

# Nokia Intrusion Prevention and IP-series updates

Harri Hämäläinen  
Technical Manager, FinBalt  
Nokia Enterprise Solutions



- Nokia IPSO operating system
- Nokia IP Platforms
- SourceFire in Nokia appliances
- Nokia Support offering



# Nokia IPSO



- **New Features:**
  - New look and feel of Network Voyager
  - Role-based management (Role-Based Access Control)
  - IP Clustering for IP2250
  - BGP 4+ (BGP For IPv6)
  - SNMP v3 USM Improvements
  - Route maps
- **New Interface Card: 10GigE**
- **Support Check Point VPN-1 NGX R60**
- **Platform Support**
  - IP120/130, IP260/265, IP330, IP350/355/380/385, IP530, IP650, IP710/740, IP1220/1260, IP2250
- **Upgrade Path: IPSO 3.5, ..., IPSO 3.9**

# IPSO 4.0: Network Voyager Layout

The screenshot shows the Nokia Network Voyager web interface in a Microsoft Internet Explorer browser window. The browser title is "Nokia Network Voyager (mazy) - Microsoft Internet Explorer provided by NOKIA". The address bar shows "http://10.10.10.10:8080". The page title is "Nokia Network Voyager" and the current configuration state is "Unsaved".

**Navigation:** A callout box points to the left-hand navigation tree. The tree is expanded to show the "System" configuration area, with sub-items like "Configuration", "Interface Configuration", "System Configuration", "High Availability", "Security and Access", "Routing", "Traffic Management", "Router Service", "IPv6 Configuration", "Asset Information", "Monitor", "Reports", "System Health", "System Logs", "Routing Protocols", and "Hardware Monitoring".

**Data:** A callout box points to the main content area. It contains a "mazy" information box with the following details:

<b>Model:</b>	IP630
<b>Software Release:</b>	4.1_BUILD019
<b>Software Version:</b>	relong 1515 09.01.2006-021932
<b>Serial Number:</b>	9N012400116
<b>Current Time:</b>	Tue Nov 7 12:00:09 2006 CET
<b>Uptime:</b>	2 hours 46 minutes
<b>Physical Memory:</b>	256 MB
<b>User:</b>	admin

Below this is an "Active Packages" table:

Package	Description
/opt/shells	Unix Shells (bash-2.05,tcsh-6.10.00,pdksh-5.2.14,tsh-3.0.8) for IPSO-3.4-FC84

**Apply:** A callout box points to the "Apply" button at the bottom of the interface, next to "Reset" and "Save" buttons.

# IPSO 4.0: Network Voyager Config Example

**Nokia Network Voyager** Current Configuration State: **Unsaved** [Log Off](#)

**System** Tue Oct 4 04:34:45 2005 GMT [Help](#)

**Clustering Configuration**

[Change admin password](#)

**Cluster Status**

Cluster ID:

Cluster Protocol State:  (master)

Time Since Join: 0:05:34:37

Number of Interfaces: 2

Cluster State:  Up  Down

Cluster Mode:  Multicast  Multicast with IGMP  Forwarding

Work Assignment:  static  dynamic

Performance Rating (default: 230):

Failure Interval (Milliseconds):

Delete cluster configuration on this system:

**Interface Configuration**

Interface	Status	Select	Networks Connected	Cluster IP Address	Primary	Secondary	Hash Selection
<a href="#">eth-s1p1c0</a>	<input checked="" type="radio"/>	<input type="radio"/> Yes <input checked="" type="radio"/> No	205.226.18.0/24	<input type="text"/>	<input type="radio"/>	<input type="radio"/>	default
<a href="#">eth-s1p2c0</a>	<input checked="" type="radio"/>	<input checked="" type="radio"/> Yes <input type="radio"/> No	10.0.20.0/24	<input type="text" value="10.0.20.101"/>	<input checked="" type="radio"/>	<input type="radio"/>	default
<a href="#">eth-s1p3c0</a>	<input checked="" type="radio"/>	<input checked="" type="radio"/> Yes <input type="radio"/> No	10.0.30.0/24	<input type="text" value="10.0.30.101"/>	<input type="radio"/>	<input type="radio"/>	default

**FireWall Related Configuration**

**FireWall Table**

Enable VPN-1/FW-1 monitoring:  Enable  Disable

# IPSO 4.0: Network Voyager Monitor Example

**Nokia Network Voyager** Current Configuration State: **Unsaved** [Log Off](#) **NOKIA**

**CPU Utilization Report** Tue Oct 4 04:56:22 2005 GMT [Help](#)

Select Report Type:

- Hourly
- Daily
- Weekly
- Monthly
- Detailed Search Start date:  End date:

Select Format:

