NIP6000 Next-Generation Intrusion Prevention System

NIP6320/6610

NIP6330/6620/6650

NIP6680

Product Overview

HUAWEI NIP6000 series is an advanced, new generation intrusion prevention system (NGIPS) designed to provide application and service security for enterprises, IDCs, campus networks, and carriers.

The NIP6000 provides context, application, and content awareness capabilities and defends against unknown threats to better protect network infrastructures, bandwidth performance, servers, and clients.

Highlights

New hardware and software architecture, providing industry-leading performance

- Uses a dedicated multi-core and multi-CPU platform, which greatly improves detection performance.
- Provides dedicated hardware for decompression and pattern matching to ensure high traffic processing efficiency and optimal performance with multi-level protection.
- Uses a new intelligent awareness engine (IAE) for threat detection, which enables multi-level protection and concurrent processing and improves threat detection efficiency.

Multi-level detection for comprehensive protection

- Protects operating systems and applications from malware and attacks.
- Identifies more than 120 types of files, prevents file name extension tampering, and identifies malicious code in files.
- Provides superior anti-DDoS capabilities to mitigate application-layer DDoS attacks (such as HTTP, DNS, and SIP attacks).
- Implements SSL encryption and advanced evasion detection.
- Detects unauthorized connections to servers and protects information assets.

Dynamic context awareness for intelligent policy tuning and hierarchical log management

- Identifies security risks to both static assets and dynamic traffic.
- Automatically tunes security policies based on the security risks.
- Analyzes the detection logs based on the security risks for hierarchical log management.

Interworking with the sandbox and reputation systems for threat detection

- Interworks with the local/cloud sandbox for suspect file analysis and threat file detection.
- Interworks with the IP and C&C reputation systems for rapid threat detection and prevention.

Fast signature update for prompt vulnerability protection

- Captures the latest attacks, worms, viruses, and Trojan horses, extracts signatures from them, and determines the threat trend using a global honeynet.
- Updates the signature database and inspection engine promptly when new and zero-day threats and vulnerabilities are identified.
- Certified "CVE-Compatible". Threat analysis and verification are compatible with Common Vulnerabilities and Exposures (CVE) requirements.

NIP6000 Next-Generation Intrusion Prevention System

Specifications

Model	NIP6610	NIP6330	NIP6620	NIP6650	NIP6680
Performance	Mid-range FE	Low-end Gigabit	Mid-range Gigabit	High-end Gigabit	Mid-range 10Gigabit
Scalability					
IPS throughput	500Mbit/s	1.0Gbit/s	2.0Gbit/s	6.0Gbit/s	15.0Gbit/s
Fixed ports	4GE+2Combo	8GE+4SFP	8GE+4SFP	8GE+4SFP	4 × 10GE + 16GE + 8SFP
Height	1U				3U
Dimensions (mm)	442×421×43.6				442×415×130.5
Weight	10 KG				24 KG
Hard disk	Optional. Supports one 300 GB hard disk (hot swappable).				Optional. Supports one 300 GB hard disk (RAID1 and hot swappable).
Redundant power supply	Optional			Standard	
AC power supply	100 V to 240 V				
DC power supply	-			-48 V to -60 V	
Power consumption	170 W				350 W
Operating environment	• Temperature 0°C to 45°C (without optional hard disk) 5°C to 40°C (with optional hard disk) • Humidity 10% to 90%				
Functions					
Intelligent management	Detects the types, operating systems, and enabled services of protected IT assets and dynamically generates suitable intrusion prevention policies for the IT environment.				
	Evaluates the risk level of attack events based on the IT environment so that administrators can process critical attack events and ignore false positive attacks.				
	Identifies application types of live network traffic and determines whether to implement intrusion detection based on the risk levels of the identified application types.				
	Provides multiple types of logs, such as threat logs, operation logs, system logs, and policy matching logs, for the administrator to learn about network events.				
	Provides multiple types of reports, such as traffic reports, threat reports, and policy matching reports, for the administrator to view network traffic and threat status. The NIP can also interwork with an eSight to provide more comprehensive and diversified reports.				
	Provides a web UI, CLI (console, Telnet, and sTelnet), and network management system (SNMP) for device management.				
Intrusion prevention	Defends against common attacks, such as Worms, Trojan horses, botnets, cross-site scripting, and SQL injection, based on the signature database, and provides user-defined signatures to defend against new attacks.				
APT detection	Detects APT attacks based on reputation systems and the sandbox. The NIP6000 sends suspect files to the sandbox for detection and then displays attack events based on the sandbox detection result.				
	Supports IP and C&C reputation to detect and prevent malicious IP addresses and domain names.				
Application Security	Automatically learns traffic patterns and defends against multiple types of DDoS attacks at the application layer, including HTTP, HTTPS, DNS, and SIP flood attacks.				
	Scans for viruses in files transmitted through HTTP, FTP, SMTP, POP3, IMAP, NFS, and SMB and prevents virus-infected files from being transmitted.				
	Identifies more than 6000 applications, including P2P, IM, online gaming, social networking, video, and audio applications, and takes actions (block, traffic limiting, application usage display) for the identified applications.				
Web security	Decrypts HTTPS traffic and detects threats.				
	Provides a URL blacklist to control online behavior.				
Network security	Detects threats in IPv6 traffic.				
	Detects threats in VLAN, QinQ, MPLS, GRE, IPv4 over IPv6, and IPv6 over IPv4 tunnel traffic.				
	Automatically learns traffic patterns and defends against multiple types of DDoS attacks at the network layer, including SYN, UDP, ICMP, and ARP flood attacks.				
	Defends against multiple types of single-packet attacks, including: • Scanning attacks, such as IP sweep and port scanning • Malformed packet attacks, such as IP spoofing, LAND, Smurf, Fraggle, WinNuke, Ping of Death, TearDrop, IP fragment, ARP spoofing, and attacks using invalid TCP flags Control message attacks, such as oversized ICMP packets, ICMP unreachable packets, ICMP redirect packets, Tracert, packets with options such as IP source routing, IP record route, and IP timestamp				
	Blacklists the source or destination IP addresses of attacks to block the follow-up packets from or to the blacklisted IP addresses.				
High availability	Supports hot backup protocols, such as VRRP, VGMP, and HRP, and provides a hot standby mechanism to ensure that services can automatically and smoothly switch to the standby device if the active device fails.				
	Provides a bypass card to ensure service continuity if the system encounters faults (such as hardware failures, and devices being powered off).				
	Provides visualized fault diagnosis for the administrator to diagnose all possible fault causes and automatically displays the diagnosis results and troubleshooting suggestions.				
Signature database update	Supports online and offline updates of the IPS-SDB, SA_SDB, and antivirus SDB for the device to have the latest defense capabilities.				

Note: Performance is tested under ideal conditions. The actual result may vary with different deployment environments.

About This Publication

This publication is for reference only and does not constitute any commitments or guarantees. All trademarks, pictures, logos, and brands mentioned in this document are the property of Huawei Technologies Co., Ltd. or a third party.