The State of Network Security

Inside the Firewall

By Charles Kaplan

I HAVE SPENT THE PAST EIGHT YEARS OF MY CAREER WORKING FOR Managed Security Service Providers (MSSPs), peddling better, faster, cheaper management and the monitoring of today's security devices; principally firewalls and network or host based IDP/S. During the years I have spoken with more than 1000 different companies about best practices, demilitarized zones, defense-in-depth, and all the other buzz words we each live and breathe each day.

Throughout these years I have had many discussions about how the insider threat is as great if not greater than the external one. I have read all the CSI/FBI Computer Crimes Surveys, saying things like, "Despite some variations from year-to-year, insider jobs occur about as often as outside jobs" (Source: 2005 CSI/FBI survey), but the choice of technical solutions to address this has been a vacuum.

When one digs into the problem, however, it quickly becomes apparent that the issues inside the firewall are not as clearly defined as those at the edge. Inside the firewall we have overlap between many different domains, and the issue isn't just one of security, but the balance between security, network integrity, and wellbeing. For example,

Network Security Teams must tackle problems such as worm outbreaks inside the network and insider breaches.

- Identify zero-day and variant worm outbreaks inside the network; isolate the entry point, determine how it is propagating, and identify which systems and segments have been compromised.
- Identify unauthorized reconnaissance such as scanning or suspicious connections to critical servers.
- Identify contractors going places they shouldn't.
- Rapidly quarantine compromised hosts by using routers and switches, while making sure to avoid unanticipated consequences.

The Problem	The Gap	How NBAD Helps
Worms and insider breaches continue to plague enterprise networks	Legacy solutions encompassing firewalls and IPS have failed here. The technology itself insufficiently handles insider threats. Furthermore, the TCO of these devices is simply too great for this purpose. The net result is less than 100 percent internal coverage, and the continuation of the cycle companies are in.	With NBA, companies achieve 100 percent network visibility combined with analytics designed to catch abnormal network activity (worm, hacker, rogue employee), independent of legacy firewall or IPS rule sets. Companies are also alerted to all systems that serve content on the network, letting you quickly root out hosts that may be participating in BOT networks, or other hostile activity. NBA may also provide visualization to understand how a threat is reaching a company, who it is targeting, and detailed real time reporting showing the impact to the network of countermeasures.
Targeted external attacks are an additional major source of problems	Spear phishing to gain credentials, low-volume viruses designed to evade anti-virus software, hostile Web sites, IM exploits, and yet to be publicized and patched attack vectors all pass right through today's firewalls. Since there is no known attack at work, IDS/IPS and anti-virus counter measures are bypassed, leaving companies at risk to targeted attacks.	The uniqueness and low volume of these attacks is exactly how NBA is able to detect them. Anomalous activity such as large volumes of data transferring out where it hasn't in the past, scanning and probing across the network, or unusual communication on ports are all descriptors of activity NBA monitors and responds to.
Enterprises often rely on circumstantial evidence to identify internal network attacks	Given the lack of IDS/IPS visibility inside the perimeter for all the reasons enumerated above (largely TCO based), detection of internal problems is often the result of human correlation, piecing together increases in help desk calls, slowness on the network, and other such circumstantial evidence. This failure to quickly detect and remediate leads to downtime, frustrated users, increased time to resolution, difficulty reaching a root cause, etc.	NBA alleviates this weak link specifically because it does provide 100 percent internal visibility. Delivering identification and attack visualization, NBA assists administrators in pinpointing where the attack is coming from and who it is directed at. Multiple factors weigh into this detection, including bandwidth surges, port scan activity, and suspicious connections. The consolidated and behavior-based model delivers a rapid and definitive detection of problems.
Organizations are allowing an increasing number of outsiders into their networks	Today's network perimeters are more sieves than check valves. Contractors, outsourcers, administrative temps, repair staff, and visitors to the facility all connect to the network with varying levels of trust, but often the same permissions. While we would like to *Trust but Audit*, the lack of controls and visibility here leaves most firms vulnerable to both malicious outsiders as well as those whose computers simply may not be current with the latest patches and anti-virus signatures.	Independent of firewall views, with NBA, companies can very quickly get a report of all systems touched by your outsider. If a hostile system enters the network, NBA will first alert and then let the organization produce a detailed report of all systems and ports touched, as well as how much traffic flowed, providing invaluable information for the cleanup effort. Many NBA systems can even deploy countermeasures.
Avoiding confidential data theft is the biggest security driver	Data theft is embarrassing and costly no matter what the root cause. Companies can not continue to place all their eggs in the firewall/IDP basket at the perimeter.	A layered defense approach, including visibility and monitoring of activity inside the perimeter, is the basis of a comprehensive solution. NBA technology is designed specifically to provide visibility beyond the firewall/IDP prevue.
Compliance efforts drain financial and staffing resources without improving regulatory readiness	Sarbanes-Oxley, HIPAA, GLBA and other regulations of the past few years have created an awareness of the problem and have forced a great deal of money to be spent ensuring compliance. But, as administrators commented in the Internal Threat Report, confidence of a truly improved security posture still waned, along with the ability to definitively know if one's network had been breached. A better balance can be struck.	NBA helps on two fronts. First, a layer of internal security and visibility helping to bolster one's overall security posture. Second, a layer of visibility and reporting to help speed through future audits with a sense of actual improved security, as opposed to merely obtaining a compliance seal.

