DPX8000 Series Deep Service Switch Gateway

DPtech
Hangzhou DPtech Technologies Co., Ltd.

Product

The DPX8000 Series Deep Service Switch Gateway is the professional high-end network routing switches integrated the comprehensive security and application delivery features for the large-scale enterprises and ISP. The series products integrate seamlessly the comprehensive L2/L3 network features, the powerful security defense functions, professional VPN services and the deep service processing features on one single hardware platform. They can reduce the Total Cost Ownership (TCO) and the deployment complexity related to basic network and security. They are an ideal high-end option of network security solution.

DPX8000 Series Deep Service Switch Gateway adopts the state-of-the-art hardware platform and architecture, achieving a leapfrog breakthrough of the security and application delivery performance.

It is able to support 480 Gigabit Ethernet ports, 324 10Gigabit Ethernet ports, 20 40Gigabit Ethernet ports, 40 10Gigabit Packet over Sonet (POS) ports, which satisfies the requirements of carrier-class applications. DPX8000 hardware platform supports 10 service slots and 2 main process unit slots. Every service slot can install Firewall / SSL VPN Service Module, IPS Service Module, UAG Service Module. On the full configuration condition, the firewall performance is over 150Gbps and the IPS performance is over 60Gbps in the single DPX8000 chassis.

The MPU module and the interface modules provide the comprehensive routing and Ethernet switch capability, and supports RIP/OSPF/BGP/routing policy and policy routing. It supports diverse QoS features.

The Firewall / SSL VPN Service Module supports such functions as external attack defense, intranet security, traffic policing, mail filtering, web page filtering and application layer filtering, effectively ensuring network security. It adopts the Application-based Packet Filter, an application state detecting technology, to detect the connectivity and abnormal commands. It provides multiple intelligent analysis and management means, supports mail alarm and multiple logs, and provides network management monitoring to assist the network administrator to complete network security management. It supports multiple VPN services, for example, GRE, L2TP, IPSec VPN, SSL VPN, Dynamic VPN, and is able to construct multiple forms of VPNs.

The IPS Service Module integrates the vulnerability database, virus definitions, and application protocol signature database in the industry. The number of signatures is more than 4000.It can exactly identify and prevent various network attacks and abuses. It also integrates the Kaspersky anti-virus engine and virus definitions. It uses the most advanced anti-virus technologies in the world, including the second generation heuristic code analysis method, and the unique script viruses blocking technology. It can therefore kill various file viruses, network viruses, and hybrid viruses in real time. In addition, it integrates the next generation virtual machine unpack engine and behavior estimation technologies to kill derived viruses and unknown viruses accurately.

The UAG Service Module provides the granular visibility and policy enforcement that network operators need to optimize the delivery and bandwidth. The service module can identify more than 800 applications and will update the signature of new applications weekly. It allows network operators to monitor, identify, classify, prioritize, and shape, network traffic per application and per user. Providing real-time monitoring, QoS and application policy enforcement and traffic steering, these flexible devices helps operators control bandwidth utilization and costs while enhancing service quality for all network users.

The ADX Service Module is the leading link load balancing and server load balancing solution. Multiple links, servers and applications can be load balance based on a specific load balancing algorithm, thus provide fast response and service continuity. High availability, redundancy, capacity and security can be achieved by using load balancing solution.

The nFlow Service Module is the leading network traffic analyzer and collector. It supports all types of traffic detection and offers detailed statistics. The statistics information reduces the time to locate root causes of traffic anomalies and help in network capacity plans, application monitoring, and fault diagnosis.

The Wireless Service Module provides refined user control and management, comprehensive RF management and security mechanism, fast roaming and strong QoS feature. Powerful WLAN access control functions provide the most ideal access control solutions for WLAN access of large enterprise campus networks, wireless MAN coverage and hot spot coverage.

DPX8000 Series Deep Service Switch Gateway takes full consideration of the requirements on high reliability by network applications.

The interface modules and service modules support hot swapping to fully satisfy the requirements on network maintenance, upgrade, and optimization. It provides the temperature detecting function within the internal environment of the chassis which ensures the system running stably and continuous. DPX8000 series supports the unified management by DPtech UMC management system.

