Maipu MPSec MSG4000-G2 NG Firewall Datasheet

Overview

MPSec MSG4000-G2 is a high-performance next-generation firewall (NGFW), 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 MSG4000-G2

MPSec MSG4000-G2 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 MSG4000-G2 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.

MPSec MSG4000-G2 provides comprehensive application security protection and flexible expansion methods. It can be deployed in various industries such as government, finance, enterprise, and education. It is widely used in Internet egress, intranet area boundaries, data centers, server area security isolation, VPN networking, and other application scenarios.

Key Features

- **Independent and controllable hardware platform**

The hardware platform of MPSec MSG4000 adopts Maipu's self-controllable hardware, integrates Maipu's independent design and manufacture, and shares Maipu's router hardware manufacturing process for more than 20 years. It can get good value guarantee in terms of product reliability and life cycle continuation.

- Stable and reliable hardware platform: Sharing Maipu's decades of router hardware manufacturing process of Maipu, which has been in the market for tens of years, and the long-term verification of hundreds of thousands units ensures the stable and reliable operation of MPSec MSG4000.
- Controllable product life cycle: MPSec MSG4000 adopts Maipu's own ARM hardware architecture instead of the X86 industrial computer platform of traditional security manufacturers, and can better control the product life cycle.

- **Refined application access control**

MPSec MSG4000 supports in-depth application identification technology, which can accurately identify thousands of network applications, including hundreds of mobile terminal applications, based on protocol features, behavior features, and correlation analysis. On this basis, MPSec MSG4000 provides users with fine and flexible application security access control.

- Integrated access control: conduct integrated control and defense from users, applications, content, time, threats, and locations. The defense of the content layer is deeply combined with application identification, and it is processed in an integrated manner. For example: Oracle traffic is identified, and then corresponding intrusion prevention is carried out in a targeted manner, with higher efficiency and fewer false positives.
- Accurate application identification: Provides a refined application identification mechanism. Users can accurately filter out the types of applications they are interested in based on application names, application categories, risk levels, technologies used, application characteristics, etc., such as communication software with file transfer functions, or browser-based WEB video applications with known vulnerabilities, etc. etc., so as to realize refined application management and control.
- Flexible application control: Based on in-depth application identification and refined application screening, it supports flexible security control functions, including policy blocking, session restriction, traffic control, application diversion or time limit, etc.

- **Comprehensive security defense capability**

MPSec MSG4000 provides intrusion prevention technology based on in-depth application identification, protocol detection and attack principal analysis, which can effectively filter security threats such as viruses, Trojan horses, worms, spyware, vulnerability attacks, escape attacks, etc., and provide users with L2-L7 layer network security protection.

- Optimized attack identification algorithm. It can effectively resist denial-of-service attacks such as SYN Flood, UDP Flood, HTTP Flood, etc., and ensure the security and availability of the network and application system.
- Professional web attack protection function: Supports detection and filtering of SQL injection, cross-site scripting, CC attacks, etc., to protect web application servers from attack damage.
- High-performance virus filtering function: The leading detection engine based on flow scanning technology can realize low-latency high-performance filtering. Support for virus scanning in HTTP, FTP, SMTP, POP3, IMAP and other traffic and compressed files (zip, gzip, rar, etc.).
- Supports the URL filtering function of tens of millions of URL signature databases, which can help network administrators easily implement web browsing access control and avoid threat penetration caused by malicious URLs.

Technical Specifications

Hardware Specification

Specification/Models		MPSec MSG4000-G2
Hardware	Hardware Version	V4
	CPU	4-Core 2.0GHZ
	Memory	8GB
	Flash	8GB
	Storage Extension Slot	1
Interface	Default 1000M Interfaces	8*GET+2*GEF
	Default 10G Interfaces	2*10G SFP+
	Expansion Slots	2
	Console Port	1
	USB Port	2
	Default Bypass Port(Pair)	2*GET
Performance	L2&L3 Firewall Throughput	8Gbps
	Max. Concurrent (Million)	3M
	New Connection/Second	80K
	Recommend Users	1K
	Max. IPSec Tunnels	1500
	Max. IPSec Throughput	1Gbps
	Max. IPS Throughput	2Gbps
	Max. AV Throughput	3Gbps
	Max. NAT Policy	4K
Power Supply	Power Supply	Dual Fixed AC
	Power Input	100-240V/50-60HZ
	Power Consumption	≤75W
Dimension	W*D*H(mm)	440*330*44mm
Environment	Working Temperature	0-45℃
	Work environment humidity	5%-90%, no-condensing
	Storage environment temperature	-25-70℃
	Storage environment humidity	5%-90%, no-condensing

