Barracuda

No todos los firewall de nueva generación son iguales.

Cómo crear su propia red segura de entrega de aplicaciones

Informe técnico

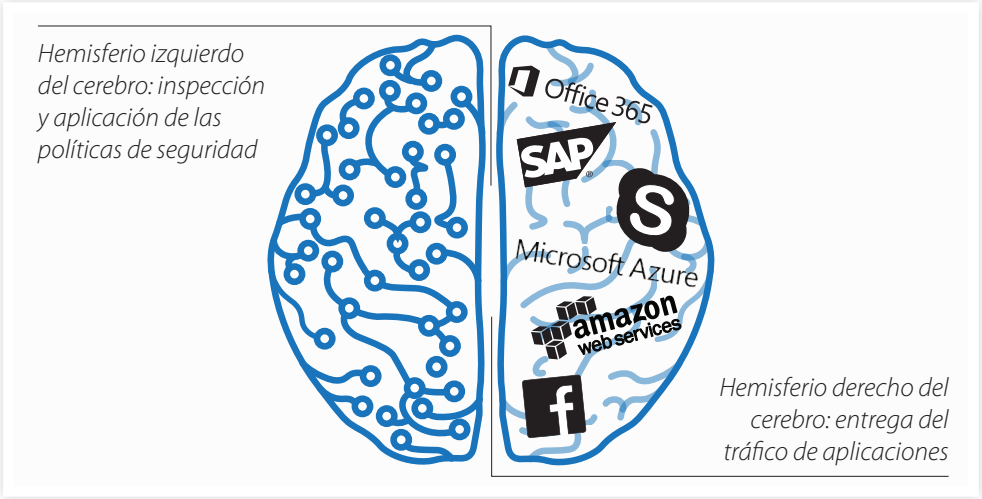
No todos los firewall de nueva generación son iguales.

Conciliación de la discrepancia entre las necesidades de los compradores del mundo real y la oferta generalizada del sector de los firewalls, o cómo crear su propia red segura de entrega de aplicaciones.

Por el Dr. Klaus Gheri, vicepresidente de Seguridad de Red Barracuda Networks, Inc. [NYSE:CUDA]

En los últimos tiempos, es posible que haya reparado en que las conversaciones típicas sobre firewalls de nueva generación han evolucionado. Debido a que el control de aplicaciones y el conocimiento por parte del usuario son elementos cada vez más frecuentes, el sector de los firewalls intenta ahora marcar la diferencia mediante la implementación de capacidades de protección frente a amenazas avanzadas. De hecho, aunque las amenazas avanzadas conforman un problema constante, existe una amplia gama de dificultades económicas y operativas que han surgido recientemente y a las que se enfrentan las organizaciones de TI en un mundo en el que las aplicaciones se emplean cada vez más como servicios.

¿Qué es un firewall? Se trata de dispositivo que actúa como enrutador y, al mismo tiempo, como un punto de paso obligatorio de la comunicación de red que permite aplicar las políticas de seguridad. Para que resulte más claro, entre sus funciones se incluye también la de **entrega de aplicaciones**. En este aspecto, es similar al funcionamiento del cerebro humano, que consta de dos hemisferios igual de importantes, cada uno de ellos con distintas tareas y habilidades. El cerebro solo funciona de manera eficaz mediante la estrecha colaboración entre ambos hemisferios.



Desafortunadamente, las conversaciones habituales en las que se mencionan las actualizaciones de firewall se centran en la aplicación de medidas de seguridad y la inspección profunda de paquetes. Sin embargo, ¿qué hay del tráfico benigno y favorable en el que se basan sus líneas de negocio? Este tráfico de aplicaciones debe proporcionarse de forma segura con una calidad de servicio predecible, ya sea de sitio a sitio o, lo que es cada vez más habitual, de nube a sitio.. Un firewall que se centra exclusivamente en la seguridad sin encargarse de forma adecuada de los aspectos relacionados con la entrega de su firewall sería comparable a un cerebro que utiliza solo un hemisferio totalmente, mientras que el otro se mantiene inactivo. Aunque un cerebro así se consideraría disfuncional, estas deficiencias comparables no parecen preocuparnos cuando se trata de un firewall.

