

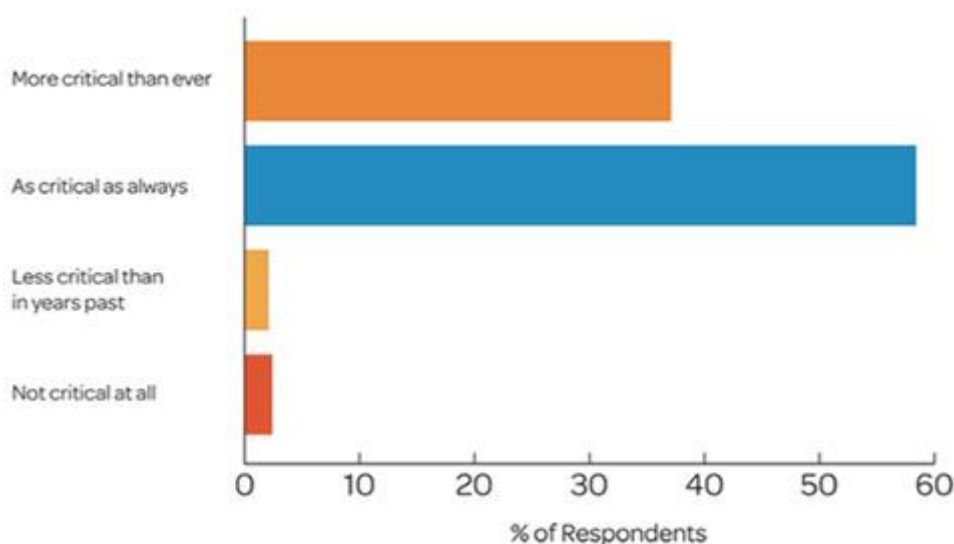
# HELP NET SECURITY

## Firewall: The king of network security

Posted on 03 March 2015.

A new FireMon report, based on a survey of over 700 network security practitioners, reveals that [firewalls](#) remain highly strategic to organizations' current and future security strategies – with an overwhelming 92 percent of respondents indicating that firewalls will stand as a “critical” component of their security infrastructures for the foreseeable future.

How critical is the network firewall as part of your overall security architecture today?



This prevailing view is not without challenges as the study also found significant, persistent and widespread management issues, most notably related to firewall policy complexity.

Conducted in Q4 2014, the survey drew response from practitioners including management, operations and audit officials working in leading vertical markets such as financial services, business services and government; more than 60 percent of respondents represented large organizations with 1,000 or more employees.

The overriding interest of the study was to surface current perceptions on the role that firewall infrastructure continues to play in the larger domain of network security management, in particular related to emerging trends such as adoption of next-generation firewalls (NGFWs), cloud computing and SDN.

The report revealed two other key trends: NGFWs have gained adoption in nearly every organization surveyed, but not without introducing their own set of related management concerns. Perhaps even more surprisingly, survey respondents affirmed that firewalls will play a significant role in the adoption and security management of emerging network paradigms including cloud computing, software-defined networking (SDN) and DevOps.

<http://www.net-security.org/secworld.php?id=18029>

Specific results include:

- 92% of respondents indicated that firewalls will be a “critical” component of their security infrastructures over the next five years.
- 88% of respondents indicated that they have already deployed NGFWs, with 25% indicating that NGFWs already account for over half their existing systems.
- Respondents indicated that traditional or NGFW devices play a valuable role in securing virtualised environments (87%) and cloud-based computing platforms (58%).
- On the whole, respondents cited API integration capabilities as a more important factor than price/performance when acquiring new firewall devices.

“Previous observations that the ‘firewall is dead’ were clearly premature or overstated,” said Jody Brazil, CEO of FireMon. “Not only do today’s practitioners consider firewalls as critical an element of their network security strategy as ever, but they also see a crucial role for the firewall within evolving paradigms including the cloud and SDN, which may surprise some industry watchers.”

Brazil continued: “At the same time, firewall policy management remains a significant challenge. In a typical large enterprise, 35-40% of firewall rules are redundant, hidden or lack a business purpose – and two-thirds of policies are completely unnecessary. When you juxtapose these conditions with research such as the forthcoming Verizon Enterprise Solutions PCI Report – which finds that firewall management remains one of the greatest threats to network security compliance – it’s clear this is a situation that commands a lot of attention.”

<http://www.net-security.org/secworld.php?id=18029>