

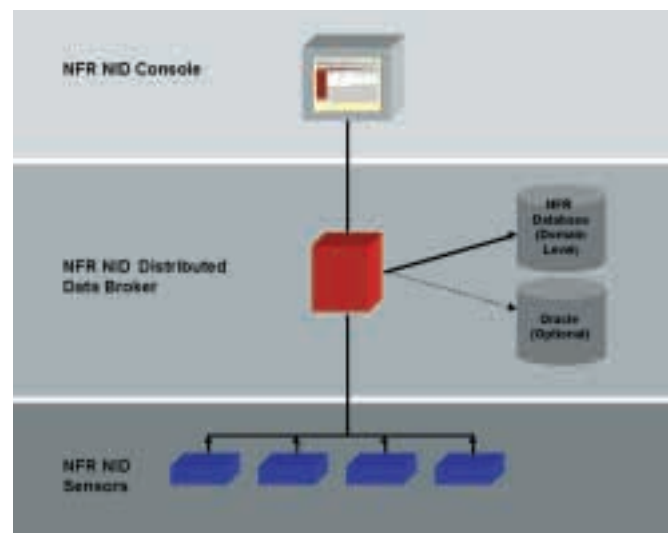
*NFR Network Intrusion Detection (NFR NID) is a comprehensive intrusion detection system that unobtrusively monitors networks, analyzes the traffic in real-time and raises alerts when suspicious activity is detected. Supplied as an appliance, NFR NID can be deployed "out of the box" and also provides extensive customization facilities such as signature tuning, development of organization specific signatures and alert annotation to document information on attacks and company security policy.*

## Features

- Sensors are delivered as pre-configured appliances: deploy fast and easily, including in lights-out environments
- Supports high performance networks: sensors available for monitoring dual or full duplex 100Mbps Ethernet networks, and GigE with failover facilities to second GigE interface, or monitoring of a backup 100Mbps Ethernet circuit.
- Performs in-depth signature and stateful protocol analysis for many network-based protocols: accurately detects all types of attacks - known, first strikes and anomalies
- Resists IDS evasion techniques: examines IP packets as well as packet fragments, reassembles TCP streams and tracks sessions
- Resists tampering: the sensor software and operating system run from the CD-ROM; the standard UNIX services, shells and drivers have been removed to make the system resistant to attack; transmissions between system components are encrypted
- Embedded operating system minimizes administration overheads: does not need to be installed nor maintained
- Fast, easy upgrade to new versions of software: simply swap out CD-ROM
- Allows users to easily tune, modify and develop signatures: enables support of customer-specific environments and proprietary protocols using powerful signature language and open signature library
- Includes extensive help information on attacks with mapping to Mitre's CVE database
- Notification is given to users as soon as new signatures are available: can be downloaded immediately from secure NFR site and mirrored to all sensors
- At user's discretion, alerts can trigger TCP resets, changes to firewall policies, and alerts can be sent to IBM Tivoli and HP OpenView

- Management console offers forensic analysis tool: enables mining of large amounts of security event data for historical and trend investigation

## System Components



An NFR NID system comprises:

NID Sensors for monitoring network traffic for attacks. The following sensors are available:

- *NID-320S* – Includes a single Gigabit Ethernet interface for monitoring gigabit circuits and 2 x 10/100Mbps Ethernet interfaces; one of which is used for management; the other can be used for monitoring a 100Mbps backup circuit
- *NID-320D* – Includes dual Gigabit Ethernet interfaces and 2 x 10/100 Mbps interfaces – one of the latter being used for management. The second gigabit interface can automatically take over if the primary interface fails

- *NID-315* – Includes 3 x 10/100 Mbps Ethernet interfaces, two for monitoring either 2 x 10/100 circuits or 1 x 10/100 full duplex. The third interface is used for management
- *NID-310* – Includes 2 x 10/100 Mbps Ethernet interfaces, one for monitoring and one for management
- *NID-100* and *NID-200* sensors from NFR NID V1

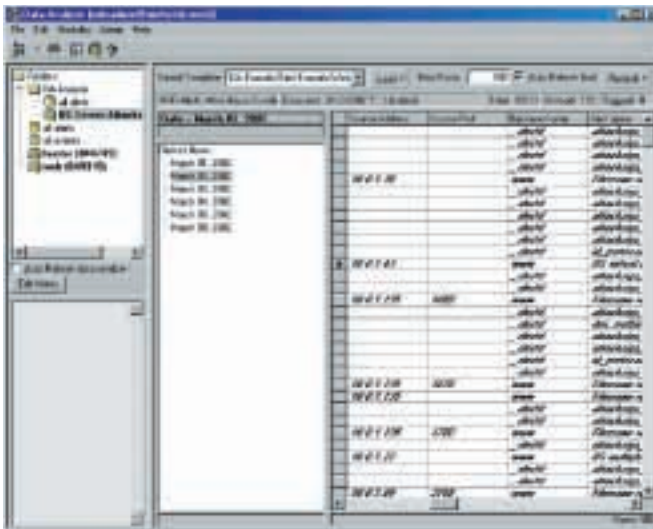
All NID-300 sensors are delivered as complete appliances. The NID-310 is also available in a software-only version.

**NFR NID Distributed Data Broker** (NFR NID DDB) – for collecting alert and event data from its associated sensors. Multiple NFR NID DDBs can be installed in a distributed environment. NFR NID DDB includes:

- NFR Central Management Server for storing data from the NID sensors
- DbExport for optional export of data from NFR CMS to an Oracle database

**NFR NID Console** for the administration, operation and analysis of sensors. NFR NID Console includes:

- NFR Administration Interface (NFR AI) for administering sensors, querying alerts and reporting.
- Data Analysis product for forensic analysis of post-event data exported from NFR NID DDB to the Oracle database.



Screen shot showing results of an investigation using DA Tool

## System Requirements

### NFR NID DDB

- NFR CMS supports:
  - Solaris 2.7
  - Redhat Linux 7.1, 7.2
- DbExport supports
  - Oracle 8.1.7. DBExport is installed on the same server as NFR CMS

### NFR NID Console

- NFR AI supports:
  - Windows, 2000, NT Server 4.0, NT workstation 4.0
- Data Analysis tool supports:
  - Windows 2000, NT or XP and requires screen resolution of at least 1024x768

### Hardware for NID-310 Software-Only Version

- Processor: Pentium III 800MHz or faster
- Memory: 512MB RAM
- Hard drive: 20GB EIDE
- Two network cards consisting of some combination of the following:
  - 3Com Fast EtherLink XL (3C905C) ethernet card
  - Standard Microsystems EtherPower II 10/100 (SMC9432-TX) ethernet card
  - Intel EtherExpress Pro 10/100+
- CD-ROM
- 1.44MB floppy drive