



ADVERTISEMENT

CLOUD COMPUTING MAKING IT WORK FOR BUSINESS

Benefit from cloud computing while keeping your data secure

[> Find out more](#)

silicon.com

Microsoft

This story was printed from ZDNet UK, located at <http://www.zdnet.co.uk/>

Blog Post URL: <http://www.zdnet.co.uk/blogs/back-office-10012454/next-gen-firewalls-go-head-to-head-10021658/>

Next-gen firewalls go head-to-head

By manek, 9 February, 2011 13:36

A pair of security vendors, Palo Alto Networks and Sourcefire, debated the various merits of their approaches to unified security live on stage at NetEvents in Barcelona today.

The spirited debate was moderated by Rick Moy, CEO of security testing company NSS Labs, and saw two fundamentally different approaches to securing the enterprise datacentre with next-generation firewalls compared.

Nir Zuk, CTO of Palo Alto, and Jason Brevnik, VP security strategy at Sourcefire, stood at either end of the stage as Moy opened the discussion. He described the threat landscape as having changed over the last four years.

Introducing the debate, Moy said that, previously, attacks originated predominantly from external hackers to today's client-side threats. The main attack vectors now consist of the likes of Twitter and Facebook, he said. The problem is that enterprise security systems generally assume that any response to a request from inside the organisation, such a link clicked in a Facebook page, is safe. Instead, said Moy, systems now need to parse incoming traffic.

Zuk and Brevnik compared their differing approaches to security. Zuk said that, in the event for example of a user plugging in a USB stick containing malware, his company's next-generation firewall would not let a machine on the network, unless it was running the right security agent.

Brevnik said: "You can't scan for everything," referring to the need to view all data. Zuk said: "You're being too PC-centric. You need 10 gigabit per second wirespeed protection. My product can do that and doesn't slow down."

Brevnik questioned whether a full 10 gigabit per second was always needed. He said that people do cost-benefit analyses on whether they need full wirespeed. Moy said that real world testing by NSS Labs shows that products often run at about 50 percent of rated throughput.

Brevnik said that next-generation firewalls collapse numerous existing security functions into a single box. He said: "Will a next-generation firewall be deployed in the core? It's more likely you'll want deep packet inspection and intrusion protection in the datacentre."

Another point of contention concerned speed of deployment of next generation firewalls. Zuk said: "Our customers are saving 60 percent on opex [operational expenditure] of their network security budget over three years by switching to our next-generation firewall. It needs fewer people to manage it. But that's not enough - and is why UTM [unified threat management] is not successful."

Brevnik said: "It will take a long time for wholesale change to occur. Enterprises don't just rip and replace. Change is slow because people are used to doing what they do."

Copyright © 1998-2011 CBS Interactive Limited. All rights reserved