Software Function

Basic networking capabilities	Deployment mode	Support routing, transparent, switching, hybrid, bypass multi-mode deployment
	Routing features	Default routing, static routing, policy routing, support RIP, RIPng, OSPF, BGP and other dynamic routing
	IP protocol	Support IPv4, IPv6 dual-stack
	NAT	Support more than four conversion methods for source/destination address and port
	Load balancing	Support multi-link load balancing, support DNS traffic load balancing, support server IP-based load balancing; support IPSec VPN multi-link backup and load
	Network service	Support DHCP server, DNS transparent proxy, ARP proxy
	VPN	IPSec VPN, L2TP VPN, PPTP VPN, GRE VPN
	Virtual system	Support full isolation of virtual system routing, switching, monitoring, auditing, protection, etc.
	High reliability	Support dual-system hot backup function, support "master-standby" and "master-master" mode under routing and transparent mode, support interface linkage, link detection.
Refined access control	Access control	Supports access control based on security domains, VLANs, geographical regions, applications, etc., and one security policy can be configured with advanced access control functions including more than six security policies, realizing fast researching and analysis for security policies
	Application identification	It can identify 6000+ Internet applications and 900+ mobile applications.
	Behavior management and control	Precisely control the abnormal behavior of SMTP, POP3, IMAP, FTP, TELNET, HTTP and other protocols
	User authentication	Support web authentication, third-party authentication linked with AD active directory, LDAP, RADIUS
	File filtering	Filter more than 30 commonly used document types in the three categories of document, compression and archiving
	Mail filtering	Supports filtering of e-mail senders and recipients, and supports anti-spam function
	URL filtering	Preset rich URL resource library, support offline/online update, support custom URL filtering policy
	Content filtering	Realize bidirectional content transmission filtering of five application protocols including HTTP, FTP, POP3, SMTP, and IMAP, and support predefined and customized sensitive information databases
	Bandwidth management	Support bandwidth management based on time, IP, user, service, application and other elements, support maximum bandwidth limit and minimum bandwidth guarantee
Integrated threat protection	Attack protection	Supported attack protection types include: SYN Flood, ICMP Flood, UDP Flood, IP Flood, DNS Flood, HTTP Flood, SYN Cookie, IP scanning attack, port scanning, IP spoofing, DHCP monitoring auxiliary inspection, Ping of Death, Teardrop, IP option , TCP exception, Smurf, Fraggle, Land, Winnuke, DNS exception, IP fragmentation, etc.
	Virus protection	Support virus cloud detection and killing technology for virus detection and killing of SMTP, POP3, IMAP, HTTP, FTP traffic
	Intrusion prevention	It can identify and block 5000+ vulnerabilities and spyware, and support generating dynamic policy
Visual	Device management	Support device management through Http, Https, SSH, Console, CLI

