NETRANGER™

NETWORK SECURITY MANAGEMENT SYSTEM

.....ENTERPRISE WIDE SECURITY

.....CENTRALIZED CONTROL

.....UNMATCHED PERFORMANCE

WheelGroup corporation

Network technology advances every day, increasing productivity and access to information. Unfortunately, those advances also allow hackers to wreak havoc on your networks and the information within. In the past, there was only one solution to this problem: a firewall. Drawbacks to first-generation security systems are numerous, however.

- Because of performance issues, firewalls do not scale to fit into multiple points within a corporate network.
- Authorized users are often prevented from conducting legitimate business activities if certain types of traffic are categorically blocked out of fear of potential misuse.
- Firewalls and static security devices only serve to prolong the time it takes to break into a network—they do not easily detect attempts to penetrate a network.
- Authorized users often cannot be stopped by a static security system from conducting unauthorized activities within or from a corporate network.
- Many security systems are host-based or have very limited management capability—their configuration and management means tiresome maintenance and upkeep on myriad hosts throughout your network.

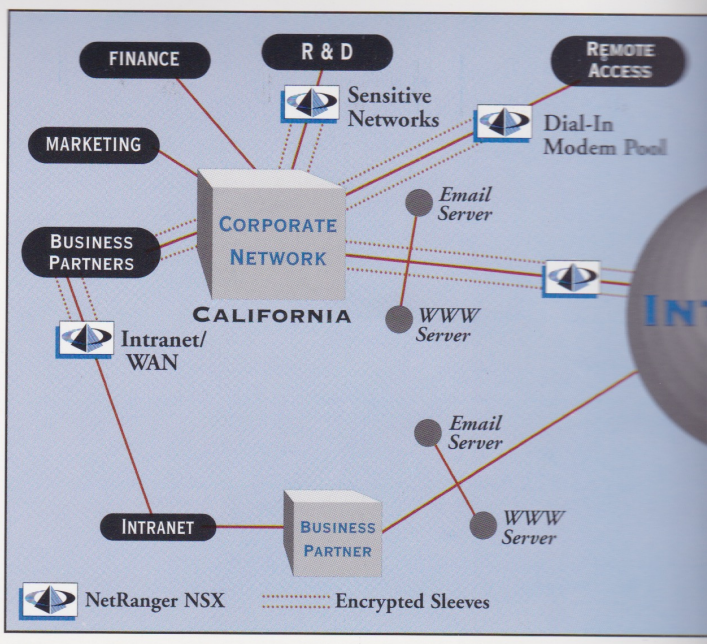
Now there's a new solution to the dilemma of providing dynamic, high-quality computer security without sacrificing network performance or capability. It's the NetRanger™ Network Security Management System by WheelGroup Corporation. NetRanger is an enterprise-wide security solution, providing intrusion detection, real-time shunning; centralized monitoring, management, and configuration; and permissive networking—all without degrading your network's performance. With real-time notification, NetRanger takes time away from hackers, allowing operators to kill an attack before any damage occurs. By working in concert with an organization's operations instead of against them, NetRanger is security that works the way people work.

An Enterprise-Wide Security Solution

NetRanger combines dynamic packet filtering with sophisticated intrusion detection technology to provide the first true enterprise-wide network security management system. The NetRanger sensor, called a Network Security eXchange (NSX) plugs into key network connections throughout the organization (such as Internet, intranet, WAN, LAN, and modem dial-up lines). It is designed to monitor the content and context of incoming as well as outgoing network traffic so that you can detect hackers attempting to break in from the outside as well as unauthorized activity originating from within your network. Because NetRanger monitors all of the network traffic, it detects and can stop even authorized users conducting unauthorized activity—unlike other security systems. The NetRanger's attack signatures employed for traffic scanning are user-configurable which gives you the flexibility needed to protect your information assets.

NetRanger is adaptable and can be scaled to different operating environments. Three categories of sensors handle different speed ranges, as follows:

- One size handles speeds up to 512kbps and is ideal for monitoring remote access (i.e., dial-up) connections.
- Another operates up to 10Mbps, covering T1 and Ethernet speeds and is ideal for Internet, WAN, and intranet connections.
- The largest works up to 100Mbps, handling T1, T3, and FDDI links—such high-speed performance is unmatched by other existing security systems.



