nAppliance
application protection & acceleration

nAppliance IntruPro Network IPS Appliances
Industry Leading Intrusion Detection and Prevention System

Datasheet

nIPS IntruPro Series: Network Protection Solutions

The Challenge

Addressing the emergence of new vulnerabilities and threats to enterprise networks is a continual security challenge. Attackers are developing new types of attacks targeting new vulnerabilities. Deploying firewall and anti-virus technology is important, but is insufficient to defend against today's threats. New attacks using hybrid approaches are becoming increasingly common. Organizations must deploy multi-layer defense-in-depth technologies to effectively defend their networks and IT infrastructure against today's dynamic and ever-changing threats.

The Need for Proactive Threat Prevention

To ensure comprehensive security, enterprises need to deploy a multi-layer architecture that proactively detects and prevents attacks, including both known and unknown (zero-day) attacks before they can affect critical assets. Intrusion Prevention solutions requireongoing research to identify new attacks. New signatures must be developed foremerging attacks, and a distribution mechanism must exist to disseminate new attack signatures to IPS systems deployed in customer networks. The proven nAppliance network intrusion prevention (IPS) solution delivers the most comprehensive, accurate, and scalable intrusion protection, helping enterprises to ensure the availability and security of their critical network infrastructure through proactive risk prevention.

The nAppliance IntruPro Solution

The nAppliance IntruPro network IPS delivers advanced real-time protection against known and zero-day (unknown) attacks, as well as spyware. The nAppliance IntruPro series is a complete, highly accurate, and scalable network IPS solution, on a choice of convenient appliance platforms, for a broad range of network applications. As part of a multi-layer, defense in depth deployment, the nAppliance IntruPro appliances deliver comprehensive and proactive intrusion prevention to ensure business availability and protect critical network infrastructure by detecting and blocking attacks before they can cause damage. The nAppliance IntruPro family includes multiple appliance platforms that scale from 100Mb/s to 750Mb/s bandwidth rates. The IntruPro appliances deliver comprehensive protection, and can be deployed in various network configurations, providing enterprise scalability in both large and small enterprise environments.

The innovative nAppliance IntruPro architecture integrates signature matching, anomaly detection, and Denial of Service (DoS) analysis techniques, enabling highly accurate attack detection and prevention at up to multi-gigabit speeds. Utilizing multiple detection techniques provides protection from both known and zero-day (unknown) attacks, DoS attacks, and spyware. IntruPro delivers advanced network IPS and internal network firewall integration, offering the most accurate and comprehensive protection available in the industry. The IntruPro product family includes the nIPS 1000, nIPS 500, and nIPS 100, four powerful and purpose-built network IPS appliances that provide the performance and functionality your mission critical networks require. As part of the complete IntruPro solution, nAppliance provides the IntruPro Security Management (ISM) system with all IntruPro appliance models. IntruPro ISM is a powerful and scalable security management solution, capable of managing one or many IntruPro appliances.

nAppliance are powered using Intoto's IntruPro technology, Intoto conducts ongoing research on new attacks, develops new signatures, and provides automatic signature updates for IntruPro appliances deployed in the field. As new attacks are identified, nAppliance customers with IntruPro appliances are automatically delivered the latest signatures to identify and prevent these attacks. The nAppliance IntruPro IPS implemention is tested and certified by NSS, a leading independent security testing organization.

Feature & Benefits

Complete Protection

Attack Detection via Signature, Network Behavior, and Protocol Anomaly:

- Protects against known, zero-day (unknown), and DoS attacks
- Signature matching for over 3,000 multi-token/multi-trigger attack signatures, with fewer false positives
- Advanced evasion resistance provides unparalleled accuracy in recognizing attacks
- Patent pending application intelligence
- P2P and IM detection, conserves bandwidth

Integrated IPS and Internal Firewall:

- Integrates traditional firewall functionality and advanced IPS capabilities in integrated platform

Intrusion Intelligence:

- Powerful capabilities provide highly accurate information related to intrusion identification, relevance, attack direction, impact, and analysis
- Highly accurate, fewer false positives
- Detects port scans

Bandwidth Management:

- Identifies P2P protocols and traffic
- Identifies IM protocols and traffic
- Bandwidth management for P2P and IM traffic-rate limiting and protocol blocking to conserve network bandwidth and provide data leak prevention capability

Scalability and Management

Enterprise-Wide Scalability:

- A full suite of appliance solutions that scale from 100 Mb/s to multigigabit data rates, IntruPro's nIPS appliances scale to address enterprises of all sizes

Central Management:

- Centralized management is enabled through IntruPro Manager Software installed on a client machine. The integrated management software enables central configuration, logging, monitoring, and reporting for all network-wide IntruPro appliances.
- Easy setup wizard, comprehensive configuration and customization
- Provides complete traffic and policing views for administrator, detects services, ports, and protocols in use on network

Flexible Deployment:

- nIPS appliances may be deployed inline at numerous places in the network, depending on your requirements. Common deployments include placement in front of the enterprise firewall, behind the firewall, on the DMZ, or in front of sensitive application servers or databases.

Continuous Threat Research, Automated Real-time Updates:

- Automated, real-time delivery of signature updates without requiring appliance reboots
- Provides protection against newly discovered threats and vulnerabilities , eliminates manual update procedures, and downtime of IPS or IDS deployment.

