HUAWEI NIP2000D/5000D

NIP2100/2200/5100

Overview

As a new generation of intrusion detection system (IDS) products, the Huawei NIP 2000/5000 series offer an integrated defense-detection-response solution by helping users locate network threats, detecting traffic in violation of security policies, and providing detailed and effective guidelines. Using multiple detection technologies and sticking to the concept of comprehensive detection, accurate analysis, and diversified presentation, the NIP improves users' security capabilities and measures.

Highlights

Comprehensive Protection for Networks, Servers, Clients, and Applications

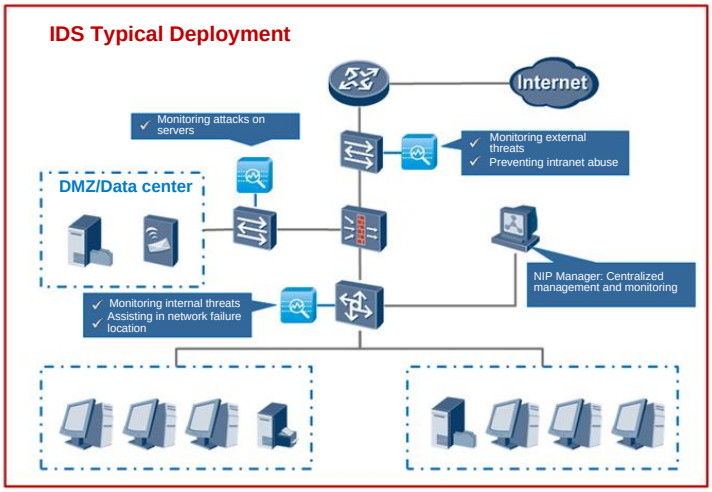
- The NIP provides traditional IDS functions such as vulnerability attack detection, Web application detection, malicious-software detection, and network-layer DoS attack prevention.
- The NIP provides comprehensive protection for client systems exposed to the prevalent attacks that target web browsers, media files, and other document file formats.
- The NIP provides industry-leading defense against application-layer DoS attacks that spread through HTTP, DNS, or SIP.
- The NTP can identify more than 1000 applications to present the real network status.
- The NIP can detect attacks and upgrade signatures in a timely manner with the global vulnerability trace capability and more than 200 security researchers.

Accurate Detection with Low False Positive Error Rate and Maintenance Cost

- The NIP detects attacks accurately based on the advanced vulnerability feature detection technology. The false positive error rate is extremely low.
- Based on traffic model self-learning, the abnormal traffic detection function of the NIP prevents false positive errors caused by manual setting of thresholds.

Diversified Presentation for Easy Determination of Response Modes

- Solution: The NIP provides detailed and comprehensive alarm information and specific response guidelines.
- Attack details: The NIP attacks packs to help users better understand the hacker behavior and collect evidence about the hackers.
- Security trend: The NIP provides more than 30 security reports to help users easily acquire the security status and trends of the network.



HUAWEI NIP2000/5000

Specifications

Model	NIP2100D	NIP2200D	NIP5100D	NIP5200D
Product performance	High-end megabit	Low-end gigabit	Mid-range gigabit	High-end gigabit
Extension and I/O				
Dedicated management port	1×GE(RJ45)	1×GE(RJ45)	1×GE(RJ45)	1×GE(RJ45)
Fixed interface	4×GE(RJ45) 4×GE(combo)	4×GE(RJ45) 4×GE(combo)	4×GE(RJ45) 4×GE(combo)	4×GE(RJ45) 4×GE(combo)
Extension slot	—	—	3×FIC	3×FIC
Extension network port	—	—	8×GE(RJ45), 8×GE(SFP) 2×XE, 2×XE+8GE	8×GE(RJ45), 8×GE(SFP) 2×XE, 2×XE+8GE
Key Features				
Attack detection technologies	Intelligent protocol identification technology, data packet and stream reassembly technology, protocol and file restoration technology, attack feature detection technology, vulnerability feature detection technology, traffic model self-learning technology, network anomaly detection technology, protocol anomaly detection technology, and advanced evasive detection technology			
Server attack detection	All-round server protection, addressing problems including system and service vulnerability exploits, brute force, SQL injection, and cross site scripting			
Client attack detection	✧ Security protection for web browsers and plug-ins (Java and ActiveX) ✧ Protection for files with common formats: PDF, Word, Flash, and AVI			
Malicious software detection	Trojans, worms, spyware, remote control, Botnet, and adware			
Traffic attack detection	✧ Malformed packet attack prevention, special packet control, scanning attack prevention, TCP/UDP flooding attack prevention ✧ Application-layer DDoS attack prevention: HTTP, HTTPs, DNS, SIP, and so on ✧ Traffic model self-learning: setting the threshold of traffic attacks based on normal traffic statistics			
Application awareness	Identification and management of more than 850 application protocols, covering mainstream application protocols including P2P, IM, online games, stock software, voice application, online video, streaming media, Web mail, mobile terminals, and remote login			
Alarm response	Real-time alarm, recording into database, Syslop, SNMP Trap, E-mail, sending short messages, third-party device linkage, attack packet capturing, TCP resetting			
Device management	✧ GUI-based configuration, hierarchical management, permission-based access control, and centralized device management ✧ Periodic upgrade of engine repository, rollback of engine repository, and Intranet upgrade			
Log and report monitoring	Device status monitoring, event information record backup, log querying and filtering, real-time monitoring of network status, and specialized reports			

Integrated System				
Dimensions (H×W×D) (mm)	442×560×43.6	442×560×43.6	442×415×130.5	442×415×130.5
Power supply	AC: 100 V to 240 V 50/60 Hz, supporting redundancy	AC: 100 V to 240 V 50/60 Hz, supporting redundancy	AC: 100 V to 240 V 50/60 Hz, supporting redundancy	AC: 100 V to 240 V 50/60 Hz DC: -48 V to -60 V supporting redundancy
Maximum power	150 W	150 W	300 W	300 W
Operating environment	Temperature: 0°C to 40°C humidity: 5% to 95%, non-condensing	Temperature: 0°C to 40°C humidity: 5% to 95%, non-condensing	Temperature: 0°C to 40°C humidity: 5% to 95%, non-condensing	Temperature: 0°C to 40°C humidity: 5% to 95%, non-condensing
MTBF	12.67 years	12.67 years	12.67 years	12.67 years