Real-Time Shunning Prevents Security Violations

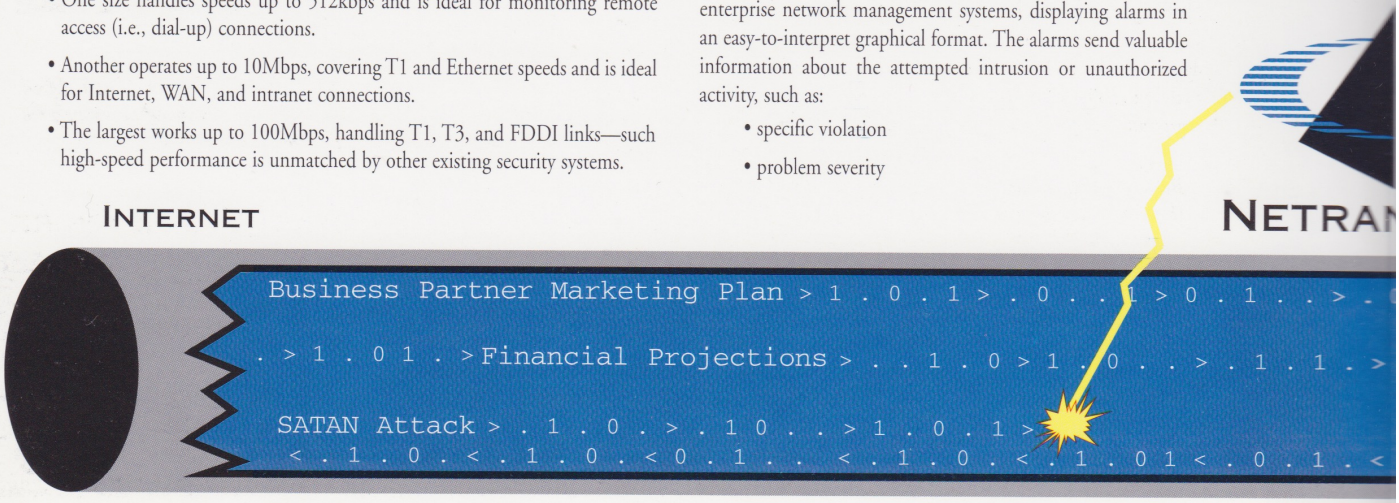
In the past, a system administrator reading through system log files may have discovered that a break-in occurred several days earlier. At this point, though, security options are almost nonexistent because network engineers had no true means to follow-up on the attack. More than likely, the extent of the damage or theft of information assets could never be determined.

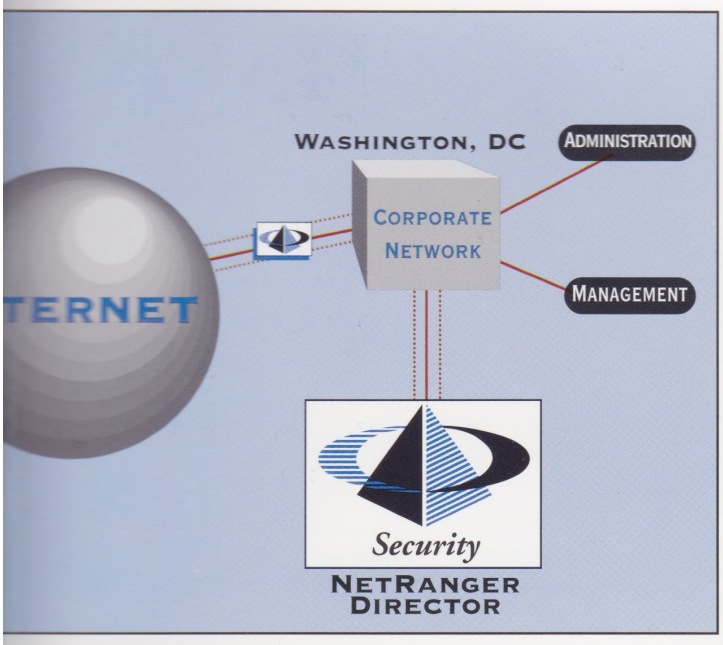
NetRanger eliminates this problem by providing real-time intrusion detection and response capability. Within seconds of detecting unauthorized activity, NetRanger can issue an alarm, log the information, and shun (i.e., block) the source of the attack or policy violation. Shunning can be performed either automatically by NetRanger, or on an attack specific basis, it can be initiated manually via the centralized Director management console. Instead of detecting something days after it has occurred, NetRanger reports the attempted violation and stops it in real time—before damage can be done.

