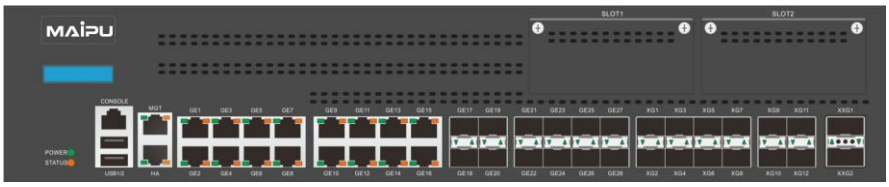
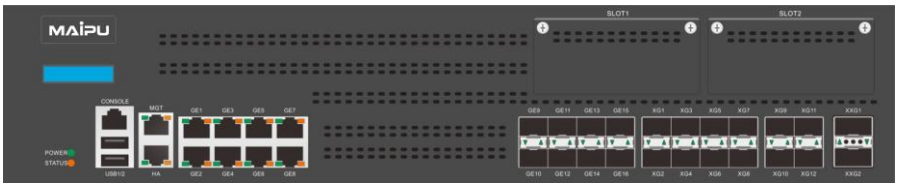
Maipu MPSec NSFW4000-X4/X8 Ultra Firewall Datasheet

Overview

MPSec NSFW4000-X4/X8 Ultra 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 NSFW4000-X4 Ultra



MPSec NSFW4000-X8 Ultra

MPSec NSFW4000-X4/X8 Ultra 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 NSFW4000-X4/X8 Ultra 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 NSFW4000-X4/X8 Ultra is deeply integrated with vulnerability scanning capabilities, which can proactively security weaknesses in network assets, thereby transforming passive defense into proactive risk management.

MPSec NSFW4000-X4/X8 Ultra 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 NSFW4000-X4/X8 Ultra 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 NSFW4000-X4/X8 Ultra.
- Controllable product life cycle: MPSec NSFW4000-X4/X8 Ultra adopts ARM hardware architecture which can better management and control the product life cycle.

- **Refined application access control**

MPSec NSFW4000-X4/X8 Ultra 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 NSFW4000-X4/X8 Ultra 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 NSFW4000-X4/X8 Ultra 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 NSFW4000-X4 Ultra	MPSec NSFW4000-X8 Ultra
Hardware	Version	V2	V2
	CPU	8-Core/2.5GHz (ARM)	8-Core/2.5GHz (ARM)
	Memory	16GB	
	Flash	16GB	
	HDD Extension Slot	1	
Interface	Default 1000M Base-T Interfaces	16*GET	8*GET
	Default 1000M SFP Interfaces	12*GEF	8*GEF
	Default 10G Interfaces	12*10G SFP+	
	Default 40/100G Interfaces	2*40/100G QSFP28	
	Port Expansion Slots	2	
	Console Port	1*RJ45 Port	
	Management Port	1*1000M RJ45 Port	
	HA Port	1*GET	
	USB Ports	2	
	Default Bypass Port (Pairs)	2	
Performance	L2&L3 Firewall Throughput	40Gbps	80Gbps
	Max. Concurrent (Million)	10,000,000+	
	New Connection /Second	750,000	
	HTTP New Connection /Second	750,000	
	Max. L7 Throughput (HTTP GET 21K)	28Gbps	
	Recommend Users	10,000+	20,000+
	Max. IPS Throughput	13Gbps	
	Max. AV Throughput	9Gbps	
	Max. WAF Throughput	12Gbps	
	Max. Security Throughput (all NGFW function enable)	9Gbps	
	Max. NAT Policy	4,000	
	Virtual Firewall	4	

VPN	Max. IPSec Throughput (1400Byte, GCM128+NULL)	16Gbps
	Max. IPSec Tunnels	5000
	IKEv2	Yes
Power Supply	Power Supply	Dual Power Slots
	Power Input	100-240V/50-60HZ
	Power Consumption	≤350W
Dimension	W*D*H(mm)	440*560*88mm(2U)
Environment	Working Temperature	0-45℃
	Working Humidity	5%-90%, no-condensing
	Storage Temperature	-25~70℃
	Storage Humidity	5%-95%, no-condensing

