.2. Después de degradar correctamente a la versión preferida de PAN-OS 10.2 o a una versión posterior de PAN-OS 10.2, puede continuar la degradación a la versión de PAN-OS de destino.

*Si va a cambiar a una versión anterior más de un cortafuegos, agilice el proceso al hacer que cada imagen de PAN-OS 10.2 específica del cortafuegos se descargue en Panorama antes de comenzar a cambiar a una versión anterior. Por ejemplo, para cambiar los cortafuegos PA-220 a la versión anterior PAN-OS 10.2, descargue las imágenes **PanOS_220-10.2.0** o **PanOS_3000-10.2.0**.*

Panorama requiere que todos los cortafuegos ejecuten la misma versión de PAN-OS o una anterior. Por eso, antes de cambiar Panorama a una versión anterior, repita las tareas siguientes que resulten oportunas según su entorno para cambiar a una versión anterior todos los cortafuegos gestionados:

1. Seleccione **Check Now (Comprobar ahora)** para ver las imágenes disponibles (**Panorama > Device Deployment [Implementación del dispositivo] > Software**).
2. Ubique la imagen de PAN-OS 10.2 para cada modelo o serie de cortafuegos que desee cambiar a una versión anterior. Si la imagen aún no se ha descargado, entonces seleccione **Download (Descargar)** imagen..

Cortafuegos no HA

Instale en la columna Action (Acción) la versión de PAN-OS 10.2 correspondiente, seleccione todos los cortafuegos que quiera cambiar a una versión anterior, seleccione **Reboot device after install (Reiniciar dispositivo tras la instalación)** y haga clic en **OK (Aceptar)**.

Cortafuegos de HA activo/activo:

1. Haga clic en **Install (Instalar)**, deshabilite (retire marca) la casilla de verificación de **Group HA Peers (Peers de HA del grupo)**, seleccione **Reboot device after install (Reiniciar dispositivo**

después de la instalación) y haga clic en **OK (Aceptar)**. Espere que el cortafuegos termine de reiniciarse antes de continuar.

2. Haga clic en **Install (Instalar)**, deshabilite (retire marca) la casilla de verificación de **Group HA Peers (Peers de HA del grupo)**, seleccione el peer de HA que todavía no actualizó, seleccione **Reboot device after install (Reiniciar dispositivo después de la instalación)** y haga clic en **OK (Aceptar)**.

Cortafuegos de HA activo/pasivo:

En este ejemplo, el cortafuegos activo se llama fw1 y el pasivo, fw2:

1. Haga clic en **Install (Instalar)** en la columna Action (Acción) para instalar la actualización adecuada, quite la marca de **Group HA Peers (Agrupar peers de HA)**, seleccione fw2, marque **Reboot device after install (Reiniciar dispositivo tras la instalación)** y haga clic en **OK (Aceptar)**.
2. Cuando fw2 termine de reiniciarse, verifique con el widget (**Dashboard [Panel] > High Availability [Alta disponibilidad]**) que fw1 sigue siendo el peer activo y fw2, el pasivo, es decir, el estado del cortafuegos local es **active [activo]** y el del peer [fw2], **passive [pasivo]**.
3. Acceda a fw1 y seleccione **Suspend local device (Suspende dispositivo local) (Device [Dispositivo] > High Availability [Alta disponibilidad] > Operational Commands [Comandos operativos])**.
4. Acceda a fw2 con (**Dashboard [Panel] > High Availability [Alta disponibilidad]**) y verifique que el estado del cortafuegos local es **active (activo)** y el del peer (fw1), **suspended (suspendido)**.
5. Acceda a Panorama, seleccione **Panorama > Device Deployment (Implementación de dispositivos) > Software**, haga clic en **Install (Instalar)** en la columna Action (Acción) para instalar la actualización adecuada, quite la marca de **Group HA Peers (Agrupar peers de HA)**, seleccione fw1, marque **Reboot device after install (Reiniciar dispositivo tras la instalación)** y haga clic en **OK (Aceptar)**. Espere que fw1 termine de reiniciarse antes de continuar.
6. Acceda a fw1 con el widget (**Dashboard [Panel] > High Availability [Alta disponibilidad]**) y verifique que el estado del cortafuegos local es **passive (pasivo)** y el del peer (fw2), **active (activo)**.



*Si habilitó la preferencia en la configuración de elección (**Device [Dispositivo] > High Availability [Alta disponibilidad] > General**), fw1 se restablecerá como el peer activo después del reinicio.*

STEP 6 | Realice el cambio a la versión anterior de cada recopilador de logs que utilice Panorama 11.0.



La degradación de PAN-OS 11.0 a una versión de función anterior requiere que primero degrade a la versión preferida de PAN-OS 10.2 o a una versión posterior de PAN-OS 10.2. Después de degradar correctamente a la versión preferida de PAN-OS 10.2 o a una versión posterior de PAN-OS 10.2, puede continuar la degradación a la versión de PAN-OS de destino.

1. Seleccione **Check Now (Comprobar ahora)** para ver las imágenes disponibles (**Panorama > Device Deployment [Implementación del dispositivo] > Software**).
2. Localice la imagen de Panorama 10.2. Si la imagen aún no se ha descargado, entonces seleccione **Download (Descargar)** imagen (columna Acción).
3. Cuando termine la descarga, haga clic en **Install (Instalar)** para instalar la imagen en todos los recopiladores de logs que ejecuten Panorama 10.2. Marque **Reboot device after install (Reiniciar dispositivo tras la instalación)** para reiniciar automáticamente el dispositivo cuando termine la actualización.

STEP 7 | Cambio de versión de Panorama a una versión anterior.



La degradación de PAN-OS 11.0 a una versión de función anterior requiere que primero degrade a la versión preferida de PAN-OS 10.2 o a una versión posterior de PAN-OS 10.2. Después de degradar correctamente a la versión preferida de PAN-OS 10.2 o a una versión posterior de PAN-OS 10.2, puede continuar la degradación a la versión de PAN-OS de destino.

1. Seleccione **Panorama > Software** y **Check Now (Comprobar ahora)** para ver las imágenes disponibles.
2. Localice la imagen de Panorama 10.2. Si la imagen aún no se ha descargado, entonces seleccione **Download (Descargar)** imagen..
3. Cuando termine la descarga, haga clic en **Install (Instalar)** para instalar la imagen en Panorama.
4. Reinicie Panorama del modo siguiente:
 - Si se le pide que reinicie, haga clic en **Yes (Sí)**. Si ve un mensaje para **CMS Login (iniciar sesión en CMS)**, pulse Intro sin introducir ningún nombre de usuario ni contraseña. Cuando aparezca el mensaje para iniciar sesión en Panorama, introduzca el nombre de usuario y contraseña que estableció durante la configuración inicial.
 - Si no se le indica que reinicie, seleccione **Panorama > Setup (Configuración) > Operations (Operaciones)** y haga clic en la opción **Reboot Panorama (Reiniciar Panorama)** de Device Operations (Operaciones con dispositivos).

STEP 8 | (Solo complemento de ZTP) Vuelva a instalar el complemento de ZTP.

1. [Inicie sesión en la interfaz web de Panorama.](#)
2. [Instale el complemento de ZTP.](#)
3. Seleccione **Panorama > Zero Touch Provisioning** y marque (habilitar) **ZTP**.

Solución de problemas del cambio a versiones posteriores de Panorama

Para solucionar los problemas del cambio de Panorama a una versión posterior, utilice la siguiente tabla para revisar los posibles problemas y cómo resolverlos.

Síntoma	Solución
La licencia de garantía del software expiró.	<p>Desde la CLI, elimine la clave de licencia caducada:</p> <ol style="list-style-type: none"> 1. Introduzca la clave de licencia de eliminación<software license key>. 2. Introduzca la clave de licencia de eliminación Software_Warranty<expiredate>.key.
Las versiones del software PAN-OS más recientes no estaban disponibles.	<p>Solo puede ver las versiones de software que están una versión de función por delante de la versión instalada actual. Por ejemplo, si tiene instalada una versión 8.1, solo las versiones 9.0 estarán disponibles para usted. Para ver las versiones 9.1, primero debe cambiar a la versión posterior 9.0.</p>
(Dispositivo virtual Panorama solo en modo heredado) La versión posterior no se pudo precargar en el administrador de software.	<p>Este problema ocurre cuando no hay suficientes recursos disponibles. Puede aumentar la capacidad de la máquina virtual o migrar del modo heredado al modo Panorama.</p>

Implementación de actualizaciones de cortafuegos, recopiladores de logs y dispositivos WildFire utilizando Panorama

Puede usar Panorama™ para admitir actualizaciones de software y contenido implementándolos en un subconjunto de los cortafuegos, recopiladores de logs dedicados o dispositivos y clústeres de dispositivos de WildFire® antes de instalar las actualizaciones en todos los dispositivos gestionados. Si desea programar actualizaciones de contenido periódicas, Panorama requiere una conexión directa a internet. Para implementar actualizaciones de software o contenido bajo demanda (no programadas), el procedimiento varía en función de si Panorama tiene o no conexión a internet. Panorama muestra una advertencia si implementa manualmente una actualización de contenido cuando se haya iniciado un proceso de actualización programado o vaya a iniciarse en un plazo de cinco minutos.

Al implementar actualizaciones, Panorama notifica a los dispositivos gestionados (cortafuegos, recopiladores de logs y dispositivos WildFire) que las actualizaciones están disponibles y los dispositivos recuperan los paquetes de actualización de Panorama. De forma predeterminada, los dispositivos gestionados recuperan las actualizaciones a través de la interfaz de gestión (MGT) en Panorama. Sin embargo, si desea reducir la carga de tráfico en la interfaz MGT utilizando otra interfaz para que los dispositivos recuperen actualizaciones, puede realizar la [Configuración de Panorama para usar varias interfaces](#).

Puede revertir con rapidez una versión de contenido de uno o más cortafuegos a la versión de contenido instalada previamente utilizando Panorama. Después de instalar una nueva versión de contenido en el cortafuegos, puede volver a la versión instalada previamente si la versión de contenido nueva desequilibra o interrumpe de otro modo las operaciones de su red.



De manera predeterminada, puede descargar hasta dos actualizaciones de software o contenido de cada tipo en Panorama. Al iniciar cualquier descarga que supere el máximo, Panorama elimina la actualización más antigua del tipo seleccionado. Para cambiar el valor máximo, consulte [Gestión de almacenamiento de Panorama para actualizaciones de software y contenido](#).

- [¿Qué actualizaciones puede enviar Panorama a otros dispositivos?](#)
- [Compatibilidad de versiones de Panorama, el recopilador de logs, el cortafuegos y WildFire](#)
- [Programación de una actualización de contenido mediante Panorama](#)
- [Actualización de los cortafuegos cuando Panorama está conectado a internet](#)
- [Actualización de los cortafuegos cuando Panorama no está conectado a internet](#)
- [Actualización de recopiladores de logs cuando Panorama está conectado a internet](#)
- [Actualización de recopiladores de logs cuando Panorama no está conectado a internet](#)
- [Cambio de un clúster de WildFire a una versión posterior desde Panorama con conexión a Internet](#)
- [Cambio de un clúster de WildFire a una versión posterior desde Panorama sin conexión a Internet](#)
- [Actualización de un cortafuegos de ZTP](#)
- [Restablecimiento de las actualizaciones de contenido de Panorama](#)

¿Qué actualizaciones puede enviar Panorama a otros dispositivos?

Las actualizaciones de contenido y software que puede instalar varían según qué suscripciones están activas en cada cortafuegos, recopilador de logs, y dispositivo WildFire® y clúster de dispositivos:

Tipo de dispositivo	Actualizaciones de software	Actualizaciones de contenido
Recopilación de logs	Panorama™	Aplicaciones (recopiladores de logs que no necesitan firmas de amenazas) Antivirus WildFire®
Rendimiento	PAN-OS® Agente o aplicación de GlobalProtect™	applications Aplicaciones y amenazas Antivirus WildFire
WildFire	PAN-OS Imágenes VM	WildFire

Programación de una actualización de contenido mediante Panorama

Panorama™ requiere una conexión a internet directa para programar [Actualizaciones compatibles](#) en cortafuegos, recopiladores de logs, y dispositivos y clústeres de dispositivos de WildFire®. De lo contrario, solo podrá realizar actualizaciones bajo demanda. (Para programar actualizaciones de antivirus, WildFire o BrightCloud URL para recopiladores de logs, los recopiladores de logs deben ejecutar Panorama 7.0.3 o una versión posterior.) Cada cortafuegos, recopilador de logs o dispositivos y clústeres de dispositivos de WildFire que reciba una actualización genera un log para indicar si la instalación se ha realizado correctamente (log de configuración) o no (log del sistema). Para programar actualizaciones en el servidor de gestión de Panorama, consulte [Instalación de actualizaciones de Panorama con una conexión a internet](#).



Antes de implementar las actualizaciones, consulte [Compatibilidad de versiones de Panorama](#), [el recopilador de logs](#), [el cortafuegos](#) y [WildFire](#) para obtener detalles importantes sobre la compatibilidad de las versiones de lanzamiento de contenido. Consulte las [Notas de versión](#) para obtener la versión de contenido mínima que debe instalar para una versión de Panorama.

Panorama puede descargar solo una actualización a la vez para actualizaciones del mismo tipo. Si programa varias actualizaciones del mismo tipo para que se descarguen durante la misma frecuencia, solo se realizará correctamente la primera descarga.

Si los cortafuegos se conectan directamente al servidor de actualizaciones de Palo Alto Networks®, también puede utilizar las plantillas de Panorama (**Device [Dispositivo] > Dynamic Updates [Actualizaciones dinámicas]**) para enviar [cronogramas de actualización de contenido](#) en los cortafuegos. Si desea demorar la instalación de actualizaciones durante un período después de que se publiquen, debe implementar los cronogramas mediante las plantillas. En casos excepcionales, una actualización de contenido puede incluir errores, el especificar una demora aumenta la probabilidad de que Palo Alto Networks identifique y quite estas actualizaciones del servidor de actualizaciones antes de que los cortafuegos las instalen.

Realice los siguientes pasos para cada tipo de actualización que desee programar.

STEP 1 | Seleccione **Panorama > Device Deployment (Implementación del dispositivo) > Dynamic Updates (Actualizaciones dinámicas)**, haga clic en **Schedules (Programas)** y en **Add (Añadir)** para fijar un programa.

STEP 2 | Especifique un nombre en **Name (Nombre)** para describir la programación, el tipo de actualización en **Type (Tipo)** y la frecuencia de actualizaciones (**Recurrence [Frecuencia]**). Las opciones de frecuencia dependen del tipo de actualización (**Type [Tipo]**).



PAN-OS® usa la zona horaria de Panorama para actualizar la programación.

Si configuró **Type (Tipo)** en **App and Threat (Aplicaciones y amenazas)**, los recopiladores de logs instalan y solo necesitan el contenido de Aplicaciones, no el contenido de Amenazas. Los cortafuegos usan el contenido de Aplicaciones y Amenazas. Para obtener más información, consulte [Compatibilidad de versiones de Panorama](#), [el recopilador de logs](#), [el cortafuegos](#) y [WildFire](#).

STEP 3 | Seleccione una de las siguientes acciones de programación y luego seleccione los cortafuegos o recopiladores de logs:

- **Download And Install (Descargar e instalar)** (**Recomendado**): seleccione **Devices (Dispositivos)** (cortafuegos), **Log Collectors (Recopiladores de logs)**, o **WildFire Appliances and Clusters (Dispositivos y clústeres de WildFire)**.
- **Download Only (Solo descargar)**: Panorama descarga la actualización pero no la instala.

STEP 4 | Haga clic en **OK (Aceptar)**.

STEP 5 | Seleccione **Commit (Confirmar) > Commit to Panorama (Confirmar en Panorama) y Commit (Confirmar)** para confirmar sus cambios

Compatibilidad de versiones de Panorama, el recopilador de logs, el cortafuegos y WildFire

Para obtener los mejores resultados, respete las siguientes pautas de compatibilidad de Panorama™:

- ❑ Instale la misma versión de Panorama tanto en el servidor de gestión de Panorama como en los recopiladores de logs dedicados.
- ❑ Panorama debe ejecutar la misma versión o una versión más reciente de PAN-OS que los cortafuegos que gestionará. Consulte [Compatibilidad con la gestión de Panorama](#) para obtener más información.

Antes de pasar los cortafuegos a la versión posterior PAN-OS 11.0, debe actualizar Panorama a la versión posterior 11.0.

- ❑ Panorama con PAN-OS 11.0 puede gestionar dispositivos WildFire® y clústeres de dispositivos WildFire que ejecutan la misma versión o una versión anterior de PAN-OS. Consulte [Compatibilidad con la gestión de Panorama](#) para obtener más información.

Se recomienda que el servidor de gestión de Panorama, los dispositivos WildFire y los clústeres de dispositivos WildFire ejecuten la misma versión de PAN-OS.

- ❑ La versión de contenido del servidor de gestión de Panorama debe ser la misma (o anterior) a las versiones de contenido de los recopiladores de logs dedicados o los cortafuegos gestionados. Consulte [Compatibilidad con la gestión de Panorama](#) para obtener más información.



Palo Alto Networks® recomienda instalar la misma versión de base de datos de Aplicaciones en Panorama que en los cortafuegos y recopiladores de logs dedicados.

Independientemente de si su suscripción incluya la base de datos de Aplicaciones o Aplicaciones y amenazas, Panorama instala solo la primera. Panorama y los recopiladores de logs dedicados no aplican reglas de políticas, por lo que no necesitan las firmas de amenazas de la base de datos de Amenazas. La base de datos de Aplicaciones incluye metadatos de amenazas (como nombres e ID de amenazas) que usa en Panorama y los recopiladores de logs dedicados cuando define reglas de políticas para los cortafuegos gestionados y cuando interpreta información de amenazas en logs e informes. Sin embargo, los cortafuegos requieren la base de datos completa de Aplicaciones y amenazas para hacer coincidir los identificadores registrados en los logs con la amenaza, URL o nombre de aplicación correspondientes. Consulte las [notas de versión](#) para obtener la versión de contenido mínima necesaria para una versión de Panorama.

Actualización de recopiladores de logs cuando Panorama está conectado a internet

Para ver la lista de actualizaciones de software o contenido que puede instalar en los recopiladores de logs, consulte [Actualizaciones compatibles](#).



Si está actualizando desde PAN-OS 8.1, PAN-OS 9.0 introdujo un nuevo formato de datos de log para recopiladores de log locales y dedicados. En la ruta de actualización para PAN-OS 10.1, los datos de logs existentes se migran de forma automática al nuevo formato cuando actualiza de PAN-OS 8.1 a PAN-OS 9.0.

Para evitar que se pierdan datos de logs, debe actualizar todos los recopiladores de log del grupo de recopiladores. Los logs no se reenvían ni se recopilan si no se ejecuta la misma versión de PAN-OS en todos ellos. Además, los datos de logs de los recopiladores del mismo grupo no se ven en las pestañas **ACC** ni **Monitor (Supervisión)** hasta que todos ejecuten la misma versión de PAN-OS. Por ejemplo, si el grupo tiene tres recopiladores de logs y actualiza dos de ellos, no se reenvía ningún log a ninguno de los recopiladores del grupo.

Palo Alto Networks recomienda actualizar los recopiladores de logs durante un intervalo de mantenimiento. Debido a la migración del formato, el proceso de actualización dura unas cuantas horas más en función del volumen de datos de logs que contienen los recopiladores locales y dedicados.

STEP 1 | Antes de actualizar los Recopiladores de logs, asegúrese de estar ejecutando la versión de software Panorama™ adecuada en el servidor de gestión de Panorama.



Palo Alto Networks® recomienda encarecidamente que Panorama y el Recopilador de logs ejecuten la misma versión de software y que Panorama, el recopilador de logs y todos los cortafuegos administrados ejecuten la misma versión de lanzamiento de contenido. Para obtener detalles importantes sobre la compatibilidad de contenido y software, consulte [Compatibilidad de versiones de Panorama, el recopilador de logs y el cortafuegos](#).

Panorama debe estar ejecutando la misma versión de software (o una posterior) que los recopiladores de logs, pero debe tener la misma versión de lanzamiento de contenido o una versión posterior:

- **Versión de lanzamiento de software:** si su servidor de gestión Panorama todavía no está ejecutando la misma versión de software (o una posterior) que la versión que desea actualizar en los recopiladores de logs, debe instalar la misma versión de Panorama o una posterior en Panorama (consulte [Instalación de actualizaciones de contenido y software para Panorama](#)) antes de actualizar cualquier recopilador de log.
- **Versión de lanzamiento del contenido:** para versiones de contenido, debe asegurarse de que todos los recopiladores de logs ejecutan la última versión de publicación de contenido o, como mínimo, ejecutan una versión posterior a la que se está ejecutando en Panorama; de no ser así, primero [Actualización del cortafuegos a PAN-OS 11.0 desde Panorama](#) y luego actualice los recopiladores de logs antes de actualizar la versión de lanzamiento de contenido en el servidor de gestión Panorama.

Para verificar las versiones de software y contenido:

- **Servidor de gestión de Panorama:** para averiguar qué versiones de software y contenido se están ejecutando en el servidor de gestión de Panorama, inicie sesión en la interfaz web de Panorama y vaya a la configuración disponible en la sección General Information (Información general) de **Dashboard (Panel)**.
- **Recopiladores de logs:** para averiguar qué versiones de software y contenido se están ejecutando en los recopiladores de logs, inicie sesión en la interfaz de línea de comandos (command-line interface, CLI) de cada uno y ejecute el comando **show system info**.

STEP 2 | Determine la ruta de actualización a PAN-OS 11.0.

No puede omitir la instalación de ninguna versión de lanzamiento en la ruta desde la versión actual en ejecución de PAN-OS a PAN-OS 11.0.0.



Revise [Lista de control para actualizar PAN-OS](#), los problemas conocidos y los cambios en el comportamiento predeterminado en las [Notas de la versión](#) y [Consideraciones sobre el cambio a versiones anteriores/posteriores de complementos de Panorama para cada versión a través de la cual pase como parte de la ruta de cambio a una versión posterior](#).

STEP 3 | Instale las últimas actualizaciones de contenido.



Consulte las [notas de versión](#) para obtener las versiones de contenido mínimas necesarias para una versión de software de Panorama.

1. [Inicie sesión en la interfaz web de Panorama](#).
2. Seleccione **Panorama > Device Deployment (Implementación del dispositivo) > Dynamic Updates (Actualizaciones dinámicas)** y haga clic en **Check Now (Comprobar ahora)** para comprobar las últimas actualizaciones. Si hay una actualización disponible, la columna Acción mostrará el enlace **Download (Descargar)**.
3. Si no está ya instalado, seleccione **Download (Descargar)** las actualizaciones de contenido apropiadas. Tras descargarlo correctamente, el enlace en la columna Action (Acción) cambia de **Download (Descargar)** a **Install (Instalar)**.
4. **Instale** la actualización de contenido (actualización de aplicaciones y amenazas) antes que las demás:

Si su suscripción incluye contenido de Aplicaciones y Amenazas, primero instale el contenido de **Aplicaciones**. Así, se instala de forma automática el contenido de aplicaciones y amenazas.



Independientemente de si su suscripción incluye contenido de aplicaciones y amenazas, Panorama instala y necesita solo el contenido de aplicaciones. Para obtener más información, consulte [Compatibilidad de versiones de Panorama](#), el [recopilador de logs](#), el [cortafuegos](#) y [WildFire](#).

5. Repita los pasos secundarios anteriores para cualquier otra actualización (de antivirus, WildFire o filtrado de URL) según sea necesario, de una a la vez, y en cualquier orden.

STEP 4 | Actualice el recopilador de logs a las versiones de PAN-OS junto con su ruta de actualización a PAN-OS 11.0.



Si actualiza más de un recopilador de logs, agilice el proceso determinando las rutas de actualización para todos los recopiladores de logs que desee actualizar antes de comenzar la descarga de imágenes.

1. [Actualización de recopiladores de logs cuando Panorama está conectado a internet](#) a PAN-OS 8.1.
2. [Actualización de recopiladores de logs cuando Panorama está conectado a internet](#) a PAN-OS 9.0.

En PAN-OS 9.0, se incorporó un nuevo formato de log. Los logs se migran de forma automática al nuevo formato después de actualizar con éxito el recopilador de logs a PAN-OS 9.0.



No continúe en su ruta de actualización hasta que verifique que la migración automática de logs se haya completado con éxito.

3. [Actualización de recopiladores de logs cuando Panorama está conectado a internet](#) a PAN-OS 9.1.
4. [Actualización de recopiladores de logs cuando Panorama está conectado a internet](#) a PAN-OS 10.0.
5. [Actualización de recopiladores de logs cuando Panorama está conectado a internet](#) a PAN-OS 10.1.

PAN-OS 11.0 presenta un nuevo formato de log. En la actualización de PAN-OS 11.0 a PAN-OS 10.1, puede optar por migrar los logs generados en PAN-OS 8.1 o una versión anterior. De lo contrario, estos logs se eliminan de forma automática cuando se actualiza correctamente a PAN-OS 10.1. Durante la migración, no se ven los datos de logs en las pestañas ACC ni Monitor (Supervisión). Mientras se lleva a cabo la migración, los datos de log continúan reenviándose al recopilador de log correspondiente, pero el rendimiento puede verse afectado.

6. [Actualización de recopiladores de logs cuando Panorama está conectado a internet](#) a PAN-OS 10.2.

STEP 5 | Actualice el recopilador de logs a PAN-OS 11.0.

1. En Panorama, seleccione **Check Now (Comprobar ahora)** (**Panorama > Device Deployment [Implementación del dispositivo] > Software**) para las actualizaciones más recientes. Si hay una actualización disponible, la columna Acción mostrará el enlace **Download (Descargar)**.
2. **Descargue** el archivo específico del modelo para la versión de lanzamiento de la versión 11.0 de PAN-OS. Por ejemplo, para actualizar un dispositivo M-Series a Panorama 11.0.0, descargue la imagen `Panorama_m-11.0.0`.

Después de una descarga correcta, la columna Acción cambia de **Download (Descargar)** a **Install (Instalar)** para esa imagen.

3. **Instale** PAN-OS 11.0 y seleccione los recopiladores de log correspondientes.
4. Seleccione una de las siguientes opciones según sus necesidades:
 - **Upload only to device (do not install) [Cargar solamente en dispositivo (no instalar)]**.
 - **Reboot device after install (Reiniciar dispositivo tras la instalación)**.
5. Haga clic en **OK (Aceptar)** para iniciar la carga o la instalación.

STEP 6 | Verifique las versiones de actualización de contenido y de software que se instalan en el recopilador de logs.

Introduzca el comando operativo **show system info**. El resultado será el siguiente o uno parecido:

```
Versión de software: Versión de la aplicación 11.0.0: 8270-6076
app-release-date: 2020/05/08 18:21:51
```

STEP 7 | (Solo modo FIPS-CC) [Actualice Panorama y dispositivos gestionados en modo FIPS-CC](#).

La actualización de un recopilador de logs dedicado en modo FIPS-CC requiere que restablezca el estado de conexión segura si agregó el recopilador de logs dedicado a la gestión de Panorama mientras el recopilador de logs dedicado ejecutaba una versión de PAN-OS 11.0.

No necesita reincorporar el recopilador de logs dedicado agregado a la gestión de Panorama mientras el recopilador de logs dedicado estaba ejecutando PAN-OS 10.0 o una versión anterior.

STEP 8 | (PAN-OS 10.2 y versiones posteriores) Vuelva a generar o a importar todos los certificados para cumplir con el nivel de seguridad 2 de OpenSSL.

Este paso es necesario si actualiza desde PAN-OS 10.1 o una versión anterior a PAN-OS 11.0. Omita este paso si actualiza desde PAN-OS 10.2 y ya volvió a generar o a importar los certificados.

Se requiere que todos los certificados cumplan con los siguientes requisitos mínimos:

- RSA de 2048 bits o superior, o ECDSA de 256 bits o superior
- Resumen de SHA256 o superior

Consulte la [Guía del administrador de PAN-OS](#) o la [Guía del administrador de Panorama](#) para obtener más información sobre cómo volver a generar o a importar los certificados.

STEP 9 | (Recomendado para el dispositivo virtual Panorama) [Aumente la memoria del dispositivo virtual Panorama](#) a 64 GB.

Después de actualizar correctamente el dispositivo virtual Panorama en el modo de recopilación de logs a PAN-OS 11.0, Palo Alto Networks recomienda aumentar la memoria del dispositivo virtual Panorama a 64 GB para cumplir con los [requisitos del sistema adicionales](#) y evitar cualquier problema relacionado con la creación de logs, la gestión y el rendimiento operativo relacionados con un dispositivo virtual Panorama con carencias.

Actualización de recopiladores de logs cuando Panorama no está conectado a internet

Para ver la lista de actualizaciones de software o contenido que puede instalar en los recopiladores de logs, consulte [Actualizaciones compatibles](#).



Si está actualizando desde PAN-OS 8.1, PAN-OS 9.0 introdujo un nuevo formato de datos de log para recopiladores de log locales y dedicados. En la ruta de actualización para PAN-OS 10.1, los datos de logs existentes se migran de forma automática al nuevo formato cuando actualiza de PAN-OS 8.1 a PAN-OS 9.0.

Para evitar que se pierdan datos de logs, debe actualizar todos los recopiladores de log del grupo de recopiladores. Los logs no se reenvían ni se recopilan si no se ejecuta la misma versión de PAN-OS en

todos ellos. Además, los datos de logs de los recopiladores del mismo grupo no se ven en las pestañas **ACC** ni **Monitor (Supervisión)** hasta que todos ejecuten la misma versión de PAN-OS. Por ejemplo, si el grupo tiene tres recopiladores de logs y actualiza dos de ellos, no se reenvía ningún log a ninguno de los recopiladores del grupo.

Palo Alto Networks recomienda actualizar los recopiladores de logs durante un intervalo de mantenimiento. Debido a la migración del formato, el proceso de actualización dura unas cuantas horas más en función del volumen de datos de logs que contienen los recopiladores locales y dedicados.

STEP 1 | Antes de actualizar los Recopiladores de logs, asegúrese de estar ejecutando la versión de software Panorama™ adecuada en el servidor de gestión de Panorama.



Palo Alto Networks® recomienda encarecidamente que Panorama y el Recopilador de logs ejecuten la misma versión de software y que Panorama, el recopilador de logs y todos los cortafuegos administrados ejecuten la misma versión de lanzamiento de contenido. Para obtener detalles importantes sobre la compatibilidad de contenido y software, consulte [Compatibilidad de versiones de Panorama, el recopilador de logs y el cortafuegos](#).

Panorama debe estar ejecutando la misma versión de software (o una posterior) que los recopiladores de logs, pero debe tener la misma versión de lanzamiento de contenido o una versión posterior:

- **Versión de lanzamiento de software:** si su servidor de gestión de Panorama no está ejecutando la misma versión de software, o una posterior, que la versión que desea actualizar en los Recopiladores de logs, entonces debe instalar la misma versión de Panorama o una posterior en Panorama (consulte [Instalación de actualizaciones de software y contenido de Panorama](#)) antes de actualizar cualquier cortafuegos.
- **Versión de lanzamiento de contenido:** para las versiones de lanzamiento de contenido, debe asegurarse de que todos los recopiladores de logs ejecuten la versión de lanzamiento de contenido más reciente o, como mínimo, una versión posterior a la que instalará o a la que se está ejecutando en Panorama; de no ser así, primero [Actualización del cortafuegos a PAN-OS 11.0 desde Panorama](#) y luego actualice los recopiladores de logs antes de actualizar la versión de lanzamiento de contenido en el servidor de gestión Panorama (consulte [Instalación de actualizaciones de contenido y software para Panorama](#)).

Para comprobar el software y las versiones de contenido:

- **Servidor de gestión de Panorama:** para averiguar qué versiones de software y contenido se están ejecutando en el servidor de gestión de Panorama, inicie sesión en la interfaz web de Panorama y vaya a la configuración disponible en la sección General Information (Información general) de **Dashboard (Panel)**.
- **Recopiladores de logs:** para averiguar qué versiones de software y contenido se están ejecutando en los recopiladores de logs, inicie sesión en la interfaz de línea de comandos (command-line interface, CLI) de cada uno y ejecute el comando **show system info**.

STEP 2 | [Determine la ruta de actualización a PAN-OS 11.0](#).

Revise [Lista de control para actualizar PAN-OS](#), los problemas conocidos y los cambios en el comportamiento predeterminado en las [Notas de la versión](#) y [Consideraciones sobre el cambio a](#)

versiones anteriores/posteriores de complementos de Panorama para cada versión a través de la cual pase como parte de la ruta de cambio a una versión posterior.



Si actualiza más de un recopilador de logs, agilice el proceso determinando las rutas de actualización para todos los recopiladores de logs que desee actualizar antes de comenzar la descarga de imágenes.

STEP 3 | Descargue las actualizaciones de contenido y software más recientes a un host que pueda conectarse y cargar los archivos en Panorama a través de SCP o HTTPS.



Consulte las [notas de versión](#) para obtener las versiones de contenido mínimas necesarias para una versión de software de Panorama.

1. Use un host con acceso a internet para iniciar sesión en el [sitio web de Atención al cliente de Palo Alto Networks](#).
2. Descargue las últimas actualizaciones de contenido:
 1. Haga clic en **Dynamic Updates (Actualizaciones dinámicas)** en la sección Recursos.
 2. **Descargue** las actualizaciones de contenido más recientes y guarde los archivos en el host. Lleve a cabo este paso para cada tipo de contenido que actualice.
3. Descargue las actualizaciones de software:
 1. Vuelva a la página principal del sitio web de atención al cliente de Palo Alto Networks® y haga clic en **Software Updates (Actualizaciones de software)** de la sección Resources (Recursos).
 2. Revise la columna Download (Descargar) para determinar la versión que desea instalar. Los nombres de archivo del paquete de actualización para dispositivos M-Series comienzan con "Panorama_m" seguido del número de versión. Por ejemplo, para actualizar un dispositivo M-Series a Panorama 11.0.0, descargue la imagen **Panorama_m-11.0.0**.



*Puede localizar rápidamente imágenes de Panorama seleccionando **Panorama M Images (Imágenes de Panorama M)** [para los dispositivos de la serie M] del menú desplegable **Filter by (Filtrar por)**.*

4. Haga clic en el nombre de archivo adecuado y guarde el archivo en el host.

STEP 4 | Instale las últimas actualizaciones de contenido.



Si necesita instalar actualizaciones de contenido, debe hacerlo antes de instalar las actualizaciones del software. Además, primero instale actualizaciones de contenido en los cortafuegos y luego en los Recopiladores de logs antes de actualizar la versión de contenido en Panorama.

Instale la actualización de aplicaciones o aplicaciones y amenazas primero, y luego instale cualquier otra actualización (antivirus, WildFire® o filtrado de URL) según sea necesario una a la vez y en cualquier secuencia.



Independientemente de si su suscripción incluye contenido de aplicaciones y amenazas, Panorama instala y necesita solo el contenido de aplicaciones. Para obtener más información, consulte [Compatibilidad de versiones de Panorama](#), [el recopilador de logs](#), [el cortafuegos](#) y [WildFire](#).

1. [Inicie sesión en la interfaz web de Panorama](#).
2. Seleccione **Panorama > Device Deployment (Implementación de dispositivos) > Dynamic Updates (Actualizaciones dinámicas)**.
3. Haga clic en **Upload (Cargar)**, seleccione el tipo de actualización en **Type (Tipo)**, haga clic en **Browse (Examinar)** para ir al archivo de actualización adecuado en el host y haga clic en **OK (Aceptar)**.
4. Haga clic en **Install From File (Instalar desde el archivo)**, seleccione el **Type (Tipo)** de actualización y seleccione el **File Name (Nombre de archivo)** de la actualización que acaba de cargar.
5. Seleccione los recopiladores de logs.
6. Haga clic en **OK (Aceptar)** para iniciar la instalación.
7. Repita estos pasos para cada actualización de contenido.

