

FIREWALL VIRTUAL VSRX DE JUNIPER NETWORKS PARA AMAZON WEB SERVICES

Descripción general del producto

El [cortafuegos virtual vSRX de Juniper Networks®](#) ofrece un cortafuegos virtual completo nativo de la nube para AWS, que incluye seguridad avanzada, SD-WAN segura, redes sólidas y funcionalidades automatizadas de gestión del ciclo de vida de las máquinas virtuales para [proveedores de servicios](#) y [empresas](#). Para activar una versión de prueba de vSRX para AWS, visita el [mercado de AWS](#).

Descripción del producto

Las cargas de trabajo siguen moviéndose a la nube pública, lo que presenta desafíos no solo en torno a cómo proteger los datos, sino también en torno a la protección de la comunicación entre las cargas de trabajo que se ejecutan en la nube y otras ubicaciones.

Los profesionales de redes y seguridad deben realizar un delicado acto de equilibrio, ofreciendo los beneficios de las tecnologías de nube sin socavar la seguridad de la organización. Este desafío solo puede superarse con una solución de seguridad que se mantenga al día con las amenazas en evolución, al tiempo que se adapta a la agilidad y escalabilidad de los entornos de nube, sin sacrificar la fiabilidad, la visibilidad y el control.

HPE Juniper Networking aborda estos desafíos de frente ampliando las funcionalidades de los galardonados firewalls de la serie SRX de Juniper Networks® como firewall virtual vSRX nativo de la nube para Amazon Web Services (AWS), lo que permite a los profesionales de la seguridad implementar y escalar la protección de cortafuegos para cargas de trabajo implementadas dentro de AWS. Este cortafuegos virtual ofrece una seguridad inigualable [de cortafuegos de última generación \(NGFW\)](#) que incluye sistema de prevención de intrusiones (IPS), protección contra malware, control de aplicaciones y detección de amenazas bajo demanda. El vSRX también admite la seguridad de las comunicaciones con WAN definida por software (SD-WAN) segura, nube privada virtual de tránsito (VPC) y LAN definida por software (SD-LAN) para una segmentación segura entre cargas de trabajo.

Las capacidades de aprovisionamiento automatizado de vSRX para AWS permiten y administradores de seguridad para aprovisionar y escalar de forma rápida y eficiente la protección de cortafuegos para satisfacer las necesidades dinámicas de los entornos de nube. Al combinar el vSRX con el poder del [Director de seguridad Junos Space®](#) o la [organización de servicios Contrail®](#), los administradores pueden mejorar significativamente la configuración, la gestión y la visibilidad de las políticas en los activos físicos y virtuales desde una plataforma común y centralizada.

HPE se compromete a ayudar a los clientes a aprovechar el valor de sus inversiones existentes y a la interoperatividad en todos los [firewalls de la serie SRX](#). Además del Director de seguridad y Contrail Service Orchestration, vSRX admite OpenContrail®, así como otras soluciones de gestión de terceros. El vSRX también se puede integrar con otras herramientas de organización de la nube de última generación, como OpenStack, ya sea directamente o a través de API enriquecidas.

Además de los casos de uso de la nube pública y la virtualización tradicional, vSRX permite a los proveedores de servicios y a las empresas implementar una estructura SD-WAN segura con defensas en el extremo que se adaptan a las necesidades individuales de cualquier sitio, al tiempo que proporciona la flexibilidad para defender aplicaciones virtualizadas y orientadas a servicios dondequiera que existan en toda la red.

El Director de seguridad puede gestionar hasta 25 000 firewalls de la serie SRX, ya sean físicos, virtuales o en contenedores, desde una única instancia de gestión. Esto permite a las organizaciones utilizar una única plataforma para gestionar, automatizar y organizar la seguridad, virtualización e interconectividad de la red, desde el extremo hasta el extremo y cada nube intermedia.

Arquitectura y componentes clave

Conectividad segura

El vSRX en AWS puede proteger las comunicaciones entre cargas de trabajo que se ejecutan en diferentes nubes privadas virtuales (VPC) y/o un centro de datos local.

