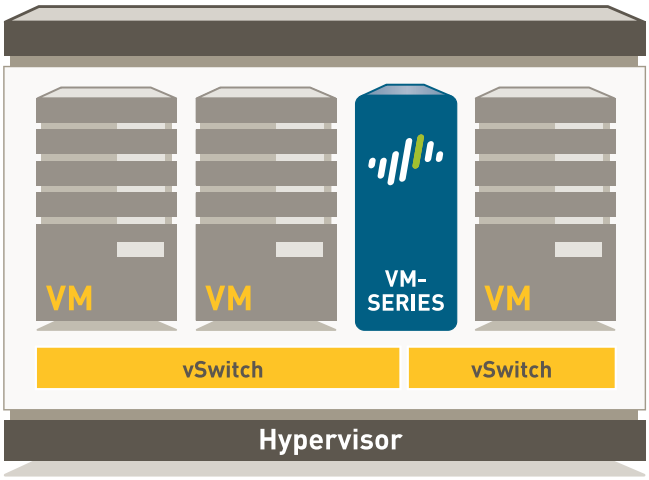
# Serie VM para KVM

## Funciones de seguridad clave:

Los cortafuegos de la serie VM de Palo Alto Networks® le ofrecen a su organización la flexibilidad necesaria para mantener servicios de seguridad de nueva generación en sus entornos de computación en la nube basados en KVM.

- Identifique y controle el tráfico que fluye en su entorno de computación en la nube basado en KVM, limite el acceso a las aplicaciones basado en usuarios y bloquee amenazas tanto conocidas como desconocidas.
- Automatice las actualizaciones de las políticas de seguridad de forma que se mantengan al día de los cambios en el entorno de computación en la nube.
- Gestione dispositivos físicos y virtuales mediante Panorama y una amplia gama de API.



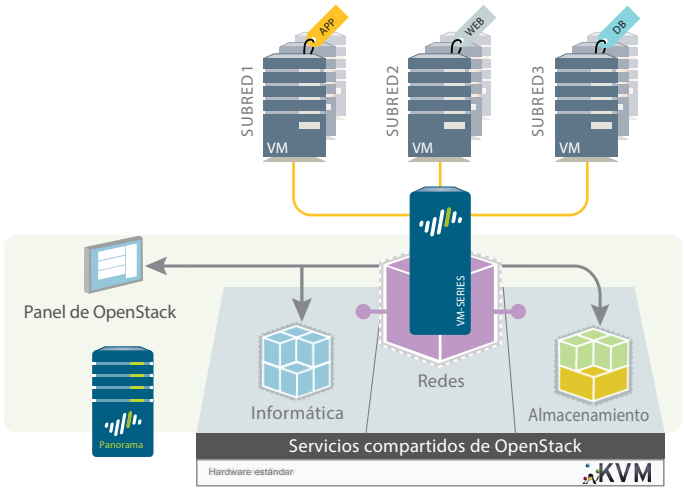

KVM (máquina virtual basada en el núcleo) constituye un hipervisor de código abierto líder que tanto las empresas como los proveedores de servicios están utilizando para implementar entornos de computación basados en la nube. KVM, junto con OpenStack, representa una solución completa basada en código abierto que le permite combinar las ventajas de reducción de costes que se logran a partir de la eficacia de la computación en la nube con las ventajas de una solución de código abierto.

Expandir la red a la nube conlleva numerosos retos, uno de los cuales es la seguridad. Entre las consideraciones de seguridad específicas se incluyen la capacidad para habilitar y controlar las aplicaciones que entran y salen de su infraestructura de nube, la prevención de las amenazas conocidas y desconocidas (en todas las aplicaciones y protocolos) y la posibilidad de garantizar que las políticas de seguridad no se quedan atrás con respecto a los cambios en la computación en la nube.