STEP 5 | Actualice el recopilador de logs a las versiones de PAN-OS junto con su ruta de actualización a PAN-OS 11.0.

1. [Actualización de recopiladores de logs cuando Panorama no está conectado a Internet](#) a PAN-OS 8.1.
2. [Actualización de recopiladores de logs cuando Panorama no está conectado a Internet](#) a PAN-OS 9.0.

En PAN-OS 9.0, se incorporó un nuevo formato de log. Los logs se migran de forma automática al nuevo formato después de actualizar con éxito el recopilador de logs a PAN-OS 9.0.



No continúe en su ruta de actualización hasta que verifique que la migración automática de logs se haya completado con éxito.

3. [Actualización de recopiladores de logs cuando Panorama no está conectado a Internet](#) a PAN-OS 9.1.
4. [Actualización de recopiladores de logs cuando Panorama no está conectado a Internet](#) a PAN-OS 10.0.
5. [Actualización de recopiladores de logs cuando Panorama no está conectado a Internet](#) a PAN-OS 10.1.

PAN-OS 10.0 presenta un nuevo formato de log. En la actualización de PAN-OS 10.0 a PAN-OS 10.1, puede optar por migrar los logs generados en PAN-OS 8.1 o una versión anterior. De lo contrario, estos logs se eliminan de forma automática cuando se actualiza correctamente a PAN-OS 10.1. Durante la migración, no se ven los datos de logs en las pestañas ACC ni Monitor (Supervisión). Mientras se lleva a cabo la migración, los datos de log continúan reenviándose al recopilador de log correspondiente, pero el rendimiento puede verse afectado.

6. [Actualización de recopiladores de logs cuando Panorama no está conectado a Internet](#) a PAN-OS 10.2.

STEP 6 | Actualice el recopilador de logs a PAN-OS 11.0.

1. Seleccione **Panorama > Device Deployment (Implementación del dispositivo) > Software**.
2. Seleccione **Upload (Cargar)** y haga clic en **Browse (Examinar)** para ir al archivo de software adecuado en el host, luego haga clic en **OK (Aceptar)**.
3. Haga clic en **Install (Instalar)** en la columna Acción de la versión que acaba de cargar.
4. **Instale** PAN-OS 11.0 y seleccione los recopiladores de log correspondientes.
5. Seleccione una de las siguientes opciones según sus necesidades:
 - **Upload only to device (do not install) [Cargar solamente en dispositivo (no instalar)].**
 - **Reboot device after install (Reiniciar dispositivo tras la instalación).**
6. Haga clic en **OK (Aceptar)** para iniciar la carga o la instalación.

STEP 7 | Verifique las versiones de contenido o de software que se instalan en cada recopilador de logs.

Inicie sesión en la CLI del recopilador de logs e ingrese el comando operativo **show system info**. El resultado será el siguiente o uno parecido:

```
Versión de software: Versión de la aplicación 11.0.0: 8270-6076
app-release-date: 2020/05/08 18:21:51
```

STEP 8 | (Solo modo FIPS-CC) Actualice Panorama y dispositivos gestionados en modo FIPS-CC.

La actualización de un recopilador de logs dedicado en modo FIPS-CC requiere que restablezca el estado de conexión segura si agregó el recopilador de logs dedicado a la gestión de Panorama mientras el recopilador de logs dedicado ejecutaba una versión de PAN-OS 11.0.

No necesita reincorporar el recopilador de logs dedicado agregado a la gestión de Panorama mientras el recopilador de logs dedicado estaba ejecutando PAN-OS 10.0 o una versión anterior.

STEP 9 | (PAN-OS 10.2 y versiones posteriores) Vuelva a generar o a importar todos los certificados para cumplir con el nivel de seguridad 2 de OpenSSL.

Este paso es necesario si actualiza desde PAN-OS 10.1 o una versión anterior a PAN-OS 11.0. Omita este paso si actualiza desde PAN-OS 10.2 y ya volvió a generar o a importar los certificados.

Se requiere que todos los certificados cumplan con los siguientes requisitos mínimos:

- RSA de 2048 bits o superior, o ECDSA de 256 bits o superior
- Resumen de SHA256 o superior

Consulte la [Guía del administrador de PAN-OS](#) o la [Guía del administrador de Panorama](#) para obtener más información sobre cómo volver a generar o a importar los certificados.

STEP 10 | (Recomendado para el dispositivo virtual Panorama) Aumente la memoria del dispositivo virtual Panorama a 64 GB.

Después de actualizar correctamente el dispositivo virtual Panorama en el modo de recopilación de logs a PAN-OS 11.0, Palo Alto Networks recomienda aumentar la memoria del dispositivo virtual Panorama a 64 GB para cumplir con los [requisitos del sistema adicionales](#) y evitar cualquier problema relacionado con la creación de logs, la gestión y el rendimiento operativo relacionados con un dispositivo virtual Panorama con carencias.

Cambio de un clúster de WildFire a una versión posterior desde Panorama con conexión a Internet

Los dispositivos WildFire en un clúster pueden actualizarse en paralelo cuando se gestionan con Panorama. Si Panorama no tiene una conexión directa a internet, puede comprobar y descargar las versiones nuevas directamente desde Panorama.



Panorama solo puede gestionar dispositivos y clústeres de dispositivos WildFire que operen la misma versión de software o un versión posterior.

STEP 1 | Actualice Panorama a una versión igual o posterior que la versión del software de destino que desea instalar en el clúster WildFire.

Para obtener más información sobre la actualización de Panorama, consulte [Instalación de actualizaciones de contenido y software de Panorama](#).

STEP 2 | Suspenda temporalmente el análisis de muestras.

1. Evite que los cortafuegos reenvíen nuevas muestras al dispositivo WildFire.
 1. Inicie sesión en la interfaz web del cortafuegos.
 2. Seleccione **Device > Setup > WildFire (Dispositivo > Configuración > WildFire)** y edite **General Settings (Configuración general)**.
 3. Borre el campo **WildFire Private Cloud (Nube privada de WildFire)**.
 4. Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)**.
2. Confirme que el análisis de las muestras que el cortafuegos envió al dispositivo haya finalizado:
 1. Inicie sesión en la interfaz web de Panorama.
 2. Seleccione **Panorama > Managed WildFire Clusters (Panorama > Clústeres WildFire gestionados)** y haga clic en **View (Visualizar)** para ver la **Utilization (utilización)** del entorno de análisis del clúster.
 3. Compruebe que el **Virtual Machine Usage (Uso de máquina virtual)** no muestre ningún análisis de muestra en progreso.



Si no desea esperar a que el dispositivo WildFire complete el análisis de las muestras recién enviadas, puede continuar con el próximo paso. Sin embargo, considere que el dispositivo WildFire descarta las muestras pendientes en la cola de análisis.

STEP 3 | Instale las últimas actualizaciones de contenido del dispositivo WildFire.

Estas actualizaciones le proporciona al dispositivo la información de amenazas más reciente para detectar malware con mayor precisión.



Debe instalar las actualizaciones de contenido antes que las actualizaciones de software. Consulte las [Notas de versión](#) para obtener la versión de contenido mínima que debe instalar para una versión de Panorama.

1. Descargue la actualización de contenido de WildFire:
 1. Seleccione **Panorama > Device Deployment (Implementación de dispositivos) > Dynamic Updates (Actualizaciones dinámicas)**.
 2. Seleccione un paquete de versión de actualización de contenido de WildFire y haga clic en **Download (Descargar)**.
2. Haga clic en **Install (Instalar)**.
3. Seleccione los clústeres o los dispositivos individuales WildFire que desea actualizar.
4. Haga clic en **OK (Aceptar)** para iniciar la instalación.

STEP 4 | Descargue la versión de software PAN-OS en el dispositivo WildFire.

No puede omitir ninguna versión importante al actualizar el dispositivo WildFire. Por ejemplo, si desea actualizar de PAN-OS 9.1 a PAN-OS 11.0, primero debe descargar e instalar PAN-OS 10.0, PAN-OS 10.1 y PAN-OS 10.2.

1. Descargue la actualización de software de WildFire:
 1. Seleccione **Panorama > Device Deployment > Software (Panorama > Implementación de dispositivos > Software)**.
 2. Haga clic en **Check Now (Comprobar ahora)** para recuperar una lista actualizada de las versiones.
 3. Seleccione la versión de WildFire que desea instalar y haga clic en **Download (Descargar)**.
 4. Haga clic en **Close (Cerrar)** para salir de la ventana **Download Software (Descargar software)**.
2. Haga clic en **Install (Instalar)**.
3. Seleccione los clústeres WildFire que desea actualizar.
4. Seleccione Reboot device after install (Reiniciar dispositivo tras la instalación).
5. Haga clic en **OK (Aceptar)** para iniciar la instalación.
6. (Opcional) Supervise el progreso de la instalación en Panorama.

STEP 5 | (Opcional) Consulte el estado de las tareas de reinicio en el nodo controlador de WildFire.

En el controlador del clúster WildFire, ejecute el siguiente comando y busque el tipo de trabajo **Install** y el estado **FIN**:

```
admin@WF-500(active-controller)> show cluster task pending
```

STEP 6 | Compruebe que el dispositivo WildFire esté listo para reanudar el análisis de muestras.

1. Compruebe si en el campo sw-version (versión de software) figura 11.0.0:

```
admin@WF-500(passive-controller)> show system info | match sw-version
```

2. Confirme que todos los servicios se ejecuten:

```
admin@WF-500(passive-controller)> show system software status
```

3. Confirme que el trabajo de confirmación automática (**AutoCom**) se haya completado:

```
admin@WF-500(passive-controller)> show jobs all
```

Cambio de un clúster de WildFire a una versión posterior desde Panorama sin conexión a Internet

Los dispositivos WildFire en un clúster pueden actualizarse en paralelo cuando se gestionan con Panorama. Si Panorama no tiene una conexión directa a internet, debe descargar el contenido de software y las

actualizaciones del sitio de soporte de Palo Alto Networks, y alojarlos en un servidor interno antes de que Panorama los distribuya.



Panorama solo puede gestionar dispositivos y clústeres de dispositivos WildFire que operen la misma versión de software o un versión posterior.

STEP 1 | Actualice Panorama a una versión igual o posterior que la versión del software de destino que desea instalar en el clúster WildFire.

Para obtener más información sobre la actualización de Panorama, consulte [Instalación de actualizaciones de contenido y software de Panorama](#).

STEP 2 | Suspenda temporalmente el análisis de muestras.

1. Evite que los cortafuegos reenvíen nuevas muestras al dispositivo WildFire.
 1. Inicie sesión en la interfaz web del cortafuegos.
 2. Seleccione **Device > Setup > WildFire (Dispositivo > Configuración > WildFire)** y edite **General Settings (Configuración general)**.
 3. Borre el campo **WildFire Private Cloud (Nube privada de WildFire)**.
 4. Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)**.
2. Confirme que el análisis de las muestras que el cortafuegos envió al dispositivo haya finalizado:
 1. Inicie sesión en la interfaz web de Panorama.
 2. Seleccione **Panorama > Managed WildFire Clusters (Panorama > Clústeres WildFire gestionados)** y haga clic en **View (Visualizar)** para ver la **Utilization (utilización)** del entorno de análisis del clúster.
 3. Compruebe que el **Virtual Machine Usage (Uso de máquina virtual)** no muestre ningún análisis de muestra en progreso.



Si no desea esperar a que el dispositivo WildFire complete el análisis de las muestras recién enviadas, puede continuar con el próximo paso. Sin embargo, considere que el dispositivo WildFire descarta las muestras pendientes en la cola de análisis.

- STEP 3 |** Descargue las actualizaciones de contenido y software de WildFire en un host con acceso a internet. Panorama debe tener acceso al host.
1. Use un host con acceso a internet para iniciar sesión en el [sitio web de atención al cliente de Palo Alto Networks](#).
 2. Descargue las actualizaciones de contenido:
 1. Haga clic en **Dynamic Updates (Actualizaciones dinámicas)** en la sección Tools (Herramientas).
 2. Haga clic en **Download (Descargar)** para descargar la actualización de contenido deseada y guarde el archivo en el host. Lleve a cabo este paso para cada tipo de contenido que actualice.
 3. Descargue las actualizaciones de software:
 1. Vuelva a la página principal del sitio web de atención al cliente de Palo Alto Networks y haga clic en **Software Updates (Actualizaciones de software)** de la sección Tools (Herramientas).
 2. Revise la columna Descargar para determinar la versión que quiere instalar. El nombre de archivo del paquete de actualización indica el modelo y la versión de la actualización: WildFire_<release>.
 3. Haga clic en el nombre de archivo y guarde el archivo en el host.

STEP 4 | Instale las últimas actualizaciones de contenido del dispositivo WildFire.

Estas actualizaciones le proporciona al dispositivo la información de amenazas más reciente para detectar malware con mayor precisión.



Debe instalar las actualizaciones de contenido antes que las actualizaciones de software. Consulte las [Notas de versión](#) para obtener la versión de contenido mínima que debe instalar para una versión de Panorama.

1. Descargue la actualización de contenido de WildFire:
 1. Seleccione **Panorama > Device Deployment (Implementación de dispositivos) > Dynamic Updates (Actualizaciones dinámicas)**.
 2. Haga clic en **Upload (Cargar)**, seleccione el tipo de actualización en **Type (Tipo)**, haga clic en **Browse (Explorar)** para ir al archivo de actualización de contenido y, luego, en **OK (Aceptar)**.
 3. Haga clic en **Install From File (Instalar desde archivo)**, seleccione el **Type (Tipo)** de paquete, el **File Name (Nombre de archivo)**, además de los dispositivos WildFire en el clúster que desea actualizar y, luego, haga clic en **OK (Aceptar)**.
2. Haga clic en **OK (Aceptar)** para iniciar la instalación.

STEP 5 | Descargue la versión de software PAN-OS en el dispositivo WildFire.

No puede omitir ninguna versión importante al actualizar el dispositivo WildFire. Por ejemplo, si desea actualizar de PAN-OS 9.1 a PAN-OS 11.0, primero debe descargar e instalar PAN-OS 10.0, PAN-OS 10.1 y PAN-OS 10.2.

1. Descargue la actualización de software de WildFire:
 1. Seleccione **Panorama > Device Deployment > Software (Panorama > Implementación de dispositivos > Software)**.
 2. Haga clic en **Check Now (Comprobar ahora)** para recuperar una lista actualizada de las versiones.
 3. Seleccione la versión de WildFire que desea instalar y haga clic en **Download (Descargar)**.
 4. Haga clic en **Close (Cerrar)** para salir de la ventana **Download Software (Descargar software)**.
2. Haga clic en **Install (Instalar)**.
3. Seleccione los clústeres WildFire que desea actualizar.
4. Seleccione Reboot device after install (Reiniciar dispositivo tras la instalación).
5. Haga clic en **OK (Aceptar)** para iniciar la instalación.
6. (Opcional) Supervise el progreso de la instalación en Panorama.

STEP 6 | (Opcional) Consulte el estado de las tareas de reinicio en el nodo controlador de WildFire.

En el controlador del clúster WildFire, ejecute el siguiente comando y busque el tipo de trabajo **Install** y el estado **FIN**:

```
admin@WF-500(active-controller)> show cluster task pending
```

STEP 7 | Compruebe que el dispositivo WildFire esté listo para reanudar el análisis de muestras.

1. Compruebe si en el campo sw-version (versión de software) figura 11.0.0:

```
admin@WF-500(passive-controller)> show system info | match sw-version
```

2. Confirme que todos los servicios se ejecuten:

```
admin@WF-500(passive-controller)> show system software status
```
3. Confirme que el trabajo de confirmación automática (**AutoCom**) se haya completado:

```
admin@WF-500(passive-controller)> show jobs all
```

Actualización de los cortafuegos cuando Panorama está conectado a internet

Revise las [Notas de la versión PAN-OS 11.0](#) y utilice el siguiente procedimiento para cambiar los cortafuegos que gestiona con Panorama a una versión posterior. Este procedimiento aplica a los cortafuegos independientes y los cortafuegos que se implementan en una configuración de alta disponibilidad (HA).

Al actualizar los cortafuegos de HA en varias versiones de PAN-OS con funciones, debe actualizar cada peer de HA a la misma versión de PAN-OS con funciones en la ruta de actualización antes de continuar. Por ejemplo, está actualizando peers de HA de PAN-OS 10.0 a PAN-OS 11.0. Debe actualizar ambos peers de HA a PAN-OS 10.1 antes de poder continuar con la actualización a la versión de PAN-OS 11.0 de destino. Cuando los peers de HA tienen dos o más versiones con funciones de diferencia, el cortafuegos con la versión más antigua instalada entra en estado de **suspensión** y muestra un mensaje que dice **Peer version too old** (Versión del peer demasiado antigua).



Si Panorama no se puede conectar directamente al servidor de actualizaciones, siga el procedimiento para la [Actualización de los cortafuegos cuando Panorama no está conectado a internet](#) de modo que pueda descargar manualmente imágenes a Panorama y distribuir las imágenes a los cortafuegos.

La nueva función [Omitir actualización de versión de software](#) le permite omitir hasta tres versiones al implementar actualizaciones de dispositivos Panorama en PAN-OS 11.0 a cortafuegos en PAN-OS 10.1 o versiones posteriores.

Antes de actualizar los cortafuegos desde Panorama, debe realizar lo siguiente:

- ❑ Asegúrese de que Panorama ejecute una versión PAN-OS igual o posterior a la versión de actualización. Debe [cambiar Panorama](#) y sus [recopiladores de logs](#) a la versión posterior 11.0 antes de cambiar los cortafuegos gestionados a esta versión. Además, al cambiar los recopiladores de logs a la versión posterior 11.0, debe cambiar todos los recopiladores de logs a una versión posterior al mismo tiempo debido a los cambios en la infraestructura de creación de logs.
- ❑ Asegúrese de que todos los cortafuegos estén conectados a una fuente de alimentación fiable. Si se interrumpe la alimentación durante una actualización, los cortafuegos pueden resultar inútiles.
- ❑ Decida si desea permanecer en modo heredado si el dispositivo virtual Panorama está en modo heredado cuando cambia a la versión posterior PAN-OS 11.0. El modo heredado no es compatible con una nueva implementación de dispositivo virtual Panorama que ejecute PAN-OS 9.1 o una versión posterior. Si cambia el dispositivo virtual Panorama a la versión posterior PAN-OS 9.0 o una versión anterior a PAN-OS 11.0, Palo Alto Networks recomienda revisar los [requisitos previos de configuración para el dispositivo virtual Panorama](#) y cambiar al [modo Panorama](#) o al [modo solo administración](#) según sus necesidades.

Si desea mantener el dispositivo virtual Panorama en modo heredado, [aumente las CPU y la memoria](#) asignadas al dispositivo virtual Panorama a un mínimo de 16 CPU y 32 GB de memoria para cambiar con éxito a la versión posterior PAN-OS 11.0. Consulte los [Requisitos previos de configuración del dispositivo virtual Panorama](#) para obtener más información.

STEP 1 | [Inicie sesión en la interfaz web de Panorama.](#)

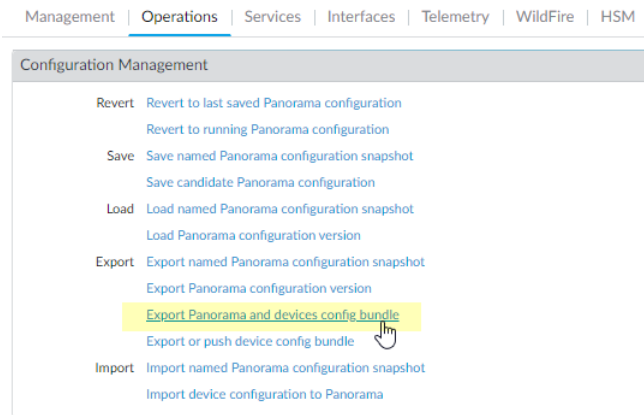
STEP 2 | Guarde una copia de seguridad del archivo de configuración actual en cada cortafuegos gestionado que desee actualizar.



A pesar de que el cortafuegos crea automáticamente una copia de seguridad de la configuración, se recomienda crear y almacenar externamente una copia de seguridad antes de la actualización.

1. Seleccione **Panorama > Setup (Configuración) > Operations (Operaciones)** y haga clic en **Export Panorama and devices config bundle (Exportar lote de configuración de**

dispositivos y Panorama) para generar y exportar la versión más reciente de la copia de seguridad de configuración de Panorama y de cada dispositivo gestionado.



2. Guarde el archivo exportado en una ubicación externa al cortafuegos. Puede usar esta copia de seguridad para restaurar la configuración si tiene problemas con la actualización.

STEP 3 | Instale la última actualización de contenido.

Consulte las [Notas de la versión](#) para obtener la versión de contenido mínima necesaria para PAN-OS 11.0. Asegúrese de seguir [Prácticas recomendadas para las actualizaciones de contenido de aplicaciones y amenazas](#) cuando implemente actualizaciones de contenido en Panorama y en los cortafuegos gestionados.

1. Seleccione **Panorama > Device Deployment (Implementación del dispositivo) > Dynamic Updates (Actualizaciones dinámicas)** y haga clic en **Check Now (Comprobar ahora)** para

comprobar las últimas actualizaciones. Si hay una actualización disponible, la columna Acción mostrará el enlace **Download (Descargar)**.

VERSION	FILE NAME	FEATURES	TYPE	SIZE	SHA256	RELEASE DATE	DOWNLOADED	ACTION	DOCUM
Last checked: 2020/07/07 17:48:29 PDT									
8287-6151	panupv2-all-contents-8287-6151	Contents	Full	56 MB		2020/06/26 17:34:56 PDT		Download	Release
8287-6151	panupv2-all-apps-8287-6151	Apps	Full	48 MB		2020/06/26 17:35:11 PDT		Download	Release
8287-6152	panupv2-all-contents-8287-6152	Contents	Full	56 MB		2020/06/29 11:55:44 PDT		Download	Release
8287-6152	panupv2-all-apps-8287-6152	Apps	Full	48 MB		2020/06/29 11:55:27 PDT	✓	Install	Release
8287-6153	panupv2-all-contents-8287-6153	Contents	Full	56 MB		2020/06/29 17:15:33 PDT		Download	Release
8287-6153	panupv2-all-apps-8287-6153	Apps	Full	47 MB		2020/06/29 17:15:51 PDT		Download	Release
8287-6154	panupv2-all-contents-8287-6154	Contents	Full	56 MB		2020/06/30 16:14:19 PDT		Download	Release
8287-6154	panupv2-all-apps-8287-6154	Apps	Full	47 MB		2020/06/30 16:14:37 PDT		Download	Release
8287-6155	panupv2-all-contents-8287-6155	Contents	Full	56 MB		2020/06/30 19:09:11 PDT		Download	Release
8287-6155	panupv2-all-apps-8287-6155	Apps	Full	47 MB		2020/06/30 19:09:28 PDT		Download	Release
8288-6157	panupv2-all-contents-8288-6157	Contents	Full	56 MB		2020/07/01 17:00:41 PDT		Download	Release
8288-6157	panupv2-all-apps-8288-6157	Apps	Full	47 MB		2020/07/01 17:00:30 PDT		Download	Release
8288-6158	panupv2-all-contents-8288-6158	Contents	Full	56 MB		2020/07/01 18:15:46 PDT		Download	Release
8288-6158	panupv2-all-apps-8288-6158	Apps	Full	47 MB		2020/07/01 18:15:33 PDT		Download	Release
8288-6159	panupv2-all-contents-8288-6159	Contents	Full	56 MB		2020/07/02 11:55:30 PDT		Download	Release

- Haga clic en **Install (Instalar)** y seleccione los cortafuegos en los que desee instalar la actualización. Si actualiza los cortafuegos de HA, deberá actualizar contenido en ambos peers.
- Haga clic en **OK (Aceptar)**.

STEP 4 | Determine la ruta de actualización a PAN-OS 11.0.



Revise la lista de control para actualizar PAN-OS, los problemas conocidos y los cambios en el comportamiento predeterminado en las [Notas de la versión](#) y las [consideraciones sobre el cambio a versiones anteriores/posteriores](#) para cada versión a través de la cual pase como parte de su ruta de actualización.



Si actualiza más de un cortafuegos, agilice el proceso determinando las rutas de actualización para todos los cortafuegos antes de comenzar la descarga de imágenes.

STEP 5 | (Prácticas recomendadas) Si está aprovechando Cortex Data Lake (CDL), instale el certificado de dispositivo.

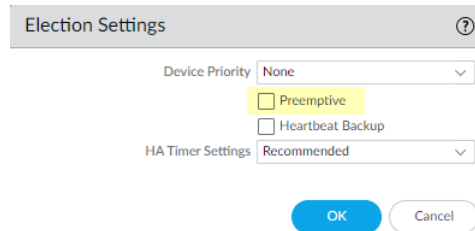
El cortafuegos cambia de forma automática al uso del certificado de dispositivo para la autenticación con ingestión de CDL y endpoints de consulta cuando se cambia a la versión posterior PAN-OS 11.0.



Si no instala el certificado del dispositivo antes de actualizar a PAN-OS 11.0, el cortafuegos continuará usando los certificados de servicio de creación de logs existentes para la autenticación.

STEP 6 | (Solo actualizaciones de cortafuegos de HA) Si actualizará los cortafuegos que forman parte de un par de HA, deshabilite la opción de preferencia. Solo debe deshabilitar esta opción en un cortafuegos de cada par de HA.

1. Seleccione **Device (Dispositivo) > High Availability (Alta disponibilidad)** y edite la sección **Election Settings (Ajustes de elección)**.
2. Si esta opción está deshabilitada, deshabilite (desmarque) la opción **Preemptive (Preferente)** y haga clic en **OK (Aceptar)**.



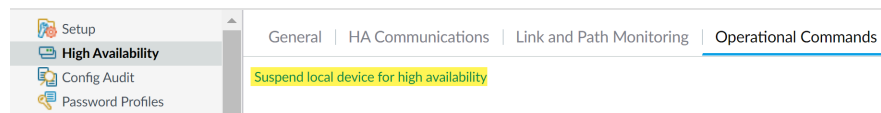
3. Haga clic en **Commit (Confirmar)** para confirmar los cambios. Asegúrese de que la confirmación se realice correctamente antes de continuar con la actualización.

STEP 7 | (Solo actualizaciones de cortafuegos de HA) Suspenda el peer de HA principal para forzar una conmutación por error.

(Cortafuegos activo/pasivo) Para los cortafuegos en una configuración de HA activa/pasiva, suspenda y actualice primero el peer de HA activo.

(Cortafuegos activo/pasivo) Para los cortafuegos en una configuración de HA activa/pasiva, suspenda y actualice primero el peer de HA activo- principal.

1. Inicie sesión en la interfaz web del cortafuegos del peer de HA del cortafuegos principal activo.
2. Seleccione **Device (Dispositivo) > High Availability (Alta disponibilidad) > Operational Commands (Comandos operativos)** y **Suspend local device for high availability (Suspende dispositivo local para alta disponibilidad)**.



3. En la esquina inferior derecha, verifique que el estado sea **suspended (suspendido)**.

La conmutación por error resultante debería hacer que el peer de HA pasivo secundario cambie al estado **activo**.



La conmutación por error resultante verifica que la conmutación por error de HA funcione correctamente antes de realizar la actualización.

STEP 8 | (Opcional) Actualice los cortafuegos gestionados a PAN-OS 10.1.

La función de omitir actualización de versión de software es compatible con los cortafuegos gestionados que ejecutan PAN-OS 10.1 o versiones posteriores. Si los cortafuegos gestionados están en PAN-OS 10.0 o una versión anterior, primero actualice a PAN-OS 10.1 o una versión posterior.

STEP 9 | (Opcional) **Exporte** el archivo a un servidor SCP configurado.

En PAN-OS 11.0, los servidores SCP están disponibles como origen de descarga cuando se implementan actualizaciones en los cortafuegos gestionados. Exporte el archivo antes de descargar el software y las imágenes de contenido en el siguiente paso.

STEP 10 | Valide y descargue las versiones de software y contenido necesarias para la versión de destino.

En este paso, puede ver y descargar el software intermedio y las imágenes de contenido necesarias para actualizar a PAN-OS 11.0.

La descarga de software y de imágenes de contenido mediante la descarga de varias imágenes es opcional. Aún puede descargar las imágenes una por una.

1. Haga clic en **Panorama > Device Deployment (Implementación del dispositivo) > Software > Action (Acción) > Validate (Validar)**.
2. Vea las versiones intermedias de software y contenido que necesita descargar.
3. Seleccione los cortafuegos que desea actualizar y haga clic en **Deploy (Implementar)**.
4. Seleccione el origen de la descarga y haga clic en **Download (Descargar)**.

STEP 11 | Instale PAN-OS 11.0.0 en el cortafuegos.



*(Solo en el caso de SD-WAN) Para conservar un estado preciso de los vínculos de SD-WAN, debe cambiar los cortafuegos de centrales a la versión posterior PAN-OS 11.0 antes de actualizar los cortafuegos de sucursales. La actualización de los cortafuegos de sucursales antes que los cortafuegos de central puede provocar datos de supervisión incorrectos (**Panorama [Panorama] > SD-WAN [SD-WAN] > Monitoring [Supervisión]**) y que los enlaces de SD-WAN se muestren de forma incorrecta como **down (inactivo)**.*

1. Haga clic en **Install (Instalar)** en la columna Action (Acción) que corresponda a los modelos de cortafuegos que desee actualizar. Por ejemplo, si desea cambiar sus cortafuegos PA-220 a una versión posterior, haga clic en **Install (Instalar)** en la fila que corresponda a PanOS_220-11.0.0.
2. En el cuadro de diálogo Deploy Software (Implementar software), seleccione todos los cortafuegos que desea actualizar.
(Solo actualizaciones de cortafuegos de HA) Para reducir el tiempo de inactividad, seleccione solo un peer en cada par de HA. En los pares activo/pasivo, seleccione el peer pasivo; en los pares activo/activo, seleccione el peer activo secundario.
3. *(Solo actualizaciones de cortafuegos de HA)* Asegúrese de que la opción **Group HA Peers (Agrupar peers de HA)** no esté seleccionada.
4. Seleccione **Reboot device after install (Reiniciar dispositivo tras la instalación)**.
5. Para comenzar la actualización, haga clic en **OK (Aceptar)**.
6. Una vez que la instalación se realiza completamente, reinicie mediante uno de los siguientes métodos:
 - Si se le pide que reinicie, haga clic en **Yes (Sí)**.
 - Si no se le solicita que reinicie, seleccione **Device (Dispositivo) > Setup (Configuración) > Operations (Operaciones)** y haga clic en **Reboot Device (Reiniciar dispositivo)**.
7. Después de que los cortafuegos terminen de reiniciarse, seleccione **Panorama (Panorama) > Managed Devices (Dispositivos gestionados)** y verifique que la versión del software sea 11.0.0 en los cortafuegos que actualizó. Además, verifique que el estado de HA de los cortafuegos pasivos que actualizó continúe siendo pasivo.

STEP 12 | *(Solo actualizaciones de cortafuegos de HA)* Restaure la funcionalidad de HA en el Peer de HA principal.

1. [Inicie sesión en la interfaz web del cortafuegos](#) del peer de HA del cortafuegos principal suspendido.
2. Seleccione **Device (Dispositivo) > High Availability (Alta disponibilidad) > Operational Commands (Comandos operativos)** y **Make local device functional for high availability (Hacer que el dispositivo local sea funcional para alta disponibilidad)**.
3. En la esquina inferior derecha, verifique que el estado sea **Passive (Pasivo)**. Para cortafuegos en una configuración activa/activa, verifique que el estado sea **Active (Activo)**.
4. Espere a que se sincronice la configuración en ejecución del peer de HA.
En el **Dashboard (Panel)**, controle el estado de la configuración en ejecución en el widget de alta disponibilidad.

STEP 13 | (Solo actualizaciones de cortafuegos de HA) Suspenda el peer de HA secundario para forzar una conmutación por error en el peer de HA principal.

1. [Inicie sesión en la interfaz web del cortafuegos](#) del peer de HA del cortafuegos secundario activo.
2. Seleccione **Device (Dispositivo) > High Availability (Alta disponibilidad) > Operational Commands (Comandos operativos)** y **Suspend local device for high availability (Suspende dispositivo local para alta disponibilidad)**.
3. En la esquina inferior derecha, verifique que el estado sea **suspended (suspendido)**.

La conmutación por error resultante debería hacer que el peer de HA pasivo principal cambie al estado **activo**.



La conmutación por error resultante verifica que la conmutación por error de HA funcione correctamente antes de realizar la actualización.

STEP 14 | (Solo actualizaciones en cortafuegos de HA) Actualice el segundo peer de HA en cada par de HA.

1. En la [interfaz web de Panorama](#), seleccione **Panorama > Device Deployment (Implementación del dispositivo) > Software**.
2. Haga clic en **Install (Instalar)** en la columna Action (Acción) que corresponda a los modelos de cortafuegos de los pares de HA que está actualizando.
3. En el cuadro de diálogo Deploy Software (Implementar software), seleccione todos los cortafuegos que desea actualizar. En este momento, seleccione solo los peers de los cortafuegos de HA que ya actualizó.
4. Asegúrese de que la opción **Group HA Peers (Agrupar peers de HA)** no esté seleccionada.
5. Seleccione **Reboot device after install (Reiniciar dispositivo tras la instalación)**.
6. Para comenzar la actualización, haga clic en **OK (Aceptar)**.
7. Una vez que la instalación se realiza completamente , reinicie mediante uno de los siguientes métodos:
 - Si se le pide que reinicie, haga clic en **Yes (Sí)**.
 - Si no se le solicita que reinicie, seleccione **Device (Dispositivo) > Setup (Configuración) > Operations (Operaciones)** y haga clic en **Reboot Device (Reiniciar dispositivo)**.

STEP 15 | (Solo actualizaciones de cortafuegos de HA) Restaure la funcionalidad de HA en el peer de HA secundario.

1. [Inicie sesión en la interfaz web del cortafuegos](#) del peer de HA del cortafuegos secundario suspendido.
2. Seleccione **Device (Dispositivo) > High Availability (Alta disponibilidad) > Operational Commands (Comandos operativos)** y **Make local device functional for high availability (Hacer que el dispositivo local sea funcional para alta disponibilidad)**.
3. En la esquina inferior derecha, verifique que el estado sea **Passive (Pasivo)**. Para cortafuegos en una configuración activa/activa, verifique que el estado sea **Active (Activo)**.
4. Espere a que se sincronice la configuración en ejecución del peer de HA.
En el **Dashboard (Panel)**, controle el estado de la configuración en ejecución en el widget de alta disponibilidad.

STEP 16 | (Solo modo FIPS-CC) Actualice Panorama y dispositivos gestionados en modo FIPS-CC.







La actualización de un cortafuegos gestionado en modo FIPS-CC requiere que restablezca el estado de conexión segura si agregó el recopilador de logs dedicado a la gestión de Panorama mientras el cortafuegos gestionado ejecutaba una versión de PAN-OS 11.0.

No necesita reincorporar el cortafuegos gestionado agregado a la gestión de Panorama si el cortafuegos gestionado ejecutaba PAN-OS 10.0 o una versión anterior.

STEP 17 | Verifique la versión de contenido y de software que se ejecutan en cada cortafuegos gestionado.

