ZyWALL USG40/40W/60/60W
Unified Security Gateway

While technology has certainly simplified many aspects of our lives, there is more than one side the story. Advancements in how people work and collaborate can often create major challenges for small businesses. These include managing the rapidly growing number of smart devices accessing networks, prioritizing and blocking a wide range of cloud-based productivity applications, and guarding against daily web-based intrusions and attacks. As threats evolve and challenges diversify, it becomes more difficult for small businesses stay on top of these changes with limited IT resources at their disposal.

The ZyWALL USG40/40W/60/60W are all-in-one UTM firewalls specifically designed with comprehensive UTM features that including malware protection, application regulation, and budget control in small business environments. The built-in wireless AP (USG40W and USG60W) and WLAN controller offer instant wireless hotspot capability and future WLAN scalability. The Zyxel USG Series supports VPN, allowing businesses to securely access resources with their partner offices or headquarters. The all-in-one design integrates everything small businesses need, delivering easier and more centralized management with a lower total cost of ownership (TCO).

- All-in-one UTM Firewall for small businesses

- Complete network protection with Anti-Virus, Anti-Spam, Content Filtering 2.0, IDP and Application Patrol

- Robust SSL, IPSec and L2TP over IPSec VPN connectivity

- Express Mode with advanced Cloud Query technology

- Integrated single-radio (USG40W) or dual-radio (USG60W) wireless access point

- SecuReporter, cloud-based intelligent analytics and report service

ICSAlabs CERTIFIED ///Excellence in Information Security Testing Award

myZyxel   OneSecurity

ZYXEL | COMMUNITY BIZ FORUM

Benefits

Peace of mind security

The ZyWALL USG40/40W/60/60W delivers enterprise-grade UTM Firewall security without the hefty price tag. It provides deep, extensive protection and effective control of Web applications—like Facebook, Google Apps and Netflix—with such anti-malware protection mechanisms as firewall, Anti-Virus, Anti-Spam, Content Filtering, IDP and Application Patrol. Newly added Content Filtering 2.0 supports Geo IP Blocking to help propel detection rates from strength to strength. No longer do small businesses need to worry about threats, spam or social networking sites decreasing productivity.

Engineered Express Mode. Uncompromising performance.

ZyWALL USG series supports Express Mode with advanced Cloud Query technology which has 30 billion of file ID in Zyxel security cloud's database and constantly adapts new malware data every minute via Threat Intelligence Machine Learning. This innovative design improves the anti-malware detection efficiency, enables it to verify the file ID within seconds to get the most optimal threat detection, so that the ZyWALL USG series can gain higher throughput performance.

WiFi where you need it

Addressing the trend of BYOD, ZyWALL USG Series helps small businesses provide WiFi wherever there is demand. The USG40W and USG60W feature built-in single-radio and dual-radio wireless access points that can provide WiFi for small offices straight out of the box. An integrated WLAN controller with Zyxel AP Controller technology enables users to manage up to 18 access points from a centralized user interface. The USG Series enables businesses to easily provide WiFi in multiple other areas like reception areas and meeting rooms when WiFi demand grows.

Swift and secure firmware upgrades

Locating firmware updates — not to mention identifying correct versions for your device and managing their installation — can be a complex and confusing ordeal. ZyWALL USG Series solves this with its new Cloud Helper service. Cloud Helper provides a simple step to look for up-to-date firmware information. New firmware is immediately made available upon release from our official database to ensure its authenticity and reliability.

Enhanced visibility

SecuReporter is a cloud-based intelligent analytics and report service with data collection and correlation capabilities. USG is bundled with 1-year SecuReporter service, giving 7 days of log retention and visual analytics. SecuReporter provides multiple analytical perspectives on overall Threat Trend, Spam Mail, Unsafe Website Categories, Most Frequent Security Threat (Malware, IDP, Spam) and user behaviors, delivering holistic visibility for security professionals.

Simplified management procedure

Managing complex configuration settings can be confusing and time-consuming. ZyWALL USG Series provides an "easy mode" setting in the GUI for entry-level and SOHO users. Easy mode provides an icon-based feature set and attractive dashboard to simplify management and monitoring of the device. Application and function settings also have integrated wizards for user-friendly setup. ZyWALL USG Series easy mode helps entry-level users and SOHO users effortlessly take advantage of high-speed and secure networking.

