IDC
Analyze the Future

IDC VENDOR SPOTLIGHT

Securing Converged Networks

August 2006

Adapted from *Worldwide Threat Management Security Appliances 2005–2009 Forecast and 2004 Vendor Shares: Security Appliances Remain a Well-Oiled Machine* by Charles J. Kolodgy, IDC #33997

Sponsored by NIKSUN

Many organizations have diverse networks addressing converged voice, video, and data; enterprise-level network access for people outside the company (physically and/or organizationally); and network support for real-time interaction (such as chat and conferencing). These new converged applications have opened more potential security holes than ever. Meanwhile, the frequency and types of threats are increasing, with new viruses, hacking attacks, and other malicious activity focused on both wireless and wired environments. Companies need to protect their converged networks with integrated multifunction security appliances that address the newest vulnerabilities, such as voice over IP (VoIP), and also protect from the constant and rapidly evolving threat to financial transactions. This document examines current trends in network convergence; identifies the opportunity for security appliances to address new and emerging information technologies and protocols, such as VoIP and XML; and profiles NIKSUN's approach to the security appliance marketplace.

The New, Expanding Threat Environment

Competitive pressures are pushing companies to integrate new communications capabilities within their IP-based networks, resulting in the convergence of voice, video, and data onto a single network infrastructure. These new communications capabilities are designed to increase the efficiency of an enterprise as well as provide new capabilities to a service provider's customers. While such convergence promises to increase worker productivity as well as revenues, the combination of data, voice, and video networks also poses new challenges, such as:

- How to manage and control the converged network
- How to monitor and ensure that voice and video quality will be satisfactory

As companies continue investing in high-speed networking technologies such as Gigabit Ethernet (with early adopters already migrating to 10 Gigabit Ethernet), more business-critical data will flow throughout the network, increasing the cost of network downtime. These high-speed converged networks also open up new security vulnerabilities, the proliferation of which cannot be adequately addressed with point solutions. An integrated and scalable enterprisewide system for network performance monitoring and security is required.

Such an enterprise solution — essentially an integrated multifunction security appliance — needs to provide rapid insight into performance or security concerns anywhere in the network, with the goal of keeping the converged network infrastructure and services performing optimally under all circumstances. The integrated appliance should have reactive analysis as well as proactive early-warning capabilities.

Given that IP-based phone systems, for example, can now become destinations for spam, hackers can target VoIP networks with denial-of-service (DoS) attacks or program a company's phones to call other businesses, shutting down the second company's phone systems. More determined hackers can spoof a phone's IP address and make calls that are billed back to the company. With a traditional phone system, hackers can intercept and listen to calls.

Attacks on a VoIP system may actually be hastened, as standards such as Session Initiation Protocol (SIP) are incorporated within a variety of applications. Open source IP private branch exchange (IP PBX) software can be downloaded from the Internet for free, providing a training ground for aspiring, next-generation phone hackers.

IDC believes that as applications such as IP telephony and storage over IP increasingly become part of today's converged network, best-effort availability services and traditional security methods will no longer be enough to protect these new applications. There is a need to neutralize security breaches such as worm and virus attacks, eavesdropping (also known as man-in-the-middle attacks), service theft, and unsecured protocol firewall transversal.

However, if a network is to remain operational, threat detection and neutralization must be dynamic. Intrusion detection systems can isolate a possible network anomaly, but a network must have the ability to manage the threat proactively using detection methods such as protocol analysis, anomaly, behavioral, or heuristics to discover unauthorized network activity.

The Need for Unified Solutions

The convergence of business communication applications with data networks and applications clearly requires a different approach to security planning and security priorities. When voice and data networks and applications were isolated from each other, different security priorities existed. Voice applications running on dedicated networks were not subject to eavesdropping or malicious hacking. With voice applications now running on converged data network infrastructures, these applications are subject to all the security vulnerabilities associated with data networks.