El cortafuegos virtual vSRX puede utilizar múltiples opciones de conectividad para conectarse de forma segura sitios, ya sean virtuales o físicos, a la estructura WAN empresarial. La conectividad segura se puede ampliar para incluir otros centros de datos que puedan alojar o necesiten comunicarse de forma segura con las cargas de trabajo en la nube.

Los centros de datos locales o colocalizados que utilizan AWS Direct Connect operan de manera similar a conectividad entre regiones dentro de AWS, mientras que los centros de datos que no utilizan Direct Connect se pueden conectar a través de Internet mediante una VPN.

SD-WAN segura

Para acceder a las aplicaciones alojadas en AWS, las sucursales tradicionalmente aprovechan las conexiones a través de las ubicaciones de campus corporativos y luego acceden a las aplicaciones en la nube de AWS. En esta situación, la SD-WAN segura se puede implementar en la sucursal y utilizar vSRX en AWS para activar una solución más optimizada para la conectividad que va directamente a AWS, evitando la necesidad de acceder a las aplicaciones de la nube a través de la red del campus.

Un vSRX implementado en AWS puede actuar como un radio o hub de SD-WAN, ofreciendo acceso seguro entre campus y sucursales y AWS directamente como parte de una implementación de SD-WAN más grande. También puede actuar como el centro SD-WAN donde proporciona acceso seguro a los recursos de nube alojados en AWS, convirtiéndose en el punto central para la división regional de Internet. Esto permite que vSRX en AWS no solo proteja las cargas de trabajo, sino que también proporcione una conectividad SD-WAN segura que se adapte a las cambiantes necesidades empresariales.

Protección de la carga de trabajo

Los cortafuegos protegen las cargas de trabajo, pero no todos los cortafuegos se crean de la misma manera. Con vSRX en AWS, los clientes pueden garantizar que las políticas se implementen de manera uniforme en toda su red, ya sea que esas cargas de trabajo operen localmente, en la nube pública o en el extremo. Los clientes que ya utilizan cortafuegos de la serie SRX en sus redes pueden extender fácilmente esas políticas a vSRX que operan en la nube pública o en otro lugar.

vSRX admite la creación e implementación de políticas de cortafuegos utilizando etiquetas de metadatos, lo que facilita la automatización de la seguridad y reduce el número de reglas necesarias durante la implementación inicial o el mantenimiento continuo. Estos metadatos proporcionan a los administradores de seguridad una mayor visibilidad al proporcionar una vista de red completa basada en las etiquetas de metadatos, lo que significa que ya no se limitan a la gestión y el filtrado de reglas basadas en direcciones IP.

Además de la aplicación de políticas, vSRX proporciona servicios de seguridad avanzados, incluidos IPS, antivirus y antimalware, para identificar y bloquear amenazas avanzadas dirigidas a cargas de trabajo alojadas en la nube de AWS.

Segmentación de la carga de trabajo

Para proteger la comunicación y garantizar la segmentación de la carga de trabajo en AWS, vSRX se puede implementar para aplicar políticas sobre qué comunicaciones se deben permitir entre segmentos de carga de trabajo. El vSRX facilita la segmentación y el control granulares de la red al aplicar políticas de seguridad a nivel de carga de trabajo virtualizada. Desde el punto de vista de la seguridad, cuanto más granular sea el nivel en el que se puede bloquear una amenaza, más eficaz será contener la propagación de la amenaza.

Servicios de seguridad avanzada

Implementar sistemas heredados no integrados construidos en torno a cortafuegos tradicionales y dispositivos y software independientes individuales ya no es suficiente para protegerse contra los sofisticados ataques actuales. HPE Advanced Security Suite permite a los usuarios implementar múltiples tecnologías para satisfacer las necesidades únicas y en evolución de las organizaciones modernas y el panorama de amenazas en constante cambio. Las actualizaciones en tiempo real garantizan que las tecnologías, políticas y otras medidas de seguridad estén siempre actualizadas.

vSRX para AWS ofrece un conjunto versátil y potente de servicios de seguridad avanzados, que incluyen IPS, protección contra malware, control de aplicaciones y seguridad de contenido.