Zyxel One Network experience

Aiming for relieving our customers from repetitive operations of deploying and managing a network, Zyxel One Network is designed to simplify the configuration, management, and troubleshooting, allowing our customers to focus on the business priorities. Zyxel One Network presents an easy-to-use tool, Zyxel One Network Utility (ZON Utility), to realize speed network setup. Zyxel Smart Connect allows Zyxel networking equipment to be aware and recognize each other and further facilitating the network maintenance via one-click remote functions such as factory reset or power cycling. Zyxel One Network redefines the network integration across multiple networking products from switch to WiFi AP and to Gateway.

ZyWALL USG Series Quick Finder

Model	USG40 /40W	USG60 /60W	USG110	USG210	USG310	USG1100	USG1900	USG2200
Description	SB		SMB			MB		
Firewall throughput (Mbps)	400	1,000	1,600	1,900	5,000	6,000	7,000	25,000
Max. concurrent sessions	50,000	100,000	150,000	200,000	500,000	1,000,000	1,000,000	1,500,000
UTM throughput (AV and IDP, Mbps)[1]	60	110	450	500	550	650	710	1,100
IDP throughput (Mbps)	95	150	590	660	900	1,000	1,200	2,000
AV throughput (Mbps)[1]	80	150	450	500	890	990	1,100	2,000
Amazon VPC[2]	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Microsoft Azure	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Cloud CNM SecuReporter[3]	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Hotspot Management[3]	-	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Device HA Pro	-	-	Yes	Yes	Yes	Yes	Yes	Yes

[1]: AV (with Express Mode) and IDP throughput measured using the industry standard HTTP performance test (1,460-byte HTTP packets). Testing done with multiple flows.
[2]: ZyWALL/USG still be able to support by CLIs
[3]: With Zyxel service license to enable or extend the feature capacity

Subscription Services

The ZyWALL USG40/40W/60/60W provides a complete feature set to perfectly fit different business requirements as well as to enable the maximum performance and security with an all-in-one appliance. Comprehensive network modularity also empowers IT professionals to customize the system to meet their individual needs.

*: Hotspot Management supports USG60/60W with firmware ZLD4.35 or later.

Anti-Virus	Anti-Spam	Intrusion Detection & Prevention	Application Patrol	Content Filtering 2.0	SecuReporter	AP Controller	Hotspot Management

Feature Highlights

Dual-WAN & Mobile broadband

The ZyWALL USG Series provides high Internet uptime with dual-WAN and mobile broadband support. Dual-WAN works with two Ethernet WAN connections for active-active load balancing or active-passive failover. Comprehensive mobile broadband USB modems are also supported for WAN backup.

Unified security policy

Unified security policy offers object-based management and a unified configuration interface for firewall and all security-related policies. Users can easily apply all policy criteria to every UTM feature, reduce configuration time, and get more streamlined policy management.

Cloud Helper

The Cloud helper provides friendly firmware upgrades so users don't need to worry about how and where to receive the latest firmware information and files. With just a few steps to download and update the firmware directly, it's very convenient and time-efficient.

Zyxel One Network utility

The ZON utility features smart functions to assist network management for administrators to perform batch firmware upgrade for devices, remote reboot of devices such as ceiling APs or redirect to device GUI for further configuration with just a click. These troublesome but necessary management tasks can now be easily done through just one platform for WiFi APs, switches and gateways.

Fanless

The ZyWALL USG Series features a robust fanless design to prevent dirt and dust from entering operating environments to cause potentially catastrophic failures. The fanless design of ZyWALL USGs offers zero-noise cooling and non-overheating features to ensure silent operation in small or quiet office environments.

Easy Mode

The ZyWALL USG Series provides friendly GUI to increase user experience, users can set up/configure device more quickly and enjoy high-speed and secure networking. Integrated Wizards help user to activate various application or functions quickly for the most used features.

Robust VPN

ZyWALL USG Series support high-throughput IPSec, L2TP over IPSec and SSL VPN for a wide range of site-to-client and site-to-site VPN deployments. Reinforced with the advanced SHA-2 authentication, the ZyWALL USG Series provide the most secure VPN for business communications.

Integrated WLAN controller

The integrated WLAN controller supports CAPWAP, and enables centralized authentication and access management of multiple APs in the network. ZyWALL USG40/40W/60/60W can manage 2 APs by default, and up to 18 APs with license upgrade.

Built-in Wireless AP

Built with single-radio and dual-radio wireless access points, the ZyWALL USG40W and USG60W are ideal for retail and office environments. The USG60W integrates 802.11 a/b/g/n technology that delivers WiFi over both the 2.4 GHz and the 5 GHz spectrums.

