

DPtech FW1000 Series Firewall



Overview

Firewall 1000 series provides security prevention solutions for 100Mbps, 1Gbps, and 10Gbps network environments. It adopts professional hardware and software systems, and provides highly reliable, stable and feature-rich security services. To effectively defend against various threats, this series delivers advanced state-based IPv4 and IPv6 filtering, as well as anti-attacks, zone isolation, Anti-Virus, remote access via VPN, and NAT. Because of the multi-purposed design, it reduces the number of the security devices to be implemented on the network and the complexity of management.

To ensure reliable and robust operation, the series provides redundancy for core components, and offers stateful failover which is based on links and state. This series rigidly conforms to the EU Restriction of Hazardous Substances Directive (RoHS), therefore, it is the best choice for enterprises that want to choose a green and secure firewall.

The DPtech FW1000 series Firewall are the professional network security products that DPtech designs for medium and small businesses, large-scale enterprises and ISP. The DPtech FW1000 series Firewall integrate seamlessly the powerful security defense functions, professional VPN services and intelligent network features on one single hardware platform. The series products can provide extensive and in-depth security protection and security connection functions. In addition, they can reduce the Total Cost Ownership (TCO) and the deployment complexity related to security. They are an ideal option of network security solution. They have become the solid foundation of the IP self-adaptive security network.

The DPtech FW1000 series Firewall are new generation carrier-class firewall equipment of DPtech oriented to medium and small businesses, large-scale enterprises and ISP. The DPtech FW1000 series Firewall adopt the state-of-the-art hardware platform and architecture, achieving a leapfrog breakthrough of the firewall performance. It is able to support 24-port Gigabit Ethernet and 2-port 10Gigabit interfaces, which satisfies the requirements of carrier-class applications.

The products support 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 state detecting technology, to detect the connectivity and abnormal commands. It provides multiple intelligent analyses 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 and IPSec VPN, and is able to construct multiple forms of VPNs. It provides the basic routing capability, and supports RIP / OSPF / BGP / routing policy and policy routing. It supports diverse QoS features.

The DPtech FW1000 series Firewall takes full consideration of the requirements on high reliability by network applications. The service interface card supports hot swapping to fully satisfy the requirements on network

maintenance, upgrade, and optimization. It supports dual-system state hot backup, and the Active/Active and Active/Passive work modes. It provides the temperature detecting function within the internal environment of the chassis, and supports the unified management by UMC (Unified Management Center).

Series

The following are the DPtech FW1000 series product's portfolio.



FW1000-TE-17N



FW1000-TA-N



FW1000-Blade-EI



FW1000-Blade-A



FW1000-Blade-S



FW1000-TA-A



FW1000-TM-E



FW1000-TS-E



FW1000-TS-A



FW1000-GA-E



FW1000-GM-A



FW1000-GM-E



FW1000-GS-N



FW1000-GC-N



FW1000-ME-N



FW1000-MA-N



FW1000-MS-N

Features

Advanced Platform Architecture

- DPtech FW1000 series Firewall adopts the carrier-class hardware platform. It satisfies the requirement on the security equipment linear processing capability by the core enterprise users through the multi-core system and self-developing ASIC.

Leading Security Protection Function in the Market

- Enhanced state security filtering: Support the virtual firewall technology. Support the default access control between security zones. Support the basic, extended and interface-based state detecting packet filtering technology. Support filtering based on time segment. Support the maintenance and monitoring of each piece of connection state information and dynamically filter packets. Support the state monitoring of FTP, HTTP, SMTP, RTSP, and H.323 (including Q.931, H.245 and RTP/RTCP) application layer protocols. Support the state monitoring of TCP/UDP.
- Anti-attack defense capability:

- Include DoS / DDoS attack defense (CC, SYN flood and DNS Query Flood) and ARP spoofing defense.
 - ✓ The following functions and features are provided:
 - ARP active reverse lookup
 - TCP packet illegal flag bit attack defense
 - Super large ICMP packet attack defense
 - Address/port scanning defense
 - 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
- Application layer content filtering:
 - ✓ Effectively identify and control applications in different P2P modes of the network, and take traffic limiting control measures for the applications to effectively protect network bandwidth.
 - ✓ Able to identify and control the IM protocol, for example, QQ and MSN.
 - ✓ Support mail filtering, and provide filtering by SMTP mail address, subject, attachment and content.
 - ✓ Support web page filtering, and provide filtering by HTTP URL and content.
 - ✓ Support application layer filtering and provide Java/ActiveX Blocking and SQL injection attack.
- Multiple security authentication services:
 - ✓ Support RADIUS protocols and domain authentication.
 - ✓ Support the authentication function of digital certificate (X.509 format) based on the PKI/CA system.
 - ✓ Support user identity management. Users with different identities own different command execution rights.
 - ✓ Support user view level division. Users at different levels are offered different management and configuration rights.
- Centralized management and audit:
 - ✓ Provide different log functions, traffic statistics & analysis functions, monitoring and statistics function of different events, and mail alarm function.
- All-round NAT application support:
 - ✓ Provide such NAT application modes as multiple-to-one, multiple-to-multiple, static network segment, bidirectional conversion, IP masquerade and DNS mapping.
 - ✓ Support the correct traversing of multiple application protocols through NAT. Provide such NAT ALG functions as DNS, FTP, SIP, RSTP, H.323 and NBT.
 - ✓ Support unlimited NAT conversion.
- Support GRE, L2TP, IPSec VPN and other multiple VPN service modes.
- Support real-time Anti-Virus which adopt Kaspersky's Anti-Virus engine to detect and remove codes of malicious attacks in time.