Table 1: Problems and Solutions

Network Operations Teams need to troubleshoot chronic network issues. Why is the network suddenly slow? Is it a new security threat or simply a mid-day backup taking place?

- Identify database replication or new servers coming online in the middle of the day.
- Show what percentage of network usage is desktops downloading data from external servers.
- Reports on the top talkers and top services on the network.

Network Architecture and Planning Teams need to understand segmentation and system inventory/usage.

- Identify what services are running in the network, what servers they are running on, and who's using them.
- Enable teams to assess what services and servers are used by each business unit, and how much network traffic they each generate.
- Help teams understand the implications of integrating an acquired network or a new application (what ports are really used, what is the network load, etc.).

Compliance Teams need to audit and enforce internal controls.

- Ensure that application developers are not touching assets in the production environment.
- Report which systems and groups accessed critical servers over the last year (this is always tricky with auditors—proving the "negative"—i.e., nothing happened).
- Identify unauthorized access to sensitive assets that are often difficult to detect using application monitoring tools (for

example, a laptop telneting into a server can fly "under the radar" of application monitoring tools).

And then we have the product realities that complicate this problem.

- Deploying more IDS or IPS
  - Ubiquitous deployment is typically ruled out due to an unmanageable TCO and to a great risk to the stability of the network core.
- End node solutions
  - These seem promising, though for the time being enterprise sized rollouts are not commonplace or proven effective.
- Firewalls everywhere
  - This does little other than stop the most basic of problems (firewalls don't address application vulnerabilities, insider threats, tunneling, etc.), and impose a high risk of connectivity failure.

Worse still, even when great resources are expended to use all of these technologies in conjunction with each other, today's products still fail to address all the different use cases enumerated above.

So we are faced with a somewhat unbounded series of internal security/integrity desires, a lack of proven technology approaches, and an entire package rolled up and called, "Security inside of the Firewall."

An ideal solution would leverage existing investment in infrastructure, NOT require forklift upgrades or total network re-engineering, give deterministic answers with very actionable follow up information (including impact analysis), alert me to not just known, but also unknown/zero day threats, and instill confidence that my networking and security teams had a firm grasp of how the network was performing inside the perimeter.

About six months ago a salesman I had worked with for years went to work for Mazu Networks, selling a product called Mazu Profiler aimed squarely at this market. The details of what happened next are un-important, but after experimenting in my lab for several weeks I was inspired to see that the industry is closing in on a solution to the inside the firewall dilemma. I was actually inspired enough that I too went on to join Mazu Networks to help spread the message.

The Mazu Profiler product is part of an emerging product category known as Network Behavior Analysis system, or NBA. NBA systems are working their way through the Gartner hype cycle, with the experts claiming that by year-end 2007, 25 percent of large enterprises will employ NBA as part of their network security strategy.

NBA is formally defined as, "NBA provides network-wide visibility to understand how systems are used, who uses them, how systems connect to and depend on each other, and which ports and protocols systems connect over. Because they analyze the behavior of network traffic, NBA systems provide protection from threats that other security systems cannot identify, such as insider attacks, unauthorized servers and services, zero-day attacks, etc. NBA systems also ease the burden of regulatory compliance by reporting on network behaviors that did or did not occur."

In general, NBA systems:

- Develop a baseline of "normal" network activity.
- Monitor network activity on a continuous basis, comparing it to the baseline.
- Identify anomalies and analyze them against heuristics libraries to identify threats.
- Propose mitigation plans and, in some cases, perform mitigation.
- Provide ad hoc and periodic reporting capabilities on network traffic and behavior.

NBA technology provides cost effective answers to the questions above that security, operations, architecture and planning, and compliance teams are asking.

The Enterprise Strategy Group recently completed a study titled, "2006 Internal Threat Report," (http://www.mazunetworks.com/2006_threatreport/) examining the state of security inside the firewall. I have examined each of their key findings and aligned the issues with how NBA technology helps to address some of the key findings.

NBA technology provides cost effective answers to the questions above that security, operations, architecture and planning, and compliance teams are asking.

If I had to sum up the entire 2006 Internal Threat Report in a sentence or less, it would clearly be "Defense-in-Depth." This is not a surprising finding, but when one examines the application of NBA on the internal network, this new layer of depth makes the discussion much more interesting.

Table 1 summarizes how ESG sees the problem, and how NBA systems help address the issues.

My number one take away from the ESG report is that defense-in-depth isn't just a catch phrase but a security mandate. With 85 percent of the dollars lost in system compromise originating on the inside of the firewall, internal network visibility is a must. The threat is pervasive and changing. NBA technology is a layer in today's defense-in-depth policy, delivering comprehensive internal network security and visibility to help companies keep pace with the shifting landscape.

NBA will without doubt continue to evolve in the network and security food pyramid, but at the moment it is providing a cost effective solution to a series of endemic problems that have long challenged administrators. Additionally, by not having a rigid use case, NBA is impacting both internal security threats in specific and the larger picture inside the firewall health and wellbeing.

NaSPA member Charles Kaplan works for Mazu Networks.