PCI DSS compliance

The Zyxel USG Series conforms to the Payment Card Industry Data Security Standard (PCI DSS), which is a global cardholder data security standard influential to a very broad group of businesses. The PCI Compliance applies to all entities such as merchants, card issuers, processors, and service providers involve in payment card processing tasks like validation, transmission and storage of cardholder data.
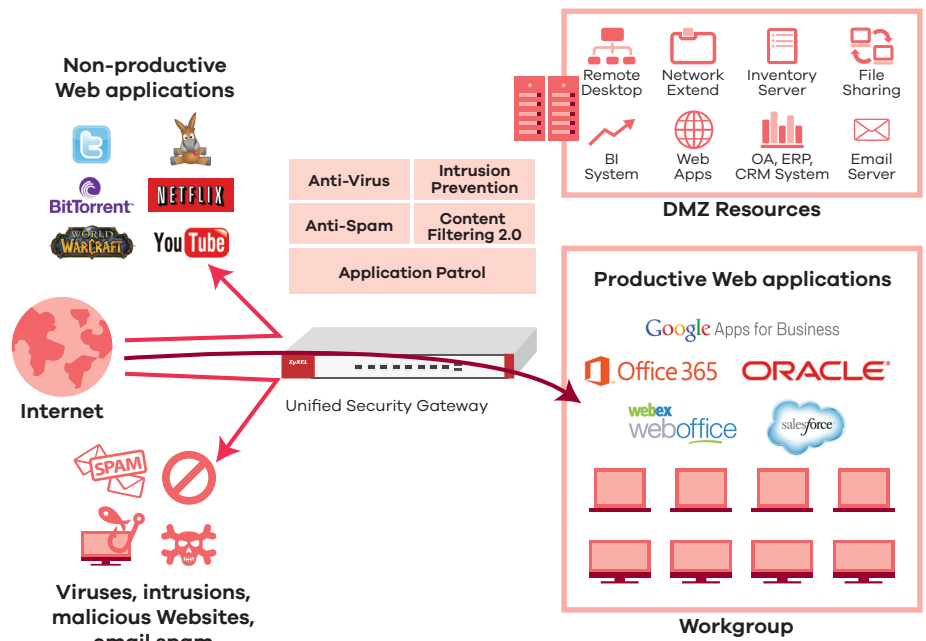
Security analytics and report

SecuReporter features a suite of analysis and reporting tools, including network security threats identification and visual analysis on security services statistics, security events, application usage, website usage, and traffic usage, and device health status. Users can also generate customized reports on-demand and setup a daily, weekly, or monthly schedule.

Application Diagram

Anti-malware protection and application optimization

- Enabling Anti-Virus, Anti-Spam and Intrusion Prevention, business networks gain deep, extensive protection against all types of malware threats
- Content Filtering 2.0 enables businesses to deny access to Websites that are malicious or not business-related
- Application Patrol technology not only enable businesses to block or throttle non-productive Web applications, but also optimize Web applications that increase productivity

Non-productive Web applications

Anti-Virus	Intrusion Prevention
Anti-Spam	Content Filtering 2.0
Application Patrol	

Internet

Unified Security Gateway

Viruses, intrusions, malicious Websites, email spam

DMZ Resources
- Remote Desktop
- Network Extend
- Inventory Server
- File Sharing
- BI System
- Web Apps
- OA, ERP, CRM System
- Email Server

Productive Web applications
- Google Apps for Business
- Office 365
- ORACLE
- webex weboffice
- salesforce