Series

DPX8000-A3

DPX8000-A5

DPX8000-A12

Features

Advanced Platform Architecture

- DPX8000 Series Deep Service Switch Gateway adopts the carrier-class hardware platform of DPtech. The hardware platform is based on the full-distributed architecture and full-modular design. It satisfies the requirement on the equipment wire-speed processing capability by the core enterprise users through the distributed multi-core and self-developing ASIC system
- DPX8000 support intelligent power and environmental management, energy efficiency which based on industry green standard.
- DPX8000 series support industry leading virtual switch clustering technology which enable multiple switches into one virtual switch, up to 4 units of DPX8000 can be virtualize.
- DPX8000 high-speed fully distributed switching architecture support up to 2.4Tbps backplane with maximum 1152Gbps switching capability, 780Mpps packet forwarding rate. Local switching architecture support maximum 6480Gbps switching capability, 4860Mpps packet forwarding rate.

Intelligent Network Integration

- Support static routing protocol, routing policy and policy routing
- Support RIP v1/2, OSPF, and BGP dynamic routing protocols
- Support 802.1Q VLAN
- Support DHCP Client/Server/Relay
- Support STP/RSTP/MSTP
- Wire-speed L2/L3 forwarding

Comprehensive Support for FW/VPN Feature

- Enhanced firewall functions: Through the Firewall / SSL VPN Service Module, DPX8000 series products provide such basic firewall functions as security zone configuration, static/dynamic blacklist, MAC-IP binding, ACL application, and instruction prevention. In addition, it offers enhanced functions like status-based filtering, virtual firewall, and transportation of 802.1Q-tagged packets. It protects the network against attacks of ARP spoofing, invalid TCP flag, large ICMP packets, Challenge Collapsar (CC), SYN flooding, address/port scanning.
- Abundant VPN features: The DPX8000 series products support access through L2TP, GRE, and IPSec VPN. The integrated hardware encryption engine implements VPN handling of high performance.
- Full support of NAT applications: The DPX8000 series products support NAT applications including many-to-one, many-to-many, static NAT, dual translation, IP Masquerade and DNS mapping. It supports NAT traversal with multiple protocols, stateful failover for asymmetric routing and delivers NAT ALG functions such as DNS, FTP, SIP, RTSP, H.323, and NBT.
- URL filtering: The DPX8000 series products implements user-based URL access control to deny access to unauthorized Websites, such as the phishing websites.
- High available feature: supports the modes of active/active and active/passive, implementing load balancing and service backup.

Advanced IPS Anti-Attack Service

- Industry-leading intrusion prevention/detection: The IPS Service Module integrates intrusion prevention and detection. By Layer-7 in-depth analysis and detection, it can timely prevent viruses, worms, Trojan horses, spyware, and webpage tampering, providing full-round protection for network applications, infrastructure and performance.
- Real-time anti-virus: The IPS Service Module adopts Kaspersky's anti-virus engine to detect and remove codes of malicious attacks in time.

Application-Oriented Network Traffic Control and Visible Management

- Application identifies and control: The DPX8000 series products identify P2P and IM applications of BitTorrent, Thunder, QQ, and so on. It also supports alarms, rate limiting, and interruption to ensure the operation of core services.
- Behavior auditing: The DPX8000 series products audit the applications of P2P, instant message, web game, mails, and data transmission, and generate logs to implement behavior auditing in granularity.

