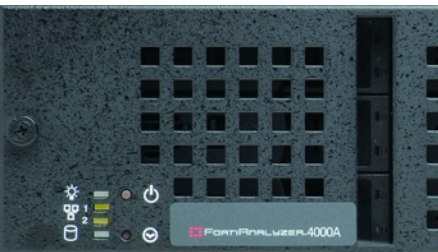


FortiAnalyzer “virtual”

Servicio FortiAnalyzer gestionado



FORTINET[®]

¿En qué consiste?

Servicio de *log*, análisis e informes de soluciones Fortinet sustentado en equipos FortiAnalyzer de gama alta.

Registra tráfico de red, eventos, virus, ataques, contenido web, e-mail, etc. y proporciona cuarentena, correlación de eventos, análisis de tráfico y archivado de contenido.

Beneficios

Evita la necesidad de adquirir un equipo FortiAnalyzer en aquellas redes donde su importe no quede suficientemente justificado, bien por que el número de equipos a monitorizar es reducido, se requiera para un análisis puntual, etc. proporcionando similares funcionalidades a un equipo FortiAnalyzer local.

Gracias a la correlación de eventos permite a los administradores de sistemas identificar y reaccionar rápidamente frente a problemas de seguridad en su red.

Dispone de gran variedad de informes predefinidos, al tiempo que permite su personalización, lo que facilita la monitorización de eventos, actividad y amenazas.

Registra todo tipo de actividad, lo que facilita el cumplimiento de normas regulatorias o de normativa interna de la compañía.

Proporciona archivado centralizado del correo electrónico, mensajería instantánea, transferencias de ficheros, tráfico web y permite la cuarentena de ficheros infectados, lo que permite su posterior recuperación.

Permite la monitorización en tiempo real de la red, tráfico y eventos de usuario; lo que facilita la evaluación de posibles amenazas de seguridad, prestaciones de la red y comportamiento de los usuarios.

El análisis forense provee un método para monitorizar y generar informes del tráfico de red, correo electrónico y mensajería instantánea de cada usuario o grupo de usuarios de acuerdo a los patrones establecidos por la compañía.

Funcionalidades
FortiAnalyzer en
modalidad pago por
uso a mínimo coste

Conocer lo que sucede en la red ayuda a prevenir incidentes

The screenshot displays the FortiAnalyzer 800 management interface. The top section shows a log table with columns for Date, Log ID, Log Type, Traffic, and various interface details. Below the logs, there are sections for 'Webfilter activity' and 'Top Allowed Categories'. The 'Top Allowed Categories' section includes a table of frequently accessed categories and a corresponding pie chart.

Category	Events	% of Total
Search Engines	202631	17.26%
Information Technology	178489	15.20%
News and Media	163654	13.94%
Advertising	107163	9.13%
Business	94070	8.01%
Reference	80707	6.87%
Sports	58563	4.99%
Shopping and Auction	56607	4.82%
Travel	42858	3.65%
Web-based Email	31718	2.70%
Other	157477	13.41%
Total	1173937	100.00%

Características

- Acceso web cifrado y restringido por IP
- Gestión de logs
- Informes personalizados
- Monitorización en tiempo real y alertas
- Tracking de la actividad de los usuarios
- Archivado de contenido
- Data Mining
- Servicios opcionales de backup cifrado
- Dominio ADOM independiente
- Almacenamiento en RAID
- Conectividad y alimentación redundantes