Intelligent Network Integration

- Support routing, transparent and hybrid operation modes.
- 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.

Carrier-Class High Equipment Reliability

- Dual-system state hot backup, Active/Active and Active/Passive work modes, and load sharing and service backup supported
- 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 the network management system.

Intelligent Graphic Management

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

Specification

Table 1 Lists the Hardware Features and Performance of DPtech FW1000-MS, MA and ME series Firewall

Item	FW1000-MS-N	FW1000-MA-N	FW1000-ME-N
Interface	1xConsole, 4xGE, 1xUSB	1xConsole, 8xGE, 1xUSB	1xConsole, 8xGE, 1xUSB
Slot	1 slot	1 slot	2 slot
CF card	1GB	1GB	1GB
DDR SDRAM	1GB	1GB	1GB
Dimensions (W × D × H)	430x261x44 mm	430x261x44 mm	430x261x44 mm
Power Supply	1	1	1
Rated Voltage Max Current	100-240VAC; 1.5A	100-240VAC; 1.5A	100-240VAC;1.5A
Max Power Consumption	54 W	54 W	54 W
MTBF	36 years	36 years	36 years
Operating Temperature	0°C to 45°C (32 to 113°F)	0°C to 45°C (32 to 113°F)	0°C to 45°C (32 to 113°F)
Relative Humidity	10% to 95%	10% to 95%	10% to 95%
Weight	3.1 kg	3.1 kg	3.1 kg

Item	FW1000-MS-N	FW1000-MA-N	FW1000-ME-N
Firewall Throughput	4Gbps	5Gbps	6Gbps
IPS Throughput	2Gbps	2.5Gbps	3Gbps
Recommended number of users	100	200	300
Concurrent Connections	1200000	1500000	2000000
New Connections per Second	10000	15000	20000
Firewall Latency(1518 bytes)	10us	10us	10us
Firewall Latency(64 bytes)	5us	5us	5us
IPSec Tunnel	1000	1000	1000
L2TP Tunnel	500	500	500
Max Policy	10000	10000	10000
Security Zones	64	64	64
VLAN Number	4096	4096	4096
Virtual Firewall	64	64	64

Table 2 Lists the Hardware Features and Performance of DPtech FW1000-GC, GS and GM series Firewall

Item	FW1000-GC-N	FW1000-GS-N	FW1000-GM-E
Interface	1xConsole, 6xGE, 2xGE SFP, 1xUSB	1xConsole, 6xGE, 2xGE SFP, 1x USB	1xConsole, 4xGE, 4xGE SFP, 2xUSB
Slot	1 slot	1 slot	2 slot
CF card	1GB	1GB	1GB
DDR SDRAM	2GB	2GB	4GB
Dimensions (W x D x H)	430x261x44 mm	430x261x44 mm	430x261x44 mm
Power Supply	2	2	2
Rated Voltage Max Current	100-240VAC; 1.5A	100-240VAC; 1.5A	100-240VAC; 1.5A
Max Power Consumption	54 W	54 W	54 W
MTBF	36 years	36 years	36 years

Item	FW1000-GC-N	FW1000-GS-N	FW1000-GM-E
Operating Temperature	0°C to 45°C (32 to 113°F)	0°C to 45°C (32 to 113°F)	0°C to 45°C (32 to 113°F)
Relative Humidity	10% to 95%	10% to 95%	10% to 95%
Weight	3.1 kg	3.1 kg	3.1 kg
Firewall Throughput	8Gbps	8Gbps	10Gbps
IPS Throughput	4Gbps	4Gbps	5Gbps
Recommended number of users	1000	2000	3000
Concurrent Connections	2600000	3000000	3000000
New Connections per Second	40000	60000	80000
Firewall Latency(1518 bytes)	10us	10us	10us
Firewall Latency(64 bytes)	5us	5us	5us
IPSec Tunnel	8000	8000	8000
L2TP Tunnel	1000	1000	1000
Max Policy	10000	10000	10000
Security Zones	128	128	128
VLAN Number	4096	4096	4096
Virtual Firewall	128	128	128

