Intrusion Prevention Will Replace Intrusion Detection

Enterprises should delay new large investments in intrusion detection systems — which have failed to provide additional security — until intrusion prevention systems emerge that provide a stronger defense against "cyberattacks."

Many Internet security maturity models have been proposed, only to be cast aside as new concepts replace failed attempts to secure the enterprise network. For example, intrusion detection systems (IDSs) have failed to provide an additional layer of security and have added complexity to the security management problem. In the post-Internet boom, with the dawn of Web services and with the network becoming an integral part of business operations, security solutions such as intrusion prevention systems (IPSs) are being introduced that offer real protection for the enterprise.

Intrusion Prevention

Similar to intrusion detection, intrusion prevention can be separated into two broad categories — host-based and network-based. Host-based intrusion prevention is software that resides on a server and prevents cyberattacks against the OS or applications. Products from Okena and Entercept Security Technologies have had early success in protecting servers, particularly against the "Code Red" and "Nimda" attacks. Host-based intrusion prevention is an immediate cure for vulnerabilities in servers, but because of the costly overhead of managing security software on many diverse platforms within the enterprise, host-based IPS will not see the same adoption rate as network-based intrusion prevention.

In the first half of 2002, security vendors introduced products that promise better security at reduced total cost of ownership. The defining characteristics and benefits of network intrusion prevention are:

- **Inline position:** Rather than tapping into a data stream from the switch or other device, these products sit inline with the data stream. Inline systems can analyze and identify packets
and sessions, verify which are malicious and drop the associated stream of packets. This is essential to these products' protective abilities.

- **Stateful signature:** To efficiently handle multigigabit traffic streams, some form of stateful inspection must be used. The state of a particular communication going over a network includes the ability to have session knowledge about the packets being analyzed. Some awareness of state enables the engine to parse only the pieces of the session that are applicable to the attack signature. This provides high throughput and low latency, which also are required for enterprise applications.

- **Combined algorithms:** No single methodology can catch the maximum number of intrusion attempts while minimizing false positives. IPSs must use a combination of methodologies:
  - Signature analysis is the most powerful method, but it must be augmented with protocol/packet anomaly detection.
  - Protocol/packet anomaly detection focuses on signatures within the protocol or packet that have been defined as hostile, malformed, out of sequence or potential "zombies" (see Note 1). Both protocol and packet are included in the detection methodology because they follow the same premise — to identify a clear violation of the parameters defined in published standards.
  - Behavior-based statistics are less exact, but they can provide a valuable function. This technique involves analyzing baseline metrics of known traffic patterns, then setting the alert threshold when extreme traffic pattern changes occur, such as massive flooding that may indicate a denial-of-service attack. (Flooding may also indicate a legitimate network traffic surge. Thus, notification can maintain or alert required infrastructure changes to meet valid traffic demand.)

- **Dropping malicious traffic:** Once a malicious session is identified, it is simply dropped, which protects the destination server or device. Logging and alerting are functions of these devices.

The advantages of these systems include the reduced importance of constant monitoring, and that an attack does not set off chimes and claxons that cause a chaotic scramble to react. Network administrators know that Code Red attacks have become part of the background radiation of the Internet. Therefore, the time spent logging and responding to these attacks is wasted. Once identified, the affected session should

---

**Note 1**

**Zombies**

Some distributed denial-of-service (DDoS) relay kits, called "zombies," can serve as transmitters for floods of packets to be sent to DDoS targets' servers. These relay kits use Internet Relay Chat channels to communicate back to controlling hackers, who can direct the relay kits to start attacking certain Web sites. By bombarding sites with bogus traffic, hackers can make it impossible for a site to respond to legitimate connections.
simply be dropped. Thus, not only are valuable resources conserved, but a better overall security posture is achieved.

**IDS: The Noisy, Expensive Burglar Alarm**

By now, IDS (see "Intrusion Detection System 1H02 Magic Quadrant") has become part of the standard architecture that includes perimeter firewalls, transaction zones (see "The DMZ Is DOA: Transaction Zones Replace the DMZ"), network IDS on critical segments and host-based IDS on critical servers.

However, we believe IDS technology has failed to deliver on its promise of markedly improved security. In many cases, IDSs have been costly and completely ineffective investments.

**Problems With IDS**

Almost universally, IS organizations’ mission is to react to business’ demands to identify, purchase and install technology solutions. The IS organization’s secondary responsibility is maintenance and repair. The need for new security measures usually is dictated by IS organizations against the will of user communities; therefore, IDS purchases have been driven by IS organizations to try to add a layer of defense that minimally affects the user base. We believe this attempt has failed; IDSs have increased IS organizations' burden by requiring full-time (24x7x365) monitoring and an incident response process that taxes their resources.

