CÓMO LOS FIREWALLS DE NUEVA GENERACIÓN DE PALO ALTO NETWORKS PROTEGEN SU NEGOCIO

Adopte innovaciones fácilmente, evite ciberataques exitosos y concéntrese en lo que importa

La rápida evolución de TI ha cambiado el aspecto del perímetro de la red. Los datos están en todos lados y los usuarios acceden a ellos desde cualquier lugar y desde todo tipo de dispositivos. Al la vez, los equipos de TI adoptan la nube, la analítica y la automatización para acelerar la implementación de nuevas aplicaciones e impulsar el crecimiento del negocio. Estos cambios fundamentales crean un panorama de amenaza que expone las vulnerabilidades en las tecnologías de seguridad tradicionales, como la seguridad de redes basada en puertos o herramientas y tecnologías dispares que no están integradas de forma nativa. Estas herramientas de seguridad que no se diseñaron para la automatización y requieren analistas que combinen manualmente conocimientos de diversas fuentes desconectadas antes de actuar.

Necesitamos un enfoque diferente: uno que comience con el Firewall de Nueva Generación (NGFW) de Palo Alto Networks® como la piedra angular de una plataforma integrada. Nuestro NGFW ofrece una arquitectura enfocada en la prevención que es fácil de implementar y operar, que utiliza la automatización para reducir los esfuerzos manuales y permitir que los equipos de seguridad puedan enfocarse en lo que importa; así lo ayuda a adoptar nuevas innovaciones fácilmente.

La Base de la Security Operating Platform

Nuestros firewalls de nueva generación inspeccionan todo el tráfico, incluso de aplicaciones, amenazas y contenido, y lo vinculan con el usuario, independientemente de la ubicación o el tipo de dispositivo. El usuario, la aplicación y el contenido (los elementos que hacen funcionar su negocio) se convierten en componentes integrales de su política de seguridad empresarial. Como resultado, puede alinear la seguridad con sus políticas de negocios, así como elaborar reglas fáciles de entender y mantener.

Como parte de nuestra Security Operating Platform, nuestros NGFWs ofrecen a las organizaciones las siguientes capacidades:

Figura 1: Elementos básicos de la seguridad de la red

- Habilitar aplicaciones en forma segura, incluidas aplicaciones de software-as-a-service (software como servicio – SaaS), usuarios y contenidos, mediante la clasificación de todo el tráfico, independientemente del puerto;
- Reducir el riesgo de ataque usando un modelo de aplicación positiva, en otras palabras, al permitir todas las aplicaciones deseadas y bloquear todo lo demás;
- Aplicar políticas de seguridad para bloquear exploits de vulnerabilidad conocidos, virus, ransomware, spyware, botnets y otro malware desconocido como las amenazas avanzadas persistentes;
- Proteger los centros de datos, incluidos los virtualizados, mediante la segmentación de datos y aplicaciones, así como la aplicación del principio Confianza Cero;
- Aplicar la seguridad en forma consistente a través de todos sus entornos físicos y en la nube;
- Adoptar una informática móvil segura al extender la Security Operating Platform a usuarios y dispositivos, sin importar dónde estén ubicados;
- Obtener visibilidad centralizada y optimizar la seguridad de la red, al tornar grandes cantidades de datos accionables para poder evitar ciberataques exitosos.

A continuación, se detallan las capacidades principales de nuestro NGFW que su negocio necesita para operar de manera segura.

Confianza Cero

Los modelos de seguridad convencionales operan bajo el pasado supuesto de que se puede confiar en todo lo que está dentro de la red de una organización. Los modelos de seguridad tradicionales están diseñados para proteger el perímetro mientras las amenazas que penetran la red pasan desapercibidas y quedan libres para poner en riesgo los datos confidenciales y valiosos del negocio. En el mundo digital, la confianza no es más que una vulnerabilidad.

