Realtime publishers
"Leading the Conversation"

The Essentials Series: Understanding & Responding to Network Threats

Evaluating Intrusion Prevention Products

sponsored by
NOKIA

by Dan Sullivan

Copyright Statement

Evaluating Intrusion Prevention Products

With a quick search, IT professionals can easily find checklists to guide their evaluations of intrusion prevention systems (IPS). Unfortunately, these lists are rarely sufficient. Although such checklists might help distinguish between features promoted by vendors, they are too general to address the specific needs of a business' environment. In an optimal scenario, an IPS is not just a set of hardware and software dropped into a network but a means of implementing a security strategy that meets the needs driving business requirements. This article examines the limits of typical evaluation criteria often used to asses intrusion prevention products and provides an alternative approach based on the broader security considerations of an organization.

Limits of Typical IPS Evaluation Criteria

A common IPS evaluation methodology starts with the IPS rather than business requirements. This approach would be sufficient if the goal of a business were to purchase an IPS; however, the real goal is to mitigate risks and implement a security management strategy. Unfortunately, an IPS-centric approach focuses too much on the trees without understanding the forest.

The impact of too narrow a focus on technical issues and less on business drivers becomes apparent when you consider common questions about IPS functionality related to:

- Attack signatures
- Speed
- Compliance-related features

There needs to be discussion and evaluation of these features at some point, but they are not the fundamental requirements motivating the use of IPS.

Comparing Attack Signatures

A common question about IPS functionality is "How large is the attack signature database?" There two problems with this question.

First, it assumes there is a standard metric for comparing signatures, but such is not the case. For example, one IPS may require two separate signatures to detect two variants of a known attack while another system may use a single, more generalized rule that can detect both variants. Is the former a better system because it has more signatures or is the latter more effective because that one rule may detect other variants as well?

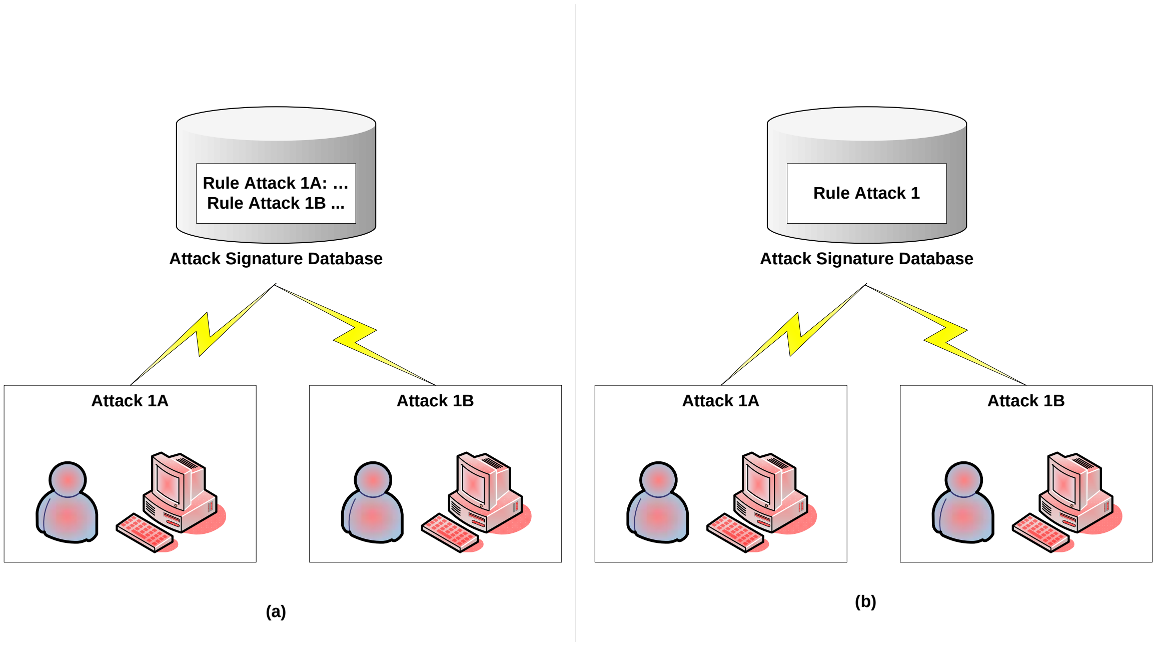

Figure 1: The number of rules in attack signature databases does not necessarily correspond to the number of threat an IPS can detect.

