Maipu MPSec IFW400-F5/F4 Firewall Datasheet

Overview

MPSec IFW400-F5/F4 is Maipu high-performance next-generation firewall (NGFW) for small-sized network which can deeply analyze users, locations, traffic, applications, content, etc. in network traffic from multiple perspectives, deeply identify application-layer threats, and provide users with effective application-layer integration security protection, protecting user borders and safe operation of business. The highly integrated multi-functional security module effectively reduces equipment stacking and simplifies user network architecture.

MPSec IFW400-F5-AC

MPSec IFW400-F4-AC

MPSec IFW400 can accurately identify thousands of network applications and provide detailed application traffic analysis and flexible policy control. Combined with user identification, application identification, and content identification, it can provide users with visualized and refined application security management. At the same time, MPSec IFW400 has a built-in threat detection engine, which can resist various network attacks including viruses, Trojan horses, SQL injection, XSS cross-site scripting, and CC attacks, effectively protecting user network health and Web application server security. It provides comprehensive application security protection and flexible expansion methods. It can be deployed in various industries such as enterprise, K12 school, hospitality, commercial building, etc. It is widely used in Internet egress, intranet area boundaries, VPN networking, and other application scenarios.

Technical Specifications

Product Models		MPSec IFW400-F5-AC	MPSec IFW400-F4-AC
Hardware Specification			
Hardware	Hardware Version	V2	V1
	CPU	2-Core 1.0GHZ (ARM)	2-Core 1.0GHZ (ARM)
	Memory	4GB	2GB
	Flash	8GB	8GB
Interface	Default 1G RJ45 Interfaces	8*1G Base-T	5*1G Base-T
	Default 1G SFP Interfaces	2*1G SFP	1*1G Combo (RJ45+SFP)
	Console Port	1	1
	USB Port	1	1
Performance	Default L2&L3 Throughput (1518Byte)	2Gbps	2Gbps
	Max. Throughput (APP)	400Mbps	400Mbps
	Max. Throughput (AV)	340Mbps	340Mbps
	Max. Throughput (IPS)	340Mbps	340Mbps
	Max. Throughput (APP+AV+IPS)	280Mbps	280Mbps
	Max. Concurrent Connection	1M	400K
	New TCP Connection/Sec.	18K	18K
	New HTTP Connection/Sec.	10K	10K
	Recommend Users	50-100	0-50
	Recommend IPSec Tunnels	100-250	50-100
Power Supply	Power Supply	Single Fixed AC	Power Adaptor
	Power Input	100-240V/50-60HZ	100-240V/50-60HZ
	Anti-Surge	±2.5KV@1.2/50us	±2.5KV@1.2/50us
Dimension	W*D*H(mm)	440*330*44mm	240*182*28mm
Weight	Weight(kg)	3.5KG	1.2KG
Environment	Working Temperature	0-45℃	0-45℃
	Storage Temperature	-25-70℃	-25-70℃
	Working Humidity	5%-90%, no-condensing	5%-90%, no-condensing
	Storage Humidity	5%-95%, no-condensing	5%-95%, no-condensing
Software Specification			
Basic Networking Capabilities	Interfaces Mode	Supports physical interfaces and bridge interfaces (supporting Pass-through), VLAN interfaces (Trunk/Access), tunnel interfaces, and loopback interfaces.	
	Routing Characteristics	Supports static routing, policy routing, dynamic routing RIPv1/2, OSPFv2, BGP4, route health check, supports equal-cost routing,	