Confianza Cero es una práctica recomendada de ciberseguridad centrada en los datos que elimina el supuesto de confianza y provee una base fiable para la seguridad. En un mundo basado en Confianza Cero, no existen dispositivos, sistemas, ni personas de confianza. Usted identifica los activos y los datos que requieren protección; determina quién o qué requiere acceso a datos específicos según el principio de la "necesidad de conocimiento", modelo de acceso basado en privilegios mínimos; define las reglas de seguridad que reflejan su política de negocios; e inspecciona y registra todo el tráfico.

Nuestros NGFWs ayudan con todos estos pasos, incluso permite un acceso seguro a todos los usuarios, independientemente de su ubicación; inspecciona todo el tráfico; implementa políticas de control de acceso basado en privilegios mínimos; y detecta y previene las amenazas avanzadas. Esto reduce considerablemente las vías de acceso de los atacantes a sus activos críticos, ya sea que esos adversarios se encuentren dentro o fuera de su organización.

Identificación de Usuarios, Protección de la Identidad del Usuario

La tecnología User-ID™ permite que nuestros NGFWs puedan identificar a los usuarios en todas las ubicaciones, independientemente de su tipo de dispositivo o sistema operativo. La visibilidad de la actividad de las aplicaciones basada en los usuarios y los grupos, en lugar de las direcciones IP, habilita las aplicaciones de manera segura al alinear el uso con los requisitos del negocio. También puede definir políticas de acceso a las aplicaciones en base a usuarios o grupos de usuarios. Por ejemplo, puede permitir que solo los administradores de TI utilicen herramientas como Secure Shell (Intérprete de Órdenes Segura - SSH), Telnet y File Transfer Protocols (Protocolos de Transferencia de Archivos - FTPs). La política sigue al usuario a donde quiera que vaya (sede central, sucursales o su hogar) y con cualquier dispositivo que utilice. Además, puede utilizar opciones de reporte predefinidas o personalizadas para generar informes más completos sobre las actividades de los usuarios.

Sin embargo, la cuestión de la identidad del usuario va más allá de la política y los informes basados en el usuario. Proteger la identidad del usuario tiene la misma importancia. En el “2017 Data Breach Investigations Report” (Informe de Investigación de Brechas de Datos de 2017) de Verizon®, se determinó que el 81 % de las brechas relacionadas con actividades de hackeo aprovecharon credenciales poco seguras o robadas.[1] Los atacantes utilizan credenciales robadas para obtener acceso a las redes de las organizaciones, donde encuentran aplicaciones y datos valiosos que pueden robar. Para evitar los ataques basados en credenciales, nuestros NGFWs logran:

- Bloquear el acceso a sitios de fraude electrónico conocidos a través de Filtrado de URLs con PAN-DB, usando la inteligencia de amenazas más reciente a nivel global, actualizada cada cinco minutos, para proteger a los usuarios frente a los intentos de robo de sus credenciales;

- Evitar que los usuarios envíen credenciales corporativas a sitios desconocidos para protegerlos de los ataques dirigidos que utilizan sitios de fraude electrónico nuevos o desconocidos para que no se los detecte;
- Aplicar multi-factor authentication (autenticación de múltiples factores – MFA) para cualquier aplicación que considere sensible, incluso aplicaciones antiguas que no se prestan fácilmente a la MFA. Esto lo protege si un atacante ya tiene en su poder credenciales robadas, al tener que aplicar mecanismos adicionales de autenticación para controlar el acceso a sistemas críticos. Puede implementar esta capacidad con el proveedor de identidad que desee, incluidos Ping Identity®, Okta®, RSA® y Duo Security, de modo que la experiencia de sus usuarios con la MFA continúe siendo la misma con todas las aplicaciones a las que accedan;

Habilitar Aplicaciones de Forma Segura

Los usuarios acceden a diversos tipos de aplicaciones, incluso aplicaciones de software-as-a-service (software como servicio – SaaS). Algunas de estas aplicaciones están aprobadas por su organización; otras son toleradas, aunque no sean obligatorias para llevar a cabo las operaciones de su negocio; y el resto no deben permitirse, ya que incrementan los riesgos. La tecnología App-ID™ de nuestros NGFWs identifica con precisión las aplicaciones en todo el tráfico que pasa por la red, incluso aquellas disimuladas como tráfico autorizado, así como aquellas que utilizan puertos dinámicos o intentan ocultarse bajo el cifrado. App-ID le permite entender y controlar las aplicaciones y sus funciones como la transmisión por video frente al chat, la carga frente a la descarga, el uso compartido de pantallas frente al control remoto de dispositivos, etc.