- Graphical View
- Delimited text (suitable for download) Delimiter:

**CPU Utilization for Mon Oct 03 2005**

**CPU Utilization**

**Pie Chart Legend:**

- 1 - Idle
- 2 - System
- 3 - User
- 4 - Interrupt

**CPU Utilization**

Reset Apply Save

# IPSO 4.0: Network Voyager Cluster configuration

The screenshot displays the Nokia Cluster Voyager web interface. At the top, the title is "Nokia Cluster Voyager" with a user "rms5.eng" and a "Current Configuration State: Unsaved" indicator. A "Log Off" button and the "NOKIA" logo are also present. The left sidebar shows a navigation tree with "Cluster" selected, containing sub-items like Configuration, Interface Configuration, System Configuration, High Availability, Clustering, Security and Access, Routing, Traffic Management, Router Service, Asset Information, and Monitor. The main content area is titled "Clustering Configuration" and shows the following settings:

- Cluster Status:** Cluster ID: 103; Cluster Mode:  Multicast  Multicast with IGMP  Forwarding; Work Assignment:  static  dynamic; Failure Interval (Milliseconds): 500.
- Cluster Members:** A table with columns "Member ID" and "Performance Rating". One member is listed: 10.0.20.55 with a performance rating of 230.
- Clustering Monitor:** A radio button option that is currently selected.
- Network Configuration:** A table with columns: Network, State, Select, Cluster IP Address, Primary, Secondary, and Hash Selection.

Network	State	Select	Cluster IP Address	Primary	Secondary	Hash Selection
10.0.20.0/24	<input checked="" type="radio"/>	<input checked="" type="radio"/> Yes <input type="radio"/> No	10.0.20.101	<input checked="" type="radio"/>	<input type="radio"/>	default
10.0.30.0/24	<input checked="" type="radio"/>	<input checked="" type="radio"/> Yes <input type="radio"/> No	10.0.30.101	<input type="radio"/>	<input type="radio"/>	default
205.226.18.0/24	<input checked="" type="radio"/>	<input type="radio"/> Yes <input checked="" type="radio"/> No		<input type="radio"/>	<input type="radio"/>	default

Below the network configuration table, there is a "FireWall Related Configuration" section with a "FireWall Table" sub-section. The "FireWall Table" includes:

- Enable VPN-1/FW-1 monitoring:  Enable  Disable
- Cold Start Interval (Seconds): 30

At the bottom of the configuration area, there are "Reset", "Apply", and "Save" buttons. The status bar at the very bottom of the browser window shows "Done".



- Support for IP560 Network Security Platform
- Support for 10 Gigabit Ethernet NIC
- IP Clustering Support for IP2250
- Improved Network Voyager User Interface
- Role-Based Administration
- SNMP v3 User Enhancements
- OSPF Not-So-Stubby-Areas (NSSA)
- BGP-4++ for IPv6
- Route Maps
- Support for Longer User Names
- Enhanced Downgrade for Flash-Based Systems

