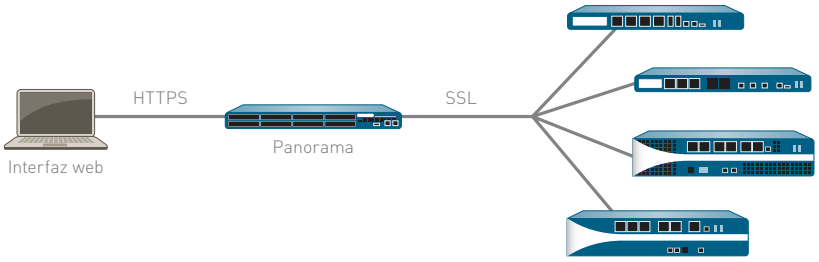
PANORAMA

Panorama ofrece administración centralizada de políticas y dispositivos en una red de firewalls de nueva generación de Palo Alto Networks.

- Muestra un resumen gráfico de las aplicaciones en la red, sus usuarios y el impacto potencial en la seguridad.
- Implementación centralizada de políticas corporativas para ser usadas junto con las políticas locales para una flexibilidad total.
- Delegación de las funciones adecuadas de gestión a nivel de equipo o a nivel global, gracias a la gestión basada en roles.
- Análisis, investigación y creación de informes de manera centralizada sobre el tráfico de red, los incidentes de seguridad y las modificaciones administrativas.



Las grandes organizaciones suelen tener muchos firewalls implementados en toda su red y, con bastante frecuencia, el proceso de administración y control es complicado debido a las complejidades e incoherencias entre los distintos dispositivos. El resultado es un aumento tanto en el esfuerzo necesario para su correcta administración como en los costes asociados.

Panorama ofrece gestión y visibilidad centralizada de los firewalls de nueva generación de Palo Alto Networks. Desde una ubicación central, los administradores podrán obtener una perspectiva de las aplicaciones, los usuarios y el contenido que atraviesa los firewalls. El conocimiento de lo que está en la red, junto con las políticas de habilitación segura de aplicaciones, maximiza la protección y el control y reduce al mínimo el esfuerzo de administración. Los administradores pueden llevar a cabo análisis centralizados, generar informes y realizar investigaciones forenses con los datos agregados hasta el momento, o sobre los datos almacenados localmente en cada firewall.

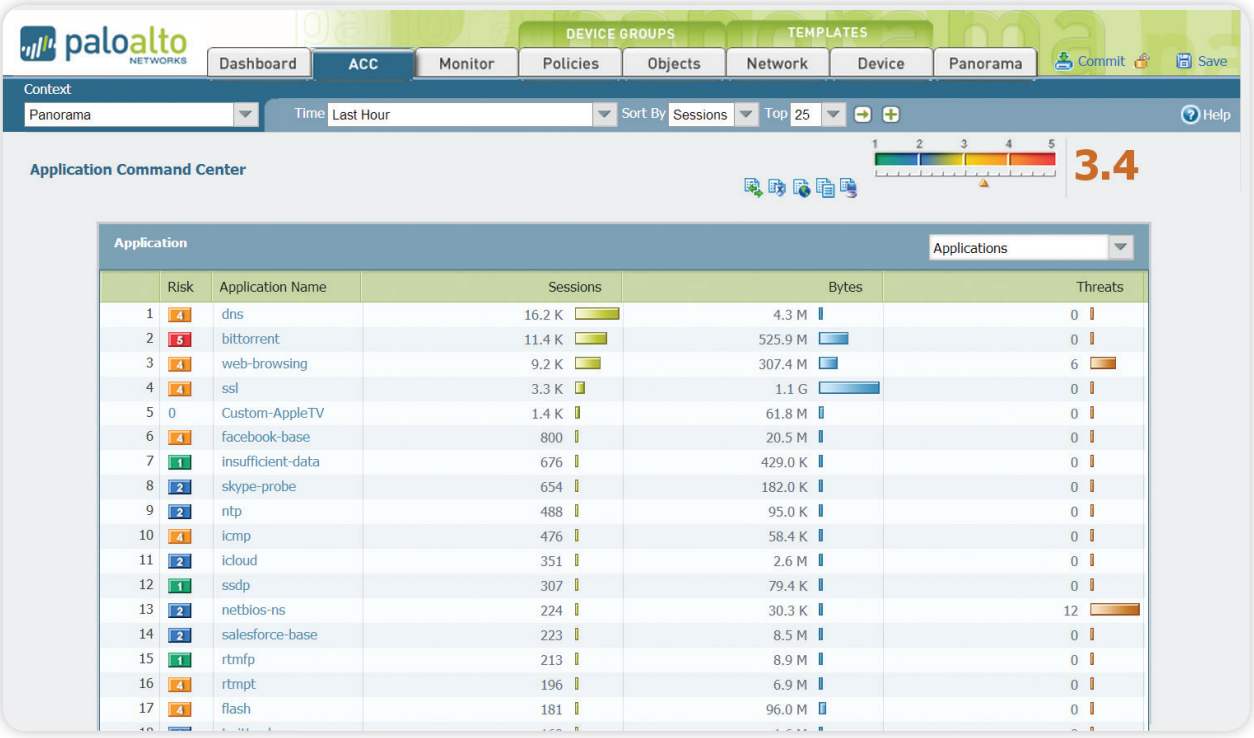
Tanto Panorama como los distintos dispositivos comparten el mismo aspecto y funcionamiento basado en web, minimizando la curva de aprendizaje o la demora en la ejecución de la tarea pertinente. Palo Alto Networks adopta una filosofía de gestión que prioriza la coherencia, ofreciendo una ventaja significativa respecto a las ofertas de la competencia.

