by Brian Partridge, Senior Analyst, bpartridge@yankeegroup.com, 617-880-0358

IBM and Narus Combine Forces for Carrier IP Security

The Bottom Line:	Comprehensive carrier IP security solutions span from the end user to the network core. Carriers and enterprises need to understand the security risks associated with the adoption of IP-based services.
Key Concepts:	Carrier IP security, service delivery architecture, anomaly detection, managed security
Who Should Read:	Chief security officer, director of marketing, director of product management

Practice Leader: Philip Marshall, Ph.D., Vice President—Enabling Technologies Service Provider, pmarshall@yankeegroup.com, 617-880-0260

IBM Introduces New Security Solution for Carrier Core

At International Telecommunication Union (ITU) Telecom World 2006 in Hong Kong, IBM announced its Telecom Core Infrastructure Security Solution (TCISS), which is a new security hardware, software and services offering spanning user security and the core of large-scale Internet Protocol (IP) carrier networks. IBM designed the solution to monitor and manage overall carrier network health down to individual IP traffic flows through a single, integrated system. IBM's announcement indicates that carrier IP networks have reached a sufficient level of critical mass to deploy the resources associated with a comprehensive solution set. In addition, the announcement indicates IBM's desire to play a strategic role in securing the next generation of service delivery architectures.

Carriers interested in deploying IP-based services (e.g., voice, IPTV, fixed-mobile convergence, push-to-x [PTTx], etc.) must do so with an understanding of the range of new attacks and the disruptions introduced when operating in an IP environment. By offering a new solution centered on holistic anomaly detection and mitigation, IBM is positioning itself to help address many of these issues. The IBM solution offers operators the tools to control policy enforcement either manually or automatically on platforms that are scalable enough to meet the needs of the world's largest carriers.

In addition, IBM's new security solution can also help drive new sources of revenue for carriers seeking to offer enterprise IT managers "clean pipes" that are guaranteed to be free of worms, viruses and other malicious traffic. Today, IT managers wrestle with building the capability to secure their networks in-house and are turning to their service providers for help. By providing their enterprise customers with managed security services based on the IBM solution, service providers can be more efficient in bringing better and more cost-effective new services to market.

There are three core components of the TCISS:

- **Tivoli Security Operations Manager** provides the monitoring and correlation of the network security elements (e.g., firewalls and intrusion detection systems).
- **NarusInsight Secure Suite** from Narus, Inc. provides holistic monitoring and correlation of all of the IP traffic flows.
- **Tivoli Netcool** provides an additional tier of correlation between the other two components.

Market Impact

The adoption of Internet Protocol as the foundation for the next generation of converged service delivery architectures has been well publicized in the marketplace. Service providers of all sizes support it, particularly the adoption of the IP multimedia subsystem (IMS) as the reference architecture of choice for IP service delivery schemes.

Yankee Group predicts that security—one of the last major hurdles to ubiquitous services over IP (SoIP) adoption—will become a major area of competitive focus and differentiation among telecommunications equipment vendors and carriers. The winners will provide the right mix of tools to achieve PSTN-quality security without eliminating the inherent benefits of a converged system.

Carrier IP Security Risks

By implementing IP-based solutions as platforms to deploy services, carriers are vulnerable to the same kinds of problems that enterprises face on their own IP networks: a continuously evolving security threat landscape as well as attacks against their networks.

The greatest security risk for carriers is the potential for distributed denial-of-service (DDoS) attacks. These are hard to defend against because they are difficult to detect, and an endless number of bots are available to be hijacked for this purpose. A solution to address this key security problem area must combine high visibility of Layer 3 through Layer 7 and data from all other network infrastructure devices (i.e., firewalls, IPS/intrusion detection signatures [IDS] and routers across the network).

Some of the other significant operational threats service providers face are in the areas of bots and botnets, where a usually unsuspecting collection of machines are controlled remotely for malevolent purposes. These zombie devices then can be turned to attack mode, with DDoS being the preferred type of attack. Worm propagation is another area of concern, but one that is distant to DDoS attacks and bots. The subsequent network congestion resulting from an effective worm payload is more harmful than the actual infection.

Few vendors can offer the carrier-grade capacity and scalability required to power the solutions that service provider infrastructure requires to address these attacks, making the IBM/Narus announcement particularly important.