Sistema de prevención de intrusiones

IPS en vSRX para AWS controla el acceso a las redes de TI, protegiendo los sistemas de los ataques mediante la inspección de datos y la adopción de medidas como bloquear ataques a medida que se desarrollan o crear una serie de reglas en el cortafuegos. IPS integra estrechamente las funciones de seguridad de las aplicaciones HPE con la infraestructura de red para mitigar aún más las amenazas y defenderse contra una amplia gama de ataques y vulnerabilidades.

Prevención avanzada de amenazas de Juniper

[Juniper® Advanced Threat Prevention](#) se integra con vSRX for AWS para proporcionar protección dinámica y automatizada contra malware conocido y amenazas avanzadas de día cero, lo que da como resultado respuestas casi instantáneas.

Visibilidad y control de aplicaciones con AppSecure

Juniper Networks® AppSecure es un paquete de seguridad de aplicaciones de última generación para vSRX en AWS, que ofrece visibilidad, protección, aplicación y control de amenazas. Esta función opcional ofrece una visibilidad potente y un seguimiento continuo de las aplicaciones. Con firmas abiertas, se pueden supervisar, medir y controlar conjuntos de aplicaciones únicos para alinearse estrechamente con las prioridades empresariales de la organización.

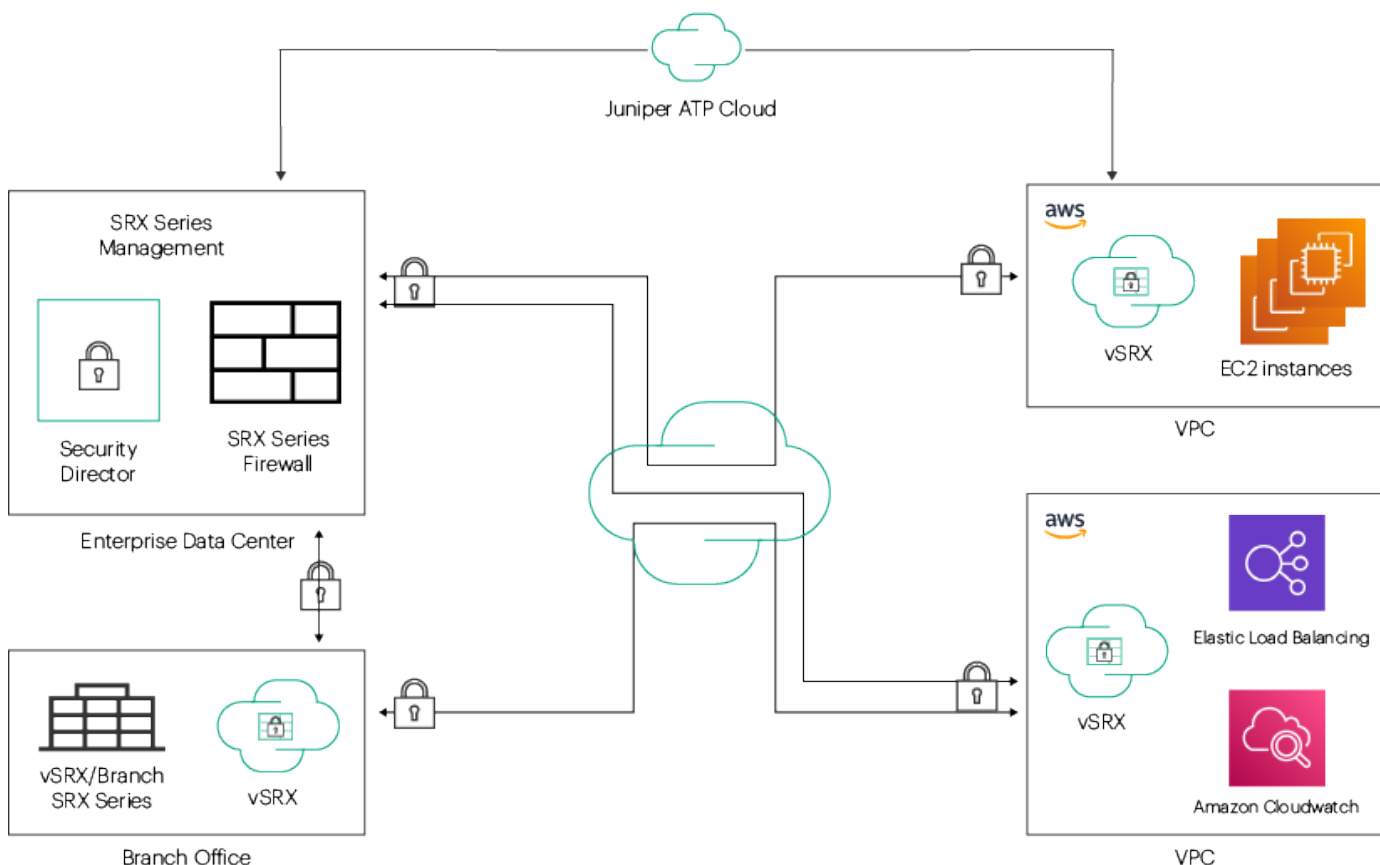


Figura 1. vSRX para proteger cargas de trabajo en la nube en AWS

Características y ventajas

Tabla 1. Características y ventajas de vSRX para AWS

Característica	Descripción de la característica	Ventaja
Hardware escalable	Te permite empezar con 2 núcleos de CPU y 4 GB de memoria y escalar hasta 36 núcleos y 93 GB de memoria	Proporciona una huella de hardware flexible y escalable para satisfacer tus necesidades de tráfico ahora y en el futuro