Visibilidad central: Application Command Center:

El Application Command Center (ACC) de Panorama ofrece al administrador una visión gráfica de las aplicaciones, las URL, las amenazas y los datos (archivos y patrones) que pueden estar atravesando cualquiera de los dispositivos de Palo Alto Networks supervisados. ACC obtiene dinámicamente los datos de cada dispositivo ofreciendo a los administradores una visión actualizada de las aplicaciones en la red, quién las utiliza y las amenazas potenciales que puedan representar. Los administradores pueden investigar las aplicaciones nuevas o las que no les resulten familiares con un solo clic, mostrando una descripción de la aplicación, sus principales características, sus patrones de comportamiento y quién está utilizándolas.

Los datos adicionales sobre las categorías de URL y las amenazas proporcionan una visión completa y detallada de la actividad de la red. La visibilidad desde ACC permite a los administradores tomar decisiones sobre políticas y responder rápidamente a las amenazas potenciales de seguridad.

paloalto NETWORKS
the network security company™



Application Command Center ofrece una visión tanto a nivel global como local sobre el tráfico de las aplicaciones, pudiendo realizar un desglose completo del mismo y obteniendo aún más información acerca de la actividad actual.

Control global de políticas: habilitación segura de aplicaciones

La habilitación segura de aplicaciones permite el acceso a aplicaciones específicas con prevención de amenazas concretas y aplicación de políticas de filtrado de archivos, datos o URL. Panorama facilita la habilitación segura de aplicaciones en toda la red de firewalls permitiendo a los administradores gestionar las reglas desde una ubicación central.

Las políticas compartidas en las que se basa Panorama ayudan a garantizar el cumplimiento de los requisitos internos o las regulaciones existentes, mientras que las reglas locales en los dispositivos garantizan la seguridad y la flexibilidad. Combinando el control administrativo centralizado y el control local sobre las políticas y los objetos, se consigue encontrar un equilibrio entre la seguridad coherente a nivel global y la flexibilidad a nivel local.

Los administradores pueden implementar políticas que habiliten de forma segura las aplicaciones o algunas funciones de las aplicaciones en base a los usuarios, gracias a la integración con los servicios de directorio, mientras que la prevención de amenazas específicas para las aplicaciones protegen el contenido y la red. La capacidad de establecer una política única que habilite de forma segura las aplicaciones en base a los usuarios –y no a las direcciones IP- permite a las organizaciones reducir drásticamente el número de políticas necesarias. Un beneficio adicional de la integración con los servicios de directorios es una reducción drástica en los gastos administrativos asociados a las altas, cambios y movimientos de empleados que pueden producirse en el día a día. Las políticas de seguridad se mantienen estables mientras los empleados se mueven de un grupo a otro.

