

# Intrusion Detection



*Businesses are concerned with protecting their intellectual property, especially when it is located on publicly accessible network systems*

Networks are vulnerable to attacks against which a firewall alone may not offer enough protection. An Intrusion Detection System provides an additional layer of security over and above a firewall.

NetWolves' IDS monitors the network's local host devices and network traffic for signs of attempted attacks and network security breaches. It is designed to detect and report unauthorized activity throughout a network, including port scans, network mapping, unauthorized access, failed access attempts, and abnormal network traffic patterns. NetWolves utilizes well-tested and proven network IDS technologies to accomplish its regimen. These technologies perform real-time traffic analysis and packet logging on IP networks, as well as host-based protection for the WolfPac security platform.

Integration with other NetWolves security services places the IDS functionality in an ideal position between the internal protected network and the unsecured external world.

- IDS protects the integrity of the WolfPac, including the operating system, firewall, mail server, file sharing server, and other resident security services.
- NetWolves' network IDS resides on the WolfPac between the protected and unprotected sides of the Internet connection. This provides an ideal vantage point for detecting unauthorized network traffic.
- NetWolves' web-based administrative interface allows for easy access to IDS logs. Highly functional sorting and searching capabilities allow the logs to be easily analyzed by authorized users.
- NetWolves' IDS can be configured to send alerts to designated contacts based on detection of various potential attacks.
- NetWolves' IDS technology can be monitored and configured from a central location using NetWolves' Secure Remote Monitoring and Management (SRM2) system.

*Networks are vulnerable to attacks against which a firewall alone may not offer enough protection. An Intrusion Detection System provides an additional layer of security over and above a firewall.*

**File system binary checking with file digest data compiled into a database, which is monitored daily for a change to the MD5 digest.**

**Uwatch (user watch) for logging user logins and associated time stamps. User activities are also reported.**

**Log watch & log surfer for monitoring system logs for key words like warnings and emergencies. Reports are sent to a specified email address.**

**Snort for network IDS, providing key command line variables for managing facilities.**

**IP trap to monitor and record all communication with outside services and locations.**

**Remote logging to maintain system log files.**

**System snapshot utility, including the current dmsg, IP configuration, firewall rule sets and logs, and database.**

**Call today to learn more about NetWolves' Intelligent Network Solutions.**