QuickSpecs

Overview

Models

HP 5820 VPN Firewall Module	JD255A

Key features

- Industry-Leading Performance, 6.5G FW throughput
- Comprehensive Security Protection
- Rich VPN Functions, IPSec/GRE/L2TP
- Advanced Virtual Firewall
- Low Running Cost

Product overview

Built on the latest state-of-art, multi-core CPU platform,this module enables advanced network protection at multi-Gigabit speeds. It combines built-in protection against denial of service (DoS) and hacking attacks with VPN support, zonal and virtual stateful packet inspection firewall, application bandwidth management, IP unicast/multicast routing, and e-mail attachment filtering. Running on the Comware®OS that powers all HP A Series enterprise switching and routing platforms also ensures a rich networking feature set that facilitates application integration and lowers an enterprise network's total cost of ownership.This module safeguards network from attacks and misuse, while at the same time delivering policy-based, multisite connectivity for mission-critical applications such as VoIP, video and collaboration tools. High-availability features ensure traffic flow even in the event of network or internal device error, or loss of power to the primary device.

Features and benefits

Firewall

- High Performance: 6.5 Gbps throughput secures traffic without compromising network performance.Support for 1.8 million concurrent connections and 50,000 new connections per second enables high-volume networks to remain secure under peak traffic
- Application Specific Packet Filter (ASPF): Dynamically determines whether to forward or drop a packet by checking its application layer protocol information (such as FTP, HTTP, SMTP, RTSP and other application layer protocols based on TCP/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 256 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: logically groups virtual LANs (VLANs) 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): deep packet inspection in the firewall discovers the IP address and service port information embedded in the application data; the firewall then dynamically opens appropriate connections for specific applications
- NAT: Fully 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 NBT

Virtual private network (VPN)

- IPsec: provides secure tunneling over an untrusted network such as the Internet or a wireless network; offers data confidentiality, authenticity, and integrity between two endpoints of the network

Overview

- 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®; will 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): can be used to transport 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 both 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

- Complete session logging: provides detailed information for problem identification and resolution
- Manager and operator privilege levels: enable read-only (operator) and read-write (manager) access on CLI and Web browser management interfaces
- 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 command-line interface for configuring the module via 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
- Remote 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: FTP allows bidirectional transfers over a TCP/IP network and is used for configuration updates; Trivial FTP is a simpler method using User Datagram Protocol (UDP)

Layer 3 routing

- Static IP routing: provides manually configured routing; includes ECMP capability
- Routing Information Protocol (RIP): provides RIPv1 and RIPv2 routing
- OSPF: includes host-based ECMP to provide link redundancy/scalable bandwidth and NSSA
- Border Gateway Protocol 4 (BGP-4): Exterior Gateway Protocol (EGP) with path vector protocol uses TCP for enhanced reliability for the route discovery process, reduces bandwidth consumption by advertising only incremental updates, and supports extensive policies for increased flexibility, as well as scales to very large networks
- Dual IP stack: maintains separate stacks for IPv4 and IPv6 to ease transition from an IPv4-only network to an IPv6-only network design
- Policy routing: allows custom filters for increased performance and security; supports ACLs, IP prefix, 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 PIM-SM/DM

Security

- Defense against attacks: A series Firewall provides defense against various attacks, such as DoS/DDoS, ARP spoofing, large ICMP packet, address/port scanning, Tracert, IP packets with the Record Route option, static and dynamic blacklists. It also supports binding of MAC address and IP address, and supports intelligent defense of worm viruses
- Application layer content filtering: A series Firewall supports mail filtering, based on SMTP mail address, titles, attachments, and contents; supports Web page filtering including HTTP URL and content filtering
- Multiple security authentication services: A series Firewall supports RADIUS and HWTACACS authentications, certificate-based (x.509 format) PKI/CA authentication, supports user identity management (different users own different rights to execute commands), supports levels of user views (users of different levels have different management rights)
- Centralized management and auditing: A Series Firewall provides logging, traffic statistics and analysis, events monitoring and statistics, and mail notification of alarms

Warranty and support

Overview

- **Electronic and telephone support**: limited electronic and telephone support is available from HP; refer to: www.hp.com/networking/warranty for details on the support provided and the period during which support is available
- **Software releases**: refer to: www.hp.com/networking/warranty for details on the software releases provided and the period during which software releases are available for your product(s)
- **1-year warranty**: with advance replacement and 10-calendar-day delivery (available in most countries)

HP 5820 VPN Firewall Module (JD255A)

