Data sheet

HP 10500/11900/7500 20Gbps VPN Firewall Module

Key features

- High-performance, 20 Gbps IMIX firewall throughput
- 4x10G ports
- 256 maximum virtual firewalls
- 1024 security zones
- 300k connections/second; 4 million concurrent sessions
- 51,200 security policies

Product overview

The HP 10500/11900/7500 20Gbps VPN Firewall Module is a high-performance, integrated network security that can deliver more than 20 Gbps of throughput. The scalable stateful firewalls can be aggregated in a single switch chassis (up to 16 modules), delivering up to 400 Gbps firewall throughput.

The firewalls unify the administration of the network and firewall, enabling customers to have simplified management, and learn once for administrating the network and firewall security. These advanced features provide high return on investment as you would be taking advantage of the existing switches for the blades.

The firewall modules have the following features:

- Integrated security functions, including firewall, virtual private network (VPN), network address translation (NAT), URL filtering, and application layer filtering
- Application Specific Packet Filter (ASPF) to detect application layer connection state in real time, implementing security protection from Layer 3 through Layer 7
- Operation logs, attack logs, stream logs, and network management and monitoring functions
- Plug-and-play with great scalability, allowing for insertion of one or more firewall modules into the network device

Features and benefits

Firewall

- **High performance:** 20 Gbps throughput helps secure traffic without compromising network performance. Support for four million concurrent connections and 150,000 new connections per second enables high-volume networks to remain secure under peak traffic.
- **ASPF:** Dynamically determines whether to forward or drop a packet by checking its application layer protocol information (such as FTP, HTTP, Simple Mail Transfer Protocol [SMTP], Real Time Streaming Protocol [RTSP], and other application layer protocols based on Transition Control Protocol [TCP] or User Datagram Protocol [UDP]) and monitoring the connection-based application layer protocol status.
- **Virtualization:** Multi-core architecture enables both multiple zones and multiple separate firewall instances to be created on the same device. Support for 1024 security zones, 256 virtual firewalls, and 4,094 virtual LANs (VLANs) offers robust protection to all corners of your network. Centralized deployment of a single device offering multiple virtual firewalls lowers total cost of ownership through streamlined training, simplified deployment and management, and reduced power consumption.
- **Zone-based access policies:** Groups VLANs logically into zones that share common security policies; allows both unicast and multicast policy settings by zones instead of by individual VLANs.
- **Application-level gateway (ALG):** Discovers the IP address and service port information embedded in the application data using deep packet inspection in the firewall; the firewall then dynamically opens appropriate connections for specific applications.
- **NAT:** Full support of NAT applications including many-to-one, many-to-many, static NAT, dual translation, easy IP, and DNS mapping. It supports NAT traversal with multiple protocols, and delivers NAT ALG functions such as DNS, FTP, H.323, and NetBIOS over TCP/IP (NBT).

Virtual private network

- **Internet Protocol Security (IPSec):** Provides secure tunneling over an untrusted network such as the Internet or a wireless network; offers data confidentiality, authenticity, and integrity between two network endpoints.
- **Layer 2 Tunneling Protocol (L2TP):** An industry standard-based traffic encapsulation mechanism supported by many common operating systems such as Windows® XP and Windows Vista®; can tunnel the Point-to-Point Protocol (PPP) traffic over the IP and non-IP networks; may use the IP/UDP transport mechanism in IP networks.
- **Generic Routing Encapsulation (GRE):** Transports Layer 2 connectivity over a Layer 3 path in a secured way; enables the segregation of traffic from site to site.
- **Manual or automatic Internet Key Exchange (IKE):** Provides either manual or automatic key exchange required for the algorithms used in encryption or authentication; auto-IKE allows automated management of the public key exchange, providing the highest levels of encryption.

Management

- **Secure Web GUI:** Provides a secure, easy-to-use graphical interface for configuring the module via HTTPS.
- **Command-line interface (CLI):** Provides a secure, easy-to-use CLI for configuring the module via secure shell (SSH) or a switch console; provides direct real-time session visibility.
- **SNMPv1, v2c, and v3:** Facilitate centralized discovery, monitoring, and secure management of networking devices.
- **Complete session logging:** Provides detailed information for problem identification and resolution.
- **Manager and operator privilege levels:** Provides read-only (operator) and read/write (manager) access on CLI and Web browser management interfaces.

