

Overview

HP U200 Unified Threat Management (UTM) Appliance Series (Retired)

Models

HP U200-S UTM Appliance

JD273A

HP U200-A UTM Appliance

JD275A

Key features

- Flexible security zone and virtual firewall
- Advanced VPN
- Comprehensive threat protection
- Antivirus, antispam, and URL filtering options
- Intelligent Web-based management

Product overview

The HP U200 Unified Threat Management (UTM) Appliance Series comprises a group of purpose-built security devices designed to provide comprehensive protection for distributed environments such as branch offices and remote sites. Utilizing a state-of-the-art multicore platform and advanced hardware acceleration, the U200 UTM appliance series delivers robust protection against malicious attacks that could compromise networks and their critical assets. Sharing the same proven technology as the HP VPN Firewall Module Family, the U200 UTM appliance series provides protection against known threats such as malware and denial-of-service (DoS) attacks while providing optional services such as antivirus, antispam, and URL filtering capabilities. This provides manageable, flexible security options for organizations and their unique deployment needs.

Features and benefits

Application highlights

- **Enhanced firewall functions:** provide basic functions such as security zone configuration, static/dynamic blacklist, MAC-IP binding, and ACL application; offer enhanced functions like status-based filtering, virtual firewall, and transportation of IEEE 802.1Q-tagged packets; protect the network against attacks from ARP spoofing, invalid TCP flag, large ICMP packets, Challenge Collapsar (CC), SYN flooding, and address/port scanning
- **Abundant VPN features:** HP U200 UTM appliances support access through L2TP VPN, GRE VPN, and IPSec VPN and SSL VPN; the integrated hardware encryption engine implements VPN handling of high performance
- **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
- **Full support of NAT applications:** HP U200 UTM appliances support NAT applications, including many-to-one, many-to-many, static NAT, dual translation, easy IP, and DNS mapping; support NAT traversal with multiple protocols, and deliver NAT ALG functions such as DNS, FTP, H.323, and NBT
- **Real-time antivirus:** HP U200 UTM appliances adopt Kaspersky's antivirus engine to detect and remove codes of malicious attacks in a timely manner
- **Real-time spam filtering:** HP U200 UTM appliances filter spam in real time, which purifies mail systems
- **URL filtering:** HP U200 UTM appliances implement user-based URL access control to deny access to unauthorized websites
- **Enterprise-class high availability:** dual-box failover protects against loss of connectivity due to hardware failure, with automatic configuration and state table synchronization to simplify administration and remove scope for security policy inconsistencies

Management

- **Complete session logging:** provides detailed information for problem identification and resolution

QuickSpecs

Overview

- **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)

Warranty and support

- **1-year warranty:** with advance replacement and 30-calendar-day delivery (available in most countries)
- **Electronic and telephone support:** limited electronic and telephone support is available from HP; to reach our support centers, refer to <http://www.hp.com/networking/contact-support>; for details on the duration of support provided with your product purchase, refer to <http://www.hp.com/networking/warrantysummary>
- **Software releases:** to find software for your product, refer to <http://www.hp.com/networking/support>; for details on the software releases available with your product purchase, refer to <http://www.hp.com/networking/warrantysummary>

Technical Specifications

HP U200-S UTM Appliance (JD273A)