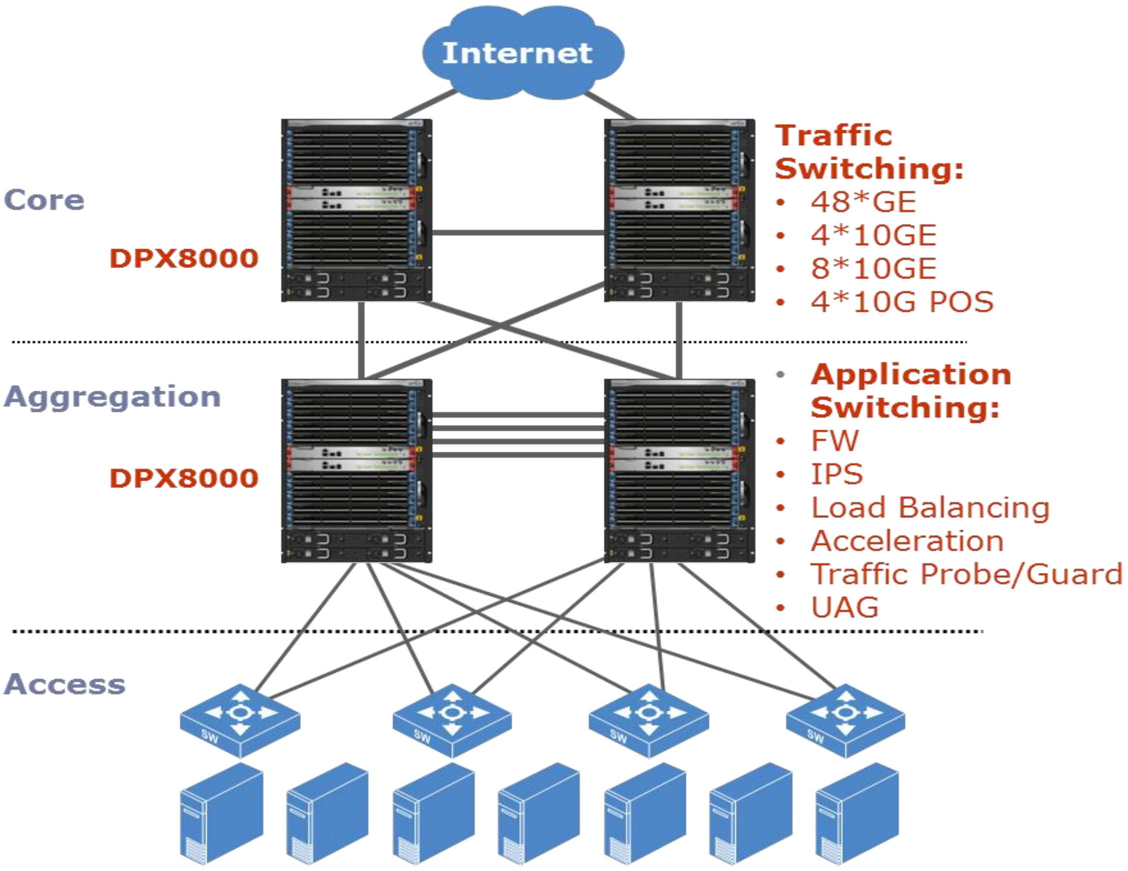
Carrier-Class High Equipment Reliability

- Dual-MPU, Fan, Clock and N+1 power redundant system
- All components support hot swap
- Dual-system state hot backup, Active/Active and Active/Passive work modes, and load sharing and service backup supported
- Powerful backplane design which separate data plane, control plane and management plane to provide high speed performance.
- 36 years of Mean Time Between Failure (MTBF)
- The key components of the equipment adopt a redundant design
- Support the automatic temperature detection of the internal environment. Able to collect alarm information automatically through DPtech UMC system

Intelligent Graphic Management

- Support remote configuration management through the Web mode
- Support the unified management of network and equipment through DPtech UMC management system

Typical Model



Specification

Table 1 Lists the Hardware Specification of DPX8000 Series Deep Service Switch Gateway

Item	DPX8000-A3	DPX8000-A5	DPX8000-A12
MPU Slots	1	1	2
Service Slots	2	4	10
Power Supply Slots	2	2	4
Switch Capability	1320Gbps	2600Gbps	6480Gbps
Packet Forwarding Rate	990Mpps	1950Mpps	4860Mpps
Maximum GE Ports	96	192	480
Maximum 10GE Ports	66	130	324
Maximum 40GE Ports	4	8	20

