

Security Analyzer FortiReporter

Fortinet has partnered with eIQnetworks to deliver the FortiReporter tool, a software-based security reporting and analysis solution. A part of the Fortilog, the FortiReporter provides information that enables users to understand and manage their networks, spot and repel attacks.

FortiReporter Security Analyzer includes more than 400 reporting options. It is a browser-based solution that allows users to combine data and generate reports from multiple, geographically distributed security devices. It easily installs on any off-the-shelf server platform and can collect and analyze data from the full range of FortiGate Antivirus Firewall models and across all functions - including firewall, antivirus, VPN, content filtering, IDS, IPS and traffic shaping. FortiReporter Security Analyzer can process up to 40 GB of syslog data per day from a large number of security devices - decreasing report processing time and enabling the delivery of instant reports.

Reports can be delivered in multiple languages and formats - including HTML, MS Word and MS Excel. Users can generate and access reports remotely from a secure Internet connection via a Web-browser. Reports can also be sent easily via e-mail or be aggregated into individual Web portals.

FortiReporter Security Analyzer also provides in-depth overviews of virus and worm activity and enables critical correlation to help IT administrators minimize response times and takes proactive measures to reduce network vulnerabilities.

Contact:

Tech pac

Tel: (022) 55960238

Fax: (022) 55960106

Website: www.fortinet.com.

Security Appliance VirusWall

Trend Micros (TM) recently introduced the TM Network VirusWall, an outbreak prevention appliance designed to scan, detect, and block threats in a company's network. The device allows security administrators to block network viruses and identify vulnerable or non-compliant network devices to help mitigate or eliminate the propagation point for internal outbreaks.



Network VirusWall can detect and block network viruses even within a data packet. So embedded worms such as "Worm_Sasser", "MSBlaster", and "Slammer" are completely taken care of. This function can be critical for data intensive companies.

The Network VirusWall plugs into the network LAN segments and from there it checks every new user for security standards. So, with the help of tools such as the TM Control Manager 3.0 and Outbreak Prevention Services, the VirusWall enables enforcement of security policies at a centralized location.

With this product In the VirusWall TM also introduced the TM Vulnerability Assessment, which allows administrators to isolate vulnerable devices from the rest of the network.