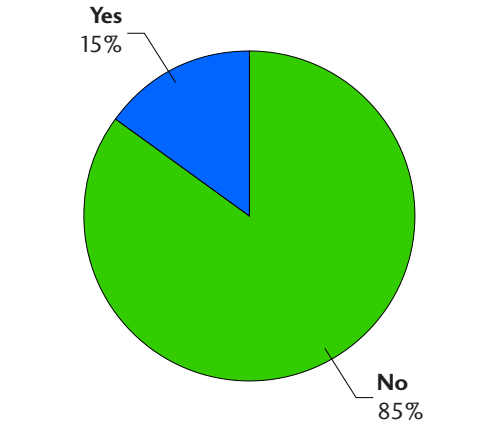
Vendor Conclusions

- **IBM** has positioned itself well for the anticipated explosion of IP services on the horizon and has a strong focus on service delivery platforms and IMS. Strengthening its core IP security solutions will further advance its strategic relevance to operators embarking on next-generation transformational projects.
- **Narus, Inc.** is well-positioned to benefit, given its central role in the TCISS solution. Narus will directly benefit from the size and scale of IBM's pervasive market reach. The NarusInsight Secure Suite is a category leader, providing a range of capabilities to detect threats across Layer 3 through Layer 7 with enormous network scale.
- IDS/IPS solutions from vendors such as **3Com/TippingPoint, Reflex, ISS and Force10** do offer carrier-grade intrusion defense. Some of these offerings are both signature- and behavior-based, providing more visibility than those that are strictly signature-based as well as decent protection against DoS attacks (i.e., large volumes of traffic from a single source to a single destination). However, these offerings only monitor changes in the volume of traffic. Because they cannot correlate, they only have visibility on a particular link. DDoS attacks (i.e., small amounts of traffic through any given link from tens of thousands of bots targeting a single destination) require a much broader view to be effective in the service provider infrastructure environment and to provide more proactive threat mitigation. Service providers need a next-generation-systems approach that can monitor actual traffic features and can correlate across the entire network. A holistic view of the broader network for DDoS mitigation and application layer threats with the scalability and capacity requirements to service a full-sized service provider architecture is a requirement for service providers whose greatest source of pain is in fighting these kinds of attacks (see Exhibit 1).

Recommendations for Service Providers

- **Build layered security architecture from the ground up and deploy security-focused management and threat mitigation tools.** The layered security architecture approach can achieve PSTN-like security. Robust management tools ensure swift resolution of security problems.
- **Conduct a comprehensive security audit and build out testing capabilities.** Regardless of where you are in the packet migration process, invest in an underlying real-time IP services security audit. Understanding today's network weaknesses will ensure you can address them proactively. Tools are available from vendors such as Spirent Communications, Ixia and Empirix.
- **Promote your security and "clean pipes."** View security as a strategic differentiator, not a necessary evil. Perceived IP-based security vulnerabilities constitute one of the last barriers to services-over-IP adoption. Once you have built a secure, layered IP architecture, tell your customers and collect a premium.

Exhibit 1.
Current Carrier Security Perceptions



Source: Yankee Group, 2006

Recommendations for IBM

- **Maximize first-to-market leadership by highlighting inter-provider functionality against common threats.** Many service providers have yet to deploy the most basic technologies to prevent against their greatest security threat—DDoS. If IBM can succeed in going to market with a strategy of offering protection against DDoS and other typical threats it faces, there is value for the service provider community to be able to offer cleaner pipes to their customers.
- **Message your portfolio of security offerings, including protection against application-level attacks.** DNS and VoIP attacks look like legitimate traffic to network infrastructure and security devices. The availability of the IP network is also a major concern. On the legacy PSTN, availability is rarely a concern. A hacker would need to overload some large circuits or physically cut a connection. It's much easier to disrupt a VoIP network. A distributed denial-of-service attack can be elusive to detect and devastating to service availability. IBM must message around the NarusInsight Secure Suite Layer 7 functionality. The typical service provider has no view into the attack and may only notice high volumes of traffic that could indicate an attack of this kind. Clearly, this is an ineffective solution for a potentially significant problem if a hacker brings down the VoIP call servers or if service providers can't resolve IP addresses if their DNS servers are down.
- **Go to market with the time-to-resolution and opex reductions this solution provides.** Service providers operate at very thin margins. If they can speed outage resolution and avoid churn, that can provide a source of customer service that service providers value highly. When the solution can provide context into reductions in bandwidth or the sources of infrastructure attacks or application layer attacks, service providers can reduce the time it takes to solve the problems—ideally before their customers feel it. As a result, there are subsequent opex reductions because the context is all right there and no system administrator has to spend valuable time tracking down the problem.