Centralized Monitoring, Management, and Configuration Simplify Security

NSX alarms travel in real-time through an encrypted sleeve to a centralized monitoring device called the NetRanger Director. The Director software works with enterprise network management systems, displaying alarms in an easy-to-interpret graphical format. The alarms send valuable information about the attempted intrusion or unauthorized activity, such as:

- specific violation
- problem severity





- source location and port
- destination location and port
- time stamp

This data is logged into a database for file management and analysis purposes. The information and its associated metrics are stored off-line and can be analyzed to determine if additional action or investigation is needed.

The same encrypted sleeve that carries alarms also provides secure remote configuration of NetRanger components. When a new attack signature is developed by WheelGroup, or a corporate policy change is required, these new countermeasures or configuration commands can be downloaded to all field sensors quickly and securely, ensuring your network remains protected from the current and ever-changing threats.

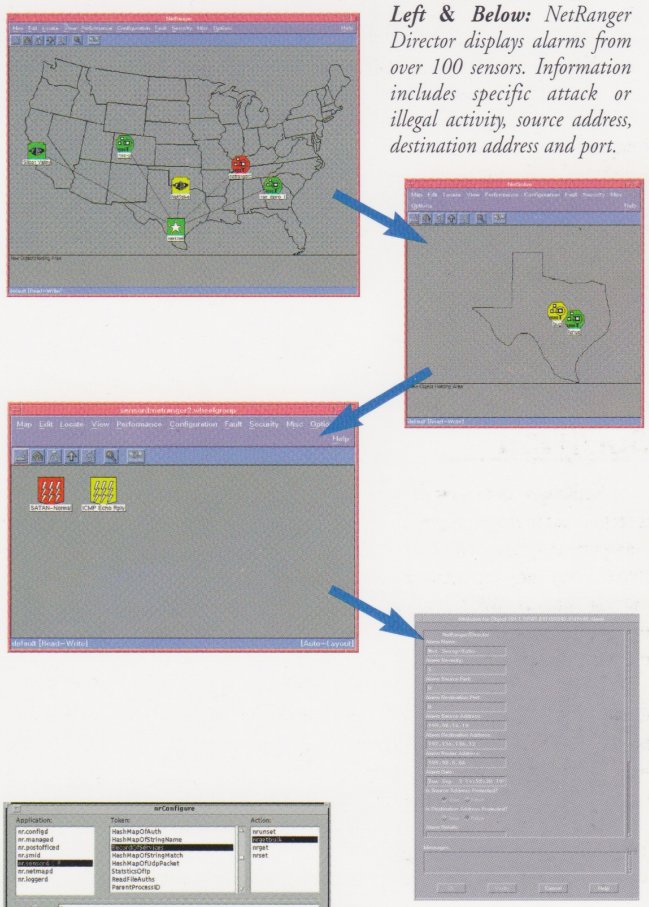
Instead of discovering days later that a hacker or employee broke into the network or critical subnet, security engineers can act quickly and effectively based on NetRanger alarms and information. They can verify that the attack was shunned successfully and, if necessary, remotely reconfigure the network router and sensor with several clicks of a button. They can even block the entire address range from which the attack originated for a period ranging from several seconds to several years. In essence, NetRanger is a proactive security solution for a potentially dangerous networked world.

In addition to allowing your organization to centralize its network security expertise, NetRanger gives you the option of outsourcing some or all of your NetRanger monitoring to a service provider whose dedicated security experts can handle security incidents 24 hours a day, 7 days a week. Centralization permits security personnel to respond to threats and incidents rapidly and consistently, thus ensuring an organization's security while effectively minimizing costs.