Second, it does not account for other forms of detection, such as behavior-based analysis. An IPS may use a baseline measure of typical network activity at different times of the day and week to detect suspicious activity on the network. This detection mode is not easily measured in terms of a number of signatures.

The disadvantage of basing evaluations on the size of signature databases is that the measure does not necessarily reflect how well the system functions. An IPS with a large number of attack signatures may work better or may not work as well as one with a smaller set of signatures. A more important consideration is how well the IPS filters and presents the large volumes of information collected. The object of an IPS is to present information useful for making decisions and too much data can undermine the user's ability to discern critical facts about the state of the network. For example, an IPS might report on a large number of port scans along with a few failed login attempts on a server. Summary information about port scans is important but details about each and every one can make it more difficult to notice the failed login attempts. Proper filtering, summarizing, and reporting is essential to effective decision making with IPS data.

IPS Speed

Performance is a key factor in determining whether an IPS will address the needs of a business. An IPS that slows network throughput so dramatically that business operations are adversely affected is of little use. Like measuring the size of signature databases, the question of speed is more complicated than it may first appear.

The speed of an IPS is, in part, determined by the way sensors are configured and the type of traffic the device analyzes. IDS sensors deployed in passive mode can collect needed data without adversely impacting performance; however, large amounts of log data generated on the sensors could degrade the IPS' ability to analyze the data in acceptable time frames.

Also, network speeds may be substantially lower than line speed. For example, a 1 gigabit sensor may suffice for a line rated for 10 gigabit speeds because network traffic does not reach line capacity. When comparing IPS speed measurements, one must be careful to understand the context in which those measurements were made. There may be so many differences in how speed measurements are done that the exercise becomes a matter of comparing apples to oranges.

Compliance Requirements

Compliance can be a key business driver behind the deployment of an IPS, but one must be careful of checkbox compliance. Regulations governing data protection require a comprehensive security strategy. You will find rules that require you to protect certain kinds of data, ensure the integrity of systems, and demonstrate that these protections are in place.

The risk of basing an IPS evaluation on a compliance checklist is that the focus may be too narrow. Comprehensive compliance comes from a comprehensive risk management strategy. Short circuiting the risk management process and jumping to a functional checklist (for example, “supports SOX reporting requirements”) leaves you at risk of leaving gaps in your ability to protect the confidentiality of data along with the integrity and availability of your systems. In additional to detailed functional requirements, do not overlook usability and manageability. Again, it is not the volume of data collected but the way the data is filtered, summarized, and reported that determines how useful that data is to IPS administrators. Ideal security devices increase security while minimizing configuration, maintenance, and customization demands.

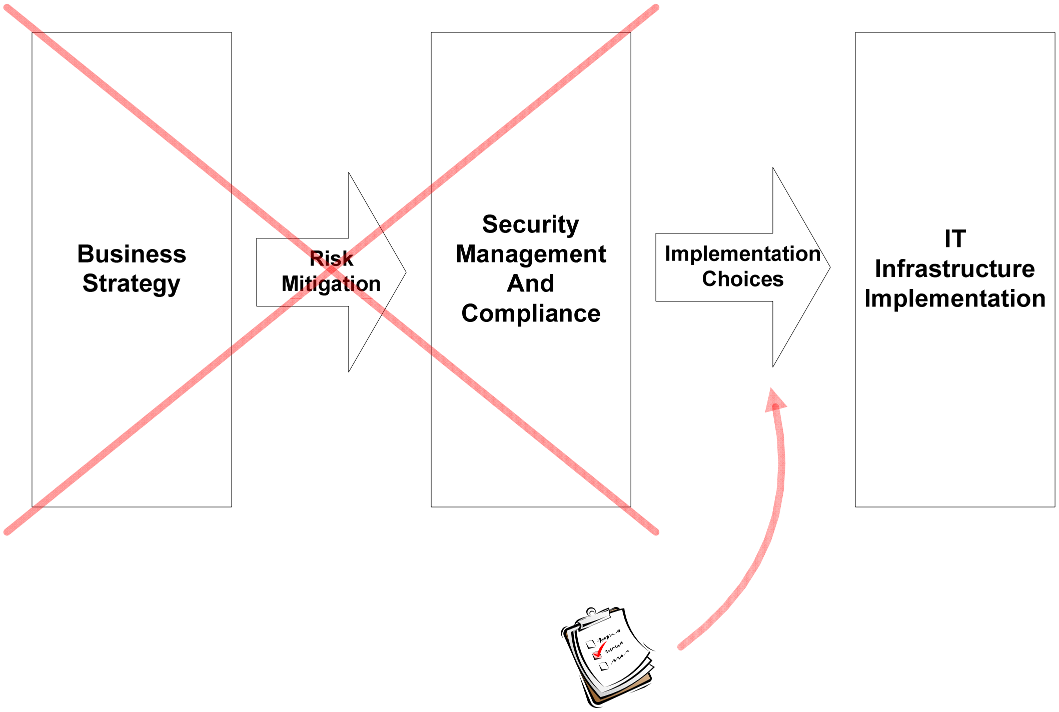
Business Strategy
Risk Mitigation
Security Management And Compliance
Implementation Choices
IT Infrastructure Implementation