Supervisión del tráfico: análisis, generación de informes e investigación forense

Panorama utiliza el mismo conjunto de potentes herramientas de supervisión y creación de informes disponibles a nivel de administración local de dispositivos y añade la posibilidad de tener una visión agregada de la actividad. Los administradores realizan consultas al log y generan informes, y Panorama extrae dinámicamente los datos más actualizados directamente desde los firewalls administrados o desde los logs reenviados a Panorama. El acceso a la información más actualizada en cualquier dispositivo permite a los administradores hacer frente a los incidentes de seguridad, así como tomar una acción proactiva para proteger los activos corporativos.

- **Visor del log:** tanto para un dispositivo individual, como para la totalidad de los dispositivos, los administradores de Panorama pueden ver rápidamente la actividad del log mediante el filtrado dinámico del mismo haciendo clic en el valor de una celda y/o utilizando el generador de expresiones para definir los criterios de ordenación. Los resultados se pueden guardar para futuras consultas o ser exportados para su posterior análisis.
- **Creación de informes personalizados:** los informes predefinidos se pueden utilizar tal y como están, o bien pueden personalizarse o agruparse en un solo informe, adaptándose a los requisitos específicos.
- **Informes de la actividad de los usuarios:** en Panorama, un informe de actividad de usuarios muestra las aplicaciones utilizadas, las categorías de URL y los sitios web visitados, y todas las URL visitadas durante un período específico de tiempo para un usuario en particular. Panorama construye los informes utilizando una visión global de la actividad de los usuarios, sin importar el firewall por el que estén protegidos, la IP o el tipo de dispositivo que estén utilizando.

Arquitectura de administración de Panorama

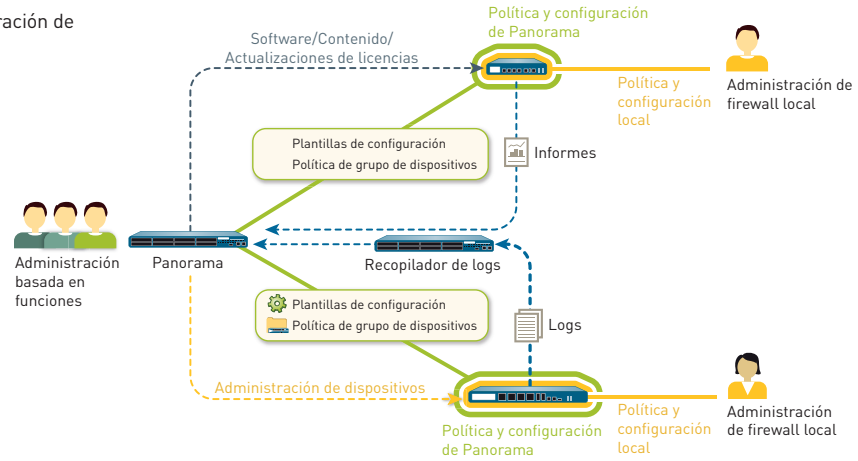
Panorama permite que las organizaciones administren sus firewalls de Palo Alto Networks utilizando un modelo que proporciona tanto supervisión central como control local. Panorama proporciona una serie de herramientas para la administración centralizada:

- **Plantillas:** panorama administra los dispositivos más comunes y la configuración de la red mediante plantillas. Las plantillas se pueden utilizar para administrar la configuración de forma centralizada y después enviar los cambios a todos firewalls administrados. Esta forma de trabajar evita hacer el mismo cambio individual en un firewall repetitivamente en muchos dispositivos. Un ejemplo de este uso es enviar configuraciones de servidor NTP y DNS comunes a cientos de firewalls, en lugar de repetir el mismo cambio en cada uno de los dispositivos individualmente.
- **Grupos de dispositivos:** panorama administra políticas y objetos comunes en grupos de dispositivos. Los grupos de dispositivos se utilizan para administrar de forma centralizada las bases de reglas de muchos dispositivos con requisitos comunes. Algunos ejemplos de formas de agrupar los dispositivos pueden ser por ubicación geográfica (Europa y Norteamérica) o por su funcionalidad (centro de datos o perimetral). Dentro de los grupos de dispositivos, los sistemas virtuales se tratan como dispositivos individuales, al mismo nivel que los firewalls físicos. Esto permite compartir bases de reglas comunes en diferentes sistemas virtuales para un mismo dispositivo.