Problems with IDS include:

- *"Monday morning blues:"* Most security administrators review firewall logs, which indicate dropped sessions, on a daily or weekly basis; it’s alright to review these logs retroactively. However, imagine reviewing IDS logs the day after a three-day weekend. Each attack has to be reviewed and its impact must be considered. Was it internal or external? Did it succeed? Have the attackers seen or stolen anything? Full-time monitoring over the holiday weekend would help; however, every alert requires a response. Reviewing IDS logs is like reviewing the videotape of burglars pilfering a jewelry store — there’s a lot of information about what happened, but little on-the-job defensive action.

- *False positives:* A well-known complaint with most IDSs is that they generate many more alerts than there are intrusions. This leads to a tuning process that leaves the IDS powerless to detect certain real-event signatures.

- *False negatives:* IDSs also miss real attacks. Established IDS vendors exert much development effort to improve the
ability to catch all malicious traffic, usually at the expense of loss of performance.

- **Encrypted traffic**: Virtual private networks and SSL sessions may carry attacks; however, an IDS that is in "promiscuous sniffer mode" (see Note 2) can't inspect encrypted packets.

- **Throughput**: At most, the best IDSs can monitor traffic between 500 Mbps to 600 Mbps. Enterprise backbone use may exceed this; therefore, the IDS will miss a lot of traffic.

- **Correlation**: IDS agents create a flood of data that is difficult to manage. IS organizations must combine the data from several IDS agents, as well as firewall and system logs, to get an accurate picture of an attack. Thus, security is turned into a data management task, with the requisite need to store that data and apply sophisticated analysis tools to it.

Another proposed technology is Active IDS; however, it has been rejected by most security administrators as potentially too disruptive to network operations. In Active IDS, the IDS agent communicates with the firewall or router to change a security policy or access control list to block or restrict access based on an identified attack. For example, if an attack comes from within a university system, an automated response could install a rule in the firewall that blocked all access from that university, malicious and friendly traffic alike. Changing firewall policies in an automated mode is too fraught with problems to be adequate for most network security architectures.

### Recent Product Developments

Host-based solutions from Entercept and Okena have been on the market for two years. They block access to system resources that are outside a norm defined by policy or learned response. Gartner believes that host-based solutions are a quick cure to vulnerabilities present in server platforms, but that these solutions will suffer from administrative overhead that will keep them in a relatively specialized market.

In 2002, several companies introduced products that enable intrusion prevention:

- OneSecure was as a managed security service provider (MSSP), which is an industry born from the "you can't protect, you must monitor" security perspective. The insight OneSecure gained regarding the overwhelming task of monitoring network events led it to rethink its business model and to become a product vendor that offers protective solutions, such as its Intrusion Detection and Prevention system.

---

**Note 2**

**Promiscuous Sniffer Mode**

While in promiscuous sniffer mode, the IDS "listens only" to packet traffic, passively analyzing data off the network.
• IntruVert has been working on inline intrusion prevention for more than two years; it introduced its product line of IntruShield appliances at nearly the same time as OneSecure’s launch.

• Vsecure Technologies is leveraging digital signal processing and “fuzzy logic” that may provide the innovation required for better detection and subsequent blocking.

Other vendors are starting to incorporate aspects of intrusion prevention into their products, such as TippingPoint Technologies’ Unity One appliance, which combines firewall and intrusion prevention capabilities. Major firewall vendors are adding signatures for protocol anomalies to their products. NetScreen has more than 70 such signatures, and Check Point Software Technologies has announced plans for a product called SmartDefense, which will provide signature updates on a subscription basis (see "SmartDefense Offers Better Protection Against Network Intrusion").

**Bottom Line:** IDS technology was built on the belief that the number of security vulnerabilities and clever hackers targeting them is too daunting a task to prevent; thus, enterprises must monitor activity, rather than attempt to block attacks. However, Gartner believes that available and emerging protective solutions, such as intrusion prevention, relegate this theory to the same dustbin that contains client/servers, banner ads and pet rocks. Therefore, Gartner recommends that early technology adopters investigate stateful inline network IPSs to improve their security postures and for significant cost savings in security monitoring and management. Enterprises that have not yet made large investments in network IDSs should delay investment while investigating the advantages of intrusion prevention solutions. MSSPs should expand their current offerings to include the management of these new technologies.

### Acronym Key

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>DDoS</td>
<td>Distributed denial of service</td>
</tr>
<tr>
<td>DMZ</td>
<td>Demilitarized zone</td>
</tr>
<tr>
<td>DOA</td>
<td>Dead on arrival</td>
</tr>
<tr>
<td>IDS</td>
<td>Intrusion detection system</td>
</tr>
<tr>
<td>IPS</td>
<td>Intrusion prevention system</td>
</tr>
<tr>
<td>MSSP</td>
<td>Managed security service provider</td>
</tr>
</tbody>
</table>