1. En Panorama, seleccione **Panorama > Managed Devices (Dispositivos gestionados)**.
2. Ubique los cortafuegos y revise el contenido y las versiones de contenido y de software en la tabla.

En los cortafuegos de HA, también puede verificar que el estado de HA de cada peer sea el esperado.

	DEVICE NAME	MODEL	IP Address	TEMPLATE	Status				SOFTWARE VERSION	APPS AND THREAT	ANTIVIRUS
			IPV4		DEVICE STATE	HA STATUS	CERTIFICATE	L... M... D...			
▼ <input type="checkbox"/> DG-VM (5/5 Devices Connected): Shared > DG-VM											
<input type="checkbox"/>	PA-VM-6	PA-VM		Stack-VM	Connected		pre-defined		8.1.0	8320-6307	3881-4345
<input type="checkbox"/>	PA-VM-73	PA-VM		Stack-Test73	Connected		pre-defined		9.1.3	8320-6307	3873-4337
<input type="checkbox"/>	PA-VM-95	PA-VM		Stack-VM	Connected		pre-defined		10.0.0	8320-6307	3881-4345
<input type="checkbox"/>	↶ PA-VM-96	PA-VM		Stack-VM	Connected	 Passive	pre-defined		10.0.0	8299-6216	3881-4345
	↶ PA-VM			Stack-Test92	Connected	 Active	pre-defined		10.0.0	8299-6216	3881-4345

STEP 18 | (Solo actualizaciones en cortafuegos de HA) Si deshabilitó la opción de preferencia en uno de sus cortafuegos de HA antes de la actualización, edite los **Election Settings (Ajustes de elección)** [**Device (Dispositivo) > High Availability (Alta disponibilidad)**], vuelva a habilitar el ajuste **Preemptive (Preferente)** para ese cortafuegos y haga clic en **Commit (Confirmar)** para confirmar el cambio.

STEP 19 | En la [interfaz web de Panorama](#) inserte toda la configuración gestionada de Panorama en los cortafuegos administrados.

Este paso es necesario para habilitar la confirmación selectiva y el envío de cambios en la configuración de la pila de plantillas y del grupo de dispositivos desde Panorama a los cortafuegos gestionados.

Esto es necesario para enviar con éxito los cambios de configuración a los cortafuegos de sistemas virtuales múltiples gestionados por Panorama después de una correcta actualización a PAN-OS 11.0 desde PAN-OS 10.1 o una versión anterior. Para obtener más información, consulte el cambio en el comportamiento predeterminado de [los objetos de configuración compartidos para cortafuegos de sistemas virtuales múltiples gestionados por Panorama](#).

1. Seleccione **Commit (Confirmar) > Push to Devices (Enviar a dispositivos)**.
2. **Push (Enviar)**.

STEP 20 | Vuelva a generar o a importar todos los certificados para cumplir con el nivel de seguridad 2 de OpenSSL.

Al actualizar a PAN-OS 10.2 o una versión posterior, se requiere que todos los certificados cumplan con los siguientes requisitos mínimos. Omita este paso si está actualizando desde PAN-OS 10.2 y ya volvió a generar o a importar los certificados.

- RSA de 2048 bits o superior, o ECDSA de 256 bits o superior
- Compendio de SHA256 o superior

Consulte la [Guía del administrador de PAN-OS](#) o la [Guía del administrador de Panorama](#) para obtener más información sobre la regeneración o reimportación de los certificados.

STEP 21 | Ver el historial de actualizaciones de software del cortafuegos.

1. Inicie sesión en la interfaz de Panorama.
2. Vaya a **Panorama > Managed Devices (Dispositivos gestionados) > Summary (Resumen)** y haga clic en **Device History (Historial de dispositivos)**.

Actualización de los cortafuegos cuando Panorama no está conectado a internet

Para obtener una lista de actualizaciones de software y contenido que puede instalar en los cortafuegos, consulte [Actualizaciones compatibles](#).

La nueva función [Omitir actualización de versión de software](#) le permite omitir hasta tres versiones al implementar actualizaciones de dispositivos Panorama en PAN-OS 11.0 a cortafuegos en PAN-OS 10.1 o versiones posteriores.

STEP 1 | Antes de actualizar los cortafuegos administrados, asegúrese de ejecutar PAN-OS 11.0 en el servidor de gestión de Panorama y los recopiladores de logs.



Palo Alto Networks® recomienda encarecidamente que Panorama y el Recopilador de logs ejecuten la misma versión de Panorama y que Panorama, Recopilador de logs y todos los cortafuegos gestionados ejecuten la misma versión de publicación de contenido.



Para obtener detalles importantes sobre la compatibilidad de contenido y software, consulte [Compatibilidad de versiones de Panorama, el recopilador de logs y el cortafuegos](#).

Panorama debe estar ejecutando el mismo (o posterior) lanzamiento de software que los cortafuegos, pero debe tener la misma versión de lanzamiento de contenido o una anterior:

- **Versión de lanzamiento de software.** si su servidor de gestión de Panorama o Recopilador de logs no está ejecutando la misma versión de software que la versión para la que desea actualizar los cortafuegos, entonces debe instalar la misma versión de Panorama o posterior en Panorama y luego en el Recopilador de logs (consulte [Instalar contenido y actualizaciones de software para Panorama](#)) antes de actualizar cualquier cortafuegos.
- **Versión de lanzamiento del contenido:** para lanzamiento de versiones de contenido, debe asegurarse de que todos los servidores de seguridad estén ejecutando la última versión de publicación de contenido o, como mínimo, ejecuten una versión posterior a la que se está ejecutando

en Panorama y Recopilador de logs; de lo contrario, actualice los cortafuegos gestionados y luego [Actualice los recopiladores de logs cuando Panorama no está conectado a Internet](#) antes de actualizar la versión de publicación de contenido en el servidor de gestión de Panorama (consulte [Instalación de actualizaciones de software y contenido de Panorama](#)).

Para comprobar el software y las versiones de contenido:

- **Servidor de gestión de Panorama:** inicie sesión en la interfaz web de Panorama y vaya a la configuración de Información general (**Dashboard [Panel]**).
- **Recopilador de logs:** inicie sesión en la CLI de cada recopilador de logs y ejecute el comando **show system info**.

STEP 2 | Guarde una copia de seguridad del archivo de configuración actual en cada cortafuegos gestionado que desee actualizar.



A pesar de que el cortafuegos crea automáticamente una copia de seguridad de la configuración, se recomienda crear y almacenar externamente una copia de seguridad antes de la actualización.

1. Asegúrese de **Export Panorama and devices config bundle (Exportar Panorama y lote de configuración de dispositivos)** (**Panorama > Setup [Configuración] > Operations [Operaciones]**) para generar y exportar la versión más reciente de la copia de seguridad de configuración de Panorama y de cada dispositivo gestionado.
2. Guarde el archivo exportado en una ubicación externa al cortafuegos. Puede usar esta copia de seguridad para restaurar la configuración si tiene problemas con la actualización.

STEP 3 | Determine qué actualizaciones de contenido necesita instalar. Consulte las [notas de versión](#) para obtener la versión de contenido mínima que debe instalar para una versión de PAN-OS®.



Palo Alto Networks recomienda encarecidamente que Panorama, los recopiladores de logs y todos los cortafuegos gestionados ejecuten la misma versión de publicación de contenido.

Para cada actualización de contenido, determine si necesita actualizaciones y tome nota sobre qué actualizaciones de contenido debe descargar en el siguiente paso.



Asegúrese de que Panorama ejecute la misma versión de publicación de contenido, pero no una posterior, que la que se ejecuta en los cortafuegos gestionados y los recopiladores de logs.

STEP 4 | [Determine la ruta de actualización del software](#) para los cortafuegos que desee actualizar a Panorama 11.0.

Inicie sesión en Panorama, seleccione **Panorama > Managed Collectors (Recopiladores gestionados)** y observe la versión de software actual para los cortafuegos que desea actualizar.



Revise [Lista de control para actualizar PAN-OS](#), los problemas conocidos y los cambios en el comportamiento predeterminado en las [Notas de la versión](#) y [Consideraciones sobre el cambio a versiones anteriores/posteriores de complementos de Panorama](#) para cada versión a través de la cual pase como parte de la ruta de cambio a una versión posterior.

STEP 5 | (Opcional) Actualice los cortafuegos gestionados a PAN-OS 10.1.

La función de omitir actualización de versión de software de es compatible con cortafuegos gestionados que ejecutan PAN-OS 10.1 o versiones posteriores. Si los cortafuegos gestionados están en PAN-OS 10.0 o una versión anterior, primero actualice a PAN-OS 10.1 o una versión posterior.

STEP 6 | Realice una comprobación de validación de la versión.

En este paso, puede ver el software intermedio y las imágenes de contenido necesarias para actualizar a 11.0.

1. Seleccione **Panorama > Device Deployment (Implementación del dispositivo) > Software > Action (Acción) > Validate (Validar)**.
2. Vea las versiones intermedias de software y contenido que necesita descargar.

STEP 7 | Descargue el contenido y las actualizaciones de software a un host que pueda conectarse y cargar los archivos en Panorama o en un servidor SCP configurado a través de SCP o HTTPS.

De forma predeterminada, puede cargar un máximo de dos actualizaciones de software o contenido de cada tipo a un dispositivo Panorama y si descarga una tercera actualización del mismo tipo, Panorama eliminará la actualización de la versión más antigua de ese tipo. Si necesita cargar más de dos actualizaciones de software o actualizaciones de un solo tipo, use el comando de la CLI **set max-num-images count <number>** para aumentar la cantidad máxima de imágenes que puede almacenar Panorama.

1. Use un host con acceso a internet para iniciar sesión en el [sitio web de Atención al cliente de Palo Alto Networks](#).
2. Descargue las actualizaciones de contenido:
 1. Haga clic en **Dynamic Updates (Actualizaciones dinámicas)** en la sección Recursos.
 2. Debe **Download (Descargar)** la última versión de publicación de contenido (o, como mínimo, la misma o una versión posterior a la que instalará o está ejecutando en el servidor de gestión de Panorama) y guardar el archivo en el host; repita para cada tipo de contenido que necesite actualizar.
3. Descargue las actualizaciones de software:
 1. Vuelva a la página principal del sitio web de Atención al cliente de Palo Alto Networks y haga clic en **Software Updates (Actualizaciones de software)** de la sección Recursos.
 2. Revise la columna Download (Descargar) para determinar las versiones que desea instalar. El nombre de archivo de los paquetes de actualización indica el modelo. Por ejemplo, para actualizar un cortafuegos PA-220 y PA-5260 a PAN-OS 11.0.0, descargue las imágenes **PanOS_220-11.0.0**, **PanOS_3000-11.0.0** y **PanOS_5200-11.0.0**.



*Puede localizar rápidamente imágenes PAN-OS específicas seleccionando **PAN-OS for the PA (PAN-OS para el PA)**-<series/model> desde el menú desplegable **Filter By (Filtrar por)**.*

4. Haga clic en el nombre de archivo adecuado y guarde el archivo en el host.

STEP 8 | Descargue las versiones de software intermedias y la última versión de contenido.

En PAN-OS 11.0, puede descargar varias versiones intermedias mediante la función de descarga de varias imágenes.

1. Seleccione los cortafuegos que desea actualizar (**Required Deployments [Implementaciones requeridas]** > **Deploy [Implementar]**).
2. Seleccione el origen de la descarga y haga clic en **Download (Descargar)**.

STEP 9 | Instale actualizaciones de contenido en cortafuegos gestionados.



Debe instalar las actualizaciones de contenido antes que las actualizaciones de software.

Instale la actualización de aplicaciones o aplicaciones y amenazas primero, y luego instale cualquier otra actualización (antivirus, WildFire® o filtrado de URL) según sea necesario una a la vez y en cualquier secuencia.

1. Seleccione **Panorama > Device Deployment (Implementación de dispositivos) > Dynamic Updates (Actualizaciones dinámicas)**.
2. Haga clic en **Upload (Cargar)**, seleccione el tipo de actualización en **Type (Tipo)**, haga clic en **Browse (Examinar)** para ir al archivo de actualización y, luego, en **OK (Aceptar)**.
3. Haga clic en **Install From File (Instalar desde el archivo)**, seleccione el **Type (Tipo)** de actualización y seleccione el **File Name (Nombre de archivo)** de la actualización de contenido que acaba de cargar.
4. Seleccione los cortafuegos en los que quiere instalar la actualización.
5. Haga clic en **OK (Aceptar)** para iniciar la instalación.
6. Repita estos pasos para cada actualización de contenido.

STEP 10 | (Cortafuegos que funcionan como portales de GlobalProtect™ únicamente) Cargue y active una actualización del software del agente/aplicación GlobalProtect en los cortafuegos.



Active la actualización en los cortafuegos de modo que los usuarios puedan descargarla en sus endpoints (sistemas cliente).

1. Use un host con acceso a internet para iniciar sesión en el [Sitio web de atención al cliente de Palo Alto Networks](#).
2. Descargue la actualización adecuada del software del agente/aplicación de GlobalProtect.
3. En Panorama, seleccione **Panorama > Device Deployment (Implementación del dispositivo) > GlobalProtect Client (Cliente GlobalProtect)**.
4. Haga clic en **Upload (Cargar)**, seleccione **Browse (Examinar)** la actualización del software del agente/aplicación GlobalProtect correspondiente en el host al que descargó el archivo, y haga clic en **OK (Aceptar)**.
5. Seleccione **Activate From File (Activar desde archivo)** y seleccione **File Name (Nombre de archivo)** de la actualización de agente/aplicación de GlobalProtect que acaba de cargar.



Puede activar solo una versión del software de agente/software de la aplicación a la vez. Si activa una nueva versión, pero algunos agentes requieren una versión anterior, tendrá que volver a activar la versión anterior para que esos agentes descarguen la actualización anterior.

6. Seleccione los cortafuegos en los que quiere activar la actualización.
7. Haga clic en **OK (Aceptar)** para activar.

STEP 11 | Instale PAN-OS 11.0.



Para evitar el estado de inactividad al actualizar el software en cortafuegos de alta disponibilidad (high availability, HA), actualice un peer de HA a la vez.

Para los cortafuegos activo/activo, no importará qué peer actualice primero.

Para los cortafuegos activo/pasivo, debe actualizar el peer pasivo primero, suspender el peer activo (conmutación por error), actualizar el peer activo y luego regresar el peer activo a un estado funcional (conmutación por recuperación).



*(Solo en el caso de SD-WAN) Para conservar un estado preciso de los vínculos de SD-WAN, debe cambiar los cortafuegos de centrales a la versión posterior PAN-OS 11.0 antes de actualizar los cortafuegos de sucursales. La actualización de los cortafuegos de sucursales antes que los cortafuegos de central puede provocar datos de supervisión incorrectos (**Panorama [Panorama] > SD-WAN [SD-WAN] > Monitoring [Supervisión]**) y que los enlaces de SD-WAN se muestren de forma incorrecta como **down (inactivo)**.*

1. Realice los pasos que se aplican a su configuración de cortafuegos para instalar la actualización del software PAN-OS que acaba de cargar.
 - **Cortafuegos que no son de HA:** Haga clic en **Install (Instalar)** en la columna Acción, seleccione todos los cortafuegos que está actualizando, seleccione **Reboot device after install (Reiniciar dispositivo después de la instalación)** y haga clic en **OK (Aceptar)**.
 - **Cortafuegos de HA activo/activo:**
 1. Confirme que la configuración de preferencia está deshabilitada en el primer peer que desea actualizar (**Device [Dispositivo] > High Availability [Alta disponibilidad] > Election Settings [Configuración de elección]**). Si está habilitado, edite **Election Settings (Configuración de elección)** y deshabilite (retire marca) el ajuste **Preemptive (Preferente)** y **Commit (Confirme)** su cambio. Solo necesita desactivar esta configuración en un cortafuegos en cada par de HA, pero asegúrese de que la confirmación sea correcta antes de continuar.
 2. Haga clic en **Install (Instalar)**, deshabilite (retire marca) la casilla de verificación de **Group HA Peers (Peers de HA del grupo)**, seleccione cualquier peer de HA, seleccione **Reboot device after install (Reiniciar dispositivo después de la instalación)** y haga clic en **OK (Aceptar)**. Espere que el cortafuegos termine de reiniciarse antes de continuar.
 3. Haga clic en **Install (Instalar)**, deshabilite (retire marca) la casilla de verificación de **Group HA Peers (Peers de HA del grupo)**, seleccione el peer de HA que todavía no actualizó, seleccione **Reboot device after install (Reiniciar dispositivo después de la instalación)** y haga clic en **OK (Aceptar)**.
 - **Cortafuegos de HA activo/pasivo:** en este ejemplo, el cortafuegos activo se llama fw1 y el cortafuegos pasivo se llama fw2:
 1. Confirme que la configuración de preferencia esté deshabilitada en el primer peer que desea actualizar (**Device [Dispositivo] > High Availability [Alta disponibilidad] > Election Settings [Configuración de elecciones]**). Si está habilitado, edite **Election Settings (Configuración de elección)** y deshabilite (retire marca) el ajuste **Preemptive**

- (Preferente) y **Commit (Confirme)** su cambio. Solo necesita desactivar esta configuración en un cortafuegos en cada par de HA, pero asegúrese de que la confirmación sea correcta antes de continuar.
2. clic en **Install (Instalar)** en la columna Action (Acción) para la actualización correspondiente, deshabilite (desmarque) **Group HA Peers (Peers del grupo de HA)**, seleccione fw2, **Reboot device after install (Reiniciar dispositivo después de la instalación)** y haga clic en **OK (Aceptar)**. Espere que fw2 termine de reiniciarse antes de continuar.
 3. Después de que fw2 termine de reiniciarse, verifique en fw1 (**Dashboard [Panel] > High Availability [Alta disponibilidad]**) que fw2 sigue siendo el peer pasivo (el estado del cortafuegos local es **active [activo]** y el del Peer fw2 es **passive [pasivo]**).
 4. Acceda a fw1 y seleccione **Suspend local device (Suspendir dispositivo local) (Device [Dispositivo] > High Availability [Alta disponibilidad] > Operational Commands [Comandos operativos])**.
 5. Acceda a fw2 (**Dashboard [Panel] > High Availability [Alta disponibilidad]**), verifique que el estado del cortafuegos local sea **active (activo)** y que el del peer sea **suspended (suspendido)**.
 6. Acceda a Panorama, seleccione **Panorama > Device Deployment (Implementación del dispositivo) > Software**, haga clic en **Install (Instalar)** en la columna Action (Acción) de la versión correspondiente, deshabilite (desmarque) **Group HA Peers (Peers de HA del grupo)**, seleccione fw1, **Reboot device after install (Reiniciar dispositivo después de la instalación)** y haga clic en **OK (Aceptar)**. Espere que fw1 termine de reiniciarse antes de continuar.
 7. Acceda a fw1 (**Device [Dispositivo] > High Availability [Alta disponibilidad] > Operational Commands [Comandos operativos]**), haga clic en **Make local device functional (Hacer dispositivo local funcional)** y espere dos minutos antes de continuar.
 8. En fw1 (**Dashboard [Panel] > High Availability [Alta disponibilidad]**), verifique que el estado del cortafuegos local sea **passive (pasivo)** y el del peer (fw2) sea **active (activo)**.

STEP 12 | (Solo modo FIPS-CC) **Actualice Panorama y dispositivos gestionados en modo FIPS-CC.**

La actualización de un cortafuegos gestionado en modo FIPS-CC requiere que restablezca el estado de conexión segura si agregó el recopilador de logs dedicado a la gestión de Panorama mientras el cortafuegos gestionado ejecutaba una versión de PAN-OS 11.0.

No necesita reincorporar el cortafuegos gestionado agregado a la gestión de Panorama si el cortafuegos gestionado ejecutaba PAN-OS 10.0 o una versión anterior.

STEP 13 | Verifique las versiones de contenido o de software que se instalan en cada cortafuegos gestionado.

1. Seleccione **Panorama > Managed Devices (Dispositivos gestionados)**.
2. Busque el cortafuegos y revise los valores de las columnas Versión de software, Aplicaciones y amenazas, Antivirus, Filtrado de URL y Cliente de GlobalProtect.

STEP 14 | Si deshabilitó la preferencia en uno de sus cortafuegos HA antes de actualizar, edite la **Election Settings (Configuración de elección) [Device (Dispositivo) > High Availability (Alta disponibilidad)]** y vuelva a habilitar el ajuste **Preemptive (Preferente)** para ese cortafuegos.

STEP 15 | En la [interfaz web de Panorama](#) inserte toda la configuración gestionada de Panorama en los cortafuegos administrados.

Este paso es necesario para habilitar la confirmación selectiva y el envío de cambios en la configuración de la pila de plantillas y del grupo de dispositivos desde Panorama a los cortafuegos gestionados.

Esto es necesario para enviar con éxito los cambios de configuración a los cortafuegos de sistemas virtuales múltiples gestionados por Panorama después de una correcta actualización a PAN-OS 11.0. Para obtener más información, consulte el cambio en el comportamiento predeterminado de [los objetos de configuración compartidos para cortafuegos de sistemas virtuales múltiples gestionados por Panorama](#).

1. Seleccione **Commit (Confirmar) > Push to Devices (Enviar a dispositivos)**.
2. **Push (Enviar)**.

STEP 16 | Vuelva a generar o a importar todos los certificados para cumplir con el nivel de seguridad 2 de OpenSSL.

Al actualizar a PAN-OS 11.0, se requiere que todos los certificados cumplan con los siguientes requisitos mínimos:

- RSA de 2048 bits o superior, o ECDSA de 256 bits o superior
- Compendio de SHA256 o superior

Consulte la [Guía del administrador de PAN-OS](#) o la [Guía del administrador de Panorama](#) para obtener más información sobre la regeneración o reimportación de los certificados.

STEP 17 | Ver el historial de actualizaciones de software del cortafuegos.

1. Inicie sesión en la interfaz de Panorama.
2. Vaya a **Panorama > Managed Devices (Dispositivos gestionados) > Summary (Resumen)** y haga clic en **Device History (Historial de dispositivos)**.

Actualización de un cortafuegos de ZTP

Después de [añadir con éxito un cortafuegos de ZTP](#) al servidor de gestión Panorama™, configure la versión de PAN-OS de destino del cortafuegos de ZTP. Panorama comprueba si la versión de PAN-OS instalada en el cortafuegos de ZTP es superior o igual que la versión de PAN-OS de destino configurada después de que se conecte correctamente a Panorama por primera vez. Si la versión de PAN-OS instalada en el cortafuegos de ZTP es inferior a la versión de PAN-OS de destino, el cortafuegos de ZTP entra en un ciclo de actualización hasta que se instala la versión de PAN-OS de destino.

STEP 1 | [Inicie sesión en la interfaz web de Panorama](#) como usuario administrador.

STEP 2 | [Añada un cortafuegos ZTP a Panorama](#).

STEP 3 | Seleccione **Panorama > Device Deployment (Implementación del dispositivo) > Updates (Actualizaciones)** y **Check Now (Comprobar ahora)** para comprobar las últimas versiones de PAN-OS.

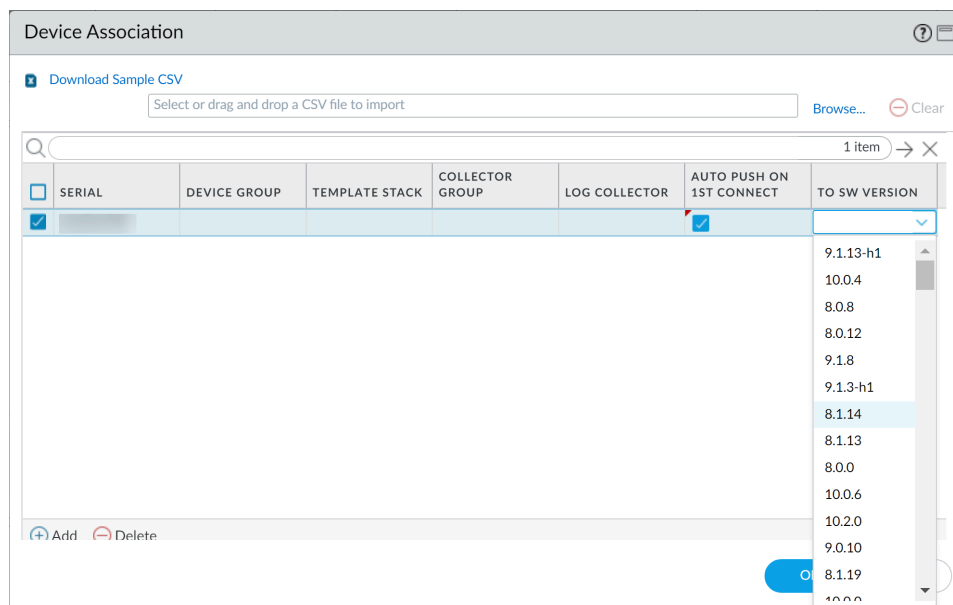
STEP 4 | Seleccione **Panorama > Managed Devices > Summary (Resumen)** y seleccione uno o más cortafuegos de ZTP.

STEP 5 | Vuelva a asociar los cortafuegos de ZTP seleccionados.

STEP 6 | Marque (habilite) Auto Push en 1st Connect Insertar automáticamente en 1.ª conexión).

STEP 7 | En la columna To SW Version (Versión de SW de destino), seleccione la versión de PAN-OS de destino para el cortafuegos de ZTP.

STEP 8 | Haga clic en Aceptar para guardar los cambios.



STEP 9 | Haga clic en Commit (Confirmar) y en Commit to Panorama (Confirmar en Panorama).

STEP 10 | Encienda el cortafuegos de ZTP.

Cuando el cortafuegos de ZTP se conecta a Panorama por primera vez, se actualiza automáticamente a la versión de PAN-OS que seleccionó.

- **Panorama con PAN-OS 11.0.0:** si está actualizando cortafuegos gestionados en versiones principales o de mantenimiento de PAN-OS, las versiones intermedias de PAN-OS en la ruta de actualización se instalan primero, antes de que se instale la versión PAN-OS de destino.

Por ejemplo, configuró **To SW Version (A la versión de SW)** de destino para el cortafuegos gestionado como PAN-OS 11.0.0 y el cortafuegos ejecuta PAN-OS 10.1. En la primera conexión a Panorama, PAN-OS 10.2.0 se instala primero en el cortafuegos gestionado. Una vez que PAN-OS 10.2.0 se instala correctamente, el cortafuegos se actualiza automáticamente a la versión PAN-OS 11.0.0 de destino.

- **Panorama con PAN-OS 11.0.1 y versiones posteriores:** si está actualizando cortafuegos gestionados en versiones principales o de mantenimiento de PAN-OS, se instalan las versiones intermedias principales de PAN-OS en la ruta de actualización y se descarga la versión base principal de PAN-OS antes de que se instale la versión de mantenimiento de PAN-OS de destino.

Por ejemplo, configuró **To SW Version (A la versión de SW)** de destino para el cortafuegos gestionado como PAN-OS 11.0.1 y el cortafuegos ejecuta PAN-OS 10.0. En la primera conexión a Panorama, PAN-OS 10.1.0 y PAN-OS 10.2.0 están instalados en el cortafuegos gestionado. Después de que el cortafuegos gestionado se reinicia, se descarga PAN-OS 11.0.0 y luego el cortafuegos se instala automáticamente en la versión de PAN-OS 11.0.1 de destino.

STEP 11 | Verifique la actualización del software del cortafuegos de ZTP.

1. [Inicio de sesión en la interfaz web de Panorama](#).
2. Seleccione **Panorama > Managed Devices > Summary (Resumen)** y diríjase a los cortafuegos de ZTP.
3. Verifique que la columna **Software Version (Versión de software)** muestre la versión correcta de PAN-OS de destino.

STEP 12 | Para todas las futuras actualizaciones de PAN-OS, consulte [Actualización del cortafuegos a PAN-OS 11.0 desde Panorama](#).

Restablecimiento de las actualizaciones de contenido de Panorama

Panorama™ le permite revertir con rapidez las aplicaciones, aplicaciones y amenazas, antivirus, WildFire®, y versiones de contenido de WildFire en uno o más cortafuegos, los recopiladores de logs o los dispositivos WildFire directamente desde Panorama. Utilice Panorama para revertir las versiones de contenido instaladas en dispositivos gestionados para aprovechar un flujo de trabajo centralizado que ayude a mitigar los riesgos asociados con la introducción o la modificación de las aplicaciones o las nuevas firmas de amenazas en una actualización de contenido. Panorama genera un log de sistema para cada dispositivo cuando revierte contenido. Asegúrese de utilizar [Prácticas recomendadas para las actualizaciones de contenido de aplicaciones y amenazas](#) cuando implemente actualizaciones de contenido en los dispositivos gestionados.

STEP 1 | [Inicie sesión en la interfaz web de Panorama](#).

STEP 2 | Seleccione **Panorama > Device Deployment (Implementación del dispositivo) > Dynamic Updates (Actualizaciones dinámicas)** y haga clic en **Revert Content (Revertir contenido)**.

STEP 3 | Seleccione el tipo de contenido que desea revertir.

Antivirus
Apps
Applications and Threats
WildFire
WildFire-Content

STEP 4 | Seleccione uno o más cortafuegos en los que se revertirá contenido y haga clic en **OK (Aceptar)**. La versión de contenido que revierte debe ser una versión más antigua que la versión instalada actualmente en el dispositivo.

Revert Antivirus Content

Filters

Device State

Connected (3)

Platforms

Log Collectors (1)

Device Groups

dg1 (2)

Templates

ts_1 (2)

Tags

HA Status

Software Version

10.0.0 (1)

Current Content Version

Devices

3 items

	DEVICE NAME	CURRENT VERSION	PREVIOUS VERSION	SOFTWARE VERSION	HA STATUS
<input type="checkbox"/>	M-200			10.0.0	
<input type="checkbox"/>	PA-3260-1	3949-4413	3873-4337	10.0.0	
<input type="checkbox"/>	PA-3260-2	3946-4410	3881-4345	10.0.0	

☐ Group HA Peers

☐ Filter Selected (0)

OK

Cancel

Cambio de PAN-OS a una versión posterior

- > Lista de control para actualizar PAN-OS
- > Consideraciones sobre el cambio a versiones anteriores/posteriores de complementos de Panorama
- > Cambio del cortafuegos a la versión posterior PAN-OS 11.0
- > Actualización del cortafuegos a PAN-OS 11.0 desde Panorama
- > Cambio a una versión anterior de PAN-OS
- > Solución de problemas del cambio a versiones posteriores de PAN-OS

Lista de control para actualizar PAN-OS

La planificación de la actualización de PAN-OS puede ayudar a garantizar una transición más fluida a una versión más reciente de PAN-OS para su Panorama o cortafuegos.

- ❑ Asegúrese de que el dispositivo esté registrado y con licencia.
- ❑ Compruebe el espacio disponible en disco.

El espacio en disco necesario varía según la versión de PAN-OS. Seleccione **Device (Dispositivo)** > **Software (Software)** y revise el **tamaño** de la versión de PAN-OS de destino para determinar el espacio en disco necesario.

- ❑ Ejecute **show system disk-space**
- ❑ Compruebe la versión mínima de lanzamiento de contenido.
- ❑ Identifique la versión preferida.

Consulte la [Guía de la versión del software de soporte de Palo Alto Networks](#) y el [Resumen del final de la vida útil](#) para obtener más información. Además, revise los problemas conocidos y resueltos, las consideraciones de cambio a versiones anteriores y posteriores, y las limitaciones de su versión de PAN-OS de destino para comprender cómo el cambio a una versión posterior de PAN-OS puede afectarlo.

- ❑ Determine la ruta de actualización.



Cuando actualiza de una versión de lanzamiento de funciones de PAN-OS a una versión de funciones posterior, no puede omitir la instalación de ninguna versión de lanzamiento de funciones en la ruta a la versión de destino.

- ❑ Revise las consideraciones sobre cambio a versiones anteriores/posteriores para todas las versiones de la ruta de actualización.
- ❑ **(Requerido para GlobalProtect)** Verifique la versión mínima del agente GlobalProtect™ para evitar que los usuarios de GlobalProtect pierdan la conectividad VPN. GlobalProtect se puede actualizar directamente a la última versión.
- ❑ Verifique las versiones mínimas de lanzamiento del complemento en la versión de lanzamiento de destino para cualquier complemento que haya instalado.
- ❑ Compruebe la conectividad desde la interfaz de administración al servidor de actualización.
- ❑ Seleccione **Device (Dispositivo)** > **Troubleshooting (Solución de problemas)** y pruebe la **conectividad del servidor de actualización** para comprobar que el DNS pueda resolver la dirección.

Si no se resuelve, cambie el DNS a **8.8.8.8** (debe usar un servidor DNS público, en lugar de su propio servidor DNS) y vuelva a hacer ping.

Si esto no se resuelve, cambie el servidor de actualización a **staticupdates.paloaltonetworks.com** y **confirme**.

- ❑ **(Solo para SD-WAN)** Identifique los cortafuegos de central y sucursal a actualizar a PAN-OS 10.2.

Para conservar un estado preciso de los vínculos de SD-WAN, debe actualizar los cortafuegos de centrales a la versión posterior PAN-OS 11.0 antes de actualizar los cortafuegos de sucursales a versiones posteriores. Cambiar los cortafuegos de sucursal a versiones posteriores antes que los

cortafuegos de central puede provocar datos de supervisión incorrectos (**Panorama [Panorama] > SD-WAN [SD-WAN] > Monitoring [Supervisión]**) y que los enlaces de SD-WAN se muestren de forma incorrecta como **down (inactivo)**.

- ❑ Si hay complementos instalados actualmente, descargue la versión del complemento compatible con PAN-OS 11.0 para todos los complementos instalados actualmente en Panorama (**Panorama > Plugins (Complementos)**) o su cortafuegos (**Device (Dispositivo) > Plugins (Complementos)**) antes de la actualización.

Consulte la [matriz de compatibilidad de complementos de Panorama](#) para la versión de complemento de Panorama compatible con PAN-OS 10.2.


Esto es necesario para actualizar correctamente Panorama y el cortafuegos de PAN-OS 11.0 a PAN-OS 10.2. La versión descargada del complemento se instala automáticamente durante la actualización a PAN-OS 10.2. La actualización a PAN-OS 11.0 se bloquea si no se descarga la versión de complemento compatible.

Consideraciones sobre el cambio a versiones anteriores/posteriores de complementos de Panorama

En la siguiente tabla, se muestran las nuevas funciones que tienen un impacto de actualización o degradación. Asegúrese de comprender todas las consideraciones sobre el cambio a versiones anteriores/posteriores antes de cambiar a una versión anterior o posterior desde una versión PAN-OS 11.0. Para obtener más información sobre las versiones de PAN-OS 11.0, consulte las [Notas de la versión de PAN-OS 11.0](#).

Función	Consideraciones de actualización	Consideraciones de degradación
Complemento de servicios en la nube	Actualizar a PAN-OS 11.0 con la última versión del complemento de servicios en la nube no es compatible. La actualización a PAN-OS 11.0 con una versión del complemento de servicios en la nube no compatible puede dar lugar a problemas desconocidos o inesperados que pueden afectar tanto a Prisma Access como a la funcionalidad del complemento dependiente.	Ninguno.
Requisito mínimo de memoria del sistema para el dispositivo virtual Panorama	Palo Alto Networks ha aumentado el requisito de memoria de la aplicación virtual Panorama recomendado a un mínimo de 64 GB, frente a los 32 GB anteriores. Esto afecta a los dispositivos virtuales Panorama en modo Panorama y en modo de recopilación de logs para evitar cualquier problema de creación de logs, gestión y rendimiento operativo relacionado con un dispositivo virtual Panorama insuficientemente aprovisionado. Para las nuevas implementaciones de dispositivos virtuales Panorama, Palo Alto Networks recomienda implementar la máquina virtual	Ninguno.