Figure 2: Shortcuts, like checklist evaluations, can circumvent strategy-driven evaluations.

Checkbox evaluation criteria can be too narrowly focused on isolated functions and in the process fail to address broader issues of risk mitigation.

IPS Evaluations: A Better Approach

A better way to evaluate IPS functionality is to start with a focus on the full spectrum of security and IT infrastructure issues in place within your organization. Starting at the beginning allows you to develop an evaluation criteria based on these needs and, indirectly, on the business drivers that established those needs to begin with.

The particular requirements of businesses will vary (one of the reasons checklist evaluations are deficient), but there are several questions that provide sound starting points for a full-scale IPS evaluation:

- What kind of traffic is on the network and what threats does it present to IT assets?
- Which resources are vulnerable to compromise or disclosure?
- How can one measure vulnerabilities for both performance improvement and compliance?
- What are requirements from a decision support perspective? Does one have the capability to drill down when an event occurs to learn from it so that I can prevent it from repeating in the future?

These questions take business processes, assets, and starting points and frames technical questions in terms of how to protect those assets—which is, after all, the real goal of deploying an IPS.

Network Threats

It might seem obvious but it is worth pointing out that an IPS must function with the particular traffic patterns and network threats of the networks on which it is deployed. Traffic patterns establish a context for understanding what applications are running on a network and what endpoints exist. For this reason, IPS evaluations should take into account the kinds of traffic on a particular network so that one can identify types of threats to the applications and endpoints on the network. For example, network with significant volumes of streaming media content will have a greater risk of malware contamination from infected media than in other networks. In the case of a Microsoft-centric shop, there is no need for Linux-specific intrusion detection signatures. The context for understanding applications and endpoints , however, is not fixed. Both threats and infrastructure are dynamic, so IPS solutions should be evaluated on how well they can accommodate changes in both traffic patterns and network threats. This, in turn, will benefit IT staff who will spend less time on alerts that are irrelevant to their operations.

Vulnerable Resources

A well-known management adage is "you can't manage what you can't measure;" an analogue for security professionals is that "you can't protect what you don't know you have." Knowing what you have is no small task. Companies should consider IPS that help keep pace with changes to network infrastructure and integrates such information with core IPS functionality.

This kind of information helps IT staff identify and remediate vulnerabilities. Furthermore, an IPS can help track vulnerabilities for both performance improvement and compliance efforts. In particular, data collected by IPS and the resulting analysis can help to identify weaknesses and enable an iterative process to improve security measures and controls throughout the network. Of course, this information can also prove essential in forensic investigations and tuning of the IPS.

Summary

IPS evaluations are challenging. It is tempting to find or develop a checklist that assesses technical features such as the number of signatures in the database, but this approach is fundamentally flawed. Evaluations should be guided by the business drivers that shape IT infrastructure and policies. The goal is to protect business assets using IPS technology, not to select a technology divorced from the business and IT environment in which it will operate. Evaluations should keep in mind key benefits provided by IPS, such as improving analysis of log data, providing useful information for compliance and operations management, and supporting forensic operations. Evaluations should not overlook usability, especially the ability of an IPS to auto-tune policies and configurations to filter, summarize, and report data that supports infrastructure management.