- **Remote Network Monitoring (RMON):** Uses standard SNMP to monitor essential network functions; supports events, alarm, history, and statistics group plus a private alarm extension group.
- **FTP, TFTP, and SFTP support:** Offers different mechanisms for configuration updates; FTP allows bidirectional transfers over a TCP/IP network; trivial FTP (TFTP) is a simpler method using UDP; secure File Transfer Protocol (SFTP) runs over an SSH tunnel to provide additional security.

Layer 3 routing

- **Static IP routing:** Provides manually configured routing; includes equal-cost multi-path routing (ECMP) capability.
- **Routing Information Protocol (RIP):** Provides RIPv1 and RIPv2 routing.
- **Open shortest path first (OSPF):** Includes host-based ECMP to provide link redundancy or scalable bandwidth and not so stubby area (NSSA).
- **Border Gateway Protocol 4 (BGP-4):** Delivers an implementation of the Exterior Gateway Protocol (EGP) utilizing path vectors; uses TCP for enhanced reliability for the route discovery process; reduces bandwidth consumption by advertising only incremental updates; supports extensive policies for increased flexibility; scales to very large networks.
- **Dual IP stack:** Maintains separate stacks for IPv4 and IPv6 to ease the transition from an IPv4-only network to an IPv6-only network design.
- **Policy routing:** Allows custom filters for increased performance and security; supports access control lists (ACLs), IP prefix, autonomous system (AS) paths, community lists, and aggregate policies.
- **Layer 3 IPv6 routing:** Provides routing of IPv6 at media speed; supports static routes, RIPng, OSPFv3, BGP+, policy route, and Protocol Independent Multicast-Sparse Mode or Dense Mode (PIM-SM/DM).

Security

- **Defense against attacks:** Firewall provides defense against various attacks, such as denial-of-service (DoS) or distributed denial-of-service (DDoS), Address Resolution Protocol (ARP) spoofing, large Internet Control Message Protocol (ICMP) packet, address or port scanning, Tracert, IP packets with the Record Route option, and static and dynamic blacklists. It also supports binding of medium access control (MAC) address and IP address, and supports intelligent defense of worm viruses.
- **Application layer content filtering:** Firewall supports mail filtering, based on SMTP mail address, titles, attachments, and contents; supports webpage filtering including HTTP URL and content filtering.
- **Multiple security authentication services:** Firewall supports Remote Authentication Dial-In User Service protocol (RADIUS) and HW Terminal Access Controller Access Control System (HWTACACS) authentications, supports certificate-based (X.509 format) public key infrastructure (PKI)/certification authority (CA) authentication, supports user identity management (different users own different rights to execute commands), and supports levels of user views (users of different levels have different management rights).
- **Centralized management and auditing:** Firewall provides logging, traffic statistics and analysis, events monitoring and statistics, and mail notification of alarms.

Warranty and support

- **Electronic and telephone support:** Limited electronic and business-hours telephone support is available from HP for the entire warranty period. To reach our support centers, refer to hp.com/networking/contact-support. For details on the duration of support provided with your product purchase, refer to hp.com/networking/warrantysummary.
- **Software releases:** To find software for your product, refer to hp.com/networking/support. For details on the software releases available with your product purchase, refer to hp.com/networking/warrantysummary.
- **1-year warranty:** Advance hardware replacement with 10-calendar-day delivery (available in most countries).

Technical specifications

HP 10500/11900/7500 20Gbps VPN Firewall Module (JG372A)

Dimensions (H x W x D)	40.1 x 399.2 x 498.8 mm (1.58 x 15.72 x 19.64 in.)
Ports	4 10G ports 1 RJ-45 serial Console port 1 Compact Flash port
Environment	
Operating temperature	0°C to 45°C (32°F to 113°F)
Operating relative humidity	10% to 95%, noncondensing
Management	Intelligent Management Center (IMC), CLI, Web browser, SNMP manager, Telnet, HTTPS, RMON1, FTP
Features	
Performance	• 20 Gbps firewall throughput • 4 million concurrent connections • 300,000 new connections per second • Maximum 51,200 security policies • 4 Gbps Triple Data Encryption Standard (3DES) and Advanced Encryption Standard (AES) VPN throughput • 8,000 IPSec tunnels • 4,000 VLANs
Firewall operation mode	• Routing mode • Transparent mode • Hybrid mode
Access approval authority (AAA) service	• Local authentication • Standard RADIUS • HWTACACS+ • RADIUS domain authentication
ASPF	• General TCP/UDP application • FTP/SMTP/HTTP/RTSP/H.323 Protocol State Detection • SIP/MGCP/QQ/MSN Protocol State Detection • Java/ActiveX blocking and detection • Port mapping • Support for the fragmented packets
Virtualization	• 256 virtual firewalls • 4 default security zones • Maximum 256 security zones