Item	DPX8000-A3	DPX8000-A5	DPX8000-A12
Dimensions (W × H × D)	436x 178 x 480	436x 283 x 480	436x 666 x 480
Full Configuration Weight	≤27kg	≤45kg	≤95kg
Power Input	DC：–48V～–60V AC： 100V～240V		
Rated Power	650w	650w	1200w
Environment Temperature	0℃～45℃		
Environment Humidity	10%～95%		
Acoustic	Power: 57 dB, Pressure: 40.2 dB		

Table 2 Lists the Performance of DPX8000 Series Service Module

Item	Description	Specification
Firewall Service Module	Packet Filter Throughput	15Gbps
	VPN Throughput	5Gbps
	Concurrent Connections	• 4,000,000 • 256,000 Concurrent NAT or PAT translations
	New connections per second	150,000
	IPSEC Tunnel	20,000
	Max Policy	10,000
	Security Zones	256
	VLAN Number	4096
	Virtual Firewall	512
Enhanced Firewall Service Module	Packet Filter Throughput	40Gbps
	VPN Throughput	10Gbps
	Concurrent Connections	• 50,000,000 • 256,000 Concurrent NAT or PAT translations
	New connections per second	1,500,000
	IPSEC Tunnel	20,000
	Max Policy	10,000
	Security Zones	256
	VLAN Number	4096
	Virtual Firewall	1,024
SSL VPN Service Module	Packet Filter Throughput	10Gbps
	SSL VPN Throughput	300Mbps

Item	Description	Specification
	Max. Concurrent Users	5,000
IPS Service Module	Throughput	6Gbps
	Concurrent Connections	4,000,000
	New connections per second	100,000
	Max Policy	20,000
Enhanced IPS Service Module	Throughput	40Gbps
	Concurrent Connections	32,000,000
	New connections per second	1,200,000
	Max Policy	20,000
UAG Service Module	Throughput	3Gbps
	Concurrent Connections	4,000,000
	New connections per second	80,000
ADX Service Module	Throughput	5Gbps
	Concurrent Connections	2,500,000
	New connections per second	160,000
nFlow Service Module	Throughput	5Gbps
	Concurrent Connections	2,500,000
Wireless Service Module	Throughput	10Gbps
	Maximum Managed AP	640

Table 3 Lists the Detailed Feature of DPX8000 Series Interface Module

Attribute	Description	
Network Interconnection	**LAN**	• Ethernet_II • Ethernet_SNAP • 802.1Q VLAN
	WAN	• PPP • POS
Layer-2 Protocol	• STP / RSTP / MSTP • FRRP(Fast Ring Redundant Protocol) • GVRP • BPDU Tunneling • LLDP and DLDP • Link Aggregation	

Attribute	Description	
	• VLAN partition based on ports, protocols, subnet and MAC • Jumbo Frame • QinQ and Selective QinQ	
Software-Defined Networking (SDN)	• Support OpenFlow 1.3 protocol • Support multi-controller, Equal or Active-standby mode • Support Normal or OpenFlow mode • Support multiple Flow Table • Support Group Table • Support Meter	
Network Protocol	**IP Service**	• IPv4 and IPv6 Dual Stack • ARP • Domain name resolution • IP UNNUMBERED • DHCP Trunk • DHCP Server • DHCP Client • DNS
	IP Routing	• IPv4 and IPv6 Routing • Static routing • RIP v1/2 • RIPng • OSPFv1 / v2 / v3 • BGP / BGP4+ / MBGP • IS-IS • Routing policy • Policy routing • ECMP • Tunneling
	Multicast Protocol	• IGMP • IGMP snooping • MLD Snooping

Attribute	Description	
		- PIM-DM / PIM-SM / PIM-SSM
MPLS / VPLS Features	- Multiple CE (MCE), Layer 2 VPN and Layer 3 MPLS VPN - VLL (Martini and Kompella) - VPLS	
High Reliability	- Key component redundancy design - Host swapping of interface module - Support VRRP - Hitless Operating System Upgrade - Automatic detection of chassis temperature - Support BFD on routing protocols	
ACL / QoS	- Standard and Extended ACL - 802.1p / DSCP priority marking and remarking - Rate Limiting and Traffic shaping - RED, WRED - CAR - SP, CBWFQ, PQ, CQ, RR and WRR	
Security	- Port Security - Port Isolation - MAC authentication - Broadcast Suppression - STP Root Guard - BPDU Guard - uRPF - DHCP Snooping - IP Source Guard - RADIUS Authentication - HWTACACS authentication - IEEE 802.1X	
Configuration Management	**Command Line Interface (CLI)**	- Perform local configuration through the Console port - Perform local or remote configuration through Telnet or SSH - The leveled protection of the configuration