Políticas de cortafuegos basadas en metadatos	Permite a los administradores aprovechar el poder de la funcionalidad Dynamic Address Group en vSRX para crear intención de usuario basada en metadatos de objetos políticas de cortafuegos	Simplifica la creación de políticas y los flujos de trabajo de mantenimiento al permitir que las políticas de cortafuegos se activen o deshabiliten en función de metadatos como las etiquetas de AWS
Escalado automático	Admite implementaciones de vSRX que requieren recursos de seguridad de puesta en marcha dinámica cuando aumentan las cargas de trabajo	Aumenta la escala y el rendimiento de seguridad sin necesidad de activar manualmente instancias de vSRX adicionales
Equilibrio de carga elástico	Aumenta la capacidad de tráfico orientado a Internet mediante el equilibrio de carga de aplicaciones	Permite implementar vSRX donde se requiere una mayor capacidad para seguir el ritmo de las demandas de tráfico
Licencias flexibles	Admite tanto pago por consumo (PAYG) * como opciones bring-your-own-license (BYOL)	Proporciona opciones flexibles de licencia y compra para proteger las cargas de trabajo en AWS y la conectividad entre tu centro de datos y AWS

Seguridad del contenido

vSRX para AWS incluye seguridad de contenido integral contra malware, virus, ataques de phishing, spam y otras amenazas con las mejores funciones de antivirus, antispam, filtrado web y filtrado de contenido de su clase.

Especificaciones

Tabla 2. Métricas clave de rendimiento de vSRX en AWS

Rendimiento y capacidad ¹	vSRX en AWS			
	Tipo de instancia de AWS	c4-xLarge	c5-Large	c5n-2xLarge
Núcleos de vCPU	4	2	8	36
Memoria	7 GB	3 GB	20 GB	93 GB
Rendimiento de firewall, paquete grande (UDP)	1,2 Gbps	10 Gbps	25.5 Gbps	51.5 Gbps
Rendimiento de IPSec VPN (AES-GCM256 TCP)	630 Mbps	2 Gbps	5.9 Gbps	15.5 Gbps
Máximo de sesiones simultáneas²	2 millones	512 000	4 millones	24 millones

¹ Todos los números de rendimiento se miden en condiciones de prueba ideales utilizando herramientas de código abierto. HPE recomienda que los clientes prueben el rendimiento en su implementación de nube pública para cumplir con sus requisitos de rendimiento de seguridad específicos.² ITAA, junio de 2024.

