PALO ALTO

NGX:

1.- NG Firewall:

Visibilidad y Control

Nuestro firewall de próxima generación clasifica todo el tráfico, incluido el tráfico cifrado, basado en la aplicación, la función de la aplicación, el usuario y el contenido. Puede crear políticas de seguridad completa y precisa, que resulten en la habilitación segura de las aplicaciones. Esto permite que sólo usuarios autorizados ejecuten aplicaciones sancionadas, reduciendo en gran medida la superficie de los ataques cibernéticos en toda la organización.

Los cortafuegos de próxima generación de Palo Alto Networks están diseñados para permitir aplicaciones y prevenir amenazas modernas. Nuestro enfoque identifica todo el tráfico de red basado en aplicaciones, usuarios, contenido y dispositivos, y le permite expresar sus políticas empresariales en forma de reglas de seguridad fáciles de entender.

Las opciones flexibles de implementación y la integración nativa con nuestra plataforma de próxima generación amplían la prevención de la aplicación de políticas y la prevención contra la ciberdelincuencia en todos los lugares donde se encuentran sus usuarios y datos: en su red, en sus puntos finales y en la nube.

Arquitectura superior, ventajas superiores

Visibilidad completa y control preciso: Nuestros firewalls de próxima generación proporcionan visibilidad completa en todo el tráfico de red basado en aplicaciones, usuarios, contenido y dispositivos.

Seguridad automatizada: las funciones innovadoras reducen las tareas manuales y mejoran su postura de seguridad, por ejemplo, mediante la diseminación de protecciones de amenazas previamente desconocidas globalmente en tiempo casi real, correlacionando una serie de eventos de amenaza relacionados para indicar un probable ataque a su red y utilizando dinámicas Grupos de direcciones en reglas de seguridad para evitar la actualización de direcciones IP de servidor con frecuencia.

Protección para sus usuarios y datos en todas partes: Nuestros cortafuegos de próxima generación están integrados nativamente con nuestra plataforma de seguridad, lo que evita amenazas cibernéticas avanzadas y desconocidas, independientemente de dónde se encuentren los usuarios y los datos: en su red, en sus puntos finales y en la nube.

2.- URL Filtering:

La función de filtrado de URL de Palo Alto Networks complementa la función de ID de aplicación al permitir configurar el firewall para identificar y controlar el acceso al tráfico web (HTTP y HTTPS).

Mediante la implementación de perfiles de filtrado de URL en las políticas de seguridad y el uso de categorías de URL como criterios de coincidencia en las políticas (portal cautivo, descifrado, seguridad y QoS), obtendrá una visibilidad y un control completos del tráfico que atraviesa su firewall y podrá Habilitar y controlar de forma segura cómo sus usuarios acceden a la web.

La solución de filtrado de URL de Palo Alto Networks utiliza una base de datos de filtrado de URL que contiene millones de sitios web y cada sitio web se coloca en una de aproximadamente 60 categorías diferentes. Un perfil de filtrado de URL que contiene la lista de categorías se aplica a una directiva de seguridad que permite el tráfico web (HTTP / HTTPS) de los usuarios internos a Internet.

3.- Threat Protección:

Los atacantes de hoy están bien financiados y bien equipados. Ellos usan tácticas evasivas para tener éxito en ganar un punto de apoyo en la red, lanzando ataques de alto volumen y sofisticados mientras permanecen invisibles a las defensas tradicionales de una organización, desde la ofuscación de paquetes, el malware polimórfico, el cifrado a las cargas múltiples y DNS de flujo rápido.

La prevención de amenazas protege su red frente a estas amenazas al proporcionar múltiples capas de prevención, enfrentando amenazas en cada fase del ataque. Además de las capacidades Tradicionales de prevención de intrusiones, ofrecemos la capacidad única de detectar y bloquear amenazas en todos y cada uno de los puertos, en lugar de invocar firmas basadas en un conjunto limitado de puertos predefinidos.

4.- Global Protect:

El mundo que necesita proteger sigue creciendo a medida que los usuarios y las aplicaciones cambian a ubicaciones fuera del perímetro de red tradicional. Los equipos de seguridad se enfrentan a retos con el mantenimiento de la visibilidad del tráfico de red y la aplicación de las políticas de seguridad para detener las amenazas. Las tecnologías tradicionales utilizadas para proteger puntos finales móviles, como el software antivirus de punto final del host y VPN de acceso remoto, no son capaces de detener las técnicas avanzadas empleadas por el atacante más sofisticado de hoy en día.