Software Function

Basic Networking Capabilities	Deployment Mode	Supports routing, transparent, switching, hybrid, bypass multi-mode deployment
	Network Protocol	Supports VLAN, manual/dynamic LACP, Jumbo Frames, BFD, LLDP, VXLAN L2/L3 gateway, support MAC, VNI, VTEP static binding
	Routing Protocol	Supports IPv4/v6 static routing, PBRv4/v6, RIPv1/v2, RIPng, OSPF v2/v3, ISIS, ISISv6, BGPv4/v6 and Multicast routing, PIM-SM
	IP Protocol	Supports IPv4, IPv6 dual-stack
	NAT	Supports SNAT, DNAT, NAT-PT, NAT46, NAT64, NAT66, NAT ALG, supports NAT Address Anti-Block Detection, supports SNAT and DNAT hit analysis, supports monitoring of SNAT address pool utilization
	Load Balancing	Supports multi-link load balancing, supports DNS traffic load balancing, supports server IP-based load balancing; supports IPSec VPN multi-link backup and load balancing, supports ISP routing load balancing, supports PBR load balancing, and intelligent route selection based on applications and services
	Network Service	Supports DHCPv4/v6 server/relay, static DNS, DNS64, DNS proxy server, DDNS, NTP
	IPSec VPN	Supports IKEv1/v2, supports multiple encryption algorithm: DES / 3DES / AES-128 / AES-256. Algorithm suites: AES-192, GCM-128, GCM-192, GCM-256, GMAC-128, GMAC-192, GMAC-256. Supports local CA, supports reverse routing injection, supports DH group16/17/18//20/21/24/27/28/29/30/31
	Other VPN	Supports 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. Supports full isolation of virtual system routing, switching, monitoring, auditing, protection, etc.
	High Reliability	Supports HA, supports "master-standby" and "master-master" mode under routing and transparent mode, supports long connection, interface linkage, link health detection, supports HA heartbeat escape
Refined Access Control	Access Control	Supports security policy based on 5-tuple/security zone/geographical region/user/application/tunnel/time/VLAN, etc., supports configure more than 10 types of advanced security functions. Supports hit time analysis and security policy recommendation, supports session limit based on address/app/time/user, etc. Supports batch operations for IP and domain blacklists
	Application Identification and Control	Application signature database: 11,000+ entries. Supports displaying the traffic statistics of application in different time and risk. Supports filtering of applications and web content; filter actions include block and log. Precisely control the abnormal behavior of SMTP, POP3, IMAP, FTP, TELNET, HTTP, SIP, MGCP, SCCP, H225-RAS, H225-931 and GDW3761 protocol
	User Authentication	Supports web authentication, local authentication, Two-factor authentication, third-party authentication linked with AD active directory, LDAP, RADIUS, TACACS+, Certificate Verification, POP3, supports 802.1x, SMS authentication
	File Filtering	Filters file transfers (upload/download/bidirectional) for IM, file sharing, forums, microblogs, webmail, etc. Content filtering supports 29+ file types (HTML, DOC, DOCX, XLS, XLSX, PPT, PPTX, etc.). File type identification is extension-independent.
	Mail Filtering	Supports filtering based on black/white list IPs, content keyword, RBL, email senders and recipients, and supports anti-spam function, email attachment size detection