Workgroup

VPN application

- Branch offices, partners and home users can deploy ZyWALL Firewalls for site-to-site IPSec VPN connections
- Branch offices can additional deploy IPSec VPN HA (load balancing and failover) for always online VPN connectivity
- Remote users can securely access company resources with their computers or smartphones via SSL, IPSec and L2TP over IPSec VPN
- The headquarter ZyWALL USGs can also establish an IPSec VPN connection with Amazon VPC/ Microsoft Azure for secured access to a variety of cloud-based applications authenticity and reliability.
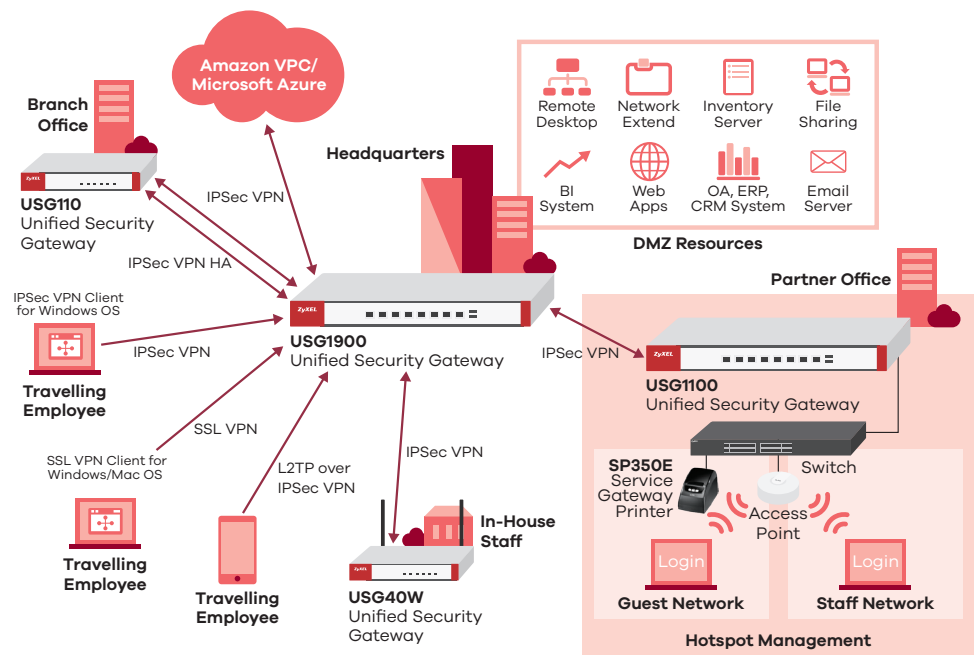
Hotspot management

- High speed internet access
- Tier of service
- Log record for regulatory compliance
- Premium security control
- Various Network access control (free or paid access, social login)

*: Hotspot Management supports USG60/60W with firmware ZLD4.35 or later

Branch Office
USG110 Unified Security Gateway

Amazon VPC/ Microsoft Azure

Headquarters

DMZ Resources
- Remote Desktop
- Network Extend
- Inventory Server
- File Sharing
- BI System
- Web Apps
- OA, ERP, CRM System
- Email Server

IPSec VPN
IPSec VPN HA

IPSec VPN Client for Windows OS

Travelling Employee — IPSec VPN

SSL VPN Client for Windows/Mac OS

Travelling Employee — SSL VPN

Travelling Employee — L2TP over IPSec VPN

USG1900 Unified Security Gateway

In-House Staff — IPSec VPN

USG40W Unified Security Gateway

IPSec VPN

Partner Office
USG1100 Unified Security Gateway

SP350E Service Gateway Printer

Switch
Access Point

Login **Guest Network**
Login **Staff Network**

Hotspot Management

Specifications

Model	USG40	USG40W	USG60	USG60W
Product photo				
Hardware Specifications				
Interfaces	3 x LAN/DMZ, 1 x WAN, 1 x OPT	3 x LAN/DMZ, 1 x WAN, 1 x OPT	4 x LAN/DMZ, 2 x WAN	4 x LAN/DMZ, 2 x WAN
USB ports	1	1	2	2
Console port	Yes (RJ-45)	Yes (RJ-45)	Yes (DB9)	Yes (DB9)
Rack-mountable	-	-	Yes	Yes
Fanless	Yes	Yes	Yes	Yes
System Capacity & Performance[1]				
SPI firewall throughput (Mbps)[2]	400	400	1,000	1,000
VPN throughput (Mbps)[3]	100	100	180	180
IDP throughput (Mbps)[4]	95	95	150	150
AV throughput (Mbps)[4]	80	80	150	150
UTM throughput (AV and IDP, Mbps)[4]	60	60	110	110
Max. TCP concurrent sessions[5]	50,000	50,000	100,000	100,000
Max. concurrent IPSec VPN tunnels[6]	20	20	40	40
Concurrent SSL VPN users (default/max.)[7]	20/30	20/30	20/60	20/60
VLAN interface	8	8	16	16
Concurrent devices logins (default/max.)[7][8]	64	64	200	200
Speedtest Performance				
SPI firewall throughput (Mbps)[9]	320	320	470	470
WLAN Management				
Managed AP number (default/max.)[7]	2/18	2/18	2/18	2/18
Recommend max. AP in 1 AP Group	10	10	10	10
Security Service				
Anti-Virus (AV)[7]	Yes	Yes	Yes	Yes
Intrusion Detection and Prevention (IDP) & Application Patrol[7]	Yes	Yes	Yes	Yes
Anti-Spam[7]	Yes	Yes	Yes	Yes
Content Filtering (CF 2.0)[7][10]	Yes	Yes	Yes	Yes
SecuReporter Premium[7]	Yes	Yes	Yes	Yes
Key Features				
VPN	IKEv2, IPSec, SSL, L2TP/IPSec	IKEv2, IPSec, SSL, L2TP/IPSec	IKEv2, IPSec, SSL, L2TP/IPSec	IKEv2, IPSec, SSL, L2TP/IPSec
SSL (HTTPS) inspection	-	-	-	-
2-Factor Authentication	Yes	Yes	Yes	Yes
EZ Mode	Yes	Yes	Yes	Yes
Hotspot Management[7]	-	-	Yes	Yes
Ticket printer support[11]/ Support Q'ty (max.)	-	-	Yes (SP350E)/10	Yes (SP350E)/10