Table 3 Lists the Hardware Features and Performance of DPtech FW1000-GA, GE and TS series Firewall

Item	FW1000-GM-A	FW1000-GA-E	FW1000-TS-A	FW1000-TS-E
Interface	1xConsole, 8xGE Combo, 16xGE SFP, 1x USB	1xConsole, 8xGE Combo, 16xGE SFP, 1x USB	1xConsole, 8xGE, 8xGE SFP, 4x10GE, 2xUSB	1xConsole, 2xGE, 4xGE Combo, 4x10GE, 1xUSB
Slot	2	2	2	4
CF card	2GB	2GB	2GB	2GB
DDR SDRAM	4GB	4GB	8GB	8GB
Dimensions (W x D x H)	436x360x44 mm	436x360x44 mm	436x424x44 mm	436x510x88 mm
Power Supply	2	2	2	2

Item	FW1000-GM-A	FW1000-GA-E	FW1000-TS-A	FW1000-TS-E
Rated Voltage Max Current	100-240VAC; 1.5A	100-240VAC; 1.5A	100-240VAC; 1.5A	100-240VAC; 4A
Max Power Consumption	150w	150w	150w	300 W
MTBF	36 years	36 years	36 years	36 years
Operating Temperature	0°C to 45°C (32 to 113°F)	0°C to 45°C (32 to 113°F)	0°C to 45°C (32 to 113°F)	0°C to 45°C (32 to 113°F)
Relative Humidity	10% to 95%	10% to 95%	10% to 95%	10% to 95%
Weight	5kg	5kg	6.2kg	10kg
Firewall Throughput	15Gbps	20Gbps	25Gbps	30Gbps
IPS Throughput	7Gbps	10Gbps	13Gbps	15Gbps
Recommended number of users	3000	5000	15000	15000
Concurrent Connections	3000000	4000000	6000000	6000000
New Connections per Second	80000	150000	300000	300000
Firewall Latency(1518 bytes)	10us	10us	10us	10us
Firewall Latency(64 bytes)	1us	1us	1us	1us
IPSec Tunnel	20000	20000	20000	20000
L2TP Tunnel	2000	2000	2000	2000
Max Policy	10000	10000	10000	10000
Security Zones	256	256	512	1024
VLAN Number	4096	4096	4096	4096
Virtual Firewall	128	128	256	1024

Table 4 Lists the Hardware Features and Performance of DPtech FW1000-TM, TA, FW1000-Blade series Firewall

Item	FW1000-TM-E	FW1000-TA-A	FW1000-Blade-S
Interface	1xConsole, 2xGE, 4xGE Combo, 4x10GE, 1xUSB	1xConsole, 2xGE, 4xGE, 4xGE SFP, 4x10GE, 1xUSB	1xConsole, 12xGE, 12xGE SFP, 1xUSB
Slot	4	4	-

Item	FW1000-TM-E	FW1000-TA-A	FW1000-Blade-S
CF card	2GB	2GB	2GB
DDR SDRAM	8GB	16GB	8GB
Dimensions (W x D x H)	436x510x88 mm	436x510x88 mm	Blade Type
Power Supply	2	2	-
Rated Voltage Max Current	100-240VAC; 4A	100-240VAC; 4A	-
Max Power Consumption	300 W	300 W	-
MTBF	36 years	36 years	36 years
Operating Temperature	0°C to 45°C (32 to 113°F)	0°C to 45°C (32 to 113°F)	0°C to 45°C (32 to 113°F)
Relative Humidity	10% to 95%	10% to 95%	10% to 95%
Weight	10kg	10kg	-
Firewall Throughput	40Gbps	80Gbps	10Gbps
IPS Throughput	20Gbps	40Gbps	5Gbps
Recommended number of users	15000	25000	8000
Concurrent Connections	6000000	16000000	5000000
New Connections per Second	300000	600000	150000
Firewall Latency(1518 bytes)	10us	10us	10us
Firewall Latency(64 bytes)	1us	1us	1us
IPSec Tunnel	20000	30000	20000
L2TP Tunnel	2000	2000	2000
Max Policy	10000	10000	10000
Security Zones	1024	1024	256
VLAN Number	4096	4096	4096
Virtual Fiewall	1024	128	128

Table 5 Lists the Hardware Features and Performance of SSLVPN-Blade-A series Firewall

Item	SSLVPN-Blade-A
Interface	1xConsole, 12xGE, 12xGE SFP, 2x10GE ,1xUSB
Slot	-
CF card	2GB
DDR SDRAM	16GB
Dimensions (W x D x H)	Blade Type
Power Supply	-
Rated Voltage Max Current	-
Max Power Consumption	-
MTBF	36 years
Operating Temperature	0°C to 45°C (32 to 113°F)
Relative Humidity	10% to 95%
Weight	-
Max Number of Users	30000

