HUAWEI IPS Module

IPS module

Overview

Huawei IPS module is a new generation of dedicated intrusion detection and prevention products. It is designed to resolve network security issues in the Web2.0 and cloud age. In the IPv4 and IPv6 network environment, the IPS module supports virtual patching, web application protection, client protection, malicious-software control, network application control, and network-layer and application-layer DoS attack defense.

With the carrier-class high availability design, the IPS module can be inserted on switches, such as the S12700, S9700, and S7700, providing plug and play and scalability features. It can be deployed flexibly in multiple network environments. This module supports zero-configuration deployment and does not require complicated signature adjustment and manual setting of network parameters and threshold baselines to block service threats. Functioning with basic network devices, the IPS module comprehensively protects network infrastructures, network bandwidth performance, servers, and clients for large and medium-sized enterprise, industry, and carriers.

Product Features

Flexible Deployment and Easy to Use

- Uses software to adjust the networking, which simplifies the installation and deployment and frees the administrators from adjusting the complex cables.
- Integrates networks with security using products from the same vendor, which facilitates unified management and simplifies the management.
- Supports zero-configuration deployment and plug and play, and does not require complicated signature adjustment and manual setting of network parameters.
- Provides diversified policy templates to simplify configurations in various scenarios and facilitate security policy customization.

Accurate Detection and Efficient Threat Prevention

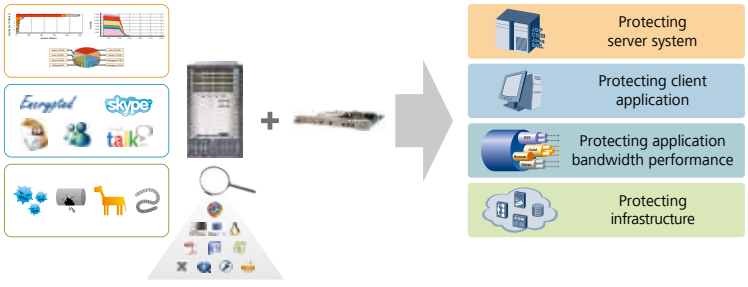
- Detects attacks accurately without false positives with the advanced vulnerability feature detection technology.
- Automatically learns the traffic baselines to prevent incorrect threshold configurations.
- Automatically blocks major and severe threats without signature modification.

Comprehensive Protection from System Service to Application Software

- Provides traditional intrusion protection system (IPS) functions, such as vulnerability-based attack defense, web application protection, malware control, application management and control, and network-layer DoS attack defense.
- Provides comprehensive protection for client systems exposed to the prevalent attacks that target web browsers, media files, and other document file formats.
- Provides industry-leading defense against application-layer DoS attacks that spread through HTTP, DNS, or SIP.
- Detects attacks and upgrades signatures in a timely manner with the global vulnerability trace capability.

Application Awareness for Accurate Control of User Behaviors

- Identifies more than 6000 network applications. With precise bandwidth allocation policies, the IPS module restricts the bandwidth used by unauthorized applications and reserves sufficient bandwidths for office applications, such as OA and ERP.
- Monitors and manages various network behaviors, such as instant messaging (IM), online games, online video, and online stock trading. This enables enterprises to identify and prevent unauthorized network behaviors and better implement security policies.



HUAWEI IPS Module

Specifications

Model	IPS module
Hardware interface	
Application scope	S12700, S9700, S7700
Fixed ports	4 x GE
USB port	1
Console port	1
Functions	
Server protection	• All-round server protection, addressing problems including system and service vulnerability exploits, brute force, SQL injection, cross site scripting, and viruses
Client protection	• Security protection for web browsers and plug-ins (Java and ActiveX) • Protection for files with common formats, such as PDF, Word, Flash, and AVI • Defense against operating system vulnerabilities, detection of infected systems, and detection of spyware and adware
Infrastructure protection	• Malformed packet attack prevention, special packet control, scanning attack prevention, TCP/UDP flooding attack prevention • Application-layer anti-DDoS: HTTP, HTTPs, DNS, SIP, and so on • Traffic model self-learning: setting the threshold of traffic attacks based on normal traffic statistics
Application control	• Identification and management of more than 6000 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 applications
Alarm and response	• Real-time alarm, audio notification, syslog, SNMP Trap, E-mail, short messages, third-party interworking, IP address isolation, capture of attack packets, and real-time session blocking
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
Logs and reports	• Device status monitoring, event information backup, log query and filtering, real-time monitoring of network status, and customized reports
Deployment	• In-line IPS deployment, off-line IDS deployment, hybrid deployment, and hot standby