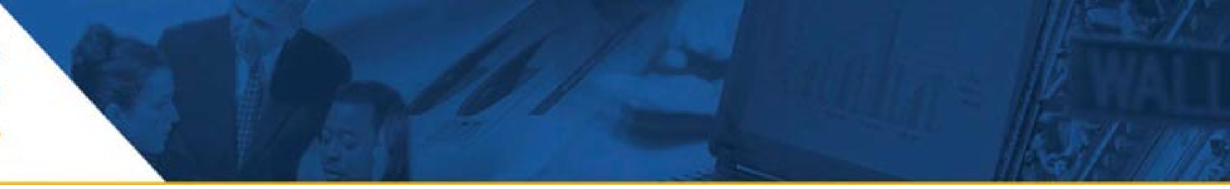
IDC
Analyze the Future



IDC ANALYST CONNECTION

Charles J. Kolodgy
Research Director, Security Products

Taking Control of Converged Network Security

August 2006

Enterprise demands for reliable and secure service will increasingly drive the broad-scale adoption and deployment of IP telephony and other VoIP technologies. For IP telephony to continue its ascension into a growing number of business processes, vendors should look no further than the wireless LAN (WLAN) market for pitfalls to avoid. WLAN was the first technology market to experience a mass-market rejection based on security. Enterprise IP telephony is poised to be the second, but IDC believes the IP telephony market is more security-aware than the WLAN market. Yet, given the exploding market for applications that tie voice and other communications applications to the business process, the potential for growing complexity and security problems will begin to come to a head in 2006.

The following questions were recently posed to Charles Kolodgy, Research Director for IDC's Security Products service, by NIKSUN on behalf of its customers.

Q. What are the most pressing network monitoring challenges for enterprises today?

A. According to IDC survey results, one of the top security challenges faced by enterprises is the increasing volume and complexity of network traffic. The amount and complexity of network traffic, coupled with increasing threats, is making it more difficult to distinguish suspect — that is, malicious or wasteful — traffic from high-priority traffic.

The situation is being made even more difficult as enterprises increase their IP traffic by moving to converged network environments, which incorporate new features such as voice and video. In the past, companies would throw bandwidth at this issue, but this approach failed to reduce the threats created by the suspicious traffic. Instead, it just masked the problem. Now, enterprises have realized they must be able to identify unwanted traffic so it can be throttled or eliminated.

Q. What are the most serious security challenges and threats facing enterprises?

A. Again, IDC surveys reveal that most enterprises are worried about the tactical threats. For example, the increasing sophistication of attack types is the top security challenge, according to IDC's 2005 *Enterprise Security Survey*. That same survey identifies the specific tactical threats as trojans, viruses, worms, spyware, spam, and other malicious code; hackers; and, interestingly enough, unintentional errors introduced by employees.

This last item also relates to another top security challenge — employees who underestimate the importance of following security policy. From a networking standpoint, this is a great concern because employees are prone to high-risk behaviors such as visiting Web sites they shouldn't, downloading content, and abusing bandwidth with streaming media. Enterprises would like their employees to keep to work-related functions and not expose the network to threats caused by "out-of-bounds" behavior.

Q. How has the growth in converged network environments affected network infrastructures and, specifically, security requirements?

A. By pushing more and more business services such as voice and video through the data network, enterprises are saving on telephony costs and adding telecommunication features. But the trade-off is a more complicated IP network. Additional converged services, as well as additional data applications such as wireless and instant messaging, make it much more difficult to monitor network performance and pinpoint trouble spots when they emerge.

From a security standpoint, there is now a larger footprint for threats to exploit. The IT staff has to be more alert for denial-of-service attacks because such attacks could conceivably shut down the whole enterprise.

Q. What can companies do to ensure that their converged network environments are operating at peak performance while remaining secure?

A. Ensuring that converged network environments operate at peak performance requires visibility into the network as well as the ability to report on network status. Specifically, companies should implement a network monitoring solution that can determine existing traffic patterns and utilizations. In this way, they can understand the normal flow of traffic within the network and easily identify spikes in utilization — or, conversely, when there are slowdowns or downright network failures. By using network analyzers, companies can provide a high level of network performance.

The security question is different because the goal is to stamp out suspect traffic, not just allow legitimate traffic. Instead of a standard network monitoring solution, enterprises should turn to a network intrusion prevention system (IPS), which can identify "bad" traffic and shut it down. One key feature of an IPS is the ability to control traffic flow. Attacks and threats need to be shut down, while at the same time, legitimate traffic must be allowed.

Q. How can companies implement advanced IP network monitoring solutions and still make use of their existing installed network analyzers and security hardware and software?

A. The best way for companies to retain their existing infrastructure is to purchase a standalone, appliance-based network monitoring solution that will not impact network performance. The device should be able to cover the whole network by being able to handle a wide variety of network interfaces — Ethernet, ATM, fiber, Packet over SONET, 802.1Q — as well as handle high and low data rates.

Generally, companies shouldn't need to replace existing solutions, provided they're performing as expected. Otherwise, the solutions should simply be upgraded. A new network monitoring solution, for example, may provide a benefit to the security infrastructure because, with better reporting, it will be much easier to determine if a real threat exists. With improved network intelligence, security solutions can be tuned to address the most egregious threats.

Q. What steps can companies take to ensure that they implement monitoring solutions that address actual needs rather than pursue technology for technology's sake?

A. It requires discipline to avoid being enticed by the charm of exciting but untested technology. The first step is for companies to determine their exact needs. What pain points are they trying to address? By quantifying their specific requirements, they can then search for those products, both established and emerging, that can best meet as many of their requirements as possible.

If companies are having some degree of difficulty determining whether or not a particular solution meets their needs, it's their responsibility to specifically ask their solution provider whether it can meet their requirements. Lastly, companies must test the products they intend to place in their IP network to ensure that the solutions really do solve their problems.

ABOUT THIS ANALYST

Charles Kolodgy is a Research Director for IDC's Security Products service. In this role, he executes primary research projects and analyzes markets for both vendors and user customers. Mr. Kolodgy's responsibilities within the Security Products service include both hardware and software security products.

ABOUT THIS PUBLICATION

COPYRIGHT AND RESTRICTIONS

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com