Attribute	Description	
		command ensures that the unauthorized user cannot intrude the equipment • The detailed debugging information helps to diagnose network faults • Provide network test tools, for example, Tracert and Ping commands, to quickly diagnose whether the network is normal • Execute the Telnet command directly to access and management other equipment • FTP Server/Client can use FTP download and upload to configure files and software applications • Support the upload/download of files through TFTP • Support the log function • File system management • User-interface configuration provides multiple modes of authentication and authorization functions of the users
	• Support standard network management SNMPv3. Compatible with SNMP v2c and SNMP v1 • Support MIB • Support NTP time synchronization • Support Port Mirroring and Remote Port Mirroring • Support sFlow • Support analysis of network performance and quality	
	• Perform remote configuration management through the Web mode • Support the DPtech UMC system to perform equipment management	

Table 4 Lists the Detailed Feature of DPX8000 Series Firewall / SSL VPN Service Module

Attribute	**Description**	
Operation Mode	- Routing mode - Transparent mode - Hybrid mode	
Network Security	**AAA Service**	- RADIUS authentication - HWTACACS authentication - PKI /CA (X.509 format) authentication - Domain authentication - CHAP authentication - PAP authentication
	Firewall	- Packet filtering - Basic and extended ACL - Interface-based ACL - Time segment-based ACL - ACL oriented to objects - Dynamic packet filtering - Modular Policy Framework (MPF) with flow-based security policies - Protocol conformance checking - Application layer protocols: IM (QQ and MSN) FTP, HTTP, SMTP, RTSP, H.323 (Q.931, H.245, and RTP/RTCP),PPTP,SIP, NetBios, RAS - Transmission layer protocols: TCP and UDP - Anti-attack feature - Land, Smurf, Fraggle, WinNuke, Ping of Death, Tear Drop, IP Spoofing, CC, SYN Flood, ICMP Flood, UDP Flood, and DNS Query Flood - ARP spoofing attack defense - ARP active reverse lookup - Unicast reverse Path Forwarding (URPF) - TCP packet illegal flag bit attack defense - Super large ICMP packet attack defense

Attribute	Description	
		• Address/port scanning defense • DoS/DDoS attack defense • TCP Proxy function • ICMP redirection or unreachable packet control function • Tracert packet control function • IP packet control function with routing record option • Static and dynamic blacklist function • MAC and IP binding function • Transparent firewall • Transparent mode supports static routing and ARP inspection • MAC-based ACL • Support 802.1Q VLAN transparent transmission • Static routing support in single- and multiple virtual systems
	Mail/Web page/Application Layer Filtering	• Mail filtering • SMTP mail address filtering • Mail subject filtering • Mail content filtering • Mail attachment filtering • Web page filtering • HTTP URL filtering • HTTP content filtering • RFC compliance checking for protocol anomaly detection, HTTP command filtering, MIME type filtering, content validation, Uniform Resource Identifier (URI) length enforcement • Application layer filtering • Java Blocking • ActiveX Blocking • SQL injection attack defense

Attribute	Description	
		- SYN Cookies
	Security Log and Statistics	- User behavior flow log - NAT conversion log - Attack real-time log - Blacklist log - Address binding log - Traffic alarm log - Traffic statistics and analysis function - Global/security domain based connection rate monitoring - Global/security domain based protocol packet percentage monitoring - Security event statistics function - E-MAIL mail real-time alarm function - E-MAIL mail periodical information release function
	NAT	- Dynamic / Static NAT and PAT - Policy-based NAT - VRF-aware NAT - Destination NAT for Multicast - Support the mapping of multiple internal addresses to a public network address - Support the mapping of multiple internal addresses to multiple public network addresses - Support the one-to-one mapping of internal address and public network address - Support the simultaneous conversion of source address and destination address - Support the access to an internal server by an