Función	Consideraciones de actualización	Consideraciones de degradación
	<p>con un mínimo de 64 GB. Para implementaciones de dispositivos virtuales Panorama existentes, consulte Aumentar las CPU y la memoria del dispositivo virtual Panorama para aumentar la memoria de un dispositivo virtual Panorama existente después de actualizar correctamente a PAN-OS 11.0.</p>	
Compatibilidad con TLSv1.3 para acceso administrativo	<p>El cortafuegos establece automáticamente Management TLS Mode (Modo de gestión TLS) en excludetls1.3_only y Certificate (Certificado) en none (ninguno) cuando actualiza el cortafuegos. Si utilizó un perfil de servicio SSL/TLS para asegurar las conexiones de gestión antes de la actualización, el perfil sigue funcionando.</p> <p>Para habilitar la compatibilidad con TLSv1.3 para el acceso administrativo, deberá ir a General Settings (Configuración general) (Device [Dispositivo] > Setup [Configuración] > Management [Gestión] > General Settings [Configuración general]), establecer Management TLS Mode (Modo de gestión TLS) en tls1.3_only o en mixed-mode (modo mixto) y luego seleccionar un certificado de servidor de gestión.</p>	<p>La compatibilidad con TLSv1.3 desaparece cuando se degrada de PAN-OS 11.0 a una versión anterior de PAN-OS.</p> <p>Si habilitó la compatibilidad con TLSv1.3 o no utilizó un perfil de servicio SSL/TLS para las conexiones de gestión, el cortafuegos admite todas las versiones de TLS excepto TLSv1.3 (TLSv1.0-TLSv1.2) y los conjuntos de cifrado asociados.</p> <p>Sin embargo, si utilizó un perfil de servicio SSL/TLS antes de la degradación, el cortafuegos seguirá utilizando ese perfil.</p>

Función	Consideraciones de actualización	Consideraciones de degradación
	 <p><i>La configuración de la compatibilidad con TLSv1.3 deshabilita el perfil de servicio SSL/TLS utilizado para las conexiones de gestión antes de la actualización.</i></p>	
Formato de syslog personalizado	Ninguno.	<p>Debe reducir el formato de syslog personalizado (Device (Dispositivo) > Server Profiles (Perfiles de servidor) > Syslog y Panorama > Server Profiles (Perfiles de servidor) > Syslog) a un máximo de 2346 caracteres para actualizar correctamente a PAN-OS 10.2.</p>
Contexto de usuario para Cloud Identity Engine	<p>Palo Alto Networks recomienda encarecidamente crear registros detallados de la arquitectura de asignación y redistribución de etiquetas antes de habilitar el servicio en la nube de contexto de usuario. Si es necesaria una degradación, utilice los registros de arquitectura para volver a crear esa configuración después de la degradación para rellenar las asignaciones y etiquetas.</p>	<p>Después de degradar de PANOS 11.0 a una versión anterior, la opción de servicio en la nube de contexto de usuario ya no está disponible. Además, la degradación borra las asignaciones de dirección IP a nombre de usuario, las asignaciones de dirección IP a número de puerto, las listas de cuarentena, las asignaciones de dirección IP a etiqueta y las etiquetas de grupo dinámico de usuarios del dispositivo degradado.</p> <p>Antes de degradar, si habilitó la opción de servicio en la nube de contexto de usuario, habilite la configuración anterior para los orígenes de las asignaciones, etiquetas y listas de cuarentena en el cortafuegos o Panorama para que la información se</p>

Función	Consideraciones de actualización	Consideraciones de degradación
		<p>vuelva a rellenar correctamente después de degradar.</p> <p>Palo Alto Networks recomienda usar los siguientes comandos de la CLI en el cortafuegos inmediatamente antes de la degradación para establecer un registro de referencia de los datos. Si es necesaria una actualización, esto le permite comparar los datos antes y después de la actualización para verificar que todos los datos necesarios estén disponibles en el cortafuegos después de la actualización:</p> <ul style="list-style-type: none">• Utilice el comando <code>show user ip-user-mapping all</code> para obtener el número actual de asignaciones de direcciones IP a nombres de usuario.• Utilice el comando <code>show user ip-port-user-mapping all</code> para obtener el número actual de asignaciones de direcciones IP a números de puerto.• Utilice el comando <code>show object registered-ip all option count</code> para obtener el número actual de asignaciones de direcciones IP a etiquetas.• Utilice el comando <code>show object registered-user all</code> para obtener el número actual de asignaciones de etiqueta a nombre de usuario.• Utilice el comando <code>debug user-id dump hip-profile-database</code> para

Función	Consideraciones de actualización	Consideraciones de degradación
		<p>obtener una lista de todos los dispositivos asociados con un perfil HIP.</p> <ul style="list-style-type: none"> • Exportar la lista de dispositivos en cuarentena en formato PDF o CSV. <p>Mediante los comandos de la CLI, compare la salida previa y posterior a la degradación para verificar que la cantidad de datos es aproximadamente la misma y asegúrese de que los datos necesarios estén disponibles en el cortafuegos antes de usar el cortafuegos para hacer cumplir la política.</p> <p>Debe restaurar manualmente todas las asignaciones de orígenes de API XML y todos los dispositivos que se añadieron manualmente a una lista de cuarentena.</p> <p>Si las asignaciones y etiquetas importadas mediante la API XML o las máquinas que se agregaron manualmente a la lista de cuarentena no se devuelven y validan después de la degradación, esto puede presentar un riesgo de seguridad, puesto que posiblemente los anteriores usuarios y dispositivos en cuarentena ya no tengan restringido el acceso a los recursos a los que no están autorizados.</p> <p>Por ejemplo, si se asignó una etiqueta específica a un usuario a través de la API XML que los agregó a un grupo de usuarios dinámicos por cuarentena, ese usuario ya no estará en el grupo de usuarios dinámicos en cuarentena hasta que agregue manualmente a ese usuario</p>

Función	Consideraciones de actualización	Consideraciones de degradación
		<p>después de la degradación. Si agregó un dispositivo a la lista de cuarentena antes de la degradación manualmente, debe agregarlo manualmente después de la degradación, o el dispositivo ya no se estará en cuarentena, lo que presenta un posible riesgo de seguridad.</p>
<p>Asignación de usuarios mediante sondeo de clientes de NetBIOS</p>	<p>Como parte de nuestros esfuerzos continuos para fortalecer aún más la seguridad de User-ID y eliminar cualquier vulnerabilidad de seguridad potencial debido a una configuración incorrecta, el método obsoleto de asignación de usuarios mediante sondeo de clientes de NetBIOS ya no es compatible en esta versión. Si actualmente utiliza este método para recopilar asignaciones de usuarios, debe configurar un método alternativo antes realizar la actualización para asegurarse de que la identificación del usuario continúe sin interrupciones. Para obtener más información sobre métodos alternativos de asignación, consulte la documentación PAN-OS. Después de actualizar, el sondeo de clientes de NetBIOS (Device [Dispositivo] > User Identification [Identificación de usuario] > User Mapping [Asignación de usuarios] > Palo Alto Networks User-ID Agent Setup [Configuración de agente de User-ID de Palo Alto Networks] > Client Probing [Sondeo de clientes]) ya no está disponible. El sondeo de clientes de NetBIOS tampoco está disponible en la versión</p>	<p>Ninguno.</p>

Función	Consideraciones de actualización	Consideraciones de degradación
	11.0 del agente de User-ID de Windows.	
OCSP a través de proxy HTTP	Ninguno.	Si actualiza a una versión de PAN-OS anterior a PAN-OS 11.0, tendrá que utilizar el método lista de revocación de certificados (CRL) para confirmar el estado de los certificados. El tráfico OCSP no puede pasar a través de proxies HTTP en versiones de PAN-OS anteriores a PAN-OS 11.0.

Cambio del cortafuegos a la versión posterior PAN-OS 11.0

La forma de cambiar a la versión posterior PAN-OS 11.0 depende de si tiene cortafuegos independientes o cortafuegos en una configuración de alta disponibilidad (HA) y, en cualquier caso, si usa Panorama para gestionar los cortafuegos. Revise las [Notas de la versión de PAN-OS 11.0](#) y luego siga el procedimiento específico de la implementación:

- [Determine la ruta de actualización a PAN-OS 11.0](#)
- [Actualización del cortafuegos a PAN-OS 11.0 desde Panorama](#)
- [Cambio de un cortafuegos independiente a una versión posterior](#)
- [Cambio de un par de cortafuegos de HA a una versión posterior](#)



Cuando cambia a una versión posterior los cortafuegos que administra con Panorama o los cortafuegos configurados para reenviar contenido a un dispositivo WildFire, primero debe [cambiar Panorama](#) y sus [recopiladores de logs](#) a una versión posterior y, a continuación, [cambiar el dispositivo WildFire a una versión posterior](#) antes de hacerlo con los cortafuegos.

Además, no se recomienda gestionar cortafuegos con una versión de mantenimiento posterior que Panorama, ya que puede provocar que algunas funciones no se comporten según lo esperado. Por ejemplo, no se recomienda administrar cortafuegos con PAN-OS 10.1.1 en ejecución o versiones de mantenimiento posteriores si Panorama se está ejecutando con PAN-OS 10.1.0.

Determine la ruta de actualización a PAN-OS 11.0

Cuando actualiza de una versión de lanzamiento de funciones de PAN-OS a una versión de funciones posterior, no puede omitir la instalación de ninguna versión de lanzamiento de funciones en la ruta a la versión de destino. Además, la ruta de actualización recomendada incluye la instalación de la última versión de mantenimiento en cada versión de lanzamiento antes de descargar la imagen base para la próxima versión de lanzamiento de funciones. Para minimizar el tiempo de inactividad de sus usuarios, realice actualizaciones fuera del horario laboral.



Para actualizaciones manuales, Palo Alto Networks recomienda instalar y actualizar desde la última versión de mantenimiento para cada versión de PAN-OS a lo largo de su ruta de actualización. No instale la imagen base de PAN-OS para una versión de funciones a menos que sea la versión de destino a la que desea actualizar.

Determine la ruta de actualización de la siguiente manera:



STEP 1 | Identifique qué versión se encuentra instalada.


- Desde Panorama, seleccione **Panorama (Panorama) > Managed Devices (Dispositivos administrados)** y verifique la versión de software en los cortafuegos que planea actualizar.
- Desde el cortafuegos, seleccione **Device (Dispositivo) > Software (Software)** y verifique qué versión tiene una marca de verificación en la columna **Currently Installed (Instalada actualmente)**.


STEP 2 | Identifique la ruta de actualización:

Revise los problemas conocidos y los cambios en el comportamiento predeterminado en las Notas de la versión [Consideraciones sobre el cambio a versiones anteriores/posteriores de complementos de Panorama](#) y para cada versión a través de la cual pase como parte de la ruta de actualización.

Versión de PAN-OS instalada	Ruta de actualización recomendada para PAN-OS 11.0
10.2.x	<ul style="list-style-type: none"> Si ya está ejecutando una versión de PAN-OS 10.2, puede actualizar directamente a PAN-OS 11.0
10.1.x	<p>Ahora puede usar la función Omitir actualización de versión de software para omitir versiones de software al actualizar un dispositivo desde PAN-OS 10.1 o versiones posteriores.</p> <ul style="list-style-type: none"> Si ya está ejecutando una versión de PAN-OS 10.1, puede actualizar directamente a PAN-OS 11.0.
10.0.x	<ul style="list-style-type: none"> Descargue e instale la versión de mantenimiento de PAN-OS 10.0 preferida más reciente y reinicie. Descargue PAN-OS 10.1.0 Descargue e instale la versión de mantenimiento de PAN-OS 10.1 preferida más reciente y reinicie. Descargue PAN-OS 10.2.0 Descargue e instale la versión de mantenimiento de PAN-OS 10.2 preferida más reciente y reinicie. Vaya a Cambio del cortafuegos a la versión posterior PAN-OS 11.0.
9.1.x	<ul style="list-style-type: none"> Descargue e instale la versión de mantenimiento de PAN-OS 9.1 preferida más reciente y reinicie. Descargue PAN-OS 10.0.0. Descargue e instale la versión de mantenimiento de PAN-OS 10.0 preferida más reciente y reinicie. Descargue PAN-OS 10.1.0 Descargue e instale la versión de mantenimiento de PAN-OS 10.1 preferida más reciente y reinicie. Descargue PAN-OS 10.2.0 Descargue e instale la versión de mantenimiento de PAN-OS 10.2 preferida más reciente y reinicie. Vaya a Cambio del cortafuegos a la versión posterior PAN-OS 11.0.

Versión de PAN-OS instalada	Ruta de actualización recomendada para PAN-OS 11.0
9.0.x	<ul style="list-style-type: none"> • Descargue e instale la versión de mantenimiento de PAN-OS 9.0 preferida más reciente y reinicie. <p> <i>Revise las consideraciones sobre cambio a versión anterior/posterior antes de actualizar cualquier recopilador de log a la versión de mantenimiento de PAN-OS 9.0 más reciente.</i></p> <ul style="list-style-type: none"> • Descargue PAN-OS 9.1.0. • Descargue e instale la versión de mantenimiento de PAN-OS 9.1 preferida más reciente y reinicie. • Descargue PAN-OS 10.0.0. • Descargue e instale la versión de mantenimiento de PAN-OS 10.0 preferida más reciente y reinicie. • Descargue PAN-OS 10.1.0 • Descargue e instale la versión de mantenimiento de PAN-OS 10.1 preferida más reciente y reinicie. • Descargue PAN-OS 10.2.0 • Descargue e instale la versión de mantenimiento de PAN-OS 10.2 preferida más reciente y reinicie. • Vaya a Cambio del cortafuegos a la versión posterior PAN-OS 11.0.
8.1.x	<ul style="list-style-type: none"> • Descargue e instale la versión de mantenimiento de PAN-OS 8.1 preferida más reciente y reinicie. • Descargue PAN-OS 9.0.0 • Descargue e instale la versión de mantenimiento de PAN-OS 9.0 preferida más reciente y reinicie. <p> <i>Revise las consideraciones sobre cambio a versión anterior/posterior antes de actualizar cualquier recopilador de log a la versión de mantenimiento de PAN-OS 9.0 más reciente.</i></p> <ul style="list-style-type: none"> • Descargue PAN-OS 9.1.0. • Descargue e instale la versión de mantenimiento de PAN-OS 9.1 preferida más reciente y reinicie. • Descargue PAN-OS 10.0.0.

Versión de PAN-OS instalada	Ruta de actualización recomendada para PAN-OS 11.0
	<ul style="list-style-type: none"> • Descargue e instale la versión de mantenimiento de PAN-OS 10.0 preferida más reciente y reinicie. • Descargue PAN-OS 10.1.0 • Descargue e instale la versión de mantenimiento de PAN-OS 10.1 preferida más reciente y reinicie. • Descargue PAN-OS 10.2.0 • Descargue e instale la versión de mantenimiento de PAN-OS 10.2 preferida más reciente y reinicie. • Vaya a Cambio del cortafuegos a la versión posterior PAN-OS 11.0.
8.0.x	<ul style="list-style-type: none"> • Descargue e instale PAN-OS 8.0.20 y reinicie. • Descargue PAN-OS 8.1.0. • Descargue e instale la versión de mantenimiento de PAN-OS 8.1 preferida más reciente y reinicie. • Descargue PAN-OS 9.0.0 • Descargue e instale la versión de mantenimiento de PAN-OS 9.0 preferida más reciente y reinicie. <p> <i>Revise las consideraciones sobre cambio a versión anterior/posterior antes de actualizar cualquier recopilador de log a la versión de mantenimiento de PAN-OS 9.0 más reciente.</i></p> <ul style="list-style-type: none"> • Descargue PAN-OS 9.1.0. • Descargue e instale la versión de mantenimiento de PAN-OS 9.1 preferida más reciente y reinicie. • Descargue PAN-OS 10.0.0. • Descargue e instale la versión de mantenimiento de PAN-OS 10.0 preferida más reciente y reinicie. • Descargue PAN-OS 10.1.0 • Descargue e instale la versión de mantenimiento de PAN-OS 10.1 preferida más reciente y reinicie. • Vaya a Cambio del cortafuegos a la versión posterior PAN-OS 11.0.
7.1.x	<ul style="list-style-type: none"> • Descargue e instale la versión de mantenimiento de PAN-OS 7.1.26 y reinicie. • Descargue PAN-OS 8.0.0.

Versión de PAN-OS instalada	Ruta de actualización recomendada para PAN-OS 11.0
	<ul style="list-style-type: none"> • Descargue e instale PAN-OS 8.0.20. • Descargue PAN-OS 8.1.0. • Descargue e instale la versión de mantenimiento de PAN-OS 8.1 preferida más reciente y reinicie. • Descargue PAN-OS 9.0.0 • Descargue e instale la versión de mantenimiento de PAN-OS 9.0 preferida más reciente y reinicie. <p> <i>Revise las consideraciones sobre cambio a versión anterior/posterior antes de actualizar cualquier recopilador de log a la versión de mantenimiento de PAN-OS 9.0 más reciente.</i></p> <ul style="list-style-type: none"> • Descargue PAN-OS 9.1.0. • Descargue e instale la versión de mantenimiento de PAN-OS 9.1 preferida más reciente y reinicie. • Descargue PAN-OS 10.0.0. • Descargue e instale la versión de mantenimiento de PAN-OS 10.0 preferida más reciente y reinicie. • Descargue PAN-OS 10.1.0 • Descargue e instale la versión de mantenimiento de PAN-OS 10.1 preferida más reciente y reinicie. • Vaya a Cambio del cortafuegos a la versión posterior PAN-OS 11.0.

Cambio de un cortafuegos independiente a una versión posterior

Revise las [Notas de la versión de PAN-OS 11.0](#) y, a continuación, utilice el siguiente procedimiento para actualizar un cortafuegos que no está en una configuración de HA a la versión posterior PAN-OS 11.0.



Si los cortafuegos están configurados para reenviar muestras a un dispositivo WildFire para su análisis, debe [cambiar la versión del dispositivo WildFire a una superior](#) antes de hacerlo con los cortafuegos de reenvío.

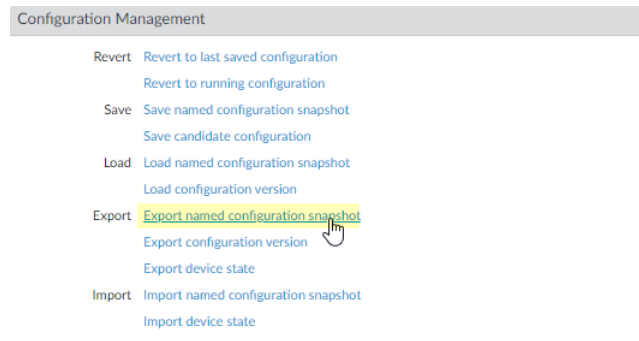


Para evitar afectar el tráfico, planifique la actualización dentro del periodo de interrupción. Asegúrese de que el cortafuegos esté conectado a una fuente de alimentación fiable. Si se interrumpe la alimentación durante una actualización, el cortafuegos puede quedar inutilizado.

STEP 1 | Guarde una copia de seguridad del archivo de configuración actual.

A pesar de que el cortafuegos crea automáticamente una copia de seguridad de la configuración, se recomienda crear y almacenar externamente una copia de seguridad antes de la actualización.

1. Seleccione **Device (Dispositivo) > Setup (Configuración) > Operations (Operaciones)** y haga clic en **Export named configuration snapshot (Exportar instantáneas de configuración con nombre)**.



2. Seleccione el archivo XML que contiene su configuración en uso (por ejemplo, **running-config.xml**) y haga clic en **OK (Aceptar)** para exportar el archivo de configuración.



3. Guarde el archivo exportado en una ubicación externa al cortafuegos. Puede usar esta copia de seguridad para restaurar la configuración si tiene problemas con la actualización.

STEP 2 | (Opcional) Si ha habilitado el ID de usuario, después de cambiar a la versión posterior, el cortafuegos borra las asignaciones actuales de dirección IP a nombre de usuario y de grupos para que puedan volver a rellenarse con los atributos de las fuentes del ID del usuario. Para calcular el tiempo necesario para que su entorno vuelva a rellenar las asignaciones, ejecute los siguientes comandos de la CLI en el cortafuegos.

- Para asignaciones de dirección IP a nombre de usuario:
 - **show user user-id-agent state all**
 - **show user server-monitor state all**
- Para asignaciones de grupo: **show user group-mapping statistics**

STEP 3 | Asegúrese de que el cortafuegos está ejecutando la última versión de contenido.

Consulte las [Notas de la versión](#) para obtener la versión de contenido mínima que debe instalar para la versión de PAN-OS 11.0. Asegúrese de seguir el [Prácticas recomendadas para las actualizaciones de contenido de aplicaciones y amenazas](#).

1. Seleccione **Device (Dispositivo) > Dynamic Updates (Actualizaciones dinámicas)** y vea qué versión de contenido de **Applications (Aplicaciones)** o **Applications and Threats (Aplicaciones y amenazas)** está instalada actualmente.

VERSION ^	FILE NAME	FEATURES	TYPE	SIZE	SHA256	RELEASE DATE	DOWNLOA...	CURRENTLY INSTALLED	ACTION	DOCUMENTAT...
v Applications and Threats Last checked: 2020/07/08 01:02:02 PDT Schedule: Every Wednesday at 01:02 (Download only)										
8287-6151	panupv2-all-contents-8287-6151	Apps, Threats	Full	56 MB	36315eff...	2020/06/26 17:34:56 PDT		✓		Release Notes
8287-6152	panupv2-all-contents-8287-6152	Apps, Threats	Full	56 MB	dced5c69...	2020/06/29 11:55:44 PDT	✓ previously		Revert Review Policies Review Apps	Release Notes
8287-6153	panupv2-all-contents-8287-6153	Apps, Threats	Full	56 MB	14af053b...	2020/06/29 17:15:33 PDT			Download	Release Notes
8287-6154	panupv2-all-contents-8287-6154	Apps, Threats	Full	56 MB	c872552f...	2020/06/30 16:14:19 PDT			Download	Release Notes
8287-6155	panupv2-all-contents-8287-6155	Apps, Threats	Full	56 MB	3f0fcb9a6...	2020/06/30 19:09:11 PDT			Download Review Policies Review Apps	Release Notes
8288-6157	panupv2-all-contents-8288-6157	Apps, Threats	Full	56 MB	54f355a1...	2020/07/01 17:00:41 PDT			Download	Release Notes
8288-6158	panupv2-all-contents-8288-6158	Apps, Threats	Full	56 MB	db9e5a8f...	2020/07/01 18:15:46 PDT			Download	Release Notes
8288-6159	panupv2-all-contents-8288-6159	Apps, Threats	Full	56 MB	b6863c96...	2020/07/02 11:55:30 PDT			Download	Release Notes


2. Si el cortafuegos no ejecuta la versión de lanzamiento de contenido mínima requerida o una versión posterior requerida para PAN-OS 11.0, haga clic en **Check Now (Comprobar ahora)** para recuperar una lista de actualizaciones disponibles.
3. Ahora debe localizar y **Download (Descargar)** la versión de lanzamiento de contenido requerida.
Después de descargar correctamente un archivo de actualización de contenido, el enlace en la columna Acción cambia de **Download (Descargar)** a **Install (Instalar)** para esa versión de contenido.
4. **Install (Instalar)** la actualización.

STEP 4 | [Determine la ruta de actualización a PAN-OS 11.0](#)

Revise [Lista de control para actualizar PAN-OS](#), los problemas conocidos y los cambios en el comportamiento predeterminado en las [Notas de la versión](#) y [Consideraciones sobre el cambio a versiones anteriores/posteriores de complementos de Panorama](#) para cada versión a través de la cual pase como parte de la ruta de actualización.

STEP 5 | ([Prácticas recomendadas](#)) Si está aprovechando Cortex Data Lake (CDL), [instale el certificado de dispositivo](#).

El cortafuegos cambia de forma automática al uso del certificado de dispositivo para la autenticación con ingestión de CDL y endpoints de consulta cuando se cambia a la versión posterior PAN-OS 11.0.

 *Si no instala el certificado del dispositivo antes de actualizar a PAN-OS 11.0, el cortafuegos continuará usando los certificados de servicio de creación de logs existentes para la autenticación.*

STEP 6 | Actualice a la versión posterior PAN-OS 11.0.



*Si su cortafuegos no tiene acceso a Internet desde el puerto de administración, puede descargar la imagen del software desde el [Portal de atención al cliente de Palo Alto Networks](#) y luego manualmente **Upload (Cargar)** la imagen en su cortafuegos.*

1. Seleccione **Device (Dispositivo) > Software** y haga clic en **Check Now (Comprobar ahora)** para mostrar las actualizaciones de PAN-OS más recientes.

Solo se muestran las versiones para la próxima versión disponible de PAN-OS. Por ejemplo, si PAN-OS 11.0 está instalada en el cortafuegos, solo se muestran las versiones de PAN-OS 11.0.

2. Seleccione **Panorama > Device Deployment (Implementación del dispositivo) > Software > Action (Acción) > Validate (Validar)**

Panorama > Device Deployment (Implementación del dispositivo) > Software > Action (Acción) > Validate (Validar) para ver todo el software intermedio y las imágenes de contenido necesarias para actualizar a 11.0.0.

3. Descargue el software intermedio y las imágenes de contenido.
4. Después de descargar la imagen (o, para una actualización manual, después de cargar la imagen), debe **Install (Instalar)** la imagen.
5. Una vez que la instalación se realiza completamente, reinicie mediante uno de los siguientes métodos:
 - Si se le pide que reinicie, haga clic en **Yes (Sí)**.
 - Si no se le solicita que reinicie, seleccione **Device (Dispositivo) > Setup (Configuración) > Operations (Operaciones)** y haga clic en **Reboot Device (Reiniciar dispositivo)**.



Llegado este punto, el cortafuegos borra las asignaciones de User-ID y se conecta a las fuentes de User-ID para volver a rellenar las asignaciones.

6. Si ha habilitado User-ID, use los siguientes comandos de la CLI para verificar que el cortafuegos ha vuelto a rellenar las asignaciones de dirección IP a nombre de usuario y de grupo antes de permitir el tráfico.
 - **show user ip-user-mapping all**
 - **show user group list**

STEP 7 | Vuelva a generar o a importar todos los certificados para cumplir con el nivel de seguridad 2 de OpenSSL.

Al actualizar a PAN-OS 11.0, se requiere que todos los certificados cumplan con los siguientes requisitos mínimos:

- RSA 2048 bits o superior, o ECDSA 256 bits o superior
- Resumen de SHA256 o superior

. Consulte la [Guía del administrador de PAN-OS](#) para obtener más información sobre la regeneración o reimportación de los certificados.

STEP 8 | Compruebe que el cortafuegos esté pasando el tráfico.

Seleccione **Monitor (Supervisar) > Session Browser (Navegador de sesión)** y compruebe que esté viendo nuevas sesiones.

	START TIME	FROM ZONE	TO ZONE	SOURCE	DESTINATI...	FROM PORT	TO PORT	PROTOC...	APPLICATI...	RULE	INGRESS I/F	EGRESS I/F	BYTES	VIRTUAL SYSTEM
⊞	07/08 11:29:02	z1	z2			56622	44060	6	ftp-data	rules6-1	ethernet1/3	ethernet1/4	558	vsys1
⊞	07/08 11:29:00	z1	z2			44823	42573	6	ftp-data	rules6-1	ethernet1/3	ethernet1/4	277874	vsys1
⊞	07/08 11:29:10	z1	z2			60162	47273	6	ftp-data	rules6-1	ethernet1/3	ethernet1/4	580	vsys1
⊞	07/08 11:29:10	z1	z2			45751	6013	6	ftp-data	rules6-1	ethernet1/3	ethernet1/4	560	vsys1
⊞	07/08 11:29:00	z1	z2			52923	42559	6	ftp-data	rules6-1	ethernet1/3	ethernet1/4	111119	vsys1
⊞	07/08 11:29:12	z1	z2			45772	8348	6	ftp-data	rules6-clone-with-group	ethernet1/3	ethernet1/4	785	vsys1
⊞	07/08 11:29:10	z1	z2			39762	61408	6	ftp-data	rules6-1	ethernet1/3	ethernet1/4	554	vsys1
⊞	07/08 11:29:06	z1	z2			53948	56596	6	ftp-data	rules6-1	ethernet1/3	ethernet1/4	792	vsys1
⊞	07/08 11:28:11	z1	z2			38185	42186	6	ftp-data	rules6-1	ethernet1/3	ethernet1/4	3243	vsys1

STEP 9 | Ver el historial de actualizaciones de software en el cortafuegos.

1. Inicie sesión en la interfaz del cortafuegos.
2. Vaya a **Device (Dispositivo) > Summary (Resumen) > Software** y haga clic en **Device History (Historial del dispositivo)**.

Cambio de un par de cortafuegos de HA a una versión posterior

Revise las [Notas de la versión de PAN-OS 11.0](#) y, a continuación, utilice el siguiente procedimiento para cambiar un par de cortafuegos en una configuración de alta disponibilidad (HA) a una versión posterior. Este procedimiento se aplica tanto a la configuración activa/pasiva como a la activa/activa.

Para evitar el estado de inactividad cuando actualiza cortafuegos de alta disponibilidad (high availability, HA), actualice un peer de HA a la vez: Para los cortafuegos activo/activo, no importa qué peer actualice primero (aunque, por sencillez, este procedimiento le muestra cómo actualizar primero el peer activo-principal). Para cortafuegos activos/pasivos, primero debe suspender (conmutar por error) y actualizar el peer activo (principal). Después de actualizar el peer principal, debe reactivar el peer principal para devolverlo a un estado funcional (pasivo). A continuación, debe suspender el peer pasivo (secundario) para que el peer principal vuelva a estar activo. Una vez que el peer principal está activo y el peer secundario está suspendido, puede continuar con la actualización. Para evitar la conmutación por error durante la actualización de los miembros del HA, debe asegurarse de que la opción de preferencia esté deshabilitada antes de continuar con la actualización. Solo necesita deshabilitar la preferencia en un miembro en la pareja.

Al actualizar los cortafuegos de HA en varias versiones de PAN-OS con funciones, debe actualizar cada peer de HA a la misma versión de PAN-OS con funciones en la ruta de actualización antes de continuar. Por ejemplo, está actualizando peers de HA de PAN-OS 10.0 a PAN-OS 11.0. Debe actualizar ambos peers de HA a PAN-OS 10.1 antes de poder continuar con la actualización a la versión de PAN-OS 11.0 de destino. Cuando los peers de HA tienen dos o más versiones con funciones de diferencia, el cortafuegos con la versión más antigua instalada entra en estado de **suspensión** y muestra un mensaje que dice **Peer version too old (Versión del peer demasiado antigua)**.



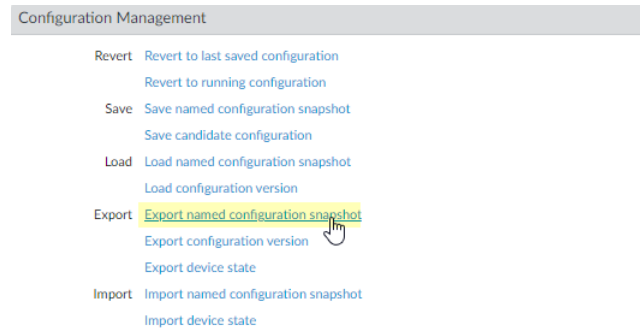
Para evitar afectar el tráfico, planifique la actualización dentro del periodo de interrupción. Asegúrese de que los cortafuegos estén conectados a una fuente de alimentación fiable. Si se interrumpe la alimentación durante una actualización, los cortafuegos pueden quedar inutilizados.

STEP 1 | Guarde una copia de seguridad del archivo de configuración actual.

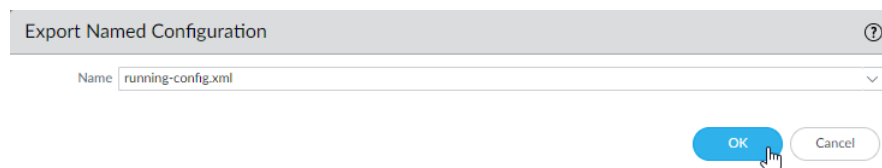
A pesar de que el cortafuegos crea automáticamente una copia de seguridad de la configuración, se recomienda crear y almacenar externamente una copia de seguridad antes de la actualización.

Lleve a cabo estos pasos en cada cortafuegos en la pareja:

1. Seleccione **Device (Dispositivo) > Setup (Configuración) > Operations (Operaciones)** y haga clic en **Export named configuration snapshot (Exportar instantáneas de configuración con nombre)**.



2. Seleccione el archivo XML que contiene su configuración en uso (por ejemplo, **running-config.xml**) y haga clic en **OK (Aceptar)** para exportar el archivo de configuración.



3. Guarde el archivo exportado en una ubicación externa al cortafuegos. Puede usar esta copia de seguridad para restaurar la configuración si tiene problemas con la actualización.

STEP 2 | Seleccione **Device (Dispositivo) > Support (Asistencia técnica) y Generate Tech Support File (Generar archivo de asistencia técnica)**.

Haga clic en **Yes (Sí)** cuando se le solicite generar el archivo de asistencia técnica.

STEP 3 | Asegúrese de que cada cortafuegos en la pareja de HA está ejecutando la última versión de contenido.

Consulte las [Notas de la versión](#) para obtener la versión de contenido mínima que debe instalar para la versión de PAN-OS 11.0. Asegúrese de seguir el [Prácticas recomendadas para las actualizaciones de contenido de aplicaciones y amenazas](#).

1. Seleccione **Device (Dispositivo) > Dynamic Updates (Actualizaciones dinámicas)** y compruebe qué **Applications (Aplicaciones)** o **Applications and Threats (Aplicaciones y amenazas)** para determinar qué actualización está instalada actualmente.

VERSION ^	FILE NAME	FEATURES	TYPE	SIZE	SHA256	RELEASE DATE	DOWNLOA...	CURRENTLY INSTALLED	ACTION	DOCUMENTAT...
Applications and Threats Last checked: 2020/07/08 01:02:02 PDT Schedule: Every Wednesday at 01:02 (Download only)										
8287-6151	panupv2-all-contents-8287-6151	Apps, Threats	Full	56 MB	36315eff...	2020/06/26 17:34:56 PDT		✓		Release Notes
8287-6152	panupv2-all-contents-8287-6152	Apps, Threats	Full	56 MB	dced5c69...	2020/06/29 11:55:44 PDT	✓ previously		Revert Review Policies Review Apps	Release Notes
8287-6153	panupv2-all-contents-8287-6153	Apps, Threats	Full	56 MB	14af053b...	2020/06/29 17:15:33 PDT			Download	Release Notes
8287-6154	panupv2-all-contents-8287-6154	Apps, Threats	Full	56 MB	c872552f...	2020/06/30 16:14:19 PDT			Download	Release Notes
8287-6155	panupv2-all-contents-8287-6155	Apps, Threats	Full	56 MB	3f0fcb9a6...	2020/06/30 19:09:11 PDT			Download Review Policies Review Apps	Release Notes
8288-6157	panupv2-all-contents-8288-6157	Apps, Threats	Full	56 MB	54f355a1...	2020/07/01 17:00:41 PDT			Download	Release Notes
8288-6158	panupv2-all-contents-8288-6158	Apps, Threats	Full	56 MB	db9e5a8f...	2020/07/01 18:15:46 PDT			Download	Release Notes
8288-6159	panupv2-all-contents-8288-6159	Apps, Threats	Full	56 MB	b6863c96...	2020/07/02 11:55:30 PDT			Download	Release Notes

2. Si el cortafuegos no ejecuta la versión de publicación de contenido mínima requerida o una versión posterior requerida para PAN-OS 11.0, haga clic en **Check Now (Verificar ahora)** para recuperar una lista de actualizaciones disponibles.
3. Ahora debe localizar y **Download (Descargar)** la versión de lanzamiento de contenido requerida.
Después de descargar correctamente un archivo de actualización de contenido, el enlace en la columna Acción cambia de **Download (Descargar)** a **Install (Instalar)** para esa versión de contenido.
4. **Install (Instalar)** la actualización. Debe instalar la actualización en ambos pares.

