NIP6000 Next-Generation Intrusion Prevention System

Thanks to the development of the cloud and mobile computing technologies, many enterprises currently allow their employees to use smart devices, such as smartphones and tablets, and popular network applications, such as Facebook and Twitter, for work to improve employee productivity. The problem with these technologies is that they blur network borders and increase the exposure to risks. The increasing number of security incidents indicates that the threat landscape in information security is changing and traditional technologies cannot protect against the new generation threats.

New generation threats are mostly zero-day vulnerability-based attacks that target specific victims. Traditional defense technologies are slow to create signatures, thereby giving attacks ample time to cause severe damage. In addition, attackers may customize the attack for the target environment and remain undetected for a long time. The increasing number of attacks proves that traditional technologies cannot help enterprises defend against new generation attacks. Enterprises now need a fundamentally different new generation solution to protect their IT infrastructures from new generation threats.

Huawei NIP6000, an advanced, new generation intrusion prevention system (NGIPS), provides context, application, and content awareness capabilities and defends against unknown threats to better protect network infrastructures, bandwidth performance, servers, and clients.

Product Appearances

NIP6320/6610

NIP6330/6620/6650

NIP6680

NIP6860

Highlights

New Hardware and Software Architecture, Providing Industry-Leading Performance

Most software matching engines process regular expressions slowly, which severely restricts the device detection performance. Huawei NGIPS engine uses an MIPS64 processor from Cavium, a world-renowned chip provider, to provide high-performance hardware pattern matching. Huawei NGIPS also employs the new intelligent awareness engine (IAE) for threat detection, which enables in-depth detection and delivers 15 Gbit/s detection efficiency.

The NIP6000 series NGIPS, with the new unified hardware-software architecture, uses a dedicated multi-core platform and coprocessors to process massive packets that require high computing performance. The packets that require less computing performance are processed using software. Such processing mechanisms improve the overall device performance.

With the asynchronous matching technology, the NIP6000 uses a hardware-based matching engine to process the most resource-intensive services (especially services that are CPU-intensive) so that the CPU is free to process other services during matching. The concurrent processing greatly improves the speed and efficiency.

The greater the number of signatures loaded, the lower the matching efficiency of traditional IPS engines and device performance. In contrast, the NIP6000 uses a hardware-based matching engine to concurrently load tens of thousands of threat signatures without affecting the matching performance.

To detect compressed web pages or files, IPS engines must have powerful decompression capabilities. The NIP6000 uses a dedicated hardware-based engine with Cavium processors for file decompression and is capable of implementing high-performance intrusion detection on compressed files, such as ZIP files.

Dynamic Context Awareness for Intelligent Policy Tuning and Severity-based Log Management

Legacy IPS devices detect attacks based only on attack signatures, without considering the attributes of the protected assets on live networks, leading to false positives. The NIP6000 is aware of environment changes and provides intelligent policy tuning and hierarchical log management functions to resolve this problem.

The NIP6000 policy tuning and risk evaluation are based on asset information, including asset type, asset value, operating system, and enabled services. The asset information can be manually entered, automatically detected, or imported from third-party scanning software.

Based on the asset information, the NIP6000 selects signatures and automatically generates intrusion prevention policies for attack defense. Upon detecting environment changes, the NIP6000 automatically tunes the policies or notifies the administrator to tune them to defend against new threats.

- Upon detecting an attack, the NIP6000 extracts from the attack signature the target information, such as the operating system and service, and compares this information with the asset information stored on the NIP6000. It then determines the risk level of the attack event based on the asset value and log severity so that administrators can prioritize high-risk attack events and ignore false positives and minor issues.
- With context awareness and real-time attack detection, the NIP6000 identifies security risks to both static assets and dynamic traffic so that enterprises can gain visibility into their network status.

Multi-level Detection for Comprehensive Protection

As the number of information assets connecting through the Internet is increasing, network attacks and information interception are also growing and have become a huge industry chain. This poses high requirements on the defense capabilities of NGIPS products. To address this challenge, the NIP6000 provides the following in-depth overall protections:

- **Intrusion prevention:** The NIP6000 detects and prevents attacks that exploit over 5000 vulnerabilities and Web attacks, such as cross-site scripting and SQL injection.
- **Antivirus:** The antivirus engine on the NIP6000 defends against more than 5 million viruses and Trojan horses, and the antivirus signature database is updated daily.
- **Unauthorized server connection detection:** The NIP6000 detects unauthorized connections to servers and port stealing to protect key information assets.
- **SSL decryption:** The NIP6000 can function as a proxy to implement application-layer security protection, such as intrusion prevention, antivirus, data leak prevention, and URL filtering, on SSL encrypted traffic.
- **Anti-DDoS:** The NIP6000 identifies and prevents more than 100 types of DDoS attacks, such as SYN and UDP floods.