Las características de las aplicaciones SaaS le permiten entender el uso de las aplicaciones. Por ejemplo, puede identificar qué aplicaciones SaaS, a las que se accede desde su organización, carecen de las certificaciones necesarias o tienen antecedentes de brechas de datos. Puede otorgar acceso de cuentas empresariales aprobadas a aplicaciones SaaS, como Microsoft® Office 365®, mientras bloquea el acceso de cuentas no aprobadas, incluidas las cuentas personales o de consumidores.

Proteger el Tráfico Cifrado Sin Comprometer la Privacidad

Los usuarios pasan más del 80 % de su tiempo en sitios web y aplicaciones encriptados. Lamentablemente, los atacantes aprovechan el cifrado para ocultar las amenazas de los dispositivos de seguridad.[2]

Nuestros NGFWs utilizan el descifrado basado en políticas para permitir que los profesionales de seguridad descifren el tráfico malintencionado con el objetivo de prevenir las amenazas mientras se preserva la privacidad del usuario y se mantiene un rendimiento predecible. Los controles flexibles le permiten dejar el tráfico cifrado si es confidencial, por ejemplo, en caso de que esté asociado a sitios web gubernamentales, militares, de salud o de compras. Puede evitar que los usuarios accedan a sitios web que utilizan certificados vencidos, no confiables o autofirmados. También puede bloquear el acceso si un sitio web utiliza versiones TLS inseguras o conjuntos de cifrado poco seguros. Para preservar la privacidad del usuario, puede definir exclusiones de descifrado por política e incluso permitir que los usuarios excluyan el descifrado para transacciones específicas que puedan incluir datos personales. El resto de su tráfico puede descifrarse y protegerse.

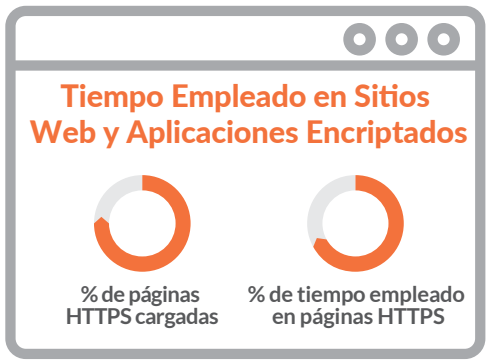

Figura 2: Creciente predominio del cifrado web

La compatibilidad con módulos de seguridad de hardware le permite gestionar claves digitales de manera segura. Perfect Forward Secrecy (Confidencialidad Directa Total) garantiza que una sesión cifrada en riesgo no comprometa la seguridad de múltiples sesiones cifradas.

Detectar y Evitar Amenazas Avanzadas

Hoy en día, la mayor parte del malware moderno, incluso las variantes de ransomware, utiliza técnicas avanzadas para transportar ataques o exploits a través de herramientas y dispositivos de seguridad de redes. Los NGFWs de Palo Alto Networks identifican las técnicas de evasión y las contrarrestan automáticamente a través de múltiples recursos:

- La tecnología Content-ID™ ofrece un enfoque innovador basado en el análisis completo de todo el tráfico permitido al utilizar múltiples tecnologías de prevención de amenazas avanzadas en un solo motor unificado;
- El servicio Threat Prevention de Palo Alto Networks trabaja con el NGFW para brindar capacidades de sistemas de prevención de intrusiones que bloquean los exploits de vulnerabilidad, absorben los desbordamientos y los escaneos de puertos, además de brindar protección frente a los métodos de evasión y ofuscación de los atacantes, así como también proveen protecciones de redes antimalware y de comando y control;
- Nuestro servicio de Filtrado de URLs bloquea el acceso a sitios conocidos de descarga de phishing o fraude electrónico y malware, además de reducir los riesgos relacionados con las transferencias de archivos y datos no autorizados;
- El servicio de prevención de malware WildFire® usa múltiples métodos de análisis para detectar amenazas desconocidas, incluso análisis estático con aprendizaje automatizado, análisis dinámico y análisis físico o bare metal. Su arquitectura basada en la nube posibilita la prevención y la detección de amenazas a gran escala a través de su red, endpoints y nubes para detener las amenazas conocidas y desconocidas.

