# Maipu MPSec MSG4000-X1 Series Firewall Datasheet

## Overview

MPSec MSG4000-X1 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-X1

MPSec MSG4000-X1 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-X1 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-X1 is deeply integrated with vulnerability scanning capabilities, which can proactively security weaknesses in network assets, thereby transforming passive defense into proactive risk management.

MPSec MSG4000-X1 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-X1 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 of units ensures the stable and reliable operation of MPSec MSG4000-X1.
- Controllable product life cycle: MPSec MSG4000-X1 adopts 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-X1 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-X1 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-X1 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 (WAF): 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-X1 |
|---|---|---|
| **Hardware** | Hardware Version | V5 |
| | CPU | 4-Core (ARM) |
| | Memory | 16GB |
| | Flash | 16GB |
| | HDD Extension Slot | 1 |
| **Interface** | Default 1000M Base-T Interfaces | 16*GET |
| | Default 1000M SFP Interfaces | 4*GEF |
| | Default 10G Interfaces | 4*10G SFP+ |
| | Expansion Slots | 2 |
| | Console Port | 1 |
| | USB Port | 2 |
| | Default Bypass Port (Pair) | N/A |
| **Performance** | L2&L3 Firewall Throughput | 20Gbps |
| | Max. Concurrent (Million) | 10M |
| | New Connection/Second | 130K |
| | HTTP New Connection Per Second | 130K |
| | Max. L7 Throughput | 12Gbps |
| | Recommend Users | 1-3K |
| | Max. IPS Throughput | 2.6Gbps |
| | Max. AV Throughput | 4.3Gbps |
| | Max. NAT Policy | 4K |
| | Virtual Firewall | 8 |
| **VPN** | Max. IPSec Throughput | 5.5Gbps |
| | Max. IPSec Tunnels | 3000 |
| | IKEv2 | Yes |
| **Power Supply** | Power Supply | Dual Power Slots |
| | Power Input | 100-240V/50-60HZ |
| | Power Consumption | ≤120W |
| **Dimension** | W*D*H(mm) | 426*330*88mm |
| **Environment** | Working Temperature | 0-45℃ |
| | Working Humidity | 5%-90%, no-condensing |
| | Storage Temperature | -25-70℃ |

| | | |
|---|---|---|
| | Storage Humidity | 5%-90%, no-condensing |

## Software Function

| | | |
|---|---|---|
| **Basic Networking Capabilities** | Deployment Mode | Support routing, transparent, switching, hybrid, bypass multi-mode deployment |
| | Network Protocol | Support VLAN, manual/dynamic LACP, Jumbo Frames, BFD, LLDP, VXLAN L2/L3 gateway, static VxLAN tunnel |
| | Routing Protocol | Support IPv4/v6 static routing, PBRv4/v6, RIPv1/v2, RIPng, OSPF v2/v3, ISIS, BGPv4/v6 and static/dynamic Multicast routing, PIM-SM, Route Policy |
| | IP Protocol | Support IPv4, IPv6 dual-stack |
| | NAT | Support SNAT, DNAT, NAT-PT, NAT46, NAT64, NAT66, NAT ALG, support SNAT and DNAT hit analysis, support monitoring of SNAT address pool utilization |
| | 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 balancing, support ISP routing load balancing |
| | Network Service | Support DHCPv4/v6 server/relay, static DNS, DNS64, DNS proxy server, DDNS, NTP |
| | IPSec VPN | Support IKEv1/v2, support multiple encryption algorithm, support local CA and PFS group, support reverse routing injection |
| | Other VPN | Support L2TP VPN, PPTP VPN, GRE VPN, GRE over IPSec VPN, L2TP over IPSec VPN, DS-Lite, 6in4 Tunnel |
| | Virtual System | Supports re-configuring performance resources of physical firewalls to generate multiple virtual firewalls. Support full isolation of virtual system routing, switching, monitoring, auditing, protection, etc. |
| | High Reliability | Support HA, support "master-standby" and "master-master" mode under routing and transparent mode, support long connection, interface linkage, link health detection. |
| **Refined Access Control** | Access Control | Support security policy based on security zone/geographical regions/users/applications/VLANs, etc., support configure more than 10 types of advanced security functions. Supports hit time analysis and security policy recommendation, support session limit based on address/app/time/user, etc. |
| | Application Identification | It can identify 6000+ Internet applications and 900+ mobile applications.<br><br>Support displays the traffic statistics of application in different time and risk. |
| | Behavior Management and Control | Precisely control the abnormal behavior of SMTP, POP3, IMAP, FTP, TELNET, HTTP, SIP, MGCP, SCCP and other protocols |
| | User Authentication | Support web authentication, local authentication, Two-factor authentication, third-party authentication linked with AD active directory, LDAP, RADIUS, TACACS+, Certificate Verification, POP3, support 802.1x, IP/MAC binding |
| | File Filtering | Filter more than 40 commonly used document types in the three categories of document, compression and archiving.<br><br>Supports upload, download, and bidirectional filtering of file transfer behaviors in sort of applications |
| | Mail Filtering | Supports filtering based on black/white list IPs, content keyword, RBL, email 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 various application protocols including HTTP, FTP, POP3, SMTP, IMAP, SMB, NFS and other protocol, and support predefined and customized sensitive information databases |