STEP 4 | [Determine la ruta de actualización a PAN-OS 11.0](#)

No puede omitir la instalación de ninguna versión de función publicada en la ruta de la versión de PAN-OS en ejecución a PAN-OS 11.0.

Revise [Lista de control para actualizar PAN-OS](#), los problemas conocidos y los cambios en el comportamiento predeterminado en las [Notas de la versión](#) y [Consideraciones sobre el cambio a versiones anteriores/posteriores de complementos de Panorama](#) para cada versión a través de la cual pase como parte de la ruta de actualización.

STEP 5 | ([Prácticas recomendadas](#)) Si está aprovechando Cortex Data Lake (CDL), [instale el certificado de dispositivo](#) en cada par de HA.

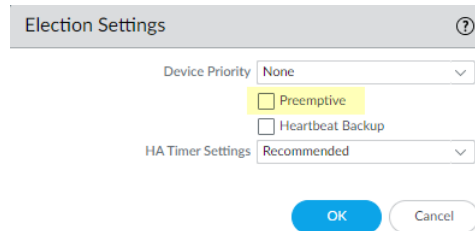
El cortafuegos cambia de forma automática al uso del certificado de dispositivo para la autenticación con ingestión de CDL y endpoints de consulta cuando se cambia a la versión posterior PAN-OS 11.0.



Si no instala el certificado del dispositivo antes de actualizar a PAN-OS 11.0, el cortafuegos continuará usando los certificados de servicio de creación de logs existentes para la autenticación.

STEP 6 | Deshabilite la preferencia en el primer miembro de cada pareja. Solo necesita desactivar esta configuración en un cortafuegos en la pareja de HA, pero asegúrese de que la confirmación sea correcta antes de continuar con la actualización.

1. Seleccione **Device (Dispositivo) > High Availability (Alta disponibilidad)** y edite la sección **Election Settings (Ajustes de elección)**.
2. Si esta opción está deshabilitada, deshabilite (desmarque) la opción **Preemptive (Preferente)** y haga clic en **OK (Aceptar)**.



3. Haga clic en **Commit (Confirmar)** para confirmar el cambio.

STEP 7 | Suspenda el peer de HA principal para forzar una conmutación por error.

(**Cortafuegos activo/pasivo**) Para los cortafuegos en una configuración de HA activa/pasiva, suspenda y actualice primero el peer de HA activo.

(**Cortafuegos activo/pasivo**) Para los cortafuegos en una configuración de HA activa/pasiva, suspenda y actualice primero el peer de HA activo- principal.

1. Seleccione **Device (Dispositivo) > High Availability (Alta disponibilidad) > Operational Commands (Comandos operativos)** y **Suspend local device for high availability (Suspende dispositivo local para alta disponibilidad)**.
2. En la esquina inferior derecha, verifique que el estado sea **suspendido**.

La conmutación por error resultante debería hacer que el peer de HA secundario se cambie al estado **activo**.



La conmutación por error resultante verifica que la conmutación por error de HA funcione correctamente antes de realizar la actualización.

STEP 8 | Instale PAN-OS 11.0 en el peer de HA suspendido.

1. En el peer de HA principal, seleccione **Device (Dispositivo) > Software** y haga clic en **Check Now (Comprobar ahora)** para obtener las últimas actualizaciones.

Solo se muestran las versiones para la próxima versión disponible de PAN-OS. Por ejemplo, si PAN-OS 11.0 está instalada en el cortafuegos, solo se muestran las versiones de PAN-OS 11.0.

2. Busque y **descargue** PAN-OS 11.0.0.



*Si su cortafuegos no tiene acceso a Internet desde el puerto de administración, puede descargar la imagen del software desde [Portal de asistencia técnica de Palo Alto Networks](#) y luego manualmente **Load (Cargar)** la imagen en su cortafuegos.*

*Si su cortafuegos tiene acceso a Internet y experimenta un error en la descarga de archivos, vuelva a hacer clic en **Check Now (Comprobar ahora)** para actualizar la lista de imágenes de PAN-OS.*

3. Después de descargar la imagen (o, para una actualización manual, después de cargar la imagen), debe **Install (Instalar)** la imagen.

VERSION ▾	SIZE	RELEASE DATE	DOWNLOADED	CURRENTLY INSTALLED	ACTION	
10.0.0	1083 MB	2020/06/28 21:36:52			Install	<input checked="" type="checkbox"/>
9.1.3	431 MB	2020/06/25 01:17:18			Download	Release Notes
9.0.9	662 MB	2020/06/24 15:38:06			Download	Release Notes

4. Una vez que la instalación se realiza completamente, reinicie mediante uno de los siguientes métodos:
 - Si se le pide que reinicie, haga clic en **Yes (Sí)**.
 - Si no se le solicita que reinicie, seleccione **Device (Dispositivo) > Setup (Configuración) > Operations (Operaciones)** y haga clic en **Reboot Device (Reiniciar dispositivo)**.
5. Una vez que el dispositivo termine de reiniciarse, observe el widget de alta disponibilidad en el **panel** y verifique que el dispositivo que acaba de actualizar esté sincronizado con el peer.

**STEP 9 |** Restaure la funcionalidad de HA al peer de HA principal.

1. Seleccione **Device (Dispositivo) > High Availability (Alta disponibilidad) > Operational Commands (Comandos operativos)** y **Make local device functional for high availability (Hacer que el dispositivo local sea funcional para alta disponibilidad)**.
2. En la esquina inferior derecha, verifique que el estado sea **Passive (Pasivo)**. Para cortafuegos en una configuración activa/activa, verifique que el estado sea **Active (Activo)**.
3. Espere a que se sincronice la configuración en ejecución del peer de HA.
En el **panel**, controle el estado de la configuración en ejecución en el widget de alta disponibilidad.

STEP 10 | En el peer de HA secundario, suspenda el peer de HA.

1. Seleccione **Device (Dispositivo) > High Availability (Alta disponibilidad) > Operational Commands (Comandos operativos)** y **Suspend local device for high availability (Suspender dispositivo local para alta disponibilidad)**.
2. En la esquina inferior derecha, verifique que el estado sea **suspendido**.

La conmutación por error resultante debe hacer que el peer de HA principal cambie al estado **Active (Activo)**.

STEP 11 | Instale PAN-OS 11.0 en el peer de HA secundario.

1. En el peer secundario, seleccione **Device (Dispositivo) > Software** y haga clic en **Check Now (Comprobar ahora)** para obtener las últimas actualizaciones.
2. Busque y **descargue** PAN-OS 11.0.0.
3. Después de descargarla, debe **Install (Instalar)** la imagen.
4. Una vez que la instalación se realiza completamente, reinicie mediante uno de los siguientes métodos:
 - Si se le pide que reinicie, haga clic en **Yes (Sí)**.
 - Si no se le solicita que reinicie, seleccione **Device (Dispositivo) > Setup (Configuración) > Operations (Operaciones)** y haga clic en **Reboot Device (Reiniciar dispositivo)**.

STEP 12 | Restaure la funcionalidad de HA en el peer de HA secundario.

1. Seleccione **Device (Dispositivo) > High Availability (Alta disponibilidad) > Operational Commands (Comandos operativos)** y **Make local device functional for high availability (Hacer que el dispositivo local sea funcional para alta disponibilidad)**.
2. En la esquina inferior derecha, verifique que el estado sea **Passive (Pasivo)**. Para cortafuegos en una configuración activa/activa, verifique que el estado sea **Active (Activo)**.
3. Espere a que se sincronice la configuración en ejecución del peer de HA.
En el **panel**, controle el estado de la configuración en ejecución en el widget de alta disponibilidad.

STEP 13 | Vuelva a habilitar la preferencia en el peer de HA donde se deshabilitó en el paso anterior.

1. Seleccione **Device (Dispositivo) > High Availability (Alta disponibilidad)** y edite la sección **Election Settings (Ajustes de elección)**.
2. Habilite (marque) la configuración **Preemptive (Preferente)** y haga clic en **OK (Aceptar)**.
3. Haga clic en **Commit (Confirmar)** para confirmar el cambio.

STEP 14 | Vuelva a generar o a importar todos los certificados para cumplir con el nivel de seguridad 2 de OpenSSL.

Al actualizar a PAN-OS 11.0, se requiere que todos los certificados cumplan con los siguientes requisitos mínimos:

- RSA de 2048 bits o superior, o ECDSA de 256 bits o superior
- Compendio de SHA256 o superior

Consulte la [Guía del administrador de PAN-OS](#) o la [Guía del administrador de Panorama](#) para obtener más información sobre la regeneración o reimportación de los certificados.

STEP 15 | Verifique que ambos miembros estén pasando el tráfico como está previsto.

En una configuración activa/pasiva, solo el miembro activo debe pasar el tráfico; en una configuración activa/activa, sin embargo, ambos miembros deberían pasar el tráfico.

Ejecute los siguientes comandos de la CLI para confirmar que la actualización se realizó correctamente:

- (Solo miembros activos) Para verificar que los miembros activos están pasando tráfico, ejecute el comando **show session all**.
- Para verificar la sincronización de la sesión, ejecute el comando **show high-availability interface ha2** y asegúrese de que los contadores de la interfaz de hardware en la tabla de la CPU aumentan de la siguiente forma:
 - En una configuración activa/pasiva, solo el par activo muestra los paquetes transmitidos; el par pasivo mostrará solo los paquetes recibidos.



Si habilitó la conexión persistente de HA2, los contadores de la interfaz de hardware en el par pasivo mostrarán los paquetes de transmisión y recepción. Esto ocurre porque HA2 keep-alive es bidireccional, lo que significa que ambos miembros transmiten paquetes de HA2 keep-alive.

- En una configuración activo/activo, verá paquetes recibidos y paquetes transmitidos de ambos peers.

Actualización del cortafuegos a PAN-OS 11.0 desde Panorama

Implemente actualizaciones de contenido y cambie PAN-OS a una versión posterior para cortafuegos administrados desde el servidor de gestión Panorama™.

- [Actualización de los cortafuegos cuando Panorama está conectado a internet](#)
- [Actualización de los cortafuegos cuando Panorama no está conectado a internet](#)
- [Actualización de un cortafuegos de ZTP](#)

Actualización de los cortafuegos cuando Panorama está conectado a internet

Revise las [Notas de la versión PAN-OS 11.0](#) y utilice el siguiente procedimiento para cambiar los cortafuegos que gestiona con Panorama a una versión posterior. Este procedimiento aplica a los cortafuegos independientes y los cortafuegos que se implementan en una configuración de alta disponibilidad (HA).

Al actualizar los cortafuegos de HA en varias versiones de PAN-OS con funciones, debe actualizar cada peer de HA a la misma versión de PAN-OS con funciones en la ruta de actualización antes de continuar. Por ejemplo, está actualizando peers de HA de PAN-OS 10.0 a PAN-OS 11.0. Debe actualizar ambos peers de HA a PAN-OS 10.1 antes de poder continuar con la actualización a la versión de PAN-OS 11.0 de destino. Cuando los peers de HA tienen dos o más versiones con funciones de diferencia, el cortafuegos con la versión más antigua instalada entra en estado de **suspensión** y muestra un mensaje que dice **Peer version too old (Versión del peer demasiado antigua)**.



Si Panorama no se puede conectar directamente al servidor de actualizaciones, siga el procedimiento para la [Actualización de los cortafuegos cuando Panorama no está conectado a internet](#) de modo que pueda descargar manualmente imágenes a Panorama y distribuir las imágenes a los cortafuegos.

La nueva función [Omitir actualización de versión de software](#) le permite omitir hasta tres versiones al implementar actualizaciones de dispositivos Panorama en PAN-OS 11.0 a cortafuegos en PAN-OS 10.1 o versiones posteriores.

Antes de actualizar los cortafuegos desde Panorama, debe realizar lo siguiente:

- ❑ Asegúrese de que Panorama ejecute una versión PAN-OS igual o posterior a la versión de actualización. Debe [cambiar Panorama](#) y sus [recopiladores de logs](#) a la versión posterior 11.0 antes de cambiar los cortafuegos gestionados a esta versión. Además, al cambiar los recopiladores de logs a la versión posterior 11.0, debe cambiar todos los recopiladores de logs a una versión posterior al mismo tiempo debido a los cambios en la infraestructura de creación de logs.
- ❑ Asegúrese de que todos los cortafuegos estén conectados a una fuente de alimentación fiable. Si se interrumpe la alimentación durante una actualización, los cortafuegos pueden resultar inútiles.
- ❑ Decida si desea permanecer en modo heredado si el dispositivo virtual Panorama está en modo heredado cuando cambia a la versión posterior PAN-OS 11.0. El modo heredado no es compatible con una nueva implementación de dispositivo virtual Panorama que ejecute PAN-OS 9.1 o una versión posterior. Si cambia el dispositivo virtual Panorama a la versión posterior PAN-OS 9.0 o una versión

anterior a PAN-OS 11.0, Palo Alto Networks recomienda revisar los [requisitos previos de configuración para el dispositivo virtual Panorama](#) y cambiar al [modo Panorama](#) o al [modo solo administración](#) según sus necesidades.

Si desea mantener el dispositivo virtual Panorama en modo heredado, [aumente las CPU y la memoria](#) asignadas al dispositivo virtual Panorama a un mínimo de 16 CPU y 32 GB de memoria para cambiar con éxito a la versión posterior PAN-OS 11.0. Consulte los [Requisitos previos de configuración del dispositivo virtual Panorama](#) para obtener más información.

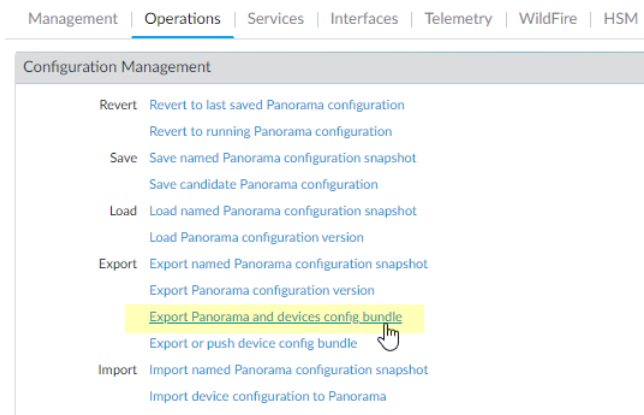
STEP 1 | Inicie sesión en la interfaz web de Panorama.

STEP 2 | Guarde una copia de seguridad del archivo de configuración actual en cada cortafuegos gestionado que desee actualizar.



A pesar de que el cortafuegos crea automáticamente una copia de seguridad de la configuración, se recomienda crear y almacenar externamente una copia de seguridad antes de la actualización.

1. Seleccione **Panorama > Setup (Configuración) > Operations (Operaciones)** y haga clic en **Export Panorama and devices config bundle (Exportar lote de configuración de dispositivos y Panorama)** para generar y exportar la versión más reciente de la copia de seguridad de configuración de Panorama y de cada dispositivo gestionado.



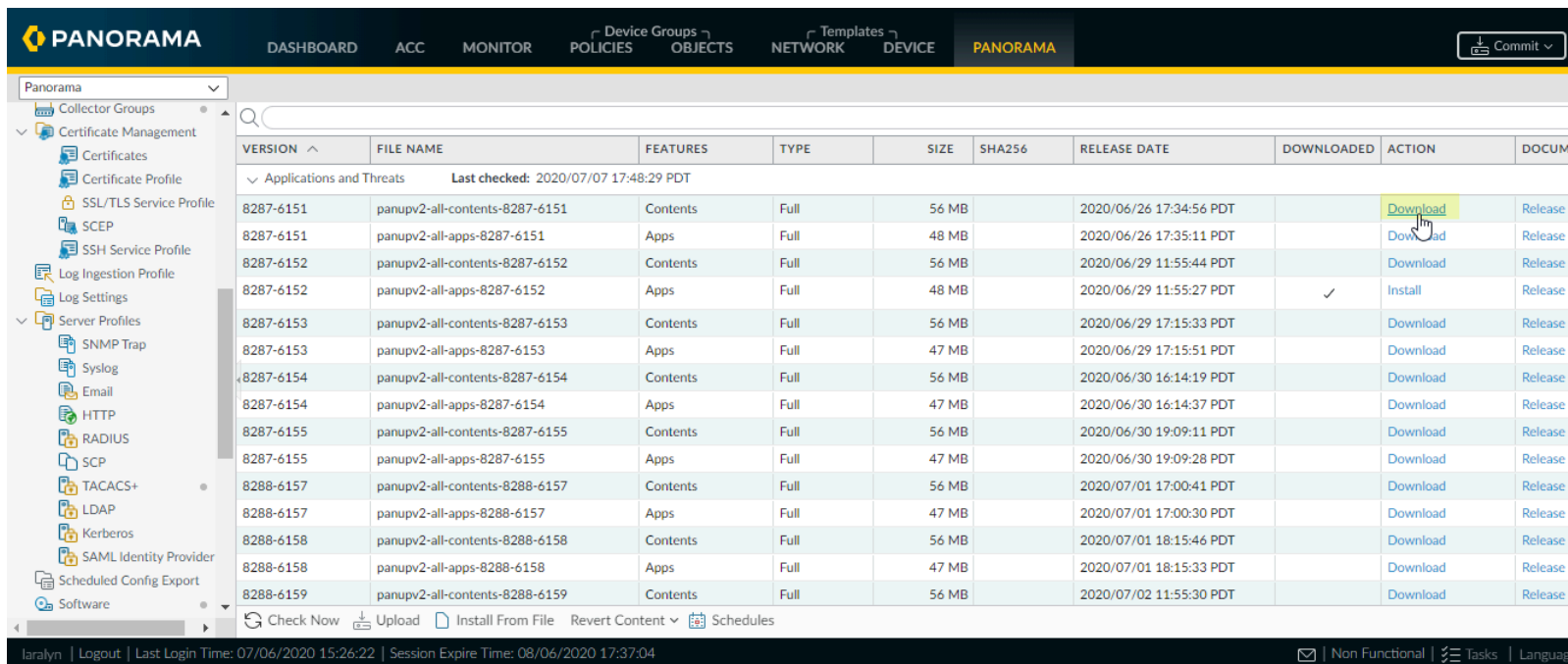
2. Guarde el archivo exportado en una ubicación externa al cortafuegos. Puede usar esta copia de seguridad para restaurar la configuración si tiene problemas con la actualización.

STEP 3 | Instale la última actualización de contenido.

Consulte las [Notas de la versión](#) para obtener la versión de contenido mínima necesaria para PAN-OS 11.0. Asegúrese de seguir [Prácticas recomendadas para las actualizaciones de contenido de aplicaciones y amenazas](#) cuando implemente actualizaciones de contenido en Panorama y en los cortafuegos gestionados.

1. Seleccione **Panorama > Device Deployment (Implementación del dispositivo) > Dynamic Updates (Actualizaciones dinámicas)** y haga clic en **Check Now (Comprobar ahora)** para

comprobar las últimas actualizaciones. Si hay una actualización disponible, la columna Acción mostrará el enlace **Download (Descargar)**.



VERSION	FILE NAME	FEATURES	TYPE	SIZE	SHA256	RELEASE DATE	DOWNLOADED	ACTION	DOCUM
8287-6151	panupv2-all-contents-8287-6151	Contents	Full	56 MB		2020/06/26 17:34:56 PDT		Download	Release
8287-6151	panupv2-all-apps-8287-6151	Apps	Full	48 MB		2020/06/26 17:35:11 PDT		Download	Release
8287-6152	panupv2-all-contents-8287-6152	Contents	Full	56 MB		2020/06/29 11:55:44 PDT		Download	Release
8287-6152	panupv2-all-apps-8287-6152	Apps	Full	48 MB		2020/06/29 11:55:27 PDT	✓	Install	Release
8287-6153	panupv2-all-contents-8287-6153	Contents	Full	56 MB		2020/06/29 17:15:33 PDT		Download	Release
8287-6153	panupv2-all-apps-8287-6153	Apps	Full	47 MB		2020/06/29 17:15:51 PDT		Download	Release
8287-6154	panupv2-all-contents-8287-6154	Contents	Full	56 MB		2020/06/30 16:14:19 PDT		Download	Release
8287-6154	panupv2-all-apps-8287-6154	Apps	Full	47 MB		2020/06/30 16:14:37 PDT		Download	Release
8287-6155	panupv2-all-contents-8287-6155	Contents	Full	56 MB		2020/06/30 19:09:11 PDT		Download	Release
8287-6155	panupv2-all-apps-8287-6155	Apps	Full	47 MB		2020/06/30 19:09:28 PDT		Download	Release
8288-6157	panupv2-all-contents-8288-6157	Contents	Full	56 MB		2020/07/01 17:00:41 PDT		Download	Release
8288-6157	panupv2-all-apps-8288-6157	Apps	Full	47 MB		2020/07/01 17:00:30 PDT		Download	Release
8288-6158	panupv2-all-contents-8288-6158	Contents	Full	56 MB		2020/07/01 18:15:46 PDT		Download	Release
8288-6158	panupv2-all-apps-8288-6158	Apps	Full	47 MB		2020/07/01 18:15:33 PDT		Download	Release
8288-6159	panupv2-all-contents-8288-6159	Contents	Full	56 MB		2020/07/02 11:55:30 PDT		Download	Release

- Haga clic en **Install (Instalar)** y seleccione los cortafuegos en los que desee instalar la actualización. Si actualiza los cortafuegos de HA, deberá actualizar contenido en ambos peers.
- Haga clic en **OK (Aceptar)**.

STEP 4 | Determine la ruta de actualización a PAN-OS 11.0.



Revise la lista de control para actualizar PAN-OS, los problemas conocidos y los cambios en el comportamiento predeterminado en las [Notas de la versión](#) y las [consideraciones sobre el cambio a versiones anteriores/posteriores](#) para cada versión a través de la cual pase como parte de su ruta de actualización.



Si actualiza más de un cortafuegos, agilice el proceso determinando las rutas de actualización para todos los cortafuegos antes de comenzar la descarga de imágenes.

STEP 5 | (Prácticas recomendadas) Si está aprovechando Cortex Data Lake (CDL), instale el certificado de dispositivo.

El cortafuegos cambia de forma automática al uso del certificado de dispositivo para la autenticación con ingestión de CDL y endpoints de consulta cuando se cambia a la versión posterior PAN-OS 11.0.



Si no instala el certificado del dispositivo antes de actualizar a PAN-OS 11.0, el cortafuegos continuará usando los certificados de servicio de creación de logs existentes para la autenticación.

STEP 6 | (Solo actualizaciones de cortafuegos de HA) Si actualizará los cortafuegos que forman parte de un par de HA, deshabilite la opción de preferencia. Solo debe deshabilitar esta opción en un cortafuegos de cada par de HA.

1. Seleccione **Device (Dispositivo) > High Availability (Alta disponibilidad)** y edite la sección **Election Settings (Ajustes de elección)**.
2. Si esta opción está deshabilitada, deshabilite (desmarque) la opción **Preemptive (Preferente)** y haga clic en **OK (Aceptar)**.

3. Haga clic en **Commit (Confirmar)** para confirmar los cambios. Asegúrese de que la confirmación se realice correctamente antes de continuar con la actualización.

STEP 7 | (Solo actualizaciones de cortafuegos de HA) Suspenda el peer de HA principal para forzar una conmutación por error.

(Cortafuegos activo/pasivo) Para los cortafuegos en una configuración de HA activa/pasiva, suspenda y actualice primero el peer de HA activo.

(Cortafuegos activo/pasivo) Para los cortafuegos en una configuración de HA activa/pasiva, suspenda y actualice primero el peer de HA activo- principal.

1. Inicie sesión en la interfaz web del cortafuegos del peer de HA del cortafuegos principal activo.
2. Seleccione **Device (Dispositivo) > High Availability (Alta disponibilidad) > Operational Commands (Comandos operativos)** y **Suspend local device for high availability (Suspende dispositivo local para alta disponibilidad)**.

3. En la esquina inferior derecha, verifique que el estado sea **suspended (suspendido)**.

La conmutación por error resultante debería hacer que el peer de HA pasivo secundario cambie al estado **activo**.



La conmutación por error resultante verifica que la conmutación por error de HA funcione correctamente antes de realizar la actualización.

STEP 8 | (Opcional) Actualice los cortafuegos gestionados a PAN-OS 10.1.

La función de omitir actualización de versión de software es compatible con los cortafuegos gestionados que ejecutan PAN-OS 10.1 o versiones posteriores. Si los cortafuegos gestionados están en PAN-OS 10.0 o una versión anterior, primero actualice a PAN-OS 10.1 o una versión posterior.

STEP 9 | (Opcional) **Exporte** el archivo a un servidor SCP configurado.

En PAN-OS 11.0, los servidores SCP están disponibles como origen de descarga cuando se implementan actualizaciones en los cortafuegos gestionados. Exporte el archivo antes de descargar el software y las imágenes de contenido en el siguiente paso.

STEP 10 | Valide y descargue las versiones de software y contenido necesarias para la versión de destino.

En este paso, puede ver y descargar el software intermedio y las imágenes de contenido necesarias para actualizar a PAN-OS 11.0.

La descarga de software y de imágenes de contenido mediante la descarga de varias imágenes es opcional. Aún puede descargar las imágenes una por una.

1. Haga clic en **Panorama > Device Deployment (Implementación del dispositivo) > Software > Action (Acción) > Validate (Validar)**.
2. Vea las versiones intermedias de software y contenido que necesita descargar.
3. Seleccione los cortafuegos que desea actualizar y haga clic en **Deploy (Implementar)**.
4. Seleccione el origen de la descarga y haga clic en **Download (Descargar)**.

STEP 11 | Instale PAN-OS 11.0.0 en el cortafuegos.



*(Solo en el caso de SD-WAN) Para conservar un estado preciso de los vínculos de SD-WAN, debe cambiar los cortafuegos de centrales a la versión posterior PAN-OS 11.0 antes de actualizar los cortafuegos de sucursales. La actualización de los cortafuegos de sucursales antes que los cortafuegos de central puede provocar datos de supervisión incorrectos (**Panorama [Panorama] > SD-WAN [SD-WAN] > Monitoring [Supervisión]**) y que los enlaces de SD-WAN se muestren de forma incorrecta como **down (inactivo)**.*

1. Haga clic en **Install (Instalar)** en la columna Action (Acción) que corresponda a los modelos de cortafuegos que desee actualizar. Por ejemplo, si desea cambiar sus cortafuegos PA-220 a una versión posterior, haga clic en **Install (Instalar)** en la fila que corresponda a PanOS_220-11.0.0.
2. En el cuadro de diálogo Deploy Software (Implementar software), seleccione todos los cortafuegos que desea actualizar.
(Solo actualizaciones de cortafuegos de HA) Para reducir el tiempo de inactividad, seleccione solo un peer en cada par de HA. En los pares activo/pasivo, seleccione el peer pasivo; en los pares activo/activo, seleccione el peer activo secundario.
3. *(Solo actualizaciones de cortafuegos de HA)* Asegúrese de que la opción **Group HA Peers (Agrupar peers de HA)** no esté seleccionada.
4. Seleccione **Reboot device after install (Reiniciar dispositivo tras la instalación)**.
5. Para comenzar la actualización, haga clic en **OK (Aceptar)**.
6. Una vez que la instalación se realiza completamente, reinicie mediante uno de los siguientes métodos:
 - Si se le pide que reinicie, haga clic en **Yes (Sí)**.
 - Si no se le solicita que reinicie, seleccione **Device (Dispositivo) > Setup (Configuración) > Operations (Operaciones)** y haga clic en **Reboot Device (Reiniciar dispositivo)**.
7. Después de que los cortafuegos terminen de reiniciarse, seleccione **Panorama (Panorama) > Managed Devices (Dispositivos gestionados)** y verifique que la versión del software sea 11.0.0 en los cortafuegos que actualizó. Además, verifique que el estado de HA de los cortafuegos pasivos que actualizó continúe siendo pasivo.

STEP 12 | *(Solo actualizaciones de cortafuegos de HA)* Restaure la funcionalidad de HA en el Peer de HA principal.

1. [Inicie sesión en la interfaz web del cortafuegos](#) del peer de HA del cortafuegos principal suspendido.
2. Seleccione **Device (Dispositivo) > High Availability (Alta disponibilidad) > Operational Commands (Comandos operativos)** y **Make local device functional for high availability (Hacer que el dispositivo local sea funcional para alta disponibilidad)**.
3. En la esquina inferior derecha, verifique que el estado sea **Passive (Pasivo)**. Para cortafuegos en una configuración activa/activa, verifique que el estado sea **Active (Activo)**.
4. Espere a que se sincronice la configuración en ejecución del peer de HA.
En el **Dashboard (Panel)**, controle el estado de la configuración en ejecución en el widget de alta disponibilidad.

STEP 13 | (Solo actualizaciones de cortafuegos de HA) Suspenda el peer de HA secundario para forzar una conmutación por error en el peer de HA principal.

1. [Inicie sesión en la interfaz web del cortafuegos](#) del peer de HA del cortafuegos secundario activo.
2. Seleccione **Device (Dispositivo) > High Availability (Alta disponibilidad) > Operational Commands (Comandos operativos)** y **Suspend local device for high availability (Suspende dispositivo local para alta disponibilidad)**.
3. En la esquina inferior derecha, verifique que el estado sea **suspended (suspendido)**.

La conmutación por error resultante debería hacer que el peer de HA pasivo principal cambie al estado **activo**.



La conmutación por error resultante verifica que la conmutación por error de HA funcione correctamente antes de realizar la actualización.

STEP 14 | (Solo actualizaciones en cortafuegos de HA) Actualice el segundo peer de HA en cada par de HA.

1. En la [interfaz web de Panorama](#), seleccione **Panorama > Device Deployment (Implementación del dispositivo) > Software**.
2. Haga clic en **Install (Instalar)** en la columna Action (Acción) que corresponda a los modelos de cortafuegos de los pares de HA que está actualizando.
3. En el cuadro de diálogo Deploy Software (Implementar software), seleccione todos los cortafuegos que desea actualizar. En este momento, seleccione solo los peers de los cortafuegos de HA que ya actualizó.
4. Asegúrese de que la opción **Group HA Peers (Agrupar peers de HA)** no esté seleccionada.
5. Seleccione **Reboot device after install (Reiniciar dispositivo tras la instalación)**.
6. Para comenzar la actualización, haga clic en **OK (Aceptar)**.
7. Una vez que la instalación se realiza completamente , reinicie mediante uno de los siguientes métodos:
 - Si se le pide que reinicie, haga clic en **Yes (Sí)**.
 - Si no se le solicita que reinicie, seleccione **Device (Dispositivo) > Setup (Configuración) > Operations (Operaciones)** y haga clic en **Reboot Device (Reiniciar dispositivo)**.

STEP 15 | (Solo actualizaciones de cortafuegos de HA) Restaure la funcionalidad de HA en el peer de HA secundario.

1. [Inicie sesión en la interfaz web del cortafuegos](#) del peer de HA del cortafuegos secundario suspendido.
2. Seleccione **Device (Dispositivo) > High Availability (Alta disponibilidad) > Operational Commands (Comandos operativos)** y **Make local device functional for high availability (Hacer que el dispositivo local sea funcional para alta disponibilidad)**.
3. En la esquina inferior derecha, verifique que el estado sea **Passive (Pasivo)**. Para cortafuegos en una configuración activa/activa, verifique que el estado sea **Active (Activo)**.
4. Espere a que se sincronice la configuración en ejecución del peer de HA.
En el **Dashboard (Panel)**, controle el estado de la configuración en ejecución en el widget de alta disponibilidad.

STEP 16 | (Solo modo FIPS-CC) **Actualice Panorama y dispositivos gestionados en modo FIPS-CC.**

La actualización de un cortafuegos gestionado en modo FIPS-CC requiere que restablezca el estado de conexión segura si agregó el recopilador de logs dedicado a la gestión de Panorama mientras el cortafuegos gestionado ejecutaba una versión de PAN-OS 11.0.

No necesita reincorporar el cortafuegos gestionado agregado a la gestión de Panorama si el cortafuegos gestionado ejecutaba PAN-OS 10.0 o una versión anterior.

STEP 17 | Verifique la versión de contenido y de software que se ejecutan en cada cortafuegos gestionado.

1. En Panorama, seleccione **Panorama > Managed Devices (Dispositivos gestionados)**.
2. Ubique los cortafuegos y revise el contenido y las versiones de contenido y de software en la tabla.

En los cortafuegos de HA, también puede verificar que el estado de HA de cada peer sea el esperado.

	Device Name	Model	IP Address	Template	Status				Software Version	Apps and Threat	Antivirus
			IPv4		Device State	HA Status	Certificate	L... M... D...			
▼ <input type="checkbox"/> DG-VM (5/5 Devices Connected): Shared > DG-VM											
<input type="checkbox"/>	PA-VM-6	PA-VM		Stack-VM	Connected		pre-defined		8.1.0	8320-6307	3881-4345
<input type="checkbox"/>	PA-VM-73	PA-VM		Stack-Test73	Connected		pre-defined		9.1.3	8320-6307	3873-4337
<input type="checkbox"/>	PA-VM-95	PA-VM		Stack-VM	Connected		pre-defined		10.0.0	8320-6307	3881-4345
<input type="checkbox"/>	PA-VM-96	PA-VM		Stack-VM	Connected	<div>● Passive</div>	pre-defined		10.0.0	8299-6216	3881-4345
	PA-VM			Stack-Test92	Connected	<div>● Active</div>	pre-defined		10.0.0	8299-6216	3881-4345

STEP 18 | (Solo actualizaciones en cortafuegos de HA) Si deshabilitó la opción de preferencia en uno de sus cortafuegos de HA antes de la actualización, edite los **Election Settings (Ajustes de elección)** [**Device (Dispositivo) > High Availability (Alta disponibilidad)**], vuelva a habilitar el ajuste **Preemptive (Preferente)** para ese cortafuegos y haga clic en **Commit (Confirmar)** para confirmar el cambio.

STEP 19 | En la [interfaz web de Panorama](#) inserte toda la configuración gestionada de Panorama en los cortafuegos administrados.

Este paso es necesario para habilitar la confirmación selectiva y el envío de cambios en la configuración de la pila de plantillas y del grupo de dispositivos desde Panorama a los cortafuegos gestionados.

Esto es necesario para enviar con éxito los cambios de configuración a los cortafuegos de sistemas virtuales múltiples gestionados por Panorama después de una correcta actualización a PAN-OS 11.0 desde PAN-OS 10.1 o una versión anterior. Para obtener más información, consulte el cambio en el comportamiento predeterminado de [los objetos de configuración compartidos para cortafuegos de sistemas virtuales múltiples gestionados por Panorama](#).

1. Seleccione **Commit (Confirmar) > Push to Devices (Enviar a dispositivos)**.
2. **Push (Enviar)**.

STEP 20 | Vuelva a generar o a importar todos los certificados para cumplir con el nivel de seguridad 2 de OpenSSL.

Al actualizar a PAN-OS 10.2 o una versión posterior, se requiere que todos los certificados cumplan con los siguientes requisitos mínimos. Omita este paso si está actualizando desde PAN-OS 10.2 y ya volvió a generar o a importar los certificados.