Inteligencia de Amenazas Compartida

Las organizaciones dependen de múltiples fuentes de inteligencia de amenazas para garantizar la mayor visibilidad posible sobre las amenazas desconocidas, pero luchan por incorporar, correlacionar, validar y compartir esa información para implementar medidas de protección a través de sus redes. Al trabajar con otros componentes de la Security Operating Platform, el NGFW ofrece mayor contexto y una protección más holística. WildFire detecta las amenazas desconocidas con datos de una comunidad global y las bloquea automáticamente; el servicio de inteligencia contextual de amenazas AutoFocus™ brinda información de contexto, agrupación y atribución para que los equipos de seguridad puedan responder más rápidamente; y la analítica de comportamiento Magnifier™ detecta las amenazas internas y coordina esa información con WildFire.

Además, WildFire ayuda al NGFW en la evaluación del tráfico mediante el análisis de amenazas desconocidas y la aplicación de protecciones automatizadas de alta fidelidad a través de redes, móviles y nubes en tan solo cinco minutos.

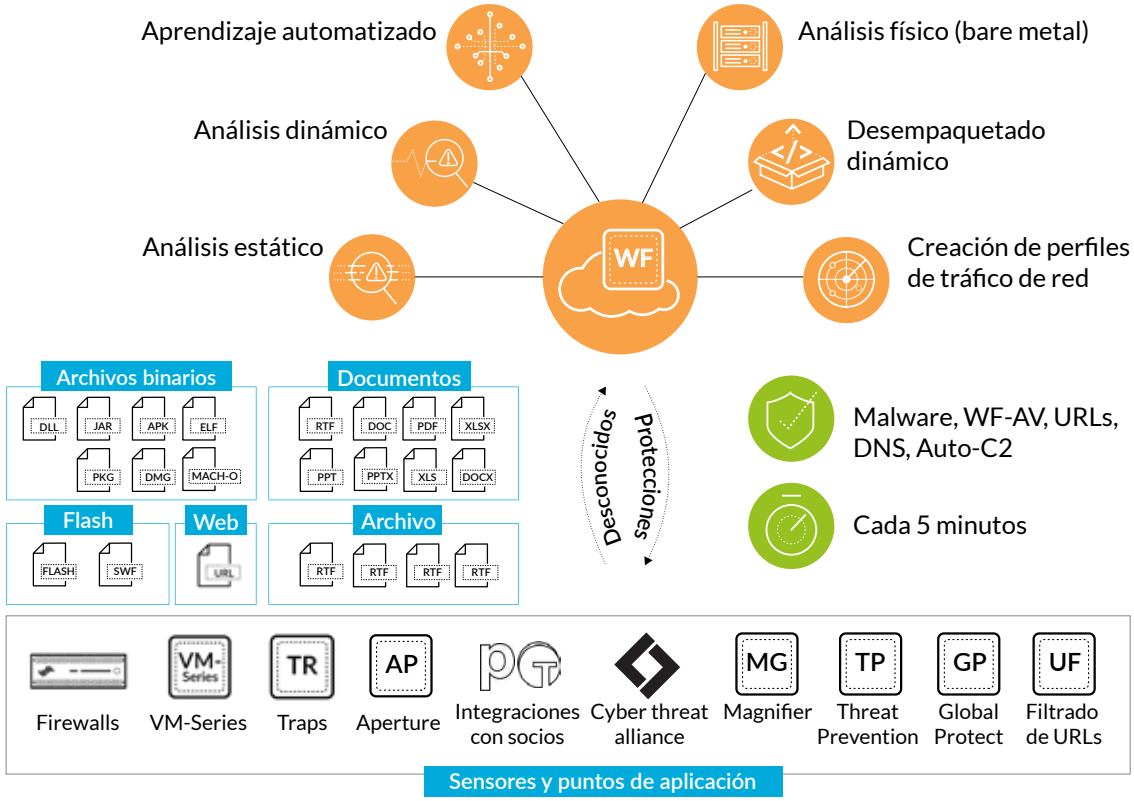

Figura 3: Detecte y evite nuevas amenazas con WildFire

Arquitectura de Paso Único

Protegerse frente al panorama de amenazas en constante evolución suele requerir la introducción de nuevas funcionalidades de seguridad. Los NGFWs de Palo Alto Networks están conformados bajo una arquitectura de paso único, lo que permite integrar de forma nativa las funciones que se agregan a un NGFW con otras funciones. Este enfoque integrado ofrece un mayor nivel de seguridad y facilidad de uso que no se pueden lograr agregando capas de nuevas capacidades en una arquitectura tradicional que aún funciona con direcciones IP, puertos y protocolos. Nuestro NGFW realiza una completa inspección de paso único de todo el tráfico a través de todos los puertos, lo que proporciona el contexto completo en torno a las aplicaciones, el contenido asociado y la identidad del usuario para formar la base de las decisiones de su política de seguridad. Su arquitectura nos permite agregar capacidades nuevas e innovadoras fácilmente, tal como lo hicimos con WildFire y, más recientemente, con Magnifier.

Si el NGFW o endpoint de un cliente en Singapur encuentra un archivo sospechoso, ese archivo se envía a WildFire para someterlo a un análisis avanzado. Los resultados del análisis, incluidos los veredictos y las protecciones, se envían automáticamente al cliente en Singapur, así como también a todos los otros clientes de WildFire de todo el mundo.

Implementación Flexible