THE RESULT IS PERMISSIVE NETWORKING

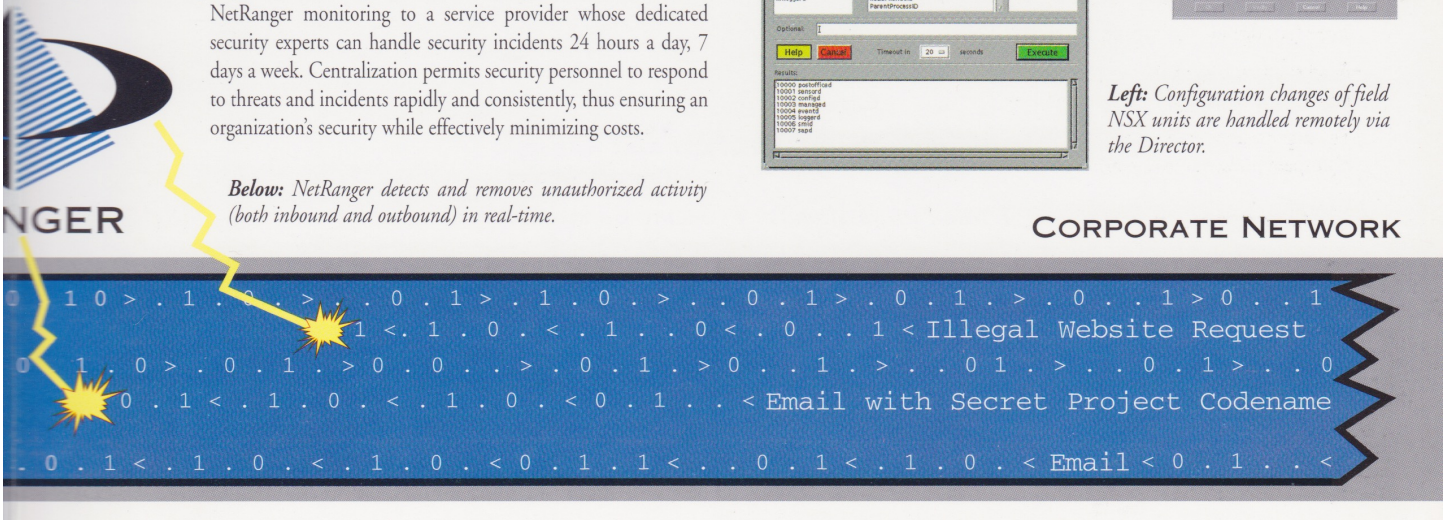
Whereas a traditional firewall often acts as a roadblock that hampers traffic on your network, NetRanger is similar to a smart traffic cop—it eliminates misuse and enforces policies while allowing legitimate users to continue their work unhampered.

In short, NetRanger allows organizations to build a permissive networking environment, where approved users are allowed to perform legitimate network-based activities without disruption. Every authorized system connection is accomplished without hindrance, but connections that violate security or misuse policies, even from authorized users, are quickly severed. Each connection is constantly monitored for misuse in real-time, giving security and network operations personnel granular levels of visibility into the network. When misuse is detected, NetRanger handles the unauthorized activity without affecting the rest of the network traffic, ensuring that an organization's operations continue.



Left & Below: *NetRanger Director displays alarms from over 100 sensors. Information includes specific attack or illegal activity, source address, destination address and port.*

Left: *Configuration changes of field NSX units are handled remotely via the Director.*



Below: *NetRanger detects and removes unauthorized activity (both inbound and outbound) in real-time.*

About WheelGroup Corporation

WheelGroup, founded in 1995, quickly established itself as the recognized leader in network-based intrusion detection and provider of original solutions to complex network security problems. The core security team honed their technical skills and methods at the U.S. Air Force Information Warfare Center and have since teamed with security and engineering experts from the commercial arena. Together, WheelGroup employees provide innovative information protection products, operational support, and consulting services to business and government organizations concerned with protecting valuable data from damage or misuse. The company is privately-held and based in San Antonio, Texas.

Trusted Professionals ◆ Secure Connections

13750 San Pedro, Suite 670
San Antonio, Texas 78232
Tel (210) 494-3383
Fax (210) 494-6303
e-mail: info@wheelgroup.com
http://www.wheelgroup.com