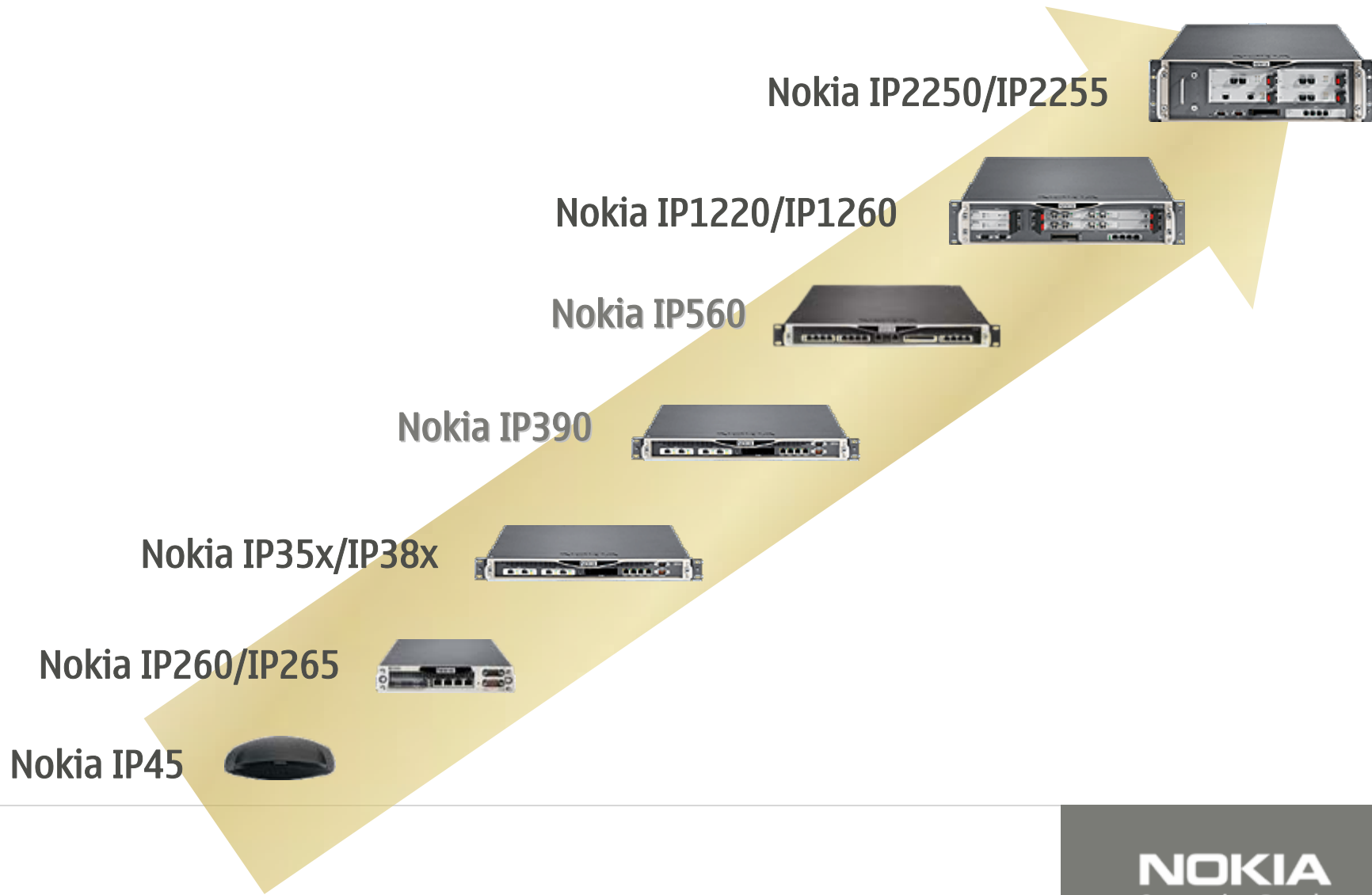
## IPSO 4.1 contains the following new features and enhancements

- Support for New Platforms
- Enhancements for Time Configuration
- Enhanced Link Detection for Fiber Connections
- Enhancement for Link Aggregation
- Enhancements for Transparent Mode
- IP Cluster Support for BOOTP/DHCP Relay
- Support for Nonlocal Users
- SSH v1 and Telnet Disabled by Default