Volvamos la vista al pasado para entender mejor por qué este desequilibrio es un problema que cada vez genera más limitaciones. No hace demasiado tiempo, existía un mundo en el que, de forma prácticamente generalizada, se usaba la red corporativa para acceder a los datos de uso compartido interno, recibir y enviar mensajes de correo electrónico y navegar tranquilamente por Internet. Los dos componentes principales de las infraestructuras corporativas eran las LAN a través de las que se conectan los usuarios y las WAN, es decir, los enlaces de red que conectan las oficinas satélite con las ubicaciones corporativas principales

La centralización de las infraestructuras de backend de las oficinas y la ampliación de aplicaciones que no estaban diseñadas específicamente para entornos de alta latencia en toda la WAN generaron al poco tiempo problemas de rendimiento y una reducción en la productividad. Esto propició la llegada de toda una nueva gama de productos de optimización de WAN que, desde aquel momento, se han empleado para hacer frente a estos problemas. Este tipo de productos ofrecen tanto la optimización genérica mediante técnicas de compresión y deduplicación de datos, como mejoras de protocolo específicas para determinadas aplicaciones populares. Por lo general, estos productos enfocados exclusivamente en dichos objetivos no proporcionan funciones de inspección profunda o VPN adecuadas. Con demasiada frecuencia, los clientes huyen de la complejidad que supone el uso paralelo de firewalls y herramientas de optimización de WAN ya que esto deriva en unos patrones de flujo de tráfico más complejos asociados con ambos dispositivos. Por este motivo, suelen recurrir a estructuras de WAN basadas en MPLS en las que todo el tráfico, incluida la navegación por Internet, se transfiere al centro de datos.

En su momento, existía un grado de dependencia muy bajo en la accesibilidad de las ofertas de SaaS o los servicios de la nube que no se encontraban dentro de los límites de las LAN corporativas. Sin embargo, actualmente, debido a la variedad de ofertas de SaaS que afectan cada vez más a las necesidades principales, como ofertas de aplicaciones de oficina (por ejemplo, Microsoft Office 365), se han detectado errores en el enfoque de transferencia del tráfico, ya que la red troncal de MPLS no diferencia entre las aplicaciones que usan la misma línea física. Por ello, podría ocurrir que un agente de actualización o una aplicación de backup interna provocaran una congestión en la línea. Esto dificultaría en gran medida el uso de las aplicaciones en línea fundamentales para el funcionamiento de la empresa.

La solución definitiva para este problema consiste en separar los distintos tipos de tráfico de aplicaciones entre sí, ya sea físicamente o lógicamente, dividiendo el flujo en distintos segmentos de calidad. Si recurrimos de nuevo a la analogía de los hemisferios, esto supondría que el hemisferio de inspección resultaría necesario para determinar la naturaleza de un flujo de tráfico, mientras que el otro serviría para tomar medidas inteligentes y proporcionar este flujo de forma distinta que otros de menor importancia.

Debido a las numerosas ofertas de SaaS que se emplean, la mejor opción es recurrir a pasarelas directas de acceso a Internet en las distintas ubicaciones. Por supuesto, estas pasarelas deben estar protegidas mediante firewalls de nueva generación adecuados. Esto puede resultar aparentemente abrumador ya que, en ese caso, existiría también la necesidad de mantener los distintos firewalls sincronizados. Esto no ocurre si el producto de firewall incorpora una potente arquitectura de gestión centralizada que permite administrar una única política (o, como mucho, varias) desde un único punto, que después se implementará en los puntos de paso obligatorios para aplicarla de forma descentralizada, es decir, siguiendo el principio de gestionar una sola vez y ejecutar en todos los puntos.

Además, la implementación de una pasarela de acceso local ofrece la ventaja de poder funcionar con una WAN híbrida. La WAN híbrida está formada por líneas WAN tradicionales complementadas por enlaces de VPN basados en Internet. También podría aplicarse un enfoque aún más radical, que consistiría en depender exclusivamente de la VPN basada en Internet, pero usando dos ISP distintas para crear varios túneles.

