PANORAMA

Las implementaciones de seguridad pueden ser complejas y sobrecargar a los equipos de TI con un incontables reglas de seguridad y toneladas de datos de múltiples fuentes. La gestión de seguridad de redes Panorama™ le provee herramientas de creación de políticas consolidadas fáciles de implementar, como también funciones de gestión centralizada. Puede gestionar los firewalls centralmente y utilizar funcionalidades líderes de la industria para crear reglas de seguridad efectivas, además de poder visualizar el tráfico y las amenazas de la red.

Funciones Clave

Gestión

- Grupos de dispositivos, jerarquías y etiquetas para organizar políticas;
- Pilas/agrupamiento de plantillas de configuración de red reutilizable;
- Compromisos específicos del administrador para evitar cambios accidentales;
- Actualizaciones y mejoras sencillas de software.

Visibilidad

- Visibilidad centralizada a través de toda la infraestructura;
- Vistas correlacionadas para facilitar acciones de respuesta;
- Elaboración de perfiles de salud para una mejor comprensión del uso de dispositivos.

Seguridad

- Transformación simple de reglas heredadas en reglas basadas en aplicaciones a partir de la inteligencia obtenida por PAN-OS;
- Análisis de la implementación de reglas para reducir la superficie de ataque y mejorar la postura de seguridad;
- Implementación centralizada de las últimas actualizaciones de contenido de seguridad.

Automatización

- Filtrado de logs (registros) y acciones automatizadas en sistemas de terceros;
- Implementaciones automatizadas de políticas para entornos dinámicos;
- REST APIs basadas en XML y JSON para una integración simple.

Potente Política Simplificada

La gestión de seguridad de redes Panorama™ provee reglas consistentes en un entorno de redes y amenazas en constante cambio. Gestione la seguridad de su red con una única base de reglas de seguridad para firewalls, Threat Prevention, URL Filtering, detección de aplicaciones, identificación de usuarios, ejecuciones en modo sandbox, bloqueo de archivos y filtrado de datos. Esta simplificación crucial, junto con reglas basadas en tecnología App-ID™, actualizaciones dinámicas de seguridad y análisis de la implementación de reglas, reduce la carga de trabajo administrativa y mejora su postura de seguridad general.

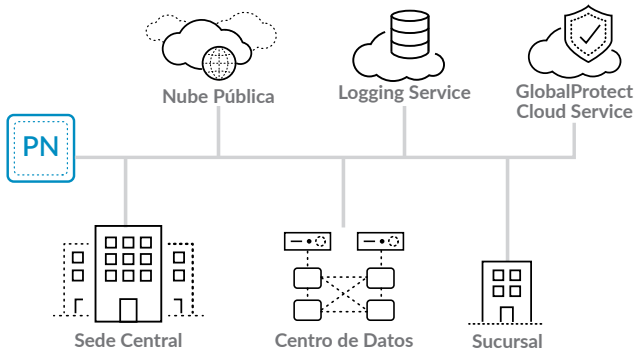

Figura 1: Implementación de Panorama

Gestión de Nivel Empresarial

Panorama mantiene el foco en los usuarios empresariales. Puede controlar sus capacidades de Internet y del centro de datos, así como también sus implementaciones en nubes públicas y privadas, todo desde una sola consola. Panorama puede implementarse mediante dispositivos virtuales, nuestros propios dispositivos diseñados específicamente o una combinación de ambos. Puede usar dispositivos como unidades de gestión de Panorama o recopiladores de logs (registros) con opciones de implementación jerárquicas. A medida que su red crezca, solo tendrá que agregar los recopiladores de logs. ¡Nosotros nos encargamos del resto!

Visibilidad Centralizada y Automatizada

La automatización del procesos de correlación de amenazas, con un conjunto de objetos de correlación predefinido, corta por lo sano la monstruosa cantidad de datos. Identifica los hosts comprometidos y correlaciona los comportamientos maliciosos que, de otro modo, se perderían entre demasiados datos. Esto reduce el tiempo de permanencia de amenazas críticas en su red. El sencillo y totalmente personalizable Application Command Center (Centro de Control de Aplicaciones - ACC) provee una perspectiva integral de sus datos de redes y de amenazas tanto actuales como históricos.