Model		USG40	USG40W	USG60	USG60W
Microsoft Azure		Yes	Yes	Yes	Yes
Amazon VPC		Yes	Yes	Yes	Yes
Device HA Pro		-	-	-	-
Link Aggregation (LAG)		-	-	-	-
Power Requirements					
Power input		12 V DC, 2.0 A max.	12 V DC, 2.0 A max.	12 V DC, 2.5 A max.	12 V DC, 2.5 A max.
Max. power consumption (watt)		14	17	19	28
Heat dissipation (BTU/hr)		47.77	58.01	64.83	95.54
Physical Specifications					
Item	**Dimensions (WxDxH) (mm/in.)**	216 x 143 x 33/ 8.50 x 5.63 x 1.30	216 x 143 x 33/ 8.50 x 5.63 x 1.30	242 x 175 x 36/ 9.53 x 6.89 x 1.42	272 x 187 x 36/ 10.7 x 7.36 x 1.42
	Weight (kg/lb.)	0.89/1.96	0.91/2	1.25/2.76	1.46/3.23
Packing	**Dimensions (WxDxH) (mm/in.)**	381 x 261 x 79/ 15.00 x 8.50 x 3.11	381 x 261 x 79/ 15.00 x 8.50 x 3.11	394 x 240 x 101/ 15.51 x 9.45 x 3.98	427 x 247 x 73/ 16.81 x 9.72 x 2.87
	Weight (kg/lb.)	1.57/3.46	1.63/3.59	2.25/4.96	2.23 (W/O bracket) 2.42 (W/ bracket)
Included accessories		• Power adapter • DB9- RJ-45 for console connection	• Power adapter • DB9- RJ-45 for console connection • Antenna	• Power adapter • Rack mounting kit	• Power adapter • Rack mounting kit (optional, by regions) • Antenna
Environmental Specifications					
Operating	**Temperature**	0°C to 40°C/ 32°F to 104°F	0°C to 40°C/ 32°F to 104°F	0°C to 40°C/ 32°F to 104°F	0°C to 40°C/ 32°F to 104°F
	Humidity	10% to 90% (non-condensing)	10% to 90% (non-condensing)	10% to 90% (non-condensing)	10% to 90% (non-condensing)
Storage	**Temperature**	-30°C to 70°C/ -22°F to 158°F	-30°C to 70°C/ -22°F to 158°F	-30°C to 70°C/ -22°F to 158°F	-30°C to 70°C/ -22°F to 158°F
	Humidity	10% to 90% (non-condensing)	10% to 90% (non-condensing)	10% to 90% (non-condensing)	10% to 90% (non-condensing)
MTBF (hr)		414,329.4	386,931.7	815,463.9	497,644
Certifications					
EMC		FCC Part 15 (Class B), CE EMC (Class B), C-Tick (Class B), BSMI	FCC Part 15 (Class A), CE EMC (Class A), C-Tick (Class A), BSMI	FCC Part 15 (Class B), CE EMC (Class B), C-Tick (Class B), BSMI	FCC Part 15 (Class A), CE EMC (Class A), C-Tick (Class A), BSMI
Safety		LVD (EN60950-1), BSMI	LVD (EN60950-1), BSMI	LVD (EN60950-1), BSMI	LVD (EN60950-1), BSMI

Note:
*: This matrix with firmware ZLD4.38 or later.
*1: Actual performance may vary depending on network conditions and activated applications
*2: Maximum throughput based on RFC 2544 (1,518-byte UDP packets).
*3: VPN throughput measured based on RFC 2544 (1,424-byte UDP packets).
*4: AV (with Express Mode) and IDP throughput measured using the industry standard HTTP performance test (1,460-byte HTTP packets). Testing done with multiple flows.
*5: Maximum sessions measured using the industry standard IXIA IxLoad testing tool.
*6: Including Gateway-to-Gateway and Client-to-Gateway.
*7: With Zyxel service license to enable or extend the feature capacity.
*8: This is the recommend maximum number of concurrent logged-in devices.
*9: The Speedtest result is conducted with 1 Gbps WAN link in real world and it is subject to fluctuate due to quality of the ISP link.
*10: SafeSearch function in CF need to enable SSL inspection firstly and not for small business.
*11: With Hotspot Management license support.