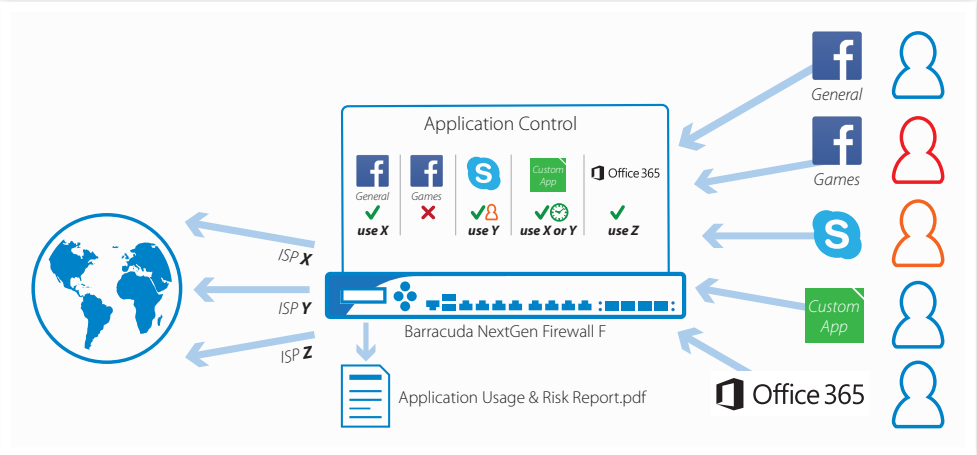
En este caso, un firewall que tenga en cuenta las aplicaciones puede encargarse de la organización y distribución de los distintos tipos de tráfico interno a los enlaces disponibles. Si ocurre algún error en un enlace, el firewall lo detectaría y redistribuiría el flujo como corresponde, sin que el servicio se viera interrumpido. Si ejecuta este tipo de firewalls y crea redundancias de red, habrá creado el sistema más adecuado para su empresa: una red troncal de comunicación segura que proporciona las funciones de inspección profunda de paquetes y reducción de amenazas que necesita, así como una entrega resistente y eficaz de las aplicaciones empresariales a los usuarios corporativos. **Este sistema se denomina "red de entrega de aplicaciones" y es lo que ayudamos a crear a nuestros clientes día a día.**

Esta solución, el Barracuda NextGen Firewall F, es nuestro firewall de nueva generación que tiene en cuenta la entrega y la conectividad de las aplicaciones para redes empresariales dispersas. Y recuerde que no todos los firewalls de nueva generación son iguales. Es mejor comprobar la capacidad cerebral que aporta su firewall actual.

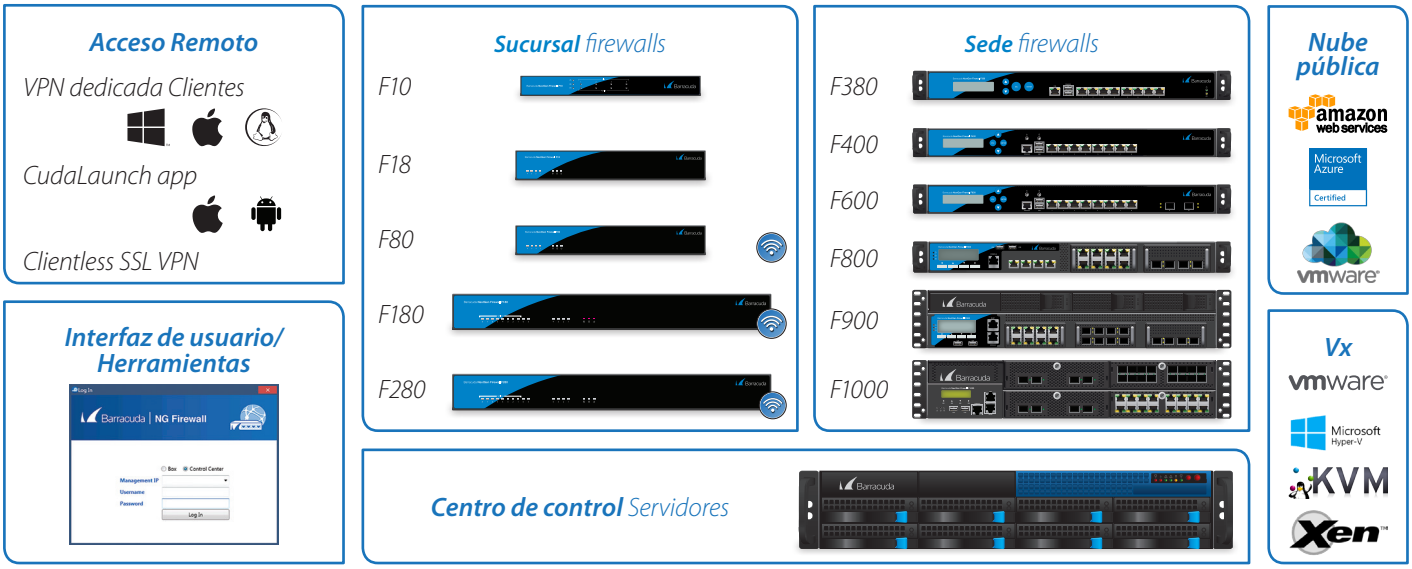
¿Cuál es la estructura de una red de entrega de aplicaciones?