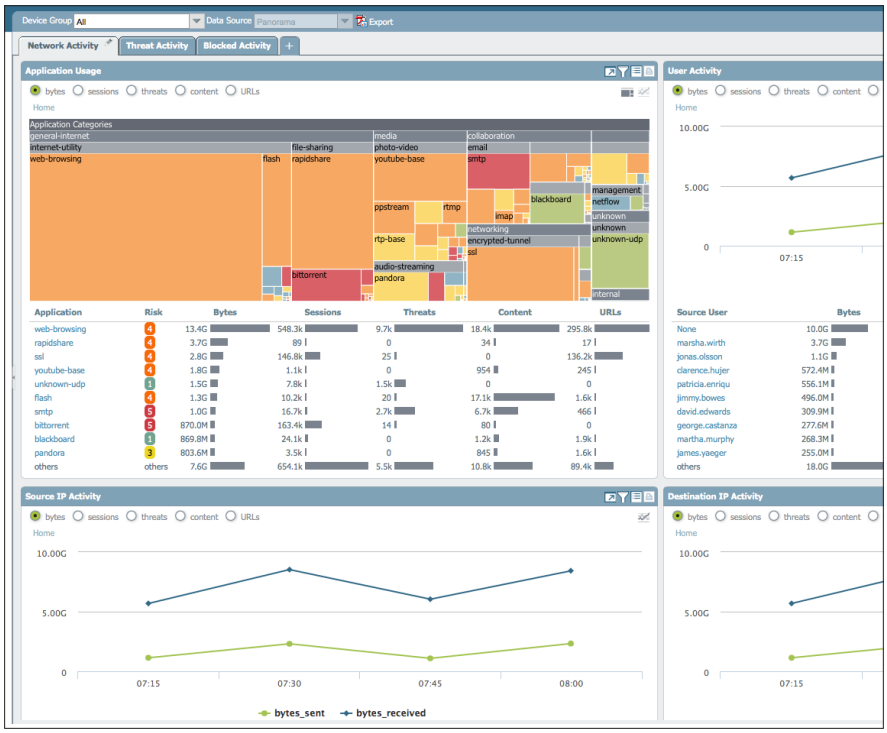

Figura 2: Application Command Center (Centro de Control de Aplicaciones - ACC)

Escala Inigualable

Utilice un solo par de dispositivos Panorama totalmente disponibles para gestionar hasta 5 000 firewalls de nueva generación o utilice el plugin o complemento Panorama Interconnect para centralizar la gestión de configuración para decenas de miles de dispositivos.

Visibilidad Potenciada de la Red

El Application Command Center (Centro de Control de Aplicaciones - ACC) le brinda una vista gráfica e interactiva de las aplicaciones, las URLs, las amenazas, los archivos de datos y los patrones que atraviesan sus firewalls de Palo Alto Networks. El ACC incluye una vista con pestañas de la actividad de red, la actividad de amenazas y la actividad bloqueada; y cada pestaña incluye widgets pertinentes para una mejor visualización de los patrones de tráfico en su red. Puede crear pestañas personalizadas con widgets que le permitan enfocarse y examinar la información más importante para la gestión. El ACC provee una vista integral y totalmente personalizable de los datos actuales e históricos.

Datos adicionales sobre las categorías de URL y amenazas ofrecen una imagen completa y concluyente de la actividad de la red. La visibilidad a través del ACC lo ayuda a tomar decisiones informadas sobre las políticas y responder rápidamente a las potenciales amenazas de seguridad.

Tiempos de Respuesta Reducidos

El motor de correlación automatizada incorporado en el firewall de nueva generación descubre amenazas críticas que pueden estar ocultas en su red. Incluye objetos de correlación, definidos por el equipo de investigación de amenazas de Unit 42 de Palo Alto Networks, que identifican patrones de tráfico o secuencias de eventos sospechosos que indican objetivos maliciosos. Algunos objetos de correlación pueden identificar patrones dinámicos observados anteriormente a partir de muestras de malware en el servicio de prevención de malware WildFire®.

Sencillo Control de Políticas

La habilitación segura de aplicaciones implica permitir el acceso a aplicaciones específicas y protegerlas con políticas específicas para Threat Prevention y Quality of Service (Calidad de Servicio - QoS), además de filtrado de archivos, datos o URLs. Puede transformar su masiva base de reglas heredadas en una política intuitiva que fortalezca la seguridad y lleve mucho menos tiempo administrarla. Panorama le facilita establecer políticas con una única base de reglas de seguridad simplificando el proceso de importar, duplicar o modificar reglas a través de toda su red. La combinación del control administrativo global y regional sobre las políticas y los objetos le permite lograr un equilibrio entre una seguridad consistente a nivel global y la flexibilidad a nivel regional.