- RSA de 2048 bits o superior, o ECDSA de 256 bits o superior
- Compendio de SHA256 o superior

Consulte la [Guía del administrador de PAN-OS](#) o la [Guía del administrador de Panorama](#) para obtener más información sobre la regeneración o reimportación de los certificados.

STEP 21 | Ver el historial de actualizaciones de software del cortafuegos.

1. Inicie sesión en la interfaz de Panorama.
2. Vaya a **Panorama > Managed Devices (Dispositivos gestionados) > Summary (Resumen)** y haga clic en **Device History (Historial de dispositivos)**.

Actualización de los cortafuegos cuando Panorama no está conectado a internet

Para obtener una lista de actualizaciones de software y contenido que puede instalar en los cortafuegos, consulte [Actualizaciones compatibles](#).

La nueva función [Omitir actualización de versión de software](#) le permite omitir hasta tres versiones al implementar actualizaciones de dispositivos Panorama en PAN-OS 11.0 a cortafuegos en PAN-OS 10.1 o versiones posteriores.

STEP 1 | Antes de actualizar los cortafuegos administrados, asegúrese de ejecutar PAN-OS 11.0 en el servidor de gestión de Panorama y los recopiladores de logs.



Palo Alto Networks® recomienda encarecidamente que Panorama y el Recopilador de logs ejecuten la misma versión de Panorama y que Panorama, Recopilador de logs y todos los cortafuegos gestionados ejecuten la misma versión de publicación de contenido.



Para obtener detalles importantes sobre la compatibilidad de contenido y software, consulte [Compatibilidad de versiones de Panorama, el recopilador de logs y el cortafuegos](#).

Panorama debe estar ejecutando el mismo (o posterior) lanzamiento de software que los cortafuegos, pero debe tener la misma versión de lanzamiento de contenido o una anterior:

- **Versión de lanzamiento de software.** si su servidor de gestión de Panorama o Recopilador de logs no está ejecutando la misma versión de software que la versión para la que desea actualizar los cortafuegos, entonces debe instalar la misma versión de Panorama o posterior en Panorama y luego en el Recopilador de logs (consulte [Instalar contenido y actualizaciones de software para Panorama](#)) antes de actualizar cualquier cortafuegos.
- **Versión de lanzamiento del contenido:** para lanzamiento de versiones de contenido, debe asegurarse de que todos los servidores de seguridad estén ejecutando la última versión de publicación de contenido o, como mínimo, ejecuten una versión posterior a la que se está ejecutando

en Panorama y Recopilador de logs; de lo contrario, actualice los cortafuegos gestionados y luego [Actualice los recopiladores de logs cuando Panorama no está conectado a Internet](#) antes de actualizar la versión de publicación de contenido en el servidor de gestión de Panorama (consulte [Instalación de actualizaciones de software y contenido de Panorama](#)).

Para comprobar el software y las versiones de contenido:

- **Servidor de gestión de Panorama:** inicie sesión en la interfaz web de Panorama y vaya a la configuración de Información general (**Dashboard [Panel]**).
- **Recopilador de logs:** inicie sesión en la CLI de cada recopilador de logs y ejecute el comando **show system info**.

STEP 2 | Guarde una copia de seguridad del archivo de configuración actual en cada cortafuegos gestionado que desee actualizar.



A pesar de que el cortafuegos crea automáticamente una copia de seguridad de la configuración, se recomienda crear y almacenar externamente una copia de seguridad antes de la actualización.

1. Asegúrese de **Export Panorama and devices config bundle (Exportar Panorama y lote de configuración de dispositivos)** (**Panorama > Setup [Configuración] > Operations [Operaciones]**) para generar y exportar la versión más reciente de la copia de seguridad de configuración de Panorama y de cada dispositivo gestionado.
2. Guarde el archivo exportado en una ubicación externa al cortafuegos. Puede usar esta copia de seguridad para restaurar la configuración si tiene problemas con la actualización.

STEP 3 | Determine qué actualizaciones de contenido necesita instalar. Consulte las [notas de versión](#) para obtener la versión de contenido mínima que debe instalar para una versión de PAN-OS®.



Palo Alto Networks recomienda encarecidamente que Panorama, los recopiladores de logs y todos los cortafuegos gestionados ejecuten la misma versión de publicación de contenido.

Para cada actualización de contenido, determine si necesita actualizaciones y tome nota sobre qué actualizaciones de contenido debe descargar en el siguiente paso.



Asegúrese de que Panorama ejecute la misma versión de publicación de contenido, pero no una posterior, que la que se ejecuta en los cortafuegos gestionados y los recopiladores de logs.

STEP 4 | [Determine la ruta de actualización del software](#) para los cortafuegos que desee actualizar a Panorama 11.0.

Inicie sesión en Panorama, seleccione **Panorama > Managed Collectors (Recopiladores gestionados)** y observe la versión de software actual para los cortafuegos que desea actualizar.



Revise [Lista de control para actualizar PAN-OS](#), los problemas conocidos y los cambios en el comportamiento predeterminado en las [Notas de la versión](#) y [Consideraciones sobre el cambio a versiones anteriores/posteriores de complementos de Panorama](#) para cada versión a través de la cual pase como parte de la ruta de cambio a una versión posterior.

STEP 5 | (Opcional) Actualice los cortafuegos gestionados a PAN-OS 10.1.

La función de omitir actualización de versión de software de es compatible con cortafuegos gestionados que ejecutan PAN-OS 10.1 o versiones posteriores. Si los cortafuegos gestionados están en PAN-OS 10.0 o una versión anterior, primero actualice a PAN-OS 10.1 o una versión posterior.

STEP 6 | Realice una comprobación de validación de la versión.

En este paso, puede ver el software intermedio y las imágenes de contenido necesarias para actualizar a 11.0.

1. Seleccione **Panorama > Device Deployment (Implementación del dispositivo) > Software > Action (Acción) > Validate (Validar)**.
2. Vea las versiones intermedias de software y contenido que necesita descargar.

STEP 7 | Descargue el contenido y las actualizaciones de software a un host que pueda conectarse y cargar los archivos en Panorama o en un servidor SCP configurado a través de SCP o HTTPS.

De forma predeterminada, puede cargar un máximo de dos actualizaciones de software o contenido de cada tipo a un dispositivo Panorama y si descarga una tercera actualización del mismo tipo, Panorama eliminará la actualización de la versión más antigua de ese tipo. Si necesita cargar más de dos actualizaciones de software o actualizaciones de un solo tipo, use el comando de la CLI **set max-num-images count <number>** para aumentar la cantidad máxima de imágenes que puede almacenar Panorama.

1. Use un host con acceso a internet para iniciar sesión en el [sitio web de Atención al cliente de Palo Alto Networks](#).
2. Descargue las actualizaciones de contenido:
 1. Haga clic en **Dynamic Updates (Actualizaciones dinámicas)** en la sección Recursos.
 2. Debe **Download (Descargar)** la última versión de publicación de contenido (o, como mínimo, la misma o una versión posterior a la que instalará o está ejecutando en el servidor de gestión de Panorama) y guardar el archivo en el host; repita para cada tipo de contenido que necesite actualizar.
3. Descargue las actualizaciones de software:
 1. Vuelva a la página principal del sitio web de Atención al cliente de Palo Alto Networks y haga clic en **Software Updates (Actualizaciones de software)** de la sección Recursos.
 2. Revise la columna Download (Descargar) para determinar las versiones que desea instalar. El nombre de archivo de los paquetes de actualización indica el modelo. Por ejemplo, para actualizar un cortafuegos PA-220 y PA-5260 a PAN-OS 11.0.0, descargue las imágenes **PanOS_220-11.0.0**, **PanOS_3000-11.0.0** y **PanOS_5200-11.0.0**.



*Puede localizar rápidamente imágenes PAN-OS específicas seleccionando **PAN-OS for the PA (PAN-OS para el PA)**-<series/model> desde el menú desplegable **Filter By (Filtrar por)**.*

4. Haga clic en el nombre de archivo adecuado y guarde el archivo en el host.

STEP 8 | Descargue las versiones de software intermedias y la última versión de contenido.

En PAN-OS 11.0, puede descargar varias versiones intermedias mediante la función de descarga de varias imágenes.

1. Seleccione los cortafuegos que desea actualizar (**Required Deployments [Implementaciones requeridas] > Deploy [Implementar]**).
2. Seleccione el origen de la descarga y haga clic en **Download (Descargar)**.

STEP 9 | Instale actualizaciones de contenido en cortafuegos gestionados.



Debe instalar las actualizaciones de contenido antes que las actualizaciones de software.

Instale la actualización de aplicaciones o aplicaciones y amenazas primero, y luego instale cualquier otra actualización (antivirus, WildFire® o filtrado de URL) según sea necesario una a la vez y en cualquier secuencia.

1. Seleccione **Panorama > Device Deployment (Implementación de dispositivos) > Dynamic Updates (Actualizaciones dinámicas)**.
2. Haga clic en **Upload (Cargar)**, seleccione el tipo de actualización en **Type (Tipo)**, haga clic en **Browse (Examinar)** para ir al archivo de actualización y, luego, en **OK (Aceptar)**.
3. Haga clic en **Install From File (Instalar desde el archivo)**, seleccione el **Type (Tipo)** de actualización y seleccione el **File Name (Nombre de archivo)** de la actualización de contenido que acaba de cargar.
4. Seleccione los cortafuegos en los que quiere instalar la actualización.
5. Haga clic en **OK (Aceptar)** para iniciar la instalación.
6. Repita estos pasos para cada actualización de contenido.

STEP 10 | (Cortafuegos que funcionan como portales de GlobalProtect™ únicamente) Cargue y active una actualización del software del agente/aplicación GlobalProtect en los cortafuegos.



Active la actualización en los cortafuegos de modo que los usuarios puedan descargarla en sus endpoints (sistemas cliente).

1. Use un host con acceso a internet para iniciar sesión en el [Sitio web de atención al cliente de Palo Alto Networks](#).
2. Descargue la actualización adecuada del software del agente/aplicación de GlobalProtect.
3. En Panorama, seleccione **Panorama > Device Deployment (Implementación del dispositivo) > GlobalProtect Client (Cliente GlobalProtect)**.
4. Haga clic en **Upload (Cargar)**, seleccione **Browse (Examinar)** la actualización del software del agente/aplicación GlobalProtect correspondiente en el host al que descargó el archivo, y haga clic en **OK (Aceptar)**.
5. Seleccione **Activate From File (Activar desde archivo)** y seleccione **File Name (Nombre de archivo)** de la actualización de agente/aplicación de GlobalProtect que acaba de cargar.



Puede activar solo una versión del software de agente/software de la aplicación a la vez. Si activa una nueva versión, pero algunos agentes requieren una versión anterior, tendrá que volver a activar la versión anterior para que esos agentes descarguen la actualización anterior.

6. Seleccione los cortafuegos en los que quiere activar la actualización.
7. Haga clic en **OK (Aceptar)** para activar.

STEP 11 | Instale PAN-OS 11.0.

Para evitar el estado de inactividad al actualizar el software en cortafuegos de alta disponibilidad (high availability, HA), actualice un peer de HA a la vez.

Para los cortafuegos activo/activo, no importará qué peer actualice primero.

Para los cortafuegos activo/pasivo, debe actualizar el peer pasivo primero, suspender el peer activo (conmutación por error), actualizar el peer activo y luego regresar el peer activo a un estado funcional (conmutación por recuperación).



*(Solo en el caso de SD-WAN) Para conservar un estado preciso de los vínculos de SD-WAN, debe cambiar los cortafuegos de centrales a la versión posterior PAN-OS 11.0 antes de actualizar los cortafuegos de sucursales. La actualización de los cortafuegos de sucursales antes que los cortafuegos de central puede provocar datos de supervisión incorrectos (**Panorama [Panorama] > SD-WAN [SD-WAN] > Monitoring [Supervisión]**) y que los enlaces de SD-WAN se muestren de forma incorrecta como **down (inactivo)**.*

1. Realice los pasos que se aplican a su configuración de cortafuegos para instalar la actualización del software PAN-OS que acaba de cargar.
 - **Cortafuegos que no son de HA:** Haga clic en **Install (Instalar)** en la columna Acción, seleccione todos los cortafuegos que está actualizando, seleccione **Reboot device after install (Reiniciar dispositivo después de la instalación)** y haga clic en **OK (Aceptar)**.
 - **Cortafuegos de HA activo/activo:**
 1. Confirme que la configuración de preferencia está deshabilitada en el primer peer que desea actualizar (**Device [Dispositivo] > High Availability [Alta disponibilidad] > Election Settings [Configuración de elección]**). Si está habilitado, edite **Election Settings (Configuración de elección)** y deshabilite (retire marca) el ajuste **Preemptive (Preferente)** y **Commit (Confirme)** su cambio. Solo necesita desactivar esta configuración en un cortafuegos en cada par de HA, pero asegúrese de que la confirmación sea correcta antes de continuar.
 2. Haga clic en **Install (Instalar)**, deshabilite (retire marca) la casilla de verificación de **Group HA Peers (Peers de HA del grupo)**, seleccione cualquier peer de HA, seleccione **Reboot device after install (Reiniciar dispositivo después de la instalación)** y haga clic en **OK (Aceptar)**. Espere que el cortafuegos termine de reiniciarse antes de continuar.
 3. Haga clic en **Install (Instalar)**, deshabilite (retire marca) la casilla de verificación de **Group HA Peers (Peers de HA del grupo)**, seleccione el peer de HA que todavía no actualizó, seleccione **Reboot device after install (Reiniciar dispositivo después de la instalación)** y haga clic en **OK (Aceptar)**.
 - **Cortafuegos de HA activo/pasivo:** en este ejemplo, el cortafuegos activo se llama fw1 y el cortafuegos pasivo se llama fw2:
 1. Confirme que la configuración de preferencia esté deshabilitada en el primer peer que desea actualizar (**Device [Dispositivo] > High Availability [Alta disponibilidad] > Election Settings [Configuración de elecciones]**). Si está habilitado, edite **Election Settings (Configuración de elección)** y deshabilite (retire marca) el ajuste **Preemptive**

- (Preferente) y **Commit (Confirme)** su cambio. Solo necesita desactivar esta configuración en un cortafuegos en cada par de HA, pero asegúrese de que la confirmación sea correcta antes de continuar.
2. clic en **Install (Instalar)** en la columna Action (Acción) para la actualización correspondiente, deshabilite (desmarque) **Group HA Peers (Peers del grupo de HA)**, seleccione fw2, **Reboot device after install (Reiniciar dispositivo después de la instalación)** y haga clic en **OK (Aceptar)**. Espere que fw2 termine de reiniciarse antes de continuar.
 3. Después de que fw2 termine de reiniciarse, verifique en fw1 (**Dashboard [Panel] > High Availability [Alta disponibilidad]**) que fw2 sigue siendo el peer pasivo (el estado del cortafuegos local es **active [activo]** y el del Peer fw2 es **passive [pasivo]**).
 4. Acceda a fw1 y seleccione **Suspend local device (Suspendir dispositivo local) (Device [Dispositivo] > High Availability [Alta disponibilidad] > Operational Commands [Comandos operativos])**.
 5. Acceda a fw2 (**Dashboard [Panel] > High Availability [Alta disponibilidad]**), verifique que el estado del cortafuegos local sea **active (activo)** y que el del peer sea **suspended (suspendido)**.
 6. Acceda a Panorama, seleccione **Panorama > Device Deployment (Implementación del dispositivo) > Software**, haga clic en **Install (Instalar)** en la columna Action (Acción) de la versión correspondiente, deshabilite (desmarque) **Group HA Peers (Peers de HA del grupo)**, seleccione fw1, **Reboot device after install (Reiniciar dispositivo después de la instalación)** y haga clic en **OK (Aceptar)**. Espere que fw1 termine de reiniciarse antes de continuar.
 7. Acceda a fw1 (**Device [Dispositivo] > High Availability [Alta disponibilidad] > Operational Commands [Comandos operativos]**), haga clic en **Make local device functional (Hacer dispositivo local funcional)** y espere dos minutos antes de continuar.
 8. En fw1 (**Dashboard [Panel] > High Availability [Alta disponibilidad]**), verifique que el estado del cortafuegos local sea **passive (pasivo)** y el del peer (fw2) sea **active (activo)**.

STEP 12 | (Solo modo FIPS-CC) **Actualice Panorama y dispositivos gestionados en modo FIPS-CC.**

La actualización de un cortafuegos gestionado en modo FIPS-CC requiere que restablezca el estado de conexión segura si agregó el recopilador de logs dedicado a la gestión de Panorama mientras el cortafuegos gestionado ejecutaba una versión de PAN-OS 11.0.

No necesita reincorporar el cortafuegos gestionado agregado a la gestión de Panorama si el cortafuegos gestionado ejecutaba PAN-OS 10.0 o una versión anterior.

STEP 13 | Verifique las versiones de contenido o de software que se instalan en cada cortafuegos gestionado.

1. Seleccione **Panorama > Managed Devices (Dispositivos gestionados)**.
2. Busque el cortafuegos y revise los valores de las columnas Versión de software, Aplicaciones y amenazas, Antivirus, Filtrado de URL y Cliente de GlobalProtect.

STEP 14 | Si deshabilitó la preferencia en uno de sus cortafuegos HA antes de actualizar, edite la **Election Settings (Configuración de elección) [Device (Dispositivo) > High Availability (Alta disponibilidad)]** y vuelva a habilitar el ajuste **Preemptive (Preferente)** para ese cortafuegos.

STEP 15 | En la [interfaz web de Panorama](#) inserte toda la configuración gestionada de Panorama en los cortafuegos administrados.

Este paso es necesario para habilitar la confirmación selectiva y el envío de cambios en la configuración de la pila de plantillas y del grupo de dispositivos desde Panorama a los cortafuegos gestionados.

Esto es necesario para enviar con éxito los cambios de configuración a los cortafuegos de sistemas virtuales múltiples gestionados por Panorama después de una correcta actualización a PAN-OS 11.0. Para obtener más información, consulte el cambio en el comportamiento predeterminado de [los objetos de configuración compartidos para cortafuegos de sistemas virtuales múltiples gestionados por Panorama](#).

1. Seleccione **Commit (Confirmar) > Push to Devices (Enviar a dispositivos)**.
2. **Push (Enviar)**.

STEP 16 | Vuelva a generar o a importar todos los certificados para cumplir con el nivel de seguridad 2 de OpenSSL.

Al actualizar a PAN-OS 11.0, se requiere que todos los certificados cumplan con los siguientes requisitos mínimos:

- RSA de 2048 bits o superior, o ECDSA de 256 bits o superior
- Compendio de SHA256 o superior

Consulte la [Guía del administrador de PAN-OS](#) o la [Guía del administrador de Panorama](#) para obtener más información sobre la regeneración o reimportación de los certificados.

STEP 17 | Ver el historial de actualizaciones de software del cortafuegos.

1. Inicie sesión en la interfaz de Panorama.
2. Vaya a **Panorama > Managed Devices (Dispositivos gestionados) > Summary (Resumen)** y haga clic en **Device History (Historial de dispositivos)**.

Actualización de un cortafuegos de ZTP

Después de [añadir con éxito un cortafuegos de ZTP](#) al servidor de gestión Panorama™, configure la versión de PAN-OS de destino del cortafuegos de ZTP. Panorama comprueba si la versión de PAN-OS instalada en el cortafuegos de ZTP es superior o igual que la versión de PAN-OS de destino configurada después de que se conecte correctamente a Panorama por primera vez. Si la versión de PAN-OS instalada en el cortafuegos de ZTP es inferior a la versión de PAN-OS de destino, el cortafuegos de ZTP entra en un ciclo de actualización hasta que se instala la versión de PAN-OS de destino.

STEP 1 | [Inicie sesión en la interfaz web de Panorama](#) como usuario administrador.

STEP 2 | [Añada un cortafuegos ZTP a Panorama](#).

STEP 3 | Seleccione **Panorama > Device Deployment (Implementación del dispositivo) > Updates (Actualizaciones)** y **Check Now (Comprobar ahora)** para comprobar las últimas versiones de PAN-OS.

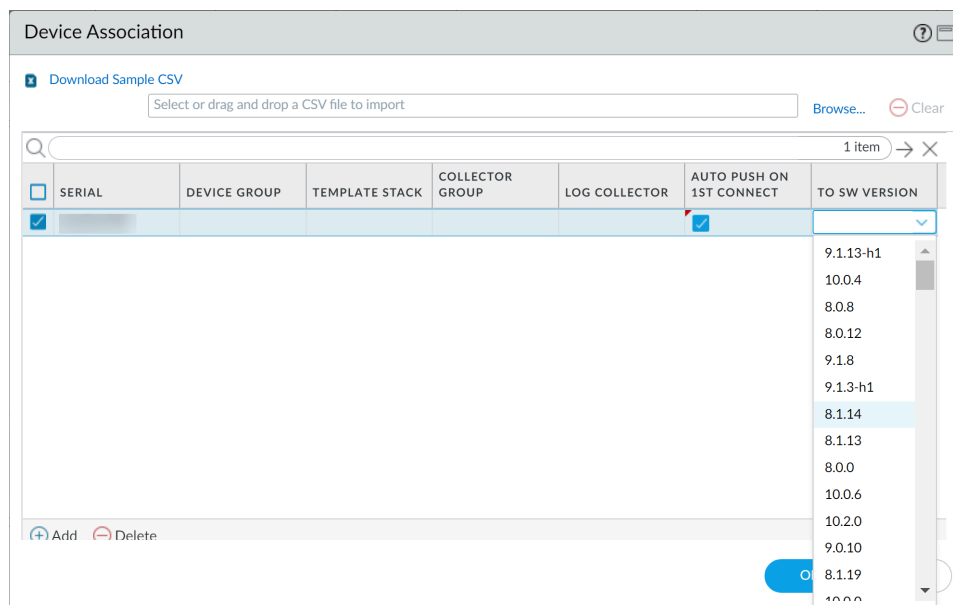
STEP 4 | Seleccione **Panorama > Managed Devices > Summary (Resumen)** y seleccione uno o más cortafuegos de ZTP.

STEP 5 | Vuelva a asociar los cortafuegos de ZTP seleccionados.

STEP 6 | Marque (habilite) Auto Push en 1st Connect Insertar automáticamente en 1.ª conexión).

STEP 7 | En la columna To SW Version (Versión de SW de destino), seleccione la versión de PAN-OS de destino para el cortafuegos de ZTP.

STEP 8 | Haga clic en Aceptar para guardar los cambios.



STEP 9 | Haga clic en Commit (Confirmar) y en Commit to Panorama (Confirmar en Panorama).

STEP 10 | Encienda el cortafuegos de ZTP.

Cuando el cortafuegos de ZTP se conecta a Panorama por primera vez, se actualiza automáticamente a la versión de PAN-OS que seleccionó.

- **Panorama con PAN-OS 11.0.0:** si está actualizando cortafuegos gestionados en versiones principales o de mantenimiento de PAN-OS, las versiones intermedias de PAN-OS en la ruta de actualización se instalan primero, antes de que se instale la versión PAN-OS de destino.

Por ejemplo, configuró **To SW Version (A la versión de SW)** de destino para el cortafuegos gestionado como PAN-OS 11.0.0 y el cortafuegos ejecuta PAN-OS 10.1. En la primera conexión a Panorama, PAN-OS 10.2.0 se instala primero en el cortafuegos gestionado. Una vez que PAN-OS 10.2.0 se instala correctamente, el cortafuegos se actualiza automáticamente a la versión PAN-OS 11.0.0 de destino.

- **Panorama con PAN-OS 11.0.1 y versiones posteriores:** si está actualizando cortafuegos gestionados en versiones principales o de mantenimiento de PAN-OS, se instalan las versiones intermedias principales de PAN-OS en la ruta de actualización y se descarga la versión base principal de PAN-OS antes de que se instale la versión de mantenimiento de PAN-OS de destino.

Por ejemplo, configuró **To SW Version (A la versión de SW)** de destino para el cortafuegos gestionado como PAN-OS 11.0.1 y el cortafuegos ejecuta PAN-OS 10.0. En la primera conexión a Panorama, PAN-OS 10.1.0 y PAN-OS 10.2.0 están instalados en el cortafuegos gestionado. Después de que el cortafuegos gestionado se reinicia, se descarga PAN-OS 11.0.0 y luego el cortafuegos se instala automáticamente en la versión de PAN-OS 11.0.1 de destino.

STEP 11 | Verifique la actualización del software del cortafuegos de ZTP.

1. [Inicio de sesión en la interfaz web de Panorama](#).
2. Seleccione **Panorama > Managed Devices > Summary (Resumen)** y diríjase a los cortafuegos de ZTP.
3. Verifique que la columna **Software Version (Versión de software)** muestre la versión correcta de PAN-OS de destino.

STEP 12 | Para todas las futuras actualizaciones de PAN-OS, consulte [Actualización del cortafuegos a PAN-OS 11.0 desde Panorama](#).

Cambio a una versión anterior de PAN-OS

La forma de cambiar un cortafuegos a la versión anterior PAN-OS 11.0 depende de si está cambiando a una versión de función anterior (donde el primer o segundo dígito en la versión de PAN-OS cambia, por ejemplo, de 9.1.2 a 9.0.8 o de 9.0.3 a 8.1.14) o si cambia a una versión de lanzamiento de mantenimiento anterior dentro de la misma versión de función (donde el tercer dígito en la versión de lanzamiento cambia, por ejemplo, de 8.1.2 a 8.1.0). Cuando cambia de una versión de función a una versión de función anterior, puede migrar la configuración de la versión posterior para incorporar nuevas funciones. Para migrar la configuración de PAN-OS 11.0 a una versión anterior de PAN-OS, primero restaure la configuración para la versión de función anterior a la que está cambiando. No es necesario restaurar la configuración cuando cambia a una versión anterior desde una versión de mantenimiento a otra dentro de la misma versión de función.

- [Cambio de un cortafuegos a una versión de mantenimiento anterior](#)
- [Cambio de un cortafuegos a una versión de funciones anterior](#)
- [Cambio de un agente de Windows a una versión anterior](#)



Siempre cambie a una configuración anterior que coincida con la versión del software. Las versiones y configuraciones de software que no coinciden pueden resultar en cambios a versiones anteriores con fallas o forzar el sistema en modo de mantenimiento. Esto solo aplica al cambiar a una versión anterior desde una versión de función a otra (por ejemplo, 9.0.0 a 8.1.3), no a cambios a versiones de mantenimiento anteriores dentro de la misma versión de función (por ejemplo, 8.1.3 a 8.1.1).

Si tiene un problema con un cambio a una versión anterior, es posible que deba ingresar al modo de mantenimiento y restablecer el dispositivo a los valores predeterminados de fábrica y, luego, restaurar la configuración del archivo de configuración original que se exportó antes de la actualización.

Cambio de un cortafuegos a una versión de mantenimiento anterior

Debido a que las versiones de mantenimiento no incorporan nuevas funciones, puede cambiar a una versión de mantenimiento anterior en la misma versión de función sin tener que restaurar la configuración anterior. Una versión de mantenimiento es una versión en la que cambia el tercer dígito en la versión de lanzamiento, por ejemplo, cambiar de 8.1.6 a 8.1.4 se considera una degradación de la versión de mantenimiento porque solo el tercer dígito en la versión de lanzamiento es diferente.

Utilice el siguiente procedimiento para cambiar a una versión de mantenimiento anterior dentro de la misma versión de función.

STEP 1 | Guarde una copia de seguridad del archivo de configuración actual.



Aunque el cortafuegos crea de forma automática una copia de seguridad de la configuración, se recomienda crear una copia de seguridad antes de cambiar a una versión anterior y almacenarla a nivel externo.

1. **Export named configuration snapshot (Exportar instantánea de configuración con nombre)** (**Device (Dispositivo)** > **Setup (Configuración)** > **Operations (Operaciones)**).
2. Seleccione el archivo XML que contiene su configuración en uso (por ejemplo, **running-config.xml**) y haga clic en **OK (Aceptar)** para exportar el archivo de configuración.
3. Guarde el archivo exportado en una ubicación externa al cortafuegos. Puede usar esta copia de seguridad para restaurar la configuración si tiene problemas con el cambio a la versión anterior.

STEP 2 | Instale la imagen de la versión de mantenimiento anterior.



*Si su cortafuegos no tiene acceso a Internet desde el puerto de gestión, puede descargar la actualización de software desde el [portal de soporte de Palo Alto Networks](#). Luego puede **cargarlo** de forma manual a su cortafuegos.*

1. **Check Now (Verificar ahora)** [**Device (Dispositivo)** > **Software**] para ver las imágenes disponibles.
2. Localice la versión anterior a la que desea cambiar. Si la imagen aún no se ha descargado, entonces seleccione **Download (Descargar)** imagen..
3. Una vez completada la descarga, debe **Install (Instalar)** la imagen.
4. Una vez que la instalación se realiza completamente , reinicie mediante uno de los siguientes métodos:
 - Si se le pide que reinicie, haga clic en **Yes (Sí)**.
 - Si no se le solicita reiniciar, vaya a Device Operations (Operaciones del dispositivo) (**Device [Dispositivo]** > **Setup [Configuración]** > **Operations [Operaciones]**) y **Reboot Device (Reiniciar dispositivo)**.

Cambio de un cortafuegos a una versión de funciones anterior

Use el siguiente flujo de trabajo para restaurar la configuración que se estaba ejecutando antes de actualizar a una versión de características diferente. Cualquier cambio realizado desde la actualización se perderá. Por lo tanto, es importante hacer una copia de seguridad de su configuración actual para que pueda restaurar esos cambios cuando vuelva a la versión de función más reciente. Revise [Consideraciones sobre el cambio a versiones anteriores/posteriores de complementos de Panorama](#) antes de cambiar el cortafuegos a una versión de función anterior.



Para degradar de PAN-OS 11.0 a una versión anterior de PAN-OS, debe descargar e instalar PAN-OS 10.1.3 o una versión posterior de PAN-OS 11.0 antes continuar la ruta de degradación a la versión de PAN-OS de destino. La versión anterior de PAN-OS 11.0 falla si intenta cambiar a PAN-OS 10.1.2 o una versión anterior de PAN-OS 11.0.

Utilice el siguiente procedimiento para cambiar a una versión de función anterior.

STEP 1 | Guarde una copia de seguridad del archivo de configuración actual.



Aunque el cortafuegos crea automáticamente una copia de seguridad de la configuración, se recomienda crear una copia de seguridad antes de actualizar y almacenarla externamente.

1. **Export named configuration snapshot (Exportar instantánea de configuración con nombre)** (**Device (Dispositivo)** > **Setup (Configuración)** > **Operations (Operaciones)**).
2. Seleccione el archivo XML que contiene su configuración en uso (por ejemplo, **running-config.xml**) y haga clic en **OK (Aceptar)** para exportar el archivo de configuración.
3. Guarde el archivo exportado en una ubicación externa al cortafuegos. Puede usar esta copia de seguridad para restaurar la configuración si tiene problemas con el cambio a la versión anterior.

STEP 2 | Instale la imagen de la versión anterior.



Las versiones de autoguardado se crean cuando actualiza a una nueva versión.

1. **Check Now (Verificar ahora)** [**Device (Dispositivo)** > **Software**] para ver las imágenes disponibles.
2. Instale PAN-OS 10.1.

Para cambiar de PAN-OS 11.0 a una versión de función anterior, primero debe cambiar a PAN-OS 10.1.3 o una versión posterior de PAN-OS 11.0. Después de cambiar correctamente a PAN-OS 10.1.3 o a una versión posterior de PAN-OS 11.0, puede continuar el cambio a la versión de PAN-OS de destino.

1. Localice y **descargue** la imagen de PAN-OS 11.0.
2. **Instale** la imagen de PAN-OS 11.0.
3. Localice la imagen de PAN-OS de destino a la que desea cambiar a una versión anterior. Si la imagen aún no se ha descargado, entonces seleccione **Download (Descargar)** imagen..
4. Una vez completada la descarga, debe **Install (Instalar)** la imagen.
5. **Select a Config File for Downgrading (Seleccionar un archivo de configuración para cambiar a versión anterior)**, que el cortafuegos cargará después de reiniciar el dispositivo. En la mayoría de los casos, debe seleccionar la configuración que se guardó automáticamente cuando actualizó desde la versión a la que ahora está volviendo. Por ejemplo, si está ejecutando PAN-OS 11.0 y cambia a PAN-OS 10.2.2, seleccione **autosave-10.2.2**.
6. Una vez que la instalación se realiza completamente, reinicie mediante uno de los siguientes métodos:
 - Si se le pide que reinicie, haga clic en **Yes (Sí)**.
 - Si no se le solicita reiniciar, vaya a Operaciones del dispositivo [**Device (Dispositivo)** > **Setup (Configuración)** > **Operations (Operaciones)**] y seleccione **Reboot Device (Reiniciar dispositivo)**.

Cambio de un agente de Windows a una versión anterior

Después de desinstalar el agente de User-ID basado en Windows de PAN-OS 11.0, realice los pasos siguientes antes de instalar una versión anterior del agente.

- STEP 1 |** Abra el menú Inicio de Windows y seleccione **Administrative Tools (Herramientas administrativas)**.
- STEP 2 |** Seleccione **Computer Management (Administración de ordenador) > Services and Applications (Servicios y aplicaciones) > Services (Servicios)** y haga doble clic en **User-ID Agent (Agente de User-ID)**.
- STEP 3 |** Seleccione **Log On (Iniciar sesión)**, luego, **This Account (Esta cuenta)**, y especifique el nombre de usuario para la cuenta de agente de User-ID.
- STEP 4 |** Especifique el valor de **Contraseña** y seleccione **Confirmar contraseña**.
- STEP 5 |** Haga clic en **OK (Aceptar)** para guardar los cambios.

Solución de problemas del cambio a versiones posteriores de PAN-OS

A fin de solucionar problemas de cambio a versiones posteriores de PAN-OS, utilice la siguiente tabla para revisar los posibles problemas y cómo resolverlos.

Síntoma	Solución
La licencia de garantía del software expiró.	<p>Desde la CLI, elimine la clave de licencia caducada:</p> <ol style="list-style-type: none"> 1. Introduzca la clave de licencia de eliminación<software license key>. 2. Introduzca la clave de licencia de eliminación Software_Warranty<expiredate>.key.
Las versiones del software PAN-OS más recientes no estaban disponibles.	<p>Solo puede ver las versiones de software que están una versión de función por delante de la versión instalada actual. Por ejemplo, si tiene instalada una versión 8.1, solo las versiones 9.0 estarán disponibles para usted. Para ver las versiones 9.1, primero debe cambiar a la versión posterior 9.0.</p>
Surgió un error al buscar actualizaciones dinámicas.	<p>Este problema se produce debido a un error de conectividad de red. Consulte el artículo de KnowledgeBase Dynamic Updates Display Error After Clicking On Check Now Button (Error de las actualizaciones dinámicas después de hacer clic en el botón Verificar ahora).</p>
No se encontró ningún certificado de dispositivo válido.	<p>En PAN-OS 9.1.3 y versiones posteriores, se debe instalar un certificado de dispositivo si está aprovechando un servicio en la nube de Palo Alto Networks. Para instalar el certificado del dispositivo:</p> <ol style="list-style-type: none"> 1. Inicie sesión en el portal de atención al cliente. 2. Seleccione Generate OTP (Generar OTP) (Assets [Activos] > Device Certificates [Certificados de dispositivo]). 3. Para Device Type (Tipo de dispositivo), seleccione Generate OTP for Next-Gen Firewalls (Generar OTP para cortafuegos de nueva generación).