  Las organizaciones pueden utilizar políticas compartidas para el control central, proporcionando al administrador del firewall la autonomía necesaria para hacer ajustes específicos según las necesidades locales. En el nivel de grupo de dispositivos, los administradores pueden crear políticas compartidas que se definen como el primer conjunto de reglas (reglas previas) y el último conjunto de reglas (reglas posteriores) que se evaluarán respecto a criterios de coincidencia. Las reglas tanto previas como posteriores pueden verse en un firewall administrado, pero solo se pueden editar desde Panorama dentro del contexto de las funciones administrativas definidas. Las reglas locales de los dispositivos (aquellas reglas que se encuentran entre las previas y las posteriores) se pueden editar tanto por un administrador local, como por un administrador de Panorama que haya cambiado a un contexto de firewall local. Además, una organización puede utilizar objetos compartidos definidos por un administrador de Panorama, que pueden hacer referencia a reglas de dispositivos administrados a nivel local.
- **Administración basada en funciones:** las organizaciones pueden utilizar la administración basada en funciones para delegar el acceso administrativo a nivel de función (activado, solo lectura, o deshabilitado y oculto a la vista) a diferentes miembros del personal. Determinados administradores pueden tener acceso a tareas correspondientes a su trabajo, mientras que otros accesos están ocultos o son de solo lectura. Un ejemplo de cómo se puede utilizar este tipo de control de acceso es definir roles diferentes para el personal responsable de las diferentes tareas en toda la empresa, como por ejemplo administradores de seguridad frente a administradores de red. Todos los cambios realizados por un administrador se registran, mostrando la hora del evento, el administrador, la interfaz de administración utilizada (interfaz de usuario web, CLI, Panorama), el comando o la acción realizada.
- **Administración de actualizaciones de software, contenidos y licencias:** a medida que una implementación crece en tamaño, muchas organizaciones quieren asegurarse de que las actualizaciones se envían a los elementos jerárquicamente inferiores de manera organizada. Por ejemplo, los equipos de seguridad prefieren valorar centralmente una actualización de software antes de su entrega a través de Panorama para todos los firewalls de producción a la vez. Usando Panorama, el proceso de actualización se puede administrar de forma centralizada para las actualizaciones de software, de contenidos (actualizaciones de aplicaciones, firmas de antivirus, firmas de amenazas, base de datos de filtrado de URL, etc.) y de licencias.

Usando plantillas, grupos de dispositivos, administración basada en funciones y administración de actualizaciones, las organizaciones pueden delegar el acceso a todas las funciones de administración: herramientas de visualización, creación de políticas, creación de informes y logs, tanto a nivel global como a nivel local.

Panorama permite a las organizaciones equilibrar la administración centralizada y local mediante plantillas, grupos de dispositivos, administración basada en funciones, así como la administración de actualizaciones



Flexibilidad de implementación

Las organizaciones pueden implementar Panorama como un dispositivo hardware o como un dispositivo virtual.

Dispositivo hardware

Las organizaciones que prefieran implementar Panorama sobre hardware dedicado de alto rendimiento, o que deseen separar la administración de Panorama y las funciones de log en caso de grandes volúmenes de logs de datos, pueden utilizar el dispositivo de hardware M-100 para satisfacer sus necesidades. Panorama sobre M-100 se puede implementar de las siguientes maneras:

- **Centralizado:** en este caso, toda la administración de Panorama y las funciones de logging se consolidan en un solo dispositivo (con opción de alta disponibilidad
- **Distribuido:** una organización puede preferir separar la administración y las funciones de logging en múltiples dispositivos. En esta configuración, las funciones se dividen entre administradores y recopiladores de logs.
    - **Administrador de Panorama:** el administrador de Panorama es responsable de gestionar las tareas relacionadas con la configuración de políticas y dispositivos en todos los equipos administrados. El administrador no almacena datos de log a nivel local, sino que utiliza recopiladores de logs independientes para manejar los datos de logging. El administrador analiza los datos almacenados en los recopiladores de logs para la generación centralizada de informes.
    - **Recopilador de logs de Panorama:** las organizaciones con grandes volúmenes de logs y con requisitos de conservación de los mismos pueden implementar dispositivos recopiladores de logs de Panorama dedicados que agregarán información de los logs de varios firewalls administrados.

La separación entre la administración y la recopilación de logs permite a las organizaciones optimizar su implementación con el fin de cumplir con los requisitos de escalabilidad, de organización o de ubicación geográfica.