| | | |
|---|---|---|
| | DNS Filtering | Support filtering based on DNS, and support custom DNS category |
| | Bandwidth Management (QoS) | Support bandwidth management based on time, IP, user, service, application and DSCP, support maximum bandwidth limit and minimum bandwidth guarantee |
| | Shared Access Management | For private routers and illegal wireless hot-spots, the control function can be optimized by setting control addresses and exception addresses, while supporting blocking or alarm actions |
| **Integrated Attack Protection** | Attack Protection | Supported attack protection types include: SYN Flood, ICMP Flood, UDP Flood, IP Flood, DNS Flood, HTTP/HTTPS Flood, NTP Query 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, Christmas tree attack, 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, IMAP, IPTUX traffic |
| | Intrusion Prevention | It can identify and block 5000+ vulnerabilities and spyware, and support generating dynamic policy |
| | Cloud Linkage Protection | Support local and cloud threat intelligence linkage,<br>support virus cloud checking and killing, URL cloud recognition, cloud sandbox, application cloud recognition, emergency response, threat intelligence cloud detection and other functions |
| | SSL Decryption | Support decryption HTTPS, POP3S, SMTPS, IMAPS both of IPv4/v6;<br>Support self-learning of decryption certificates, support transparent deployment for SSL decryption, support decrypting TLS1.3, TLS1.2, TLS1.1, TLS1.0, and SSL3.0 protocols.<br>Support decryption flow mirroring, support SSL decryption logs output |
| | Honeypot Policy | Supports IPv4/v6 honeypot drainage strategies, support drainage based on multiple conditions, supports forced drainage, supports threat drainage |
| | Vulnerability Scanning | Support network vulnerability scanning, system vulnerability scanning, and IoT vulnerability scanning. Support define TCP/UDP port range, support web login checking |
| | WEB Attack Protection (WAF) | Support WEB attack protection types includes: XSS, Malicious scanning, SQL injection, WEB attack, Code execution, Command execution, direction traversal, File inclusion, Upload exploits, Webshell exploits, etc.<br>Support sample retention, feature library supports 2500+ web attack features.<br>Support WAF white list, CSRF protection, HTTP exception protection |
| | RA Control Strategy | Support RA control strategy to prevent RA attacks. Support based on source MAC, SSLA MAC, source address, VLAN, prefix, hop count and other conditions. Support M and O marks. |
| | Weak Password Detection | Support active and passive detection, support complete scanning based on network segment, protocol, username dictionary, and weak password dictionary. Support detection based on numbers, letters, numbers and letters, natural order, keyboard order, special characters, usernames, and duplicate characters. Support custom usernames and weak password dictionary objects |
| **Visual Intelligent Management** | Device Management & Maintenance | Support device management through HTTPS, SSH, Console, WEB CLI, RESTful API, SNMPv1/v2c/v3,<br><br>Support Netflow, TFTP/FTP, Capture packets, Ping, Tracer, Dual system backup |
| | Management Authority | Support separation of three powers, support custom administrators and authorities, support trusted host and MAC, support device administrator Ukey authentication |
| | 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 |