Requiere la implementación de firewalls de nueva generación avanzados y que tengan en cuenta las aplicaciones en cada ubicación de la red.

Cada ubicación que necesita acceso a las ofertas de SaaS tiene una pasarela de acceso a Internet que se controla a través de este firewall. Cada una de estas ubicaciones utiliza más de un vínculo superior para establecer la conexión con las otras ubicaciones. El firewall usa estos vínculos superiores empleando un sistema de carácter selectivo con las aplicaciones, pero tiene la capacidad de reaccionar rápidamente a las interrupciones en la línea y redistribuir el tráfico con una política ajustada adecuadamente, es decir, con una selección dinámica e inteligente de ruta.



El tráfico entre las ubicaciones puede optimizarse de manera adecuada en cuanto a los niveles de latencia y rendimiento mediante técnicas de optimización de protocolos, compresión y deduplicación de datos. El firewall proporciona estos servicios para obtener una conexión estrecha entre la naturaleza del tráfico y las acciones de entrega aplicadas en cuanto a la calidad del servicio, el ancho de banda, la privacidad y la ruta de entrega.



Acerca de Barracuda NextGen Firewall F

Barracuda NextGen Firewall F-Series conforma una solución empresarial ideal para los administradores de TI que desean proteger los datos más importantes en las redes, que se han convertido en sistemas caóticos y vulnerables debido a la vehemente propagación del uso de los móviles y los dispositivos BYOD, las aplicaciones evasivas de la Web 2.0 y los usuarios de las redes remotas. Barracuda NextGen Control Center proporciona un portal de gestión centralizado intuitivo y potente que facilita en gran medida la implementación, la configuración, la actualización y la administración de varias unidades desde una única ubicación, al mismo tiempo que aporta una visibilidad completa en tiempo real sobre la red y funciones de elaboración de informes de ésta. Por ello, resulta una solución ideal para aquellas empresas que desean gestionar un gran número de usuarios o varios sitios con poco personal de TI y cumplir los requisitos de PCI.

For questions about the Si tiene alguna duda sobre Barracuda NextGen Firewall F o si desea probarlo gratis durante 30 días, visite http://www.barracuda.com/products/nextgenfirewall-f o póngase en contacto con Barracuda Networks a través del teléfono +43 (0) 508 100 (Austria).

Acerca de Barracuda Networks, Inc.

Barracuda proporciona soluciones de almacenamiento y seguridad conectadas a la nube que facilitan la TI. Más de 150 000 organizaciones de todo el mundo confían ya en estas soluciones potentes, fáciles de usar y asequibles, que se proporcionan a través de implementaciones de dispositivos físicos, virtuales, en la nube o híbridos. El modelo empresarial centrado en los clientes de Barracuda se centra en proporcionar soluciones de IT de gran valor mediante suscripciones que proporcionan una seguridad completa de los datos y de la red. Para obtener más información, visite barracuda.com.

Barracuda Networks
Eduard-Bodem-Gasse 1
6020 Innsbruck
Austria

t: +43 (0) 508 100
e: office@barracuda.com
w: barracuda.com

ES 2.0 • Copyright © Barracuda Networks, Inc. • barracuda.com
Barracuda Networks y el logotipo de Barracuda Networks son marcas comerciales registradas de Barracuda Networks, Inc. en los Estados Unidos.
Todos los demás nombres son propiedad de sus respectivos titulares.