		source in and source out based on source address preservation and five-tuple
	IP Protocol	Support IPv4/IPv6 dual protocol stack
	LACP	Supports port trunking and LACP (Link Aggregation Control Protocol), as well as static trunking. Supports aggregation algorithms including source/destination MAC hash, source/destination IP hash, source IP hash, source MAC hash, destination MAC hash, destination IP hash etc.
	NAT	Supports source NAT, destination NAT, static NAT, transparent NAT, and NAT backflow, cross-protocol NAT It support non-standard ALG for FTP,TFTP, SIP protocols. The NAT address pool selection algorithm supports source and destination address hashing, polling, and source address retention.
	ISP Routing	Supports ISP routing, built-in multiple operator address libraries, supports health check, and supports multi-path selection based on source IP and connection
	Internet Service	Support DHCP server and relay, support excluded IP, support DHCP status monitoring. The DNS proxy supports transparent DNS proxy functionality. Proxy algorithms include: Priority, Weight, and Traffic; session persistence is supported. Supports multi-interface DNS transparent proxy functionality. In case of link failure, it automatically switches to other links and DNS servers. Supports domain-specific resolution by designated DNS servers.
	VPN	Supports IPSec VPN protocol, supports gateway-to-gateway and remote access deployment modes; supports GRE over IPSec VPN; supports SSL VPN protocol;
	High Reliability	Supports active-active and active-standby modes, interface linkage, and link detection; supports standard VRRP protocol; HA monitoring supports health check, interface monitoring, and link aggregation monitoring
Fine-Grained Access Control	Access Control	Support IPv4/IPv6 8-tuple firewall policy based on source/destination interface/security domain, source/destination IP address/geographical area object, user, service, application, time; support configuration of intrusion prevention, virus protection, WEB access control, application filtering, and other security protection functions; supports session restrictions based on source IP and new limit per second; supports layer 2 and layer 3 network IP-MAC binding; supports adding attack source IP to the blacklist, supports automatic addition or manual addition, supports blacklist life cycle management; supports restricted host or access interface access to local services, such as DNS, https and other services; supports protocol custom session timeout management

	Application Identification	Supports application identification and application behavior identification, supports desktop, Web and mobile application identification, inbuilt with 5000+ applications, supports overseas application libraries and local application libraries; supports custom applications, defining unknown applications based on protocols, ports, IP, domain names and other dimensions; supports manual, automatic and regular updates of the feature database; supports application control policies based on applications, behaviors, and content, and can control and record logs of applications, application behaviors and content such as IM, streaming media, P2P, games, and stocks; support filtering the subject, text keyword, recipient, sender, file name and length of incoming and outgoing emails
	Internet Behavior Audit	Supports QQ, WeChat, WhatsApp account, login, sending and receiving files and other action audits; supports FTP/HTTP file transfer, network disk file upload and download audit; supports website access audit based on URL classification library; supports audit whitelist based on user and IP address; supports all application audits, including audit of accounts, usernames, application names, messages sent and received, content, etc.
	User Authentication	The user authentication supports local authentication, RADIUS authentication, LDAP authentication, Portal authentication, mixed authentication, remote server authentication, SMS authentication, no-auth, AD domain single sign-on, and guest two-dimensional code authentication and other user authentication functions. Supports configuration of mandatory re-login intervals and client timeout settings. Supports custom authentication redirect URLs.
	File Filtering	Supports filtering based on file type
	Email Filtering	Supports filtering the subject, text keyword, recipient, sender, file name and length of incoming and outgoing emails
	Url Filtering	Supports filtering, URL query, blocking and logging based on URL classification library, supports URL keyword filtering, supports local URL classification library and overseas URL classification library
	Intelligent Flow Control	Supports 4-level nested application flow control management policies based on lines and channels, supports upstream and downstream management of total bandwidth based on interfaces and security domains, supports five-tuple channel matching policies for applications, users, source addresses, services, and time, and supports bandwidth restriction, bandwidth guarantee and flexible bandwidth, support per-IP speed limit, per-user speed limit, and support user-based and address-based exclusion policies
Integrated Threat Protection	Attack Protection	Supports IPv4/6 anti-application DOS attack protection, such as HTTP Flood, DNS query flood and other attack protection; supports anti-traffic attack protection, such as SYN Flood, UDP Flood, ICMP Flood, TCP Flood and other attack protection; supports IPv4/6 Anti-DOS attack protection, such as Jolt2, Land-base, Ping-of-Death SYN Flag, Teardrop, Win-nuke, Smurf, IP Spoof, etc.; supports Anti-ARP Spoofing, Anti-ARP Flood attack; supports control of ARP learning mechanism; supports scanning protection based on TCP, UDP and ICMP; supports firewall self-scanning protection
	Virus Protection	Supports virus scanning for HTTP, HTTPS, FTP, POP3, SMTP, and IMAP protocols, automatic updating of virus databases, virtual unpacking, customized scanning file size, suspicious virus scanning, suspicious scripts, picture viruses, and viruses