Wireless Specifications

Model		USG40W	USG60W
Standard compliance		802.11 b/g/n	802.11 a/b/g/n
Wireless frequency		2.4 GHz	Concurrent 2.4 & 5 GHz
Radio		1	2
SSID number		8	16
Maximum transmit power (Max. total channel)	US (FCC) 2.4 GHz	24.3 dBm, 2 antennas	24.3 dBm, 2 antennas
	US (FCC) 5 GHz	-	25.8 dBm, 2 antennas
	EU (ETSI) 2.4 GHz	19.6 dBm (EIRP), 2 antennas	18.6 dBm (EIRP), 2 antennas
	EU (ETSI) 5 GHz	-	28.4 dBm (EIRP), 2 antennas
No. of antenna		2.4 GHz: 2T2R MIMO (Detachable, SMA-R)	2.4 GHz: 2T2R MIMO 5 GHz: 2T2R MIMO (Detachable, SMA-R)
Antenna gain		3 dBi	3 dBi
Data rate		• 802.11b/g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48 and 54 Mbps • 802.11n: up to 300 Mbps in MCS15 (40 MHz; GI = 400 ns)	• 802.11b/g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48 and 54 Mbps • 802.11a: 6, 9, 12, 18, 24, 36, 48 and 54 Mbps • 802.11n: up to 300 Mbps in MCS15 (40 MHz; GI = 400 ns)
Frequency Band	2.4 GHz (IEEE 802.11 b/g/n)	• USA (FCC): 2.412 to 2.462 GHz • Europe (ETSI): 2.412 to 2.472 GHz • TWN (NCC): 2.412 to 2.462 GHz	• USA (FCC): 2.412 to 2.462 GHz • Europe (ETSI): 2.412 to 2.472 GHz • TWN (NCC): 2.412 to 2.462 GHz
	5 GHz (IEEE 802.11 a/n)	-	• USA (FCC): 5.150 to 5.250 GHz; 5.725 to 5.850 GHz • Europe (ETSI): 5.15 to 5.35 GHz; 5.470 to 5.725 GHz • TWN (NCC): 5.25 to 5.35 GHz; 5.725 to 5.850 GHz
Receive sensitivity	2.4 GHz	11 Mbps ≤ -87 dBm 54 Mbps ≤ -77 dBm HT20, MCS15 ≤ -71 dBm HT40, MCS15 ≤ -68 dBm	11 Mbps ≤ -87 dBm 54 Mbps ≤ -74 dBm HT20 ≤ -71 dBm HT40 ≤ -68 dBm
	5 GHz	-	54 Mbps ≤ -75 dBm HT20, MCS15 ≤ -71 dBm HT40, MCS15 ≤ -69 dBm

Features Set

Software Features

Firewall
• ICSA-certified corporate firewall
• Routing and transparent (bridge) modes
• Stateful packet inspection
• User-aware policy enforcement
• SIP/H.323 NAT traversal
• ALG support for customized ports

• Protocol anomaly detection and protection
• Traffic anomaly detection and protection
• Flooding detection and protection
• DoS/DDoS protection
• RPS-enabled for desirable performance in chaotic environments

IPv6 Support
• Dual stack
• IPv4 tunneling (6rd and 6to4 transition tunnel)
• IPv6 addressing
• DNS
• DHCPv6
• Bridge
• VLAN
• PPPoE

- Static routing
- Policy routing
- Session control
- Firewall and ADP
- IPSec VPN
- Intrusion Detection and Prevention (IDP)
- Application Patrol
- Content Filtering 2.0
- Anti-Virus, Anti-Malware
- Anti-Spam

