



Network Intrusion Detection System (NIDS)

Today, any network administrator or corporate security manager knows the feeling when confronted with evidence that critical security has been compromised by an intruder's electronic attack. What went wrong? How could this have happened? Why didn't the corporate Firewall prevent the intrusion? Is there anything available on the market for our network that performs inspection of all data traffic *before* it gets inside of our network and does damage?

The answer is, Yes: Network Intrusion Detection System (NIDS), from PenTeleData. **What is PenTeleData's Network Intrusion Detection System?**

- PenTeleData's NIDS is a round-the-clock watchdog that never sleeps, closely guarding your network's security.
- NIDS rests at the gateway of your network and inspects every packet of data that arrives from the Internet or leaves the domain of your network, operating as an inspection utility workstation scrutinizing every last packet that traverses the router or firewall.
- NIDS is not a Firewall, is less expensive than a Firewall and works best in cooperation with a Firewall to increase network protection: a Firewall prevents and protects while NIDS observes and alerts.
- NIDS is an inexpensive solution that improves an administrator's confidence in the security of his or her organization's network.
- NIDS protects any network's sensitive contents from unwanted external intrusion.

How does NIDS protect sensitive materials?

It observes and alerts, although does not respond.

- NIDS will not affect network performance.
- NIDS maintains a database – updated daily – that contains a history, nearly a decade's worth of documented attack attempts, detecting similarities.

A PenTeleData Network Intrusion Detection System (NIDS) performs the same function as a sophisticated alarm system. NIDS, however, monitors and inspects your organization's most coveted property: access to the network and its precious contents. Where any routine property alarm system detects noise, motion or a break in a circuit surrounding a door, PenTeleData's NIDS inspects, analyzes and catalogs intruders' patterns of attack, interprets slight – or not-so-subtle – alterations of the vital signs of the computer network's system, individually scrutinizing every single packet of data coming and going. NIDS immediately detects the intrusion and reports the violation to PenTeleData; the customer's security policy or intrusion response procedures determine the recourse. Choose NIDS to find out who and what is trying to gain access to your network – NIDS can tell you that it's happening. A complete NIDS is reactive and in constant use.

Typically, once an intruder has breached a private corporate network, critical systems files are modified either as an unintended consequence of the intrusion, or in order to further compromise the security of the entire computer network. What busywork do they usually undertake once inside the computer network? Damaging intruder activities are the

“As a security defense, both small and large organizations are turning to PenTeleData to create customized Network Intrusion Detection System solutions for their networks.”

Jeff Reinhard

*General Manager
- PenTeleData*

Network Intrusion Detection System

installation of Trojans, backdoor programs and password recorders. This means that not only is the electronic burglar now inside your computer network, but – like a worm – the intruder is both broadening the route through your critically sensitive, private materials while making himself increasingly familiar with your network secrets by monitoring your *own* administrative activities through alteration, modification of system files and retrieval of internal private information such as banking information, personal records, etc.

PenTeleData's NIDS is capable of monitoring network activity for certain patterns of suspicious behavior, commonly known as "attack signatures". Also, "Ping bombs", "smurf" attacks, "syn floods", "Code Red" and "Nimba" are all examples of attacks. Every day, the customer's NIDS receives specific attack signature additions to detect new kinds of attacks. PenTeleData also provides updates to the NIDS software that includes even more new attack signatures to defend against intruders. Updating the customer database every day stops an intruder's newest method to break into a system, as new attacks are already documented and added to the NIDS software.

A NIDS is similar to a security guard – its job is to detect and report, not to deter or respond. The NIDS will not tell the customer how to react or what to do in response to an attack or compromise. These types of items are normally covered in a written network security policy, or network usage policy.

How Does It Work? The NIDS device connects to a network hub or a switch that connects to the network router or Firewall. All traffic passing to or from the customer is inspected by the NIDS device. This is a one-piece solution from PenTeleData, a custom-made proprietary software service bundle. The NIDS managed intrusion service option includes the sensor, either of two software applications and a monitoring service. Due to security reasons, a customer cannot acquire parts piecemeal and must purchase the entire server suite software center. You can choose your response and options, but the package comes as a bundle. An on-site evaluation does NOT come with the PenTeleData NIDS service.

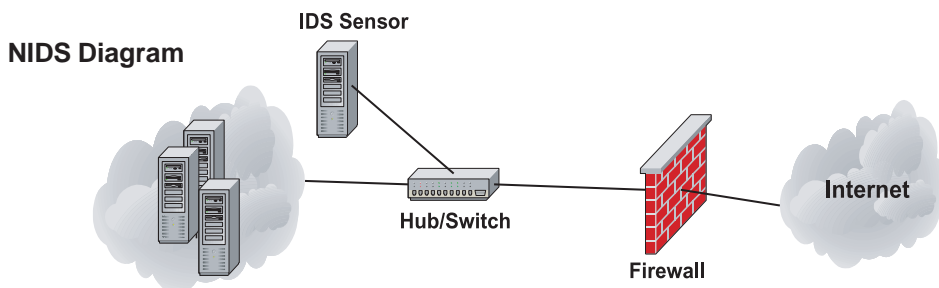
Network Control Center – Rapid Response (Managed Service Only) According to the severity of the emergency, NIDS creative response packages are tailored for various events. From simply notifying the customer in the event of a reported incident, to a response that locks down the customer facility and immediately calls law enforcement authorities, PenTeleData's emergency response team monitors and responds to a wide range of emergency reports through our 24-hour Network Control Center.

Firewalls and NIDS If you have a Firewall, do you need NIDS? Although it has its limitations, a Firewall is essential to any network security system. Firewalls prevent certain kinds of attacks, and control what type of traffic (such as Web, FTP, Telnet or IRC) passes between your internal network and the Internet. However, there are attacks that Firewalls don't prevent or detect, such as an attack on Port 80 of your web server. Firewalls protect communications between networks (typically your internal network and the Internet), and offer no or little protection from attacks or misuse within your local network. If your network perimeter is breached, or if the misuse is internal to your organization, a Firewall offers no help. NIDS helps you catch, analyze, understand and react to these types of security breaches.

NIDS vs. HIDS What's the difference between NIDS and HIDS (Host Intrusion Detection System)?

HIDS (Host Intrusion Detection System) – HIDS is a host-based PenTeleData intrusion detection tool that watches and reports on modified files critical to the operation of a customer system or systems. The HIDS generates a checksum of a directory and all files contained within that directory, if a file or directory being monitored has been altered the HIDS reports the error as a possible successful host intrusion.

NIDS (Network Intrusion Detection System) – NIDS is the network-based intrusion detection system already discussed throughout this document that monitors network activity for what is deemed as harmful activity.



Keep your network spotless: Contact **PenTeleData** IST or Sales **TODAY** to customize your system.

*Make PenTeleData work
overtime for your network
as an early warning watch-
dog: establish trustworthy,
advanced protection for
your entity by implementing
a corporate-wide
PenTeleData Network
Intrusion Detection System.*

FOR MORE INFORMATION

*To learn how your company
can take advantage of this
and the other industry leading
technologies from PenTeleData -
call us at 1-800-281-3564 or*

E-Mail: prosales@ptd.net

PenTeleData

540 Delaware Avenue
Palmerton, PA 18071
Tele: 1.800.281.3564
Fax: 610.826.4707

Product Information:

E-mail: prosales@ptd.net
Web: www.penteledata.net