# New Nokia IP-Platforms

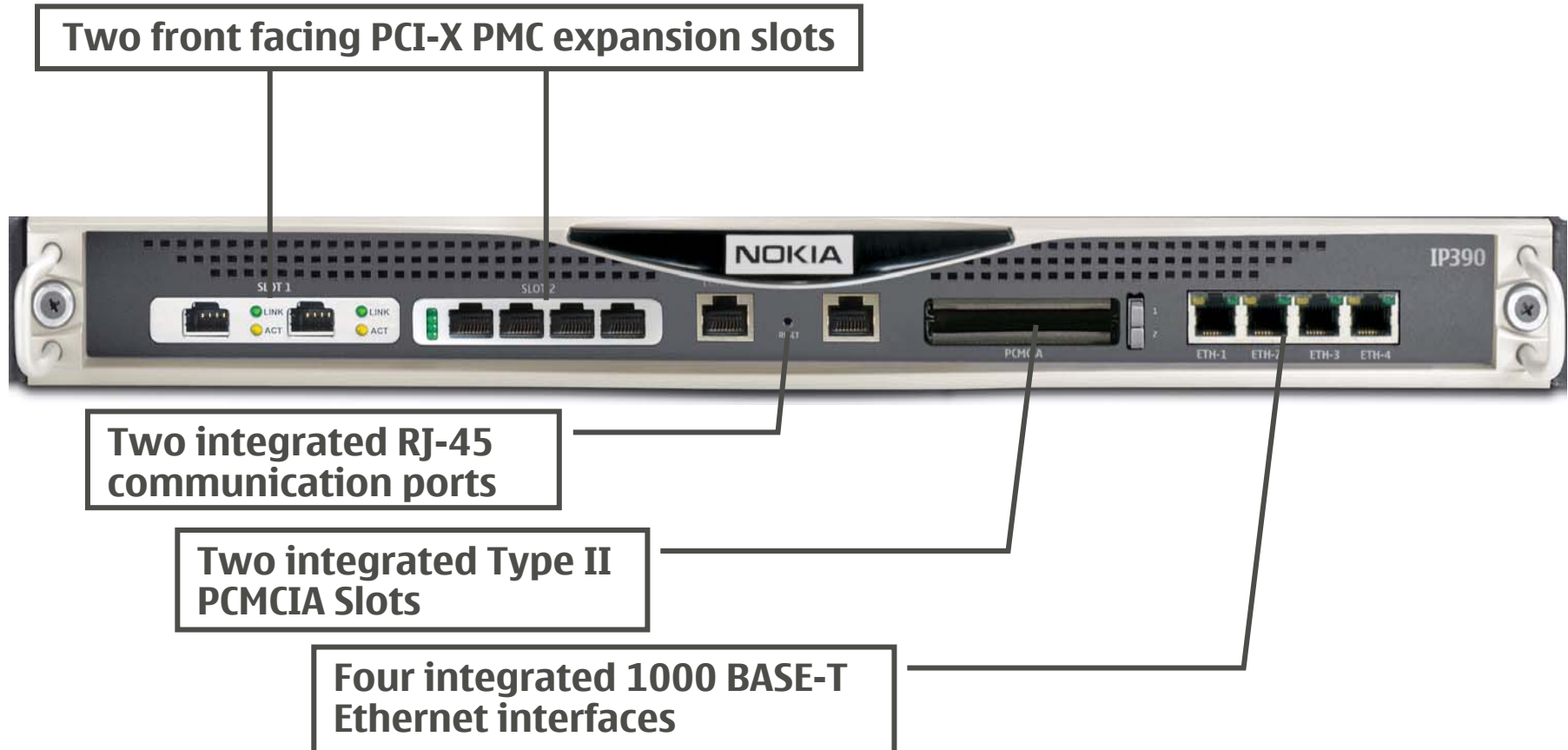
Nokia for  
Business





- New Vstream Anti-Virus - Antivirus Configuration (Signatures), Policy (Rule Base)
- Advanced Antivirus Settings (File Types, Archive File Handling and Corrupt Files)
- 802.1x port-based security
- Integrated L2TP VPN Server
- Enhanced Syn-Defender Configuration
- Smart Defense Policy Wizard
- New Administrative Role: Users Manager
- High Availability - WAN Virtual IP
- Backup DHCP Relay
- New Internet Connection Wizard
- New Security Level - Block All
- Enhancements in wireless HotSpots