Gestión Centralizada Fácil de Usar

La implementación de grupos de dispositivos jerárquicos garantiza que los grupos de niveles inferiores hereden los parámetros de configuración de los grupos de niveles superiores. Esto agiliza la gestión centralizada y permite organizar los dispositivos según su función y ubicación sin que la configuración sea redundante. Pilas/agrupamiento de plantillas posibilitan una configuración optimizada de redes y dispositivos. Además, una interfaz de usuario común para los firewalls de nueva generación y para la administración tornan la gestión intuitiva. Funciones tales como Búsqueda General, comentarios de auditoría, universal unique identifier (identificador universal único - UUID) para todas las reglas y agrupamiento de reglas basado en etiquetas habilitan a sus administradores de TI para aprovechar toda la información de su red con facilidad.

Monitoreo de Tráfico: Análisis, Informes e Investigaciones Forenses

Panorama extrae logs (registros) de los firewalls, tanto físicos como virtuales, y de Traps™ advanced endpoint protection, y los almacena en su propio almacén de logs. Ante sus consultas de logs y generación de informes, Panorama extrae de manera dinámica los logs relevantes del almacén y presenta los resultados al usuario.

- **Log viewer (Visor de registros):** Ya sea para un dispositivo individual, para todos los dispositivos o para Traps, las actividades de logs se pueden ver rápidamente con el filtro dinámico de logs al hacer clic en un valor de celda o al usar el generador de expresiones para definir criterios de clasificación. También puede guardar los resultados para consultas futuras o exportarlos para un mayor análisis.

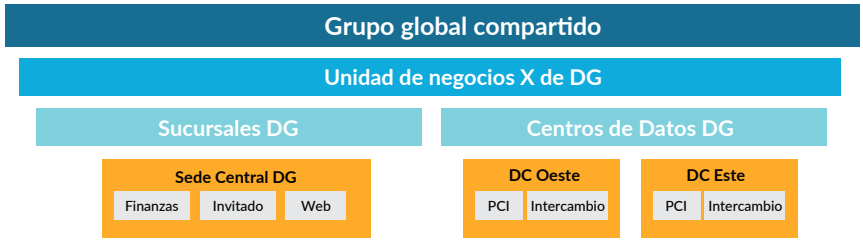

Figura 3: Jerarquía de Grupos de Dispositivos

Figura 4: Pilas/Agrupamiento de Plantillas

- **Informes personalizados:** Los informes predefinidos pueden usarse como están, personalizarse o agruparse en un informe para responder a requerimientos específicos.
- **Informes de actividad del usuario:** Estos informes muestran las aplicaciones usadas, las categorías de URL visitadas, los sitios web visitados y todas las URLs visitadas en un período determinado para usuarios individuales. Panorama elabora estos informes a partir de una visión agregada de la actividad del usuario, sin importar el dispositivo ni la IP del usuario ni qué firewall protege a determinado usuario.
- **Informes SaaS:** Un informe de uso y amenazas SaaS proporciona visibilidad detallada de toda la actividad Software as a Service (Software como servicio - SaaS) en los firewalls, así como las amenazas relacionadas.
- **Reenvío de logs:** Panorama puede reenviar logs recopilados de Traps y de todos sus firewalls de Palo Alto Networks a destinos remotos con distintos fines, como su almacenamiento prolongado, investigaciones forenses e informes de cumplimiento. Panorama puede reenviar todos los logs o solo los seleccionados, trampas Simple Network Management Protocol (Protocolo Simple de Administración de Red - SNMP) y notificaciones de correo electrónico a un destino remoto de generación de logs como un servidor Syslog (a través de UDP, TCP o SSL). Además, Panorama puede lanzar un flujo de trabajo y enviar logs a un servicio de terceros que proporcione una API basada en HTTP como un servicio de emisión de boletos o un producto de gestión de sistemas.

Arquitectura de Gestión Panorama

Panorama le permite gestionar sus firewalls de Palo Alto Networks con un modelo que proporciona supervisión global y control regional. Panorama ofrece múltiples herramientas para la gestión global o centralizada.