Síntoma	Solución
	<ol style="list-style-type: none"> 4. Seleccione el número de serie de su dispositivo PAN OS. 5. Genere el OTP y copie la contraseña de un solo uso. 6. Inicie sesión en el firewall como usuario administrador. 7. Seleccione Device Certificate (Certificado de dispositivo) (Device [Dispositivo] > Setup [Configuración] > Management [Administración] > Device [Dispositivo] > Certificate [Certificado] y Get Certificate [Obtener certificado]). 8. Pegue la OTP y haga clic en OK (Aceptar).
El archivo de imagen de software no se pudo cargar en el administrador de software debido a un error de autenticación de imagen.	Para actualizar la lista de imágenes de software, haga clic en Check Now (Comprobar ahora) . Esto establece una nueva conexión con el servidor de actualizaciones.
La versión del complemento VMware NSX no era compatible con la nueva versión del software.	El complemento VMware NSX se instaló de forma automática cuando se pasó a la versión posterior 8.0. Si utiliza el complemento, puede desinstalarlo.
El tiempo de reinicio después de pasar a la versión posterior PAN-OS 9.1 fue más prologando de lo esperado.	Cambie a la versión de lanzamiento de contenido de aplicaciones y amenazas 8221 o posterior. Para obtener más información sobre las versiones mínimas de software y contenido, consulte <xref to 11.0 Associated Software and Content Versions> .
El dispositivo no tenía soporte por más que las licencias estaban activas.	<p>En Device (Dispositivo) > Software (Software), haga clic en Check Now (Comprobar ahora).</p> <p>De esta forma se actualiza la información de licencia del cortafuegos al establecer una nueva conexión con el servidor de actualización.</p> <p>Si esto no funciona desde la interfaz web, utilice la verificación del software del sistema de solicitud.</p>
El servidor de seguridad no tenía una dirección DHCP asignada por el servidor DHCP.	Configure una regla de la política de seguridad que permita el tráfico desde el servidor DHCP del ISP a las redes internas.

Síntoma	Solución
El cortafuegos inicia continuamente en modo de mantenimiento.	En la CLI, acceda a la Maintenance Recovery Tool (Herramienta de recuperación de mantenimiento, MRT) En la ventana MRT, seleccione Continue (Continuar) > Disk Image (Imagen de disco) . Seleccione Reinstall (Reinstalar) <current version> o Revert to (Volver a) <previous version> Una vez finalizada la operación de reversión o reinstalación, seleccione Reboot (Reiniciar) .
En una configuración de HA, el cortafuegos pasa a un estado de suspensión después de actualizar el cortafuegos del peer con un mensaje de error de que el cortafuegos es demasiado antiguo.	Actualizar un cortafuegos a una versión que está a más de una versión principal por delante resultará en una interrupción de la red. Debe actualizar ambos cortafuegos solo una versión principal antes de actualizar a la siguiente versión principal. Degrade el cortafuegos del peer a la versión en la que se detuvo el cortafuegos suspendido.

Actualización del cortafuegos VM-Series

- > Cambio del software PAN-OS VM-Series a una versión posterior (independiente)
- > Cambio del software PAN-OS VM-Series a una versión posterior (par de HA)
- > Cambio del software PAN-OS de VM-Series a una versión posterior mediante Panorama
- > Actualización de la versión de software de PAN-OS (VM-Series para NSX)
- > Actualización del modelo VM-Series
- > Actualización del modelo VM-Series en un par de HA
- > Cambio a versión posterior del cortafuegos VM-Series

Cambio del software PAN-OS VM-Series a una versión posterior (independiente)

Revise las nuevas características, los problemas abordados y los problemas conocidos y luego utilice el siguiente procedimiento para actualizar un cortafuegos que no esté en una configuración de alta disponibilidad.



Para evitar afectar el tráfico, planifique la actualización dentro del periodo de interrupción. Asegúrese de que el cortafuegos esté conectado a una fuente de alimentación fiable. Si se interrumpe la alimentación durante una actualización, el cortafuegos puede quedar inutilizado.

STEP 1 | Compruebe que haya suficientes recursos de hardware disponibles para el cortafuegos VM-Series.

Consulte los [Requisitos del sistema VM-Series](#) para ver los requisitos de recursos de cada modelo VM-Series. Asigne recursos de hardware adicionales antes de continuar con el proceso de actualización; el proceso para asignar recursos de hardware adicionales difiere en cada hipervisor.

Si el cortafuegos VM-Series no tiene los recursos necesarios para el modelo, la capacidad asociada con el VM-50 es la predeterminada.

STEP 2 | Desde la interfaz web, desplácese hasta **Device (Dispositivo) > Licenses (Licencias)** y asegúrese de que tiene la licencia correcta para el cortafuegos VM-Series y que la licencia está activada.

En la versión independiente del cortafuegos VM-Series, vaya a **Device (Dispositivo) > Support (Asistencia técnica)** y asegúrese de que tiene activada la licencia de asistencia técnica.

STEP 3 | Guarde una copia de seguridad del archivo de configuración actual.



A pesar de que el cortafuegos crea automáticamente una copia de seguridad de la configuración, se recomienda crear y almacenar externamente una copia de seguridad antes de la actualización.

1. Seleccione **Device (Dispositivo) > Setup (Configuración) > Operations (Operaciones)** y haga clic en **Export named configuration snapshot (Exportar instantáneas de configuración con nombre)**.
2. Seleccione el archivo XML que contiene su configuración en uso (por ejemplo, **running-config.xml**) y haga clic en **OK (Aceptar)** para exportar el archivo de configuración.
3. Guarde el archivo exportado en una ubicación externa al cortafuegos. Puede usar esta copia de seguridad para restaurar la configuración si tiene problemas con la actualización.

STEP 4 | Si ha habilitado User-ID, después de la actualización, el cortafuegos borra las asignaciones actuales de dirección IP a nombre de usuario y de grupo para que puedan volver a rellenarse con los atributos

de las fuentes de User-ID. Para calcular el tiempo necesario para que su entorno vuelva a rellenar las asignaciones, ejecute los siguientes comandos de la CLI en el cortafuegos.

- Para asignaciones de dirección IP a nombre de usuario:
 - **show user user-id-agent state all**
 - **show user server-monitor state all**
- Para asignaciones de grupo: **show user group-mapping statistics**

STEP 5 | Asegúrese de que el cortafuegos está ejecutando la última versión de contenido.

1. Seleccione **Device (Dispositivo) > Dynamic Updates (Actualizaciones dinámicas)** y vea qué versión de contenido de **Applications (Aplicaciones)** o **Applications and Threats (Aplicaciones y amenazas)** está instalada actualmente.
2. Si el cortafuegos no ejecuta la versión de lanzamiento de contenido mínima requerida o una versión posterior requerida para PAN-OS, debe **Check Now (Comprobar ahora)** para recuperar una lista de actualizaciones disponibles.
3. Ahora debe localizar y **Download (Descargar)** la versión de lanzamiento de contenido requerida.

Después de descargar correctamente un archivo de actualización de contenido, el enlace en la columna Acción cambia de **Download (Descargar)** a **Install (Instalar)** para esa versión de contenido.

4. **Install (Instalar)** la actualización.

STEP 6 | Actualización del complemento de VM-Series.

1. Antes de realizar la actualización, consulte las Notas de la versión más recientes para obtener información sobre si un nuevo plugin de VM-Series afecta su entorno.

Por ejemplo, supongamos que una nueva versión del plugin VM-Series solo incluye las funciones de AWS. Para aprovechar las nuevas funciones, debe actualizar el plugin en sus instancias de cortafuegos VM-Series en AWS.



No instale una actualización que no corresponda a su entorno.

2. Inicie sesión en el cortafuegos VM-Series y verifique el panel para ver la versión del plugin.
3. Seleccione **Device (Dispositivo) > Plugins (Complementos)** para ver la versión del complemento. Utilice **Check Now (Comprobar ahora)** para comprobar si hay actualizaciones.
4. Seleccione la versión del complemento y haga clic en **Install (Instalar)** en la columna Action (Acción) para instalar el complemento.

STEP 7 | Actualización de PAN-OS.



*Si su cortafuegos no tiene acceso a Internet desde el puerto de administración, puede descargar la imagen del software desde el [Portal de atención al cliente de Palo Alto Networks](#) y luego manualmente **Upload (Cargar)** la imagen en el cortafuegos.*

1. Seleccione **Device (Dispositivo) > Software** y haga clic en **Check Now (Comprobar ahora)** para mostrar las actualizaciones de PAN-OS más recientes.
2. Debe localizar y **Download (Descargar)** la versión de PAN-OS de destino.
3. Después de descargar la imagen (o, para una actualización manual, después de cargar la imagen), debe **Install (Instalar)** la imagen.
4. Una vez que la instalación se realiza completamente, reinicie mediante uno de los siguientes métodos:
 - Si se le pide que reinicie, haga clic en **Yes (Sí)**.
 - Si no se le solicita que reinicie, seleccione **Device (Dispositivo) > Setup (Configuración) > Operations (Operaciones)** y haga clic en **Reboot Device (Reiniciar dispositivo)**.



Llegado este punto, el cortafuegos borra las asignaciones de User-ID y se conecta a las fuentes de User-ID para volver a rellenar las asignaciones.

5. Si ha habilitado User-ID, use los siguientes comandos de la CLI para verificar que el cortafuegos ha vuelto a rellenar las asignaciones de dirección IP a nombre de usuario y de grupo antes de permitir el tráfico.
 - **show user ip-user-mapping all**
 - **show user group list**
6. Si está actualizando a una versión XFR por primera vez, repita este paso para actualizar a la versión XFR correspondiente.

STEP 8 | Compruebe que el cortafuegos esté pasando el tráfico.

Seleccione **Monitor (Supervisar) > Session Browser (Navegador de sesión)** y compruebe que esté viendo nuevas sesiones.

Cambio del software PAN-OS VM-Series a una versión posterior (par de HA)

Utilice el siguiente procedimiento para actualizar un par de cortafuegos en una configuración de alta disponibilidad (HA). Este procedimiento se aplica tanto a la configuración activa/pasiva como a la activa/activa.

Para evitar el estado de inactividad cuando actualiza cortafuegos de alta disponibilidad (high availability, HA), actualice un peer de HA a la vez: Para los cortafuegos activo/activo, no importa qué miembro actualice primero (aunque, por sencillez, este procedimiento le muestra cómo actualizar primero el miembro activo-secundario). Para los cortafuegos activo/pasivo, debe actualizar el peer pasivo primero, suspender el peer activo (conmutación por error), actualizar el peer activo y luego devolver el peer a un estado funcional (conmutación por recuperación). Para evitar la conmutación por error durante la actualización de los miembros del HA, debe asegurarse de que la opción de preferencia esté deshabilitada antes de continuar con la actualización. Solo necesita deshabilitar la preferencia en un miembro en la pareja.



Para evitar afectar el tráfico, planifique la actualización dentro del periodo de interrupción. Asegúrese de que los cortafuegos estén conectados a una fuente de alimentación fiable. Si se interrumpe la alimentación durante una actualización, los cortafuegos pueden quedar inutilizados.

STEP 1 | Compruebe que haya suficientes recursos de hardware disponibles para el cortafuegos VM-Series.

Consulte los [Requisitos del sistema VM-Series](#) para ver los requisitos de recursos de cada modelo VM-Series. Asigne recursos de hardware adicionales antes de continuar con el proceso de actualización; el proceso para asignar recursos de hardware adicionales difiere en cada hipervisor.

Si el cortafuegos VM-Series no tiene los recursos necesarios para el modelo, la capacidad asociada con el VM-50 es la predeterminada.

STEP 2 | Desde la interfaz web, desplácese hasta **Device (Dispositivo) > Licenses (Licencias)** y asegúrese de que tiene la licencia correcta para el cortafuegos VM-Series y que la licencia está activada.

En la versión independiente del cortafuegos VM-Series, vaya a **Device (Dispositivo) > Support (Asistencia técnica)** y asegúrese de que tiene activada la licencia de asistencia técnica.

STEP 3 | Guarde una copia de seguridad del archivo de configuración actual.



A pesar de que el cortafuegos crea automáticamente una copia de seguridad de la configuración, se recomienda crear y almacenar externamente una copia de seguridad antes de la actualización.

Lleve a cabo estos pasos en cada cortafuegos en la pareja:

1. Seleccione **Device (Dispositivo) > Setup (Configuración) > Operations (Operaciones)** y haga clic en **Export named configuration snapshot (Exportar instantáneas de configuración con nombre)**.
2. Seleccione el archivo XML que contiene su configuración en uso (por ejemplo, **running-config.xml**) y haga clic en **OK (Aceptar)** para exportar el archivo de configuración.
3. Guarde el archivo exportado en una ubicación externa al cortafuegos. Puede usar esta copia de seguridad para restaurar la configuración si tiene problemas con la actualización.

STEP 4 | Si ha habilitado User-ID, después de la actualización, el cortafuegos borra las asignaciones actuales de dirección IP a nombre de usuario y de grupo para que puedan volver a rellenarse con los atributos de las fuentes de User-ID. Para calcular el tiempo necesario para que su entorno vuelva a rellenar las asignaciones, ejecute los siguientes comandos de la CLI en el cortafuegos.

- Para asignaciones de dirección IP a nombre de usuario:
 - **show user user-id-agent state all**
 - **show user server-monitor state all**
- Para asignaciones de grupo: **show user group-mapping statistics**

STEP 5 | Asegúrese de que cada cortafuegos en la pareja de HA está ejecutando la última versión de contenido.

Consulte las [notas de versión](#) para obtener la versión de contenido mínima que debe instalar para una versión de PAN-OS 11.0. Asegúrese de seguir las [Prácticas recomendadas para las actualizaciones de aplicaciones y amenazas](#).

1. Seleccione **Device (Dispositivo) > Dynamic Updates (Actualizaciones dinámicas)** y compruebe qué **Applications (Aplicaciones)** o **Applications and Threats (Aplicaciones y amenazas)** para determinar qué actualización está instalada actualmente.
2. Si los cortafuegos no ejecutan la versión de lanzamiento de contenido mínima requerida o una versión posterior requerida para la versión de software que está instalando, debe **Check Now (Comprobar ahora)** para recuperar una lista de actualizaciones disponibles.
3. Ahora debe localizar y **Download (Descargar)** la versión de lanzamiento de contenido requerida.
Después de descargar correctamente un archivo de actualización de contenido, el enlace en la columna Acción cambia de **Download (Descargar)** a **Install (Instalar)** para esa versión de contenido.
4. **Install (Instalar)** la actualización. Debe instalar la actualización en ambos pares.

STEP 6 | Actualización del complemento de VM-Series.

1. Antes de realizar la actualización, consulte las Notas de la versión más recientes para obtener información sobre si un nuevo plugin de VM-Series afecta su entorno.

Por ejemplo, supongamos que una nueva versión del plugin VM-Series solo incluye las funciones de AWS. Para aprovechar las nuevas funciones, debe actualizar el plugin en sus instancias de cortafuegos VM-Series en AWS.



No instale una actualización que no corresponda a su entorno.

2. Inicie sesión en el cortafuegos VM-Series y verifique el panel para ver la versión del plugin.
3. Seleccione **Device (Dispositivo) > Plugins (Complementos)** para ver la versión del complemento. Utilice **Check Now (Comprobar ahora)** para comprobar si hay actualizaciones.
4. Seleccione la versión del complemento y haga clic en **Install (Instalar)** en la columna Action (Acción) para instalar el complemento.

Al instalar el complemento en los cortafuegos VM-Series en una pareja de HA, instale el complemento en el miembro pasivo antes de hacerlo en el miembro activo. Después de instalar el complemento en el peer pasivo, pasará a un estado no funcional. La instalación del plugin en el peer activo devuelve el peer pasivo a un estado funcional.

STEP 7 | Deshabilite la preferencia en el primer miembro de cada pareja. Solo necesita desactivar esta configuración en un cortafuegos en la pareja de HA, pero asegúrese de que la confirmación sea correcta antes de continuar con la actualización.

1. Seleccione **Device (Dispositivo) > High Availability (Alta disponibilidad)** y edite la sección **Election Settings (Ajustes de elección)**.
2. Si esta opción está deshabilitada, deshabilite (desmarque) la opción **Preemptive (Preferente)** y haga clic en **OK (Aceptar)**.
3. Haga clic en **Commit (Confirmar)** para confirmar el cambio.

STEP 8 | Instale la versión PAN-OS en el primer miembro.

Para minimizar el tiempo de inactividad en una configuración activa/pasiva, actualice primero el miembro pasivo. Para una configuración activa/activa, actualice primero el miembro secundario. Como

práctica recomendada, si está utilizando una configuración activa/activa, recomendamos actualizar ambos miembros durante el mismo periodo de mantenimiento.



Si desea comprobar que la HA está funcionando correctamente antes de la actualización, considere actualizar primero el miembro activo en una configuración activa/pasiva para asegurarse de que la conmutación por error se lleva a cabo sin incidentes.

1. En el primer miembro, seleccione **Device (Dispositivo) > Software** y haga clic en **Check Now (Comprobar ahora)** para obtener las últimas actualizaciones.
2. Debe localizar y **Download (Descargar)** la versión de PAN-OS de destino.



*Si su cortafuegos no tiene acceso a Internet desde el puerto de administración, puede descargar la imagen del software desde [Portal de asistencia técnica de Palo Alto Networks](#) y luego manualmente **Load (Cargar)** la imagen en su cortafuegos.*

3. Después de descargar la imagen (o, para una actualización manual, después de cargar la imagen), debe **Install (Instalar)** la imagen.
4. Una vez que la instalación se realiza completamente, reinicie mediante uno de los siguientes métodos:
 - Si se le pide que reinicie, haga clic en **Yes (Sí)**.
 - Si no se le solicita que reinicie, seleccione **Device (Dispositivo) > Setup (Configuración) > Operations (Operaciones)** y haga clic en **Reboot Device (Reiniciar dispositivo)**.
5. Una vez que el dispositivo termine de reiniciarse, vea el widget de Alta disponibilidad en el **Dashboard (Panel)** y verifique que el dispositivo que acaba de actualizar sigue siendo el miembro pasivo o activo secundario en la configuración de HA.

STEP 9 | Instale la versión PAN-OS en el segundo miembro.

1. (Solo configuraciones activas/pasivas) Suspenda el miembro activo para que HA realice la conmutación por error al miembro que acaba de actualizar.
 1. En el miembro activo, seleccione **Device (Dispositivo) > High Availability (Alta disponibilidad) > Operational Commands (Comandos operativos)** y haga clic en **Suspend local device (Suspend dispositivo local)**.
 2. Vea el widget de alta disponibilidad en el **Dashboard (Panel)** y verifique que el estado cambie a **Passive (Pasivo)**.
 3. En el otro miembro, verifique que esté activo y que esté pasando tráfico (**Monitor (Supervisar) > Session Browser (Navegador de sesión)**).
2. En el segundo miembro, seleccione **Device (Dispositivo) > Software** y haga clic en **Check Now (Comprobar ahora)** para obtener las últimas actualizaciones.
3. Debe localizar y **Download (Descargar)** la versión de PAN-OS de destino.
4. Después de descargarla, debe **Install (Instalar)** la imagen.
5. Una vez que la instalación se realiza completamente, reinicie mediante uno de los siguientes métodos:
 - Si se le pide que reinicie, haga clic en **Yes (Sí)**.
 - Si no se le solicita que reinicie, seleccione **Device (Dispositivo) > Setup (Configuración) > Operations (Operaciones)** y haga clic en **Reboot Device (Reiniciar dispositivo)**.
6. (Solo configuraciones en parejas activo/pasivo) En la CLI del par que actualizó, ejecute el siguiente comando para que el cortafuegos vuelva a funcionar:

request high-availability state functional

STEP 10 | Verifique que ambos miembros estén pasando el tráfico como está previsto.

En una configuración activa/pasiva, solo el miembro activo debe pasar el tráfico; en una configuración activa/activa, sin embargo, ambos miembros deberían pasar el tráfico.

Ejecute los siguientes comandos de la CLI para confirmar que la actualización se realizó correctamente:

- (Solo miembros activos) Para verificar que los miembros activos están pasando tráfico, ejecute el comando **show session all**.
- Para verificar la sincronización de la sesión, ejecute el comando **show high-availability interface ha2** y asegúrese de que los contadores de la interfaz de hardware en la tabla de la CPU aumentan de la siguiente forma:
 - En una configuración activa/pasiva, solo el par activo muestra los paquetes transmitidos; el par pasivo mostrará solo los paquetes recibidos.



Si habilitó la conexión persistente de HA2, los contadores de la interfaz de hardware en el par pasivo mostrarán los paquetes de transmisión y recepción. Esto ocurre porque HA2 keep-alive es bidireccional, lo que significa que ambos miembros transmiten paquetes de HA2 keep-alive.

- En una configuración activo/activo, verá paquetes recibidos y paquetes transmitidos de ambos peers.

STEP 11 | Si ha deshabilitado la preferencia antes de la actualización, vuelva a habilitarla ahora.

1. Seleccione **Device (Dispositivo) > High Availability (Alta disponibilidad)** y edite la sección **Election Settings (Ajustes de elección)**.
2. Seleccione **Preemptive (Preferente)** y haga clic en **OK (Aceptar)**.
3. Haga clic en **Commit (Confirmar)** para confirmar el cambio.

Cambio del software PAN-OS de VM-Series a una versión posterior mediante Panorama

Utilice el siguiente procedimiento para actualizar los cortafuegos que gestiona con Panorama. Este procedimiento aplica a los cortafuegos independientes y los cortafuegos que se implementan en una configuración de alta disponibilidad (HA).



Si Panorama no se puede conectar directamente al servidor de actualizaciones, siga el procedimiento para la [Implementación de actualizaciones a los cortafuegos cuando Panorama no está conectado a internet](#) de modo que pueda descargar manualmente imágenes a Panorama y luego distribuirlas a los cortafuegos.

Antes de actualizar los cortafuegos desde Panorama, debe realizar lo siguiente:

- ❑ Asegúrese de que Panorama ejecute una versión PAN-OS igual o posterior a la versión de actualización. Debe [actualizar Panorama](#) y sus [Recopiladores de logs](#) a 9.1 antes de actualizar los cortafuegos gestionados a esta versión. Además, al actualizar los Recopiladores de logs a 9.1, debe actualizar todos los Recopiladores de logs al mismo tiempo debido a los cambios en la infraestructura de generación de logs.
- ❑ Planifique un periodo de mantenimiento extendido de hasta seis horas cuando actualice Panorama a 9.1. Esta versión incluye cambios significativos en la infraestructura, lo que significa que la actualización de Panorama llevará más tiempo que otras versiones anteriores.
- ❑ Asegúrese de que todos los cortafuegos estén conectados a una fuente de alimentación fiable. Si se interrumpe la alimentación durante una actualización, los cortafuegos pueden resultar inútiles.

STEP 1 | Después de [actualizar Panorama](#), [confirme y envíe](#) la configuración a los cortafuegos que planifica actualizar.

STEP 2 | Compruebe que haya suficientes recursos de hardware disponibles para el cortafuegos VM-Series.

Consulte los [Requisitos del sistema VM-Series](#) para ver los requisitos de recursos de cada modelo VM-Series. Asigne recursos de hardware adicionales antes de continuar con el proceso de actualización; el proceso para asignar recursos de hardware adicionales difiere en cada hipervisor.

Si el cortafuegos VM-Series no tiene los recursos necesarios para el modelo, la capacidad asociada con el VM-50 es la predeterminada.

STEP 3 | Desde la interfaz web, desplácese hasta **Device (Dispositivo) > Licenses (Licencias)** y asegúrese de que tiene la licencia correcta para el cortafuegos VM-Series y que la licencia está activada.

En la versión independiente del cortafuegos VM-Series, vaya a **Device (Dispositivo) > Support (Asistencia técnica)** y asegúrese de que tiene activada la licencia de asistencia técnica.

STEP 4 | Guarde una copia de seguridad del archivo de configuración actual en cada cortafuegos gestionado que desee actualizar.



A pesar de que el cortafuegos crea automáticamente una copia de seguridad de la configuración, se recomienda crear y almacenar externamente una copia de seguridad antes de la actualización.

1. En la interfaz web de Panorama, seleccione **Panorama > Setup (Configuración) > Operations (Operaciones)** y haga clic en **Export Panorama and devices config bundle (Exportar lote de configuración de dispositivos y Panorama)** para generar y exportar la copia de seguridad de configuración más reciente de Panorama y cada dispositivo gestionado.
2. Guarde el archivo exportado en una ubicación externa al cortafuegos. Puede usar esta copia de seguridad para restaurar la configuración si tiene problemas con la actualización.

STEP 5 | Actualice la versión de contenido de los cortafuegos que desea actualizar.

Consulte las [Notas de la versión](#) para obtener la versión de contenido mínima necesaria para PAN-OS 11.0. Siga las [prácticas recomendadas para las actualizaciones de aplicaciones y amenazas](#) cuando implemente actualizaciones de contenido en Panorama y los cortafuegos gestionados.

1. Seleccione **Panorama > Device Deployment (Implementación del dispositivo) > Dynamic Updates (Actualizaciones dinámicas)** y haga clic en **Check Now (Comprobar ahora)** para comprobar las últimas actualizaciones. Si hay una actualización disponible, la columna Acción mostrará el enlace **Download (Descargar)**.
2. Si aún no instaló la actualización, seleccione **Download (Descargar)** para descargar la versión de contenido más reciente.
3. Haga clic en **Install (Instalar)**, seleccione los cortafuegos en los que desee instalar la actualización y haga clic en **OK (Aceptar)**. Si actualiza los cortafuegos de HA, deberá actualizar contenido en ambos peers.

STEP 6 | (Solo actualizaciones de cortafuegos de HA) Si va a actualizar los cortafuegos que forman parte de un par de HA, deshabilite la opción de preferencia. Solo debe deshabilitar esta opción en un cortafuegos de cada par de HA.

1. Seleccione **Device (Dispositivo) > High Availability (Alta disponibilidad)** y edite la sección **Election Settings (Ajustes de elección)**.
2. Si esta opción está deshabilitada, deshabilite (desmarque) la opción **Preemptive (Preferente)** y haga clic en **OK (Aceptar)**.
3. Haga clic en **Commit (Confirmar)** para confirmar los cambios. Asegúrese de que la confirmación se realice correctamente antes de continuar con la actualización.

STEP 7 | Descargue la imagen de la versión de PAN-OS que le interesa.

1. Seleccione **Panorama > Device Deployment (Implementación del dispositivo) > Software** y haga clic en **Check Now (Comprobar ahora)** para comprobar las últimas actualizaciones.
2. **Download (Descargar)** el archivo (o los archivos) específico del cortafuegos para la versión publicada a la que está actualizando. Debe descargar un archivo de instalación separado para cada modelo de cortafuegos (o serie de cortafuegos) que desee actualizar.

STEP 8 | Instale la actualización de software PAN-OS en los cortafuegos.

1. Haga clic en **Install (Instalar)** en la columna Action (Acción) que corresponda a los modelos de cortafuegos que desee actualizar.
2. En el cuadro de diálogo Deploy Software (Implementar software), seleccione todos los cortafuegos que desea actualizar. Para reducir el estado de inactividad, seleccione solo un peer en cada par de HA. En los pares activo/pasivo, seleccione el peer pasivo; en los pares activo/activo, seleccione el peer activo secundario.
3. **(Solo actualizaciones de cortafuegos de HA)** Asegúrese de que la opción **Group HA Peers (Agrupar miembros de HA)** no esté seleccionada.
4. Seleccione **Reboot device after install (Reiniciar dispositivo tras la instalación)**.
5. Para comenzar la actualización, haga clic en **OK (Aceptar)**.
6. Una vez que la instalación se realiza completamente, reinicie mediante uno de los siguientes métodos:
 - Si se le pide que reinicie, haga clic en **Yes (Sí)**.
 - Si no se le solicita que reinicie, seleccione **Device (Dispositivo) > Setup (Configuración) > Operations (Operaciones)** y haga clic en **Reboot Device (Reiniciar dispositivo)**.
7. Después de que los cortafuegos terminen de reiniciarse, seleccione **Panorama > Managed Devices (Dispositivos gestionados)** y verifique que la versión de software sea 9.1.0 en los cortafuegos que actualizó. Además, verifique que el estado de HA de los cortafuegos pasivos que actualizó continúe siendo pasivo.

STEP 9 | (Solo actualizaciones de cortafuegos en HA) Actualice el segundo par de HA en cada miembro de HA.

1. (Solo actualizaciones en pares activo/pasivo) Suspenda el dispositivo activo en cada miembro activo/pasivo que actualice.
 1. Cambie el contexto al cortafuegos activo.
 2. En el widget de alta disponibilidad en el **Dashboard (Panel)**, verifique que el estado del cortafuegos **Local** sea **Active (Activo)** y el **Peer** sea **Passive (Pasivo)**.
 3. Seleccione **Device (Dispositivo) > High Availability (Alta disponibilidad) > Operational Commands (Comandos operativos) > Suspend local device (Suspender dispositivo local)**.
 4. Vuelva al widget de alta disponibilidad en el **Dashboard (Panel)** y verifique que el cortafuegos **Local** cambie a **Passive (Pasivo)** y que el **Peer** cambie a **Active (Activo)**.
2. Vuelva al contexto de Panorama y seleccione **Panorama > Device Deployment (Implementación del dispositivo) > Software**.
3. Haga clic en **Install (Instalar)** en la columna Action (Acción) que corresponda a los modelos de cortafuegos de los pares de HA que está actualizando.
4. En el cuadro de diálogo Deploy Software (Implementar software), seleccione todos los cortafuegos que desea actualizar. En este momento, seleccione solo los peers de los cortafuegos de HA que ya actualizó.
5. Asegúrese de que la opción **Group HA Peers (Agrupar peers de HA)** no esté seleccionada.
6. Seleccione **Reboot device after install (Reiniciar dispositivo tras la instalación)**.
7. Para comenzar la actualización, haga clic en **OK (Aceptar)**.
8. Una vez que la instalación se realiza completamente, reinicie mediante uno de los siguientes métodos:
 - Si se le pide que reinicie, haga clic en **Yes (Sí)**.
 - Si no se le solicita que reinicie, seleccione **Device (Dispositivo) > Setup (Configuración) > Operations (Operaciones)** y haga clic en **Reboot Device (Reiniciar dispositivo)**.
9. (Solo actualizaciones en miembros activo/pasivo) En la CLI del miembro que actualizó, ejecute el siguiente comando para que el cortafuegos vuelva a funcionar:
request high-availability state functional

STEP 10 | (Actualización de PAN-OS XFR solo) Actualice el primer miembro y el segundo miembro a PAN-OS XFR repitiendo [Paso 8](#) y [Paso 9](#) .

STEP 11 | Verifique la versión de contenido y de software que se ejecutan en cada cortafuegos gestionado.

1. En Panorama, seleccione **Panorama > Managed Devices (Dispositivos gestionados)**.
2. Ubique los cortafuegos y revise el contenido y las versiones de contenido y de software en la tabla.

En los cortafuegos de HA, también puede verificar que el estado de HA de cada peer sea el esperado.

STEP 12 | (Solo actualizaciones en cortafuegos de HA) Si deshabilitó la opción de preferencia en uno de sus cortafuegos de HA antes de la actualización, edite los **Election Settings (Ajustes de elección) [Device (Dispositivo) > High Availability (Alta disponibilidad)]**, vuelva a habilitar el ajuste

Preemptive (Preferente) para ese cortafuegos y haga clic en **Commit (Confirmar)** para confirmar el cambio.

Actualización de la versión de software de PAN-OS (VM-Series para NSX)

Seleccione el método de actualización que se adapte mejor a su implementación.

- [Actualización de VM-Series para NSX durante una ventana de mantenimiento](#): use esta opción para actualizar el cortafuegos VM-Series durante una ventana de mantenimiento sin cambiar la URL de OVF en la definición del servicio.
- [Actualización de VM-Series para NSX sin interrumpir el tráfico](#): use esta opción para actualizar el cortafuegos VM-Series sin interrumpir el servicio de las VM invitadas o cambiar la URL de OVF en la definición del servicio.

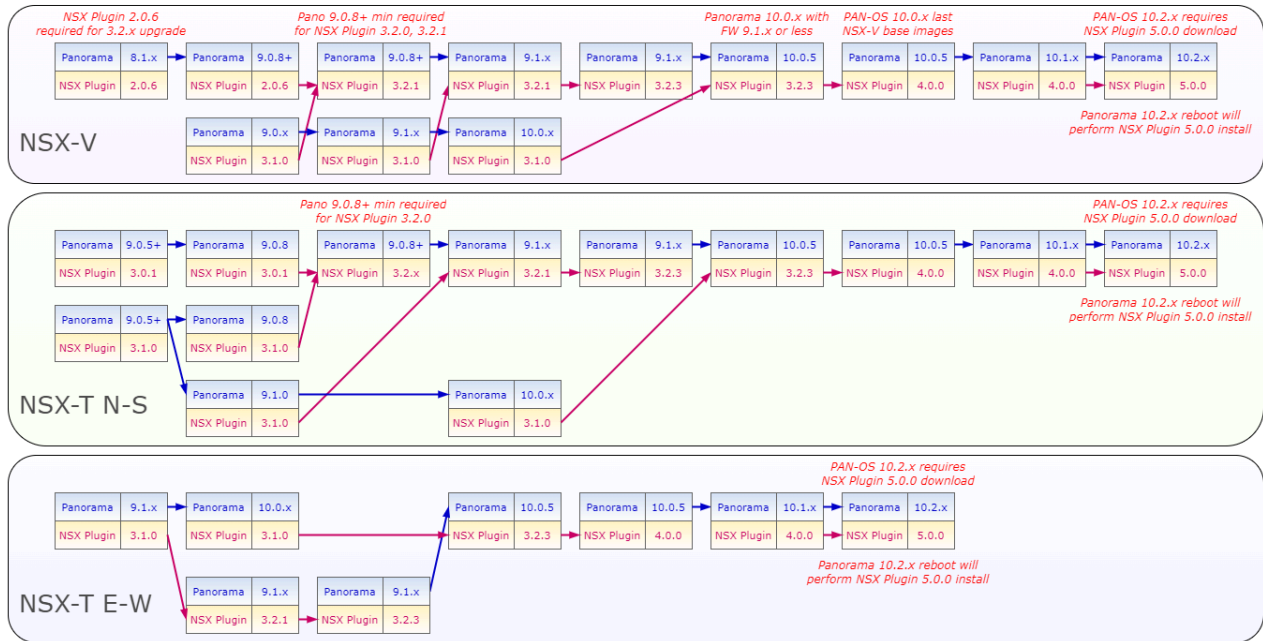
Los siguientes gráficos muestran las combinaciones admitidas actualmente de Panorama y el complemento Panorama para VMware NSX, así como las rutas de actualización que debe seguir para actualizar correctamente.

- Cada cuadro a continuación representa una combinación compatible.
- Al actualizar el complemento de Panorama para NSX o Panorama en un par de HA, actualice primero el par pasivo de Panorama, seguido del par de HA activo.

Antes de actualizar su implementación de VM-Series para VMware NSX, revise las rutas de actualización que se muestran a continuación para comprender los pasos de actualización para llegar a la combinación del complemento y PAN-OS que mejor se adapte a su entorno.

Panorama and PAN NSX Plugin Upgrade Paths for NSX-V, NSX-T N-S, NSX-T E-W

- IMPORTANT! PAN-OS 8.1.x and 9.0.x are EOL (they are illustrated for reference only)
- For Panorama HA and NSX Plugin deployments: upgrade HA Passive first, then HA Active



Actualización de la serie VM para NSX durante una ventana de mantenimiento

Para el cortafuegos VM-Series edición NSX, use Panorama para actualizar la versión de software en los cortafuegos.

STEP 1 | Revise las [rutas de actualización](#) de VM-Series para VMware NSX.