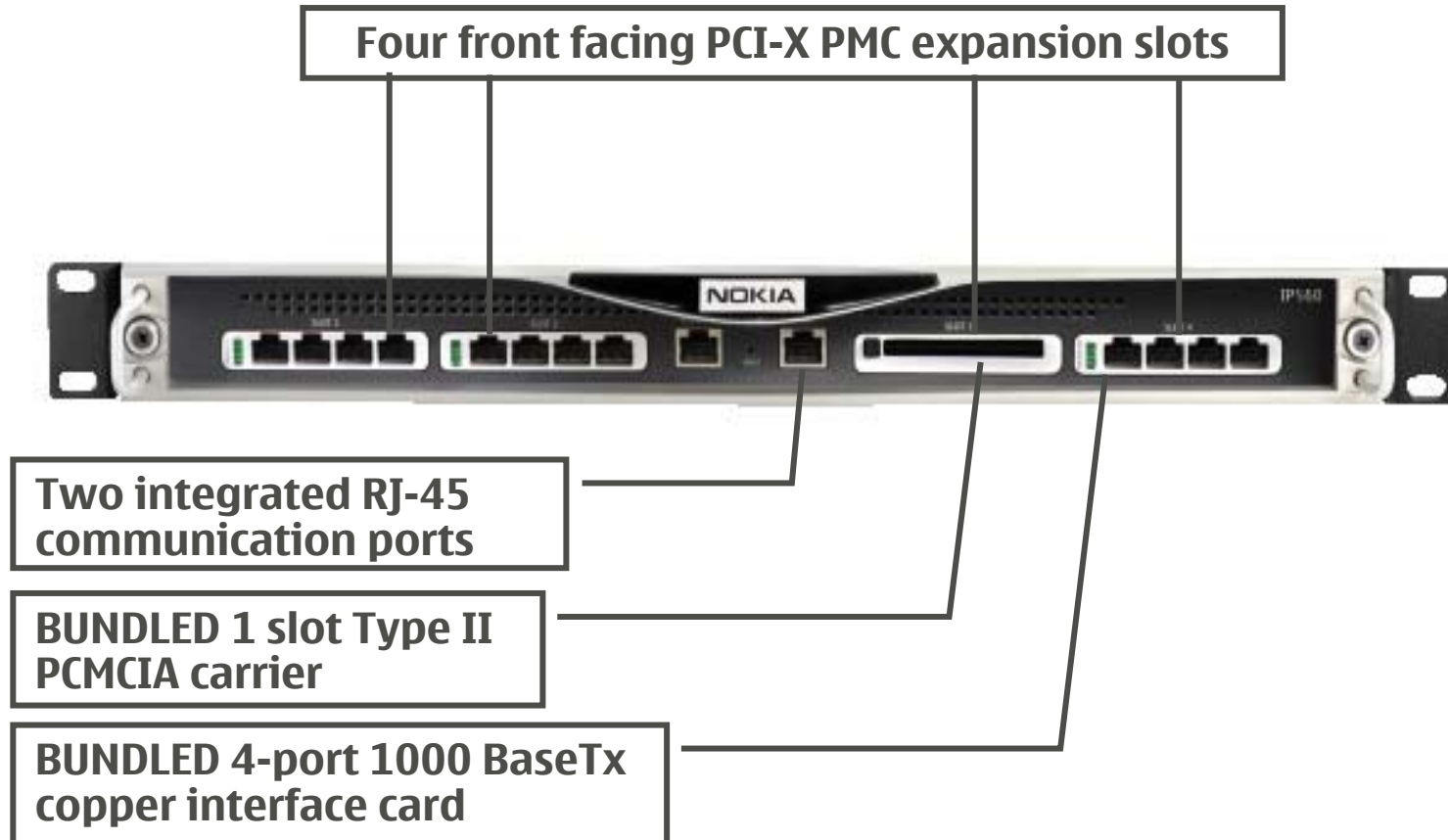




- Pricing
  - Nokia IP390 - \$6,995
  - **Nokia IP390“G”: IP390 + two 2-port 1000 BASE-T cards - \$10,995**
- RoHS compliant / lead-free manufacturing
- Four integrated 10/100/1000 BASE-T Ethernet interfaces
- Integrated Type II PCMCIA slots
- 1 GB RAM, expandable to 2 GB
- 1GB Solid-state compact flash
- 40 Gig hard disk drive
- Two external facing PCI-X PMC card slots
- Supported network interface cards
  - Four-port 10/100 BASE-TX Ethernet
  - Two-port 1000 BASE-SX Fiber Ethernet
  - Two-port 10/100/1000 BASE-T Ethernet
- Two RJ-45 Communication Ports

- Software requirements
  - Nokia IPSO 4.1
  - Check Point R55P, NGX R60, NGX R61
  
- Performance highlights
  - 3 Gbps large packet firewall (1518-byte UDP)
  - 300 Mbps small packet firewall (64-byte UDP)
  - 5,600 HTTP transactions per second
  - 3,000 TCP connections per second
  - 500 Mbps large packet encrypted VPN (1450-byte UDP)
  
- Keep in mind
  - Nokia IP390 does NOT support WAN cards
  - Nokia IP390 does NOT support non-RoHS interface cards
  - Nokia IP390 interface cards are not hot-swappable
  - Check Point management cannot be run on Nokia IP390 Flash version





- Up to 2GB RAM
- Solid-state slot (Compact Flash)
- Up to two hard disk drives
- Disk mirroring
- Four external facing PCI-X PMC card slots
  - One pre-populated with four-port 10/100/1000 Mbps Ethernet
  - Supported network interface cards
    - Four-port 10/100 Mbps Ethernet
    - Four-port 10/100/1000 Mbps Ethernet
    - Two-port 1000 Mbps Fiber Ethernet
    - Two-port 10/100/1000 Mbps Ethernet
- Single Internal PCI-X PMC Card Slots
  - Bundled VPN accelerator card

- Software requirements
  - Nokia IPSO 4.0.1
  - Check Point R60 NGX, R55P under Selective Availability program
- Pricing
  - **Nokia IP560 - \$16,495**
  - 4 port 10/100 card - \$1,500
  - 2 port GigE (copper and fiber) card - \$4,500
  - 4 port GigE card - \$6,000
- Performance highlights
  - 6.0 Gbps large packet firewall (1518-byte UDP)
  - 440 Mbps small packet firewall (64-byte UDP)
  - 8,900 HTTP transactions per second
  - 58,000 TCP connections per second
  - 1,500 Mbps Nokia traffic mix
- Keep in mind
  - Nokia IP560 does NOT support WAN cards
  - Nokia IP560 does NOT support non-RoHS interface cards
  - Nokia IP560 interface cards are not hot-swappable
  - Check Point management cannot be run on Nokia IP560 Flash only version

