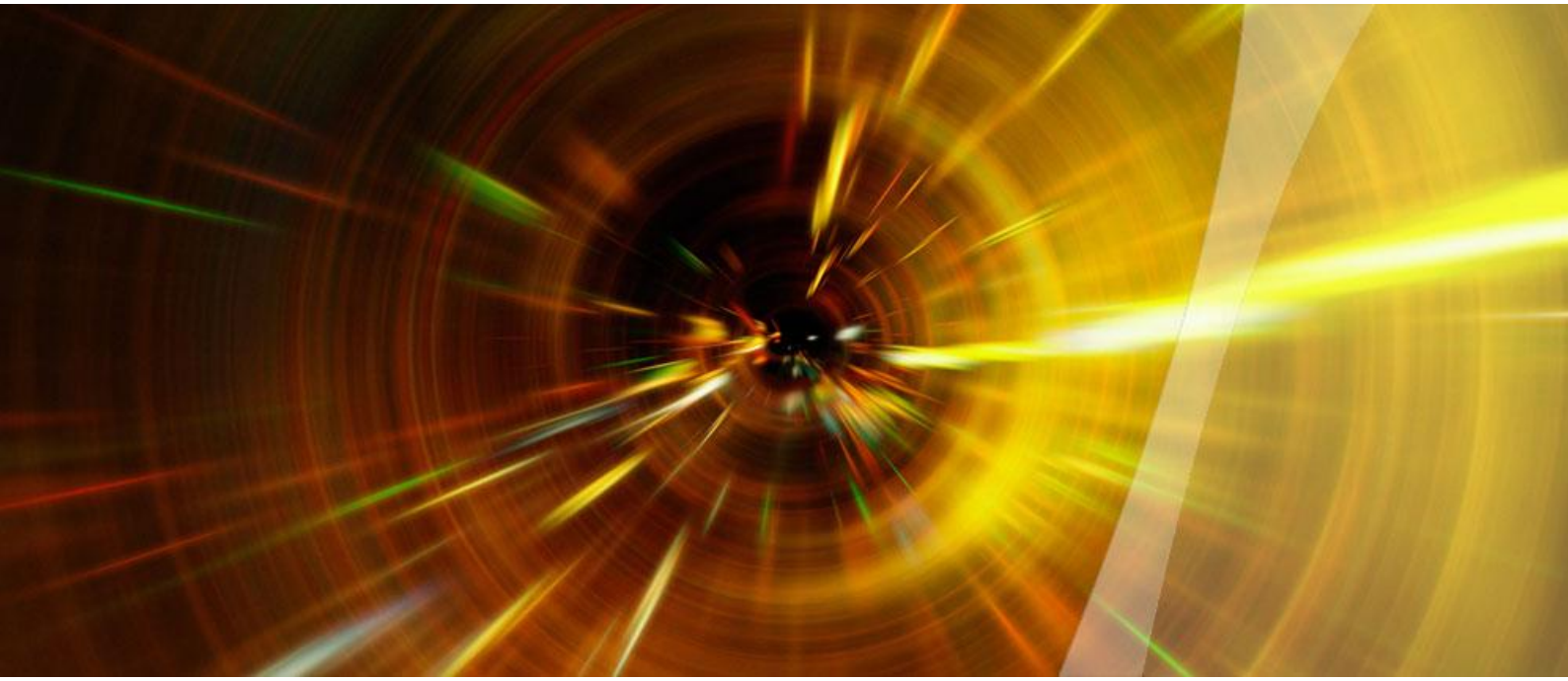

NIP IDS

Huawei Technologies Co., Ltd.

NIP IDS

Product Overview

The Network Intelligent Police (NIP) Intrusion Detection System (IDS) is a new generation of session-based intelligent network IDS developed by Huawei Symantec. Deployed in key positions in the network, the NIP monitors various datagram and network behaviors in real time, providing an instant alarm and response mechanism upon detecting intrusions or suspicious behaviors. A powerful defense system emerges through combining the dynamic security response system of the NIP IDS with the static security system of the firewall, thus protecting users' networks and systems from both external and internal attacks. The NIP IDS is especially suitable for institutions with high network security demands such as telecommunications, auditing, security consultation and law enforcement bodies, large-scale enterprises, Internet service providers, and training centers and institutions involving sensitive information.

Product Family

Carrier-class: 4-probe Gigabit intrusion detection
Applicable to: large-scale enterprises and Internet data centers

NIP1000

High-speed type: 3-probe double-100 M intrusion detection
Applicable to: medium-sized enterprises or enterprise branches

NIP200

Product Features

Powerful intrusion detection and monitoring capacity

- The NIP IDS can detect thousands of intrusions across 30 categories including network scanning, Trojan horses, worm viruses, DoS or DDoS attacks, and malicious code attacks.
- By adopting application layer analysis technique and integrating the powerful application protocol decoder, the NIP IDS thoroughly analyzes various application protocols in fine granularity.

- With the unique advanced protocol identifying technique, the NIP IDS also accurately resolves non-standard port protocols.
- The NIP IDS monitors mails, MSN communications, real-time sessions, file transfers, and servers' working state. Thus, it offers timely detection of network and server abnormalities .

High-performance network traffic processing mechanism

- Through Huawei Symantec's unique, optimized software technique, the NIP IDS transfers data between the network interface and analysis engine at high speed using a dedicated data channel. In this data collection process, no data gets copied, greatly enhancing the product's performance in a high bandwidth environment.
- The NIP IDS delivers line-speed processing capacity by integrating the following:

  High-speed packet capturing engine based on the zero-copy technique

  Optimized high-speed matching algorithm

  Powerful reassembling technique of IP segmentations

  Optimized TCP flow management and location technique
- The NIP IDS combines feature analysis and abnormality detection, thus greatly enhancing the accuracy and efficiency of detection and reducing the number of false alarms and omissions.