Nuestros NGFWs pueden implementarse en múltiples factores de forma:

- Hardware, una combinación de potencia, inteligencia, simplicidad y versatilidad protege las implementaciones de empresas y proveedores de servicios en sedes centrales, centros de datos y sucursales;
- VM-Series, nuestro firewall de nueva generación virtualizado protege sus implementaciones de nube pública y privada mediante la segmentación de aplicaciones y la prevención de amenazas;
- Servicio en la nube GlobalProtect, nuestro firewall de nueva generación brinda seguridad global eficaz en términos operativos desde la nube a través de GlobalProtect™, seguridad de redes para endpoints.

Puede elegir una de estas opciones, o una combinación de acuerdo a sus requisitos por ubicación, y administrar todas las implementaciones de manera centralizada a través de la gestión de la seguridad de redes Panorama™.

Gestión de Seguridad de Redes

Los equipos de TI están presionados al límite intentando administrar las complejas implementaciones de seguridad de hoy. La Security Operating Platform ayuda a facilitar la gestión de la seguridad, así como la visualización y la interacción con los datos. Cada firewall individual puede administrarse a través de una interfaz con funciones completas, basada en un explorador. Para las implementaciones a gran escala, puede usar Panorama para obtener visibilidad centralizada, editar políticas de seguridad y automatizar acciones para todos sus firewalls, en cualquier factor de forma. El aspecto y la disposición son idénticos en cualquiera de las interfaces. Cuando es necesario, el plugin

Interconnect de Panorama puede vincular múltiples nodos de Panorama para centralizar la gestión de la configuración y adaptar la vista unificada para sus cientos de miles de firewalls.

El control de acceso basado en funciones de Panorama, combinado con reglas previas y posteriores, le permite encontrar un equilibrio entre la supervisión centralizada y la necesidad de contar con flexibilidad para editar políticas y configurar dispositivos en forma local. El Application Command Center (Centro de Comando de Aplicaciones – ACC) y las capacidades de gestión de logs, o registros, generan una sola pantalla que otorga visibilidad accionable a través de múltiples dispositivos, sin importar dónde estén implementados. La compatibilidad adicional con herramientas basadas en estándares, como el Simple Network Management Protocol (Protocolo Simple de Administración de Redes - SNMP) y las APIs basadas en REST, permite integrar herramientas de gestión de terceros fácilmente.

