TippingPoint®

Eight Questions To Ask About Your Intrusion-Security Solution

Why Intrusion Prevention -- Not Detection -- Is Essential

WHITE PAPER

Contents

Introduction

There is some confusion in the marketplace about intrusion-security systems. Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) have similar names. Indeed, market analysts tend to lump them together into a single security category – IDP (Intrusion Detection and Prevention). Even IDS vendors are blurring the lines, claiming to provide both intrusion detection and prevention.

The truth is: the capabilities and underlying design of intrusion detection and intrusion prevention systems couldn't be more different. Yes, the acronyms and product claims sound similar.

However, if you probe a little deeper and ask a few basic but important questions, you'll soon discover that only one approach to network security can block a wide variety of security attacks throughout your network without slowing down your network applications or devouring human IT resources.

The Fundamental Difference

After all, IDS and IPS solutions are designed and engineered for fundamentally different purposes.

An Intrusion Detection System is a classical out-of-band device that merely detects and generates alerts for suspicious traffic, making it ideal for security analysis and forensics. An Intrusion Prevention System, on the other hand, relies on purpose-built in-band devices both to detect and block unwanted traffic.

For companies and organizations of all sizes, this isn't about taking sides in a technology turf war. Detection solutions were adequate in the days when network security attacks were few in number and easy to manage, and they're still well-suited for security analysis and forensics. But, today, network-intrusion security has become a chief business boardroom concern. In the late 1990s, unique network and application vulnerabilities averaged just over 400 per year, according to the Computer Emergency Readiness

Team (CERT). In 2007, the number of vulnerabilities grew to just over 7,200 per year.[1] The growth in identified vulnerabilities has averaged more than 50 percent annually over the last ten years.

These network attacks are costing companies millions in lost business, repair costs and productivity losses. TeleChoice calculates that the average security incident costs an organization nearly $50,000.[2]

The growth in identified vulnerabilities has averaged more than 50 percent annually over the last ten years.

Eight Basic Questions

With so much at stake, companies of all sizes are taking a closer look at intrusion-security solutions. In order to sift through the claims and separate the intrusion-prevention contenders from pretenders, we suggest that you ask your intrusion-security system vendor eight basic questions:

1. Is your intrusion-security solution in-band?
2. Does your intrusion-security solution support maximum network and application availability?
3. Does your intrusion-security solution provide the performance needed to deeply inspect traffic without slowing down the network or business applications?
4. Does your intrusion-security solution protect not just your network perimeter but also key points within the core of your network?
5. Does your intrusion-security solution provide attack coverage that is broad and deep?
6. How accurate is your attack coverage? Does it block bad traffic without blocking good traffic?
7. How timely and up-to-date is the attack coverage?
8. Can your security vendor provide you with reference customers who are running in-band devices with a high percentage of blocking filters turned on?

Let's examine these questions in a little more detail.

1. Is your intrusion-security solution in-band?

There's no getting around it: To block unwanted traffic in real time,

intrusion-security devices must be placed in-band rather than off a tap or mirror port. Out-of-band devices can detect network attacks, but they can't stop them. In-band devices can provide real-time, deep inspection of data packets at layers 2 through 7.

In-band security – while essential – is merely the price of admission for network security. But it doesn't guarantee network uptime and performance, or that your security coverage will be broad, accurate and up-to-date.

Prevention systems must be designed from the ground up to provide both high-performance networking (availability and throughput) and high-performance security (broad, accurate, up-to-date coverage).

Detection systems were never designed to be networking devices. Still, some traditional IDS vendors have moved their devices in-band so that they can claim to provide intrusion prevention. The answers to a few additional questions should help you determine whether their intrusion-prevention capabilities actually measure up.

2. Does your intrusion-security solution support maximum network and application availability?

Your network shouldn't go down just because one of your in-band security devices fails. Your intrusion-security system should ensure that network traffic always flows at wire speeds, even in the event of a network error, internal device error or even complete power loss.

There are several checklist items regarding network-availability protection:

- Does the intrusion system offer dual hot swappable power supplies?
- Can the security devices transparently and automatically remove themselves from the network without disrupting normal business traffic?
- If an internal error is detected, can the devices go into a Layer 2 fallback mode and act as a simple network wire?

If the answers are no, failed in-band devices could bring down the network.

Detection systems were never designed to be networking devices. Still, some traditional IDS vendors have moved their devices in-band so that they can claim to provide intrusion prevention.