El cliente de seguridad de red GlobalProtect ™ para puntos finales, de Palo Alto Networks®, permite a las organizaciones proteger la fuerza de trabajo móvil extendiendo la Plataforma de Seguridad de Próxima Generación a todos los usuarios, independientemente de la ubicación. Asegura el tráfico mediante la aplicación de las capacidades de la plataforma para comprender el uso de las aplicaciones, asociar el tráfico con usuarios, dispositivos y hacer cumplir las políticas de seguridad con las tecnologías de próxima generación.

5.- WildFire:

Prevención automática de explotaciones y malware altamente invasivos a día cero.

El servicio de análisis de amenazas Cloud-based de Palo Alto Networks® WildFire ™ es el
El motor de análisis y prevención más avanzado de la industria para aplicaciones altamente evasivas explotaciones de día cero y malware.

El servicio emplea una técnica multi-única, enfoque combinando análisis dinámico y estático, aprendizaje de máquinas innovadores técnicas y un innovador entorno de análisis de metales desnudos para y prevenir incluso las amenazas más evasivas.

Análisis de amenazas WildFire, servicio de prevención:

- Detecta explotaciones evasivas de día cero.
- Malware con una única combinación dinámica y estática.
- Análisis, aprendizaje de máquina novela.
- Técnicas, y una industria-primero.
- Ambiente de análisis de metal desnudo.
- Orchestrates automatizados.
- Prevención de amenazas desconocidas.
- En tan sólo 5 minutos del primer descubrimiento en cualquier lugar del Mundo, sin necesidad de manuales de respuesta.
  Construye inmunidad colectiva para Malware desconocido y exploits
- Con inteligencia en tiempo real compartida de más de 15.500 suscriptores.
- Análisis y contexto con AutoFocus ™ amenaza contextual
- Servicio de inteligencia.

6.- Traps (Advanced EndPoint Protection):

Palo Alto Networks ahora ofrece un segundo producto de punto final, además del Existente GlobalProtect. El entorno de análisis de malware de Palo Alto, WildFire, un componente de su Nube de Inteligencia de Amenazas, continuó viendo altas tasas de conexión para clientes nuevos y existentes en 2015.
Prevenir las infracciones cibernéticas, bloquee de forma preventiva el malware conocido, desconocido y las amenazas de día cero con el enfoque de prevención multi-método único de la protección avanzada de Endpoint de Traps ™.

Automatizar la prevención, reprograma automáticamente tus puntos finales para bloquear las amenazas conocidas y desconocidas, sin intervención humana, utilizando la inteligencia de amenazas obtenida de nuestra comunidad global de clientes y socios.

Proteger y habilitar usuarios, capacitar a los usuarios a utilizar aplicaciones basadas en web, móviles y en la nube sin temor a las amenazas cibernéticas. Proteja a los usuarios de comprometer inadvertidamente sus sistemas sin pesadas exploraciones de virus.

7.- Management (Panorama):

Política simplificada y poderosa

La gestión de la seguridad de la red de Panorama ™ proporciona reglas estáticas y actualizaciones de seguridad dinámicas en un paisaje de amenazas que cambia constantemente. Reduzca la carga de trabajo del administrador y mejore su postura de seguridad general con una sola base de reglas para firewall, prevención de amenazas, filtrado de URL, conocimiento de aplicaciones, identificación de usuarios, bloqueo de archivos y filtrado de datos.

La administración de seguridad de la red Panorama le permite controlar su red distribuida de nuestros firewalls desde una ubicación central. Vea todo su tráfico de firewall, administre todos los aspectos de la configuración del dispositivo, empuje políticas globales y genere informes sobre patrones de tráfico o incidentes de seguridad, todo desde una sola consola.

Panorama está disponible como un dispositivo de gestión dedicado o como una máquina virtual. En resumen, panorama ofrece:

- Gestión racionalizada de las políticas.
- Operaciones simplificadas.
- Visibilidad incomparable de redes y amenazas.
- Una completa colección de registros que incluye registros de todos los firewalls de su próxima generación y protección avanzada de puntos finales Traps ™.
- Opciones flexibles de implementación.