IPSec VPN
- Encryption: AES (256-bit), 3DES and DES
- Authentication: MD5, SHA1, SHA2 (512-bit)
- Key management: IKEv1 (x-auth, mode-config), IKEv2 (EAP, configuration payload)
- Perfect forward secrecy (DH groups) support 1, 2, 5, 14, 15
- IPSec NAT traversal (NAT-T)
- Dead peer detection and relay detection
- PSK and PKI (X.509) certificate support
- VPN concentrator
- Support Route-based VPN Tunnel Interface (VTI)
- Simple wizard support
- VPN auto-reconnection
- VPN High Availability (HA): load-balancing and failover
- L2TP over IPSec
- GRE and GRE over IPSec
- NAT over IPSec
- Zyxel VPN client provisioning
- Support iOS L2TP/IKE/IKEv2 VPN Client provision

SSL VPN
- Supports Windows and Mac OS X
- Supports full tunnel mode
- Supports 2-step authentication

Intrusion Detection and Prevention (IDP)
- Routing and transparent (bridge) mode
- Signature-based and behavior-based scanning
- Automatic signature updates
- Customizable protection profile
- Customized signatures supported

Application Patrol
- Granular control over the most important applications
- Identifies and controls application behavior

- Supports over 15 application categories
- Application bandwidth management
- Supports user authentication
- Real-time statistics and reports
- IDP/ADP support on social networks such as likes and posts on Facebook

Anti-Virus
- Stream-based scan engine (Stream Mode)
- HTTP, FTP, SMTP, POP3, and IMAP4 protocol supported
- No file size limitation
- Automatic signature updates
- Newly added hash-based cloud query technology (Express Mode)
- Works with local cache and over 30 billion database and still growing
- HTTP, HTTPS, and FTP protocol supported
- Multiple file types supported

Anti-Spam
- Transparent mail interception via SMTP and POP3 protocols
- Configurable POP3 and SMTP ports
- Sender-based IP reputation filter
- Recurrent Pattern Detection (RPD) technology
- Zero-hour virus outbreak protection
- X-Header support
- Blacklist and whitelist support
- Supports DNSBL checking
- Spam tag support
- Statistics report

Content Filtering 2.0
- Social media filtering
- Malicious Website filtering
- URL blocking and keyword blocking
- Blacklist and whitelist support
- Blocks java applets, cookies and ActiveX
- Dynamic, cloud-based URL filtering database
- Unlimited user license support
- Customizable warning messages and redirection URL
- HTTPs Domain filtering
- GeoIP Blocking
- Monitors traffics based on country policy
- URL blocking and keyword blocking

Unified Security Policy
- Unified policy management interface
- Supported UTM features: Anti-Virus, Anti-Spam, IDP, Content Filtering 2.0, Application Patrol, firewall (ACL)

- 3-tier configuration: object-based, profile-based, policy-based
- Policy criteria: zone, source and destination IP address, user, time
- Pre-defined UTM profiles for different user groups

WLAN Management
- Support AP Controller (APC) version 3.40
- Wireless L2 isolation
- Supports auto AP FW update
- Scheduled WiFi service
- Dynamic Channel Selection (DCS)
- Client steering for 5GHz priority and sticky client prevention
- Auto healing provides a stable and reliable coverage
- IEEE 802.1x authentication
- Captive portal Web authentication
- Customizable captive portal page
- RADIUS authentication
- WiFi Multimedia (WMM) wireless QoS
- CAPWAP discovery protocol
- Multiple SSID with VLAN
- Supports ZyMesh
- Support AP Forward Compatibility

Hotspot Management*
- Integrated account generator, Web-based authentication portal and billing system
- Supports external RADIUS servers
- Per account bandwidth management
- User agreement login
- SP350E Service Gateway Printer enables one-click account and billing generation
- Built-in billing system
  - Time-to-finish accounting mode
  - Accumulation accounting mode
- Supports PayPal online payment
- Marketing tool
  - Advertisement link
  - Walled garden
  - Portal page
- Billing Replenish

* Supports USG60/60W with firmware ZLD4.35 or later

Mobile Broadband
- WAN connection failover via 3G and 4G* USB modems
- Auto fallback when primary WAN recovers

* For specific models supporting the 3G and 4G dongles on the list, please refer to the Zyxel product page at 3G dongle document.