Diversified response modes

- The NIP IDS provides real-time response upon detecting intrusions or activities against security policies. It records attack behaviors, reports them to the system administrator, and acts against such attack behaviors in the following different response modes:

  Disconnecting sessions

  Generating database records

  Creating logs (system logs and audit logs)

  Generating alarms through emails, SNMP, and system logs

  Cooperating with firewalls and routers

Powerful cooperative capacity

- Supporting mainstream cooperation standards, the NIP IDS cooperates with other security products, provides well-designed scalable cooperation interfaces, and easily cooperate with firewalls.
- The NIP IDS cooperates with many mainstream switches. Upon detecting highly risky intrusions, the NIP IDS shuts the ports of the switches or blocks the specified IP addresses to isolate the attack sources.

Flexible deployment modes

- The NIP IDS supports distributed architecture consisting of a control center and search engines. Intrusion detection engines are distributed in the users' sub-networks, and collect and analyze data in real time; the control center implements centralized management and configuration of all intrusion detection engines. In this way, the IDS provides intrusion detection for large-scale networks, meeting the demands of users in complex networking situations.
- The NIP IDS adopts modularized architecture. Besides supporting distributed scalability, it delivers multiple engine combinations to meet the requirements of various sized networks and application environments. Users can decide the number of probes each detection engine carries according to the size of their networks, realizing the optimal cost effectiveness for their security investment.

Comprehensive database of attack features and user-defined defense rules

- The NIP IDS delivers a well-designed mechanism for users to define attack events. It enables users to define the attribute fields of 47 protocol types. In addition, the NIP IDS allows users to define sensitive information they are concerned with and define related behaviors of specified users, email accounts, and IP addresses. The NIP IDS allows users to define their own rules for intrusion detection. Users can choose from the current rules by type and severity level according to their networking environment and actual needs, and define alarm response methods for these rules. In addition, users can define detection rules on their own to detect certain special attacks, or detect complex attack behaviors made up of associated events by defining their own associated rules.
- Huawei Symantec has established a professional laboratory dedicated to improving network security and keeping pace with state-of-the-art network security technology in the world by communicating with its peers on the latest progress in attack defense techniques. Huawei Symantec has also cooperates with information security

providers and institutions both at home and abroad. This ensures that Huawei Symantec updates its products with the latest intrusion rules in line with the latest advances in network security technology, and that products are able to detect the most recent attack behaviors.

Powerful event management and traffic statistics functions

- The NIP IDS allows users to browse its control panel intrusion alarms from multiple perspectives, and provides powerful search engines for users. Users can quickly and precisely locate the attack events they are concerned with from a large number of alarm events.
- For each attack event, users can view detailed information including the attack time, the attack type, the source and destination addresses, the source and destination ports, and frequency. Users can also view detailed explanations of the attack event, its severity level, and the solution to it.
- By analyzing and auditing intrusion events from multiple perspectives, the NIP IDS generates detailed and diversified reports. It provides over 100 styles of report, containing comprehensive contents that help users evaluate their network security at any time.
- The NIP IDS generates statistics on network traffic, Web traffic, and intrusion traffic by time, event, severity level, response method, protocol, and IP address, and exports analytical reports containing scores of specifications.

Real virtual engine technique

- The NIP adopts the real virtual engine technique. One independent device can be deployed with multiple detection engines; each engine has its own memory and system resources and can be configured with specific detection policies according to the physical network areas it monitors. This technique both improves detection efficiency and helps users reduce costs.

Comprehensive self-protecting capacity

In addition to guaranteeing the security of users' networks, the NIP IDS can also comprehensively defend itself. The system adopts many security measures including:

- Data and management channels based on the SSL protocol
- Secure OS and secure authentication through physical media

NIP IDS

- Concealing of the IP addresses of the probes
- Hierarchical user management and access control
- Auditing of system logs

Product Specifications

Item	NIP200	NIP1000
Device type	High-speed type: 3-probe double-100 M intrusion detection	Carrier-class: 4-probe Gigabit intrusion detection
Fixed interface	Three 10/100/1000 M detection ports (electrical) One 10/100/1000 M management port (electrical) 1 configuration serial port	Two 10/100/1000 M detection ports (electrical) Two 10/100/1000 M detection ports (optical) One 10/100/1000 M management port (electrical) 1 configuration serial port
Dimensions (mm) width x depth x height	430 x 225 x 44	440 x 390 x 88
Weight	3.5 kg	8 kg
Power supply	AC 100-240V	AC 110-240V
Maximum power	150 W	350 W
Working ambient temperature	5°C to 40°C	5°C to 40°C
Working ambient humidity	20% to 80%	20% to 80%
Attack feature	Number of attack features: over 3000 rules in 30 categories	
Response mode	Logging TCP active disconnection Reconfiguration of edge devices, such as switches and firewalls E-mail alarms SNMP trap alarms Syslog	

『Order Information』

Item Code	Item description	Type
98090006	NIP 200-1*Serial Port,4*10/100/1000Base-TX, AC(110V/220V),Includes Software CD	NIP200
98090007	NIP 1000-1*Serial Port, 1*10/100Base-TX,2*10/100/1000Base-TX,	NIP1000

	2*1000Base-FX(LC,Multi-mode),AC(110V/220V),Includes Software CD	

Typical Networking