

FortiAnalyzer "Virtual"

Servicio FortiAnalyzer gestionado

Servicio de *log*, análisis e informes de soluciones Fortinet y otros dispositivos compatibles *syslog* 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, evaluación de vulnerabilidades, 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 (número de equipos a monitorizar reducido, análisis puntual, etc.).

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 y tráfico web; realiza 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, no disponible en FortiAnalyzer-100, provee un método para monitorizar y generar informes del tráfico de internet, correo electrónico y mensajería instantánea de cada usuario o grupo de usuarios de acuerdo a los patrones establecidos por la compañía.



Características

- Acceso web cifrado.
- Conexión cifrada equipos FortiGate.
- Gestión de *logs*.
- Más de 300 informes predefinidos.
- Informes personalizados.
- Informes específicos FortiClient.
- Monitorización en tiempo real.
- *Tracking* actividad usuarios.
- Soporte para informes FortiGuard.
- Alertas.
- Archivado contenido.
- Cuarentena de ficheros.
- *Data Mining*.
- Servicios opcionales de *backup* cifrado.

Especificaciones

- Dominio ADOM independiente.
- Soporte hasta FortiGate-800, FortiClient y dispositivos *syslog*.
- Almacenamiento en RAID.
- Alojado CPD.
- Conexiones redundantes.
- Alimentación redundante.
- SAIs redundantes.
- Aislado físicamente resto equipos CPD.