Plantillas/Pilas de Plantillas Agrupadas

Panorama gestiona la configuración de dispositivos y redes comunes a través de plantillas que se pueden utilizar para gestionar la configuración centralmente y aplicar cambios a los firewalls gestionados. Este enfoque evita la necesidad de realizar los mismos cambios individuales a los firewalls reiteradas veces a través de muchos dispositivos. Para facilitar aún más las cosas, las plantillas pueden agruparse y usarse como bloques de construcción durante la configuración de dispositivos y redes.

Grupos de Dispositivos Jerárquicos

Panorama gestiona las políticas y los objetos comunes a través de grupos de dispositivos jerárquicos. Los grupos de dispositivos de varios niveles se usan para gestionar de manera central las políticas a través de todas las ubicaciones de implementación con requerimientos comunes. Las jerarquías de grupos de dispositivos pueden ser creadas geográficamente (por ejemplo, Europa, América del Norte y Asia); funcionalmente (por ejemplo, centro de datos, campus principal y sucursales); como a partir de una combinación de ambas o basadas en otros criterios. Esto permite compartir las políticas comunes a través de diferentes sistemas virtuales de un dispositivo.

Se pueden usar políticas compartidas de control global y a la vez proveer a los administradores de firewalls regionales la autonomía para realizar ajustes específicos de acuerdo con sus requerimientos. A nivel de los grupos de dispositivos, se pueden crear políticas compartidas que estén definidas como el primer conjunto de reglas (reglas previas - pre-rules) y el último conjunto de reglas (reglas posteriores - post-rules) para que se evalúen según los criterios establecidos. Las reglas previas y posteriores pueden verse en un firewall gestionado, pero solo pueden editarse desde Panorama dentro del contexto de las funciones administrativas que hayan sido definidas. Las reglas de dispositivos, es decir, aquellas que están entre las reglas previas y las posteriores, pueden ser editadas por su administrador de firewall regional o un administrador de Panorama que haya cambiado a un contexto de dispositivo de firewall. Además, una organización puede usar objetos compartidos definidos por un administrador de Panorama, que pueden tomarse como referencia para las reglas de dispositivos gestionados a nivel regional.

Administración Basada en Funciones/Roles

La administración basada en funciones se usa para delegar el acceso administrativo de acuerdo con el nivel de funciones; esto incluye la disponibilidad de datos (habilitados, de solo lectura o deshabilitados y ocultos de visualización) para los diferentes integrantes de su personal.

Puede dar el acceso adecuado a personas específicas para las tareas que corresponden con su trabajo mientras otros accesos se dejan ocultos o de solo lectura. Los administradores pueden realizar o revertir cambios que hacen en la configuración de Panorama, independientemente de los cambios realizados por otros administradores.

Software, Actualización de Licencias y Gestión de Contenido

Según cómo avance su implementación, probablemente quiera asegurarse de que se envíen las actualizaciones hacia las estructuras inferiores de manera organizada. Por ejemplo, los equipos de seguridad pueden preferir calificar de forma central la actualización de un software antes de que sea enviado a través de Panorama a todos los firewalls de producción automáticamente. Panorama le permite gestionar centralmente el proceso de actualización para las actualizaciones de software, licencias y contenido; esto incluye actualizaciones de aplicaciones, firmas de antivirus, firmas de amenazas, entradas en la base de datos de URL Filtering, etc.

Al utilizar plantillas, grupos de dispositivos, administración basada en funciones y gestión de actualizaciones, puede habilitar el acceso adecuado a todas las funciones de gestión, herramientas de visualización, creación de políticas, generación de informes y generación de logs tanto a nivel global como regional.

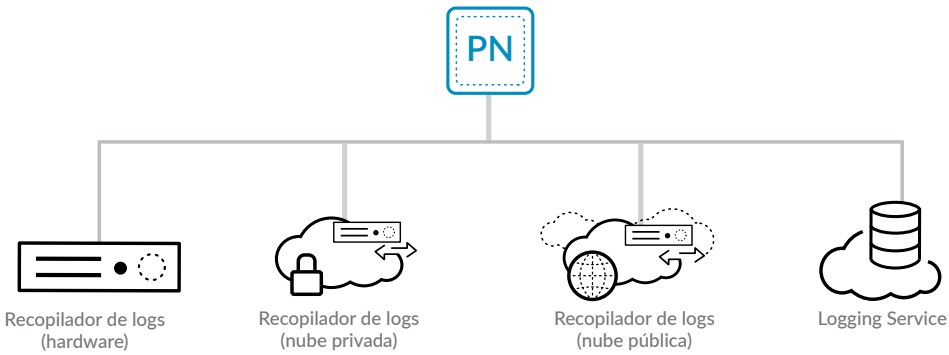

Figura 5: Administración de Logs (Registros) de Panorama

Flexibilidad de Implementación

Puede implementar Panorama como un dispositivo de hardware o como un dispositivo virtual.

