

Managed IDS

In the past year, the majority of large corporations and government agencies have experienced a security breach. Of those, over half were considered serious, involving theft of proprietary information, sabotage of data, and financial loss. The threat is clearly out there, making it imperative that you are continuously aware of any suspicious activity.

The **Intrusion Detection System (IDS)** will alert you in real-time to any hostile activity on your network.

The IDS can be deployed on your perimeter networks to protect your Internet access point, or used to protect key segments of your internal network.

Standard features

- Detect and alert based on pattern matching for threats including buffer overflows, stealth port scans, CGI attacks, SMB probes and NetBIOS queries, NMAP and other port scanners, well-known backdoors and system vulnerabilities, DDoS clients, and many more.
- "Passive Trap" to record the presence of traffic that should not be found on a network, such as NFS or Napster connections.

Advanced feature

- **Dynamic Firewall Rule Insertion** - Rules are dynamically inserted in the Nextwall® Firewall to block denial of service attacks, hacking attempts, black-listed IP addresses and IP addresses that are sending malformed packets such as runts (very small packets), giants (very large packets), fragments (a piece of a message transferred over a packet-switched network) or packets that exhibit aberrant behavior.

The Nextwall® Security Suite