Generación de Informes y Logs (Registros)

Para identificar, investigar y responder a incidentes de seguridad, la Security Operating Platform ofrece:

- **Generación de Logs (Registros)**, Palo Alto Networks va más allá de los eventos de procesamiento y listados tradicionales. Puede ver logs o registros de maneras que hacen sentido, incluso gráficos, mapas, tablas de tendencias y demás para interpretar los datos de la red. El motor de correlación automatizado elimina las tareas manuales de correlación y detecta amenazas que, de lo contrario, pasarían desapercibidas a causa del ruido. También puede reenviar registros usando criterios de filtrado para crear flujos de trabajo que puedan automatizar acciones dentro de nuestra Security Operating Platform o de sistemas de terceros. Cuenta con la flexibilidad de agrupar registros de forma local o en el Logging Service basado en la nube.
- **Generación de Informes,** puede usar nuestros informes estándares o crear versiones personalizadas para trabajar los datos de acuerdo a sus requerimientos específicos. Todos los informes pueden exportarse a formato CSV o PDF, así como ejecutarse y enviarse por correo electrónico de forma programada.
- **Detección de Amenazas,** con los conocimientos colectivos de miles de empresas, proveedores de servicios y gobiernos de todo el mundo, AutoFocus brinda una visibilidad sin precedentes de las amenazas desconocidas. La integración de AutoFocus en PAN-OS® acelera los flujos de trabajo de análisis y detección de amenazas sin necesidad de contar con recursos especializados adicionales.

¿Por Qué Elegir los NGFWs de Palo Alto Networks?

Nuestros NGFWs permiten que sus usuarios accedan a datos y aplicaciones de acuerdo a los requisitos del negocio, le brindan protección frente a los ataques basados en credenciales y previenen las amenazas conocidas y las previamente desconocidas, incluso en el tráfico cifrado. La automatización le permite ahorrar tiempo con reglas de seguridad que reflejan su política comercial, son fáciles de mantener, se adaptan a su dinámico entorno y generan acciones automatizadas basadas en sus políticas. Nuestros NGFWs, disponibles en factores de forma físicos, virtualizados o a través de la nube, se administran de forma consistente a través de Panorama.

Como parte de la Security Operating Platform, los firewalls de nueva generación de Palo Alto Networks ayudan a las organizaciones a adoptar innovaciones de seguridad integradas en forma nativa, como WildFire y Magnifier, mientras comparten datos e inteligencia a través de los endpoints y las nubes.

Figura 4: Security Operating Platform de Palo Alto Networks

Más de 54 000 clientes en más de 150 países han adoptado nuestra arquitectura enfocada en la prevención. Reconocidos como Líderes en el Magic Quadrant® de Gartner para Firewalls de Redes Empresariales siete veces consecutivas, también recibimos la calificación de Recomendado de NSS Labs, que es la calificación más alta que ofrece NSS Labs.

Aquí encontrará algunos recursos útiles para comenzar:

✓ ¿Quiere conocer más sobre nuestros NGFWs? Visite nuestra página de descripción general de seguridad de redes.

✓ ¿Está listo para probar nuestros NGFWs? Realice una Prueba Definitiva.

✓ ¿Desea incorporar una arquitectura orientada a la prevención a su negocio? Realice una Evaluación de Su Postura de Prevención.

✓ ¿Está listo para aprovechar al máximo las funciones y las herramientas que necesita para proteger su negocio? Regístrese para una Evaluación de Mejores Prácticas.

1. Verizon Communications. “2017 Data Breach Investigations Report” (Informe de Investigación de Brechas de Datos de 2017), 26 de julio de 2017. https://www.knowbe4.com/hubfs/rp_DBIR_2017_Report_execsummary_en_xg.pdf
2. Google, Inc. “Google Transparency Report: HTTPS encryption on the web” (Informe de Transparencia de Google: Cifrado HTTPS en la Web), con acceso el 6 de septiembre de 2018. https://transparencyreport.google.com/https/overview?hl=en

3000 Tannery Way
Santa Clara, CA 95054
Línea principal: +1.408.753.4000
Ventas: +1.866.320.4788
Soporte técnico: +1.866.898.9087
www.paloaltonetworks.com