Typical Application Scenarios

Internet Border Protection:

In such a scenario, the NIP6000 is often deployed in the downstream of an egress firewall or a router and transparently connects to the network. To protect multiple links, you can use multiple interface pairs on the NIP6000.

- **Intrusion prevention:** The NIP6000 defends against worms, browser exploits, and plug-in vulnerabilities to ensure the enterprise network remains healthy. In addition, the NIP6000 stops Trojan horses and spyware that exploit vulnerabilities to protect key data information, such as privacy and identity information in office computers.
- **Antivirus:** The NIP6000 scans the files downloaded from the Internet for viruses to protect the PCs on the enterprise network.
- **URL filtering:** The NIP6000 restricts the websites accessible to enterprise users to prevent productivity loss and network threats.
- **Application control:** The NIP6000 controls P2P, video, and IM application traffic to guarantee major enterprise services operate smoothly.

IDC/Server Upstream Protection:

In such a scenario, dual NIP6000s are often deployed to avoid a single point of failure. The NIP6000s can be deployed in-line in front of servers to transparently access the network or attached to switches or routers. In the latter deployment mode, traffic exchanged between the Internet and servers is diverted to the NIP6000s for processing, after which it is injected back.

- **Intrusion prevention:** The NIP6000 defends against worms targeting web, mail, and DNS servers and exploits of service and platform vulnerabilities to prevent malware from damaging, tampering with, or stealing data on the servers. The NIP6000 also defends against SQL injection, scanning, guessing, and sniffing attacks targeting web applications.
- **Unauthorized server connection detection:** The NIP6000 detects unauthorized connections to servers to prevent information leaks.
- **Antivirus:** The NIP6000 scans the files to be uploaded to the servers for viruses to protect the servers.
- **Anti-DDoS:** The NIP6000 defends against DoS and DDoS attacks targeting servers.

Network Border Protection:

For a large or medium-sized enterprise, the network is often divided into zones of different security

levels. Isolation or security control is applied to communications between the zones. For example, departments or headquarters and branches must be isolated from each other for security.

- **Intrusion prevention:** The NIP6000 logically isolates the zones and detects and prevents sniffing, reconnaissance, worms, and Trojan horses from external networks.
- **Violation monitoring:** The NIP6000 monitors and controls unauthorized connections from enterprise networks to external networks.

Off-line Monitoring:

Intrusion prevention products can be deployed in off-line mode on networks to monitor the network security conditions. In such a scenario, the intrusion prevention product records attack events and web application traffic conditions, to provide evidence for cyber security event audit and user behavior analysis, but does not take defense actions. The NIP6000 is attached to a switch, and the switch sends a copy of traffic to be checked to the NIP6000 for detection and analysis.

- **Intrusion detection:** The NIP6000 detects the attacks initiated from the Internet and from enterprise employees, and then displays the attack events through logs and reports for the enterprise administrators to evaluate network security status. In addition, the NIP6000 provides an attack event risk evaluation function that makes it easier for administrators to evaluate risk.
- **Application identification:** The NIP6000 identifies and collects statistics on P2P, video, and IM application traffic and provides reports for enterprise managers to gain visibility into application usage.
- **Firewall interworking:** The NIP6000 notifies a connected firewall of attack events, so that the firewall blocks the attack traffic.
- **Compliance:** The NIP6000 complies with related laws and regulations.

Product Specifications

Model	NIP6610	NIP6330	NIP6620	NIP6650	NIP6680	NIP6860
Performance	Mid-range FE	Low-end Gigabit	Mid-range Gigabit	High-end Gigabit	Mid-range 10Gigabit	High-end 200 Gigabit
Scalability						
IPS throughput	500Mbit/s	1.0Gbit/s	2.0Gbit/s	6.0Gbit/s	15.0Gbit/s	Maximum 200Gbit/s
Fixed ports	4GE + 2Combo	8GE + 4SFP	8GE + 4SFP	8GE + 4SFP	4×10GE + 16GE + 8SFP	None Support 24xGE, 6x10GE, 12x10GE, 3x40GE, 1x100GE
Height	1U				3U	14U
Dimensions (mm)	442×421×43.6				442×415×130.5	442×650×620
Weight	10kg				24kg	Empty 43.2kg Full 112.9kg

Model	NIP6610	NIP6330	NIP6620	NIP6650	NIP6680	NIP6860
Hard disk	Optional. Supports one 300 GB hard disk (hot swappable).				Optional. Supports one 300 GB hard disk (RAID1 and hot swappable).	None
Redundant power supply	Optional			Standard		
AC power supply	100 V to 240 V					90V to 264V
DC power supply	-			-48 V to -60 V		-72 to -38V
Power consumption	170 W				350 W	DC typical: 4025W, DC Max: 4823W AC typical: 4282W, AC Max: 5132W

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%
						• Temperature
						  0°C to 45°C
						• Humidity
						  5% to 85%

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.

Model	NIP6610	NIP6330	NIP6620	NIP6650	NIP6680	NIP6860
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.					

About This Publication