Executive Summary

Network Performance and Security

CIOs and CISOs can avoid risky tradeoffs and boost threat defenses by deploying next-generation firewalls built for both security and network performance now.

In recent years, the network firewall has evolved from a relatively simple security appliance to assume a prominent role in the enterprise's cybercrime defenses. Next-generation firewalls (NGFWs) represent the state of the art, incorporating features such as intrusion prevention, anti-malware, and deep packet inspection (DPI), technologies formerly implemented as separate point solutions.

These capabilities are essential tools in the fight against increasingly sophisticated attacks known as advanced persistent threats (APTs). As security experts were developing ways to defend against APTs, cybercriminals came up with new ways to defeat those defenses, the so-called advanced evasion techniques (AETs).

Though essential in the fight against APTs and AETs, enabling advanced protections on NGFWs can adversely affect network performance—sometimes dramatically. In response to users' complaints about poor application responsiveness, system administrators often disable key NGFW features such as DPI to restore performance levels. This action creates an existential tug-of-war between security administration's mandate to keep the business safe from intruders and network operation's requirement to ensure employee and customer usability and productivity. Compounding the problem, most CIOs and CISOs don't even know that tradeoffs are being made by their operations staff—until it's too late.

Faced with this troubling situation, IT executives must act. For starters, they need to institute internal training programs and awareness campaigns to ensure that every person in the IT organization understands the nature of advanced threats and the security implications of their actions. Fostering collaboration between operations and security leads to a more proactive stance and coordinated response to security incidents. Most importantly, CIOs and CISOs should aggressively push to deploy NGFWs that eliminate the performance-security tradeoff, boost proactive defenses against advanced threats, and improve IT staff efficiency.

Upgrading firewalls can meet with resistance from budget-conscious executive staffs, particularly when the proposed firewall replacement is ahead of a planned refresh cycle. In this event, the CIO or CISO must build a convincing financial case, documenting benefits such as risk mitigation, productivity increases, and infrastructure cost reductions from real-world deployments.

The evaluation process must include internal testing of candidate offerings based on the organization's individual performance and scalability needs. Testing should also verify that the NGFW is effective in detecting APTs, especially those employing AETs.

CIOs and CISOs who follow these recommendations will not only improve the effectiveness of both users and IT staff, but they will be successful in their most important job—protecting their organization's invaluable data assets and customer information.

To read the complete white paper on Network Performance and Security, click here (**www.mcafee.com/us/resources/reports/rp-network-performance-security.pdf**). For more information on McAfee Next Generation Firewalls, visit **www.mcafee.com/ngfw**.

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com