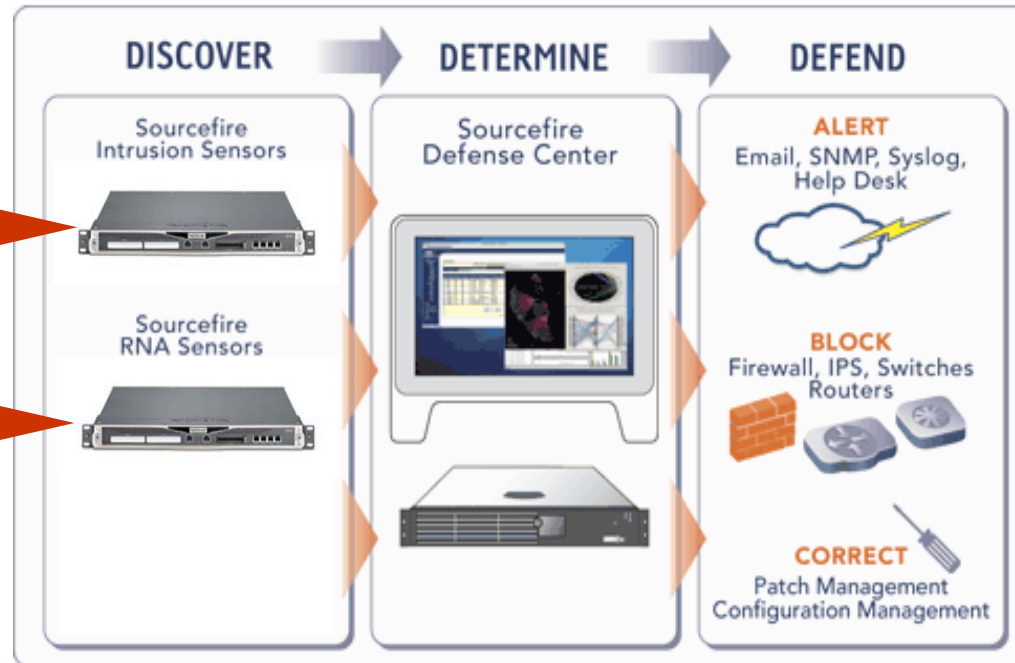
# Nokia Intrusion Prevention

Nokia for  
Business



## Sourcefire 3D System

- Sourcefire Intrusion Sensor for Nokia IP390
- Sourcefire RNA Sensor for Nokia IP390
- Sourcefire Defense Center for Nokia



- 1 RU system and with single AC power
  - Same exact system as IP390
- Base Configuration
  - Built in 4 port 10/100/1000Base-TX and PCMCIA Slots
  - 2 empty PMC slot (uses current I/F modules common to IP390 & IP560)
    - **NEW** 'fail-open' 2 port 10/100/1000BaseTX and 1000Base-SX for 'inline' IPS' deployment
  - Console (RJ45) and AUX (RJ45)
  - HDD version only (64 Mb Flash + 1 Gig DRAM + 40 Gig HDD)
- Software:
  - IPSO – LX + SF application



- Sourcefire Intursion Sensor
  - SNORT® based detection Engine
  - In-line or Passive Monitoring
  - Pre-loaded on appliance
- Sourcefire RNA Sensor
  - Real-Time Network Awareness
  - Asset Monitoring
  - Enhanced Awareness
  - Pre-loaded on appliance