Voice is not the only consideration, however. Converged networks must also handle the following data traffic and connections that warrant an integrated security solution:

- Increasing storage needs and associated security to protect critical company and client data
- Increasing importance and volume of Internet-based financial transactions (e.g., online banking, ecommerce, and security trading), which make many companies heavily dependent on their networks for revenue and profits
- Increasing quality-of-service (QoS) requirements for all converged services (voice, video, data), which can be negatively impacted by attacks
- Increasing awareness of potential security threats, accidental or deliberate, from users inside an organization

To successfully control and manage the converged network, organizations need a unified solution that seamlessly works across a diverse network infrastructure and mix of applications. A unified solution brings many benefits because it provides visibility into *all* traffic, including voice and data. Such complete visibility is essential for network managers because they need to set application traffic priorities so that communications receive the real-time quality they require. In addition, network managers need to be able to troubleshoot the impact of data on voice and vice versa.

Converged networks increase security risks because they increase the number of IP ends on the network, opening certain network ports and adding new protocols, thereby increasing the number of weak points in the network subject to attacks. A lack of awareness still exists in the market regarding the security threats related to converged networks, but companies shouldn't panic because most of these threats can be managed easily if addressed properly. To secure a VoIP system, for instance, organizations must implement security measures at different levels, including:

- **Network infrastructures.** VoIP systems sit on a company's network; therefore, it is crucial to begin with a secure network infrastructure to protect a VoIP system. The main security threats that can affect VoIP systems via attacks to a network infrastructure include DoS and spam over Internet telephony (SPIT), among others, which can be deterred by firewalls and intrusion detection and prevention (ID&P) security appliances. Many companies have already implemented firewalls in their networks, but they still have not installed a unified ID&P system.
- **VoIP standards.** These standards include H.323, SIP, Media Gateway Control Protocol (MGCP), and other proprietary protocols. Most VoIP implementations use H.323 or SIP standards that can be subjected to attacks if hackers are able to access a network. For example, a functional protocol testing method (i.e., fuzzing) finds bugs and vulnerabilities by pushing the protocols' specifications over their limits and breaking them, thus leading to DoS and buffer overflow vulnerabilities in VoIP networks. One way to prevent such vulnerabilities is by installing an ID&P appliance that's familiar with SIP traffic and able to detect suspicious traffic. That way the appliance can preempt an attack by taking action to protect the network.
- **Administration and monitoring.** Billing, accounting, maintenance, and monitoring are also very important when deploying a VoIP system. Monitoring the flow of VoIP packets from IP phones to a server, the number of dropped calls, and the response times of the server are some of the performance indicators that should be controlled to ensure optimal performance and QoS.

The primary function of ID&P security appliance products is to provide continuous monitoring of networks and to report or react to malicious activity. ID&P products compare current activity with a list of signatures known to represent malicious activity, or they use other detection methods such as protocol analysis, anomaly, behavioral, or heuristics to discover unauthorized network activity. ID&P appliances generally have strong DoS defensive capabilities and antiworm capabilities.

Security appliance vendors continue to improve the technology to address new and emerging information technologies and protocols, such as VoIP and XML. This capability is required because as networks with data and voice convergence grow in popularity, they will soon become targets of attacks. IDC would expect to first see special-purpose appliances dealing with these technologies, and eventually all the different types of threat management security appliances will address converged technologies.

The market for security appliances continues to expand, fueled in part by several key advantages for user organizations, including convenience, ease of installation, and centralized management. The following list provides more detailed factors that are encouraging the growing number of security appliance installations:

- **Reduced complexity.** The all-in-one approach simplifies product selection, product integration, and ongoing support.
- **Avoidance of software installation and proliferating servers.** Customers or service providers can easily install and maintain the products. Increasingly, this process is handled remotely.
- **Ability to install and forget.** The appliances are generally plug and play, with very little installation required. User configuration errors and changes are minimized.
- **Synergy with high-end software solutions.** Appliances are used in remote sites where an enterprise does not have security professionals on the ground. A plug-and-play appliance can be installed and then managed remotely. This management is synergistic with large, centralized software-based firewalls.
- **Performance.** With an appliance, application performance is standardized.
- **Troubleshooting ease.** When a box fails, it is easier to swap it out than to troubleshoot. This process gets the node back online quicker, and it can also be done by a nontechnical person. This feature is especially important for remote offices without a dedicated technical staff onsite.
- **Centralized management.** Management of appliance operation and performance and application functionality can be done using a centralized management console.

Considering NIKSUN

NIKSUN Inc. is an eight-year-old, privately held company headquartered in Monmouth Junction, New Jersey, with sales offices in major cities throughout the United States, Europe, and Asia/Pacific. NIKSUN takes a multidisciplinary approach to product design, drawing from and integrating several application areas, including security surveillance, anomaly/intrusion detection, forensics, compliance, interception, network performance, QoS/service-level management (SLM), and root-cause analytics.