Dispositivo virtual

Panorama puede implementarse como un dispositivo virtual en VMware ESX(i), lo que permite a las organizaciones mantener sus iniciativas de virtualización y consolidar el espacio en los racks de un centro de datos, que a menudo es limitado o costoso. El dispositivo virtual se puede implementar de dos maneras:

- **Centralizado:** toda la administración de Panorama y las funciones de logging se consolidan en un solo dispositivo virtual (con opción de alta disponibilidad).
- **Distribuido:** la recopilación de logs distribuida de Panorama permite la combinación de dispositivo hardware y virtuales.
    - **Administrador de Panorama:** el dispositivo virtual puede servir como administrador de Panorama y es responsable de gestionar las tareas relacionadas con la configuración de políticas y dispositivos en todos los equipos administrados.
    - **Recopilador de logs de Panorama:** los recopiladores de logs de Panorama son responsables de realizar las tareas intensivas de recopilación y procesamiento de logs, y pueden ser implementados utilizando el M-100. El dispositivo virtual no puede utilizarse como un recopilador de logs de Panorama.

Con la posibilidad de elegir entre hardware o una plataforma virtualizada, así como contando con la opción de combinar o separar las funciones de Panorama, se ofrece a las organizaciones máxima flexibilidad para la administración de múltiples firewalls de Palo Alto Networks en un entorno de red distribuido.
Especificaciones de Panorama

ESPECIFICACIONES DE PANORAMA

Número de dispositivos admitidos	Hasta 1.000
Alta disponibilidad	Activo/Pasivo
Autenticación del administrador	Base de datos local RADIUS

ESPECIFICACIONES DEL DISPOSITIVO DE ADMINISTRACIÓN M-100

E/S

- (1) 10/100/1000, (3) 10/100/1000 (para usos futuros), (1) puerto serie de consola DB9

ALMACENAMIENTO (DOS OPCIONES)

- M-100 1 TB RAID: 2 x 1 TB disco duro certificado RAID para 1 TB de almacenamiento RAID
- M-100 4 TB RAID: 8 x 1 TB disco duro certificado RAID para 4 TB de almacenamiento RAID

FUENTE DE ALIMENTACIÓN/CONSUMO ELÉCTRICO MÁXIMO

- 500 W/500 W

BTU/H MÁXIMO

- 1.705 BTU/h.

VOLTAJE DE ENTRADA (FRECUENCIA DE ENTRADA)

- 100-240 VAC (50-60 Hz)

CONSUMO MÁXIMO DE CORRIENTE

- 10 A a 100 VAC

TIEMPO MEDIO ENTRE FALLOS (MTBF)

14,5 años

PREPARADO PARA MONTAJE EN BASTIDOR (DIMENSIONES)

- 1U, bastidor estándar de 19"
  (4,45 x 43,18 x 43,18 cm – 1,75 x 23 x 17,2 pulgadas)

PESO (SOLO DISPOSITIVO/DISPOSITIVO PREPARADO PARA ENVÍO)

- 12,11 Kg/15,88 Kg

SEGURIDAD

- UL, CUL, CB

INTERFERENCIA ELECTROMAGNÉTICA

- Clase A de FCC, Clase A de CE, Clase A de VCCI

ENTORNO

- Temperatura de funcionamiento: De 5 a 40 ºC (de 40 a 104 ºF)
- Temperatura de almacenamiento: De -40 a 65 ºC (de -40 a 149 ºF)

ESPECIFICACIONES DEL DISPOSITIVO VIRTUAL

REQUISITOS MÍNIMOS DEL SERVIDOR

- Disco duro de 40 GB
- 4 GB RAM
- Quad-Core CPU (2GHz+)

SOPORTE VMWARE

- VMware ESX 4.1 o posterior

NAVEGADOR

- IE v7 o posterior
- Firefox v3.6 o posterior
- Safari v5.0 o posterior
- Chrome v11.0 o posterior

ALMACENAMIENTO PARA LOGGING

- VMware Virtual Disk: Máximo 2 TB
- NFS

paloalto NETWORKS
the network security company™

3300 Olcott Street
Santa Clara, CA 95054

Accueil : +1.408.573.4000
Ventes : +1.866.320.4788
Assistance : +1.866.898.9087

www.paloaltonetworks.com