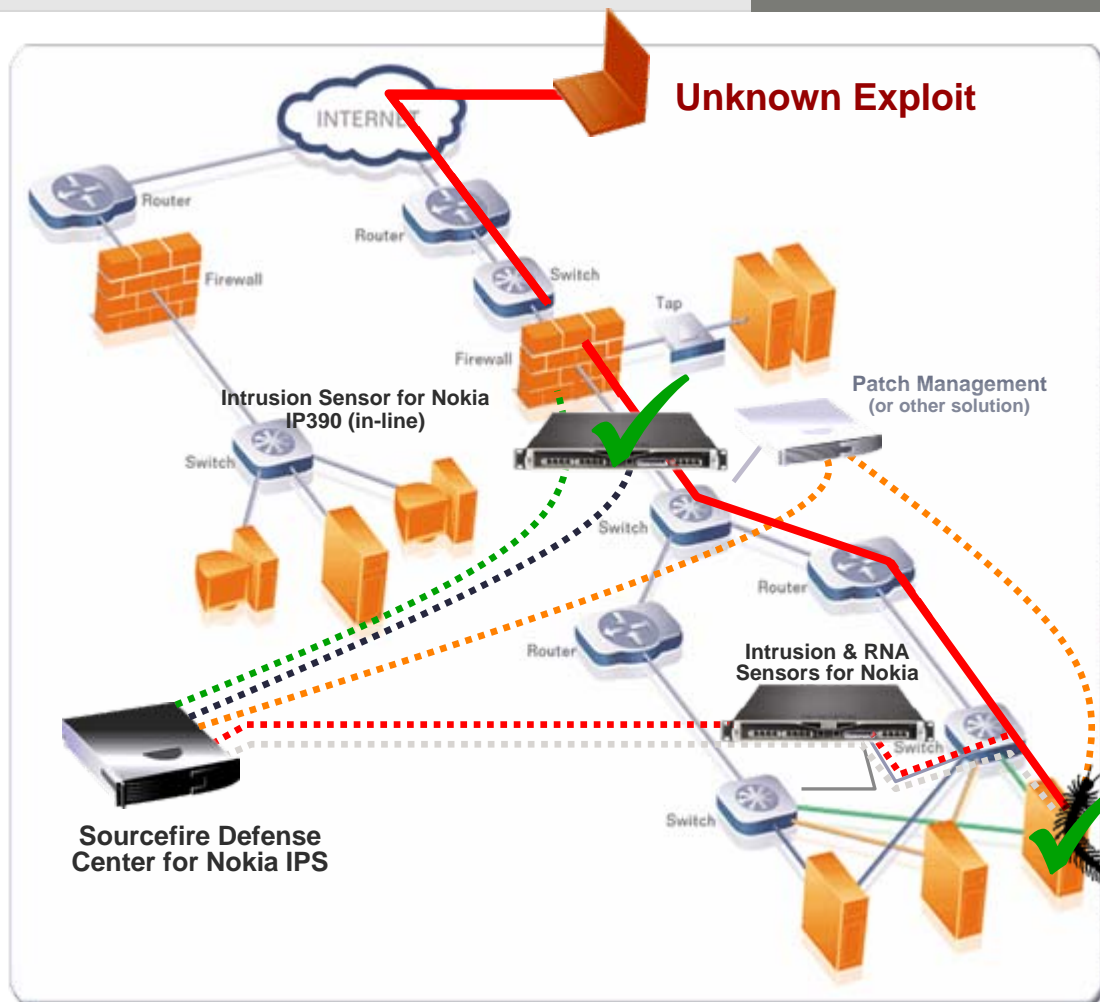


- Both Intrusion Sensor and RNA Sensor can run at the same time on a single appliance

- IP390 Sensors can have up to 2 Detection Engines (DE)
- Each Detection Engine can be used for the following
  - In-line prevention – on a single port pair
  - Passive monitoring for Detection – for any number of ports
  - Passive monitoring for RNA – for any number of ports
- IP390 Interface card options
  - 4 on-board ports, dual-port fail open Gigabit and dual-port passive Gigabit
  
- The deployment options with various ports
  - With Fail-Open cards:
    - 1 port-pair In-Line (1-DE), 2 port-pairs In-Line (2-DEs) and 1 port-pair In-Line & rest of the ports (up to 5) can be monitored by IDS or RNA mode (2-DEs)
  - With non fail open cards:
    - 1-7 ports monitored by IDS (1-DE), 1-7 ports monitored by RNA (1-DE), and x of 7 monitored by RNA AND x of 7 monitored by IDS (2-DEs) or
    - All 7 could be monitored by RNA and IDS at the same time (2 DEs)



1. Reconnaissance activity detected by passive Intrusion Sensor, events associated with the target assigned higher priority.
2. RNA detects change in the behavior and/or composition of the compromised asset.
3. Correlated events trigger remediation policy:
  - Isolate compromised server
  - Block attacker at firewall
  - Direct configuration mgmt.
  - Notify system administrator
4. In-line Intrusion Sensor policy updated to prevent recurrence.





Nokia for  
Business

# News on ES Services

**NOKIA**  
Connecting People

- We still sell Essential and Access Service
  - Well established and known procedures
  - This scheme normally applies to all even new service offerings as the model is well understood by the whole channel
  
- What is going to change in very near future is the **response times**
  - This is also to align with IntelliSync service offerings
  - 12x5 response time to be established instead of 8x5
    - Next Business Day Advance Replacement definitions remain the same (8x5xNBD)
  - 24x7 remains as it is
  
- **Onsite** (Essential or Access Plus offerings) coverage keeps changing, new areas are being established, check always the latest offerings from [support.nokia.com](http://support.nokia.com) at QuoteService – View Service Availability
  
- **Access and Access Plus Services** are also available, especially for big end customers that have good technical expertise and want direct access Nokia technical support personnel

## Nokia Access

### Business Model:

- Sold through the channel
- Support provided directly by Nokia



### Channel Benefits:

- Low cost - no additional resource requirement for channel
- Complete leverage of Nokia expertise of solution