Table 6 Lists the Feature of DPtech FW1000 series Firewall

Attribute	Description	
Operation Mode	<ul style="list-style-type: none"> • Routing mode • Transparent mode • Hybrid mode 	
Network Security	AAA service	<ul style="list-style-type: none"> • RADIUS authentication • PKI /CA (X.509 format) authentication • Domain authentication • CHAP authentication • PAP authentication
	Firewall	<ul style="list-style-type: none"> • Packet filtering • Dynamic packet filtering • Full State Detecting • Application layer protocols: IM (QQ and MSN) FTP, HTTP, SMTP, POP3, RTSP, SIP, H.323 (Q.931,

Attribute	Description	
		<p>H.245, and RTP/RTCP)</p> <ul style="list-style-type: none"> • 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, SYN Cookie Proxy • ARP spoofing attack defense • ARP active reverse lookup • TCP packet illegal flag bit attack defense • Super large ICMP packet attack defense • 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 • Support 802.1Q VLAN transparent transmission
	Anti-Virus	<ul style="list-style-type: none"> • Virus definition-based detection • Library upgrading manually and automatically • Flow handing mode • Supporting protocols of HTTP, FTP, SMTP, and POP3. • Preventing virus types of Backdoor, Email-Worm, IM-Worm, P2P-Worm, Trojan, Ad Ware, Virus • Supporting virus logs and reports
	Mail / Web Page / Application Layer Filtering	<ul style="list-style-type: none"> • Mail filtering • SMTP mail address filtering • Mail subject filtering • Mail content filtering

Attribute	Description	
		<ul style="list-style-type: none"> • Mail attachment filtering • Web page filtering • HTTP URL filtering • HTTP content filtering • Application layer filtering • Java Blocking • ActiveX Blocking • SQL injection attack defense
	Security Log and Statistics	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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 external network host • Support the direct mapping of the internal address to

Attribute	Description	
		<p>the IP address of the interface public network</p> <ul style="list-style-type: none"> • 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.
	IPSec/IKE	<ul style="list-style-type: none"> • Support AH and ESP protocols. • Support the automatic establishment of a security alliance manually or through IKE. • ESP supports DES, 3DES and AES algorithms. • Support MD5 and SHA-1 authentication algorithms. • Support the IKE main mode and aggressive mode. • Support NAT traversing. • Support DPD detection.
Network Interconnection	LAN Protocol	<ul style="list-style-type: none"> • Ethernet_II • Ethernet_SNAP • 802.1q VLAN
Layer-2 Protocol	<ul style="list-style-type: none"> • STP / RSTP / MSTP • Link Aggregation • VLAN partition based on ports, protocols, subnet and MAC 	
Network Protocol	IP Service	<ul style="list-style-type: none"> • ARP • Domain name resolution • DHCP Relay • DHCP Server • DHCP Client • DNS • PPPoE
	IP Routing	<ul style="list-style-type: none"> • Static routing • RIP v1/2 • RIPng • OSPFv1 / v2 / v3 • BGP / BGP4+

Attribute	Description	
		<ul style="list-style-type: none"> • Routing policy • Policy routing
	Multicast Protocol	<ul style="list-style-type: none"> • IGMP • IGMP snooping • MLD Snooping • PIM-DM / PIM-SM / PIM-SSM
High Reliability		<ul style="list-style-type: none"> • Dual-system state hot backup, Active/Active and Active/Passive work modes, configurations, load sharing and service backup supported • WAN links load balancing • Backup VPN Peers • Key component redundancy design • Host swapping of interface module • Support VRRP • Automatic detection of chassis temperature
Quality of Service (QoS)	Traffic Policing	<ul style="list-style-type: none"> • Rate Limiting and Traffic Shaping • Support LLQ, WRR and CBWFQ • Support WRED and CAR
Configuration Management	Command Line Interface	<ul style="list-style-type: none"> • Perform local configuration through the Console port. • Perform local or remote configuration through Telnet or SSH. • The leveled protection of the configuration 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.

Attribute	Description	
		<ul style="list-style-type: none"> • Support the log function. • File system management • User-interface configuration provides multiple modes of authentication and authorization functions of the users.
	<ul style="list-style-type: none"> • Support standard network management SNMPv3. Compatible with SNMP v2c and SNMP v1. • Support NTP time synchronization. 	
	<ul style="list-style-type: none"> • Perform remote configuration management through the Web mode. • Support HTTP / HTTPS management • Support IPv6 management • Support UMC(Unified Management Center) 	

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.

Copyright©2013 Hangzhou DPtech Technologies Co., Ltd. All rights reserved.

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.