Attribute	Description	
		external network host • Support the direct mapping of the internal address to the IP address of the interface public network • Support the DNS mapping function • Able to configure the valid time of address conversion • Support multiple NAT ALGs, including DNS, FTP, H.323, ILS, MSN, NBT, PPTP, and SIP
VPN	**IPSec/IKE**	• Support AH and ESP protocols • Support the automatic establishment of a security alliance manually or through IKE • Support IKE-XAUTH, Internet Key Exchange (IKE; RFCs 2407-2409),IKE-CFG-MODE • ESP supports DES, 3DES and AES algorithmes • Support MD5 and SHA-1 authentication algorithms • Support the IKE main mode and aggressive mode • Support NAT traversing • Support DPD detection • Support of site-to-site IPsec, remote-access IPsec, and certificate authority/public key infrastructure (CA/PKI). • Support the following CA/PKI: Entrust,VeriSign, Microsoft, Netscape, Baltimore Technologies, IPlanet • Support X.509 digital certificates (RSA signatures), Encrypted Nonces (RSA encryption), Preshared keys, RADIUS (RFC 2138) , Simple Certificate Enrollment Protocol (SCEP)
	SSL VPN	• Support high-performance IP SSL VPN services for secure transport across the network • Support the flexibility and density as they scale their network infrastructure and expand secure, remote services to branch offices and offsite users • Support 1 console port

Attribute	Description	
		• Support integration with Switch to implement convenient, fast, secure remote access. • Support web browser to access internal network resources securely, easily, and quickly • Support all client-side configuration information is saved on the SSL VPN server, which resides on the internal network • Support clearing the relevant buffers, cookies, and configuration files automatically to prevent sensitive information from being leaked when user logs out • Support multiple access modes (including Web access, TCP access, and IP access) • Support granular access control of resources (such as URLs and servers) • Support providing multiple popular authentication and external authorization platforms, including local authentication, RADIUS, LDAP, AD, RSA SecurID and third-party PKI authentication, supporting authentication, authorization, and management of different users • Support RSA digital signature algorithm • Support MD5 and SHA1 digest algorithms • Support encryption algorithms of RC4, DES, 3DES, and AES • Supports the client/server model and, through its SSL VPN channels, can service various applications, such as Exchange, FTP, Outlook, and VNC
QoS	**Traffic Policing**	• CAR
	Queue Schedule	• PQ, CQ, RR, WRR
Web Management	• HTTP/HTTPS/USB Key	
Log information	• Support attack log, URL filtering log ,System log, Operation log, Syslog	
High Reliability	• Dual-system state hot backup	

Attribute	Description
	• Active/Active and Active/Passive work modes • Load sharing and service backup supported

Table 5 Lists the Detailed Feature of DPX8000 Series IPS Service Module

Features	Description
Signature	• More than 4000 number and updated weekly, CVE compliant signature database
Attack Protection Types	• Support Web protection, mail server protection, FTP server protection, DNS vulnerability protection, cross-site script protection, SNMP vulnerability protection, worm and virus protection, violent attack protection, SQL injection protection, backdoor program prevention, Trojan horse protection, spyware protection, detection/scanning protection, web phishing protection, and IDS/IPS bypass attack protection
Anti-DDoS	• SYN Flood, RST Flood, ACK Flood, ICMP Flood, UDP Flood, DNS Query Flood, DNS Response Flood, DNS Guard, HTTP Get Flood, CC attack
Protocol Abnormally Detect	• H.323, SIP, TCP, UDP,SMTP, POP3, IMAP4,FTP
Attack Detect	• IP Fragmentation and Reassembly, TCP normalization, session status track
Anti-Virus Types	• File viruses, network viruses and hybrid viruses
P2P Identification	• BT, eDonkey, eMule, FlashGet, Thunder, PPTV, and QQLive
Instant Messaging (IM) Identification	• MSN, QQ, Google/Gtalk, and Yahoo Messenger, ICQ
URL Filtering	• Support 50 URL category, 1,000,000 URL filter database
Response Actions	• Blocking, traffic limiting, redirecting, isolating, and alerting by Email.
Signature Upgrade Mode	• Automatic/Manual
HA	• Support A/A, application Bypass, hardware Bypass
Centralized Management	• IPS event monitor and report: Top N attack events, Top N attack source addresses, Top N destination addresses, Top N anti-virus attack etc. Centralized policy manager
Deployment Mode	• Support transparent mode, offline mode, hybrid mode

