# NIP2000/5000
# Network Intelligent Protection System

## Overview

Huawei Network Intelligent Protection System (NIP) is a dedicated intrusion detection and prevention product. It is designed to resolve the network security issues in new IT environment such as Web 2.0 and cloud computing. The NIP provides various functions such as virtual patch, Web application protection, client protection, malicious software control, network application management, and network-layer and application-layer DoS attack defense, providing full protection of network infrastructures, bandwidths, servers, and clients for customers such as large and medium-sized enterprises and carriers.


## Product Features

### Full Protection: from System Service to Application Software

- The NIP provides traditional IPS functions such as vulnerability-based attack defense, Web application protection, malicious software control, application management and control, and network-layer DoS attack defense.
- The NIP provides comprehensive protection for the online clients exposed to the rampant attacks that aim at Web browsers, media files, and diversified documents).
- The NIP provides industry-leading defense against application-layer DoS attacks that spread through HTTP, DNS, or SIP.
- With the advanced vulnerability-based signatures and detection capability, the NIP detects attacks accurately and updates the signatures in a timely manner.

### Accurate Detection: Efficient Threat Prevention

- Ensures the detection accurancy and zero false positive based on the advanced signature-based vulnerability detection technology.
- Blocks mid-risk/high-risk attacks automatically, and does not require signature adjustment by experts.

### Application-Awareness: Refined User Behavior Control

- The NIP identifies more than 1200 application. With the delicate bandwidth allocation strategies, the NIP restricts the bandwidth occupied by illegitimate applications. In this manner, the NIP ensures the bandwidth for office applications such as OA and ERP and therefore accelerates the network access speed.
- The NIP monitors and controls applications such as instant messaging (IM), online games, online video, and online stock, helping enterprises identify and restrict unauthorized network behaviors and implement security policies.

### Easy Use and Zero Configuration Deployment

- Zero configuration deployment: The NIP starts working after power on, requiring no complex signature check and network parameter adjustment.
- Various policy templates: The NIP provides simple configurations for different scenarios, convenient for customers to implement customized security policies.
- The NIP monitors the system and security trend in real time, and provides ten types of reports for you to learn about the security status easily.

## Product Specifications

| Model | NIP2100 | NIP2200 | NIP5100 | NIP5200 |
|---|---|---|---|---|
| | | | | |
| Product performance | Multiple megabyte channels | Entry-level gigabit channels | Standard gigabit channels | High-end gigabit channels |
| Expansion and I/O | | | | |
| Dedicated management port | 1×GE (RJ45) | 1×GE (RJ45) | 1×GE (RJ45) | 1×GE (RJ45) |
| Fixed port | 4×GE (RJ45)<br>4×GE (combo) | 4×GE (RJ45)<br>4×GE (combo) | 4×GE (RJ45)<br>4×GE (combo) | 4×GE (RJ45)<br>4×GE (combo) |
| Expansion slot | 2×FIC | 3×FIC | 3×FIC | 3×FIC |
| Expansion network port | 4×GE (RJ45) BYPASS<br>2 Line (LC/UPC) BYPASS<br>8×GE (RJ45) and 8×GE (SFP) | 4×GE (RJ45) BYPASS<br>2 Line (LC/UPC) BYPASS<br>8×GE (RJ45) and 8×GE (SFP) | 4×GE (RJ45) BYPASS<br>2 Line (LC/UPC) BYPASS<br>8×GE (RJ45) and<br>8×GE (SFP) | 4×GE (RJ45) BYPASS<br>2 Line (LC/UPC) BYPASS<br>8×GE (RJ45)<br>8×GE (SFP) |
| Feature | | | | |
| Client protection | • Security protection for Web browsers and their plug-ins (Java and ActiveX)<br>• Protection for PDF, Word, Flash, and AVI files, defense against loopholes in operating systems<br>• Detection on vulnerability-based attacks, spyware, and advertising software | | | |
| Server protection | All-round server protection, addressing problems including system and service vulnerability-based attacks, brute force, SQL injection, and cross site scripting | | | |
| Infrastructure protection | • Malformed packet attack defense, special packet control, scanning attack defense, and TCP/UDP flood attack defense<br>• Application-layer DDoS attack defense: HTTP, HTTPs, DNS, SIP and so on<br>• Traffic model self-learning: setting the threshold of traffic attacks based on the statistics on normal customer traffic | | | |
| Network application management and control | Identification and control of more than 1200 application protocols, covering mainstream application protocols such as P2P, IM, online games, stock software, voice application, online video, streaming media, Web mail, mobile terminal applications, and remote login | | | |
| Device management | • GUI-based configuration, hierarchical management, permission-based access control, and centralized device management<br>• Periodically upgrade of engine repository, rollback of engine repository, and centralized repository upgrade on the intranet | | | |
| Log and report monitoring | Device status monitoring, event record backup, log query and filtering, real-time monitoring of network status, and customized report generation | | | |
| Deployment and availability | • In-line IPS deployment, off-line IDS deployment; and mixed deployment with some interfaces in-line and some others off-line<br>• Hardware bypass and dual-system hot backup | | | |
| Integrated System | | | | |
| Dimensions (H × W × D) | 1.7 × 16.6 × 22.0 in. (43.6mm × 442mm × 560mm) | 5.1 × 16.6 × 16.3 in. (130.5mm × 442mm × 415mm) | | |
| Weight (full configuration) | 19.6 lbs (8.9 kg) | 39.6 lbs (18 kg) | | |
| Power | 150 W | 300 W | | |
| AC power supply | 100 V to 240 V, 50Hz to 60Hz, supporting redundancy | | | |
| Operating environment | Temperature: 32 °F to 104 °F (0 °C to 40 °C); humidity: 5% to 95%, non-condensing | | | |
| MTBF | 12.67 years | | | |