

Firewall



Attacks on network systems have become more prevalent in recent years. Businesses are experiencing different types of losses, ranging from service interruptions to alterations and theft of vital data

Any business with a connection to the Internet requires firewall protection. Many companies unknowingly increase their network vulnerability by adding insecure Internet access points. Making matters worse, network security policies can be difficult to enforce without the implementation of a proven security platform.

Implicit Lockdown

NetWolves can protect a company's private network infrastructure from intruders with its high performance firewall technology. Valuable company information is protected from malicious persons who use their skills to perpetrate attacks against corporate networks and inflict costly damage. With NetWolves' proven firewall standing watch, businesses can implement and strictly enforce their network security policies to thwart would-be network predators.

NetWolves' firewall technology uses a combination of advanced security features for protecting systems on a company's network, while simultaneously allowing users to easily exchange information with others on the Internet. The firewall and network address translation (NAT) services offer total control over the creation of custom rules used to meet the stringent demands of nearly any IT security policy. Both the firewall and NAT also offer pre-defined rule sets, which provide for immediate security between your protected network systems and the Internet. A secure web-based administrative interface provides a familiar environment from which all NetWolves security services can be configured to meet the network requirements of today's global business community.



Any business with a connection to the Internet requires firewall protection. Many companies unknowingly increase their network vulnerability by adding insecure Internet access points. Making matters worse, network security policies can be difficult to enforce without the implementation of a proven security platform.

Packet filters ensure that all IP packets coming from the Internet have been requested by an authorized user on the protected network.

Proxies prevent unauthorized Internet connections, or have been permitted by the security policy from accessing the protected LAN.

NAT makes the protected network invisible to outside Internet users by hiding the IP address.

NetWolves' firewall technology is standard on all WolfPac security platforms. It can also be monitored and configured from a central location using NetWolves' Secure Remote Monitoring and Management (SRM²) system.

ICSA, an independent standards organization that promotes continuous improvement of commercial Internet security, has awarded Firewall Certification to NetWolves. ICSA-certified firewall products are tested to protect against a standardized and evolving suite of attacks, while allowing business functions to be accomplished.

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