

Why do You need Intrusion Detection & Prevention?

An Intrusion Detection/Prevention System (IDPS) monitors packets passing in and out of the network and attempts to discover if an intruder is attempting to break into or bring down your network. The IDPS runs constantly on your system taking action when malicious traffic is encountered. These actions can range from alerting an Administrator to blocking the offending IP.

Implementing an Intrusion Detection System on your network brings you a step closer to responding to attacks. However, responding to attacks in a timely and effective manner is costly and time consuming for local IT Administrators. Effectively monitoring an IDPS is a job on its own and only proves useful if it is being monitored 24x7.

This enables you to detect an intruder or malicious activity in real-time and not after servers are compromised. When an IDPS is combined with a firewall you have the ability to react to this intrusion immediately.

Features of having an Intrusion Detection/Prevention System combined with a firewall for maximum effectiveness include:

1. Detect a hack/intrusion in progress.
2. Provides the ability to block attacks in Real-Time.
3. Helps protect the network against mis-configured firewalls.
4. Detects attacks that firewalls legitimately allow through (such as attacks against web servers).
5. Protects systems with known vulnerabilities until the necessary patch can be installed.
6. Managed compliance with corporate policies for network and protocol use by restricting protocols such as instant messaging and peer to peer networks.

In addition, the following traffic analysis features can be provided:

1. Sorts network traffic according to protocol*
2. Shows network traffic sorted according to various criteria
3. Displays traffic statistic
4. Identifies the identity (e.g. email address) of computer users
5. Passively identifies the host O/S
6. Shows IP traffic distribution among various protocols
7. Analyzes IP traffic and sorts it according to the source/destination
8. Displays IP Traffic Subnet matrix
9. Reports IP protocol usage sorted by protocol type

Managed Intrusion Detection and Prevention System (MIDPS) is integrated into our **Network Security Appliance** and is responsible for detecting anomalous, inappropriate, or other data that may be considered unauthorized on your network. A regular firewall is configured to allow or deny access to a particular service or host based on a set of rules.

If the traffic matches an acceptable rule, it is permitted regardless of what the packet contains. However, the **MIDPS** enables our Security Operations Center (SOC) to capture and inspect all traffic, regardless of whether it's permitted or not. Based on the content of each and every packet, we determine if it is safe or not.

If it is dangerous, an alert is generated. We **Detect, Alert and Block** for security threats including buffer overflows, stealth port scans, CGI attacks, SMB probes and NetBIOS queries, NMAP and other port scanners, backdoors, Trojans, and Microsoft operating system and applications vulnerabilities, DDoS clients, and many more.

Why Outsource these important Functions?

The **MIDPS** Network Security Appliance provides a fully integrated suite of security services, consisting of hardware, software, consulting, monitoring, and management tools to actively assess and defend an organization's Internet network vulnerabilities and exposures. Our internal systems automate many of the labor-intensive tasks involved with monitoring various system logs used to detect anomalies and attacks.

Customers have the flexibility to create and implement with our analysts an easy-to-use, yet uniquely tailored set of security policies, regardless of dedicated access speeds, network size, or types of Internet applications.

Cost Savings: The cost of hiring in-house, full-time security experts to manage your network 24/7, 365 days a year, in addition to the ongoing hardware and software investments can be vastly more expensive than an outsourced solution. Our service also prevents expensive security incidents.

Control Operational Expenses: MIDPS is able to block unapproved traffic preserving network bandwidth for critical applications and services (such as your future VOIP deployment).

Dedicated and Credentialed Security Professionals: Implementation and management of security systems is a distinct and mature discipline, requiring skills separate than those required to install and maintain PC's and networks. Having an extensive team of dedicated security professionals whose sole responsibility is to be aware of and respond to the latest security threats is likely to be more competent than professionals who only deals with security on a part-time basis.

We manage thousands of networks so we see hundreds or thousands of potentially destructive attacks every day providing us with tremendous insight on on-going security issues.

Instantly Implement Best Practices: Security experts leverage industry best practices and our own proprietary methodologies to identify real security events before systems are compromised, eliminating time-consuming and costly security incidents.

We watch every security mailing list, CERT advisory; FBI Bulletin and we work very closely with the HoneyNet Project to ensure that your network is protected from every new security threat. Use our secure Browser based reporting tool to see how we are defending your network at your convenience.

Guaranteed Responsiveness: Once a security event is detected, escalation begins within seconds to identify the source of the problem and block it before it affects your operations. Aggressive Service Level Agreements (SLAs) ensures that you will be notified immediately with the appropriate amount of information.

NSA (Network Security Appliance) is designed and built by our team of security experts and is continually enhanced to meet the challenging needs of today's corporate environment. Built around a secure and locked down Linux kernel and open source security tools, we provide a rich set of features that are upgraded continually without the customer ever being involved. This guarantees that our customers have the latest technology without having to do anything!

Minimize Operational Complexity: Intrusion Detection Systems generate high volumes of alerts that must be analyzed to determine the nature of the event and appropriate action to be taken. This requires dedicated resources with the technical skill set to understand the situation and necessary response. Not to mention the burden of constantly evaluating and distributing signature updates to ensure protection from the latest threats.

We supplement your staff by offloading these tedious tasks involving them with only high-level incidents that require immediate attention. Escalation and response is tailored to fit your corporate security policies, allowing your staff to focus on internal security policies, procedures and daily business activities.

Who's Watching Your Network 7x24?

Contact **IntraSource** to discuss how to implement an effective MIDPS for your business!

Call (859) 278-5500 or (888) 552-5543 or email us at businessnet@intrasource.com