Ports	1 RJ-45 serial console port 5 auto-negotiating 10/100/1000 ports (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T) 1 Compact Flash port 1 module slot	
Physical characteristics	Dimensions	11.81(w) x 10.59(d) x 1.72(h) in (30 x 26.9 x 4.36 cm) (1U height)
	Weight	5.51 lb (2.5 kg)
Memory and processor	512 MB DDR2 SDRAM	
Performance	MAC address table size	4000 entries
Environment	Operating temperature	32°F to 113°F (0°C to 45°C)
	Operating relative humidity	10% to 95%, noncondensing
Electrical characteristics	Voltage	100-240 VAC
	Current	1.5 A
	Maximum power rating	54 W
	Frequency	50 / 60 Hz
	Notes	Maximum power rating and maximum heat dissipation are the worst-case theoretical maximum numbers provided for planning the infrastructure with fully loaded PoE (if equipped), 100% traffic, all ports plugged in, and all modules populated.
Safety	IEC 60950-1, Second Edition; UL60950-1, First Edition; EN60950-1, First Edition	
Emissions	VCCI Class B; EN 55022 Class B; ICES-003 Class B; FCC Part 15, Class B; EN 61000-3-2; EN 61000-3-3	
Management	IMC - Intelligent Management Center; command-line interface; Web browser; SNMP Manager; Telnet; HTTPS; FTP; Support HP A-IMC UTM Manager Software as unified management platform	
Notes	Performance	
	• 200 Mbps firewall throughput	
	• 60,000 concurrent connections under firewall mode/16,000 concurrent connections under UTM mode	
	• 6,000 new connections per second under firewall mode/2,000 new connections per second under UTM mode	
	• 1,000 security policies	
	• 100 Mbps 3DES/AES VPN throughput	
	• 100 IPsec tunnels	
	• 30 Mbps antivirus throughput	
Services	Refer to the HP website at: http://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.	

HP U200-A UTM Appliance (JD275A)

Ports	RJ-45 serial console port 6 auto-negotiating 10/100/1000 ports (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T) 1 Compact Flash port 2 module slots	
Physical characteristics	Dimensions	17.4(w) x 16.06(d) x 1.74(h) in (44.2 x 40.8 x 4.42 cm) (1U height)
	Weight	8.82 lb (4 kg)
Memory and processor	1 GB DDR2 SDRAM	

QuickSpecs

Technical Specifications

Performance	MAC address table size	4000 entries
Environment	Operating temperature	32°F to 113°F (0°C to 45°C)
	Operating relative humidity	10% to 95%, noncondensing
Electrical characteristics	Voltage	100-240 VAC
	Current	2.5 A
	Maximum power rating	100 W
	Frequency	50 / 60 Hz
	Notes	Maximum power rating and maximum heat dissipation are the worst-case theoretical maximum numbers provided for planning the infrastructure with fully loaded PoE (if equipped), 100% traffic, all ports plugged in, and all modules populated.
Safety	IEC 60950-1, Second Edition; UL60950-1, First Edition; EN60950-1, First Edition	
Emissions	VCCI Class B; EN 55022 Class B; ICES-003 Class B; FCC Part 15, Class B; EN 61000-3-2; EN 61000-3-3	
Management	IMC - Intelligent Management Center; command-line interface; Web browser; SNMP Manager; Telnet; HTTPS; FTP; Support HP A-IMC UTM Manager Software as unified management platform	
Notes	Performance	
	• 800 Mbps firewall throughput	
	• 500,000 concurrent connections under firewall mode/100,000 concurrent connections under UTM mode	
	• 10,000 new connections per second under firewall mode/5,000 new connections per second under UTM mode	
	• 10,000 security policies	
	• 400 Mbps 3DES/AES VPN throughput	
	• 1000 IPsec tunnels	
Services	• 100 Mbps antivirus throughput	
	Refer to the HP website at http://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 (applies to all products in series)

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)

VPN continued

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

Technical Specifications

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 and AH

RFC 2404 The Use of HMAC-SHA-1-96 within ESP and AH

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

PKCS#10

PKCS#12

PKCS#7

Features**Operating mode**

Routing mode

Transparent mode

Hybrid mode

AAA services

RADIUS authentication

HWTACACS authentication

PKI/CA (x.509 format) authentication

Domain authentication

CHAP authentication

PAP authentication

Firewall

Virtual firewall

Security zone configuration

Basic and extended ACLs

Interface-based access control

Time range-based access control

L2TP VPN

LNS, LAC

L2TP Multi-instance

GRE VPN**IPSec/IKE**

AH/ESP protocols

Manual SA setup or through IKE

ESP supports encryption algorithms of DES, 3DES, AES

Algorithms of MD5 and SHA-1

IKE main mode and aggressive mode

NAT traversal

DPD detection

IP services

IPv4/v6

ARP

Technical Specifications

Dynamic packet filtering
 ASPF packet filtering
 Static and dynamic blacklists
 MAC-IP binding
 MAC-based access control
 Transportation of 802.1Q-tagged packets