3. Does your intrusion-security solution offer the performance needed to deeply inspect traffic without slowing down your network or business applications?

Once an Intrusion Prevention System is placed in-band, it must offer performance that keeps the network and applications flowing smoothly. Security filtering must not negatively impact applications running at the perimeter, on internal network segments, remote-site locations or at the network core.

One recent test of an in-band IDS system revealed that latency peaked at 167 seconds – more than two minutes delay – which would be devastating to delay-sensitive applications.

There are two components to network performance: throughput and latency. As the intrusion-security devices perform checks on each packet, the security system must run at speeds equal to the network segment in which it is installed. In other words, in-band security devices should offer switch-like throughput and speeds of up to 10 gigabits per second to support new 10 gigabit-per-second networking. Second, intrusion-security systems should have low latency – packet delay should be no more than 100 microseconds – regardless of the number of filters applied.

As more IDS vendors respond to market demand for intrusion prevention and start to move their devices in-band, network performance often suffers. Why? Traditional out-of-band software and appliance solutions operate on general-purpose hardware and processors that are simply unable to perform without degrading network performance. Latency is a particular problem with retrofitted in-band IDS systems, since these devices were originally designed to buffer packets for non-real-time inspection. One recent test of an in-band IDS system revealed that latency peaked at 167 seconds-more than two minutes delay-which would be devastating to delay-sensitive applications.

Well-engineered IPS solutions, on the other hand, will not only keep up with applications, but can actually enhance application performance. TippingPoint, for instance, offers automatic throttling to give higher priority to critical applications on the network.

4. Does your intrusion-security solution protect not just your network perimeter but also key points in the core of your network?

The notion of placing Intrusion Prevention Systems only at the WAN perimeter is quickly becoming outdated. Why?

Because there are simply too many entry points into modern networks. There is a very diverse set of assets located at a variety of locations within the network, and each of these network locations has different performance requirements. What's more, attacks can come from inside the network as well as from outside. Therefore, the need to inspect and remove malicious traffic at high-throughput traffic points has never been greater.

Network-intrusion devices should be placed not only at the perimeter but also between major network segments and in front of data centers and demilitarized zones (DMZ). But are those devices designed to handle core demands?

Ask your security-solution vendor: Can its devices support up to 10-gigabit throughput without creating significant network latency – all with a broad set of filters enabled to automatically block malicious traffic? If not, your intrusion security will be limited to the perimeter, exposing your core business applications to devastating attacks.

5. Does your intrusion-security solution provide attack coverage that is broad and deep?

The number, variety and sophistication of security attacks is multiplying each year, so the coverage of your prevention system must be broad and deep.

This means that your IPS should be able to stop all kinds of attacks, including: worms, viruses, Trojans, denial of service attacks, peer-to-peer bandwidth floods, spyware, phishing, cross-site scripting, SQL injections, PHP file includes, VoIP attacks and more.

Because hackers are always trying to figure out new ways to get around prevention systems, broad and deep coverage requires your security vendor to go beyond preventing a few well-known attacks. Blocking known attacks by providing exploit filters that recognize attack signatures is relatively simple. Unfortunately, there can be tens – if not hundreds – of different exploits for any single software vulnerability.

These exploit filters guard against single attacks, but don't protect vulnerabilities in operating systems and applications from all possible attacks. In order to stop all known and new unknown attacks that target operating system and application vulnerabilities, your security system must also provide the latest vulnerability filters.

...Your IPS should be able to stop all kinds of attacks, including: worms, viruses, Trojans, denial of service attacks, peer-to-peer bandwidth floods, spyware, phishing, cross-site scripting, SQL injections, PHP file includes, VoIP attacks and more.

These vulnerability filters act like a "virtual software patch" preventing all known and unknown attacks on the software vulnerability.

However, identifying application vulnerabilities and developing filters to close them requires a sophisticated security research team focused on vulnerability research.

6. How accurate is your attack coverage? Does it block bad traffic without blocking good traffic?

Security research / filter development teams...must extensively test their filter designs with real-world customer traffic and adjust filters to ignore anomalies that are part of legitimate traffic to ensure filter accuracy prior to distribution to customers.

Your IPS attack coverage must not only be broad and deep, it must also be highly accurate. Otherwise, it could block good traffic (what are known as false positives) or allow bad traffic (what are known as false negatives). The ability to design highly accurate filters that block a broad range of malicious traffic types is extremely critical for any intrusion-security vendor. In fact, one might argue that an IPS is only as good as the filter set it has enabled to block malicious traffic from entering your network.