² El máximo de sesiones simultáneas admitidas depende de la memoria asignada al vSRX. Consulta la ficha técnica de vSRX para obtener más información [juniper.net/us/en/products-services/security/srx-series/datasheets/1000489.page](https://www.juniper.net/us/en/products-services/security/srx-series/datasheets/1000489.page).

Información sobre pedidos

Para obtener más información sobre la licencia vSRX Virtual Firewall BYOL de Juniper Networks para AWS, visita juniper.net/us/en/products-services/security/srx-series/vsrx o ponte en contacto con tu representante de ventas de HPE. Para activar una versión de prueba de vSRX para AWS, visita el [mercado de AWS](#).

Los clientes que deseen comprar directamente a través de AWS Marketplace tienen dos opciones para implementar vSRX pay-as-you-go (PAYG)*, ya sea como suscripciones de una hora o de un año.

* Puede estar sujeto a mínimos o a capacidad de reserva

Acerca de HPE

HPE es líder en tecnología empresarial esencial y reúne el poder de la IA, la nube y las redes para ayudar a las organizaciones a lograr más. Como pioneros de la posibilidad, nuestra innovación y experiencia hacen avanzar la forma en que las personas viven y trabajan. Capacitamos a nuestros clientes de todos los sectores para optimizar el rendimiento operativo, transformar los datos en previsión y maximizar su impacto. Desbloquea tus ambiciones más audaces con HPE. Descubre más en [HPE.com](https://hpe.com).

Visita [HPE.com](https://hpe.com)

Tabla 3. Información de pedidos para PAYG en el mercado de AWS

Ofertas de vSRX PAYG	PAGO vSRX características
cortafuegos vSRX de última generación	<ul style="list-style-type: none">— Características principales de cortafuegos, VPN IPSec, traducción de direcciones de red (NAT), clase de servicio (CoS) y servicios de enrutamiento enriquecidos— Funciones de AppSecure que incluyen AppID, AppFW, AppQoS y AppTrack— Servicios de seguridad de contenido que incluyen IPS
cortafuegos vSRX de última generación con protección antivirus	<ul style="list-style-type: none">— Funciones de cortafuegos principales, VPN IPSec, NAT, CoS y servicios de enrutamiento enriquecidos— Funciones de AppSecure que incluyen AppID, AppFW, AppQoS y AppTrack— Servicios de seguridad de contenido que incluyen IPS, antivirus, antispam, filtrado de contenido y web

Exención de responsabilidad: Esta ficha técnica ha sido realizada en alemán/francés/italiano/español/japonés/coreano mediante traducción automática por medio de inteligencia artificial para tu mayor comodidad. Ten en cuenta que la traducción no ha sido revisada ni verificada por traductores humanos y, por tanto, puede contener ligeras distorsiones o errores lingüísticos. Consulta la versión original en inglés de la ficha técnica para disfrutar de la versión más precisa y fiable.

[Iniciar chat ahora](#)

© Copyright 2025 Hewlett Packard Enterprise Development LP. La información que contiene este documento está sujeta a cambios sin previo aviso. Las únicas garantías de los productos y servicios de Hewlett Packard Enterprise figuran en las declaraciones expresas de garantía incluidas en los mismos. Nada de lo que aquí se indica debe interpretarse como una garantía adicional. Hewlett Packard Enterprise no se responsabilizará de los errores u omisiones técnicos o editoriales que pudiera contener el presente documento.

a00151269ESE, Rev. 1

HEWLETT PACKARD ENTERPRISE

hpe.com