Anti virus

Virus definition-based detection
 Library upgrading manually and automatically
 Flow handing mode
 Supporting protocols of HTTP, FTP, SMTP, and POP3.
 Preventing virus types of Backdoor, Email-Worm, IM-Worm, P2P-Worm, Trojan, AdWare, Virus
 Supporting virus logs and reports

URL filtering

Custom-defined URL filtering library
 Supporting Java Blocking and ActiveX Blocking

Mail filtering

Blacklist of IP addresses
 Matching keywords of the mail address, attachment
 name, content, sender, and receiver

Security logs and statistics

User behavior flow logs
 NAT translation logs
 Real time logs of attacks
 Blacklist logs
 Address binding log
 Traffic alarm logs
 Traffic statistics and analysis
 Global/security zone-based connection rate monitoring
 Global/security zone-based protocol packet rate monitoring
 Events statistics
 E-mail notification of real-time alarms
 Information distribution through E-mail

NAT

NAPT
 PAT
 NAT Server
 Port mapping
 Bidirectional NAT
 Static NAT

Domain name resolution
 IP unnumbered
 DHCP relay
 DHCP server
 DHCP client

IP routing

Static routing
 RIP v1/2
 OSPF
 BGP (only for U200-A)
 Policy routing

High reliability (only for U200-A)

Active/Active mode
 Active/Passive mode
 Session Synchronization for Firewall

Attack prevention

DDoS
 DNS query/SYN/ICMP/UDP/ARP flood
 SYN cookie proxy SQL injection filtering
 IP/MAC binding
 IP spoofing detection
 ARP reverse query checking
 Management interfaces disabled by default

System and administration

Web interface via HTTP/HTTPS
 Command line interface via console, telnet, SSH
 RADIUS/TACACS+ server and local database authentication
 DNS support for dynamic IP allocation
 SNMP v1, 2c and 3

IPv6 Routing & Multicast

RIPng
 OSPFv3
 BGP4+ (only for U200-A)
 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

QuickSpecs

HP U200 Unified Threat Management (UTM) Appliance Series

Accessories

Memory	HP X600 1G Compact Flash Card	JC684A
	HP X600 512M Compact Flash Card	JC685A
	HP X600 256M Compact Flash Card	JC686A
HP U200-S UTM Appliance (JD273A)	HP U200-S 2-port Gig-T Module	JD265A
	HP U200-S 1-year Anti-Virus Service License	JG076A
	HP U200-S 1-year Anti-Spam Service LTU	JG075A
	U200-S 1-year URL Filter Service LTU	JG078A
HP U200-A UTM Appliance (JD275A)	HP U200-A 2-port Gig-T Module	JD266A
	HP U200-A 4-port GbE SFP Module	JD267A
	HP U200-A 1-year Anti-Spam Service License	JG064A
	HP U200-A 1-year Anti-Virus Service LTU	JG065A
	HP U200-A 1-year URL Filter Service LTU	JG067A

QuickSpecs

HP U200 Unified Threat Management (UTM) Appliance Series

Summary of Changes

Date	Version History	Action	Description of Change
24-Jul-2014	From Version 4 to 6	Changed	This QuickSpecs was retired; no further updates will be made.
25-Jul-2012	From Version 3 to 4	Changed	Updated the Specifications sections of each model.
14-Jun-2012	From Version 2 to 3	Changed	Updated the Specifications section.
26-Mar-2012	From Version 1 to 2	Changed	Updated the Accessories and Features and Benefits sections.

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

© Copyright 2015 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.