	URL Filtering	Preset rich URL resource library, supports offline/online update, supports custom URL filtering policy, supports URL keyword filtering, supports pushing URL filter notifications/messages
	Content Filtering	Realize bidirectional content transmission filtering of various application protocols including HTTP, FTP, POP3, SMTP, IMAP, SMB, NFS and other protocol, and supports predefined and customized sensitive information databases
	DNS Filtering	Supports filtering based on DNS, supports DNS black/white list, and supports custom DNS category
	Bandwidth Management (QoS)	Supports bandwidth management based on time, IP, user, service, application and DSCP, supports 5-level bandwidth management, per-IP bandwidth quotas, dynamic allocation of remaining bandwidth by priority
	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	Supports security domain attacks: SYN Flood, ICMP Flood, UDP Flood, IP Flood, DNS Request/Reply Flood, HTTP/HTTPS Flood, NTP Query/ Reply Flood, SYN Cookie, IP scanning attack, port scanning, IP spoofing, DHCP monitoring auxiliary inspection, etc. Supports anti-DDos attacks: Ping of Death, Teardrop, IP option, TCP exception, Smurf, Fraggle, Land, Winnuke, Christmas tree attack, DNS exception, IP fragmentation, NTP monlist, etc. Supports protection against brute-force attacks on HTTP, SMTP, databases, FTP, SSH, and RDP.
	Virus Protection	Supports a local virus database of no fewer than 30 million signatures, virus detection and removal over HTTP, FTP, POP3, SMTP, IMAP, SMB, IPTUX, and NFS, and sample retention. Supports 16-level compressed file scanning/removal, virus sample upload, local retention, cloud scanning, and page message push.
	Intrusion Prevention	IPS signature database supports 3000+ signature, supports vulnerability protection and anti-spyware for DoH, FTP, HTTP, IMAP, OTHER_APP, POP3, SMTP, NFS, SMB, DNS, and DCERPC,etc. Vulnerability protection signature database queries: attack type, name, CVE ID, CNNVD ID, CWE ID, severity, platform, category, description, remediation suggestions, etc. Supports custom vulnerability signatures for HTTP, TCP, UDP, Telnet, SMB, FTP, IMAP, SMTP, and POP3.
	Cloud Linkage Protection	Supports local and cloud threat intelligence linkage, supports virus cloud checking and killing, URL cloud recognition, cloud sandbox, application cloud recognition, emergency response, threat intelligence cloud detection and other functions
	SSL Decryption	Supports decryption HTTPS, POP3S, SMTPS, IMAPS both of IPv4/v6; Supports self-learning of decryption certificates, supports transparent deployment for SSL decryption, supports decrypting TLS1.3, TLS1.2, TLS1.1, TLS1.0, and SSL3.0 protocols. Supports decryption flow mirroring, supports SSL decryption logs output
	Honeypot Policy	Supports IPv4/v6 honeypot drainage strategies, supports drainage based on multiple conditions, supports forced drainage, supports threat drainage
	Threat intelligence	Supports correlation between local and cloud threat intelligence. Local threat intelligence can be updated manually or automatically, and supports control, allow, block, and DNS sinkhole actions for DNS behavior.
	Vulnerability Scanning	Supports network vulnerability scanning, system vulnerability scanning, and IoT vulnerability scanning. Supports define TCP/UDP port range, supports web login checking
	WEB Attack Protection (WAF)	Supports 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. Supports sample retention, feature library supports 2500+ web attack features. Supports WAF white list, CSRF protection, HTTP exception protection
	RA Control Strategy	Supports RA control strategy to prevent RA attacks. Supports based on source MAC, SSLA MAC, source address, VLAN, prefix, hop count and other conditions. Supports M and O marks.
	Weak Password Detection	Supports active and passive detection, supports complete scanning based on network segment, protocol, username dictionary, and weak password dictionary. Supports detection based on numbers, letters, numbers and letters, natural order, keyboard order, special characters, usernames, and duplicate characters. Supports custom usernames and weak password dictionary objects
Visual Intelligent Management	Device Management & Maintenance	Supports device management through HTTPS, SSH, Console, WEB CLI, RESTful API, SNMPv1/v2c/v3, Supports Netflow, TFTP/FTP, SPAN, Capture packets, Ping, Tracer, Dual system backup
	Management Authority	Supports separation of three powers, supports custom administrators and authorities, supports trusted host and MAC, supports device administrator Ukey authentication, supports per-administrator enable/disable and password expiration
	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	Supports querying URL filtering/mail filtering/threat/domain/name/behavior/traffic/SSL proxy/content/NAT444/IM/Operation/system log, and supports sending different types of logs to designated server separately. Log export supports TLS encryption, and log storage space supports custom allocation
	Alarm Notification	Supports 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. Supports historical statistics of new connections and concurrent connections. Supports 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, tunnels, service chain, assets, sessions, routes, etc.