Systems designed to zealously block bad traffic – if not well designed – can block good traffic and endanger your important business applications. Minimizing false positives is a major challenge for many IPS vendors, in part because (1) they don't invest sufficiently in the security research required to develop extremely accurate vulnerability filters, and (2) their hardware inspection engines don't deliver the performance necessary to run large numbers of these complex, yet highly accurate vulnerability filters. To prevent blocking good traffic, security research / filter development teams at your IPS vendor must do their homework. They must extensively test their filter designs with real-world customer traffic and adjust filters to ignore anomalies that are part of legitimate traffic to ensure filter accuracy prior to distribution to customers.

We recommend asking intrusion-security vendors to demonstrate their filter accuracy in the lab. In fact, test the IPS devices for yourself.

7. How timely and up-to-date is the attack coverage?

Attack protection that comes too late is no better than no attack protection at all. How – and how often – does your security vendor update its filters? And does your security vendor have the researchers and expertise needed to constantly identify and

prevent against emerging threats – even before vulnerabilities are discovered by software companies?

So-called "Zero Day" threats involve vulnerabilities discovered by hackers that are not yet known by software vendors or even most security companies, and they can make your network a sitting duck. What's more, it can take days or even weeks before a software company discovers the vulnerability and pushes out a patch to address it.

Ask your security vendor if it employs an experienced team of researchers dedicated to discovering Zero Day vulnerabilities and how it compares to competitors. Also ask if it can quickly and transparently deliver filters to protect your network.

A good example is TippingPoint. TippingPoint's DVLabs team is a world-renowned security-research organization that was recently recognized as the fastest growing discoverer of new security vulnerabilities and for having industry leadership in the percentage of Microsoft vulnerabilities discovered as well as holding the lead in high-severity vulnerability discoveries. In fact, in the last four years, DVLabs Microsoft vulnerability filters have been delivered on average 52 days before the Microsoft patches became available.

Through DVLabs, TippingPoint transparently delivers Digital Vaccine® filters to customers as often as twice weekly – and, if need be, immediately when critical Zero Day and other vulnerabilities and threats emerge.

8. Can your security vendor provide you with reference customers who are running in-band prevention devices with a high percentage of filters turned on?

It's easy to talk about intrusion prevention, but can your vendor prove that it offers effective IPS in a real-world environment? Ask your vendor to put you in contact with multiple customers who are running in-band devices designed to block unwanted traffic.

Be sure not only to ask reference customers about the total number of filters deployed but also about how many are turned on to block rather than just alert. Fewer filters in block mode might mean the vendor is not confident that its filters will minimize false positives. Then ask the reference customer how many attacks the

Fewer filters in block mode might mean the vendor is not confident that its filters will minimize false positives.

systems have prevented. With this information, you'll discover whether the vendor is trying to sell retrofitted detection systems or systems that are designed from the ground up to prevent attacks.

Summary

At TippingPoint, we can address confidently, and in detail, these eight essential questions. Our in-band solutions were designed from the ground up to block all kinds of attacks – from the perimeter to the network core – without degrading network performance, blocking good traffic or burying IT staff in alarms. In fact, TippingPoint pioneered Intrusion Prevention Systems back in 2002, and we continue to provide the industry's most complete intrusion prevention solution.

Network security is too important to fall victim to marketplace confusion and misleading claims. Before you commit to an intrusion-security solution, ask the right questions. And expect to hear clear, compelling answers that will keep your network safe.

Can your vendor prove that it offers effective IPS in a real-world environment?

[1] Computer Emergency Readiness Team (CERT). http://www.cert.org/stats/fullstats.html

[2] "Making A Case for IPS." 1 May 2006. TeleChoice. http://www.telechoice.com/Presentations/CaseforIPS.pdf

Corporate Headquarters:
7501B North Capital of Texas Hwy.
Austin, Texas 78731 USA
+1 512 681 8000
+1 888 TRUE IPS

European Headquarters:
Herengracht 466, 2nd Floor
1017 CA Amsterdam
The Netherlands
+31 20 521 0450

Asia Pacific Headquarters:
47 Scotts Road
#11-03 Goldbell Towers
Singapore 228233
+65 6213 5999

TippingPoint®

www.tippingpoint.com

503199-001 09/08