Environmental Protection Standard	- RoHS
Web Management	- HTTP/HTTPS/USB Key
Log Information	- Support attack log, anti-virus log, URL filtering log ,System log, Operation log, Syslog
Management Interface Language	- English / Chinese

Table 6 Lists the Detailed Feature of DPX8000 Series UAG Service Module

Features	**Description**
Signature	- More than 800 type applications and updated weekly, CVE compliant signature database
P2P Identification	- BT, eDonkey, eMule, FlashGet, Thunder, PPTV, and QQLive
Instant Messaging (IM) Identification	- MSN, QQ, Google/Gtalk, and Yahoo Messenger, ICQ
Anti-DDos	- SYN Flood, RST Flood, ACK Flood, ICMP Flood, UDP Flood, DNS Query Flood, DNS Response Flood, DNS Guard, HTTP Get Flood, CC attack
Response Actions	- Blocking, traffic limiting, redirecting, isolating, and alerting by Email
Anti-Virus Types	- File viruses, network viruses and hybrid viruses
URL Filtering	- Support 50 URL category, 1,000,000 URL filter database
Signature Upgrade Mode	- Automatic/Manual
HA	- Support A/A, application Bypass, hardware Bypass
Centralized Management	- Traffic and Applications monitor and report: Top N Application type, Top N user traffic statistics, Top N destination addresses, Top N anti-virus attack etc. Centralized policy manager
Deployment Mode	- Support transparent mode, offline mode, hybrid mode
Environmental Protection Standard	- RoHS
Web Management	- HTTP/HTTPS/USB Key
Log Information	- Support attack log, anti-virus log, URL filtering log ,System log, Operation log, Syslog

Management Interface Language	- English / Chinese

Table 7 Lists the Detailed Feature of DPX8000 Series ADX Service Module

Features	**Description**
Deployment Mode	- Support transparent mode, offline mode, hybrid mode
Load Balancing Algorithm	- Round robin - Weighted round robin - Least connections - Random - Weighted random
Health Check	- Ping (ICMP), TCP, HTTP, FTP, SSL, RADIUS, and DNS
Environmental Protection Standard	- RoHS
Web Management	- HTTP/HTTPS/USB Key
Management Interface Language	- English / Chinese

Table 8 Lists the Detailed Feature of DPX8000 Series nFlow Service Module

Features	**Description**
Deployment Mode	- Support transparent mode, bidirectionnel traffic flow mirroring mode
Format	- Version 5 - Version 9
HA	- Support A/A, application Bypass, hardware Bypass
Environmental Protection Standard	- RoHS
Web Management	- HTTP/HTTPS/USB Key
Management Interface Language	- English / Chinese

Table 9 Lists the Detailed Feature of DPX8000 Series Wireless Service Module

Features	**Description**
802.11 LAN protocols	• 802.1a/b/g/n Access Point Management
Roaming	• Inter and intra AC Roaming
802.11 security and privacy	• Multi-SSID • Hidden SSID • 802.11i, (with 802.1X and PSK authentication) • WEP (WEP64/WEP128) • WPA,WPA2 • TKIP • CCMP
Environmental Protection Standard	• RoHS
Web Management	• HTTP/HTTPS/USB Key
Management Interface Language	• English / Chinese

Order Information

Ordering List

Part Number	**Model Description**	**Remarks**
02050027	DPtech DPX8000-A3 Host	Required
02050026	DPtech DPX8000-A5 Host	Required
02050025	DPtech DPX8000-A12 Host	Required
02010025	DPtech MPUA Module	Required
02010022	DPtech MPUA Module, with 2-port 10Gigabit Interfaces (XFP Req.)	Optional
02010043	DPtech Firewal Service Module, with 12-port 1000Base-X Ethernet Optical Interface (SFP Req.) and 12-port 10/100/1000Base-T Electrical (RJ45) Interface	Optional