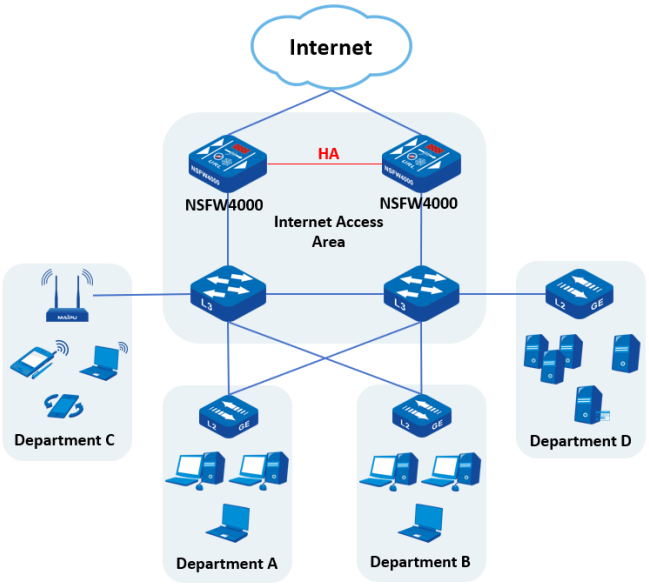
Order Information

MPSec NSFW4000-X4 Ultra	Description
MPSec NSFW4000-X4 Ultra	V2 Version: MPSec NSFW4000-X4 Ultra Firewall, 16*1000M Base-T (Including 2*Pairs 1000M RJ45 Bypass Ports), 12*1000M SFP, 12*10G SFP+ interfaces, 2*40/100G QSFP28 interfaces, 1*1000M RJ45 HA Interface, 1*1000M MGT RJ45 Interface, 2*Expansion Slots,

	1*HDD Disk Slot, Dual Power Slots (Standard with dual power supplies), 2U Height. (Including 100 IPsec VPN Tunnels License by default)
MPSec NSFW4000-X8 Ultra	V2 Version: MPSec NSFW4000-X8 Ultra Firewall, 8*1000M Base-T (Including 2*Pairs 1000M RJ45 Bypass Ports), 8*1000M SFP, 12*10G SFP+ interfaces, 2*40/100G QSFP28 interfaces, 1*1000M RJ45 HA Interface, 1*1000M MGT RJ45 Interface, 2*Expansion Slots, 1*HDD Disk Slot, Dual Power Slots (Standard with dual power supplies), 2U Height. (Including 100 IPsec VPN Tunnels License by default)
License	
MPSec NS-COMM-V	MPSec NS-COMM-V, License for the software system of MPSec NSFW series products
NSFW4000-X4-Ultra-IAA-1Y	NSFW4000-X4-Ultra-IAA-1Y, 1-year license for upgrading service, including application identification, URL identification, AV prevention, IPS prevention library
NSFW4000-X4-Ultra-VAS-1Y	NSFW4000-X4-Ultra-VAS-1Y, 1-year license for vulnerability scanning signature library upgrade
NSFW4000-X4-Ultra-WAF-1Y	NSFW4000-X4-Ultra-WAF-1Y, 1-year license for Web application protection signature library upgrade
NSFW4000-X8-Ultra-IAA-1Y	NSFW4000-X8-Ultra-IAA-1Y, 1-year license for upgrading service, including application identification, URL identification, AV prevention, IPS prevention library
NSFW4000-X8-Ultra-VAS-1Y	NSFW4000-X8-Ultra-VAS-1Y, 1-year license for vulnerability scanning signature library upgrade
NSFW4000-X8-Ultra-WAF-1Y	NSFW4000-X8-Ultra-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
Interface Module	
MPSec-2QFP	2-Port 100G QSFP28 interfaces Extension Module
MPSec-2QXGEF	2-Port 40G QSFP+ interfaces Extension Module
MPSec-4XGEF	4-Port 10G SFP+ interfaces Extension Module
MPSec-4GET4GEF	4-Port 1000M Base-T interfaces and 4-Port 1000M SFP interfaces Extension Module
Hard Disk	
MPSec-HD-1T	MPSec-HD-1T, 1TB HDD Module
MPSec-HD-4T	MPSec-HD-4T, 4TB HDD Module