Technical specifications (continued)

NAT	• Network Address and Port Translation (NAPT) • Port Address Translation (PAT) • NAT server • Port mapping • Bidirectional NAT • Static NAT
Network security	• Add blacklist by hand or automatically • IP/MAC binding • ARP Reverse Query • ARP Cheat Check • Management ports closed by default
DDOS	• DNS query flood • SYN flood • Auto starts TCP proxy when detects SYN flood • ICMP flood • UDP flood • IP spoofing • SQL injection filter
L2TP VPN	• L2TP Network Server (LNS) • L2TP Access Concentrator (LAC) • L2TP multi-instance GRE • GRE tunneling protocol
IPSec	• Authentication Header (AH)/Encapsulating Security Payload (ESP) • Transport/tunnel • NAT traversal • Strategy template
IKE	• Preshare key authentication method • Support aggressive mode and main exchange mode • IKE Dead Peer Detection (DPD), PKI/CA
Network feature	• IEEE 802.1Q VLAN • 4,000 subinterfaces • Static and dynamic ARP • Multicast, PIM • Internet Group Multicast Protocol (IGMP) v1/v2/v3
Routing	• RIP • OSPF • BGP • Static route • Policy route
High availability	• Active-active mode • Active-passive mode • Session synchronization for firewall

Technical specifications (continued)

System management	• Web management support for Internet Explorer/Firefox • CLI (Console/Telnet/SSH) • Classification manager • Unified management through IMC • SNMPv1/v2c/v3
Administration	• Software upgrades • Configuration backup and restore
Logging/Monitoring	• Syslog • Mini RMON network time protocol (NTP) • NAT/ASPF/firewall log stream (binary log)
IPv6 routing and multicast	• RIPng • OSPFv3 • BGP4+ • Static route • Policy route • PIM-SM/DM
IPv6 security	• Network Address Translation-Protocol Translation (NAT-PT) • Manual tunnel • IPv6 over IPv4 GRE tunnel • 6 to 4 tunnel (RFC 3056) • Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) tunnel • IPv6 packet filter • RADIUS • NAT64
Services	• 3-year, parts only, global next-day advance exchange (UZ896E) • 3-year, 4-hour onsite, 13x5 coverage for hardware (UZ897E) • 3-year, 4-hour onsite, 24x7 coverage for hardware (UZ900E) • 3-year, 4-hour onsite, 24x7 coverage for hardware, 24x7 software phone support and software updates (UZ904E) • 3-year, 24x7 software phone support, software updates (UZ907E) • 1-year, post-warranty, 4-hour onsite, 13x5 coverage for hardware (HR735E) • 1-year, post-warranty, 4-hour onsite, 24x7 coverage for hardware (HR736E) • 1-year, post-warranty, 4-hour onsite, 24x7 coverage for hardware, 24x7 software phone support (HR737E) • 4-year, 4-hour onsite, 13x5 coverage for hardware (UZ898E) • 4-year, 4-hour onsite, 24x7 coverage for hardware (UZ901E) • 4-year, 4-hour onsite, 24x7 coverage for hardware, 24x7 software phone (UZ905E) • 4-year, 24x7 software phone support, software updates (UZ908E) • 5-year, 4-hour onsite, 13x5 coverage for hardware (UZ899E) • 5-year, 4-hour onsite, 24x7 coverage for hardware (UZ902E) • 5-year, 4-hour onsite, 24x7 coverage for hardware, 24x7 software phone (UZ906E) • 5-year, 24x7 software phone support, software updates (UZ909E) • 3-year, 6-hour Call-to-Repair Onsite (UZ910E) • 4-year, 6-hour Call-to-Repair Onsite (UZ911E) • 5-year, 6-hour Call-to-Repair Onsite (UZ912E) • 1-year, 6-hour Call-to-Repair Onsite for hardware (HR739E) • 1-year, 24x7 software phone support, software updates (HR738E) Refer to the HP website at hp.com/networking/services for details on the service-level descriptions and product numbers. For details about services and response times in your area, please contact your local HP sales office.