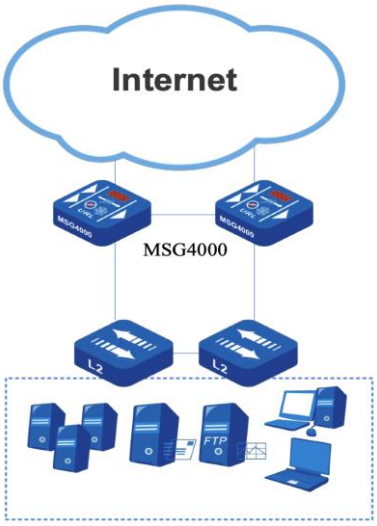
| | | |
|---|---|---|
| | | in the intranet, or that the current security policy is not perfect |
| | Blocking Analysis | Supports displaying blocking logs of users, applications, threats, content, URLs, etc. Administrators can judge malicious behaviors and potentially risky terminals in the network, and also judge whether normal behaviors have been blocked by mistake |
| | Log Output | Support querying URL filtering/mail filtering/threat/domain name/behavior/traffic/SSL proxy/content/NAT444/IM/Operation/system log, and support sending different types of logs to designated server separately. |
| | Alarm Notification | Support SNMP Trap, email, voice, SMS and other forms to notify administrators of alarm information |
| | Statistics Analysis | Supports the sorting of applications, IPs, users, etc. within a specified time range.<br>Support historical statistics of new connections and concurrent connections.<br>Support ranking statistics based on traffic in the network.<br>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, tunnels, service chain, assets, sessions, routes, etc. |

# Order Information

| MPSec MSG4000-X1 | Description |
|---|---|
| MPSec MSG4000-X1 | MPSec MSG4000-X1 Firewall, 16*1000M Base-T, 4*1000M SFP, 4*10G SFP+ interfaces, 2*Expansion Slots, Dual Power Slots. (Including 16 IPsec VPN Tunnels License by default) |
| AD75M-HS0N | 75W AC Power Supply Module |
| MPSec-4GET | 4-Port 1000M Base-T interfaces Extension Module |
| MPSec-4GEF | 4-Port 1000M SFP interfaces Extension Module |
| MPSec-4XGEF | 4-Port 10G SFP+ interfaces Extension Module |
| **License** | |
| MSG4000-X1-IAA-1Y | MSG4000-X1-IAA-1Y License upgrading service for one year, including application identification, URL identification, AV prevention, IPS prevention library |
| MSG4000-VAS-1Y | MSG4000-VAS-1Y, 1-year license for vulnerability scanning signature library upgrade |
| MSG4000-WAF-1Y | MSG4000-WAF-1Y, 1-year license for Web application protection signature library upgrade |
| MPSec-IPSecVPN-50 | 50 IPSec VPN Tunnel License |
| MPSec-IPSecVPN-200 | 200 IPSec VPN Tunnel License |
| MPSec-IPSecVPN-1000 | 1000 IPSec VPN Tunnel License |
| **Hard Disk** | |
| MPSec-HD-2T | MPSec-HD-2T, 2TB HDD Module |
| MPSec-HD-4T | MPSec-HD-4T, 4TB HDD Module |

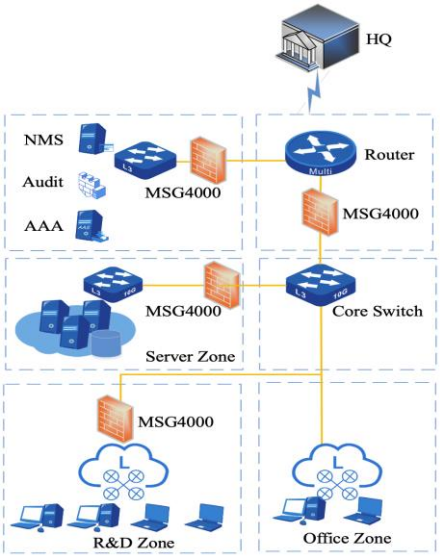
# Application Scenario

## 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*
Maipu Mansion, 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