

Antivirus Protection

With more and more companies providing direct access to the web, end-users are casually surfing to sites that may be known malware download sources, or unknowingly revealing personal or corporate private data (credit cards, passwords, corporate trade secrets, etc) via email scams or hidden background programs that collect and forward data. This means that an IT manager must not only stop attacks at each layer network, application and content, but they also need to stop both inbound and outbound threats.

While most enterprises have deployed some type of desktop antivirus protection, viruses continue to remain the number one threat to security. Although desktop antivirus software is an effective tool, users either turn off their software or don't keep the antivirus pattern files up-to-date. Once one desktop is infected, other devices on the network are prone to infection causing network downtime leading to productivity loss and IT management disturbances.

Network-based antivirus protection, unlike desktop or host based antivirus, scans network traffic for viruses giving IT administrators control of how and when to scan for viruses in the network. By scanning for viruses in the most commonly used protocols – including content such as mail, web and file transfers – as it crosses the network perimeter, network-based antivirus solutions can stop viruses before they spread and infect desktops. Using a multi-layered security strategy gives IT administrator the ability to control how best to protect the organization at every level. Moreover, network-based antivirus products are cost-effective, as one single license can protect distributed systems in the network segment.

By integrating a best-in-class gateway antivirus (AV) offering from Kaspersky Lab, Juniper Networks integrated security appliances can protect web traffic, email and web mail from file-based viruses, worms, backdoors, Trojans and malware. Using policy-based management, inbound and outbound traffic can be scanned, thereby protecting the network from attacks originating from outside the network, as well as those that originate from inside the network. Unlike other integrated antivirus solutions that are packet or network signature-based, the Juniper-Kaspersky solution deconstructs the payload and files of all types, evaluating them for potential viruses and then reconstructs them, sending them on their way.

The Juniper-Kaspersky solution detects and protects against over 100,000 viruses, worms, malicious backdoors, dialers, keyboard loggers, password stealers, Trojans and other malicious code. Included in the joint solution is a best-of-class detection of Spyware, Adware and other malware-related programs. Unlike some solutions that will use multiple non-file based scanners to detect different types of malware, the Juniper-Kaspersky solution is based upon one unified comprehensive best-of-breed scanner, database, and update routine to protect against all malicious and malware-related programs. Antivirus is available on the NetScreen-HSC, NetScreen-5GT Series, and the SSG Family as an annually licensed feature.