Standards and protocols

(applies to all products in series)

IPv6	RFC 1981 IPv6 Path maximum transmission unit (MTU) Discovery RFC 2460 IPv6 Specification	RFC 2465 Management Information Base (MIB) for IP version 6: Textual Conventions and General Group (partial support, only "IPv6 Interface Statistics table") RFC 3484 Default Address Selection for IPv6 RFC 3513 IPv6 Addressing Architecture	RFC 3587 IPv6 Global Unicast Address Format RFC 4007 IPv6 Scoped Address Architecture RFC 4862 IPv6 Stateless Address Auto-configuration
Security	IEEE 802.1X: Port-Based Network Access Control (2001) RFC 1321 The MD5 Message-Digest Algorithm RFC 1334 PPP Authentication Protocols (PAP) RFC 1994 PPP Challenge Handshake Authentication Protocol (CHAP)	RFC 2104 Keyed-Hashing for Message Authentication RFC 2138 RADIUS Authentication RFC 2618 RADIUS Authentication Client MIB RFC 2620 RADIUS Accounting Client MIB RFC 2716 PPP Extensible Authentication Protocol (EAP) Transport Layer Security (TLS) Authentication Protocol RFC 2865 RADIUS Authentication	RFC 2866 RADIUS Accounting RFC 2867 RADIUS Accounting Modifications for Tunnel Protocol Support RFC 2868 RADIUS Attributes for Tunnel Protocol Support RFC 2869 RADIUS Extensions draft-grant-tacacs-02 (TACACS)
VPN	RFC 1701 Generic Routing Encapsulation RFC 1702 Generic Routing Encapsulation over IPv4 networks RFC 1828 IP Authentication using Keyed MD5 RFC 1829 The ESP DES-Cipher-block chaining (CBC) Transform RFC 1853 IP in IP Tunneling RFC 2085 HMAC-MD5 IP Authentication with Replay Prevention RFC 2401 Security Architecture for the Internet Protocol	RFC 2402 IP Authentication Header RFC 2403 The Use of HMAC-MD5-96 within ESP and AH RFC 2404 The Use of HMAC-SHA-1-96 within ESP and AH RFC 2405 The ESP DES-CBC Cipher Algorithm With Explicit IV RFC 2406 IP Encapsulating Security Payload (ESP) RFC 2410 The NULL Encryption Algorithm and its use with IPSec RFC 2411 IP Security Document Roadmap RFC 2451 The ESP CBC-Mode Cipher Algorithms	RFC 2473 Generic Packet Tunneling in IPv6 Specification RFC 2529 Transmission of IPv6 over IPv4 Domains without Explicit Tunnels RFC 2661 Layer Two Tunneling Protocol RFC 2784 Generic Routing Encapsulation RFC 2868 RADIUS Attributes for Tunnel Protocol Support RFC 2893 Transition Mechanisms for IPv6 Hosts and Routers RFC 3602 The AES-CBC Cipher Algorithm and its use with IPSec
IKEv1	RFC 2407 The Internet IP Security Domain of Interpretation for Internet Security Association and Key Management Protocol (ISAKMP)	RFC 2408 Internet Security Association and Key Management Protocol RFC 2409 The Internet Key Exchange RFC 2412 The Oakley Key Determination Protocol	RFC 3526 More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange RFC 3706 A Traffic-Based Method of Detecting Dead Internet Key Exchange Peers
PKI	RFC 2510 Internet X.509 Public Key Infrastructure Certificate Management Protocols RFC 2511 Internet X.509 Certificate Request Message Format	RFC 3279 Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile RFC 3280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List Profile draft-nourse-scep-06: Public-Key Cryptography Standards (PKCS) #1	PKCS #10 PKCS #12 PKCS #7

Customize your IT lifecycle management, from acquisition of new IT, management of existing assets, and removal of unneeded equipment.
hp.com/go/hpfinancialservices

HP Factory Express

HP Factory Express provides customization and deployment services along with your storage and server purchases. You can customize hardware to your exact specifications in the factory—helping speed deployment. hp.com/go/factoryexpress

Customer Technical Training

Gain the skills you need with ExpertOne training and certification from HP. With HP training, you will accelerate your technology transition, improve operational performance, and get the best return on your HP investment. Our training is available when and where you need it, through flexible delivery options and a global training capability. hp.com/learn/networking

Learn more at
hp.com/networking

Sign up for updates
hp.com/go/getupdated

Share with colleagues

Rate this document

4AA4-9063ENW, October 2013