Dispositivos de Hardware

Panorama puede implementarse como el dispositivo de gestión M-200, M-500 o M-600.

Dispositivos Virtuales

Panorama puede implementarse como un dispositivo virtual en VMware ESXi™ o en entornos de nube pública como Amazon Web Services, AWS® GovCloud, Microsoft Azure® y Azure GovCloud.

Modos de Implementación

Puede separar las funciones de gestión y generación de logs de Panorama mediante los modos de implementación. Los tres modos de implementación admitidos son los siguientes:

1. **Solo Gestión,** Panorama administra las configuraciones de los dispositivos gestionados, pero no recopila ni gestiona los logs.
2. **Panorama,** controla tanto las funciones de gestión de políticas como de logs para todos los dispositivos gestionados.
3. **Recopilador de Logs,** Panorama recopila y gestiona los logs de los dispositivos gestionados. Esto supone que otra implementación de Panorama está operando en el modo "Solo Gestión".

La separación entre gestión y recopilación de logs le permite optimizar su implementación de Panorama para cumplir con los requisitos de escalabilidad, organizacionales y geográficos. La elección del factor de forma y el modo de implementación le ofrece la máxima flexibilidad para gestionar los firewalls de nueva generación de Palo Alto Networks en una red distribuida.

Escala de Implementación

El plugin o complemento Panorama Interconnect conecta múltiples instancias de Panorama para escalar la gestión de firewalls a decenas de miles de firewalls. Al aprovechar el complemento, el Controlador de Panorama le permite sincronizar la configuración, activar firewalls rápidamente y programar actualizaciones de contenido desde una ubicación central (ver Figura 6) y, a su vez, simplificar la gestión de todos sus firewalls sin importar su ubicación, ya sea física o en la nube.

Nota: *Panorama Interconnect se admite solo en dispositivos M-600 o en VMs con recursos similares.*