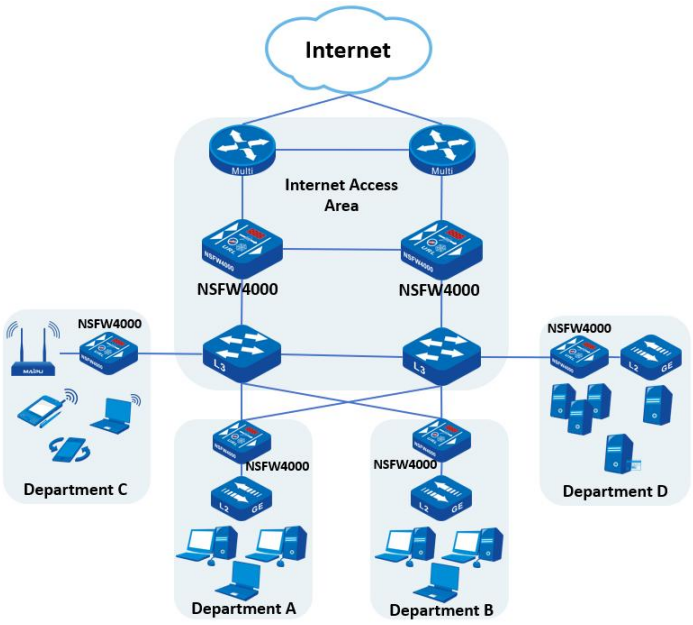
Application Scenario

Application One: Internet Access



- Provide intelligent multi-exit route selection through ISP policy-based routing, ECMP (Equal-Cost Multi-Path) routing, link detection, and other mechanisms.
- Deliver defense against external threats-including viruses, attacks, and malicious sites through the integrated security engine's IPS, AV, and URL filtering capabilities.
- Enforce user network access management through application-layer access control, bandwidth management, URL filtering, content filtering, and other policy-based controls.

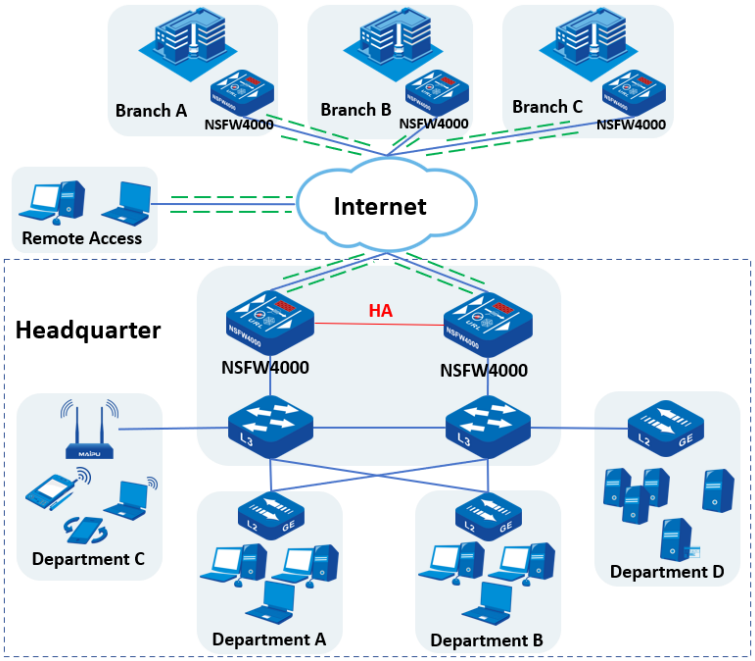
Application Two: Department Isolation



- Divide the entire network into hierarchical security domains based on business characteristics, to ensure a well-structured network with clearly defined boundaries.
- Deploy next-generation firewalls between security domains and enforce strict access control policies to achieve logical isolation at domain boundaries.

- Enable IPS, AV, vulnerability prevention, and URL filtering to prevent malware (including viruses, Trojans, and worms) from spreading across security domains.

Application Three: Multi-Branch VPN Access



- Deploy the NSFW4000 firewall at the network egress, establish VPN tunnels between branches and the headquarters to enable link redundancy and load sharing, and enforce perimeter security isolation along with protection against external Internet threats and attacks.
- Perform in-depth threat detection on all network traffic, and leverage local threat intelligence to conduct thorough analysis of suspicious behaviors. This enables the blocking of virus propagation and vulnerability exploits, while also providing real-time alerting and blocking of highly concealed threats.
- Integrate with the cloud-based sandbox to enable dual-layer antivirus scanning at both the gateway and the local endpoint, as well as access control based on endpoint risk levels.

All rights reserved. Printed in the People's Republic of China.

No part of this document may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise without the prior written consent of Maipu Communication Technology Co., Ltd.

Maipu makes no representations or warranties with respect to this document contents and specifically disclaims any implied warranties of merchantability or fitness for any specific purpose. Further, Maipu reserves the right to revise this document and to make changes from time to time in its content without being obligated to notify any person of such revisions or changes.

Maipu values and appreciates comments you may have concerning our products or this document. Please address comments to:

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

All other products or services mentioned herein may be registered trademarks, trademarks, or service marks of their respective manufacturers, companies, or organizations.