Ports	2 RJ-45 auto-negotiating 10/100/1000 ports (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE TX, IEEE 802.3ab Type 1000BASE-T) 2 dual-personality ports; auto-sensing 10/100/1000Base-T or SFP 1 RJ-45 serial console port 1 Compact Flash port	
Physical characteristics	**Dimensions**	9.84(d) x 9.84(w) x 14.45(h) in. (25 x 25 x 36.7 cm)
	Weight	3.31 lb. (1.5 kg)
Environment	**Operating temperature**	32°F to 113°F (0°C to 45°C)
	Operating relative humidity	10% to 95%, noncondensing
Management	IMC - Intelligent Management Center; command-line interface; Web browser; SNMP Manager; Telnet; HTTPS; RMON1; FTP	
Features	Performance - 6.5Gbps Firewall Throughput - 1.8M Concurrent connection - 50K New connection per second - Max 20480 security policies - 2Gbps 3DES/AES VPN Throughput - 5000 IPSec tunnel - 4K VLAN Firewall operation mode - Routing mode - Transparent mode - Hybrid mode AAA service - Local Authentication - Standard Radius - HWTACACS+ - RADIUS domain Authentication ASPF - General TCP / UDP application - FTP/SMTP/HTTP/RTSP/H323 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 Firewall - 4 default Security Zone - Max 256 Security Zone NAT - NAPT - 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 start TCP Proxy when Detect SYN Flood
- ICMP Flood
- UDP Flood
- IP Spoofing
- SQL injection filter

L2TP VPN
- LNS,LAC
- L2TP Multi-instance

GRE
- GRE tunneling protocol

IPSec
- AH/ESP
- ESP
- Transport/tunnel
- NAT traversal
- Strategy template

IKE
- DH
- Pre-share Key authentication-method
- Support aggressive mode and main exchange mode
- IKE DPD, PKI / CA

Network Feature
- 802.1q VLAN
- 4K sub-interface
- Static and dynamic ARP
- Multicast, PIM
- IGMP v1/v2/v3

Routing
- RIP
- OSPF
- BGP
- Static Route
- policy Route

High Availability
- Active/Active mode
- Active/Passive mode
- Session Synchronization for Firewall

System management
- Web Management support IE/Firefox
- Command line interface (Console/Telnet/SSH)
- Classification Manager

- Unified management through iMC
- SNMPv1/v2c/v3

Administration
- Software Upgrades
- Configuration Backup and Restore

Logging/Monitoring
- Syslog
- Mini RMON
- NTP
- NAT/ASPF/firewall log stream(Binary log)

IPv6 Routing & Multicast
- RIPng
- OSPFv3
- BGP4+
- Static Route
- Policy Route
- PIM-SM/DM

IPv6 Security
- NAT-PT
- Manual tunnel
- IPV6 OVER ipv4 GRE tunnel
- 6to4 tunnel (RFC3056)
- ISATAP Tunnel
- IPv6 Packet Filter
- Radius
- NAT64

Services

3-year, parts only, global next-day advance exchange (UZ914E)
3-year, 4-hour onsite, 13x5 coverage for hardware (UZ915E)
3-year, 4-hour onsite, 24x7 coverage for hardware (UZ918E)
3-year, 4-hour onsite, 24x7 coverage for hardware, 24x7 SW phone support and SW updates (UZ922E)
3-year, 24x7 SW phone support, software updates (UZ925E)
1-year, post-warranty, 4-hour onsite, 13x5 coverage for hardware (HR740E)
1-year, post-warranty, 4-hour onsite, 24x7 coverage for hardware (HR741E)
1-year, post-warranty, 4-hour onsite, 24x7 coverage for hardware, 24x7 software phone support (HR742E)
4-year, 4-hour onsite, 13x5 coverage for hardware (UZ916E)
4-year, 4-hour onsite, 24x7 coverage for hardware (UZ919E)
4-year, 4-hour onsite, 24x7 coverage for hardware, 24x7 software phone (UZ923E)
4-year, 24x7 SW phone support, software updates (UZ926E)
5-year, 4-hour onsite, 13x5 coverage for hardware (UZ917E)
5-year, 4-hour onsite, 24x7 coverage for hardware (UZ920E)
5-year, 4-hour onsite, 24x7 coverage for hardware, 24x7 software phone (UZ924E)
5-year, 24x7 SW phone support, software updates (UZ927E)
3 Yr 6 hr Call-to-Repair Onsite (UZ928E)
4 Yr 6 hr Call-to-Repair Onsite (UZ929E)
5 Yr 6 hr Call-to-Repair Onsite (UZ930E)
1-year, 6 hour Call-To-Repair Onsite for hardware (HR744E)
1-year, 24x7 software phone support, software updates (HR743E)

Refer to the HP website at: www.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

IPv6
RFC 1981 IPv6 Path MTU Discovery
RFC 2460 IPv6 Specification
RFC 2465 Management Information Base for IP Version 6: Textual Conventions and General Group(partially 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
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 EAP 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 (GRE)
RFC 1702 Generic Routing Encapsulation over IPv4
networks.
RFC 1828 IP Authentication using Keyed MD5
RFC 1829 The ESP DES-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
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 "L2TP"
RFC 2784 Generic Routing Encapsulation (GRE)
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
RFC 4214 Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)

IKEv1
RFC 2407 The Internet IP Security Domain of Interpretation for ISAKMP
RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP).
RFC 2409 The Internet Key Exchange (IKE)
RFC 2412 The OAKLEY Key Determination Protocol
RFC 3526 More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)
RFC 3706 A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) 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 (CRL) Profile
draft-nourse-scep-06:
PKCS#1

and AH	PKCS#10
RFC 2404 The Use of HMAC-SHA-1-96 within ESP	PKCS#12
and AH	PKCS#7

To learn more, visit: www.hp.com/networking