STEP 2 | Asigne recursos de hardware adicionales al cortafuegos VM-Series.

Compruebe que haya suficientes recursos de hardware disponibles para el cortafuegos VM-Series. Consulte los [Requisitos del sistema VM-Series](#) para ver los nuevos requisitos de recursos para cada modelo VM-Series. Asigne recursos de hardware adicionales antes de continuar con el proceso de actualización. El proceso para asignar recursos de hardware adicionales varía según el hipervisor.

STEP 3 | Guarde una copia de seguridad del archivo de configuración actual en cada cortafuegos gestionado que quiera actualizar.



Aunque el cortafuegos creará automáticamente una copia de seguridad de la configuración, se recomienda crear una copia de seguridad antes de actualizar y almacenarla externamente.

1. Seleccione **Device (Dispositivo) > Setup (Configuración) > Operations (Operaciones)** y haga clic en **Export Panorama and devices config bundle (Exportar Panorama y lote de configuración de dispositivos)**. Esta opción se utiliza para generar manualmente y exportar la versión más reciente de la copia de seguridad de configuración de Panorama y de los dispositivos gestionados.
2. Guarde el archivo exportado en una ubicación externa al cortafuegos. Puede usar esta copia de seguridad para restaurar la configuración si tiene problemas con la actualización.

STEP 4 | Consulte las notas de la versión para comprobar la versión de la publicación de contenido necesaria para la versión de PAN-OS.

Los cortafuegos que vaya a actualizar deberán estar ejecutando la versión de publicación de contenido necesaria para la versión de PAN-OS.

1. Seleccione **Panorama > Device Deployment (Implementación del dispositivo) > Dynamic Updates (Actualizaciones dinámicas)**.
2. Compruebe las actualizaciones más recientes. Haga clic en **Check Now (Comprobar ahora)** (ubicado en la esquina inferior izquierda de la ventana) para buscar las actualizaciones más recientes. El enlace de la columna **Action (Acción)** indica si una actualización está disponible. Si una versión está disponible, se muestra el enlace **Download (Descargar)**.
3. Haga clic en **Download (Descargar)** para descargar una versión seleccionada. Tras descargarlo correctamente, el enlace en la columna **Action (Acción)** cambia de **Download (Descargar)** a **Install (Instalar)**.
4. Haga clic en **Install (Instalar)** y seleccione los dispositivos en los que desee instalar la actualización. Cuando se complete la instalación, aparecerá una marca de verificación en la columna **Currently Installed (Instalado actualmente)**.

STEP 5 | Implemente las actualizaciones de software en los cortafuegos seleccionados.



*Si tiene dispositivos configurados en HA, asegúrese de borrar la casilla de verificación **Group HA Peers (Agrupar peers de HA)** y actualice cada peer de HA por separado.*

1. Seleccione **Panorama > Device Deployment (Implementación del dispositivo) > Software**.
2. Compruebe las actualizaciones más recientes. Haga clic en **Check Now (Comprobar ahora)** (ubicado en la esquina inferior izquierda de la ventana) para comprobar las actualizaciones más recientes. El enlace de la columna **Action (Acción)** indica si una actualización está disponible.
3. Revise el **File Name (Nombre del archivo)** y haga clic en **Download (Descargar)**. Verifique que las versiones de software que ha descargado coinciden con los modelos de cortafuegos

implementados en su red. Tras descargarlo correctamente, el enlace en la columna **Action (Acción)** cambia de **Download (Descargar)** a **Install (Instalar)**.

4. Haga clic en **Install (Instalar)** y seleccione los dispositivos en los que desee instalar la versión de software.
5. Seleccione **Reboot device after install (Reiniciar dispositivo tras instalar)** y haga clic en **OK (Aceptar)**.
6. Si tiene dispositivos configurados en HA, borre la casilla de verificación **Group HA Peers (Agrupar peers de HA)** y actualice cada peer de HA por separado.

STEP 6 | Verifique la versión de actualización de contenido y de software que se ejecutan en cada dispositivo gestionado.

1. Seleccione **Panorama > Managed Devices (Dispositivos gestionados)**.
2. Ubique los dispositivos y revise el contenido y las versiones de contenido y de software en la tabla.

Actualización de VM-Series para NSX sin interrumpir el tráfico

Use el siguiente procedimiento para actualizar la versión de PAN-OS de los cortafuegos VM-Series en su entorno de VMware NSX. Este procedimiento le permite realizar la actualización de PAN-OS sin interrumpir el tráfico migrando las VM a diferentes hosts ESXi.

STEP 1 | Revise las [rutas de actualización](#) de VM-Series para VMware NSX.

STEP 2 | Guarde una copia de seguridad del archivo de configuración actual en cada cortafuegos gestionado que quiera actualizar.



Aunque el cortafuegos creará automáticamente una copia de seguridad de la configuración, se recomienda crear una copia de seguridad antes de actualizar y almacenarla externamente.

1. Seleccione **Device (Dispositivo) > Setup (Configuración) > Operations (Operaciones)** y haga clic en **Export Panorama and devices config bundle (Exportar Panorama y lote de configuración de dispositivos)**. Esta opción se utiliza para generar manualmente y exportar la versión más reciente de la copia de seguridad de configuración de Panorama y de los dispositivos gestionados.
2. Guarde el archivo exportado en una ubicación externa al cortafuegos. Puede usar esta copia de seguridad para restaurar la configuración si tiene problemas con la actualización.

STEP 3 | Consulte las notas de la versión para comprobar la versión de la publicación de contenido necesaria para la versión de PAN-OS.

Los cortafuegos que vaya a actualizar deberán estar ejecutando la versión de publicación de contenido necesaria para la versión de PAN-OS.

1. Seleccione **Panorama > Device Deployment (Implementación del dispositivo) > Dynamic Updates (Actualizaciones dinámicas)**.
2. Compruebe las actualizaciones más recientes. Haga clic en **Check Now (Comprobar ahora)** (ubicado en la esquina inferior izquierda de la ventana) para buscar las actualizaciones más

recientes. El enlace de la columna Action (Acción) indica si una actualización está disponible. Si una versión está disponible, se muestra el enlace **Download (Descargar)**.

3. Haga clic en **Download (Descargar)** para descargar una versión seleccionada. Tras descargarlo correctamente, el enlace en la columna **Action (Acción)** cambia de **Download (Descargar)** a **Install (Instalar)**.
4. Haga clic en **Install (Instalar)** y seleccione los dispositivos en los que desee instalar la actualización. Cuando se complete la instalación, aparecerá una marca de verificación en la columna **Currently Installed (Instalado actualmente)**.

STEP 4 | Descargue la imagen de PAN-OS en todos los cortafuegos VM-Series en el clúster.

1. Inicie sesión en Panorama.
2. Seleccione **Panorama > Device Deployment (Implementación del dispositivo) > Software**.
3. Haga clic en **Refresh (Actualizar)** para ver la versión de software más reciente; asimismo, revise **Release Notes (Notas de versión)** para ver una descripción de los cambios de una versión y la ruta de migración para instalar el software.
4. Haga clic en **Download (Descargar)** para recuperar el software y, a continuación, haga clic en **Install (Instalar)**.



No reinicie el cortafuegos VM-Series después de instalar la nueva imagen de software.

5. Seleccione los dispositivos gestionados que se actualizarán.
6. Desmarque la casilla de verificación **Reboot device after install (Reiniciar dispositivo tras instalar)**.

☐ Upload only to device (do not install) ☐ Reboot device after install ☐ Group HA Peers ☐ Filter Selected (0)

OK Cancel

7. Haga clic en **OK (Aceptar)**.

STEP 5 | Actualice el cortafuegos VM-Series en el primer host ESXi en el clúster.

1. Inicie sesión en vCenter.
2. Seleccione **Hosts and Clusters (Hosts y clústeres)**.
3. Haga clic derecho sobre el host y seleccione **Maintenance Mode (Modo de mantenimiento) > Enter Maintenance Mode (Introducir modo de mantenimiento)**.
4. Migre (automática o manualmente) todas las VM, excepto el cortafuegos VM-Series, fuera del host.
5. Desactive el cortafuegos VM-Series. Esto debe suceder automáticamente tras introducir el modo de mantenimiento en el host.
6. (Opcional) Asigne CPU o memoria adicional al cortafuegos VM-Series antes de continuar con el proceso de actualización.

Compruebe que haya suficientes recursos de hardware disponibles para el cortafuegos VM-Series. Consulte los [modelos VM-Series](#) para ver los nuevos requisitos de recursos para cada modelo VM-Series.

7. Haga clic derecho sobre el host y seleccione **Maintenance Mode (Modo de mantenimiento) > Exit Maintenance Mode (Salir del modo de mantenimiento)**. Salir del modo de mantenimiento causa que el gestor de agentes de ESX (ESX Agent Manager, EAM) de NSX encienda el cortafuegos VM-Series. El cortafuegos se reinicia con la nueva versión de PAN-OS.
8. Migre (automática o manualmente) todas las VM al host original.

STEP 6 | Repita este proceso para cada cortafuegos VM-Series en cada host ESXi.

STEP 7 | Verifique la versión de actualización de contenido y de software que se ejecutan en cada dispositivo gestionado.

1. Seleccione **Panorama > Managed Devices (Dispositivos gestionados)**.
2. Ubique los dispositivos y revise el contenido y las versiones de contenido y de software en la tabla.

Actualización del modelo VM-Series

El proceso de licencia del cortafuegos de la serie usa la UUID y la Id. de CPU para generar un número de serie único para cada cortafuegos VM-Series. Así, cuando genera una licencia, esta se asigna a una instancia específica del cortafuegos VM-Series y no puede modificarse.

Use las instrucciones de esta sección si está:

- Migrando desde una licencia de evaluación a otra de producción.
- Actualizando el modelo para permitir una mayor capacidad. Por ejemplo, si desea actualizar del VM-100 al modelo VM-300.



- *Actualización de la capacidad, que reinicia algunos procesos críticos en el cortafuegos. Se recomienda una configuración HA para minimizar la interrupción del servicio; para actualizar la capacidad en un par de HA, consulte [Actualización del modelo VM-Series en un par de HA](#).*
- *En una implementación de nube pública o privada, si su cortafuegos tiene licencia con la opción BYOL, debe [desactivar su máquina virtual \(VM\)](#) antes de cambiar el tipo de instancia o el tipo de VM. La actualización del modelo o la instancia cambia el UUID y el ID de la CPU, por lo que debe aplicar la licencia cuando el .*

STEP 1 | Asigne recursos de hardware adicionales al cortafuegos VM-Series.

Antes de iniciar la actualización de capacidad, debe comprobar que haya suficientes recursos de hardware disponibles para el cortafuegos VM-Series para asumir la nueva capacidad. El proceso para asignar recursos de hardware adicionales varía según el hipervisor.

Para comprobar los requisitos de hardware para su nuevo modelo VM-Series, consulte [Modelos VM-series](#).

Aunque la actualización de capacidad no requiere que reinicie el cortafuegos VM-Series, debe apagar la máquina virtual para cambiar la asignación de hardware.

STEP 2 | Recupere la clave de API de la licencia del portal de [Servicio de atención al cliente](#).

1. Inicie sesión en el portal de atención al cliente.



Asegúrese de usar la misma cuenta que utilizó para registrar la licencia inicial.

2. En el menú de la izquierda, seleccione **Assets (Activos) > API Key Management (Gestión de clave de API)**.
3. Copie la clave de API.



STEP 3 | En el cortafuegos, use la CLI para instalar la clave API copiada en el paso anterior.

```
request license api-key set key <key>
```

STEP 4 | (Si tiene acceso a Internet) Habilite el cortafuegos para **Verify Update Server identity (Verificar la identidad del servidor de actualización)** en **Device (Dispositivo) > Setup (Configuración) > Service (Servicio)**.

STEP 5 | Haga clic en **Commit (Confirmar)** para compilar los cambios. Asegúrese de que tiene un usuario configurado localmente en el cortafuegos. Es posible que los usuarios enviados de Panorama no estén disponibles después de la desactivación si la configuración supera el límite de objetos PA-VM sin licencia.

STEP 6 | Actualice la capacidad.

Seleccione **Device (Dispositivo) > Licenses (Licencias) > Upgrade VM Capacity (Actualizar capacidad de VM)** y luego active sus licencias y suscripciones de alguna de las siguientes maneras:

- **(internet) Recuperar claves de licencia del servidor de licencias:** use esta opción si ha activado su licencia en el portal del [Servicio de atención al cliente](#).
- **(internet) Usar un código de autorización:** Use esta opción para actualizar la capacidad de la VM-Series usando un código de autorización para licencias que no han sido previamente activadas en el portal de asistencia técnica. Cuando se le indique, introduzca el **Authorization Code (Código de autorización)** y haga clic en **OK (Aceptar)**.
- **(sin internet) Cargar manualmente la clave de licencia:** use esta opción si su cortafuegos no tiene conexión a internet y no puede conectarse al portal del [Servicio de atención al cliente](#) de Palo Alto Networks. Desde un ordenador con acceso a Internet, inicie sesión en el CSP, descargue un archivo de clave de licencia, transfíralo a un ordenador en la misma red que el cortafuegos y cárguelo en el cortafuegos.

STEP 7 | Compruebe que su cortafuegos tiene licencia.

En la página **Device (Dispositivo) > Licenses (Licencias)** compruebe que la licencia se haya activado correctamente.

Actualización del modelo VM-Series en un par de HA

La actualización del cortafuegos VM-Series le permite aumentar la capacidad en el cortafuegos. La capacidad se define por el número de sesiones, reglas, zonas de seguridad, objetos de dirección, túneles VPN de IPSec y túneles VPN de SSL que el cortafuegos VM-Series está optimizado para gestionar. Cuando aplica una licencia con nueva capacidad en el cortafuegos VM-Series, el número de modelo y las capacidades asociadas se implementan al cortafuegos.



Compruebe los [Requisitos del sistema para VM-Series](#) para el modelo de cortafuegos antes de actualizar. Si su cortafuegos tiene menos de 5,5 GB de memoria, la capacidad (número de sesiones, reglas, zonas de seguridad, objetos de direcciones, etc.) en el cortafuegos estará limitada a la del VM-50 Lite.

Este proceso es similar al de actualizar un par de cortafuegos basados en hardware que están en una configuración de HA. Durante el proceso de actualización de la capacidad, la sincronización de la sesión continúa, si esta función está habilitada. Para evitar el estado de inactividad cuando actualiza cortafuegos de alta disponibilidad (high availability, HA), actualice un peer de HA a la vez.



No realice cambios a la configuración de los cortafuegos durante el proceso de actualización. Durante el proceso de actualización, la sincronización de configuración se desactiva automáticamente cuando se detecta una incoherencia en la capacidad y luego se vuelve a habilitar cuando ambos pares de HA tienen licencias de capacidad coincidentes.

Si los cortafuegos en el pareja de HA tienen diferentes versiones principales de software (como 9.1 y 9.0) y capacidades diferentes, ambos dispositivos entrarán en el estado de HA suspendido. Por lo tanto, se recomienda que se asegure de que ambos cortafuegos estén ejecutando la misma versión de PAN-OS antes de actualizar la capacidad.

STEP 1 | Actualice la licencia de capacidad en el cortafuegos pasivo.

Siga el procedimiento para [Actualizar el modelo VM-Series](#).

El nuevo modelo VM-Series se muestra en el panel después de que algunos procesos se reinicien en este par pasivo. Este par actualizado es ahora en un [estado no funcional](#) debido a la falta de coincidencia de capacidad con su par activo.

Si ha habilitado la sincronización de sesiones, compruebe que las sesiones se sincronizan entre pares de alta disponibilidad antes de continuar con el siguiente paso. Para verificar la sincronización de la sesión, ejecute el comando **show high-availability interface ha2** y asegúrese de que los contadores de la interfaz de hardware en la tabla de la CPU aumentan de la siguiente forma:

- En una configuración activa/pasiva, solo el par activo muestra los paquetes transmitidos; el par pasivo mostrará solo los paquetes recibidos.

Si habilitó la conexión persistente de HA2, los contadores de la interfaz de hardware en el par pasivo mostrarán los paquetes de transmisión y recepción. Esto ocurre porque HA2 keep-alive es bidireccional, lo que significa que ambos peers transmiten paquetes de HA2 keep-alive.

- En una configuración activo/activo, verá paquetes recibidos y paquetes transmitidos de ambos peers.

STEP 2 | Actualice la licencia de capacidad en el cortafuegos activo.

Sigue el procedimiento para la [Actualización del modelo VM-Series](#).

El nuevo modelo VM-Series se muestra en el panel después de reiniciar los procesos críticos. El cortafuegos pasivo se activa y este peer (cortafuegos previamente activo) pasa del estado inicial a convertirse en el peer pasivo en el par de HA.

Cambio a versión posterior del cortafuegos VM-Series

Use el siguiente flujo de trabajo para restaurar la configuración que se estaba ejecutando antes de actualizar a una versión de características diferente. Cualquier cambio realizado desde la actualización se perderá. Por lo tanto, es importante hacer una copia de seguridad de su configuración actual para que pueda restaurar esos cambios cuando vuelva a la versión más reciente.

Utilice el siguiente procedimiento para cambiar a una versión anterior.

STEP 1 | Guarde una copia de seguridad del archivo de configuración actual.



Aunque el cortafuegos crea automáticamente una copia de seguridad de la configuración, se recomienda crear una copia de seguridad antes de actualizar y almacenarla externamente.

1. **Export named configuration snapshot (Exportar instantánea de configuración con nombre) (Device (Dispositivo) > Setup (Configuración) > Operations (Operaciones)).**
2. Seleccione el archivo XML que contiene su configuración en uso (por ejemplo, **running-config.xml**) y haga clic en **OK (Aceptar)** para exportar el archivo de configuración.
3. Guarde el archivo exportado en una ubicación externa al cortafuegos. Puede usar esta copia de seguridad para restaurar la configuración si tiene problemas con el cambio a la versión anterior.

STEP 2 | Instale la imagen de la versión anterior.



Las versiones de autoguardado se crean cuando actualiza a una nueva versión.

1. **Check Now (Verificar ahora) [Device (Dispositivo) > Software]** para ver las imágenes disponibles.
2. Localice la imagen a la que desea volver. Si la imagen aún no se ha descargado, entonces seleccione **Download (Descargar)** imagen..
3. Una vez completada la descarga, debe **Install (Instalar)** la imagen.
4. **Select a Config File for Downgrading (Seleccionar un archivo de configuración para cambiar a versión anterior)**, que el cortafuegos cargará después de reiniciar el dispositivo. En la mayoría de los casos, debe seleccionar la configuración que se guardó automáticamente cuando actualizó desde la versión a la que ahora está volviendo. Por ejemplo, si está ejecutando PAN-OS 9.1 y está cambiando a PAN-OS 9.0.3, seleccione **autosave-9.0.3**.
5. Una vez que la instalación se realiza completamente , reinicie mediante uno de los siguientes métodos:
 - Si se le pide que reinicie, haga clic en **Yes (Sí)**.
 - Si no se le solicita reiniciar, vaya a Operaciones del dispositivo [**Device (Dispositivo) > Setup (Configuración) > Operations (Operaciones)**] y seleccione **Reboot Device (Reiniciar dispositivo)** .

Cambio complementos de Panorama a versiones posteriores

- > Consideraciones sobre el cambio a versiones anteriores/posteriores de complementos de Panorama
- > Actualice el complemento de DLP empresarial
- > Actualización del complemento Panorama Interconnect
- > Actualización del complemento de SD-WAN

Consideraciones sobre el cambio a versiones anteriores/posteriores de complementos de Panorama

En la siguiente tabla, se muestran las nuevas funciones que tienen un impacto de actualización o degradación. Asegúrese de comprender las consideraciones de cambio a una versión anterior/posterior antes de hacerlo desde una versión PAN-OS 11.0. Para obtener más información sobre las versiones de PAN-OS 11.0, consulte las [Notas de la versión de PAN-OS 11.0](#).

Table 1: Consideraciones sobre el cambio a versiones anteriores/posteriores de complementos de Panorama

Función	Consideraciones de actualización	Consideraciones de degradación
Complementos de Panorama	Antes de actualizar a PAN-OS 11.0, debe descargar la versión del complemento Panorama compatible con PAN-OS 11.0 para todos los complementos instalados en Panorama. Esto es necesario para actualizar con éxito a PAN-OS 11.0. Consulte la Matriz de compatibilidad para obtener más información.	Para cambiar a una versión anterior de PAN-OS 11.0, debe descargar la versión del complemento Panorama compatible con PAN-OS 10.2 y versiones anteriores para todos los complementos instalados en Panorama. Consulte la Matriz de compatibilidad de complementos de Panorama para obtener más información.
<ul style="list-style-type: none"> Complemento de AWS Complemento de Azure Complemento de Kubernetes Complemento de licencia de cortafuegos de software Complemento PAN-OS SD-WAN Complemento convertidor de firmas IPS Complemento de ZTP Complemento de DLP empresarial Complemento de Openconfig Complemento de GCP Complemento de Cisco ACI Complemento de Nutanix Complemento de VCenter 	<p>(DLP empresarial) Después de actualizar Panorama a PAN-OS 10.2, debe instalar la versión 8520 de publicación de contenido de aplicaciones y amenazas en todos los cortafuegos gestionados que ejecutan PAN-OS 11.0 o una versión anterior. Esto es necesario para enviar correctamente los cambios de configuración a los cortafuegos gestionados que aprovechan DLP empresarial que no fue actualizado a PAN-OS 10.2.</p> <p>(DLP empresarial) Al cargar una copia de seguridad de la configuración de Panorama que contiene la configuración de DLP empresarial compartida, se elimina el filtro de exclusión de aplicaciones compartidas necesario para analizar el tráfico no basado en archivos.</p>	

Función	Consideraciones de actualización	Consideraciones de degradación
	<p>(SD-WAN) El complemento Panorama para SD-WAN 2.2 y versiones anteriores no son compatibles con PAN-OS 11.0.</p> <p>La actualización de un servidor de gestión de Panorama a PAN-OS 11.0 cuando está instalado el complemento de Panorama para SD-WAN 2.2 o una versión anterior hace que el complemento de SD-WAN se oculte en la interfaz web de Panorama o que se elimine la configuración de SD-WAN. En ambos casos, no se puede instalar una nueva versión del complemento SD-WAN ni desinstalar el complemento SD-WAN.</p>	
PAN-OS SD-WAN	<p>Después de actualizar correctamente Panorama a la versión posterior PAN-OS 11.0 y el complemento de Panorama de SD-WAN versión 2.0.0 a SD-WAN versión 3.0.0, debe borrar la caché de SD-WAN en Panorama solo para implementaciones SD-WAN existentes.</p> <p>Al borrar la memoria caché de SD-WAN, no se elimina ninguna configuración SD-WAN existente, sino que se eliminan las convenciones de nomenclatura de direcciones IP, túneles y puertas de enlace para el nuevo formato incorporado en el complemento de Panorama para SD-WAN versión 3.0.</p> <p>En el caso de nuevas implementaciones de SD-WAN, no es necesario borrar la memoria caché de SD-WAN en Panorama si instala el complemento de Panorama para SD-WAN versión 3.0 en Panorama después</p>	Ninguno.

Función	Consideraciones de actualización	Consideraciones de degradación
	<p>de cambiar a la versión posterior PAN-OS 11.0.</p> <ol style="list-style-type: none">1. Inicio de sesión en la CLI de Panorama.2. Borre la memoria caché de SD-WAN en Panorama. <pre data-bbox="623 457 1003 613">admin> debug plugins sd_wan drop-config-cache all</pre>	

Actualice el complemento de DLP empresarial

Instale y configure el complemento de prevención de pérdida de datos (DLP) empresarial en el servidor de gestión Panorama™.

Consulte la [Matriz de compatibilidad de complementos de Panorama de Palo Alto Networks](#) y revise la versión mínima requerida de PAN-OS para la versión del complemento de DLP empresarial de destino.

STEP 1 | [Inicie sesión en la interfaz web de Panorama.](#)

STEP 2 | Actualice la versión del complemento de DLP empresarial en Panorama.

Si Panorama tiene una configuración de alta disponibilidad (HA, High Availability), repita este pasos en el peer de HA de Panorama.

1. Seleccione **Panorama > Plugins (Complementos)** y **Check Now (Comprobar ahora)** para buscar la versión más reciente del complemento **DLP**.
2. **Descargue e instale** la versión más reciente del complemento DLP empresarial.
3. Después de que la nueva versión del complemento se instale correctamente, vea el **Panel** de Panorama y verifique en el widget de información general que la versión del **Plugin DLP (Complemento DLP)** muestre la versión del complemento DLP empresarial a la que actualizó.

STEP 3 | [\(Actualización a 4.0.0 solamente\) Edite la configuración de filtrado de datos de DLP empresarial](#) para reducir el **tamaño máximo de archivo** a 20 MB o menos.

Esto es necesario cuando se actualiza desde el complemento Panorama para DLP empresarial 3.0.3 o versiones posteriores a DLP empresarial 4.0.0, ya que esta versión del complemento no admite una [inspección de archivos de gran tamaño](#).

Actualización del complemento Panorama Interconnect

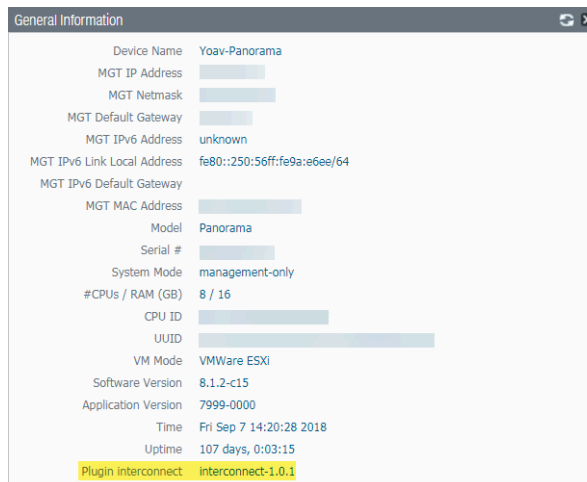
Use el siguiente procedimiento para actualizar el complemento Panorama™ Interconnect en el controlador Panorama y los nodos de Panorama. Cuando actualiza el complemento de Panorama Interconnect, debe actualizar el controlador Panorama antes de actualizar los nodos de Panorama a la misma versión de complemento que el controlador. La nueva versión de complemento que descargue e instale en el nodo de Panorama debe ser la misma versión de complemento que instaló en el controlador Panorama para garantizar que la versión del complemento en el controlador Panorama y los nodos de Panorama seleccionados permanezcan sincronizados.

Si es la primera vez que instala el complemento, consulte [Set up the Panorama Interconnect Plugin \(Configurar el complemento de interconexión de Panorama\)](#).

STEP 1 | Inicie sesión en la interfaz web de Panorama del controlador Panorama.

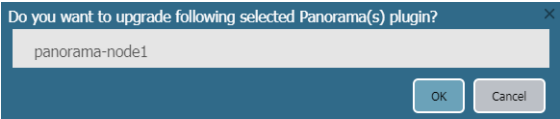
STEP 2 | Actualice el complemento Panorama Interconnect en el controlador Panorama.

1. Seleccione **Panorama > Plugins (Complementos)** y busque **Interconnect**.
2. Haga clic en **Download (Descargar)** y en **Install (Instalar)** para descargar e instalar la nueva versión de complemento Interconnect. Se muestra un mensaje que le notifica después de que se complete la instalación.
3. Verifique que el **Dashboard (Panel)** muestre la versión de complemento Interconnect instalada recientemente.



STEP 3 | Actualice el complemento Panorama Interconnect en el nodo de Panorama.

1. Seleccione **Panorama > Interconnect > Panorama Nodes (Nodos de Panorama)**, seleccione uno o más nodos de Panorama Nodes y haga clic en **Upgrade Plugin (Actualizar complemento)**.
2. Verifique los nodos de Panorama seleccionados y haga clic en **OK (Aceptar)** para iniciar la actualización del complemento.



3. Espere hasta que el trabajo de actualización de complemento este **Completed**. Haga clic en **Panorama > Interconnect > Tasks (Tareas)** para ver el progreso del trabajo.

	Admin ID	Job ID	Type	Start Time	End Time	Status
	admin	05624D4E-A29E-432D-AE07-328806F50E6B	PLUGIN-UPGRADE	6/19/2018, 10:57:09 AM	6/19/2018, 10:57:20 AM	Completed

4. Después de que se complete correctamente la actualización, seleccione **Panorama > Interconnect > Panorama Nodes (Nodos de Panorama)** para verificar que la versión de **Plugin (Complemento)** sea adecuada para los nodos de Panorama seleccionados.

<input type="checkbox"/>	Name	IP Address	Plugin	Software	Apps and Threats
<input type="checkbox"/>	panorama-node1		interconnect-1.0.1	8.1.2-c15	8021-4730

Actualización del complemento de SD-WAN

Actualice la versión del complemento de SD-WAN instalada en su servidor de gestión Panorama™ y cortafuegos que aprovechan SD-WAN.

Consulte la [Matriz de compatibilidad de complementos de Panorama de Palo Alto Networks](#) y revise la versión mínima requerida de PAN-OS para la versión del complemento SD-WAN de destino.

STEP 1 | Inicie sesión en la interfaz web de Panorama.

STEP 2 | Actualización de la versión del complemento de SD-WAN en Panorama.

Si Panorama tiene una configuración de alta disponibilidad (HA, High Availability), repita este pasos en el peer de HA de Panorama.

1. Seleccione **Panorama > Plugins (Complementos)** y **Check Now (Comprobar ahora)** para buscar la versión del complemento **sd_wan** más reciente.
2. **Descargue e instale** la última versión del complemento de SD-WAN.

STEP 3 | Después de que la nueva versión del complemento se instale correctamente, vea el **panel** Panorama y en el widget de información general verifique que el **complemento SD-WAN** muestre la versión del complemento SD-WAN a la que actualizó.

Comandos de la CLI para realizar la actualización

> Utilizar los comandos de la CLI para las tareas de cambio a versión posterior

Utilizar los comandos de la CLI para las tareas de cambio a versión posterior


Utilice los siguientes comandos de la CLI para realizar tareas de cambio a una versión posterior.

Si quiere...	Use...
Verifique las versiones actuales del cortafuegos	
<ul style="list-style-type: none">Verifique la versión actual del software y contenido del cortafuegos.	<pre>show system info</pre>
Acceda a las actualizaciones dinámicas disponibles y cambie el contenido del cortafuegos a una versión posterior	
<ul style="list-style-type: none">Verifique las versiones de contenido disponibles de las actualizaciones dinámicas directamente desde los servidores de Palo Alto Networks.	<pre>check request content upgrade</pre>
<ul style="list-style-type: none">Verifique las versiones de contenido disponibles de las actualizaciones dinámicas directamente desde el cortafuegos.	<pre>info request content upgrade</pre>
<ul style="list-style-type: none">Descargue la versión del contenido directamente al cortafuegos.	<pre>request content upgrade download <content version></pre>
<ul style="list-style-type: none">Instale la versión del contenido.	<pre>request content upgrade install <content version></pre>

Si quiere...	Use...
Acceda a las versiones de software disponibles y cambie el cortafuegos a una versión posterior	
<ul style="list-style-type: none"> Verifique las versiones de software disponibles para descargar. 	<pre>info request system software</pre>
<ul style="list-style-type: none"> Verifique las versiones disponibles cargadas en el cortafuegos. 	<pre>check request system software</pre>
<ul style="list-style-type: none"> Descargue una versión específica del software. 	<pre>download version <version> request system software</pre>
<ul style="list-style-type: none"> Verifique el estado de un trabajo de descarga específico. 	<pre>show job id <jobid></pre>
<ul style="list-style-type: none"> Instale el software descargado. 	<pre>install version 10.1.0 request system software</pre>
<ul style="list-style-type: none"> Reiniciar el cortafuegos. 	<pre>request restart system</pre>

Si quiere...	Use...

Acceda a los parches de software disponibles para el cortafuegos:

 *La función de parche se ofrece actualmente en modo de vista previa. El soporte completo no está disponible con esta funcionalidad.*

Si quiere...	Use...
<ul style="list-style-type: none">Verifique los parches de software disponibles para descargar.	<pre>request system patch c heck</pre>
<ul style="list-style-type: none">Verifique los parches disponibles para la versión de cortafuegos actualmente instalada.	<pre>request system patch i nfo</pre>
<ul style="list-style-type: none">Descargue una versión de parche específica.	<pre>request system patch do wnload version <version></pre>
<ul style="list-style-type: none">Consulte información más detallada para una versión de parche específica.	<pre>request system patch in fo version <version></pre>
<ul style="list-style-type: none">Instale el parche descargado.	<pre>request system patch in stall version <version></pre>

Si quiere...	Use...
<ul style="list-style-type: none">Aplicar el parche instalado.	<pre>request system patch apply</pre>

API para realizar la actualización

> Usar la API para tareas de actualización

Usar la API para tareas de actualización

Utilice los siguientes comandos de la CLI para realizar tareas de cambio a una versión posterior.

Si quiere...	Use...
Verifique las versiones actuales del cortafuegos	
<ul style="list-style-type: none">Verifique la versión actual del software y contenido del cortafuegos.	<pre>https://firewall/api/? type=op&cmd=<request><system><software><check></software></system></pre>
Acceda a las actualizaciones dinámicas disponibles y cambie el contenido del cortafuegos a una versión posterior	
<ul style="list-style-type: none">Verifique las versiones de contenido disponibles de las actualizaciones dinámicas directamente desde los servidores de Palo Alto Networks.	<pre>https://firewall/api/? type=op&cmd=<request><content><upgrade><check></upgrade></content></request></pre>
<ul style="list-style-type: none">Verifique las versiones de contenido disponibles de las actualizaciones dinámicas directamente desde el cortafuegos.	<pre>https://firewall/api/? type=op&cmd=<request><content><upgrade><info></upgrade></content></request></pre>
<ul style="list-style-type: none">Descargue la versión de contenido más reciente directamente en el cortafuegos.	<pre>https://firewall/api/? type=op&cmd=<request><content><upgrade><download></download></upgrade></content></request></pre>
<ul style="list-style-type: none">Descargue la versión de contenido específica directamente en el cortafuegos.	<pre>https://firewall/api/? type=op&cmd=<request><content><upgrade><download><file></download></upgrade></content></request></pre>
<ul style="list-style-type: none">Instale la versión del contenido.	<pre>https://firewall/api/? type=op&cmd=<request><content><upgrade><install><content version></version></install></upgrade></content></request></pre>
Acceda a las versiones de software disponibles y cambie el cortafuegos a una versión posterior	
<ul style="list-style-type: none">Verifique las versiones de software disponibles para descargar.	<pre>https://firewall/api/? type=op&cmd=<request><system><software><info></pre>

Si quiere...	Use...
	<code>info></software></system></request></code>
<ul style="list-style-type: none"> Verifique las versiones disponibles cargadas en el cortafuegos. 	<code>https://firewall/api/?type=op&cmd=<request><system><software><check></software></system></request></code>
<ul style="list-style-type: none"> Descargue una versión específica del software. 	<code>https://firewall/api/?type=op&cmd=request><system><software><download></download></software></system></request></code>
<ul style="list-style-type: none"> Verifique el estado de un trabajo de descarga específico. 	<code>https://firewall/api/?type=op&cmd=<show><jobs></jobs></show></code>
<ul style="list-style-type: none"> Instale el software descargado. 	<code>https://firewall/api/?type=op&cmd=<request><system><software><install></install></software></system></request></code>
<ul style="list-style-type: none"> Reiniciar el cortafuegos. 	<code>https://firewall/api/?type=op&cmd=<request><restart><system></system></restart></request></code>

