

Get better ROI on firewall investments

Investing in a best-of-breed firewall gives companies excellent protection against security threats but they could be missing real insight into what's really happening on the firewall - and who is doing what on the web. The result: the firewall is not leveraged to its fullest potential.



Image: www.freedigitalphotos.net

"A lot of South African companies have invested in Fortigate Firewalls because they are without a doubt the world's leading and most-trusted UTM firewalls. However, poor monitoring and lack of visibility of what's happening on the firewall means companies aren't getting real return on their investment," says Richard Broeke, national sales manager at Securicom, a managed IT security services vendor which distributes logMojo's innovative, cloud-based reporting service for Fortigate Firewalls on the African Continent.

He says companies could be getting greater return on their investment in Fortigate technologies with better monitoring and reporting tools.

"Stock standard monitoring capabilities don't deliver the type of actionable intelligence required to fine-tune the configuration and management of the firewall, or empower appropriate control over web usage.

"Companies for instance can control which websites users can and can't visit, but they have no insight into what they are doing on the websites they are permitted to go to. They also know when usage quotas have been reached, but they don't know which users were responsible, who spent the most time online, or what the bandwidth was used for.

Monitor usage behaviour

"To really get control over users' web usage and web security, you want the ability to monitor usage behaviour in real time on a per user or per website basis for instance. This allows for the proactive management of quotas and enforcement of fair usage," explains Broeke.

According to Broeke, the logMojo security incident and event management (SIEM) solution provides unparalleled capabilities for monitoring reporting on Fortigate Firewalls and delivers actionable insight that ensures companies leverage the true power of the technology.

logMojo can identify atypical situations such as an abnormal number of firewall sessions, SMTP traffic, DNS traffic, bandwidth usage and more. It also identifies when a unit's configuration is not being backed up. logMojo can further identify issues that are occurring in real-time to include identification of FortiGate units which are off-line or non-responsive as well as real-time firewall session monitoring.

Dashboards provide real-time visibility and updates of individual, custom groups, or multiple FortiGate devices from a single portal.

The Real-Time Session Monitor provides real-time detailed and, more importantly, summarised information about the bandwidth and active sessions on the FortiGate. It can quickly answer the ever popular question of "Who or what is using all of the bandwidth?"

Filtering of reports by FortiGate device, interface, users, user groups, services, and IP addresses allows for very specific reports to be created. The easy-to-understand reports can be configured to be automatically emailed to managers and department heads for review of their employees' internet usage and security events.

"Monitoring and reporting on the Fortigate at this level enables more effective internal cost centre analysis so that IT can recover costs from different business units based on usage. Importantly, real time data on the health and performance of the Fortigate ensures that the configuration of the technology can be proactively adapted to address new threats or vulnerabilities that would otherwise have gone undetected. This is when the capabilities of the technology are truly leveraged," concludes Broeke.

For more, visit: <https://www.bizcommunity.com>