02010060	DPtech Enhanced Firewall Service Module, with 24-port 1000Base-X Ethernet Optical Interface (SFP Req.) and 4-port 10GE Ethernet SFP+ Optical Interface (SFP+ Req.)	Optional
02010082	DPtech SSL VPN Module,24 Ports GigaBit(12*SFP+12*RJ45)	Optional
01100031	DPtech IPS Service Module, with 12-port 1000Base-X Ethernet Optical Interface (SFP Req.) and 12-port 10/100/1000Base-T Electrical (RJ45) Interface	Optional
01100038	DPtech Enhanced IPS Service Module, with 24-port 1000Base-X Ethernet Optical Interface (SFP Req.) and 4-port 10GE Ethernet SFP+ Optical Interface (SFP+ Req.)	Optional
01100032	DPtech UAG Service Module, with 12-port 1000Base-X Ethernet Optical Interface (SFP Req.) and 12-port 10/100/1000BASE-T Electrical(RJ45) Interface	Optional
02010034	DPtech ADX Service Module, with 12-port 1000Base-X Ethernet Optical Interface (SFP Req.) and 12-port 10/100/1000BASE-T Electrical(RJ45) Interface	Optional
01100033	DPtech Wireless Service Module, with 12-port 1000Base-X Ethernet Optical Interface (SFP Req.) and 12-port 10/100/1000Base-T Electrical (RJ45) Interface	Optional
01100034	DPtech nFlow Service Module, with 12-port 1000Base-X Ethernet Optical Interface (SFP Req.) and 12-port 10/100/1000BASE-T Electrical(RJ45) Interface	Optional
02010023	DPtech 4-Port 10Gigabit Ethernet Optical Interface Module, XFP Req.	Optional
02010036	DPtech 8-Port 10Gigabit Ethernet Optical Interface Module, XFP Req.	Optional
02010027	DPtech 48-Port 1000Base-X Gigabit Ethernet Optical Interface Module, SFP Req.	Optional
02010032	DPtech 48-Port 10/100/1000BASE-T Ethernet Interface Module (RJ45)	Optional

02010114	DPtech 32-Port 10GBASE Ethernet Optical SFP+ Interface Module, SFP+ Req.	Optional
02010028	DPtech AC Power Supply Module, 650W	Optional
02010038	DPtech DC Power Supply Module, 650W	Optional

Advanced Service List

Part Number	Description	Remarks
53010135	FW12GEP12GET,1 Year Application Signature Update	Optional
53010136	FW12GEP12GET,1 Year URL- Signature Update,1 Year URL-Filter Update	Optional
53010130	IPS12GEP12GET,1 Year Signature Update,1 Year Antivirus Update	Optional
53010131	UAG12GEP12GET,1 Year Application Signature Update	Optional
53010132	UAG12GEP12GET,1 Year Antivirus Signature Update,1 Year Antivirus Update	Optional

SSL VPN License

Part Number	Model Description	Remarks
53010137	DPtech SSL VPN 10 Users License	Optional
53010138	DPtech SSL VPN 50 Users License	Optional
53010139	DPtech SSL VPN 100 Users License	Optional
53010140	DPtech SSL VPN 250 Users License	Optional
53010141	DPtech SSL VPN 500 Users License	Optional
53010142	DPtech SSL VPN 1000 Users License	Optional
53010143	DPtech SSL VPN 2500 Users License	Optional
53010144	DPtech SSL VPN 5000 Users License	Optional

📖 **Note:**

“Required” indicates that the item described is provided directly with the ordered host. The user does not need to purchase it specially.

“Optional” indicates the item described should be purchased by the user if it is needed.

Statement: DPtech attempts to provide the accurate information for users, but they cannot take any responsibility for the technical error or print mistake, DPtech has all rights to modify the document without any notify or information.