The company likens the network monitoring capabilities of its products to having an intelligent camera on the network able to perform real-time motion analysis. For example, NIKSUN's flagship product, NetVCR®, is a network analysis appliance that proactively alerts users to network, service, or application performance issues, providing root-cause analytical and predictive capability. NetVCR features include the following:

- Real-time visibility and capture of all network events
- End-to-end network and application performance monitoring and troubleshooting
- Integrated performance reports on all traffic

NetVCR is a full-function appliance for advanced real-time network, service, and application performance monitoring and troubleshooting. It seamlessly integrates the following vital functions in an integrated and scalable solution:

- Proactive end-to-end SLM/QoS monitoring for data and voice traffic
- Online continuous super analyzer from link to application
- Multi-timescale auto-analysis

The integration of these critical capabilities on a single appliance makes NetVCR well-suited for the proactive management of converged networks. NetVCR's architecture and design allow for quick and easy correlation of information to identify root causes in a few mouse clicks. The advantage of aggregating several key functions onto a single appliance is a dramatic increase in the availability and quality of the network services and applications.

Similarly, the company's security appliance, NetDetector®, provides surveillance, detection, analytics, and forensics. NetDetector is intended to complement an organization's existing network security infrastructure, including firewalls and other ID&P devices, to help provide a stronger defense. The product continuously captures and warehouses network traffic, alerting users to specific signatures and traffic patterns. Built-in modules provide complementary signature and statistical anomaly detection, thus locating the "needles" of actionable information in the "haystack" of raw data. Reconstruction capabilities allow for a detailed review of Web, email, instant messaging (IM), FTP, Telnet, and other applications.

For measuring, recording, and reporting on IP-based voice flow over a network, NIKSUN offers NetVoice®. The network management and security device offers complete or filtered VoIP recording, analysis, and playback (audio and video) and also collects, records, and analyzes an unlimited number of calls. NetVoice measures, records, and reports on every VoIP flow in the network in real time at production network traffic rates. The product enables no-loss VoIP monitoring for enterprise and service provider networks. Its distributed and scalable architecture enables complete end-to-end monitoring in large-scale environments. NetVoice offers complete call-level QoS details, including delay, loss, jitter, and mean opinion score (MOS).

NIKSUN's entire product line leverages a scalable data warehouse back end that acts as an intelligent repository of information — and a common information source ensuring consistency of information across an enterprise. Atop this knowledge data warehouse, NIKSUN has developed specific data mining applications designed to leverage the common knowledge repository and provide solutions tailored to various business requirements.

For example, NIKSUN's NetDetector uses a data mining application designed for security surveillance, detection, forensics, and other security-related applications. Similarly, NetVCR is a data mining application suitable for network performance, QoS, SLM, and troubleshooting. Organizations are able to correlate and aggregate information for an enterprisewide view.

Challenges

With most security implementations, it's better to build in security rather than bolt it on as an afterthought — and converged networks are no exception. However, the challenge is that many enterprises considering converged networks are concentrating on performance, cost, and QoS.

NIKSUN's challenge is to get in front of the decision makers associated with implementing VoIP, for example, so that customers can utilize NIKSUN's solutions from the beginning. In this respect, the challenge to NIKSUN is no different from that of any other vendor in the advanced security market.

A more specific challenge is for enterprise customers to understand that NIKSUN is a vendor that can offer the security solutions they need for converged networks. Although NIKSUN has strong technologies, products, and loyal customers, the company is still not well-known.

Conclusion

Deployments of networks with converged data and voice are increasing, but the technology is still fairly new. Securing VoIP systems, in particular, will continue to be a priority for enterprises migrating to this technology. Organizations need to create a multifaceted security system that addresses all these types of network security across every type of network they maintain. Converged networks must be made into a coherent and secure whole, ensuring security without burdening users with lag times and complex security procedures. IT staff and outside providers must have a holistic view of the entire system.

When looking at the potential market for products and services associated with securing converged networks, vendors of integrated, multifaceted management and security appliances have considerable opportunities. To the extent that vendors such as NIKSUN can offer enterprise solutions that meet the demanding needs of converged networks, the company should enjoy continued success.