		contained in email text, attachments, web pages and downloaded files; supports the scanning and killing of more than 2 million viruses, the virus database is updated regularly and timely, and supports custom virus signatures based on MD5
	Intrusion Prevention	Supports multiple detection technologies such as pattern matching, anomaly detection, statistical analysis, and anti-IDS/IPS escape, and supports online and bypass deployment; supports 8000+ release library event sets, supports 11000+ detection libraries, compatible with CVE/CNCVE, and supports events Set customization, support manual, automatic or regular upgrades; support IPS custom rules; can analyze HTTP, SMTP, POP3, FTP, Telnet, VLAN, MPLS, ARP, GRE and other protocols; support SQL injection detection, Trojan backdoor attack protection, security vulnerability attack protection, denial of service attack protection, weak password detection and other suspicious behavior protection, worm virus protection, network database attacks, CGI access, CGI attacks, IPS advanced alarms, etc.
Visual Intelligent Management	Device Management	Supports WEB (HTTP/HTTPS), SSH, TELNET, and Console for management configuration, supports host name and device DNS settings, and supports custom HTTP/HTTPS management ports
	Administrative Permissions	Supports administrator authority division, supports predefined configuration, auditing, security administrators, separation of three powers, and supports administrator settings and grouping
	Diagnostic Tools	Supports network debugging and diagnostic commands in web graphics mode, and can conduct traffic debugging based on protocols, IPv4/v6, source and destination addresses, etc.; supports export of diagnostic information/exception information; supports ping\trace\token tool; The port mirroring supports inbound traffic mirroring, outbound traffic mirroring, and bidirectional traffic mirroring. The mirroring policy supports traffic mirroring policies based on port, source/destination IP, service, user, application, and time priority. It provides network capabilities such as VLAN stripping and MAC modification for third-party devices to perform data analysis or forwarding.
	Policy Analysis	Supports policy analysis, supports detection of redundant policies, hidden policies, conflicting policies, mergeable policies, empty policies, and expired policies, and provides optimization suggestions
	Log Output	Supports log policy setting, supports local storage and outgoing of logs, supports system logs, flow logs, security logs and audit logs. All logs support query, export and clearing; supports interface, HA, routing and health check logs and other system operation log; supports all application names and behavior logs, logs are stored locally, hard disk, and out-sending; supports local export to excel, txt, and xml formats;
	Statistical Analysis	Supports real-time traffic statistics and analysis functions, supports TOP10 application traffic ranking, supports traffic trend display, supports TOP50 application traffic data analysis, supports TOP50 user traffic statistics; supports traffic report export;
	Monitoring and Analysis	Support online user monitoring and management, support system information alarms, such as CPU, memory, hard disk occupancy, etc., support outgoing alarm logs, syslog, email, etc.;

Order Information

Model	Description
MPSec IFW400-F4-AC	
MPSec IFW400-F4-AC	V1 Version: MPSec IFW400-F4-AC, next-generation firewall host, configured with 5*Gigabit RJ45 Interfaces, 1*GE Combo Interfaces, One power adaptor, 1U Height.
License	
IFW400-F4-IAA-1Y	V1 Version: IFW400-F4-IAA-1Y, Software library 1-year upgrade license, such as application identification library, URL classification feature library, virus protection feature library, intrusion prevention library.
IFW400-F4-IAA-3Y	V1 Version: IFW400-F4-IAA-3Y, Software library 3-year upgrade license, such as application identification library, URL classification feature library, virus protection feature library, intrusion prevention library.
MPSec IFW400-F5-AC	
MPSec IFW400-F5-AC	V2 Version: MPSec IFW400-F5-AC, next-generation firewall host, configured with 8*Gigabit RJ45 Interfaces, 2*GE SFP Interfaces, One AC power supply, 1U Height.
License	
IFW400-F5-IAA-1Y	V2 Version: IFW400-F5-IAA-1Y, Software library 1-year upgrade license, such as application identification library, URL classification feature library, virus protection feature library, intrusion prevention library.
IFW400-F5-IAA-3Y	V2 Version: IFW400-F5-IAA-3Y, Software library 3-year upgrade license, such as application identification library, URL classification feature library, virus protection feature library, intrusion prevention library.

Maipu Communication Technology Co., Ltd
No.16, Jiuxing avenue
Hi-Tech Zone
Chengdu, Sichuan Province
P. R. China
610041
Tel: (86) 28-65544850,
Fax: (86) 28-65544948,
URL : http://www.maipu.com
Email: overseas@maipu.com

FACEBOOK

LINKEDIN