PLAN FEATURES	Nokia Access 5x12	Nokia Access 7x24
Audience	ENTERPRISE	ENTERPRISE
Plan Type	Extended Business Day (5x12)	7x24
Plan Term	1 Year	1 Year
Annual Min. Support Fee	\$1000	\$1000
Access to Technical Assistance Centers	✓	✓
Named Contacts	2	4
Response Times	<2 hours	<2 hours
Software Updates	✓	✓
Access to Support Web and Electronic Support	✓	✓
Multi-Vendor Coordination	✓	✓
Migration/Upgrade Support	✓	✓
<b>PLAN OPTIONS</b>		
Onsite Installation Services	Optional	Optional
Technical Account Management	Optional	Optional
Additional Named Contacts	Optional	Optional
Pre-scheduled On-site Support	Optional	Optional
On Site Technical Training	Optional	Optional

## Nokia Essential

### Business Model:

- Sold and delivered by Channel
- Nokia provides backline support to channel



### Channel Benefits:

- Channel has full power and maximum customer intimacy
- Complete leverage of Nokia expertise of solution

PLAN FEATURES	ESSENTIAL 7x24
Audience	CHANNEL PARTNER
Plan Type	7x24
Plan Term	1 Year
Annual Min. Support Fee	\$1000
Access to Technical Assistance Centers	✓
Named Contacts	2
Response Times	<2 hours
Software Updates	✓
Access to Support Web and Electronic Support	✓
Multi-Vendor Coordination	✓
Migration/Upgrade Support	✓
PLAN OPTIONS	
Onsite Installation Services	Optional
Technical Account Management	Optional
Additional Named Contacts	Optional
Pre-scheduled On-site Support	Optional
On Site Technical Training	Optional

## ❑ *With Support, ES provides:*

- ❑ Next business day HW replacement
  - ❑ Minimized downtime for best customer satisfaction
  - ❑ Optional onsite support available
- ❑ SW updates and knowledge base web
  - ❑ Keep your SW up-to-date and secure
  - ❑ Get all product knowledge you need
- ❑ 24x7 technical support
  - ❑ Technical Assistance Centers you can count on

## ❑ *Without Support:*

- ❑ 12 months limited HW warranty (30 day turnaround)
- ❑ No SW updates / upgrades
- ❑ No knowledge base access
- ❑ No technical backup support from Nokia ES
- ❑ ***IMPLICATIONS:***
  - ❑ No fast HW replacements
  - ❑ System SW not maintained
  - ❑ No technical support from TAC

- **Global footprint**
  - Expert resources strategically located
- **TAC 7x24 availability**
  - Deep technical expertise on Device, Security & Mobility apps
  - Annually certified through SCP
- **Single Point of Contact**
  - First Call – Final Resolution
  - Collaborative support
- **Nokia Support Web**
  - Online Ask Nokia - Knowledge Base
  - Documentation & Self help
  - QuoteService
- **Expansive labs to replicate and troubleshoot customer issues**



*A strong market differentiator....*

Issues	Crossbeam Problem	Result	Nokia Solution
<b>Single-source support</b>	<ul style="list-style-type: none"> <li>• Crossbeam commitment to and ability to support its application partners is questionable</li> <li>• Multiple customers have indicated application support is a problem</li> </ul>	<ul style="list-style-type: none"> <li>• Slow time-to-resolution slows when customer needs it the most</li> <li>• Must purchase both Crossbeam &amp; application vendors support increasing overall support costs</li> </ul>	Nokia First Call – Final Resolution support offerings includes support for Check Point VPN-1 Pro.
<b>Replicating/ troubleshooting customer issues</b>	Customers have indicated Crossbeam does not have the ability to replicate a customer issue at its TAC centers	<ul style="list-style-type: none"> <li>• Slow time-to-resolution</li> <li>• Customer must expend extra resources to document issues</li> </ul>	Nokia Product Line Support specialists have the resources necessary to reproduce customer environments and issues
<b>Comprehensive knowledge base</b>	Customers have indicated that Crossbeam's knowledgebase is "non-existent"	Inhibits the customers ability to troubleshoot problems	Nokia maintains a complete knowledgebase, often regarded as superior to Check Point's
<b>Language skills</b>	<ul style="list-style-type: none"> <li>• Customers have indicated that Crossbeam's thin TAC resources – especially in EMEA – can run into language skills issues, even for English</li> <li>• This is symptomatic of overall thin support resources</li> </ul>	<ul style="list-style-type: none"> <li>• Slows time-to-resolution</li> <li>• Problems with English in EMEA may impact U.S. 7x24 support offerings</li> </ul>	Nokia TAC centers are able to provide support all over the world 7x24*  <i>* Nokia leverages channels in several countries for local language Level 1 and Level2 support</i>

Nokia for  
Business



THANK YOU!

**NOKIA**  
Connecting People