Networking
- Routing mode, bridge mode and hybrid mode
- Ethernet and PPPoE
- NAT and PAT
- VLAN tagging (802.1Q)
- Virtual interface (alias interface)
- Policy-based routing (user-aware)
- Policy-based NAT (SNAT)
- Dynamic routing (RIPv1/v2 and OSPF)
- DHCP client/server/relay
- Dynamic DNS support
- WAN trunk for more than 2 ports
- Per host session limit
- Guaranteed bandwidth
- Maximum bandwidth
- Priority-bandwidth utilization
- Bandwidth limit per user
- Bandwidth limit per IP
- GRE
- BGP

Authentication
- Local user database
- Microsoft Windows Active Directory integration
- External LDAP/RADIUS user database
- XAUTH, IKEv2 with EAP VPN authentication
- Web-based authentication
- Forced user authentication (transparent authentication)
- IP-MAC address binding
- SSO (Single Sign-On) support
- Supports 2-Factor authentication

System Management
- Role-based administration
- Multiple administrator logins
- Supports Cloud Helper
- Multi-lingual Web GUI (HTTPS and HTTP)
- Command line interface (console, Web console, SSH and telnet)
- SNMP v1, v2c, v3
- System configuration rollback
- Firmware upgrade via FTP, FTP-TLS and Web GUI
- Dual firmware images
- Cloud CNM SecuManager

Logging and Monitoring
- Comprehensive local logging
- Syslog (to up to 4 servers)
- Email alerts (to up to 2 servers)
- Real-time traffic monitoring
- Built-in daily report
- Cloud-based analytics and reporting with SecuReporter

Zyxel One Network
- ZON Utility
  - IP configuration
  - Web GUI access
  - Firmware upgrade
  - Password configuration
- Smart Connect
  - Location and system name update
  - Discover neighboring devices
  - One-click remote management access to the neighboring Zyxel devices

Licenses

Security

Product	Anti-Virus	Application Patrol & IDP	Content Filtering 2.0	Anti-Spam	SecuReporter Premium
USG40/40W	1 year/2 years	1 year/2 years	1 year/2 years	1 year/2 years	1 year/2 years
USG60/60W	1 year/2 years	1 year/2 years	1 year/2 years	1 year/2 years	1 year/2 years

1. Zyxel USGs can be purchased with bundled 12-month standard license (Anti-Virus, Anti-Spam, Content Filtering, IDP and SecuReporter) with extra 1-month trial.
2. Licenses can be easily activated, renewed and managed at myZyxel.
3. License bundles may vary according to region. Please contact your local sales representative for more information.

Connectivity & Industrial Solution

Product	SSL VPN Tunnels	SSL VPN Client*	IPSec VPN Client
USG40/40W	Add 5/10 tunnels	For 1/5/10 client(s)	For 1/5/10/50 client(s)
USG60/60W	Add 5/10 tunnels	For 1/5/10 client(s)	For 1/5/10/50 client(s)

*: Support OS: MAC OS 10.7 or later

Product	Hotspot Management	Managed APs
USG40/40W	-	Add 2/4/8 APs
USG60/60W*	1 year/One-time	Add 2/4/8 APs

*: Support Hotspot Management feature since ZLD4.35 or later

Access Point Compatibility List

Product	Unified AP		Unified Pro AP	
Models	• NWA5121-NI • NWA5121-N • NWA5123-NI • NWA5123-AC	• NWA5123-AC HD • NWA5301-NJ • WAC5302D-S • WAX510D*	• WAC6103D-I • WAC6303D-S • WAC6502D-E • WAC6502D-S	• WAC6503D-S • WAC6552D-S • WAC6553D-E • WAX650S*
Functions				
Central management	Yes		Yes	
Auto provisioning	Yes		Yes	
Data forwarding	Local bridge		Local bridge/Data tunnel	
ZyMesh	Yes		Yes	

*: From APC3.0, commercial gateways supporting APC technology are able to recognize APs with FW release higher than APC3.0 as Forward Compatible APs. Resellers can introduce newly-available Zyxel APs with basic features supported without upgrading any new controller firmware.

Accessories

SecuExtender Software

Item	Description	Supported OS
IPSec VPN Client*	IPSec VPN client software for the ZyWALL and USG Series with Easy VPN for zero-configuration remote access	• Windows XP (32-bit) • Windows Server 2003 (32-bit) • Windows Server 2008 (32/64-bit) • Windows Vista (32/64-bit) • Windows 7 (32/64-bit) • Windows 8 (32/64-bit) • Windows 10 (32/64-bit)
SSL VPN Client*	Secured VPN connection between PC/MAC and ZyWALL Firewall	• Windows 7 (32/64-bit) • Windows 8/8.1 (32/64-bit) • Windows 10 (32/64-bit) • MAC OS 10.7 or later

*: A 30-day trial version of IPSec VPN client and SSL VPN client for MAC OS can be downloaded from official Zyxel website. To continue using the application, please contact your regional sales representatives and purchase a commercial license for the application.

ZYXEL

NETWORKS

Datasheet ZyWALL USG40/40W/60/60W