The nIPS 1000

The IntruPro nIPS 1000 delivers the high performance and scalability required by mid-large enterprises environments. It offers operational redundancy required to secure a high availability network infrastructure, along with economics of scale needed by large enterprises, data centers, and service providers.

- Two Gigabit Ethernet detection ports with LAN By-Pass
- One Management port, One Aux port
- Redundant Hot-Swappable Power Supply
- Purpose-built for high performance, and low latency
- Up to 750Mb/s performance

The nIPS 500

The IntruPro nIPS 500 is a cost-effective IPS solution for mid-size, remote/branch office networks, or for deployment at the perimeter of enterprise networks.

- Two Gigabit Ethernet detection ports
- One Management port, One Aux port
- Purpose-built for high performance, and low latency
- Up to 400Mb/s performance
- Best Price Performance Ration in the Industry

The nIPS 100

The IntruPro nIPS 100 is a cost-effective solution for smaller enterprises, or for remote locations and branch office networks.

- Two Gigabit Ethernet detection ports
- Purpose-built for performance, and low latency
- Up to 100Mb/s performance

IntruPro Appliance Specifications

Appliance Models	**I-1000**	**I-500**	**I-100**
Network Deployment	Core/Perimeter	Branch Office Or Perimeter	Branch Office
Appliance Throughput	Up to 750Mb/s	Up to 400Mb/s	Up to 100 Mb/s
Maximum Simultaneous Connections	200,000	80,000	40,000
Ports			
Gigabit Ethernet GbE Detection Ports	4	4	2
Fast Ethernet (FE) Detection Ports	–	–	–
Dedicated GbE Management Port	Yes	Yes	No
By-pass Support	Yes	No	No
Auxiliary Port	Yes	Yes	No
Console Port	Yes	Yes	Yes
In-Line Mode	Yes	Yes	Yes
No. of Virtual IPS Systems	100	32	16
Traffic Monitoring on Active-Active Links	Yes	Yes	Yes
Traffice Monitoring on Active-Passive Links	Yes	Yes	Yes
Monitoring of Asymmetric Traffic Routing	Yes	Yes	Yes
Redundant Power	No (optional)	No	No
Device Failure Detection	Yes	Yes	Yes
Link Failure Detection	Yes	Yes	Yes
Physical Dimensions			
(all models rack-mountable)	2U 17” (W) x 3.5” (H) x 17” (D)	1U 17” (W) x 1.7” (H) x 14” (D)	1U 17” (W) x 1.7” (H) x 14” (D)
Weight	50lbs.	17lbs.	17lbs.
Power	100- 240VAC (50/60Hz) Redundant hot swappable	100- 240VAC (50/60Hz)	100- 240VAC (50/60Hz)
Memory	2GB	1GB	1GB
MTBF	40,000 hrs	30,000 hrs	30,000 hrs
Power Consumption	250 Watts	140 Watts	110 Watts
Temperature	0° to 40° C Operating -40° to 70° C (Non-operating)	Same for All Models	Same for All Models
Relative Humidity (non-condesing)	Operational: 10% to 90% Non-operational: 5% to 95%	Same for All Models	Same for All Models
	Altitude 0-10, feet	Same for All Models	Same for All Models
Certification	FCC Part 15, CE	Same for All Models	Same for All Models

IntruPro nIPS Appliance Software Capabilities

Model	nIPS - 1000	nIPS - 500	nIPS - 100
Stateful Traffic Inspection	Yes	Yes	Yes
IP Defragmentation and TCP Stream Reassembly	Yes	Yes	Yes
Detailed Protocol Analysis	Yes	Yes	Yes
Asymmetric Traffic bypass	Yes	Yes	Yes
Protocol Normalization	Yes	Yes	Yes
Advanced Evasion Protection	Yes	Yes	Yes
Forensic Data Collection	Yes	Yes	Yes
P2P & IM Protocol Discovery & Traffic Policy Enforcement	Yes	Yes	Yes
Signature Detection	Yes	Yes	Yes
User - Defined Signatures	Yes	Yes	Yes
Real - time Signature Updates	Yes	Yes	Yes
Anomaly Detection	Yes	Yes	Yes
Statistical (Traffic) Anomaly	Yes	Yes	Yes
Protocol Anomaly	Yes	Yes	Yes
DoS Detection	Yes	Yes	Yes
Threshold-Based Detection	Yes	Yes	Yes
Self-Learning Profile-Based Detection	Yes	Yes	Yes
Maximum DoS Profiles	300	120	100
Intrusion Prevention	Yes	Yes	Yes
Stop Attacks in Progress in Real Time	Yes	Yes	Yes
Drop Attack Packets/Sessions	Yes	Yes	Yes
Initiate TCP Reset/ICMP Unreachable	Yes	Yes	Yes
Packet Logging	Yes	Yes	Yes
Automated and User-Initiated Prevention	Yes	Yes	Yes
Internal Firewall	Yes	Yes	Yes
Blocks Unwanted and Nuisance Traffic	Yes	Yes	Yes
Granular Security Policy Enforcement	Yes	Yes	Yes
Management			
Command Line Interface (Console)	Yes	Yes	Yes
Manager Communication	Yes	Yes	Yes
Configuration	Yes	Yes	Yes
Log & Real time event reporting & analysis	Yes	Yes	Yes
Report Generation	Yes	Yes	Yes
Packet capture	Yes	Yes	Yes
Firmware Upgrade	Yes	Yes	Yes
Configuration Import/Export	Yes	Yes	Yes