La serie VM para KVM aborda estos retos clave con el mismo cortafuegos de nueva generación y las funciones de prevención de amenazas avanzadas disponibles en nuestros dispositivos físicos. Se analiza de forma nativa todo el tráfico en un solo paso para determinar la identidad de la aplicación, su contenido y el usuario que la emplea. A continuación, la identidad del usuario, el contenido y la aplicación se utilizan como componentes integrales de su política de seguridad, lo que le permite controlar perfectamente el acceso a sus recursos de computación en la nube, así como aislar las aplicaciones esenciales para protegerlas de las amenazas conocidas y desconocidas.

paloalto networks

Para garantizar que la seguridad evoluciona a la vez que los cambios en su entorno de KVM, las funciones de automatización, como la máquina virtual (VM), la supervisión, los grupos de direcciones dinámicas y una API basada en REST, le permiten recopilar y supervisar de forma proactiva eliminaciones o adiciones de VM, y eliminaciones y cambios de atributos automáticamente. Estos datos contextuales de VM recopilados pueden introducirse directamente en las políticas de seguridad, con lo que se consigue que estas se actualicen de forma dinámica y se elimina el desfase en las políticas que puede tener lugar cuando cambian sus VM. A continuación, puede usar Panorama para gestionar de forma central toda su implementación de cortafuegos de nueva generación de Palo Alto Networks y, si se combina con el complemento de OpenStack opcional, se integrarán mejor la gestión de las políticas de seguridad y la gestión de VM.




## CASO DE USO DE LA SERIE VM PARA KVM: PUERTA DE ENLACE DEL PERÍMETRO

En el caso de las empresas que están emprendiendo la creación de su propio entorno de computación en la nube, la serie VM de KVM les permite aplicar el cortafuegos de nueva generación de Palo Alto Networks y las funciones de prevención de amenazas avanzadas al tráfico que atraviesa su perímetro de computación en la nube.

En este caso de uso, la serie VM para KVM puede implementarse como su cortafuegos de la puerta de enlace; podrá habilitar las aplicaciones que desee e inspeccionarlas en busca de amenazas conocidas y desconocidas independientemente del puerto.

El acceso a las cargas de trabajo virtualizadas se controla en función de la identidad del usuario, con lo que se añade otro nivel de protección más. A medida que se modifican o añaden nuevas cargas de trabajo, las funciones de automatización de la serie VM, las API y el complemento de OpenStack opcional le permiten actualizar de forma dinámica las políticas de seguridad. De este modo, se garantiza que se vayan actualizando en función de los cambios en la computación en la nube respectivos.

## CASO DE USO DE LA SERIE VM PARA KVM: OFERTAS PARA LOS CLIENTES DE LOS PROVEEDORES DE SERVICIOS

Los proveedores de servicios utilizan habitualmente KVM y OpenStack para adaptar de forma eficiente y rentable sus ofertas de servicios de computación en la nube para los clientes. Al tratarse de una solución de código abierto, se pueden lograr servicios diferenciados y con un elevado grado de personalización. Cuando se combina con el cortafuegos de nueva generación y las funciones de automatización de la serie VM, los proveedores de servicios pueden crear ofertas de servicios de computación en la nube muy rentables.

## RESUMEN

La serie VM para KVM permite a los proveedores de servicios y empresas por igual proteger sus entornos de computación en la nube con servicios completos de prevención de amenazas y un cortafuegos de nueva generación. El tráfico que fluye en su nube basada en KVM se identifica en función de la aplicación y, a continuación, se inspecciona en busca de amenazas informáticas conocidas y desconocidas. Las funciones de automatización y la gestión centralizada con Panorama permiten garantizar que la política de seguridad se adapte a cualquier cambio contextual que tenga lugar en su entorno de computación en la nube.

La serie VM para KVM es compatible con CentOS/RHEL y Ubuntu que admiten la computación virtual, así como el paso (passthrough) a través de SR-IOV y PCI, por lo que puede elegir cuál es la mejor forma de aplicar la potencia de procesamiento de computación en la nube.

paloalto networks
the enterprise security company™

4401 Great America Parkway
Santa Clara, CA 95054 (EE. UU.)

Central: +1.408.753.4000
Ventas: +1.866.320.4788
Asistencia: +1.866.898.9087

www.paloaltonetworks.com