Product Brochure
IPS2000 Series

DPtech IPS2000
Intrusion Prevention System

Overview

Designed for application system protection, the DPtech IPS2000 Intrusion Prevention System is a professional security device which provides professional application-layer protection for core assets, including user operating systems, middleware, databases, mail servers, DNS servers, and FTP servers.

The IPS2000 Intrusion Prevention System is characterized by a comprehensive signature library, state-of-the-art dual virus engines, and four specialized detection engines, offering comprehensive protection and reinforcement against vulnerability threats and attacks that keep popping up. In addition, thanks to the attack monitoring platform and the unknown threat monitoring platform integrated in the IPS2000 Intrusion Prevention System, the user's network security status can be displayed in an all-round manner, helping them gain an intuitive understanding of the current network security status and eliminate potential security risks without delay.

Product Features

- **10,000 Signatures Provides Comprehensive Protection**

  A signature library consisting of nearly 10,000 attack signatures provides users with comprehensive application-layer attack protection, effectively preventing attacks such as buffer overflow, worms, Trojan horse, viruses, and SQL injections.

- **Specialized Engines for Accurate Identification**

  Four specialized detection engines are available, i.e., anti-escape detection engine, protocol intelligent derivation engine, protocol semantic analysis engine, and virtual environment detection engine.

  - Anti-escape detection engine: fragmentation escape, out-of-order escape, encoding malformed escape and other malformed attacks;
  - Protocol intelligent derivation engine: Identify multiple protocols and facilitate traffic testing by introducing them into various filters based on protocol classification;

- Protocol semantic analysis engine: Make in-depth analysis on traffic through feature matching and semantic analysis to ensure accurate detection of attacks and threats;
- Virtual environment detection engine: By running files in the virtual environment, tracking and recording their behaviors, it is effective in APT attack detection to ensure network security with the aid of such technologies as statistical classification based on big data and dynamic behavior analysis.

■ **Double Virus Engine Ensures Effective Virus Scans**

State-of-the-art dual virus scanning engines: Streaming virus scanning engine and file recovery virus scanning engine are combined to provide users with on-demand flexibility based on current network situations.

- Streaming virus scanning engine: Feature matching enables a quick virus detection. The number of signature libraries can be expanded through continuous learning during use, thus significantly improving the virus detection efficiency.
- File recovery virus scanning engine: By extracting and running files, static features, behavior analysis and other technologies help discover hidden malicious code in files and accurately detect viruses;

■ **Sensitive Data is Leak Proof**

Upon identification of sensitive data and file types in the system, the usage of sensitive data is monitored to eliminate data leakage and ensure a full range of protection for user’ s core data. To prevent the leakage of critical and sensitive data, users may adopt multi-dimensional metrics such as application type, file type, key words, and time, while taking into consideration of the current network status.

■ **Visualization of Network Threats**

With an attack and unknown threat monitoring platform, it can display network situation, attack trend, and attack logs in real time. Traceability of attacks can be realized by displaying attack distribution from around the world in a map and recording the current attack stage of the attacked IP. Across-the-board display of known and unknown threats on the current network is thus enabled.

■ **Behavior Identification Enables Application-layer Control**

A signature library consisting of more than 5,000 protocols can be customized based on user needs to control network access behavior of the user and at the application layer.

■ **Easy Deployment in Complex Networks**

It is easy to deploy in IPv4/IPv6 dual stack, MPLS VPN, BGP and other complex network environments.

It can also identify and detect QinQ, PPPoE, MPLS, GRE and other encapsulated packets.

Product Series

IPS2000-Blade-X

IPS2000-Blade-XA

IPS2000-Blade-XE

IPS2000-MA-X

IPS2000-ME-X

IPS2000-GS-X

IPS2000-GA-X

IPS2000-TS-X

IPS2000-TM-X

IPS2000-TM-X

IPS2000-TA-A

Function Descriptions

Product Functions	Function Descriptions
Attack Detection and Defense	With comprehensive application detection and defense capabilities at layers 4-7, it effectively prevents attacks such as buffer overflow, worms, Trojan horse, viruses, SQL injections, malicious codes, phishing, brute force and weak password scanning. It is provided with a built-in attack signature library consisting of nearly 10,000 entries and is in compliance with CVE.
Four Detection Engines	The integration of anti-escape detection engine, protocol intelligent derivation engine, protocol semantic analysis engine, and virtual environment detection engine .They ensure accurate detection of attacks and threats.
Professional Antivirus Protection	Streaming virus scanning engine and file recovery virus scanning engine are combined to provide users with on-demand flexibility.The streaming virus signatures are constantly expanded through self-learning to achieve more efficient detection and processing.
Sensitive Data is Leak Proof	Capable of identification of application and sensitive data, it can effectively protect the user's key data by applying protection policies that take effect at a specified time.
Application-layer Control	A signature library consisting of more than 5,000 protocols can be customized to support access behavior control of the user from the perspectives of application type and time.
Deep Packet Detection Technology	It supports IPv4/IPv6 dual stack, MPLS VPN, BGP and other complex network environments, and can identify and detect QinQ, PPPoE, MPLS, GRE and other encapsulated packets.
Full DDOS Attack Defense	It supports fingerprinting in TCP, UDP, ICMP and other protocols, and offers protection against SYN Flood and DNS Flood.
Bandwidth Limits	Supporting bandwidth limit based on single user and user groups, it can adopt different policies that take effect at different times.
Visualization Management	A user friendly graphical management interface, which supports Web GUI, SSH and serial console. Centralized management platform through UMC network management is also made possible. With an attack and unknown threat monitoring platform, it enables across-the-board display of network threats.
Logs and Reports	An independent log server is provided, on which regular automatic backups can be performed. With its built-in multi-dimensional reports, functions such as graphic inquiry, audit, statistics and retrieval of various network behavior logs on the intranet are enabled to facilitate the management in understanding and controlling the network.
Multiple Guarantee	Equipped with a multiple guarantee mechanism of high reliability, it

Mechanism of High Reliability	supports key component redundancy and hot-plug, application of Bypass and PFP Power Fail Safeguards, and dual-system hot standby. Truly seamless switching is thus enabled to guarantee highly stable and reliable Network Security operations.
Deployments	Available in routing mode, transparent mode and hybrid mode.

Hangzhou DPtech Technologies Co., Ltd.

Address：6th Floor, Zhongcai Building, No. 68 Tonghe Road, Binjiang District, Hangzhou City, Zhejiang Province

Postcode：310051

Official Website：www.dptech.com

Service Hotline：400-6100-598