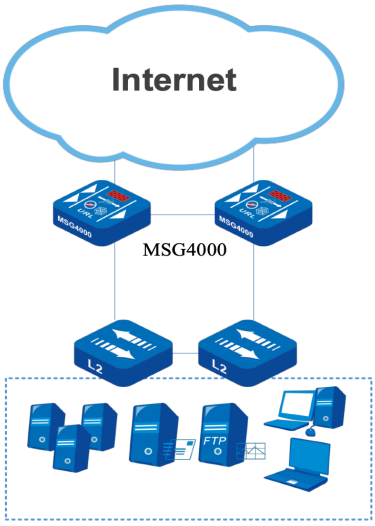
intelligent management	Management authority	Support separation of three powers, support custom administrators and authorities
	Network analysis	location, perform statistics and ranking through 5 dimensions of session, threat, content, URL, and byte count, displaying the current policy usage and network activity status, and locating abnormal behavior
	Threat analysis	The firewall presents advanced threat behaviors in the network based on hosts accessing malicious URLs and malicious domain names, combined with threat activity policies. In this way, it can be judged that there are compromised hosts in the intranet, or that the current security policy is not perfect
	Blocking analysis	Supports displaying blocking logs of users, applications, threats, content, URLs, etc. Administrators can judge malicious behaviors and potentially risky terminals in the network, and also judge whether normal behaviors have been blocked by mistake
	Log output	Support querying URL filtering logs, mail filtering logs, threat logs, domain name logs, behavior logs, and traffic logs, and support sending logs outside
	Statistics analysis	Supports the sorting of applications, IPs, users, etc. within a specified time range. Support historical statistics of new connections and concurrent connections. Support ranking statistics based on traffic in the network. Supports threat maps to help users understand the geographic location-based threat distribution in large networks.
	Monitoring analysis	Supports monitoring and analysis of system resources, users, assets, sessions, routes, etc.

Order Information

MPSec MSG4000-G2	Description
MPSec MSG4000-G2	MPSec MSG4000-G2 Firewall, 8*1000M Base-T, 2*1000M SFP, 2*10G SFP+ interfaces, 2*Expansion Slots, 2*1000M RJ45 bypass interfaces, Fixed Dual Power Supply. (Including 16 IPsec VPN Tunnels License by default)
MPSec-4GET	4-Port 1000M Base-T interfaces Extension Module
MPSec-4GEF	4-Port 1000M SFP interfaces Extension Module
License	
MSG4000-G2-IAA-1Y	MSG4000-G2-IAA-1Y License upgrading service for one year, including application identification, URL identification, AV prevention, IPS prevention library
MSG4000-IPSecVPN-50	50 IPSec VPN Tunnel License
MSG4000-IPSecVPN-200	200 IPSec VPN Tunnel License
MSG4000-IPSecVPN-1000	1000 IPSec VPN Tunnel License
Hard Disk	
MPSec-HD-1T	MPSec-HD-1T, 1TB HDD Module
MPSec-HD-4T	MPSec-HD-4T, 4TB HDD Module
MPSec-SSD-512	MPSec-SSD-512, 512GB SSD Module

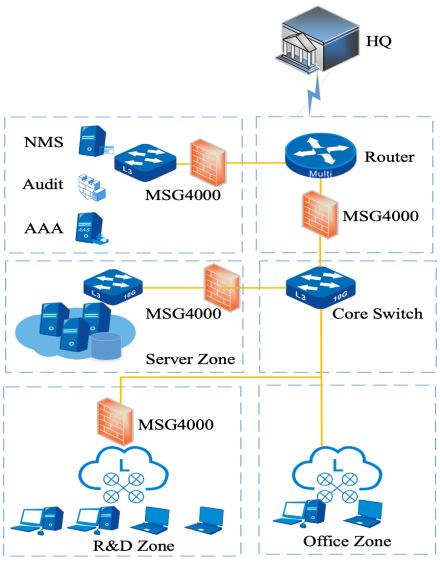
Application Scenario

Application One： Internet Access



- Realize multi-exit intelligent route selection function through ISP policy routing, equal-cost routing, link detection, etc.
- Realize defense against external viruses, attacks, and malicious sites through IPS, AV, and URL filtering in the integrated engine.
- Realize user network access management through the application layer access control, bandwidth management, URL filtering, content filtering and other policies.

Application Two： Department isolation



- Divide the entire network into different levels of security domains according to business characteristics, so that the network structure is reasonable and the boundaries are clear;
- Deploy next-generation firewalls between security domains, and improve access control measures to achieve logical isolation of regional borders.
- Enable functions such as IPS, AV, vulnerability protection, and URL filtering to prevent viruses, Trojans, and worms from spreading across regions in the network.

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