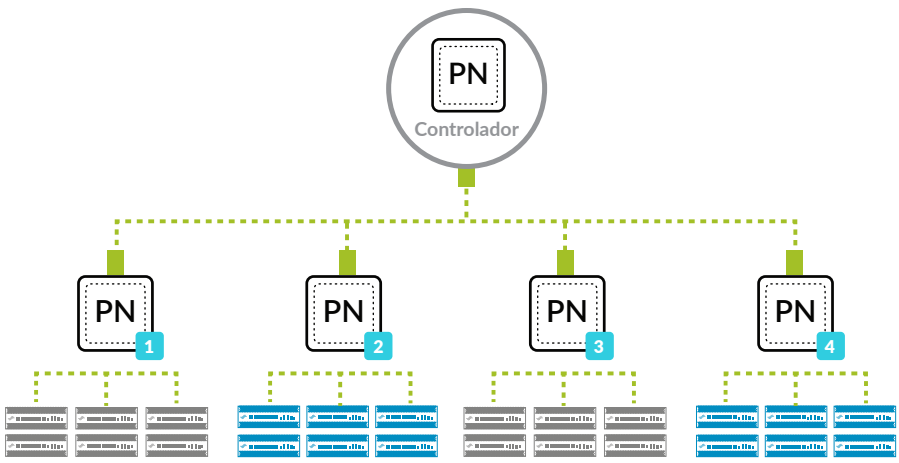

Figura 6: Configuración Sincronizada de Todos los Firewalls



	M-200	M-500	M-600
I/O	(4) 10/100/1000, [1] puerto serial de consola DB9, (1) puerto USB	(4) 10/100/1000, (1) puerto serial de consola DB9, (1) puerto USB, (2) 10 puertos GigE	(4) 10/100/1000, (1) puerto serial de consola DB9, (1) puerto USB, (2) 10 puertos GigE
Almacenamiento	Configuración máxima: 4 unidades de disco duro certificado RAID de 8 TB para 16 TB de almacenamiento RAID Configuración de envío predeterminada: RAID de 4 x 8 TB HDD certificado para 16 TB de almacenamiento RAID	Configuración máxima: RAID de 24 x 2 TB HDD certificado para 24 TB de almacenamiento RAID Configuración de envío predeterminada: RAID de 4 x 2 TB HDD certificado para 4 TB de almacenamiento RAID	Configuración máxima: RAID de 12 x 8 TB HDD certificado para 48 TB de almacenamiento RAID Configuración de envío predeterminada: RAID de 4 x 8 TB HDD certificado para 16 TB de almacenamiento RAID
Fuente de Alimentación/Consumo de Energía Máx.	Suministro de energía dual, configuración redundante de intercambio de calor 750 W/300 W	Suministro de energía dual, configuración redundante de intercambio de calor 1200 W/493 W (sistema total)	Suministro de energía dual, configuración redundante de intercambio de calor 750 W/486 W (sistema total)
BTU/hr. máximo	1 114 BTU/hr.	1 681 BTU/hr.	1 803 BTU/hr.
Voltaje de Entrada (Frecuencia de Entrada)	CA de 100 V a 240 V (de 50 Hz a 60 Hz)	CA de 100 V a 240 V (de 50 Hz a 60 Hz)	CA de 100 V a 240 V (de 50 Hz a 60 Hz)
Consumo de Corriente Máximo	9,5A a 110 VAC	4,2A a 120 VAC	4,5A a 220 VAC
Mean Time Between Failures (Tiempo Medio Entre Fallas - MTBF)	10 años	6 años	8 años
Montaje en Rack (Dimensiones)	1U, rack estándar de 19" (48,26 cm), 1,7" alto x 29" prof. x 17,2" ancho (4,32 cm alto x 73,66 cm prof. x 43,69 cm ancho)	2U, rack estándar de 19" (48,26 cm), 3,5" alto x 21" prof. x 17,5" ancho (8,89 cm alto x 53,34 cm prof. x 44,45 cm ancho)	2U, rack estándar de 19" (48,26 cm), 3,5" alto x 28,46" prof. x 17,2" ancho (8,9 cm alto x 72,29 cm prof. x 43,69 cm ancho)
Peso	26 libras (11,8 kg)	42,5 libras (19,28 kg)	36 libras (16,33 kg)
Seguridad	UL, CUL, CB	UL, CUL, CB	UL, CUL, CB
EMI	FCC Pieza 15, EN 55032, CISPR 32	Clase FCC A, Clase CE A, Clase VCCI A	FCC Pieza 15, EN 55032, CISPR 32
Entorno	Temperatura Operativa: 41 °F a 104 °F, 5 °C a 40 °C Temperatura No Operativa: -40 °F a 140 °F, -40 °C a 60 °C	Temperatura Operativa de 50 °F a 95 °F, de 10 °C a 35 °C Temperatura No Operativa de -40 °F a 158 °F, de -40 °C a 70 °C	Temperatura Operativa: 41 °F a 104 °F, 5 °C a 40 °C Temperatura No Operativa: -40 °F a 140 °F, -40 °C a 60 °C

Especificaciones de Panorama

Cantidad de Dispositivos Admitidos

- Hasta 5 000

High Availability (Alta Disponibilidad - HA)

- Activo/Pasivo

Autenticación del Administrador

- Base de datos local
- RADIUS
- SAML
- LDAP
- TACACS+

Herramientas de Gestión y APIs

- Graphical User Interface (Interfaz Gráfica de Usuario - GUI)
- Interfaz de Línea de Comandos
- REST API basado en XML y JSON

Nubes Públicas Compatibles

GCP, AWS, AWS GovCloud, Azure, Azure GovCloud

Especificaciones para el Hipervisor Privado

	Modo "Solo Gestión"	Modo Panorama	Modo de Recopilación de Logs
Núcleos Compatibles	4 CPUs	8 CPUs	16 CPUs
Memoria (mínimo)	8 GB	32 GB	32 GB
Unidad de Disco	Sistema de Disco de 81 GB	Almacenamiento de logs de 2 TB a 24 TB	Almacenamiento de logs de 2 TB a 24 TB

Tipos de Instancia de Nube Pública (Licencia BYOL)

	Modo "Solo Gestión"	Modo Panorama	Modo de Recopilación de Logs
Amazon AWS	t2.xlarge m4.2xlarge	m4.2xlarge m4.4xlarge	m4.4xlarge c4.8xlarge
Microsoft Azure	D4_V3 Standard D4S_V3 Standard	D16_V3 Standard	D16_V3 Standard D32_V3 Exceeds

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

panorama-ds-011419